

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



**CASIG 1 – Gobierno de la Ciberseguridad**

**Preguntas de Auditoría**

**Definir el Rol en la Cadena de Suministro**

|  |
| --- |
| **Competencias Básicas del Auditor**   1. Conocimientos en el funcionamiento y las interacciones dentro de la cadena de suministro. 2. Conocimientos en el marco legal y regulatorio aplicables a la ciberseguridad. 3. Conocimiento para identificar, analizar y evaluar los riesgos de 4. ciberseguridad en la cadena de suministro |

# Visión General

Definir el rol de la función de seguridad de la información y ciberseguridad (SIC) en la cadena de suministro implica dirigir la creación de una estrategia de comunicación que asegure que las necesidades, preferencias y expectativas de cada grupo de partes interesadas sean comprendidas y atendidas. La implementación de mecanismos de validación y aprobación de informes de ciberseguridad garantiza que toda la información compartida cumpla con los requisitos de elaboración de informes obligatorios. Además, el desarrollo de una matriz de comunicación permite identificar y coordinar los canales adecuados para una comunicación efectiva y bidireccional, utilizando herramientas tecnológicas que aseguren la transparencia y la responsabilidad en cada interacción.

**1.1 Mecanismos y Procesos para la Gestión de Compromiso y Reporte con Partes Interesadas**

Para optimizar la gestión de comunicación en la cadena de suministro, es fundamental establecer un equipo responsable de la coordinación, comunicación y elaboración de informes con las partes interesadas relevantes para SIC. La creación de procesos documentados asegura que los compromisos, reportes e intercambios de información se realicen de manera estructurada y transparente. Estos procesos incluyen mecanismos de escalamiento y documentación formal para los informes, y se apoyan en una retroalimentación continua para capturar las necesidades y preocupaciones de los involucrados. La elaboración de informes periódicos permite a las partes interesadas obtener una visión completa del estado de la seguridad de la información, abarcando actividades, desempeño, logros, perfil de riesgo, tecnologías emergentes y actualizaciones de la estrategia de SIC. Informes financieros detallados también respaldan la capacidad de análisis de costos y el monitoreo de inversiones en SIC, proporcionando a las partes interesadas datos financieros relevantes para la toma de decisiones.

**1.2 Rol de la Auditoría en la Evaluación y Mejora de la Gestión de Comunicación en la Cadena de Suministro**

Desde la perspectiva de auditoría, definir el rol de SIC en la cadena de suministro implica evaluar la efectividad de los procesos de comunicación y reporte establecidos con las partes interesadas. Los auditores revisan si se han implementado metas cuantitativas específicas para medir la efectividad del compromiso, asegurando que los mecanismos de comunicación sean adecuados y cumplan con las expectativas. La auditoría también examina los sistemas de revisión y mejora continua, que deben basarse en datos y resultados obtenidos a través de auditorías y análisis cuantitativos. Estos sistemas permiten optimizar la gestión de comunicación con las partes interesadas, promoviendo un enfoque adaptativo y colaborativo que fortalece las relaciones y asegura la protección de la seguridad de la información en toda la cadena de suministro.

# Modelo de Madurez

|  |  |
| --- | --- |
| 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 ciberseguridad para la empresa.  2.1 Asegurar que se desarrolla una matriz de comunicación que identifique las necesidades, preferencias y expectativas de cada grupo de partes interesadas relevante. 3. Establecer mecanismos para la validación y aprobación de la elaboración de informes obligatorios. 4. Asegurar que se establecen canales de comunicación efectivos y bidireccionales con las partes interesadas relevantes, utilizando herramientas y tecnologías adecuadas. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Establecer un equipo responsable de la gestión de compromiso, comunicación y reporte con las partes interesadas relevantes para la función de SIC. 2. Desarrollar y documentar procesos claros y estructurados para el compromiso, la comunicación y el reporte con las partes interesadas relevantes.  2.1. Establecer formalmente los mecanismos de escalamiento y documentación de los informes 3. Establecer mecanismos de retroalimentación y consulta con las partes interesadas relevantes para recopilar sus necesidades, expectativas y preocupaciones en relación con la función de SIC. 4. Asegurar que se producen para las partes interesadas informes regulares sobre el estado de la seguridad de la información y la estrategia SIC que incluya:  1.1 Actividades de seguridad de la información  1.2 Desempeño  1.3 Logros   1.4 Perfil de riesgo   1.5 Beneficios comerciales  1.6 Tecnologías emergentes  1.7 Riesgo pendiente   1.8 Brechas de capacidad  1.9 Actualizaciones de la estrategia de SIC 5. Asegurar que se producen para las partes interesadas informes financieros regulares con detalle suficiente para permitir capacidades de análisis detallado y de costos, así como también, datos financieros relacionados con las inversiones en SIC |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Realizar evaluaciones internas y externas para medir la eficacia del programa de gobierno de la seguridad de la información. |
| 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 del compromiso, la comunicación y el reporte con las partes interesadas relevantes |
| 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. Asegurar que se mejoran continuamente los procesos y mecanismos de compromiso, comunicación y reporte con las partes interesadas relevantes, basándose en los resultados de las auditorías, análisis cuantitativos y retroalimentación de las partes interesadas. 2. Asegurar que se establece un sistema de revisión y mejora continua basado en datos y resultados para optimizar el compromiso, la comunicación y el reporte con las partes interesadas relevantes. |

