Pantalla de computadora con imágen de hombre

Descripción generada automáticamente con confianza media

**CASIG 1 – Gobernanza de la Ciberseguridad**

**Preguntas de Auditoría**

**Evaluar la Gestión de Recursos**

1. Visión General

Evaluar la gestión de recursos en la función de seguridad de la información y ciberseguridad (SIC) implica examinar las opciones de abastecimiento y asignación de recursos para desarrollar capacidades que respondan a las necesidades presentes y futuras de SIC. Definir principios claros de asignación y gestión de recursos permite que SIC cumpla con los objetivos empresariales respetando los límites presupuestarios y priorizando las necesidades estratégicas de la organización.

* 1. **Políticas y Estrategias para la Gestión Eficiente de Recursos**

Para una gestión de recursos eficaz, es esencial definir y comunicar principios que regulen la asignación de capacidades y recursos de SIC, así como formalizar responsabilidades en la evaluación de esta gestión. Esto incluye el desarrollo de políticas para la recopilación y análisis de datos relevantes, identificando métricas clave que permitan evaluar la efectividad de los recursos en SIC. Realizar análisis comparativos entre recursos asignados y resultados alcanzados ayuda a determinar el grado de alineación con las necesidades de la organización, mientras que un proceso formal de revisión periódica permite identificar áreas de mejora. Además, el uso de herramientas avanzadas como el análisis predictivo y la minería de datos proporciona una comprensión profunda de patrones y tendencias en la gestión de recursos, facilitando ajustes continuos que optimicen su aprovechamiento.

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

Desde la perspectiva de auditoría, la evaluación de la gestión de recursos de SIC implica verificar la eficiencia y eficacia de los procesos de administración de recursos en términos de provisión, capacitación y competencias. Las auditorías regulares permiten evaluar la conformidad con estándares y mejores prácticas, ofreciendo una visión objetiva sobre la efectividad de la asignación de recursos y su alineación con los objetivos empresariales. Además, la auditoría revisa la implementación de sistemas de gestión del conocimiento y de datos para capturar y compartir prácticas óptimas en la gestión de recursos. Mediante un enfoque de mejora continua basado en datos y resultados, la auditoría respalda la optimización de la gestión de recursos, promoviendo una cultura de aprendizaje y colaboración que potencia el desempeño de SIC y contribuye al éxito organizacional.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Partiendo de las estrategias actuales y futuras, examinar las posibles opciones para proporcionar recursos relacionados con SIC (recursos tecnológicos, financieros y humanos), y desarrollar capacidades para hacer frente a las necesidades actuales y futuras (incluidas opciones de abastecimiento).  2. Definir los principios fundamentales de la asignación y gestión de recursos y capacidades, de forma que la función de SIC pueda satisfacer las necesidades de la empresa conforme a las prioridades acordadas y los límites presupuestarios. Por ejemplo, definir opciones preferidas de abastecimiento definidas para determinados servicios y los límites presupuestarios por opción de abastecimiento.  3. Revisar y aprobar las estrategias del plan de recursos y de la arquitectura empresarial para proporcionar valor y mitigar el riesgo con los recursos asignados una vez que se haya proporcionado la documentación adecuada para asegurarse de que se sustentarán los procesos de negocio con capacidades y aptitudes requeridas, incluyendo la continuidad de la operación normal de la organización y la gestión de los riesgos asociados a SIC  4. Entender los requisitos para el alineamiento de la gestión de recursos de SIC con la planificación de recursos humanos y financieros de la organización. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Definir los principios para la gestión y el control de la arquitectura organizacional.  2. Evaluar la efectividad de los recursos de seguridad de la información en términos de provisión, capacitación, concientización y competencias.  3. Formalizar las responsabilidades de la actividad de evaluación de la gestión de recursos en la función de SIC.  4. Definir y comunicar claramente los objetivos de la evaluación de la gestión de recursos y los criterios de efectividad.  5. Desarrollar políticas y procedimientos para recopilar datos relevantes sobre la gestión de recursos en la función de SIC.  5.1 Identificar y recopilar métricas clave para evaluar la efectividad de la gestión de recursos.  6. Realizar análisis comparativos entre los recursos asignados y los resultados obtenidos en relación con los objetivos empresariales y de seguridad.  7. Evaluar el grado de alineación de los recursos asignados con las necesidades y prioridades de la organización.  8. Establecer un proceso formal de revisión y evaluación periódica de la gestión de recursos asignados que permita identificar y documentar las áreas que requieren mejoras o cambios en la gestión de recursos  asignados. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Evaluar la eficiencia y eficacia de los procesos utilizados para gestionar los recursos asignados a la función de SIC.  2. Realizar auditorías regulares y más detalladas para evaluar la efectividad de la gestión de recursos y la conformidad con los estándares y las mejores prácticas establecidas. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Implementar técnicas avanzadas de análisis de datos, como el análisis predictivo y la minería de datos, para obtener una comprensión más profunda de los patrones y tendencias relacionados con la gestión de recursos en la función de SIC.  2. Establecer un sistema de gestión del conocimiento más robusto para capturar, compartir y utilizar las mejores prácticas en la gestión de recursos asignados a la función de SIC.  3. Implementar un sistema de gestión de datos más robusto para recopilar, almacenar y analizar información relevante sobre la gestión de recursos.  4. Realizar análisis comparativos y de tendencias a largo plazo para identificar patrones y áreas de mejora sostenida. |
| 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. Promover una cultura de aprendizaje y colaboración, donde se compartan experiencias y conocimientos para impulsar la mejora continua en la gestión de recursos en la función de SIC.  2. Mejorar continuamente la estrategia y el proceso de evaluación de la gestión de recursos en función de los hallazgos de las auditorías y los análisis cuantitativos.  3. Establecer un sistema de revisión y mejora continua basado en datos y resultados para impulsar la optimización de la gestión de recursos asignados a la función de SIC. |

