Y

**05 - Control de Acceso**

**CASIG 1– Gobierno de la Ciberseguridad**

**Preguntas de Auditoría**

**Monitorear el Sistema de Gobierno**

|  |
| --- |
| **Competencias Básicas del Auditor**   1. Conocimientos en normativa de seguridad de la información y ciberseguridad. 2. Conocimiento en la normativa legal general, sectorial y específica a la que la organización es afecta. 3. Conocimiento sobre métodos de monitoreo y evaluación del desempeño. 4. Conocimientos en de la estrategia de gobierno corporativo de la ciberseguridad. 5. Conocimientos básicos sobre riesgos e impactos en el negocio. |

# Visión General

Monitorear la eficacia y el rendimiento del gobierno de seguridad de la información y ciberseguridad (SIC) implica realizar evaluaciones periódicas de los procesos, estructuras y principios acordados para el SIC, garantizando que se establezcan y operen de forma efectiva y repetible. Al evaluar la eficacia del diseño del gobierno de SIC y la adecuación de sus mecanismos, las organizaciones pueden detectar desviaciones y tomar acciones correctivas de manera proactiva para cumplir con sus obligaciones y mantener la integridad de sus sistemas de seguridad de la información.

**1.1 Procesos y Herramientas para el Monitoreo del Rendimiento de SIC**

El monitoreo del gobierno de SIC debe basarse en procesos documentados y estandarizados, donde se definan roles, responsabilidades, indicadores clave de desempeño (KPI) y criterios específicos de monitoreo. Estos indicadores deben estar alineados con las metas empresariales y permitir medir la eficacia y rendimiento del sistema de gobierno. Cada KPI debe contar con límites y umbrales específicos, además de métodos de análisis que identifiquen la necesidad de acciones correctivas cuando se presenten desviaciones. Asimismo, para una supervisión eficaz, se deben utilizar herramientas y sistemas adecuados, como software de monitoreo de seguridad, paneles de control y sistemas de generación de informes, que permitan recopilar y analizar datos en tiempo real. Estas herramientas facilitan la observación constante del entorno de amenazas, asegurando que el SIC responda de manera adecuada a los cambios en el panorama de riesgos y que cumpla con las regulaciones, estándares y políticas de seguridad internos y externos.

**1.2 Rol de la Auditoría en el Monitoreo del Sistema de Gobierno de SIC**

Desde la perspectiva de auditoría, el monitoreo de la eficacia y el rendimiento del gobierno de SIC implica una evaluación continua del cumplimiento de las obligaciones regulatorias y contractuales, así como de las políticas internas y guías de seguridad de la organización. Los auditores revisan si los mecanismos establecidos cumplen con los estándares requeridos y si el proceso de monitoreo está documentado, incluyendo la formalización de los KPI y los criterios de monitoreo. Además, la auditoría verifica la efectividad de los procesos de inteligencia de amenazas y su impacto en la seguridad organizacional, así como el desempeño de las partes interesadas responsables del gobierno de SIC. A través de informes detallados y recomendaciones, la auditoría proporciona retroalimentación sobre la eficacia del sistema, garantizando que los controles de seguridad se mantengan sólidos y alineados con los objetivos empresariales, y permitiendo a la organización tomar decisiones informadas para fortalecer su postura de seguridad.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Monitorear de forma periódica si los mecanismos de SIC que se han acordado (procesos, estructuras, principios, procesos, etc.) se han establecido y operan de forma eficiente, para garantizar que sea consistentes y repetibles.  2. Monitorear la eficacia del diseño de gobierno e identificar acciones para rectificar cualquier desviación que se encuentre.   3. Monitorear la supervisión de hasta qué punto la SIC satisface las obligaciones (regulación, legislación, leyes comunes, contractuales), políticas internas, estándares y guías profesionales.   4. Monitorear los mecanismos regulares y rutinarios para garantizar que el uso de SIC cumpla con las obligaciones (regulación, legislación, leyes comunes, contractuales), estándares y guías (Incluídas las que estén orientadas a la seguridad de la información)   5. Analizar el impacto y las implicaciones generales del cambiante panorama de amenazas en la empresa.  6.Monitorear la eficacia y el rendimiento de aquellas partes interesadas a las que se le ha delegado la responsabilidad y autoridad para el gobierno empresarial de SIC. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Determinar si la empresa tiene un proceso de inteligencia de amenazas.  2. Formalizar el proceso de monitoreo documentado y estandarizado para el monitoreo del sistema de gobierno de SIC. Esto incluye definir los pasos y actividades necesarias, los roles y responsabilidades de los involucrados, los documentos de referencia y los entregables del proceso. El proceso de monitoreo debería definir:  2.1 Los indicadores clave del desempeño relevantes para el gobierno de SIC, alineados con las metas empresariales y que permitan medir el rendimiento y efectividad del sistema de gobierno.  2.2 Los criterios de monitoreo, límites y umbrales para cada uno de los indicadores definidos.  2.3 Métodos de análisis y responsables de las decisiones sobre las acciones correctivas frente a desviaciones de los KPI definidos. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Identificar y utilizar herramientas y sistemas de monitoreo adecuados para recopilar y analizar los datos necesarios. Esto puede incluir el uso de software de monitoreo de seguridad, sistemas de generación de informes, paneles de control u otras soluciones tecnológicas. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Proporcionar la supervisión de la eficacia del sistema de control de la empresa y el cumplimiento con el mismo. |

