Pantalla de computadora con imágen de hombre

Descripción generada automáticamente con confianza media

**CASIG 1 – Gobernanza de la Ciberseguridad**

**Preguntas de Auditoría**

**Evaluar el Sistema de Gobierno**

1. Visión General

La evaluación del sistema de gobierno de seguridad de la información y ciberseguridad (SIC) en relación con los objetivos empresariales implica un análisis detallado de cómo los controles y prácticas de SIC soportan la estrategia general de la empresa, identificando cualquier área de mejora y adaptando el sistema de gobierno a las necesidades cambiantes del negocio y a las tendencias del entorno. Reconocer la importancia de esta evaluación permite a las organizaciones gestionar mejor los riesgos y cumplir con los requisitos normativos, proporcionando una estructura organizativa sólida en la que los roles y responsabilidades están claramente definidos.

**1.2 Implementación de la Evaluación de Gobierno de Seguridad y Asignación de Roles**

Para ejecutar una evaluación eficaz del sistema de gobierno de SIC, es esencial establecer un equipo dedicado, designando un líder del proyecto y miembros especializados. La revisión inicial de prácticas y controles de SIC se realiza ad-hoc, permitiendo un primer vistazo sin una planificación detallada. Este equipo debe analizar los factores ambientales internos y externos, incluyendo las obligaciones legales y contractuales, y considerar la evolución del negocio y los procesos de SIC, asegurando que se atiendan las necesidades futuras de la organización. Esta revisión abarca desde la identificación de riesgos asociados hasta el análisis de la cultura de toma de decisiones y la forma en que las decisiones sobre seguridad se alinean con los objetivos comerciales y regulatorios. Un enfoque sistemático permite identificar fortalezas y debilidades del sistema, documentando los hallazgos preliminares para construir un plan de evaluación estructurado que incluya métodos de recopilación de datos y un cronograma detallado de actividades.

**1.3 Rol de la Auditoría en la Evaluación del Sistema de Gobierno de SIC**

Desde la perspectiva de auditoría, la evaluación del sistema de gobierno de SIC debe seguir una metodología exhaustiva, empleando técnicas de evaluación como entrevistas, análisis de brechas y benchmarking. La auditoría examina en qué medida las prácticas de SIC cumplen con las regulaciones vigentes y si se alinean con las tendencias y expectativas legales y comerciales. Este proceso también evalúa si la estructura de gobierno facilita la toma de decisiones óptima para la seguridad de la información y si se entienden las responsabilidades asignadas en SIC. Los auditores comunican sus resultados mediante informes detallados que identifican las fortalezas y áreas de mejora en el sistema de gobierno, priorizando recomendaciones específicas según el impacto en los objetivos empresariales. Implementar tecnologías avanzadas y herramientas de monitoreo permite optimizar estas evaluaciones, incorporando un ciclo de retroalimentación continua que enriquece los procesos de revisión con lecciones aprendidas y facilita la mejora constante de la seguridad de la información y ciberseguridad en la organización.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Reconocer la necesidad de evaluar el sistema de gobierno de Seguridad de la Información y Ciberseguridad en relación con los objetivos empresariales.  2. Establecer un equipo responsable de la evaluación del sistema de gobierno de SIC, designando un líder del proyecto y los miembros del equipo.  3. Realizar una revisión inicial de las prácticas y controles existentes del sistema de gobierno de SIC. Esta revisión se realiza ad-hoc y no cuenta con una planificación previa.  4. Identificar los riesgos asociados con la falta de efectividad del sistema de gobierno de SIC en la protección de los activos de información y la mitigación de riesgos.  5. Documentar los hallazgos y recomendaciones preliminares basados en la revisión inicial |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Formalizar la evaluación del sistema de gobierno en procesos y procedimientos con roles y responsabilidades definidas. El proceso de evaluación del sistema de gobierno debería considerar:  1.1 Analizar e identificar los factores ambientales internos y externos (obligaciones legales, regulatorias y contractuales), así como las tendencias en el entorno de negocio que pueden influir en el diseño del gobierno y de su sistema de gobernanza de seguridad de la información  1.2 Evaluar la importancia de SIC y su papel con respecto al negocio  1.2.1 Se debe tener en cuenta la evolución de la SIC y los procesos del negocio para asegurar que la SIC proporcionará apoyo a las futuras necesidades de la organización  1.3. Evaluar el entorno normativo externo: las regulaciones, leyes, y obligaciones contractuales externas y determinar cómo deberían aplicarse dentro del gobierno de SIC de una empresa. [VER CONTROL: ANÁLISIS DEL ENTORNO INTERNO Y EXTERNO]  1.4. Evaluar en qué medida la seguridad de la información está alineada con las tendencias legales y reglamentarias.  1.5. Determinar las implicaciones de todo el entorno de control de la empresa con respecto a SIC.  1.6. Evaluar hasta qué punto la seguridad de la información satisface las necesidades comerciales y de cumplimiento/regulatorias.  1.7. Evaluar la cultura de toma de decisiones de la empresa y determinar el modelo de toma de decisiones es óptimo para la seguridad de la información. Evaluar las opciones óptimas para asegurar la eficaz y oportuna toma de decisiones relativas a SIC para alcanzar los objetivos del negocio.  1.8 Evaluar si se entienden y asumen las responsabilidades delegadas en materias de 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 plan detallado para la evaluación del sistema de gobierno de SIC, incluyendo los criterios de evaluación, los métodos de recopilación de datos y el cronograma de actividades.  2. Identificar y documentar las fortalezas y debilidades del sistema de gobierno de SIC, basándose en los hallazgos de la evaluación.  3. Priorizar las áreas de mejora o cambios identificadas en función de su impacto en los objetivos empresariales y la criticidad de los riesgos asociados.  4. Comunicar los resultados de la evaluación del sistema de gobierno, por ejemplo, a través de un informe detallado de evaluación que incluya recomendaciones específicas para abordar las áreas de mejora o cambios identificadas. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Realizar una evaluación exhaustiva del sistema de gobierno de SIC utilizando técnicas de evaluación apropiadas, como revisiones documentales, entrevistas, análisis de brechas y benchmarking. |
| 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 proceso de retroalimentación y aprendizaje organizacional para incorporar las lecciones aprendidas de las evaluaciones y revisiones anteriores en las actividades de evaluación, para mejorar las técnicas de evaluación, la presentación de resultados, la comunicación de los hallazgos y cualquier otra salida de la actividad.  2. Implementar tecnologías y soluciones avanzadas para mejorar la eficiencia y eficacia de las actividades de evaluación del sistema de gobierno de SIC, como la automatización de procesos y la implementación de herramientas de monitoreo. |

