

**05 - Control de Acceso**

**CASIG 1 – Gobernanza de la Ciberseguridad**

**Preguntas de Auditoría**

**Dirigir el Sistema de Gobierno**

|  |
| --- |
| **Competencias Básicas del Auditor**   1. Conocimientos en normativa de seguridad de la información y ciberseguridad. 2. Conocimientos en contextos de riesgos de SIC. 3. Conocimientos en modelos de gobernanza, 3 LoD, roles y responsabilidades en SIC. 4. Conocimientos en análisis y alineamiento estratégico. |

# Visión General

La dirección del sistema de gobierno se refiere a un enfoque estructurado y efectivo para garantizar que la seguridad de la información y ciberseguridad se alinee adecuadamente con los objetivos estratégicos de una organización.

Uno de los pilares fundamentales de este enfoque es establecer una clara estructura de roles y responsabilidades para la gestión de la seguridad de la información y ciberseguridad. Esto implica definir de manera precisa las funciones y tareas dentro de la organización, asignándolas a individuos o grupos específicos.

De esta forma, se evita la duplicación de esfuerzos y se fomenta la responsabilidad, facilitando una toma de decisiones más ágil y efectiva.

Además, se enfatiza la importancia de establecer objetivos claros y medibles para la gestión de la seguridad de la información y ciberseguridad, alineados con los objetivos estratégicos de la organización. Estos objetivos proporcionan una base para evaluar el desempeño y el progreso en la gestión de la seguridad de la información y ciberseguridad, identificando áreas de mejora y permitiendo una toma de decisiones informada.

La comunicación efectiva también es un factor clave en la dirección del sistema de gobierno de la seguridad de la información y ciberseguridad. La información relevante sobre la gestión de la seguridad de la información y ciberseguridad debe fluir de manera clara y oportuna entre todas las partes interesadas, incluyendo la alta dirección, los responsables de SIC y otros miembros del equipo. De esta manera, se garantiza que todos estén alineados en cuanto a los objetivos y las decisiones tomadas.

* 1. **Herramientas para la Dirección del Sistema de Gobierno**
* **Política:** Las políticas establecen el marco de referencia y las directrices para la toma de decisiones relacionadas con la gestión de la seguridad de la información y ciberseguridad. Estas políticas definen los principios, objetivos y procedimientos que deben seguirse en toda la organización para asegurar una adecuada protección de los activos de información.
* **Roles y Responsabilidades:** Establecer una clara estructura de roles y responsabilidades es crucial para la gestión efectiva de la seguridad de la información y ciberseguridad. Esto implica definir las funciones y tareas específicas de cada miembro del equipo, asegurando que cada uno tenga responsabilidades bien definidas y sepan a quién acudir en caso de dudas o incidentes.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Identificar los objetivos empresariales clave de la organización: la visión, misión y metas estratégicas de la organización, así como los planes de negocio y las necesidades de los stakeholders.  2. Establecer los requisitos específicos para el marco de gobierno de SIC que aseguren su alineamiento con los objetivos empresariales. Estos requisitos deben reflejar las necesidades de la organización y abordar los riesgos y requisitos de seguridad de la información. ***[Ver Control: Política de SIC]*** |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Comunicar los principios de gobierno de SIC, la definición de seguridad de información y los principios de gestión de riesgos. Acordar con la administración ejecutiva la forma de establecer un liderazgo informado y comprometido de acuerdo a las responsabilidades asignadas de SIC. El plan de comunicación debe contener:  1.1 Aspecto y métricas a informar  1.2 Preparadores y receptores  1.3 Frecuencia  1.4 Procedimientos de escalamiento 2. Establecer o delegar el establecimiento de estructuras, procesos y prácticas de gobierno en línea con los principios de diseño de arquitectura actuales y previstos previamente acordado.  2.1 El marco de gobierno debe estar organizado por procesos e incluir información sobre las actividades de los procesos, los propietarios y las áreas de mejora. ***[Ver Control: Estructura Organizacional]***  2.2 Establecer un comité estratégico de SIC (o equivalente). Este comité estratégico debería garantizar que el gobierno de SIC, como parte del gobierno de la empresa, se aborda de forma adecuada; aconsejar sobre la dirección estratégica a seguir; y determinar la priorización de los programas de inversión habilitados por SIC en línea con la estrategia y prioridades del negocio de la empresa. ***[Ver Control: Estructura Organizacional]***  3. Garantizar que las funciones y responsabilidades de la junta directiva estén documentadas y entendidas. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Asignar la responsabilidad, autoridad y rendición de cuentas por las decisiones de SIC en línea con los principios de diseño de gobierno, de los modelos de toma de decisiones y de delegación acordados. 2. Los responsables y las practicas se documentan en marcos de gobernanza. El CISO (o máximo responsable de la función de seguridad de la información) asiste a las reuniones de la junta ejecutiva y se analiza la contribución de la SIC a los objetivos empresariales. 3. Asegurar que los mecanismos de comunicación y presentación de informes proporcionan la información adecuada a los responsables de la supervisión y toma de decisiones, que incluyan reuniones periódicas con el fin de revisar las iniciativas de SIC actuales y futuras para reevaluar la alineación con los objetivos organizacionales y la oportunidad de presentar iniciativas que respalden la estrategia de SIC. 4. Direccionar al personal para que siga las directrices relevantes en cuanto al comportamiento ético y profesional y asegurar que se conozcan y se apliquen las consecuencias del incumplimiento. 5. Direccionar el establecimiento de un sistema de recompensas para fomentar el cambio cultural deseado en base a la compensación del personal, el establecimiento de objetivos y la evaluación del desempeño  5.1 Deben incluir medidas y planes de incentivo diseñadas y ejecutadas para prevenir o detectar comportamientos inaceptables o toma de riesgos excesivos y para respaldar acciones alineadas con los objetivos estratégicos de la organización ***[VER CONTROL: CONCIENCIACIÓN Y CAPACITACIÓN]*** 6. Implementar procedimientos jerárquicos de información y escalamiento de decisiones. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Garantizar informes periódicos de iniciativas y problemas clave de seguridad de la información a la junta directiva. |
| 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 la participación activa de los stakeholders en la identificación de nuevas prácticas, tecnologías o enfoques que puedan mejorar la alineación con los objetivos empresariales y la eficacia del marco de gobierno. 2. Mantenerse actualizado sobre las nuevas tecnologías y soluciones emergentes relacionadas con la gestión de la seguridad de la información y el marco de gobierno. Realizar investigaciones y evaluaciones para determinar si estas tecnologías pueden mejorar el alineamiento con los objetivos empresariales y considerar su implementación.  3. Buscar evaluaciones externas, como auditorías o revisiones independientes, para obtener una perspectiva objetiva sobre la eficacia y alineación del marco de gobierno de SIC con los objetivos empresariales. Utilizar los resultados de estas evaluaciones para identificar oportunidades de mejora y fortalecer el proceso de gestión del marco de gobierno. |