# Preguntas de Auditoría para Monitorear el Sistema de Gobierno

|  |
| --- |
| 3.1 Temática: Evaluar el monitoreo de los mecanismos del Sistema de Gobierno. |
| Al asegurar que estos mecanismos funcionen de manera eficiente, se optimiza la detección, prevención y respuesta ante incidentes de seguridad. La consistencia y repetibilidad en su implementación aseguran que los estándares y procedimientos se sigan de manera uniforme en toda la organización, lo que ayuda a evitar brechas y vulnerabilidades en la seguridad.   * ¿Se evalúa la eficacia de los mecanismos SIC acordados? ¿Existen indicadores clave de rendimiento asociados? * ¿Se verifica que los mecanismos de SIC operan de forma consistente y repetibles? ¿Son coherentes con los acuerdos y estándares establecidos, y no existen conflictos o contradicciones entre ellos? ¿Se implementan de manera uniforme en toda la organización? * ¿Se realiza un seguimiento y un monitoreo periódico para el análisis de desviaciones? ¿Se toman medidas para corregir estas desviaciones? |

|  |
| --- |
| **3.2 Temática: Monitoreo del diseño de Gobierno y rectificaciones de cualquier desviación.** |
| El monitoreo de la eficacia del diseño de gobierno es esencial para asegurar que la estructura y los procesos que rigen una organización funcionen de manera efectiva y eficiente. El objetivo principal de este monitoreo es garantizar que la organización alcance sus metas y objetivos de manera adecuada y que las políticas y estrategias establecidas sean implementadas de manera coherente.   * ¿Se evalúa el cumplimiento de los mecanismos SIC acordados, tales como procesos, estructuras y principios? ¿Se compara su cumplimiento con los objetivos y metas definidas? * ¿Cuál es el nivel de consistencia de los mecanismos SIC en la organización? * ¿ Se realizan revisiones, evaluaciones y se asegura la implementación de manera uniforme en todas las áreas? * ¿Se mide el tiempo promedio de implementación de acciones de gobierno empresarial? ¿Están estos definidos con plazos acordados y objetivos definidos? ¿Se cumplen? * ¿Se mide la gestión del cambio y el cumplimiento de los procesos de gestión de cambios en el gobierno empresarial? |

|  |
| --- |
| **3.3 Temática: Monitoreo de la satisfacción de las obligaciones de cumplimiento.** |
| La supervisión de cumplimiento de obligaciones, políticas internas, estándares y guías profesionales es esencial para asegurar el cumplimiento normativo, proteger contra riesgos de seguridad, garantizar la adhesión a políticas internas, estándares y guías profesionales, evaluar el desempeño de la SIC y responder rápidamente a incidentes de seguridad.   |  | | --- | | ℹ Estas prácticas de auditoría se desarrollan con más profundidad en el  control: Monitorear el compromiso de las partes interesadas. |  * ¿Se mide el cumplimiento de plazos y objetivos establecidos en materia de cumplimiento de obligaciones, políticas internas, estándares y guías profesionales? ¿Mantienen los mecanismos y herramientas adecuadas para realizarlo? * ¿Existe un indicador especifico? ¿Se realiza un seguimiento de este y se toman medidas en caso de desviaciones? * ¿Existen registros de cambios o actualizaciones que incluyan modificaciones por lecciones aprendidas u otras medidas para corregir desviaciones? |

