

**05 - Control de Acceso**

**CASIG 1– Gobierno de la Ciberseguridad**

**Preguntas de Auditoría**

**Establecer la Política SIC**

|  |
| --- |
| **Competencias Básicas del Auditor**   1. Conocimientos en normativa de seguridad de la información y ciberseguridad. 2. Conocimientos en contextos de riesgos de SIC. 3. Conocimientos en modelos de gobernanza, 3 LoD, roles y responsabilidades en SIC. 4. Conocimientos en análisis y alineamiento estratégico. |

# Visión General

Una Política de Seguridad de la Información es un conjunto de reglas, directrices, procedimientos y prácticas diseñadas para salvaguardar la confidencialidad. integridad y disponibilidad de la información de una organización. Esta política actúa como un marco estratégico que define los objetivos, principios y responsabilidades en relación con la seguridad de la información dentro de la entidad.

La relevancia de la Política se ha vuelto cada vez más crítica debido a la creciente sofisticación de las amenazas cibernéticas y los ataques informáticos. Las organizaciones manejan una gran cantidad de información confidencial, desde datos de clientes hasta secretos comerciales, y deben protegerla de forma proactiva para evitar posibles consecuencias negativas, como:

* **Brechas de seguridad y filtraciones:** Sin una política adecuada, las organizaciones corren el riesgo de sufrir brechas de seguridad que pueden resultar en la exposición de datos sensibles y privados, erosionando la confianza de los clientes y dañando la reputación de la empresa.
* **Pérdida de propiedad intelectual:** Las políticas inadecuadas pueden llevar a la pérdida de información valiosa y propiedad intelectual, lo que podría dar lugar a competencia desleal o pérdidas financieras significativas.
* **Interrupción del negocio:** Un ataque cibernético exitoso puede causar
* interrupciones operativas y pérdidas financieras, afectando la continuidad del negocio.
* **Incumplimiento regulatorio:** Muchas industrias están sujetas a regulaciones estrictas sobre la protección de datos. La falta de una política adecuada podría dar lugar a sanciones legales y multas.

**Componentes Principales de una Política de Seguridad de la Información**

* **Declaración de la Política:** Esta sección debe contener una declaración clara y concisa sobre los objetivos y propósitos de la PSI, estableciendo el compromiso de la alta dirección hacia la seguridad de la información.
* **Alcance:** Especifica a qué activos y datos se aplica la política y qué partes de la organización están cubiertas.
* **Roles y Responsabilidades:** Define los roles y responsabilidades de las personas dentro de la organización en relación con la seguridad de la información. Esto puede incluir administradores de sistemas, usuarios finales, equipo de seguridad de la información y otros empleados clave.

