

**1- Políticas de Control de Acceso e Identidad**



**CASIG 1 – Gobierno de la Ciberseguridad**

**Preguntas de Auditoría**

**Evaluar el Compromiso y Requisitos de las Partes Interesadas**

|  |
| --- |
| **Competencias Básicas del Auditor**   1. **-** Conocimientos en normativa de seguridad de la información y ciberseguridad 2. - Conocimientos en gobierno y gestión. 3. - Conocimiento de las partes interesadas. 4. - Conocimientos sobre gobernanza corporativa. |

# Visión General

Evaluar el compromiso y los requisitos de las partes interesadas en la función de seguridad de la información y ciberseguridad (SIC) comienza con la identificación y categorización de todas las partes interesadas, tanto internas como externas, agrupándolas según requisitos similares. Evaluar los requisitos de informes obligatorios actuales y futuros, incluyendo los relacionados con regulaciones, leyes y contratos, permite a SIC anticiparse a las demandas de información, ajustando el nivel de detalle, la frecuencia y el alcance de los informes. Además, se determinan los medios y canales adecuados para comunicar temas de seguridad de la información, asegurando que las comunicaciones sean comprensibles tanto para audiencias de TI como de áreas no técnicas.

**1.1 Establecimiento de Procesos y Equipos para la Gestión de Compromiso y Requisitos de Reportes**

Para gestionar eficazmente el compromiso y los requisitos de reportes de las partes interesadas, es fundamental establecer un equipo específico y un proceso formal documentado para evaluar sus necesidades y expectativas en relación con SIC. Este proceso debe incluir la definición de principios de comunicación que especifiquen los formatos, canales y procedimientos para la aceptación y firma de informes, proporcionando transparencia y una estructura coherente en cada interacción. Comunicar los resultados de esta evaluación a las partes interesadas fortalece la transparencia y asegura una comprensión mutua de las expectativas y compromisos, facilitando una cooperación alineada con los objetivos de SIC.

**1.2 Rol de la Auditoría en la Evaluación del Compromiso y Requisitos de las Partes Interesadas en SIC**

Desde la perspectiva de auditoría, evaluar el compromiso y los requisitos de las partes interesadas en SIC implica realizar un seguimiento y control continuo del desempeño en relación con los compromisos de comunicación y reporte. Los auditores revisan el uso de métricas y KPIs para medir la efectividad de los procesos, además de realizar análisis cuantitativos y comparativos detallados para evaluar el cumplimiento de las expectativas de las partes interesadas. La auditoría también fomenta la mejora continua mediante la retroalimentación basada en los hallazgos de auditorías y análisis previos. Al ajustar los procesos de comunicación y reporte según estos resultados, SIC puede optimizar su relación con las partes interesadas, asegurando una comunicación efectiva y proactiva que refuerce la confianza y el alineamiento con los objetivos de seguridad de la información.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Identificar todas las partes interesadas de SIC relevantes dentro y fuera de la empresa. Agrupar a las partes interesadas en categorías de partes interesadas con requisitos similares.  2. Examinar y juzgar los requisitos de informes obligatorios actuales y futuros relacionados con el uso de SIC dentro de la empresa (regulación, legislación, leyes comunes, contractuales), incluidos su alcance y frecuencia.  3. Examinar y juzgar los requisitos de comunicación e informes actuales y futuros para otras partes interesadas relacionados con el uso de SIC dentro de la empresa, incluidos el nivel requerido de participación/consulta y el alcance de la comunicación/nivel de detalle y condiciones. 4. Determinar la audiencia, incluidos individuos o grupos internos y externos, para la comunicación y la presentación de informes sobre actividades relacionadas con la seguridad de la información. 5. Identificar los requisitos para informar sobre la seguridad de la información a las partes interesadas (p. ej., qué información se requiere, cuándo se requiere, cómo se presenta) Deben estar estructurados de manera que sean fáciles de entender para las partes interesadas de TI y no TI. 6. Identificar los medios y canales para comunicar los temas de seguridad de la información. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Establecer un equipo responsable de evaluar el compromiso y los requisitos de reportes de las partes interesadas en relación a la gestión de SIC. 2. Establecer un proceso formal y documentado de evaluación 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. Mantener los principios para la comunicación con partes interesadas externas e internas, incluidos formatos y canales de comunicación, así como la aceptación y firma de informes de las partes interesadas. 2. Comunicar de manera efectiva los resultados de la evaluación a las partes interesadas relevantes, asegurando la transparencia y la comprensión mutua. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Implementar un sistema de seguimiento y control continuo del desempeño en relación con el compromiso y los requisitos de reportes de las partes interesadas, utilizando métricas y KPIs 2. Realizar análisis cuantitativos y comparativos detallados para evaluar la efectividad del compromiso y los requisitos de reportes de las partes interesadas en relación con la gestión de SIC. |
| 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 procesos de evaluación del compromiso y los requisitos de reportes de las partes interesadas en relación con la gestión de SIC basándose en los resultados de las auditorías, análisis cuantitativos y retroalimentación de las partes interesadas. |