# Preguntas de Auditoría para Dirigir el Compromiso, Comunicación y Reporte de las Partes Interesadas

|  |
| --- |
| 3.1 Temática: Evaluaciones del proceso de gestión de riesgos de las partes interesadas. |
| Se enfoca en asegurar que exista un proceso sólido y efectivo para identificar, evaluar, mitigar y monitorear los riesgos relacionados con la comunicación y el compromiso con todas las partes interesadas, tanto internas como externas, en el ámbito de la ciberseguridad.   |  | | --- | | ℹ Estas prácticas de auditoría son claves en el proceso de Gestión de Riesgos, por ello, se encuentran contenidas en los controles: Dirigir la Gestión de Riesgos, Evaluar la Gestión de Riesgos, Monitorizar la  Gestión de Riesgos y el Proceso de Gestión de Riesgos |  * ¿Cómo se involucran las partes interesadas externas e internas en el proceso de gestión de riesgos?   + Revise los mecanismos para solicitar la opinión de las partes interesadas y obtener retroalimentación sobre el proceso de gestión de riesgos, como lo son entrevistas, encuestas o reuniones.   + Revise si se considera las preocupaciones de las partes interesadas al llevar a cabo la gestión de riesgos. * ¿Se comunica la gestión de riesgos a las partes interesadas externas e internas?   + Revise si existen canales de comunicación claros y efectivos para la gestión de riesgos, como boletines informativos, informes periódicos, comunicados de prensa, redes sociales, reuniones o intranet corporativa. * ¿Se promueve la transparencia en la comunicación de la gestión de riesgos?   + Verifique que la información sobre la gestión de riesgos se presenta de manera comprensible y accesible para las partes interesadas. |

|  |
| --- |
| 3.2 Temática: Compromisos de Cumplimiento |
| Se centra en asegurar que los compromisos establecidos con las partes interesadas en materia de ciberseguridad se cumplan de manera efectiva. Esta práctica es fundamental para evaluar el compromiso y comunicación, así como para garantizar la transparencia y rendición de cuentas en el proceso de reporte a las partes interesadas.   |  | | --- | | ℹ Estas prácticas de auditoría se encuentran contenidas y complementan al control “Asegurar el Cumplimiento de Requerimientos Legales y Regulatorios” |  * ¿Existe en la estructura organizativa de la empresa un equipo específico o una función designada para la gestión de compromiso, comunicación y reporte con las partes interesadas en el ámbito de la Seguridad de la Información y Ciberseguridad? * ¿Existe documentación relacionada con la gestión de compromiso, comunicación y reporte con las partes interesadas, como políticas, procedimientos, manuales o guías?   + Evalué si se mencionan los procesos y mecanismos específicos para estas actividades.   + Verifique si se han registrado las mejoras implementadas en las prácticas de compromiso y comunicación con las partes interesadas.   + ¿Se describen los procedimientos y métodos utilizados en dicho sistema? * ¿Los procesos de compromiso, comunicación y reporte con las partes interesadas están definidos de manera clara y estructurada? * Verifique si se establecen pasos específicos, roles y responsabilidades, y las actividades a realizar en cada etapa del proceso para asegurar que existe un marco establecido para llevar a cabo estas actividades de manera coherente. * ¿Se han proporcionado las herramientas y recursos necesarios para llevar a cabo el compromiso, la comunicación y el reporte con las partes interesadas, como sistemas de gestión de la información, herramientas de seguimiento o software de reporte, para facilitar el proceso y asegurar la documentación adecuada? * ¿Existe evidencia en la organización de un ciclo de mejora continua en los procesos establecidos para el cumplimiento de los requerimientos de cumplimiento, la comunicación y el reporte con las partes interesadas, incluyendo la identificación de áreas de mejora, la implementación de acciones correctivas, el seguimiento de los resultados y la retroalimentación de las partes interesadas?   + Verifique si se están cerrando los ciclos de mejora y se están aplicando lecciones aprendidas en el proceso. |