La política de seguridad debe contener temas específicos como: el control de acceso, la gestión de contraseñas, criptografía, etc. Estas pueden también estar configuradas como políticas complementarias.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Identificar los objetivos empresariales clave de la organización: la visión, misión y metas estratégicas de la organización, así como los planes de negocio y las necesidades de los stakeholders.  2. Establecer los requisitos específicos para el marco de gobierno de SIC que aseguren su alineamiento con los objetivos empresariales. Estos requisitos deben reflejar las necesidades de la organización y abordar los riesgos y requisitos de seguridad de la información. ***[Ver Control: Política de SIC]*** |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Comunicar los principios de gobierno de SIC, la definición de seguridad de información y los principios de gestión de riesgos. Acordar con la administración ejecutiva la forma de establecer un liderazgo informado y comprometido de acuerdo a las responsabilidades asignadas de SIC. El plan de comunicación debe contener:  1.1 Aspecto y métricas a informar  1.2 Preparadores y receptores  1.3 Frecuencia  1.4 Procedimientos de escalamiento  2. Establecer o delegar el establecimiento de estructuras, procesos y prácticas de gobierno en línea con los principios de diseño de arquitectura actuales y previstos previamente acordado.  2.1 El marco de gobierno debe estár organizado por procesos e incluir información sobre las actividades de los procesos, los propietarios y las areas de mejora. ***[Ver Control: Estructura Organizacional]***  2.2 Establecer un comité estratégico de SIC (o equivalente). Este comité estratégico debería garantizar que el gobierno de SIC, como parte del gobierno de la empresa, se aborda de forma adecuada; aconsejar sobre la dirección estratégica a seguir; y determinar la priorización de los programas de inversión habilitados por SIC en línea con la estrategia y prioridades del negocio de la empresa. ***[Ver Control: Estructura Organizacional]***  3. Garantizar que las funciones y responsabilidades de la junta directiva estén documentadas y entendidas. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Asignar la responsabilidad, autoridad y rendición de cuentas por las decisiones de SIC en línea con los principios de diseño de gobierno, de los modelos de toma de decisiones y de delegación acordados.  2. Los responsables y las practicas se documentan en marcos de gobernanza. El CISO (o máximo responsable de la función de seguridad de la información) asiste a las reuniones de la junta ejecutiva y se analiza la contribución de la SIC a los objetivos empresariales.  3. Asegurar que los mecanismos de comunicación y presentación de informes proporcionan la información adecuada a los responsables de la supervisión y toma de decisiones, que incluyan reuniones periódicas con el fin de revisar las iniciativas de SIC actuales y futuras para reevaluar la alineación con los objetivos organizacionales y la oportunidad de presentar iniciativas que respalden la estrategia de SIC.  4. Direccionar al personal para que siga las directrices relevantes en cuanto al comportamiento ético y profesional y asegurar que se conozcan y se apliquen las consecuencias del incumplimiento.  5. Direccionar el establecimiento de un sistema de recompensas para fomentar el cambio cultural deseado en base a la compensación del personal, el establecimiento de objetivos y la evaluación del desempeño  5.1 Deben incluír medidas y planes de incentivo diseñadas y ejecutadas para prevenir o detectar comportamientos inaceptables o toma de riesgos excesivos y para respaldar acciones alineadas con los objetivos estratégicos de la organización ***[VER CONTROL: CONCIENCIACIÓN Y CAPACITACIÓN]***    6. Implementar procedimientos jerárquicos de información y escalamiento de decisiones. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Garantizar informes periódicos de iniciativas y problemas clave de seguridad de la información a la junta directiva. |
| 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. Promover la participación de los stakeholders en la identificación de nuevas prácticas, tecnologías o enfoques que puedan mejorar la alineación con los objetivos empresariales y la eficacia del marco de gobierno.  2. Mantenerse actualizado sobre las nuevas tecnologías y soluciones emergentes relacionadas con la gestión de la seguridad de la información y el marco de gobierno. Realizar investigaciones y evaluaciones para determinar si estas tecnologías pueden mejorar el alineamiento con los objetivos empresariales y considerar su implementación.  3. Buscar evaluaciones externas, como auditorías o revisiones independientes, para obtener una perspectiva objetiva sobre la eficacia y alineación del marco de gobierno de SIC con los objetivos empresariales. Utilizar los resultados de estas evaluaciones para identificar oportunidades de mejora y fortalecer el proceso de gestión del marco de gobierno. |

# Preguntas de Auditoría para Establecer la Política de SIC

|  |
| --- |
| 3.1 Temática: Bases para la Política de SIC |
| Para establecer la política, el primer paso es determinar si la organización se encuentra preparada para su adopción. Lo principal es que ella comprenda la necesidad y relevancia del instrumento, que aborde los temas esenciales de seguridad en cumplimiento con los estándares y mejores prácticas, y se encuentre alineada con las declaraciones estratégicas. Este levantamiento puede incluir análisis específicos tales como:   * ¿La organización reconoce la necesidad de la existencia de una Política de SIC? ¿Existe evidencia en forma de: entrevistas con las partes interesadas clave, registros y documentos de incidentes anteriores y/o planes estratégicos e informes de riesgos que establezcan la necesidad de la política? * ¿La Política de SIC y las Políticas Complementarias que de ella dependan abordan aspectos específicos de seguridad de la información y ciberseguridad (por ejemplo, protección de datos, acceso a la información, seguridad física) de forma coherente y sin duplicidades? * ¿La organización posee un documento oficial que establezca la política de SIC y que contenga los elementos requeridos por la norma? * Chequee que la política contiene como mínimo, de forma clara y bien definida: objetivos de la función de ciberseguridad, definición y principios de la seguridad de la información, compromiso de satisfacción y mejora continua del SGSI, principales responsables de la función de SIC e identificación del procedimiento para el tratamiento de desviaciones. * ¿Se organizan regularmente sesiones de capacitación sobre seguridad de la información para los empleados, en donde se aborden temas específicos relacionados con la seguridad de la información? ¿Se realizan entrevistas, ya sean individuales o grupales, para evaluar la comprensión de las políticas de seguridad de la información? * ¿Se ha comunicado apropiadamente la política de SIC a los empleados?   ¿Demuestran un conocimiento adecuado de las políticas y están implementando las medidas de seguridad de acuerdo con lo establecido en la política de seguridad de la información? |