# Preguntas de Auditoría para Compromiso y Requisitos de las Partes Interesadas

|  |
| --- |
| 3.1 Temática: Revisiones de las políticas, procedimientos y contratos |
| Revisar las políticas, normativas y contratos relacionados con la ciberseguridad y la gestión de partes interesadas. Esto permitirá evaluar si la organización tiene en cuenta las expectativas y requisitos de las partes interesadas y si ha establecido controles adecuados para abordarlos. Este levantamiento puede incluir análisis específicos tales como:   * Revise la documentación relacionada con la gestión de partes interesadas en SIC, como planes estratégicos, informes de gestión, políticas y procedimientos.   + Verifique si se menciona la identificación y categorización de partes interesadas relevantes. * ¿Se examinan los contratos y acuerdos vigentes de la empresa, tanto internos como externos, para evaluar los requisitos de informes en materia de seguridad de la información y los compromisos específicos establecidos en términos de alcance y frecuencia de los informes?   + Revise los contratos con proveedores, acuerdos de confidencialidad, contratos de servicios de seguridad u otros tipos de acuerdos relacionados. * ¿Se evalúan los requisitos identificados en las políticas, procedimientos y documentos relacionados con la seguridad de la información para informar a las partes interesadas sobre este tema?   + Revise si existe alguna información específica que se deba proporcionar en los informes. * ¿Se establece la frecuencia de los informes y los formatos de presentación? * Revise la documentación como políticas, procedimiento, acuerdos o contratos para evaluar los requisitos de comunicación e informes de las partes interesadas relacionados con SIC. * ¿Se abordan adecuadamente los requisitos de comunicación e informes de las partes interesadas en la documentación existente? * ¿Qué medios y canales de comunicación se encuentran en las políticas, procedimientos y documentos relacionados con la seguridad de la información para tratar temas de seguridad? |

|  |
| --- |
| 3.2 Temática: Evaluaciones del compromiso de las partes interesadas |
| Las pruebas se centrarán en obtener evidencias confiables y relevantes que me permitan comprender y evaluar adecuadamente el grado de compromiso de las partes interesadas en el gobierno de la ciberseguridad.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Están claramente definidos y asignados en la organización los roles y responsabilidades específicos relacionados con la evaluación del compromiso y los requisitos de reportes de las partes interesadas en relación con la gestión de Seguridad de la Información? * ¿Los roles y responsabilidades aparecen en la estructura organizativa de la empresa, se identifican los equipos, departamentos o roles específicos encargados de la gestión de la seguridad de la información?   + ¿Cuáles son los pasos del proceso de evaluación del compromiso y los requisitos de reportes de las partes interesadas en relación con la ciberseguridad? * Revise si se identifican las partes interesadas relevantes durante la evaluación. * ¿Se evalúa el nivel de compromiso de las partes interesadas con respecto a la ciberseguridad? * ¿Los procesos de evaluación del compromiso y los requisitos de reportes está debidamente documentado? * Revise si se ha creado un procedimiento formal que describa los pasos, las responsabilidades, los plazos y los criterios utilizados en la evaluación. * ¿La documentación está disponible y es conocida por otras partes interesadas relevantes?   + Verifique que esta documentación esté disponible y sea conocida por los responsables de la gestión de SIC. * ¿Se examinan los informes y análisis previos relacionados con el compromiso y los requisitos de reportes de las partes interesadas?   + Verifique si se han llevado a cabo análisis cuantitativos y comparativos para evaluar la efectividad de dichos compromisos y requisitos.   + ¿Se realiza un análisis cuantitativo de los datos recopilados para evaluar el desempeño en términos de compromiso y requisitos de reportes? * Revise los procesos para examinar las métricas y los indicadores clave de rendimiento (KPIs) con el fin de identificar tendencias, oportunidades de mejora y posibles brechas en el cumplimiento de los requisitos. * ¿Cómo se recopila la retroalimentación de las partes interesadas relevantes sobre el compromiso y los requisitos de reportes?   + Revise los métodos que se utilizan, como encuestas, entrevistas u otros, para obtener sus comentarios y perspectivas.   + Evalúe si existen áreas en las que las partes interesadas expresan insatisfacción o sugieren mejoras. * ¿Con base en los hallazgos identificados, se han implementado acciones correctivas y mejoras en los procesos de evaluación del compromiso y los requisitos de reportes?   + ¿Qué medidas se toman para garantizar la asignación de responsabilidades claras y el establecimiento de plazos para la implementación de estas acciones? |

