Pantalla de computadora con imágen de hombre

Descripción generada automáticamente con confianza media

**CASIG 1 – Gobernanza de la Ciberseguridad**

**Preguntas de Auditoría**

**Establecer el Objetivo de Inversión en SIC**

1. Visión General

Definir un objetivo de inversión en ciberseguridad requiere crear y mantener un portafolio de programas de inversión habilitados por los activos y servicios de TI y SIC, formando una base sólida para el presupuesto de seguridad y permitiendo decisiones bien informadas que respaldan la infraestructura y el cumplimiento de la estrategia empresarial. A través de una comunicación clara entre SIC y otras funciones de la empresa, se logra una comprensión compartida de cómo las inversiones en seguridad pueden contribuir a las prioridades generales de recursos y decisiones de inversión de la organización.

* 1. **Estructura y Balance en la Estrategia de Inversión de SIC**

Para garantizar que las inversiones se alineen con los objetivos de la organización, es esencial establecer una mezcla balanceada de inversión en ciberseguridad que abarque dimensiones como resultados a corto y largo plazo, beneficios financieros y no financieros, y niveles de riesgo adecuados. Esto implica identificar las categorías de sistemas, aplicaciones, servicios de TI, y activos de SIC necesarios para respaldar las metas estratégicas, manteniendo además un inventario actualizado de activos de TI para la evaluación continua de necesidades. El establecimiento de un comité de inversión en seguridad o la delegación de estas responsabilidades a un comité estratégico asegura que las decisiones de inversión estén orientadas a las mejores opciones para construir y mejorar la infraestructura de TI y SIC. Asimismo, es importante desarrollar políticas y procedimientos que integren las inversiones en SIC con la estrategia empresarial, considerando sinergias con otras unidades y aprovechando los aportes de los líderes de TI y otros departamentos para maximizar el cumplimiento de los objetivos de cada unidad organizativa.

**1.3 Rol de la Auditoría en la Revisión y Mejora Continua de la Estrategia de Inversión**

Desde el enfoque de auditoría, la supervisión de la estrategia de inversión en SIC requiere un proceso de revisión continua para asegurar su vigencia y efectividad en relación con los objetivos de la organización. Los auditores evalúan las métricas y metas cuantitativas establecidas para las inversiones en SIC, verificando que se realicen análisis de riesgos y que las decisiones de inversión se ajusten a los controles de valor definidos. Además, la auditoría proporciona retroalimentación basada en los resultados de las revisiones y auditorías previas, permitiendo mejoras en la estrategia de inversión y la mezcla de recursos destinados a SIC. Este enfoque de monitoreo y mejora continua facilita una gestión optimizada de la seguridad de la información, asegurando que la organización maximice el valor de sus inversiones y mantenga una estructura de seguridad robusta y alineada con las mejores prácticas.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Crear y mantener portafolios de programas de inversión habilitados por SIC, servicios y activos de TI, que forman la base para el presupuesto actual de seguridad, que respalden las decisiones clave para llevar a cabo los planes tácticos y estratégicos de SIC.  1.1 Cualquier activo, ya sea sistema o infraestructura, debe adquirirse de manera apropiada e incluir la documentación adecuada, al tiempo que se debe asegurar que se obtienen las capacidades requeridas.  2. Obtener un conocimiento común entre SIC y otras funciones empresariales sobre las posibles oportunidades para que la función de seguridad habilite y contribuya en las prioridades de recursos, iniciativas y decisiones generales de inversión para el cumplimiento de la estrategia empresarial.  3. Identificar las categorías generales de sistemas de información, aplicaciones, datos, servicios de TI, infraestructura, activos de SIC, recursos, habilidades, prácticas, controles y relaciones de TI necesarias para respaldar la estrategia empresarial.  4. Identificar y registrar los requisitos de las partes interesadas (como accionistas, reguladores, auditores y clientes) para proteger sus intereses y entregando valor a través de la actividad de seguridad de la información. Establezca la dirección en consecuencia.  5. Asegurar que la organización mantiene un inventario de activos de TI. [Ver Control: Inventario de Activos de TI] |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Definir una mezcla de inversión que logre el equilibrio adecuado entre distintas dimensiones, incluido un equilibrio adecuado de resultados a corto y largo plazo, beneficios financieros y no financieros, inversiones de alto y bajo riesgo y actividades de seguridad de la información que respalden las mejores opciones para proveerse de la infraestructura de TI necesarias para SIC y para desarrollar las propuestas aprobadas.  2. Establecer un comité responsable de la mezcla de inversión en seguridad, o delegar la autoridad y función a los comités estratégicos o ejecutivos de SIC para definir la estrategia de inversión y evaluar opciones de mejora.  3. Desarrollar políticas, procesos y procedimientos para determinar las inversiones propuestas en materias de seguridad de la información.  3.1 Asegurar que los procesos y políticas integran la inversión en SIC con la estrategia empresarial.  4. Acordar las metas de SIC, tener en cuenta las interrelaciones entre la estrategia de la empresa y los servicios de SIC, activos y otros recursos. Identificar y aprovechar las sinergias que pueden lograrse. Se debe tener en cuenta los puntos de vista de los lideres de las unidades organizativas y otros líderes de TI para determinar métodos más efectivos para apoyar y permitir aún más el logro de los objetivos de cada líder de unidad para el cumplimiento de la estrategia empresarial. |
| 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 de revisión periódica de la estrategia de inversión en SIC para asegurar su vigencia y relevancia. [VER CONTROL: MONITOREAR LA OPTIMIZACIÓN DE VALOR, EVALUAR LA OPTIMIZACIÓN DE VALOR] |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Establecer métricas y metas cuantitativas para evaluar el rendimiento de las inversiones en SIC.  1.1 Realizar análisis de riesgos para identificar y mitigar los posibles riesgos asociados a inversiones en SIC. [VER CONTROL: MONITOREAR LA OPTIMIZACIÓN DE VALOR] |
| 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 la estrategia de inversión en TI y la mezcla de inversión en SIC mediante la retroalimentación de la monitorización y las auditorías.  2. Establecer un proceso de revisión y mejora continua de la estrategia de inversión en TI y la mezcla de inversión en SIC, basado en los resultados de la monitorización, las auditorías y las lecciones aprendidas. |

