Pantalla de computadora con imágen de hombre

Descripción generada automáticamente con confianza media

**CASIG 1 – Gobernanza de la Ciberseguridad**

**Preguntas de Auditoría**

**Dirigir la Optimización del Valor**

1. Visión General

La optimización del valor en la gestión de seguridad de la información y ciberseguridad (SIC) implica definir los requisitos para las revisiones de cada etapa y de otros puntos de control, evaluando cómo el portafolio de inversiones en SIC se alinea con los objetivos empresariales, la tolerancia al riesgo y los beneficios continuos que genera. Las decisiones sobre la optimización del valor en SIC deben considerar cómo cada inversión en seguridad impacta la competitividad y la capacidad de la empresa para enfrentar nuevas oportunidades y retos, promoviendo un uso innovador de SIC que apoye el crecimiento empresarial.

* 1. **Gestión Estratégica del Portafolio de Inversiones en SIC**

Para dirigir la optimización de valor, es fundamental implementar una gestión estratégica del portafolio de inversiones en SIC que permita ajustes continuos según las prioridades y riesgos emergentes. Este proceso implica definir y comunicar claramente los tipos y criterios de inversión, desarrollando políticas para la recopilación de datos de desempeño y facilitando la integración de la evaluación del portafolio de SIC en la toma de decisiones estratégicas. La creación de una estructura de evaluación formal y periódica asegura que la organización pueda responder a cambios en los objetivos empresariales y a la evolución de amenazas en el entorno. Asimismo, incluir innovaciones y mejoras operativas en el análisis permite a SIC contribuir de manera directa al aumento del valor organizacional, adaptándose a las necesidades actuales y futuras.

* 1. **Rol de la Auditoría en la Evaluación de la Optimización de Valor**

Desde la perspectiva de auditoría, dirigir la optimización del valor en SIC requiere una revisión exhaustiva del desempeño del portafolio de inversiones y una comunicación clara de metas y resultados. Los auditores evalúan la efectividad de las inversiones en SIC, implementando técnicas avanzadas como el análisis de tendencias y la minería de datos para obtener una visión precisa sobre el impacto de cada iniciativa de seguridad en el valor empresarial. Además, la auditoría asegura que las lecciones aprendidas y los resultados de análisis previos se integren en la toma de decisiones futuras, proporcionando recomendaciones para ajustar el portafolio de SIC y maximizando su contribución al éxito organizacional. Este enfoque de mejora continua permite que las inversiones en seguridad de la información se mantengan alineadas con los objetivos estratégicos y optimicen el valor en toda la empresa.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Definir los requisitos para los cambios de fase (stage-gate) y otras revisiones para ver el peso de la inversión para la empresa y el riesgo asociado, las planificaciones del programa, los planes de financiación y la entrega de capacidades y beneficios y contribución continua al valor.  2. Dirigir a la gestión para que considere los potenciales usos innovadores de SIC que permiten a la empresa responder a nuevas oportunidades y retos, emprender nuevos negocios, aumentar la competitividad o mejorar los procesos.  3. Dirigir cualquier cambio requerido en la asignación de rendición de cuentas y responsabilidades para ejecutar el portafolio de inversiones y entrega de valor por parte de los procesos y servicios empresariales.  4. Dirigir cualquier cambio requerido al portafolio de inversiones y servicios para realinearse con los objetivos y/o  limitaciones empresariales actuales y esperadas.  5.Recomendar la consideración de innovaciones, cambios organizativos o mejoras operativas posibles que podrían generar un mayor valor para la empresa a partir de iniciativas de SIC.  6. Dirigir los cambios necesarios a la cartera de inversiones y servicios para realinearlos con los nuevos riesgos e implicaciones relacionados con la seguridad. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Definir y comunicar los tipos, categorías, criterios y peso relativo al criterio de portafolio e inversiones que permitan puntajes de valor relativo total.  2. Desarrollar políticas y procedimientos para la recopilación y análisis de datos de desempeño del portafolio de inversiones en SIC.  2.1 Integrar la evaluación del desempeño del portafolio de inversiones en SIC con los procesos de toma de decisiones estratégicas.  3. Documentar y comunicar claramente la estrategia y los objetivos de evaluación del desempeño del portafolio  de inversiones en SIC. |
| 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 formal de revisión y evaluación periódica del desempeño del portafolio de inversiones en SIC. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Definir y comunicar las metas y medidas de resultados de la entrega de valor a nivel de empresa para permitir una supervisión eficaz.  2. Implementar técnicas de análisis avanzadas, como el análisis de tendencias y la minería de datos, para obtener  información más precisa sobre el desempeño del portafolio de inversiones en SIC. |
| 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. Incluir lecciones aprendidas y resultados de análisis de tendencia y minería de datos para la mejora del proceso para dirigir la optimización del valor. |