# Preguntas de Auditoría para Dirigir el Sistema de Gobierno

|  |
| --- |
| 3.1 Temática: Análisis del entorno de Gobierno |
| El análisis del entorno de gobierno incluye la documentación detallada y sistemática de todos los aspectos externos e internos que son necesarios para definición de los instrumentos de dirección.  Desde la perspectiva del auditor, esto implica verificar que se han realizado los análisis necesarios para la comprensión del entorno de organización en su totalidad.  Este levantamiento puede incluir análisis específicos tales como:  **3.1.1 Establecimiento de la visión y misión de la organización**  Estos son los elementos constitutivos que establece la dirección futura y el propósito de la empresa y suelen encontrarse en las declaraciones estratégicas de alto nivel, como la planificación estratégica o documentadas en las memorias. Aunque no es probable que se encuentren en la misión y visión declaraciones respecto a la ciberseguridad, si es importante verificar si se ha considerado los ciber riesgos como una entrada relevante para el diseño de estas definiciones.   * ¿Es la visión de la organización relevante y coherente con el entorno de negocios actual, los objetivos estratégicos y con el panorama de ciber riesgos en el que la organización se encuentra inmersa? * ¿Las declaraciones estratégicas son claras, concisas y comprensibles para todos los miembros de la organización? ¿Es posible transmitir estas declaraciones de manera efectiva a los empleados y otras partes interesadas? |
| **3.1.2 Definición de las metas estratégicas establecidas por la organización**  Los objetivos o metas estratégicas son los resultados específicos que la empresa desea alcanzar para cumplir con su visión y misión. En ellos, si se puede esperar una mención directa a resultados clave de la función de SIC, y su planteamiento debería darse siempre en consideración del panorama de riesgos y amenazas.   * ¿Las metas estratégicas son coherentes y se encuentran alineadas con la visión, misión de la organización? * ¿Las metas estratégicas consideran el entorno de amenazas y los ciber riesgos a los que la organización enfrenta? * ¿Las metas organizacionales son suficientemente claras y concretas? ¿Son específicas y medibles? ¿Considera en la medición la probabilidad de materializar un ciber riesgo? * ¿El plazo establecido para lograr las metas estratégicas y su prioridad en relación con otras iniciativas y objetivos de la organización es realista? ¿Las metas están adecuadamente priorizadas? * ¿Se identifican los indicadores clave de rendimiento (KPI) y de riesgo (KRO) asociados a cada meta estratégica?   **3.1.3 Alineamiento entre los requisitos específicos para el marco de gobierno de SIC y los objetivos empresariales**   * ¿Se ha establecido un marco de gobierno de SIC? ¿Considera este marco de gobierno todos los requisitos de seguridad de la información, los requisitos derivados de la estrategia de negocio, los requisitos establecidos por la función de riesgo y los requisitos que emanan de las partes interesadas relevantes? * ¿Existe evidencia de que se han identificado las brechas o falta de alineación entre el marco de gobierno actual de ciberseguridad actual y los objetivos empresariales? * ¿Se han implementado medidas para cumplir con los requisitos definidos en el marco de gobierno, tales como: la implementación de controles, la implementación de procesos de seguridad adicionales, ¿y la asignación de responsabilidades? |

