Pantalla de computadora con imágen de hombre

Descripción generada automáticamente con confianza media

**CASIG 1 – Gobernanza de la Ciberseguridad**

**Preguntas de Auditoría**

**Evaluar la Optimización del Valor**

1. Visión General

Evaluar la optimización del valor en la gestión de seguridad de la información y ciberseguridad (SIC) implica evaluar cómo se integran las estrategias de SIC con los objetivos estratégicos de la empresa, asegurando que la inversión en seguridad agregue valor tanto en aspectos financieros como no financieros. Además, la evaluación debe incluir la revisión de la eficacia de los roles, responsabilidades y órganos de toma de decisiones en la creación de valor desde SIC, así como el análisis de la alineación entre la gestión de inversiones, servicios y activos de SIC y las prácticas de gestión financiera y empresarial.

* 1. **Proceso de Evaluación y Políticas para Optimización del Valor**

Para evaluar la optimización del valor de los servicios y activos de SIC, es fundamental establecer objetivos y criterios de medición claros, apoyados por políticas que permitan la recopilación de datos de desempeño relevantes. Esto incluye métodos de generación de informes que comuniquen el valor añadido de las iniciativas de seguridad desde una perspectiva centrada en el negocio, midiendo también los costos de los incidentes de seguridad. Un proceso formal de revisión periódica permite evaluar gastos en seguridad de la información contra incidentes y potenciales multas regulatorias, proporcionando así una visión integral de cómo SIC contribuye al valor general de la empresa. La inclusión de métodos avanzados de análisis, como el análisis de costo-beneficio y la evaluación de impacto, permite comprender mejor el valor de las iniciativas de SIC y facilita la toma de decisiones informada.

* 1. **Rol de la Auditoría en la Optimización del Valor de SIC**

Desde la perspectiva de auditoría, la evaluación de la optimización del valor en SIC implica un análisis exhaustivo del valor agregado de los servicios de seguridad, tanto mediante medidas financieras como no financieras. Los auditores revisan si las prácticas de SIC están alineadas con los elementos clave de gobierno y si se están implementando técnicas avanzadas de análisis para evaluar la efectividad de las inversiones en seguridad. Asimismo, la auditoría examina los métodos para demostrar el valor de SIC, incluyendo la definición y recopilación de datos relevantes, y asegura que haya un programa de mejora continua que promueva acciones correctivas y preventivas. Al proporcionar retroalimentación detallada, la auditoría apoya la optimización constante del valor de SIC, ayudando a la organización a maximizar el rendimiento y la eficiencia en el uso de sus activos de seguridad.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Evaluar la eficacia con la que las estrategias organizacionales y de SIC se han integrado y alineado dentro de la empresa y con los objetivos de la empresa para entregar valor.  2. Conocer y considerar la eficacia de los roles, responsabilidades, rendición de cuentas y órganos de toma de decisiones actuales a la hora de asegurar la creación de valor a partir de las inversiones, servicios y activos de SIC.  3. Evaluar lo bien que está alineada la gestión de las inversiones, servicios y activos de SIC con la gestión de valor empresarial y las prácticas de gestión financiera.  4. Evaluar el portafolio de inversiones, servicios y activos para su alineación con los objetivos estratégicos de la empresa; el valor de la empresa, tanto financiera como no financiera; el riesgo, tanto el riesgo de entrega como el riesgo de beneficios; el alineamiento del proceso de negocio; la eficacia en términos de usabilidad, disponibilidad y capacidad de respuesta; y la eficiencia en cuanto a costes, redundancia y salud técnica. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Definir y comunicar claramente los objetivos de la evaluación de la optimización del valor y los criterios de medición.  2. Desarrollar políticas y procedimientos para recopilar datos de desempeño de los servicios entregados por la función de SIC.  3. Establecer un proceso formal de revisión y evaluación periódica de la optimización del valor de los servicios entregados.  3.1 Establecer procesos para evaluar los gastos de seguridad de la información contra incidentes de seguridad conocidos públicamente y posibles multas regulatorias en la industria  4. Utilizar métodos de generación de informes centrados en el negocio sobre el valor añadido de las iniciativas de seguridad de la información.  5. Establecer métodos para medir el costo de los incidentes de seguridad. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Conocer los elementos clave de gobierno para ofrecer de forma confiable, segura y económica un valor óptimo procedente del uso de servicios, activos y recursos de SIC actuales y nuevos.  2. Entender y discutir regularmente las oportunidades que podrían surgir para la empresa derivadas de los cambios habilitados por las tecnologías actuales, nuevas o emergentes, y optimizar el valor creado a partir de esas oportunidades. Se debe incluir al CISO a reuniones de la junta para analizar los riesgos y oportunidades relacionados con SIC.  3. Conocer lo que constituye valor para la empresa y considerar lo bien que se comunica, conoce y aplica en todos los procesos de la empresa.  4. Establecer un método para demostrar el valor de la seguridad de la información (incluida la definición y recopilación de datos relevantes) para garantizar el uso eficiente de los activos existentes relacionados con la seguridad de la información. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Asegurar el uso de medidas financieras y no financieras para describir el valor agregado de las iniciativas de seguridad de la información.  2. Implementar técnicas avanzadas de análisis, como el análisis de costo-beneficio y la evaluación de impacto, para obtener una comprensión más profunda de la optimización del valor de los servicios entregados |
| 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. Establecer un programa de mejora continua que promueva la implementación de acciones correctivas y preventivas para optimizar el valor de los servicios entregados por la función de SIC del valor. |