# Preguntas de Auditoría para Dirigir la Optimización del Valor

|  |
| --- |
| **3.1 Temática: Dirección del valor de inversiones en SIC** |
| La evaluación constante permite a la empresa identificar oportunidades de mejora, fortalecer su postura de seguridad, mantenerse alineada con los objetivos estratégicos y cumplir con las expectativas de seguridad de sus clientes y partes interesadas. Es un enfoque holístico que promueve una cultura de excelencia en todos los aspectos de la organización y garantiza la protección de sus activos digitales y la confianza de sus stakeholders. Para esto el auditor debe abordar los siguientes puntos:  **3.1.1 Auditar el alineamiento de las inversiones con los objetivos y metas empresariales**  Auditar el alineamiento de las inversiones con los objetivos y metas empresariales es crucial para una gestión eficiente y eficaz de los recursos financieros, asegurando que todas las partes de la organización estén trabajando cohesivamente hacia las mismas metas. Esta alineación no solo optimiza el rendimiento y la rentabilidad, sino que también reduce los riesgos innecesarios al identificar desalineamientos tempranamente. Además, fomenta la responsabilidad y la transparencia, mejorando la confianza de los stakeholders y permitiendo una mayor adaptabilidad y agilidad en un entorno empresarial en constante cambio.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se han logrado mejoras en la seguridad de la información, reducción de riesgos, cumplimiento normativo, eficiencia operativa, protección de activos y confianza de los clientes como resultado de la estrategia de SIC? * ¿La gestión de inversiones, servicios y activos de SIC está alineada con los objetivos estratégicos de la organización? * ¿Cómo se definen los tipos y categorías de inversiones en ciberseguridad en la organización?   + ¿Existen criterios claramente establecidos para evaluar las inversiones en ciberseguridad?   + ¿Cómo se determina y justifica el peso relativo asignado a cada criterio?   + ¿Hay evidencia de que estos criterios y pesos relativos se aplican consistentemente en la toma de decisiones de inversión?     - ¿Cómo se controla y verifica la aplicación correcta de estos criterios? * ¿Cómo se comunican estos tipos, categorías y criterios a las partes interesadas relevantes? * ¿Hay evidencia de que esta comunicación ha sido efectiva y entendida por los destinatarios? * ¿Existen procedimientos formales para garantizar que los cambios en los criterios se comuniquen de manera oportuna?   **3.1.2 Auditar roles y responsabilidades**  Dirigir cualquier cambio requerido en la asignación de rendición de cuentas y responsabilidades para ejecutar el portafolio de inversiones y entrega de valor es fundamental para la agilidad organizacional, permitiendo una rápida adaptación a nuevas oportunidades o desafíos. Esta dirección asegura una alineación continua con los objetivos estratégicos, optimiza la eficiencia en procesos y rentabilidad, y mitiga los riesgos mediante la claridad en las responsabilidades. Además, fomenta la transparencia y la rendición de cuentas, fortaleciendo la confianza entre los empleados y otros stakeholders, y facilita el cumplimiento regulatorio al mantenerse al día con los cambios legislativos. También contribuye a la satisfacción y el compromiso de los empleados, al proporcionar una asignación clara y justa de responsabilidades, y asegura la coherencia en la entrega de valor a los clientes.   |  | | --- | | **Atención**: Este control puede ser complementado con: Establecer Roles y Responsabilidades y todos los controles asociados al Dominio IV: Gestión de RRHH |   Este levantamiento puede incluir análisis específicos tales como:   * ¿Cómo identifica la organización los cambios necesarios en la rendición de cuentas y responsabilidades para el portafolio de inversiones? ¿Qué métodos y criterios utiliza la organización para determinar cuándo es necesario un cambio en la asignación de responsabilidades? * ¿Qué procesos y procedimientos están en lugar para planificar y ejecutar cambios en la asignación de rendición de cuentas y responsabilidades? * ¿Cómo se asegura que los cambios se realicen de manera oportuna y eficaz, y en alineación con los objetivos de la empresa? * ¿Cómo se comunican los cambios en la rendición de cuentas y responsabilidades a las partes interesadas relevantes?   + ¿Se ha obtenido feedback de las partes interesadas sobre la comprensión y aceptación de estos cambios * ¿Cómo evalúa la organización el impacto de los cambios en la rendición de cuentas y responsabilidades en la ejecución del portafolio de inversiones y la entrega de valor?   + ¿Se realizan análisis de riesgo antes de implementar los cambios?   + ¿Cómo se mitigan los riesgos identificados? * ¿Están documentados adecuadamente los cambios en la asignación de rendición de cuentas y responsabilidades? * ¿Existen registros claros que muestren cómo y por qué se tomaron las decisiones de cambio? * ¿Cómo se revisan y evalúan los cambios una vez implementados para asegurar que están teniendo el efecto deseado?   + ¿Existen procesos para la mejora continua en la asignación de rendición de cuentas y responsabilidades?   **3.1.3 Auditar la innovación en las inversiones SIC**  Auditar los temas de dirigir la gestión hacia los usos innovadores en la función de SIC y recomendar consideraciones para innovaciones y cambios es vital para asegurar una alineación estratégica con los objetivos de la empresa, manteniendo la competitividad en un mercado en rápida evolución. Permite una gestión eficaz de riesgos asociados con la introducción de cambios, establece métricas claras para evaluar el valor y el ROI, y garantiza el cumplimiento con leyes y regulaciones, protegiendo la integridad y reputación de la empresa.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Cómo identifica y evalúa la gestión los potenciales usos innovadores en la función de SIC que puedan presentar nuevas oportunidades o retos? * ¿Existe un proceso estructurado para investigar y explorar nuevas tecnologías o metodologías en la función de SIC que puedan contribuir a emprender nuevos negocios o aumentar la competitividad? * ¿Cómo se integran y promueven las innovaciones dentro de la función de SIC en la estrategia general de la empresa? * ¿Qué métricas y KPIs se utilizan para medir el impacto de las innovaciones en la función de SIC sobre los procesos y la competitividad de la empresa? * ¿Se proporciona formación y recursos suficientes para fomentar la innovación dentro de la función de SIC? * ¿Cómo se gestionan los riesgos asociados con la implementación de innovaciones en la función de SIC? * ¿Cómo se identifican y evalúan las posibles innovaciones, cambios organizativos o mejoras operativas que podrían generar un mayor valor a través de la función de SIC? * ¿Quién es responsable de hacer recomendaciones sobre estas innovaciones, y cómo se integran estas recomendaciones en la toma de decisiones estratégicas? * ¿Existe un proceso claro y documentado para evaluar cómo estas recomendaciones podrían implementarse y qué impacto podrían tener en la entrega de valor? * ¿Cómo se alinean las recomendaciones de innovación y mejora con los objetivos estratégicos y metas empresariales generales? * ¿Qué métricas se utilizan para evaluar el éxito de las innovaciones, cambios organizativos o mejoras operativas implementadas a través de la función de SIC? * ¿Se consulta y tiene en cuenta la opinión y feedback de los stakeholders internos y externos en el proceso de recomendación e implementación? * ¿Cómo se gestionan los riesgos y se asegura el cumplimiento legal y regulatorio cuando se consideran estas innovaciones y cambios? |

