Pantalla de computadora con imágen de hombre

Descripción generada automáticamente con confianza media

**CASIG 1 – Gobernanza de la Ciberseguridad**

**Preguntas de Auditoría**

**Monitorear el Compromiso de las Partes Interesadas**

1. Visión General

Monitorear el compromiso de las partes interesadas en la función de seguridad de la información y ciberseguridad (SIC) comienza con la definición de una estrategia de consulta y comunicación específica para las partes interesadas internas y externas, estableciendo los mecanismos necesarios para asegurar que toda la información y los informes de SIC cumplan con los criterios obligatorios de la empresa. Además, la creación de un sistema de monitoreo basado en indicadores clave de rendimiento (KPI) permite evaluar el estado de seguridad de la información y la gestión de riesgos en función de métricas cuantitativas, lo que facilita una comprensión clara y transparente del compromiso organizacional con la seguridad.

**1.1 Establecimiento de Procesos y Equipos para el Monitoreo del Compromiso de las Partes Interesadas**

Para apoyar el monitoreo eficaz, es fundamental establecer un equipo especializado que supervise el cumplimiento de los requisitos de comunicación y reporte de las partes interesadas. Este equipo debe operar bajo un proceso formal documentado que asegure la consistencia en la recopilación, evaluación y comunicación de los resultados de monitoreo a todas las partes interesadas relevantes. El uso de técnicas de análisis de datos permite identificar patrones y tendencias, impulsando mejoras en el marco de gobierno de SIC basadas en hallazgos específicos. Además, la implementación de metas cuantitativas y métricas específicas de desempeño asegura que el equipo pueda evaluar la efectividad de los mecanismos de monitoreo y ajuste, promoviendo un compromiso continuo y bien fundamentado con cada grupo de partes interesadas.

**1.2 Rol de la Auditoría en el Monitoreo del Compromiso de las Partes Interesadas en SIC**

Desde la perspectiva de auditoría, el monitoreo del compromiso de las partes interesadas en SIC implica una revisión exhaustiva de los mecanismos de monitoreo y comunicación establecidos, evaluando su eficacia en la generación de informes, el cumplimiento de métricas y el fortalecimiento del compromiso de las partes interesadas. La auditoría realiza análisis cuantitativos y comparativos detallados que verifican el desempeño de estos mecanismos y su alineación con los objetivos organizacionales. A través de la retroalimentación obtenida en auditorías y la respuesta de las partes interesadas, se impulsa la mejora continua de los mecanismos de monitoreo, permitiendo a SIC adaptarse a las necesidades emergentes y optimizar la confianza y el alineamiento con los objetivos estratégicos de seguridad de la organización.

# Matriz de Controles

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Dirigir el establecimiento de la estrategia de consulta y comunicación para las partes interesadas externas e internas.  2. Dirigir la implementación de mecanismos para asegurar que la información cumple con todos los criterios de los requisitos de elaboración de informes obligatorios de SIC para la empresa.  3. Establecer mecanismos para la validación y aprobación de la elaboración de informes obligatorios 4. Establecer el monitoreo y la generación de informes de seguridad de la información (p. ej., utilizando indicadores clave de rendimiento [KPI] para la seguridad de la información y la gestión de riesgos de la información que se basan en métricas y mediciones en el dominio MEA). |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Establecer un equipo responsable de monitorizar el compromiso y los requisitos de reportes de las partes interesadas en relación con la gestión de SIC. 2. Establecer un proceso formal y documentado de monitorización del compromiso y los requisitos de reportes de las partes interesadas en relación a la gestión de SIC. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1.Utilizar técnicas de análisis de datos para identificar tendencias, patrones y áreas de mejora en el compromiso de las partes interesadas. 2. Comunicar los resultados del monitoreo a las partes interesadas relevantes y utilizar la retroalimentación recibida para impulsar mejoras y ajustes en el marco de gobierno de SIC. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Establecer metas cuantitativas específicas para evaluar la efectividad de los mecanismos de monitoreo del compromiso de las partes interesadas en el marco de gobierno de SIC. 2. Implementar un sistema de seguimiento y control continuo del desempeño en relación con el monitoreo del compromiso de las partes interesadas, utilizando métricas y KPIs. 3. Realizar análisis cuantitativos y comparativos detallados para evaluar la eficacia de los mecanismos de monitoreo y su contribución al fortalecimiento del compromiso de las partes interesadas. |
| 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 los mecanismos de monitoreo del compromiso de las partes interesadas en el marco de gobierno de SIC basándose en los resultados de las auditorías, análisis cuantitativos y retroalimentación de las partes interesadas. |