|  |
| --- |
| **3.2 Temática: Formalización documental de la Política de SIC** |
| Al formalizar la política de SIC en un documento tangible y accesible, la organización establece directrices claras y un conjunto coherente de principios que guían a los empleados y partes interesadas en su comportamiento y acciones relacionadas con la seguridad de la información Este levantamiento puede incluir análisis específicos tales como:  .   * ¿Existe una repositorio consolidado y unificado de la Políticas de SIC y las Políticas Complementarias que permita su revisión y análisis? * ¿La política de SIC ha sido aprobada por la alta dirección y por el personal pertinente según su nivel de autoridad y competencia técnica? ¿Se han realizado entrevistas con los miembros de la alta dirección para confirmar que han aprobado la política de SIC y entienden su importancia? * ¿Existe documentación que demuestre que se llevó a cabo una evaluación de la estrategia, entorno técnico, reglamentos, estatus, legislación y contratos relevantes de la organización, riesgos, entorno actual y proyectado, y lecciones aprendidas de eventos e incidentes de seguridad de la información, que haya influido en la definición de la política de SIC? * La organización ha identificado los dominios o alcances en los que se requieren políticas específicas dentro de la función de SIC (ejemplo: acceso a la red, gestión de incidentes, protección de datos personales, seguridad física, control de acceso, criptografía, ¿entre otros)? |

|  |
| --- |
| **3.3 Temática: Capacidad de medir el cumplimiento de la Política y la aplicación de la mejora continua** |
| La mejora continua de la política de SIC de la Información es de vital importancia para mantener una protección efectiva en un entorno en constante cambio. Para evaluar si la organización ha establecido instrumentos fiables para la obtención de entradas de mejora, y si ha incorporado verdaderamente la información levantada, el auditor debe abordar los siguientes puntos:  **3.3.1 – El levantamiento de información relevante sobre desempeño, mejoras y lecciones aprendidas**   * ¿La organización ha identificado claramente los objetivos y beneficios de la política de SIC y políticas complementarias de seguridad de información? ¿Se han definido indicadores clave de rendimiento (KPI’s) que permitan medir los objetivos y beneficios establecidos? * ¿Existen sistemas o herramientas que se hayan implementado para el monitoreo efectivo de estas actividades? (como software de seguimiento, registro de actividad, auditorias, entre otros). * ¿Existen mecanismos de monitoreo para evaluar el cumplimiento de las políticas de seguridad de la información y ciberseguridad, precisión de los datos y uso eficiente de la TI? ¿Se lleva a cabo una revisión sistemática y periódica de los resultados del monitoreo? * ¿Se analiza regularmente el entorno de seguridad de la información para identificar cambios significativos que puedan afectar a la organización? * ¿Se han identificado desviaciones significativas en el desempeño de la política SIC y políticas complementarias en relación con los resultados esperados? * ¿Existe documentación respecto a las revisiones y auditorías previas realizadas para evaluar la efectividad de la gestión de la seguridad de la información y ciberseguridad establecidas? * ¿Se ha evaluado si la organización está utilizando técnicas de auditoría (como revisión de código fuente o pruebas de penetración) para evaluar la eficacia de sus políticas de seguridad de la información y ciberseguridad? * ¿Se han revisado informes de auditoría anteriores o realizado entrevistas a miembros de la alta dirección y empleados clave, para evaluar si la organización ha realizado mejoras y optimización continua en sus políticas de seguridad de la información y ciberseguridad?   **3.3.2 – La incorporación de mejoras y lecciones aprendidas**   * ¿Se ha verificado si se han documentado y seguido las acciones correctivas recomendadas en las revisiones y auditorías previas? * ¿Se documentan de manera clara y concisa (justificaciones, requisitos específicos y fechas de implementación) las actualizaciones realizadas a la política SIC y políticas complementarias? * ¿Se comunican los resultados del monitoreo a la alta dirección y otros empleados clave? * ¿Existe un programa de revisiones establecido que contemple la frecuencia y el alcance de las revisiones periódicas de seguridad de la información y ciberseguridad en la organización? ¿El personal encargado de realizar las revisiones cuenta con la formación y conocimientos necesarios para llevar a cabo evaluaciones efectivas? * ¿Se ha asegurado que la innovación y la adopción de nuevas tecnologías en las políticas de seguridad de la información estén alineadas con los objetivos estratégicos de la organización?   ¿Las políticas se ajustan para abordar las vulnerabilidades y riesgos identificados? |