# Preguntas de Auditoría para Evaluar el Sistema de Gobierno

|  |
| --- |
| **3.1 Temática: Evaluación del sistema de gobierno** |
| Asegurar la evaluación del Sistema de Gobierno es esencial para garantizar una gestión efectiva y sólida de la seguridad de la información en la organización. La evaluación brinda una visión completa del estado de la seguridad y permite tomar decisiones estratégicas para mejorar la protección de la información y minimizar riesgos. Para esto el auditor debe abordar los siguientes puntos: 3.1.1 Auditar la evaluación del equipo responsable de la evaluación del sistema de gobierno de SIC Contar con un equipo responsable de la evaluación del sistema de gobierno de SIC aporta conocimientos especializados, independencia, objetividad y enfoque dedicado, lo que contribuye a fortalecer la seguridad de la información y proteger los activos de la organización frente a las amenazas cibernéticas en constante evolución.   |  | | --- | | **Atención**: Estas prácticas de auditoría se desarrollan con más profundidad en el control: Establecer roles y responsabilidades |   Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe un equipo establecido y respaldado dentro de la estructura organizativa actual? ¿Existe documentaciones existentes relacionada con responsabilidad y el liderazgo? * ¿Se reconocen las habilidades y competencias requeridas dentro del equipo? ¿Se realizó una evaluación de descripciones del puesto y las competencias requeridas para los roles relacionados? * ¿Se ha nombrado un líder en el proyecto para la evaluación? ¿Mantiene las experiencias y competencias necesarias para liderar el proyecto?  3.1.2 Auditar la evaluación inicial de las prácticas y controles existentes junto con los riesgos asociados Realizar una evaluación inicial de las prácticas y controles existentes junto con los riesgos asociados proporciona una visión clara de las áreas críticas y los riesgos potenciales, lo que permite tomar acciones proactivas para proteger la información de la organización y mejorar continuamente su postura de seguridad.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se realizó una revisión inicial del sistema de gobierno de SIC? * ¿Se evalúan la practicas y controles existentes del sistema para identificar posibles riesgos? * ¿Se realizan las pruebas de cumplimiento para identificar brechas en la relación con las políticas y estándares establecidos? * ¿Se evalúa la eficacia y eficiencia de los controles existentes para reconocer cualquier deficiencia o debilidad en su implementación? * ¿Existen indicadores y registros que respalden las mediciones y evaluaciones realizadas?   **3.1.3 Auditar la evaluación del sistema junto con criterios de evaluación establecidos**  La formalización de la evaluación del sistema junto con criterios de evaluación establecidos es clave para asegurar una evaluación efectiva, objetiva y consistente de la seguridad de la información en la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se incluye dentro de la documentación las obligaciones legales, regulatorias y contractuales que afectan al sistema de gobierno de SIC? * ¿Se incluye dentro de la documentación la necesidad de realizar un análisis del entorno del negocio para identificar las tendencias que puedan influir en el diseño del gobierno y el sistema de gobernanza de seguridad de la información? * ¿Se incluye dentro de la documentación que la organización deba comparar las prácticas de seguridad de la información existentes con los requisitos legales y reglamentarios aplicables? * ¿Se incluye que la organización deba medir en qué medida se satisface las necesidades del negocio y los requisitos de cumplimiento regulatorio? * ¿Se incluye la necesidad de mantener un modelo de toma de decisiones óptimo que permita una toma de decisiones eficaz y oportuna en relación con SIC para alcanzar los objetivos del negocio? * ¿Se incluye la necesidad de identificar áreas de mejora o ajustes necesarios para realizar acciones correctivas o mejoras necesarias? * ¿La documentación sobre evaluación del sistema está formalizada y aprobada por la dirección? |