# Preguntas de auditoría para Establecer el Objetivo de Inversión en SIC

|  |
| --- |
| **3.1 Temática: Identificación de los activos de TI** |
| Desde el punto de vista del auditor, es necesario verificar que exista documentación que establezca los objetivos empresariales y la estrategia de inversión en TI de la organización, y que el portafolio de programas de inversión se encuentre alineado a estos. Como primer punto, es necesario comprender el contexto interno e interno de la organización, y de forma particular, comprender cuales son los activos de TI que tiene la organización.  Los activos de TI representan una parte vital del capital de una empresa y su identificación permite evaluar su valor actual y potencial, lo cual es esencial para la planificación financiera y la asignación de recursos. La identificación asegura que las inversiones estén alineadas con los objetivos estratégicos de la organización, optimizando la distribución de recursos y evitando duplicaciones   |  | | --- | | **Atención**: Estas prácticas de auditoría se desarrollan con más profundidad en el control específico: Inventario de Activos de TI. |   Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización ha categorizado adecuadamente los diferentes activos físicos, sistemas de información y aplicaciones de software utilizados, y están alineados con las necesidades y objetivos estratégicos?   + Verifique que existe una taxonomía definida y documentada que permita homologar todos los registros de activos TI a lo largo de la organización * ¿La organización cuenta con un inventario de activos de TI que incluye todos los componentes relevantes?   + Verifique que el inventario de activos de TI cumpla con los requisitos expuestos en la norma ISO 27002:2022 (5.9, 5.10) como: Uso aceptable, etiquetado y eliminación segura. * ¿Se implementan medidas de seguridad física y lógica para proteger el inventario de activos de TI y garantizar que solo personas autorizadas tengan acceso? |