# Preguntas de Auditoría para Monitorizar el Compromiso de las Partes Interesadas

|  |
| --- |
| **3.1 Temática: Revisión del Marco de Gobierno de SIC** |
| Este tema implica evaluar y analizar el marco de gobierno establecido por la organización para supervisar y garantizar el compromiso de las partes interesadas en relación con la seguridad de la información y ciberseguridad (SIC). Esta práctica se enfoca en verificar si la organización tiene en su lugar una estructura sólida para gestionar las expectativas y requisitos de las partes interesadas relacionados con la seguridad de la información y si se monitorea adecuadamente el cumplimiento de estos compromisos.   |  | | --- | | **Atención**: Más ejemplos de pruebas de auditoría sobre este tema puede ser encontrado en el tema: “Compromiso de las Partes Interesadas”. |   Este levantamiento puede incluir análisis específicos tales como:   * ¿Se han implementado acciones de mejora y ajustes en el marco de gobierno de SIC en respuesta a la retroalimentación recibida por el resultado del monitoreo a las partes interesadas relevantes?   + Revise los tipos de acciones de mejora que se han llevado a cabo en el marco de gobierno de SIC como resultado de la retroalimentación recibida. * ¿Cuál ha sido la efectividad de las acciones implementadas en el marco de gobierno de SIC para abordar las preocupaciones planteadas por las partes interesadas? * Revise si estas mejoras han permitido abordar los problemas identificados y mejorar la entrega de valor. * ¿Se analizan los mecanismos establecidos para monitorear el compromiso de las partes interesadas en el marco de gobierno?   + Verifique la existencia de metas cuantitativas específicas establecidas para evaluar la efectividad de estos mecanismos.   + Evalúe los mecanismos actuales utilizados para monitorear el compromiso de las partes interesadas en el marco de gobierno.   + Revise los documentos, políticas, procedimientos y las diferentes evidencias de los mecanismos de monitoreo implementados en la organización. |

|  |
| --- |
| **3.2 Temática: Mecanismos de monitoreo de las partes interesadas** |
| Esta Tema se enfoca en verificar la efectividad de los mecanismos y procesos establecidos para supervisar y evaluar el compromiso y la participación de las partes interesadas en la gestión de la ciberseguridad de la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se han identificado y considerado adecuadamente las partes interesadas internas y externas relevantes?   + Revise si se han establecido mecanismos para involucrarlas en el proceso de consulta y comunicación. * Evalúe la contribución de los mecanismos de monitoreo al fortalecimiento del compromiso de las partes interesadas.   + ¿Los resultados obtenidos a través de los mecanismos de monitoreo se utilizan para tomar decisiones, implementar mejoras o fortalecer las relaciones con las partes interesadas? * ¿El equipo responsable realiza un monitoreo regular y sistemático del cumplimiento de los compromisos y requisitos de reportes de las partes interesadas?   + Revise que mecanismos utilizados por el equipo responsable para llevar a cabo dicho monitoreo. * ¿En la organización hay procedimientos establecidos para comunicar los resultados del monitoreo a las partes interesadas relevantes?   + Verifique que exista un plan de comunicación claro y efectivo para la entrega de resultados del monitoreo a las partes interesadas relevantes.   + Evalúe si existe un plan de comunicación que abarque la entrega de resultados, la identificación de problemas y las acciones correctivas propuestas. * ¿Se evalúa la forma en que se comunican los resultados del monitoreo a las partes interesadas?   + Revise los criterios que se utilizan para asegurar que las comunicaciones de los resultados y verifique si son claros, precisos y comprensibles para las partes interesadas.   + Evalúe si se utiliza un lenguaje apropiado para comunicar los resultados del monitoreo a las partes interesadas. * ¿Se recopila la retroalimentación recibida de las partes interesadas sobre los resultados del monitoreo?   + Verifique si se registra adecuadamente la retroalimentación recibida de las partes interesadas sobre los resultados del monitoreo.   + ¿Se realiza un análisis de retroalimentación para identificar áreas de mejora? * ¿Se evalúa la claridad y especificidad de las metas cuantitativas establecidas, para asi revisar la efectividad de los mecanismos de monitoreo?   + Verifique que las metas cuantitativas sean adecuadas y relevantes para medir el compromiso y la participación de las partes interesadas en relación con la ciberseguridad. * Revise los resultados obtenidos a través de los mecanismos de monitoreo del compromiso de las partes interesadas.   + ¿Los resultados reflejan el compromiso esperado, o se detectan desviaciones significativas? * ¿Se han implementado acciones correctivas en respuesta a hallazgos anteriores o problemas identificados en los mecanismos de monitoreo? |

