Pantalla de computadora con imágen de hombre

Descripción generada automáticamente con confianza media

**CASIG 1 – Gobernanza de la Ciberseguridad**

**Preguntas de Auditoría**

**Dirigir la Gestión de Recursos**

1. Visión General

Dirigir la gestión de recursos en la función de seguridad de la información y ciberseguridad (SIC) implica identificar y evaluar los recursos actuales, dirigir la adopción de estrategias de gestión de recursos, y asegurar que la alta dirección esté informada sobre las implicaciones financieras de la asignación de recursos a SIC. La dirección efectiva de los recursos permite que SIC cumpla con las necesidades de la empresa y apoye la planificación financiera y de recursos humanos, asegurando que las decisiones de inversión en seguridad estén respaldadas por una gestión de recursos bien fundamentada.

* 1. **Desarrollo de Estrategias y Políticas de Gestión de Recursos en SIC**

Para alinear los recursos de SIC con los objetivos de la organización, es crucial definir y comunicar los objetivos empresariales y de seguridad que deben alcanzarse con los recursos asignados. Esto requiere documentar y comunicar la estrategia de gestión de recursos, que incluya criterios claros de asignación y un proceso de seguimiento eficaz. La implementación de políticas y procedimientos para la asignación, control y seguimiento de recursos en SIC asegura que los responsables tengan una estructura definida que permita responder adecuadamente a las necesidades de la organización. La creación de un comité de gestión de recursos o la delegación de esta responsabilidad a un comité ejecutivo de SIC permite definir la estrategia de recursos, los criterios de asignación y los procesos de monitoreo necesarios para mantener una alineación continua con las prioridades de negocio.

* 1. **Rol de la Auditoría en la Evaluación de la Gestión de Recursos en SIC**

La auditoría desempeña un rol crítico en la evaluación de la efectividad de la gestión de recursos en SIC, proporcionando retroalimentación basada en la evaluación de riesgos y el análisis costo-beneficio y ROI de las inversiones en seguridad. Las auditorías periódicas permiten identificar áreas de mejora, verificar la alineación de los recursos con los objetivos empresariales y medir la eficacia de la estrategia de recursos a través de métricas clave. Además, la auditoría revisa el sistema de gestión del cambio y los sistemas de incentivos para asegurar que se adapten rápidamente a las necesidades cambiantes y motiven un uso óptimo de los recursos. Al proporcionar una revisión estructurada y recomendaciones específicas, la auditoría apoya la mejora continua de la estrategia de recursos, asegurando que SIC cuente con una gestión de recursos robusta que maximice su contribución a la seguridad organizacional y el logro de los objetivos empresariales.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Identificar y comprender los recursos asignados a la función de SIC, incluyendo personal, presupuesto, infraestructura y herramientas.  2. Evaluar el estado actual de la gestión de recursos en la función de SIC.  3. Dirigir la adopción de estrategias de gestión de recursos, principios y del plan de recursos y arquitectura empresarial acordados, las cuales se deben comunicar periódicamente a la alta dirección junto con las implicaciones de la financiación en SIC para los recursos de la empresa.  4. Alinear la gestión de recursos con la planificación financiera y de RR. HH. de la empresa.  5.Asegúrese de que la gestión de recursos de seguridad de la información esté alineada con las necesidades comerciales. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Definir y comunicar claramente los objetivos empresariales y de seguridad que deben alcanzarse con los recursos asignados. 1.1 Documentar y comunicar claramente la estrategia de gestión de recursos en la función de SIC, incluyendo los criterios de asignación y el proceso de seguimiento.  2. Desarrollar políticas y procedimientos para la asignación, seguimiento y control de los recursos en la función de SIC.  3. Asignar responsabilidades para la ejecución de la gestión de recursos.  3.1 Se debe dirigir a los responsables para asegurar que, cuando sea necesario por razones de negocio, la TI proporciona soporte al negocio con información actualizada, correcta y protegida ante pérdidas o usos inadecuados.  3.2 Establecer un comité o equipo responsable de la gestión de recursos, o asignar la responsabilidad y autoridad a los comités estratégicos o ejecutivos de SIC para definir la estrategia de gestión de recursos, los criterios de asignación y los procesos de seguimiento. |
| 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 recursos a largo plazo que tenga en cuenta las necesidades actuales y futuras de la función de SIC.  2. Establecer un proceso de asignación de presupuesto y control financiero para garantizar la utilización efectiva de los recursos asignados.  3. Realizar evaluaciones de riesgos para identificar y mitigar posibles riesgos que puedan afectar la gestión de recursos en la función de SIC. [VER CONTROL: EVALUAR LA OPTIMIZACIÓN DE LOS RECURSOS] |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Definir las metas, mediciones y métricas clave para la gestión de recursos  1.1 Con el fin de que la junta directiva y la alta gerencia tomen las mejores decisiones posibles, se debe incluir como base el uso de un análisis costo- beneficio y cálculos ROI de las posibles inversiones en TI.  2. Realizar auditorías periódicas para evaluar la efectividad de la gestión de recursos y su alineación con los objetivos establecidos. [VER CONTROL: MONITOREAR LA OPTIMIZACIÓN DE LOS 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 la estrategia y el proceso de gestión de recursos en la función de SIC, basado en la retroalimentación de las auditorías y las revisiones periódicas.  2. Establecer un sistema de gestión del cambio que permita adaptar rápidamente la asignación de recursos a los cambios en los objetivos empresariales y de seguridad.  3. Promover la formación y el desarrollo profesional del personal de la función de SIC para optimizar su rendimiento y utilizar eficazmente los recursos asignados.  4. Fomentar la colaboración y la comunicación efectiva entre los equipos de la función de SIC y otras áreas de la organización para asegurar una gestión de recursos integrada.  5. Establecer un sistema de incentivos y reconocimiento para motivar y recompensar el desempeño excepcional en la gestión de recursos en la función de SIC. |

