

**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. Identificar los tipos de proveedores (p. ej., servicios de TIC, logística, servicios públicos, servicios financieros, componentes de infraestructura de TIC) que pueden afectar la confidencialidad, integridad y disponibilidad de la información de la organización. 2. Evaluar y seleccionar productos o servicios de proveedores que tengan controles adecuados de seguridad de la información y revisarlos, en particular, la precisión y completitud de los controles implementados por el proveedor que aseguren la integridad de la información y el procesamiento de la información del proveedor y, por lo tanto, la seguridad de la información de la organización. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Establecer y comunicar una política específica del tema sobre las relaciones con proveedores a todas las partes interesadas relevantes. 2. Definir los servicios de TIC de la organización y la infraestructura física a los que los proveedores pueden acceder, monitorear, controlar o utilizar. 3. Establecer cómo evaluar y seleccionar proveedores según la sensibilidad de la información, productos y servicios (p. ej., con análisis de mercado, referencias de clientes, revisión de documentos, evaluaciones in situ, certificaciones). 4. Proporcionar conciencia y capacitación para el personal de la organización que interactúa con el personal del proveedor con respecto a las reglas apropiadas de participación, políticas específicas del tema, procesos y procedimientos y comportamiento basado en el tipo de proveedor y el nivel de acceso del proveedor a los sistemas e información de la organización. 5. Gestionar la transferencia necesaria de información, otros activos asociados y cualquier otra cosa que necesite ser cambiada y garantizar que se mantenga la seguridad de la información durante el período de transferencia. 6. Establecer requisitos para garantizar una terminación segura de la relación con el proveedor, incluyendo la eliminación de los derechos de acceso. 7. Establecer medidas para garantizar la continuidad del procesamiento de la información en caso de que el proveedor se vuelva incapaz de suministrar sus productos o servicios, como identificar un proveedor alternativo de antemano o siempre usar proveedores alternativos |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Evaluar y gestionar los riesgos de seguridad de la información asociados con el uso de la información y otros activos asociados de la organización por parte de los proveedores, incluidos los riesgos originados por posibles personas malintencionadas del proveedor. 2. Evaluar y gestionar los riesgos de seguridad de la información asociados con fallos o vulnerabilidades de los productos o servicios proporcionados por los proveedores. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Monitorear el cumplimiento de los requisitos de seguridad de la información establecidos para cada tipo de proveedor y tipo de acceso, incluida la revisión de terceros y la validación del producto y monitorizar si los proveedores mantienen y comparten el propósito de la organización. 2. Mitigar el incumplimiento de un proveedor, ya sea que se haya detectado mediante el monitoreo o por otros medios. |

# Preguntas de Auditoría para Definir el Rol en la Cadena de Suministro

|  |
| --- |
| 3.1 Temática: Políticas, procedimientos y controles. |
| Revisar las políticas, procedimientos y controles relacionados con la definición de roles en la cadena de suministro en el gobierno es una tarea fundamental para garantizar una gestión efectiva de la ciberseguridad en toda la cadena. Esta revisión permitirá evaluar la idoneidad y eficacia de las medidas implementadas y realizar ajustes necesarios para fortalecer la seguridad.   |  | | --- | | ℹ El establecimiento del rol en la cadena de suministro es un tema que puede ser abordado en la Política General de Seguridad de la Información. La política se detalla en el control “Política de Seguridad de la Información” |   Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe un registro o maestro que contenga los tipos de proveedores y clientes que hay en la organización?   + Verifique que el maestro de proveedores y clientes considera información relevante y útil para los procesos de SIC, como:     - Criticidad de los Proveedores     - Impacto en el Incumplimiento de los SLA (desde el proveedor) Características de la Información Compartida     - ¿La organización ha establecido una política específica sobre relaciones con proveedores y la ha comunicado a todas las partes interesadas relevantes? * Revise la documentación relevante, como políticas, procedimientos y contratos relacionados con la gestión de proveedores y los acuerdos de nivel de servicio (SLA), para identificar si se han definido los servicios de   + SIC de la organización y la infraestructura física a los que los proveedores.   + Verifique el cumplimiento de los acuerdos de nivel de servicio con los proveedores para confirmar que se están cumpliendo los términos y condiciones definidos. * ¿Qué controles de seguridad se establecen para garantizar que la seguridad de la información se mantenga durante la transferencia?   + Verifique si se han implementado los controles de seguridad antes, durante y después de la transferencia para garantizar que se hayan implementado de manera efectiva. * Revise la documentación relevante, como las políticas, procedimientos y contratos relacionados con la gestión de proveedores, para identificar si se han definido medidas para garantizar la continuidad del procesamiento de la información.   + ¿Se han evaluado y aprobado los proveedores alternativos para garantizar que cumplan con los requisitos de seguridad y cumplimiento? |