|  |
| --- |
| **3.2 Temática: Definición de objetivos, procesos de evaluación y política para el establecimiento de objetivo de inversión** |
| La definición de objetivos, los procesos de evaluación y la política para el establecimiento de objetivos de inversión son componentes cruciales en la gestión de inversiones y se explican de la siguiente manera:   1. **Definición de Objetivos:** Los objetivos de inversión son las metas financieras y estratégicas que la organización quiere lograr mediante la inversión. La definición de objetivos ayuda a guiar la estrategia de inversión, asegurando que los recursos se utilicen de manera que se alineen con las metas a corto y largo plazo. 2. **Procesos de Evaluación:** Evaluar el desempeño de la inversión con respecto a los objetivos establecidos permite la supervisión continua de la inversión, identificando áreas de mejora y riesgos potenciales. 3. **Política de Inversión en SIC:** Esta política guía cómo se definen, revisan y cumplen los objetivos de inversión, asegura que la definición de objetivos esté alineada con la misión y visión de la organización, y que se realice de manera coherente y responsable.   Este levantamiento puede incluir análisis específicos tales como:   * ¿La documentación relacionada con los programas de inversión se confecciona considerando la información crítica relevante, como planes de negocio, análisis de costo-beneficios y evaluaciones de riesgos? Verifique que la organización haya utilizado una o varias de las siguientes herramientas: * Análisis FODA (Debilidades, Amenazas, Fortalezas y Oportunidades * Marco de gestión de riesgos * Evaluación de vulnerabilidades y riesgos * Benchmarking * Marco de cumplimiento y regulaciones * Evaluación de capacidades de seguridad * Análisis de costo-beneficio. * Consultoría y asesoría especializada * ¿Existe un objetivo claro para la mezcla de inversión en SIC que sea consistente con los objetivos empresariales y la estrategia de inversión? * ¿El objetivo está adecuadamente comunicado a través de encuestas y es entendido por los responsables de la toma de decisiones y los equipos de SIC? * ¿Incluyen el riesgo organizacional, ciber riesgo, el retorno, el horizonte temporal, las restricciones legales y fiscales, y los requerimientos de liquidez? * ¿Se evalúa sistemáticamente los beneficios empresariales esperados de lasinversiones propuestas en SIC, teniendo en cuenta los aspectos económicos, estratégicos y de ciberriesgos?   + ¿Existe evidencia de que se ha comunicado los beneficios de la inversión en SIC a todas las partes interesadas y a la organización en su conjunto? * ¿Los procesos utilizados para identificar y priorizar las inversiones en SIC siguen criterios claros y consistentes?   + ¿Existe evidencia de que se adoptan mejores prácticas o existe evidencia del cálculo de indicadores relevantes tales como TIR, VAN, o utilizando métodos tales como Gordon Loeb para determinar si las inversiones en seguridad de la información son relevantes? * ¿La documentación relacionada respalda el proceso de determinación de inversiones en seguridad de la información y se mantienen registros adecuados? * ¿Existen comunicaciones documentadas y actividades generales tales como: charlas, campañas de concienciación o la instalación de signos en la organización que apoyen la comunicación efectiva?   + 1. **Políticas y procesos de inversión**  |  | | --- | | **Atención**: La disposición de recursos para la ejecución de las prácticas y proyectos en SIC es un tema relevante que debe ser abordado en la Política de Seguridad de la Información |   Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización cuenta con políticas formales que aborden la seguridad de la información y la asignación de recursos para inversiones en SIC? * ¿Existe un mecanismo de comunicación y colaboración efectivo entre los lideres de las unidades organizativas y los lideres de TI para garantizar la alineación estratégica? |

|  |
| --- |
| **3.3 Temática: Auditar el monitoreo y evaluación del objetivo de inversión** |
| Monitorear y evaluar el objetivo de inversión permite evaluar el rendimiento y realizar ajustes oportunos, identificar y gestionar riesgos, y asegurar la transparencia y la responsabilidad. Esta supervisión continua también fomenta una toma de decisiones más informada, permite cumplir con los requisitos legales o reglamentarios y medir el impacto real de la inversión en términos financieros, sociales o ambientales. Además, contribuye al aprendizaje organizacional y a la mejora continua de las estrategias de inversión.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización tiene proceso formal para revisar periódicamente la estrategia de inversión en TI y SIC para garantizar su vigencia y relevancia?   + ¿Este proceso se encuentra documentado? ¿Se han definido roles, responsabilidades, plazos, indicadores e interfaces con otros procesos relevantes? * ¿Se evalúa el rendimiento de las inversiones en términos de resultados a corto y largo plazo, comparándolos con las metas establecidas?   + ¿Se han establecido métricas idóneas para medir la eficiencia de las inversiones en SIC? ¿Estas métricas se comparan con el rendimiento esperado? * ¿Se han implementado los controles y salvaguardias adecuadas para reducir o eliminar riesgos identificados en los procesos de monitoreo y evaluación de inversión?   + Verifique que estos riesgos se incluyen como información de entrada en los procesos de gestión de riesgos. Puede consultar los procesos de gestión de riesgos asociados. * ¿La organización implementa acciones basadas en lecciones aprendidas u otras experiencias relevantes para mejorar la estrategia de inversión en TI y SIC? |