# Preguntas de auditoría para Dirigir la Gestión de Recursos

|  |
| --- |
| **3.1 Temática: Análisis de gestión de recursos** |
| El análisis de gestión de recursos debe incluir documentación clara y actualizada del sistema dentro del marco de políticas y procedimientos definidos, que describa los recursos asignados a la función de SIC. Desde este punto de vista, es necesario que el auditor verifique la existencia y vigencia de: organigrama, la política de recursos humanos, presupuestos, inventarios de infraestructura y herramientas, registro de gastos y cualquier otro documento relevante para la SIC, que demuestre que se designa un presupuesto adecuado para:   * Necesidades de personal * Necesidades de Infraestructura * Necesidades de Herramientas * Necesidades financieras   Para ello, el auditor debe considerar lo siguiente:  **3.1.1 - Auditar la Planificación financiera**  La auditoría de la planificación financiera para ciberseguridad es un proceso crítico que asegura que los fondos destinados a la ciberseguridad se utilicen de manera eficiente y efectiva, y que estén alineados con los objetivos y riesgos de seguridad de la organización.   |  | | --- | | **Atención**: Estas prácticas de auditoría se pueden observar en conjunto con Dirigir la Optimización de Valor |  * ¿Existe documentación que describa la planificación financiera y gestión de recursos humanos de la empresa en función de la SIC?   + ¿Existe un proceso documentado y establecido para la asignación de presupuesto y control financiero que describa cómo se asignan los recursos financieros y cómo se lleva a cabo el control y seguimiento de los gastos? * ¿Los recursos financieros asignados son suficientes para respaldar las actividades y proyectos relacionados con la SIC? * ¿La organización está optimizando el uso de personal, presupuesto, infraestructura y herramientas? ¿se están alcanzando los resultados esperados? * ¿Existe un plan documentado que establezca los recursos necesarios para la función de SIC a largo plazo?   + ¿Tiene en cuenta las necesidades actuales y futuras de la función de SIC?   + ¿Se consideran factores como el crecimiento de la organización, los avances tecnológicos, las amenazas y los riesgos emergentes, y las regulaciones o requisitos cambiantes?   **3.1.2 - Auditar la Planificación de Recursos humanos**   * ¿Se considera la contratación de personal especializado en seguridad de la información? * ¿La organización cuenta con un programa formal de formación y desarrollo para el personal de la función de SIC? (capacitaciones, cursos, talleres, entre otros.)   + ¿El programa de formación se encuentra alienado con los objetivos y necesidades de la SIC proporcionando capacitación en áreas claves de conocimiento y habilidades? * ¿La organización evalúa el desempeño de la gestión de recursos?   + ¿Existe un sistema de incentivos y reconocimientos de la SIC, que se otorguen en base a metas claras y medibles específicas para la gestión de recursos en SIC?   **3.1.3. - Auditar los objetivos y estrategias para la gestión de recursos**   * ¿Se han establecido metas y objetivos claros relacionados con la gestión de recursos que sean específicas, medibles, alcanzables, relevantes y con límites de tiempo, y que estén alineadas con las estrategias y necesidades comerciales? * ¿Los recursos propuestos en el plan respaldan los objetivos y las metas establecidas en la estrategia general de seguridad de la información, y existe coherencia entre ambos? * ¿La organización comunica los objetivos empresariales y de seguridad claramente a las partes interesadas relevantes, tanto internas como externas?   + ¿Se verifica la eficacia de la comunicación?   **3.1.4 - Auditar los roles y responsabilidades para la gestión de recursos**   * ¿La política de la SIC o políticas complementarias, establecen claramente los roles y responsabilidades de las partes involucradas en la asignación, seguimiento y control de recursos? * ¿Se identifican los roles y responsabilidades específicos para dirigir a los responsables de TI y garantizar la entrega de información actualizada, correcta y protegida? * ¿Existe un comité o equipo designado específicamente para la gestión de recursos en el ámbito de la SIC?   ¿Tienen la responsabilidad y autoridad de establecer los criterios de asignación de recursos y los procesos de seguimiento, y cuentan con el respaldo y apoyo de la alta dirección? |