|  |
| --- |
| 3.2 Temática: Verificar la implementación del Sistema de Gobierno |
| Es igualmente relevante la verificación de las herramientas y elementos necesarios para la dirección efectiva del sistema de gobierno, evaluar si estos se encuentran presentes en la organización y si consideran las prácticas mínimas establecidas en los estándares de buenas prácticas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización ha establecido los roles y responsabilidades necesarios para la gestión y operación de la función de SIC? * ¿Demuestra la arquitectura organizacional los principios de diseño para las estructuras, procesos y prácticas aplicables a la función de SIC? * ¿La organización ha establecido políticas, procedimientos y estructuras de responsabilidades en organigramas específicas para la función de SIC, de acuerdo con los principios de diseño declarados por la organización y alineados con sus declaraciones estratégicas? * ¿Existe un órgano que cumpla con las características de comité estratégico o consejo de administración de gobierno de SIC? * ¿Existen evidencias en matrices RACI, organigramas, definiciones de responsabilidades en los procesos, procedimientos o políticas, definiciones de cargo, y cualquier otra documentación que evidencie la existencia de un consejo de administración de gobierno de SIC? * ¿La organización ha declarado en un documento formal Verificar que la organización haya establecido los objetivos y responsabilidades del comité estratégico de SIC en documentos? |

|  |
| --- |
| 3.3 Temática: Evaluación y mejora del Sistema de Gobierno |
| La evaluación y mejora continua del sistema de gobierno de SIC es clave para alcanzar los objetivos que este plantea, por ello, la organización debe implementar los mecanismos necesarios para incorporar las lecciones aprendidas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existen registros válidos, sistematizados y periódicos que identifiquen potenciales iniciativas de mejora o problemas en el sistema de gobierno? * Estos registros podrían incluir: análisis de riesgos, reportes de incidentes de seguridad, propuestas y avances de proyectos, resultados de auditorías internas y externas, entre otros. * ¿Los registros que contengan mejoras se han presentado al comité estratégico, SGSI, la dirección u otro órgano con capacidad de toma de decisión? ¿Hay evidencia de que han sido recibidos, tales como actas o cartas de recepción? * ¿Existen iniciativas, que involucren a las partes interesadas clave, y que se enfoquen en la detección de oportunidades de mejora? * Estas iniciativas podrían incluir, pero no estar limitadas a: reuniones, grupos de trabajo, encuestas, sistemas de retroalimentación, plataformas de colaboración, etc. * ¿Existe evidencia de que se han incorporado las contribuciones y acciones de mejora, resultantes de la información recopilada y las iniciativas de detección de mejoras en las actuales y futuras iteraciones del sistema de gobierno de ciberseguridad? * ¿Se han documentado las investigaciones y evaluaciones de las nuevas tecnologías y soluciones que puedan aportar a la función de ciberseguridad? * ¿Hay evidencia que demuestre que se analiza su aplicabilidad, ventajas, desventajas y potencial impacto en la gestión de la seguridad de la información y el marco de gobierno de la organización? * ¿Hay evidencia que demuestre que se ha analizado los factores de su implementación? (costos, compatibilidad con sistemas existentes, capacitación necesaria, tiempo de implementación, recursos necesarios y la capacidad para implementar y gestionar las soluciones de manera efectiva) * ¿Existen informes de evaluación externa realizados? * ¿Estos informes cumplen con evaluar la eficacia y alineación del marco de gobierno de SIC con los objetivos empresariales? ¿Resaltan los aspectos positivos y las áreas que requieran mejoras o ajustes en el marco de gobierno de SIC dentro de los hallazgos, recomendaciones y conclusiones de la evaluación? * ¿Existen planes de acción detallados para las oportunidades de mejora identificadas? * ¿Estos planes definen las actividades específicas, los responsables, los plazos y los recursos necesarios para implementar las mejoras propuestas? |