|  |
| --- |
| **3.3 Temática: Compromiso de las partes interesadas** |
| Es un proceso esencial para garantizar que las partes interesadas relevantes estén adecuadamente comprometidas y cumpliendo con los requisitos de seguridad establecidos. Esta práctica se enfoca en evaluar la participación activa y responsable de las partes interesadas clave en el proceso de ciberseguridad de la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se realiza la revisión de los compromisos establecidos con las partes interesadas con relación a la gestión de SIC para garantizar que estén * debidamente documentados, con plazos definidos y responsables asignados para cumplir los compromisos de reporte? * ¿Se realiza el análisis de la documentación de reportes generada en relación a la gestión de SIC?   + Verifique si los reportes cumplen con los requisitos establecidos por las partes interesadas y proporcionan la información necesaria de manera clara y precisa. * ¿Se obtiene retroalimentación de las partes interesadas sobre la calidad y utilidad de los reportes recibidos?   + Evalúe si los reportes satisfacen las necesidades de las partes interesadas y si se han tomado acciones correctivas en caso de insatisfacción. * ¿Se evalúan las técnicas utilizadas para analizar los datos de compromiso de las partes interesadas, verificando si se emplean técnicas adecuadas como minería de datos, análisis de tendencias o segmentación? * ¿Se lleva a cabo el análisis de los datos recopilados para identificar tendencias y patrones significativos en el compromiso de las partes interesadas, así como para detectar cambios o variaciones en el compromiso a lo largo del tiempo, y cuál es el proceso para determinar las causas subyacentes de dichos cambios o variaciones? * ¿Se evalúan los resultados del análisis de datos para identificar áreas de mejora en el compromiso de las partes interesadas y detectar brechas o desviaciones en relación con los objetivos o expectativas establecidas? * Revise si la organización realiza un análisis de los informes de auditoría relacionados con el compromiso de las partes interesadas en el marco de gobierno.   + Verifique los hallazgos, recomendaciones o áreas de mejora identificadas en relación con el compromiso de las partes interesadas. * ¿Qué métodos utiliza la organización para recopilar la retroalimentación de las partes interesadas sobre su nivel de compromiso en el marco de gobierno? * Revise la retroalimentación recibida y evalúe la satisfacción y percepción de las partes interesadas sobre su participación en el proceso de seguridad de la información y ciberseguridad. |