# Preguntas de Auditoría para Evaluar la Gestión de Recursos

|  |
| --- |
| **3.1 Temática: Evaluación de la asignación y gestión de recursos y capacidades** |
| Evaluar la alineación de la asignación de recursos y capacidades con la estrategia y los objetivos de la organización. Esto implica asegurarse de que los recursos se asignen de manera coherente con las prioridades estratégicas y las metas establecidas, para que la organización pueda centrarse en las áreas más críticas y estratégicas.  Además, el auditor debe verificar si se han establecido mecanismos para monitorear y evaluar la eficacia de la asignación de recursos y si se realizan ajustes o mejoras de manera proactiva. Se analiza si la organización cuenta con indicadores clave de rendimiento que permitan medir y evaluar la utilización y eficiencia de los recursos y si estos se utilizan como base para la toma de decisiones y se revisa si se realiza un seguimiento y una evaluación periódica de la asignación de recursos y capacidades. Esto implica verificar si la organización realiza revisiones regulares para evaluar la efectividad de la asignación actual y si se realizan ajustes cuando sea necesario.    Este levantamiento puede incluir análisis específicos tales como:   * ¿Cómo se alinea la estrategia general de seguridad de la información con las necesidades y objetivos empresariales actuales y futuros? * ¿Qué procesos y criterios se utilizan para evaluar y seleccionar las posibles opciones de recursos tecnológicos, financieros y humanos en relación con SIC? * ¿Cómo se identifican y evalúan las opciones de abastecimiento, incluyendo la externalización y colaboración con proveedores terceros? * ¿Existen métricas y KPIs claros para medir la eficacia y eficiencia de los recursos y capacidades desarrollados? Algunos ejemplos de métricas ad-hoc 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. * ¿Cómo se asegura que los recursos y capacidades desarrollados cumplen con las regulaciones y estándares de seguridad aplicables? * ¿Qué procesos y políticas existen para garantizar que la asignación de recursos esté en línea con las prioridades acordadas y los límites presupuestarios?   + ¿Qué planes y procedimientos existen para adaptarse a cambios o emergencias en las necesidades de seguridad de la información? * ¿Cómo se definen y comunican los principios fundamentales de la asignación y gestión de recursos y capacidades para la función de seguridad? * ¿Cómo se asegura la colaboración y comunicación efectiva entre los diferentes departamentos y stakeholders en la asignación y gestión de recursos? * ¿Qué métodos se utilizan para monitorear y revisar la utilización y gestión de recursos, y cómo se ajustan en respuesta a cambios en las necesidades y prioridades de la empresa?   + ¿Qué controles y salvaguardias existen para prevenir la malversación o uso ineficiente de los recursos asignados a la función de seguridad? * ¿Cómo se integran los principios de gestión de recursos en la planificación y ejecución general de la estrategia de seguridad de la empresa? |