|  |
| --- |
| 3.3 Temática: Canales de Comunicación |
| Evaluar los canales de comunicación existentes utilizados por la organización para interactuar con las partes interesadas sobre ciberseguridad. Estos canales pueden incluir reuniones, boletines informativos, correos electrónicos, plataformas de colaboración, encuestas, entre otros. Determinar si los canales de comunicación actuales son efectivos para difundir información relevante sobre ciberseguridad y si permiten una comunicación bidireccional adecuada con las partes interesadas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Cómo se lleva a cabo la comunicación con las partes interesadas en la práctica?   + ¿Qué informes y comunicaciones se han enviado a las partes interesadas en relación con el objetivo de la auditoría? * ¿Se siguen los principios establecidos en las comunicaciones con las partes interesadas?   + Revise los formatos que se utilizan en los informes y comunicaciones dirigidos a las partes interesadas, verifique que sean claros y concisos en la entrega de resultados.   + Verifique los canales de comunicación que se emplean para interactuar con las partes interesadas.   + Revise que los informes sean aceptados y firmados por parte de las partes interesadas en el proceso de comunicación. * ¿Se examinan los canales de comunicación utilizados para transmitir los resultados de la evaluación a las partes interesadas?   + Evalúe los aspectos en relación con su adecuación y accesibilidad para las partes interesadas relevantes. * ¿Se revisa la claridad y el contenido de la comunicación transmitida a las partes interesadas en relación con la evaluación?   + Revise el uso de términos técnicos comprensibles para el público objetivo y se proporciona suficiente detalle y contexto para una comprensión completa de los resultados.   + Verifique si se asegura que los aspectos relevantes sean abordados y se proporciona la información necesaria para que las partes interesadas tomen decisiones informadas. |

|  |
| --- |
| 3.4 Temática: Sistemas de Seguimiento y Control |
| Al verificar los sistemas de seguimiento y control para la evaluación del compromiso y los requisitos de las partes interesadas, es importante asegurarse de que estos sistemas sean efectivos, confiables y estén alineados con los objetivos de ciberseguridad y las políticas establecidas por la organización.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se han establecido sistemas de seguimiento y control para monitorear el desempeño en relación con el compromiso y los requisitos de reportes de las partes interesadas?   + Verifique que herramientas tecnológicas, software especializado o sistemas internos se utilizan para recopilar y analizar los datos relevantes. * ¿Existe un sistema de monitoreo continuo para evaluar el impacto de las acciones correctivas implementadas?   + Revise si el sistema de monitoreo sigue de cerca los resultados obtenidos de las acciones correctivas implementadas.   + ¿Se lleva a cabo un seguimiento para determinar si las mejoras realizadas han generado cambios positivos?   + ¿El sistema de monitoreo evalúa el impacto en el compromiso de las partes interesadas en relación con la gestión de SIC? * ¿El sistema de monitoreo también evalúa el nivel de satisfacción de las partes interesadas respecto a la gestión de SIC?   + Evalúe si el sistema de monitoreo tiene en cuenta métricas y KPIs específicos para evaluar el compromiso y la satisfacción de las partes interesadas. * ¿Se analiza de manera continua y periódica la efectividad de las acciones correctivas implementadas?   + ¿Se utiliza la retroalimentación de las partes interesadas para mejorar las acciones correctivas y el sistema de monitoreo?   + Revise si se documentan y comunican los resultados del sistema de monitoreo y las mejoras obtenidas a las partes interesadas relevantes. |