# Preguntas de auditoría para Evaluar la Optimización del Valor

|  |
| --- |
| **3.1 Temática: Evaluación de los elementos clave de las inversiones en SIC** |
| Al evaluar los elementos clave de las inversiones en SIC, la organización puede determinar si se están destinando los recursos adecuados para proteger los activos de información más críticos y si las estrategias de seguridad implementadas son efectivas y actualizadas para enfrentar las amenazas emergentes.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha comprobado si se siguen prácticas financieras sólidas y se prioriza y asignan recursos de manera efectiva para maximizar el valor organizacional (en términos de continuidad operacional y minimización de la materialización de * incidentes) y financiero en la función de SIC? * ¿Se evalúa en que grado las definiciones estratégicas definen como se define y comprende el "valor" dentro de la organización en relación con los procesos organizacionales y el rol de las inversiones en SIC para su logro?   + ¿Cómo se evalúa el alineamiento entre el concepto de valor con la misión, visión y objetivos estratégicos de la empresa?   + ¿Cómo se evalúa que el concepto de valor se aplique de manera coherente en todas las áreas de la empresa? * ¿Se evalúan los documentos elementos clave de gobierno en relación con los servicios, activos y recursos de SIC?   + Verifique que se evalúe quiénes son los responsables de la gobernanza de estos elementos, y cómo se les rinde cuentas   + Verifique que se evalúe cómo se integran los elementos de gobernanza de SIC en los que se invertirá, con los objetivos y estrategias generales de la empresa   + Verifique se evalúe cómo se monitorea y evalúa la eficiencia económica de los servicios, activos y recursos de SIC * ¿Cómo se evalúan las perspectivas de diferentes stakeholders (como clientes, empleados, accionistas) en la definición y aplicación del valor? * ¿Cómo se evalúan y gestionan los riesgos asociados con los servicios, activos y recursos de SIC? * ¿Qué métodos se utilizan para evaluar la comunicar la comprensión del valor a través de diferentes niveles y funciones en la empresa? |

|  |
| --- |
| **3.2 Temática: Evaluación del alineamiento de la gestión de inversiones y la cartera de inversiones SIC con la estrategia organizacional** |
| El objetivo principal de este control es garantizar que las inversiones en SIC estén alineadas con los objetivos estratégicos de la organización y con su tolerancia al riesgo. Esto implica identificar y priorizar las áreas de mayor riesgo y asignar recursos adecuados para implementar medidas de seguridad efectivas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha realizado un análisis exhaustivo para verificar si la estrategia de SIC se ha integrado adecuadamente dentro de los procesos y actividades de la empresa? ¿Se ha identificado en qué áreas específicas se ha considerado la seguridad de la información? * ¿Se ha evaluado cómo la estrategia de SIC ha contribuido a la entrega de valor a la empresa? ¿Existen métricas y KPIs establecidos para medir el impacto de * la estrategia en términos de seguridad de la información, reducción de riesgos y cumplimiento normativo? * ¿Se han identificado mejoras concretas en la seguridad de la información, reducción de riesgos, eficiencia operativa, protección de activos y confianza de los clientes como resultado de la implementación de la estrategia de SIC? ¿Se han recopilado datos y evidencias que respalden estas mejoras? * ¿Existe un proceso formal para realizar mediciones periódicas y obtener resultados tangibles que demuestren la efectividad de la estrategia de SIC? ¿Se ha comunicado esta información a las partes interesadas relevantes? * ¿Se ha asegurado de que la estrategia de SIC se alinea de manera coherente con la estrategia empresarial más amplia? ¿Se ha evaluado la coherencia entre los objetivos estratégicos de la organización y las iniciativas de seguridad de la información? |

