

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



**CASIG 1 – Gobierno de la Ciberseguridad**

**Preguntas de Auditoría**

**Monitorear la Optimización de Valor**

|  |
| --- |
| **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 optimización del valor en la gestión de seguridad de la información y ciberseguridad (SIC) incluye la definición de un conjunto equilibrado de objetivos, métricas y benchmarks que permitan evaluar tanto el avance como los retrasos, incluyendo mediciones financieras y no financieras. La colaboración con TI y otras funciones empresariales, así como con partes interesadas clave, permite acordar métricas claras y un sistema de seguimiento integral. Recopilar y analizar datos precisos y oportunos permite obtener una vista completa del rendimiento de los portafolios y programas de SIC, asegurando que los resultados se alineen con los objetivos comerciales establecidos.

**1.1 Procedimientos de Monitoreo y Evaluación de Resultados**

Para lograr un monitoreo efectivo de los activos y recursos de SIC, es esencial desarrollar y documentar procesos específicos para evaluar la entrega de valor en relación con los objetivos comerciales. Esto incluye recopilar informes periódicos de rendimiento y realizar comparaciones entre los resultados obtenidos y las expectativas para asegurar que se cumplan los objetivos estratégicos. Además, la implementación de un sistema robusto de gestión de datos facilita el análisis de desempeño y permite la identificación de patrones y oportunidades de mejora continua. El análisis cuantitativo y comparativo, junto con las técnicas avanzadas de análisis de datos, aporta una comprensión profunda de las tendencias en la optimización de valor, ayudando a realizar ajustes basados en datos y a tomar decisiones informadas para mejorar la eficiencia y el valor de SIC.

**1.2 Rol de la Auditoría en la Optimización de Valor de los Activos y Recursos de SIC**

Desde la perspectiva de auditoría, el monitoreo de la optimización de valor en SIC implica una evaluación continua de los procesos y sistemas de monitoreo implementados, verificando su alineación con las mejores prácticas y objetivos de la organización. La auditoría revisa los hallazgos documentados en los informes de monitoreo, asegurando que se adopten y controlen las acciones correctivas necesarias para optimizar el valor de los activos y recursos. Además, el proceso de auditoría fomenta la mejora continua mediante un sistema de revisión basado en datos y resultados, permitiendo que SIC se adapte de forma proactiva a los cambios en el entorno y maximice su contribución al éxito empresarial. Este enfoque asegura que la optimización de valor se mantenga como una prioridad, reforzando la capacidad de SIC para apoyar los objetivos organizacionales a largo plazo.

# 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 Optimización de Valor**

|  |
| --- |
| 3.1 Temática: Revisión de la estrategia, objetivos y métricas de la SIC |
| El objetivo principal de esta revisión es garantizar que la estrategia de SIC esté alineada con los objetivos generales de la organización y sea integral en su alcance. Esto implica asegurar que la SIC no sea simplemente una función reactiva para responder a incidentes de seguridad, sino que sea un componente estratégico y proactivo que se adelante a posibles amenazas. La revisión debe asegurar que los objetivos de SIC sean claros, medibles y relevantes, y que se alineen con las metas generales de la organización en términos de protección de datos, continuidad del negocio y cumplimiento normativo.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe documentación de la estrategia y objetivos de seguridad de la información y ciberseguridad? * ¿Se utilizan métricas apropiadas y específicas para permitir el monitoreo efectivo del valor de las inversiones en SIC?   + ¿Se mencionan métricas financieras y no financieras en la documentación?   + ¿Las métricas incluyen indicadores de avance y retraso, rendimiento y puntos de referencia?   + Verifique que se incluyen métricas suficientes y precisas, tales como:     - Número de nuevas oportunidades empresariales logradas como resultado directo de los desarrollos de I&T     - Porcentaje de objetivos empresariales estratégicos obtenidos como resultado de iniciativas estratégicas de I&T     - Nivel de satisfacción de la dirección ejecutiva con el coste y la entrega de valor de I&T     - Nivel de satisfacción de las partes interesadas con el avance hacia las metas identificadas (entrega de valor basada en encuestas)     - Nivel de satisfacción de las partes interesadas con la capacidad de la empresa para obtener valor de las iniciativas habilitadas por I&T     - Número de incidentes que tienen lugar debido a la evasión actual o intentada de los principios y prácticas de gestión de valor establecidos     - Porcentaje logrado del valor esperado * ¿Se considera adecuadamente el costo de incidentes de seguridad, impacto en la productividad, satisfacción del cliente y reducción de riesgos? * ¿Las métricas cubren mediciones de actividad (inputs) y resultados (outputs)? * ¿Están alineadas las métricas con la estrategia empresarial y métricas de otras áreas? |

|  |
| --- |
| 3.2 Temática: Revisión de procedimientos de recopilación de datos de rendimiento |
| Al revisar los procedimientos de recopilación de datos de rendimiento la organización asegura que los datos obtenidos sean relevantes y representativos de los aspectos críticos del rendimiento de la organización. Esto implica definir claramente qué datos son necesarios para medir el progreso hacia los objetivos establecidos y cómo se deben recopilar. La revisión también busca verificar que los métodos de recopilación sean confiables y consistentes, garantizando que los datos sean comparables y que se puedan detectar tendencias y patrones a lo largo del tiempo.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe documentación de los procedimientos para recopilar datos de rendimiento del portafolio, programa y SIC? * ¿Se han definido claramente los datos necesarios, métodos de recopilación y fuentes de datos utilizadas? * ¿Los datos recopilados son relevantes para evaluar el progreso y la entrega de valor? * ¿Se capturan datos relacionados con los objetivos establecidos y su utilidad en la toma de decisiones? * ¿Los datos se recopilan de manera oportuna y completa, siguiendo plazos definidos? * ¿Se han implementado controles de calidad de datos, como verificaciones y auditorías, para garantizar su credibilidad y precisión? |