|  |
| --- |
| **3.2 Temática: Comunicación en el marco de una gestión de recursos integrada.** |
| Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe una interacción y colaboración entre los equipos de la SIC y otras áreas de la organización   + ¿Se trabaja en conjunto en proyectos o actividades?   + ¿Se integra el presupuesto de SIC con el presupuesto maestro?   + ¿Se consideran los beneficios y externalizares positivas de los proyectos de SIC, como un impacto financiero en la organización?   + ¿Se identifican áreas donde se puedan aprovechar las inversiones de forma que cubran más de una sola función en la organización? * ¿Existen canales de comunicación establecidos para facilitar la colaboración entre los equipos de la SIC y otras áreas (ejemplo: reuniones, herramientas de colaboración en línea, correo electrónico, intranet u otros medios de comunicación)? |

|  |
| --- |
| **3.3 Temática: Mejora continua de la estrategia y del proceso de gestión de recursos.** |
| La identificación de oportunidades de mejoras en el proceso de gestión de recursos está apoyado en los resultados de auditorías previas, evaluaciones de desempeño, informes de revisión, y documentación relevante que permita realizar una retroalimentación al proceso.   * ¿Se han definido mediciones y métricas clave para evaluar el desempeño de la gestión de recursos en la SIC? ¿Se utilizan indicadores relevantes, como el cumplimiento de presupuesto, la eficiencia en la asignación de recursos, la satisfacción del cliente interno y otros aspectos que reflejen el éxito en la gestión de recursos en base al análisis costo-beneficio y cálculos ROI de las posibles inversiones en TI?. Algunos ejemplos de estas métricas pueden ser:   + - * Número de desviaciones y de excepciones con respecto a los principios de gestión de recursos       * Porcentaje de reutilización de componentes de la arquitectura * ¿Existen registros o documentos que indiquen la realización de auditorías periódicas para evaluar la gestión de recursos? * ¿La organización ha realizado seguimientos y acciones correctivas como resultado de las auditorías? * ¿Se han implementado acciones de mejora propuestas como resultado de las auditorías y las revisiones periódicas? |