|  |
| --- |
| **3.2 Temática:Mejora continua del proceso de evaluación del Sistema de Gobierno** |
| Medir la efectividad de la evaluación del Sistema de Gobierno es clave para asegurar la calidad, relevancia y utilidad de este proceso. Proporciona una base para tomar decisiones informadas respecto a al proceso de evaluación del sistema de gobierno, mejorar la seguridad de la información y garantizar la continuidad de un proceso de evaluación, de manera que este siga siendo efectivo y significativo en la organización. Para esto el auditor debe abordar los siguientes puntos:   * + 1. **Auditar el proceso de retroalimentación y aprendizaje**   Establecer un proceso de retroalimentación y aprendizaje para el proceso de evaluar el sistema de gobierno de SIC es fundamental para asegurar la mejora continua, adaptación a los cambios, y la eficiencia del proceso de evaluación. Facilita la identificación de oportunidades de mejora, la promoción de una cultura de seguridad y la toma de decisiones informadas para fortalecer la seguridad de la información en la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe indicadores para medir el desempeño del proceso de evaluación del sistema de gobierno? ¿Existen los mecanismos necesarios para realizarlo? * ¿Existe un proceso para el análisis de datos recopilados? ¿Se comparan estos datos con objetivos y metas definidas? * ¿Se realizan análisis de brechas comparando los requisitos de gobierno de SIC con la situación actual de la organización? ¿Se identifican brechas o desviaciones en la evaluación de la efectividad de los controles y procesos existentes? * ¿Se realizan análisis comparativos de las prácticas de gobierno con las organizaciones similares o de referencias para identificar las mejores prácticas y áreas de mejora? * ¿Se identifican las lecciones aprendidas y las áreas de mejora en evaluaciones anteriores o los procesos de retroalimentación y aprendizaje?   **3.2.2 Auditar evaluación de las tecnologías y soluciones avanzadas para mejorar la eficiencia y eficacia de las actividades de evaluación**  La implementación de tecnologías y soluciones avanzadas es esencial para mejorar la eficiencia y eficacia de las actividades de evaluación en un proceso de retroalimentación y aprendizaje del sistema de gobierno de SIC. Estas herramientas proporcionan capacidades mejoradas de análisis, automatización y gestión de riesgos, lo que permite una evaluación más completa, ágil y efectiva de la seguridad de la información en la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe un plan de implementación de tecnologías avanzadas para evaluar si se han establecido objetivos claros, plazos y recursos para la adopción de estas soluciones? * ¿Se han adquirido y desplegado las tecnologías y soluciones avanzadas planificadas? (p.ej. herramientas de análisis de datos, automatización de procesos, detección de anomalías, etc.) * ¿Se han integrado estas soluciones correctamente con otros sistemas y fuentes de datos relevantes para la evaluación de la seguridad de la información? * ¿Las soluciones avanzadas han mejorado la identificación, evaluación y gestión de los riesgos de seguridad de la información en la organización? ¿Se ha medido continuamente la evolución de indicadores que lo avalen? |