|  |
| --- |
| **3.4 Temática: Comunicación efectiva y los canales de comunicación** |
| La práctica es fundamental para asegurar que la información relevante sobre ciberseguridad se transmita adecuadamente entre todas las partes involucradas. Se sugiere Evaluar la eficiencia y efectividad de los canales de comunicación existentes. Es importante asegurarse de que la información proporcionada a través de los canales de comunicación sea accesible y comprensible para todas las partes interesadas. Si la terminología técnica se utiliza, debe ir acompañada de explicaciones claras y sencillas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha analizado la documentación relacionada con la estrategia de consulta y comunicación establecida para determinar si se ha definido claramente la estrategia, incluyendo los objetivos, las partes interesadas relevantes y los canales de comunicación a utilizar? * ¿Se evalúa la eficacia de los canales de comunicación utilizados para interactuar con las partes interesadas?   + Verifique si se emplean diversos métodos y medios de comunicación para llegar de manera efectiva a las diferentes partes interesadas.   + Revise la calidad de la comunicación para verificar si se proporciona   + información relevante y oportuna a las partes interesadas con el fin de mantenerlos informados sobre asuntos importantes. * Evalúe la efectividad de la comunicación entre la función de Seguridad de la Información y las partes interesadas en relación con los compromisos y requisitos de los reportes.   + ¿Se han establecido canales adecuados de comunicación y se ha proporcionado la información requerida de manera oportuna? * ¿Se revisa documentos para evaluar el cumplimiento de las metas establecidas, incluyendo informes, registros de reuniones y comunicaciones con las partes interesadas? |

|  |
| --- |
| 3.5 Temática: Definiciones de las métricas e indicadores clave para los mecanismos de monitoreo |
| Las practica tiene como objetivo asegurarse de que las medidas utilizadas para medir el compromiso de las partes interesadas sean efectivas, relevantes y proporcionen una visión clara del grado de implicación y satisfacción de las partes interesadas en relación con la ciberseguridad. Se definen las métricas e indicadores clave que permitirán evaluar el compromiso, una vez recopilados los datos, se realiza un análisis exhaustivo. Los resultados obtenidos se comparan con los objetivos y metas establecidos previamente. Esto permite determinar si se están alcanzando los niveles deseados de compromiso y detectar desviaciones que requieran atención.  Este levantamiento puede incluir análisis específicos tales como:   * Evalúe de la disponibilidad y calidad de los datos utilizados en el análisis de compromiso   + Verifique la integridad y precisión de los datos recopilados y almacenados en los sistemas correspondientes. * ¿Se han definido métricas y KPIs específicos para monitorear el compromiso de las partes interesadas?   + Verifique que estas métricas y KPIs están alineados con los objetivos estratégicos de la organización y reflejan los aspectos clave del compromiso de las partes interesadas. * ¿Se realiza un análisis y evaluación regular de los resultados obtenidos a través del monitoreo del compromiso de las partes interesadas?   + Verifique que se utilicen los KPIs y métricas definidas para medir el rendimiento, identificar tendencias y áreas de mejora, y se toman acciones correctivas cuando sea necesario. * ¿Se evalúa la efectividad de los mecanismos de monitoreo en términos de su capacidad para recopilar información relevante y verificar si proporcionan datos cuantitativos y comparativos detallados sobre el desempeño y la contribución de las partes interesadas? * ¿Se revisa los análisis cuantitativos para medir el nivel de compromiso de las partes interesadas y su evolución en el tiempo?   + Compare los resultados obtenidos con metas o estándares establecidos, así como con datos de referencia o benchmarks externos. * ¿Se ha implementado un sistema que permita el seguimiento y control continuo del desempeño en relación con el compromiso de las partes interesadas?   + ¿Qué aspectos se deben verificar para asegurarse de que el sistema   + incluya la recopilación regular de los datos relevantes, el análisis de las métricas y KPIs, y la generación de informes para respaldar la toma de decisiones en el ámbito de la ciberseguridad? * ¿Se evalúa si se monitorean de manera efectiva las actividades y acciones para fomentar y mantener el compromiso de las partes interesadas?   + Verifique el uso de indicadores específicos KPI para evaluar la efectividad de estas acciones y actividades, tales como la participación en capacitaciones, la retroalimentación recibida, la adopción, entre otros. * ¿Se recopilan datos cuantitativos relevantes relacionados con el compromiso de las partes interesadas?   + Evalúe los análisis estadísticos o métricos para verificar la efectividad y el nivel de compromiso de las partes interesadas. |