|  |
| --- |
| 3.2 Temática: Evaluación de los Proveedores |
| Al realizar evaluaciones a los proveedores, la organización puede identificar posibles riesgos asociados a sus procesos de adquisición, como interrupciones en la cadena de suministro, problemas de calidad o incumplimientos éticos, y tomar medidas preventivas para mitigarlos. Evaluar a los proveedores permite identificar oportunidades de mejora, y promover relaciones comerciales sólidas basadas en la transparencia y la colaboración. Contribuye a optimizar los costos, mejorar la satisfacción del cliente, fortalecer la reputación de la empresa en el mercado y fortalecer la seguridad a lo largo de toda la cadena de suministro.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se han evaluado a los proveedores y los productos o servicios seleccionados por la empresa?   + Revise si se han definido los criterios de selección de proveedores.   + Revise la documentación que respalde su selección, como evaluación de riesgos, informes de prueba de seguridad, acuerdos de nivel de servicio y contratos. * ¿Se han llevado a cabo evaluaciones de seguridad de los proveedores y se han realizado controles periódicos de seguridad para garantizar que estos controles sigan siendo efectivos y se mantengan actualizados? * ¿Se han entrevistado a los responsables de la definición de servicios de TIC de la organización y la infraestructura física para confirmar si se han definido los servicios que los proveedores pueden acceder, monitorear, controlar o utilizar?   + Verifique a través de las entrevistas si los servicios definidos están alineados con los objetivos de seguridad de la organización y los requisitos de cumplimiento. |
| 3.3 Temática: Nivel de Conocimiento de los miembros de la cadena de suministro |
| Asegura que todos los participantes comprendan y cumplan con los estándares éticos, sociales y ambientales requeridos. Esta concienciación promueve prácticas sostenibles, garantiza la integridad de los productos y servicios, y mitiga riesgos relacionados con la reputación y la responsabilidad corporativa. Una cadena de suministro consciente puede adaptarse mejor a los cambios regulatorios y las demandas del mercado, lo que conduce a relaciones comerciales más sólidas y a una contribución positiva tanto a nivel local como global.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Se ha proporcionado conciencia y capacitación al personal de la organización que interactúa con el personal proveedor?   + Evalué la efectividad de la capacitación del personal de la organización que interactúa con el personal del proveedor.   + Evalué si el personal de la organización y los proveedores conocen los mecanismos para reportar incidentes de seguridad de la información.   + Evalúe si los miembros de la cadena de suministro tienen conocimiento de las medidas higiénicas de SIC.     - ¿Siguen las recomendaciones mínimas de seguridad?     - ¿Tienen mecanismos de seguridad en las comunicaciones para evitar ataques de ingeniería social?     - ¿Se han instalado llaves de seguridad como DKIM para asegurar la autenticidad de los correos? * ¿Se han realizado actualizaciones periódicas de la capacitación para asegurar que el personal de la organización esté actualizado sobre las reglas de participación, políticas específicas del tema, procesos, procedimientos, y comportamiento adecuado en función del tipo de proveedor y el nivel de acceso del proveedor? |