|  |
| --- |
| **3.3 Temática: Evaluación de las oportunidades de mejora e innovación en la cartera de inversiones SIC** |
| El objetivo principal de este control es identificar áreas en las que la cartera de inversiones en SIC pueda ser optimizada y enriquecida para lograr mejores resultados en términos de seguridad y eficiencia. Esto implica revisar de manera exhaustiva las soluciones y tecnologías existentes, así como explorar nuevas herramientas y enfoques que puedan mejorar la protección de los activos de información y la respuesta a incidentes de seguridad.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha realizado un análisis de alineación entre el portafolio de inversiones, servicios y activos de SIC y los objetivos de la empresa?   + ¿Se han identificado áreas donde se pueden mejorar los resultados o se pueden generar nuevas oportunidades a través de la cartera de inversiones de SIC?   + ¿Se evalúa con métricas e indicadores específicos el valor de las inversiones? Algunos ejemplos de estos indicadores son:     - Desviación entre la mezcla de inversión objetivo y real.     - Porcentaje de portafolio de inversiones habilitadas por SIC con el fin de determinar la probabilidad de alcanzar los objetivos de la empresa y proporcionar un valor a un coste razonable. * ¿Se han establecido métricas y KPI’s específicos para medir el valor generado por el portafolio de inversiones de SIC?   + ¿Se están utilizando estas métricas para evaluar el desempeño del portafolio y su contribución al valor empresarial?   + ¿Se utilizan métricas específicas y apropiadas para evaluar las oportunidades de mejora e innovación? * ¿Se ha llevado a cabo una evaluación adecuada de los riesgos asociados con el portafolio de inversiones, servicios y activos de SIC? ¿Existen planes de mitigación para abordar los riesgos identificados? * ¿Se ha identificado cómo los elementos del portafolio de proyectos e * inversiones en SIC contribuyen a mejorar la seguridad de los procesos de la organización?   + ¿Existen casos de estudio o ejemplos específicos que demuestren cómo el portafolio ha generado valor a través de mejoras operativas y la minimización de riesgos? * ¿Se han aplicado prácticas de gestión de servicios y activos sólidas para optimizar el rendimiento y la eficiencia del portafolio? * ¿Se ha llevado a cabo una revisión detallada de los costos, redundancias y salud técnica de los activos de SIC? |

|  |
| --- |
| **3.4 Temática: Evaluación de los roles y responsabilidades asignados para la creación de valor en las inversiones SIC** |
| Esto implica revisar y evaluar si los roles asignados tienen la capacidad y las competencias necesarias para cumplir con sus responsabilidades en la protección de los activos de información. Al evaluar los roles y responsabilidades, la organización puede identificar posibles brechas y áreas de mejora para garantizar que todas las áreas y funciones relevantes estén adecuadamente representadas y comprometidas con la seguridad de la información.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha llevado a cabo una revisión completa para analizar el desempeño de los roles y responsabilidades dentro de la función de SIC?   + ¿Se han identificado áreas de mejora en el cumplimiento de tareas y contribución a la creación de valor?   + ¿Se ha verificado que los comités o grupos de decisión relevantes están involucrados en la toma de decisiones estratégicas relacionadas con las inversiones, servicios y activos de SIC?   + ¿Se ha evaluado si se consideran los aspectos clave de la creación de valor en las decisiones? * ¿Se ha establecido un proceso claro para evaluar el desempeño de los responsables y si están siendo responsables de los resultados en términos de creación de valor? ¿Se ha demostrado que existen consecuencias apropiadas para el incumplimiento de las responsabilidades? |