|  |
| --- |
| 3.3 Temática: Canales de Comunicación |
| El control se enfoca en analizar y evaluar la eficacia y efectividad de los medios utilizados para transmitir información relevante sobre ciberseguridad a todas las personas y entidades involucradas en la seguridad de la información. Esta evaluación tiene como objetivo asegurar que los canales de comunicación utilizados sean adecuados, accesibles y permitan una interacción efectiva y bidireccional con las partes interesadas.   * Verifique si se ha desarrollado una matriz de comunicación que identifique las necesidades, preferencias y expectativas de cada grupo de partes interesadas relevante en relación con la ciberseguridad.   + Revise si se han llevado a cabo encuestas, entrevistas u otros métodos para recopilar la perspectiva de las partes interesadas.   + ¿La matriz de comunicación se utiliza como base para la comunicación efectiva y adecuada con cada grupo de partes interesadas? * ¿Las herramientas y tecnologías de comunicación utilizadas en la empresa son apropiadas y efectivas?   + Revise si se incluyen plataformas de colaboración en línea, sistemas de gestión de relaciones con clientes (CRM), redes sociales corporativas, correo electrónico, videoconferencias, entre otros.   + ¿Cómo se utilizan estas herramientas y tecnologías de comunicación para facilitar la interacción con las partes interesadas relevantes en la organización? * ¿Los canales de comunicación permiten una interacción bidireccional entre la organización y las partes interesadas? * ¿Se asegura de que las partes interesadas puedan expresar sus opiniones y plantear inquietudes a través de los canales de comunicación utilizados? * Verifique si se han establecido canales de comunicación adecuados para permitir la retroalimentación y consulta con las partes interesadas en el ámbito de la ciberseguridad   + Revise si se realizan encuestas, entrevistas, reuniones, buzones de sugerencias, plataformas en línea u otros medios para recibir retroalimentación de las partes interesadas sobre ciberseguridad. * ¿Se están aplicando en la práctica mecanismos de retroalimentación y consulta con las partes interesadas?   + ¿Se llevan a cabo actividades periódicas de retroalimentación y consulta con las partes interesadas?   + ¿Se recopilan y registran de manera sistemática las necesidades, expectativas y preocupaciones de las partes interesadas durante las actividades de retroalimentación y consulta? |

|  |
| --- |
| 3.4 Temática: Informes y mecanismos de distribución |
| Se centra en asegurar que existan sistemas y procesos adecuados para generar y transmitir informes relevantes, precisos y oportunos sobre ciberseguridad a todas las partes interesadas involucradas. Este proceso es fundamental para mantener una comunicación efectiva y transparente con las partes interesadas y garantizar la toma de decisiones informadas en materia de seguridad de la información.   * ¿Se han establecido informes periódicos que aborden el estado de la seguridad de la información y la estrategia del SIC? * Verifique si existen mecanismos establecidos en la organización que aseguren que la información contenida en los informes y comunicaciones con las partes interesadas cumplan con los requisitos de los informes obligatorios de ciberseguridad.   + ¿Se han identificado criterios específicos para la elaboración de informes de ciberseguridad?   + ¿Los criterios identificados se siguen adecuadamente durante la elaboración de informes de ciberseguridad?   + ¿Los criterios establecidos se encuentran alineados con los requisitos regulatorios y de cumplimiento?  |  | | --- | | Recuerde que los requisitos regulatorios se encuentran identificados como parte de los controles específicos de este dominio |      * ¿Se revisa los informes de ciberseguridad generados por la empresa?   + Revise los criterios que se consideran para determinar si los informes cumplen con los requisitos de los informes obligatorios de ciberseguridad. * ¿Los roles específicos que se encargan de validar los informes en el proceso de elaboración son los idóneos, considerando su experiencia técnica en materias de SIC?   + Revise que los roles están asignados para la aprobación de los informes una vez que han sido validados. * ¿Se examinan en la auditoría los mecanismos establecidos para el escalado de problemas, preocupaciones o informes relevantes a las instancias correspondientes?   + Verifique si se define claramente cómo y cuándo se debe realizar el escalado, así como los responsables de dicha acción. * ¿Se observa y evalúa la distribución y entrega de los informes con las partes interesadas relevantes?   + Verifique si se han implementado de mecanismos adecuados para asegurar que los informes lleguen a los destinatarios correctos de manera oportuna.   + Evalúe si las partes interesadas tienen acceso fácil y transparente a los informes. * ¿Los mecanismos de distribución y entrega de informes se encuentran correctamente protegidos? ¿Su riesgo se ha evaluado?   + ¿Los canales y artefactos utilizados para la distribución de informes han pasado por el proceso de gestión de riesgo?   + ¿Se han aplicado opciones de tratamiento de riesgo, siguiendo la metodología de riesgo definida por la organización, para minimizar cuando corresponda los riesgos inherentes de los canales y artefactos de comunicación de la información?   + ¿Se informa del riesgo residual a las partes interesadas relevantes?   + ¿Se monitorea el cambio en el panorama de riesgos y amenazas de los canales y artefactos de comunicación? |