|  |
| --- |
| **3.4 Temática: Monitoreo de los mecanismos para garantizar se cumplan los requerimientos del Sistema de Gobierno en SIC.** |
| El objetivo principal de este monitoreo es asegurar que las prácticas y procedimientos de seguridad de la organización estén alineados con las políticas internas, regulaciones legales, contratos y estándares de la industria, para proteger eficazmente los activos de información y prevenir posibles riesgos y amenazas a la seguridad de la información.   |  | | --- | | ℹ Estas prácticas de auditoría se desarrollan con más profundidad en los controles: Monitorear el cumplimiento de los requerimientos legales y regulatorios. |  * ¿Se mide el nivel de cumplimiento del cumplimiento de políticas por parte de las partes interesadas? ¿Se establecen KPI específicos para el cumplimiento de políticas? * ¿Se mide el índice de cumplimiento normativo? * Verifique que existe indicador de cumplimiento de las obligaciones normativas y regulatorias de SIC y que sea parte de los tableros de control clave de la organización. * ¿Se mide el nivel de cumplimiento de regulaciones y legislación? ¿El nivel de cumplimiento está acorde a los requisitos legales aplicables? * ¿Se mide el nivel de cumplimiento de políticas internas establecidas en materia de gobierno empresarial de ciberseguridad? * ¿Se monitorea y registra regularmente el rendimiento de estas mediciones?   ¿Existen los mecanismos apropiados para realizarlo? |

|  |
| --- |
| 3.5 Temática: Monitoreo de la eficacia y rendimiento de los responsables del Gobierno empresarial de SIC. |
| El monitoreo del rendimiento de partes interesadas con responsabilidad y autoridad radica en asegurar una gestión adecuada y eficiente de la seguridad de la información dentro de la organización. Es crucial para evaluar el cumplimiento de sus responsabilidades, identificar áreas de mejora, garantizar la eficacia de las políticas y estrategias de SIC, asegurar el uso adecuado de los recursos, medir el nivel de madurez de la SIC, facilitar la rendición de cuentas y garantizar la continuidad del negocio.   |  | | --- | | ℹ Estas prácticas de auditoría se desarrollan con más profundidad en los  controles asociados al Dominio IV: Gestión de RRHH |  * ¿Se han identificado las partes interesadas responsables de la supervisión de la SIC, como el Comité de Seguridad de la Información, el Oficial de Seguridad de la Información (CISO), ¿los gerentes de TI y otros roles relevantes dentro del monitoreo? ¿Existen controles adecuados para asegurar el cumplimiento de las políticas y estándares? * ¿Se mide la eficacia y el rendimiento de los responsables del gobierno empresarial de SIC? ¿Existen indicadores clave de desempeño (KPI) para medirlos? * Verifique que estas medidas de desempeño se encuentran alienadas con los perfiles de cargo, que son parte de los esquemas de control y que son conocidas por quienes ostentan los cargos. * ¿Se toman medidas para abordar cualquier deficiencia o desviación identificada? ¿Se realizan seguimientos de las acciones correctivas? * Verifique la existencia de un registro de acciones correctivas, así como de un manual o instructivo integrado en los procesos de gestión de personas. |

|  |
| --- |
| 3.6 Temática: Monitoreo de los objetivos y metas de desempeño. |
| El establecimiento de objetivos y metas de desempeño, así como la recopilación de datos para la toma de decisiones y la mejora continua del proceso de monitoreo del sistema de gobierno, es esencial para asegurar la eficacia y la eficiencia de este proceso. Los objetivos y metas proporcionan una dirección clara y una visión de lo que se quiere lograr con el monitoreo, mientras que la recopilación de datos proporciona información fundamentada para evaluar el progreso y tomar decisiones informadas.   * ¿Se ha realizado el proceso de selección adecuado de herramientas y sistema de monitoreo, con KPI y porcentajes de cumplimiento y numero de criterios de selección definidos? * ¿Se consideraron los requisitos de la organización, como los objetivos de monitoreo, los tipos de dato a recopilar y analizar, y las capacidades técnicas requeridas? * ¿Se mide la efectividad de las herramientas implementadas en términos de recopilación, análisis y presentación de datos relevantes para la seguridad? * ¿Se verifica la medición de la efectividad de las herramientas y sistemas de monitoreo? * Verifique si se cumplen los tiempos definidos para los indicadores clave de los procesos críticos establecidos en el sistema de gobierno, por ejemplo: * Verifique si se cumplen, contra los umbrales definidos, el tiempo medio de detección. * Verifique si se cumplen, contra los umbrales definidos, el tiempo de respuesta a incidentes de seguridad. * ¿Se realizan mejoras en el proceso de monitoreo del sistema de gobierno, acorde a la información recopilada, lecciones aprendidas o análisis de brechas y oportunidades? ¿Se consideran indicadores clave del monitoreo del sistema de gobierno? * Ciclo de vida real vs. objetivo para decisiones clave. * Frecuencia de revisiones independientes del gobierno de SIC. * Nivel de satisfacción de las partes interesadas, por ejemplo, medido a partir de encuestas. * Número de problemas de gobierno de SIC comunicados a las partes interesadas relevantes. |