|  |
| --- |
| 3.3 Temática: Revisión de informes periódicos de rendimiento |
| Estos informes son herramientas clave para evaluar el progreso, identificar tendencias y tomar decisiones estratégicas basadas en datos objetivos. La revisión periódica de estos informes asegura que la alta dirección y otros stakeholders tengan una visión clara y precisa del rendimiento de la organización en diferentes áreas y niveles.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se generan informes periódicos para evaluar el rendimiento del portafolio, programa y SIC? * ¿Los informes abordan aspectos clave desde una perspectiva tecnológica y funcional? * ¿Se incluyen métricas relevantes y datos que permitan evaluar el grado de realización de los objetivos planificados? * ¿Los informes brindan una visión clara y detallada del progreso hacia las metas establecidas? |

|  |
| --- |
| 3.4 Temática: Revisión del uso de KPIs |
| Revisar el uso de KPIs busca asegurar que los indicadores elegidos sean relevantes, medibles y accionables. Los KPIs deben proporcionar información valiosa y útil para tomar decisiones informadas y mejorar el rendimiento en áreas clave. La revisión busca verificar que los KPIs estén definidos con claridad y que sean representativos de los resultados que se desean alcanzar.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se han identificado KPI’s relevantes para medir el desempeño de las iniciativas de seguridad? * ¿Se recolectan datos relacionados con el rendimiento de las iniciativas de seguridad y se comparan con los KPI’s establecidos? ¿Se generan informes que incluyan comparativas, tendencias y datos históricos? * ¿Las iniciativas de seguridad contribuyen a los objetivos comerciales y generan valor agregado? * ¿Se toman medidas de gestión adecuadas en caso de desviaciones o áreas de mejora identificadas? * ¿Se utilizan KPI’s específicos para medir el impacto de las acciones de mejora implementadas? * ¿Se comparan los resultados con benchmarks externos para identificar áreas de mejora? |

|  |
| --- |
| 3.5 Temática: Análisis de procesos y procedimientos de monitoreo |
| El objetivo principal del análisis de procesos y procedimientos de monitoreo es evaluar la efectividad de los métodos de monitoreo utilizados y asegurar que sean adecuados para medir y evaluar el rendimiento de manera precisa. Esto incluye verificar si los indicadores y métricas utilizados son relevantes y apropiados para medir los resultados deseados. También se busca asegurar que los procesos de monitoreo sean confiables y consistentes, proporcionando información oportuna y precisa para la toma de decisiones.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe documentación detallada sobre los procesos y procedimientos de monitoreo de activos y recursos de SIC? * ¿Los documentos abarcan todos los aspectos críticos del monitoreo, como identificación de activos, criterios de monitoreo, proceso en sí, responsabilidades y acciones correctivas? * ¿Los procesos y procedimientos están claramente definidos y estructurados para su comprensión y seguimiento por el personal involucrado? |

|  |
| --- |
| 3.6 Temática: Monitoreo de la infraestructura tecnológica y calidad de datos |
| El análisis de procesos y procedimientos de monitoreo busca evaluar la efectividad de los métodos de monitoreo utilizados y asegurar que sean adecuados para medir y evaluar el rendimiento de manera precisa. Esto incluye verificar si los indicadores y métricas utilizados son relevantes y apropiados para medir los resultados deseados. También se busca asegurar que los procesos de monitoreo sean confiables y consistentes, proporcionando información oportuna y precisa para la toma de decisiones.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se cuenta con la infraestructura tecnológica adecuada para la gestión de datos de monitoreo? * ¿Los datos recopilados tienen una alta calidad en términos de precisión, integridad y actualización? * ¿Se utilizan técnicas avanzadas de análisis de datos para evaluar el rendimiento y optimización del valor? |

|  |
| --- |
| 3.7 Temática: Plan estratégico de monitoreo a largo plazo |
| Mantener un plan estratégico de monitoreo a largo plazo es esencial para una gestión efectiva de la ciberseguridad y la tecnología de la información. Proporciona una guía clara y coherente para asegurar la seguridad y el rendimiento de los sistemas y servicios, mejorar la toma de decisiones y promover la mejora continua en la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿El plan estratégico de la función de SIC incluye una sección dedicada al monitoreo a largo plazo de activos y recursos? * ¿Se establecen objetivos específicos, indicadores de desempeño y cronogramas para el monitoreo continuo? * ¿El plan abarca todos los activos asignados a la función de SIC, incluyendo sistemas, redes, bases de datos, equipos y personal? * ¿Se define la frecuencia y duración de los procesos de monitoreo a largo plazo con plazos de revisión y actualización? |

|  |
| --- |
| 3.8 Temática: Revisión de la mejora continua |
| El objetivo principal de la revisión de la mejora continua es evaluar el impacto y los resultados de las iniciativas de mejora implementadas. Esto implica analizar los datos y métricas relevantes para determinar si las acciones tomadas han logrado los resultados esperados y si han generado un valor agregado para la organización. Si bien la mejora continua busca pequeños cambios graduales, la revisión busca asegurar que esos cambios estén teniendo un impacto positivo y significativo.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe documentación detallada de los procesos y sistemas de monitoreo utilizados, así como de las acciones tomadas en respuesta a evaluaciones y revisiones? * ¿Se sigue un ciclo de mejora continua en los procesos y sistemas de monitoreo? * ¿Se llevan a cabo revisiones periódicas de los activos y recursos con criterios de evaluación definidos? * ¿Las decisiones de optimización se basan en datos y resultados recopilados con métricas relevantes? |