|  |
| --- |
| **3.2 Temática: Evaluación de la estrategia, arquitectura y alineamiento** |
| Es una práctica esencial para asegurar que la organización tenga una visión clara y bien definida de sus objetivos estratégicos, y que estos estén alineados adecuadamente con su arquitectura organizativa y operativa. Esta evaluación se enfoca en revisar cómo la organización desarrolla, evalúa y ajusta su estrategia, asegurando que esté bien alineada con su estructura y procesos internos.  La alineación también es un aspecto crucial en esta auditoría. Se revisa si los procesos y actividades de la organización están alineados con los objetivos estratégicos y si se han establecido mecanismos adecuados para monitorear y medir el progreso hacia el logro de estos objetivos. Esto incluye evaluar la definición y el uso de indicadores clave de rendimiento (KPIs) para medir el desempeño estratégico.   |  | | --- | | **Advertencia:** Considere complementar este control con el Dominio IV “Gestión de Recursos Humanos” |   Este levantamiento puede incluir análisis específicos tales como:   * ¿Cómo se desarrollan y documentan las estrategias del plan de recursos para la función de SIC y de la arquitectura empresarial?   + ¿Qué procesos y criterios se utilizan para revisar y aprobar estas estrategias? ¿Cuentan con participación de la dirección?   + ¿Cómo se alinean estas estrategias con los objetivos y metas empresariales generales?   + ¿Cómo se integran los planes de recursos de SIC con la planificación de recursos humanos y financieros a nivel empresarial? * ¿Cómo se asegura que las estrategias propuestas proporcionen valor y mitiguen el riesgo con los recursos asignados? * ¿Quiénes son los responsables de revisar y aprobar estas estrategias, y tienen la formación y experiencia adecuadas? * ¿Qué mecanismos existen para monitorear y ajustar las estrategias a medida que cambian las circunstancias y necesidades de la empresa? * ¿Cómo se comunican y aplican las estrategias aprobadas a lo largo de la organización * ¿Qué procesos y herramientas se utilizan para entender y documentar los requisitos para alinear la gestión de recursos de SIC con la planificación de recursos humanos y financieros? * ¿Cómo se asegura que los responsables de la gestión de recursos de SIC comprendan y actúen de acuerdo con estos requisitos? * ¿Existen mecanismos claros de comunicación y colaboración entre los equipos de SIC y los departamentos de recursos humanos y financieros? * ¿Qué métricas y KPIs se utilizan para evaluar el éxito del alineamiento entre la gestión de recursos de SIC y la planificación de recursos humanos y financieros? * ¿Cómo se gestionan los riesgos asociados con el desalineamiento de la gestión de recursos de SIC con la planificación de recursos humanos y financieros? * ¿Existen procedimientos para revisar y actualizar regularmente los requisitos y el alineamiento a medida que cambian las necesidades y objetivos de la empresa? |

|  |
| --- |
| **3.3 Temática: Principios para la gestión y el control de la arquitectura organizacional** |
| La auditoría implica una revisión exhaustiva de los principios fundamentales que guían el diseño y la estructura de la organización. Estos principios proporcionan una base sólida para la toma de decisiones, la planificación estratégica y el logro de los objetivos empresariales. La auditoría se enfoca en evaluar si estos principios están bien definidos, implementados y si se siguen adecuadamente en todas las áreas de la organización. El auditor analiza la documentación y los documentos que describen los principios de la arquitectura organizacional. Estos pueden incluir manuales, políticas, directrices y otros documentos estratégicos.  Se proporcionan recomendaciones para fortalecer y mejorar los principios de gestión y control de la arquitectura organizacional. Estas recomendaciones pueden incluir clarificar la comunicación de los principios, proporcionar capacitación adicional al personal o revisar la estrategia para asegurar que esté alineada con los principios definidos.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Cómo se han definido los principios para la gestión de la arquitectura organizacional, y quiénes participaron en su formulación?   + Verifique que se consulta a los responsables de la función de SIC por recomendaciones y observaciones de ciberriesgo que ayuden en el diseño y establecimiento de los principios de la gestión de la arquitectura empresarial * ¿Cómo se alinean estos principios con la estrategia y objetivos globales de la organización y con la estrategia y objetivos de la función de seguridad?   + ¿Existen mecanismos para revisar y actualizar estos principios conforme cambian los objetivos de la función de SIC o emergen nuevos riesgos?   + ¿Cómo se integran estos principios en los procesos de toma de decisiones y planificación estratégica general de la organización?   + ¿Se han considerado las regulaciones y normativas relevantes para SIC en la definición de los principios para la arquitectura organizacional?   + ¿Cómo se asegura que los principios de gestión de la arquitectura organizacional se mantienen al día con los cambios en los panoramas de amenazas? * ¿Existe una documentación clara y accesible que explique estos principios y cómo deben ser aplicados?   + ¿Cómo se comunican y difunden estos principios entre los empleados y otras partes interesadas? * ¿Qué mecanismos de control y supervisión están en lugar para asegurar que los principios de la arquitectura organizacional sean seguidos y aplicados consistentemente?   + ¿Cómo se gestionan los riesgos asociados con la implementación y cumplimiento de estos principios? * ¿Qué entrenamiento o apoyo se ofrece para ayudar a los empleados y líderes a comprender y aplicar estos principios? * ¿Cómo se evalúa y mide el éxito o cumplimiento de estos principios en la arquitectura organizacional? |