|  |
| --- |
| **3.2 Temática: Mejora continua del proceso de evaluación de la optimización del valor.** |
| Establecer metas claras y medibles permite a la empresa tener una dirección clara y específica hacia la cual trabajar. Al contar con metas definidas, la organización puede medir su progreso y desempeño en función de los resultados obtenidos, lo que facilita la identificación de áreas que requieren mejora y la toma de decisiones informadas.   * ¿La organización ha establecido objetivos y criterios de medición para la evaluación de la optimización de valor? ¿Se han definido en documentación relevante (como políticas, procedimientos, planes estratégicos o comunicaciones internas)?   + ¿Los criterios de medición utilizados para evaluar la optimización del valor están claramente establecidos y alineados con los objetivos estratégicos de la organización?   + ¿Existe un entendimiento claro y coherente de los objetivos? ¿Los criterios de medición están bien definidos y comprensibles para todos los involucrados? Es necesario entrevistar a los responsables clave como; Gerentes de proyectos, Líderes de equipos y/o Directivos de la organización.   **3.2.2 Auditar la implementación de técnicas de análisis para evaluar la optimización de valor**  La implementación de técnicas de análisis para evaluar la optimización de valor y la seguridad de la información es esencial para una gestión eficiente y efectiva en ambos aspectos. Estas técnicas proporcionan una visión profunda y fundamentada de los datos, lo que permite a la organización tomar decisiones informadas, mejorar su rendimiento y garantizar una protección más sólida de sus activos digitales y la confidencialidad de la información.   * ¿Se utilizan técnicas avanzadas de análisis, como el análisis de costo-beneficio y la evaluación de impacto para evaluar la optimización del valor de SIC?   + ¿Estas técnicas utilizan un enfoque sistemático y estructurado? * ¿Se han establecido políticas y procedimientos específicos para la recopilación de datos de desempeño de los servicios de SIC?   **3.2.3 Auditar el proceso de mejora continua en base a resultados de análisis y lecciones aprendidas**  Al utilizar el análisis de datos y la información recopilada, la empresa puede identificar áreas de oportunidad, identificar patrones y tendencias, y tomar decisiones más fundamentadas para maximizar el valor generado para los clientes y partes interesadas.   * ¿Se han establecido métodos y herramientas para mejorar el proceso de evaluación en base a los resultados de análisis y lecciones aprendidas?   + ¿Se utilizan métricas específicas y contingentes para este proceso? Por ejemplo:     - Porcentaje de iniciativas de SIC en el portafolio general donde el valor se administra durante todo el ciclo de vida.     - Porcentaje de iniciativas de SIC que usan principios y prácticas de gestión de valor * ¿La organización cuenta con un ciclo de mejora continua establecido como el ciclo PDCA (Planificar, Hacer, Verificar, Actuar)?   + ¿Se siguen los pasos del ciclo de mejora continua para identificar áreas de mejora?   + ¿Se promueve la implementación de acciones correctivas y preventivas?   + ¿Se realizar seguimiento y evaluación?   + ¿Se realizan ajustes según sea necesario? * ¿Se realizan entrevistas con los responsables de las iniciativas de seguridad de la información para medir el valor agregado de las iniciativas y cómo se seleccionan y calculan esas medidas? |