

**05 - Control de Acceso**

**CASIG 1 – Gobierno de la Ciberseguridad**

**Preguntas de Auditoría**

**Asegurar el Cumplimiento de Requerimientos Legales y Regulatorios**

|  |
| --- |
| **Competencias Básicas del Auditor**   1. Conocimientos en normativa de seguridad de la información y ciberseguridad 2. Conocimientos en contexto normativo nacional e internacional de SIC 3. Conocimientos en mejores prácticas y normativa estándar sobre SIC 4. Conocimientos básicos sobre riesgos e impactos en el negocio 5. Conocimiento en la normativa legal general, sectorial y específica a la que la organización es afecta. |

# Visión General

Este proceso implica asegurarse de que las prácticas y políticas de seguridad de la información estén alineadas con las normativas y leyes vigentes, protegiendo tanto a la organización como a sus clientes de posibles sanciones y riesgos legales. Mantenerse al día con los cambios regulatorios permite a las empresas actuar de manera proactiva para mitigar amenazas legales y mejorar su postura de seguridad.

**1.1 Implementación de Controles para el Cumplimiento Regulatorio**

Para garantizar el cumplimiento, las organizaciones deben implementar controles específicos que aborden las normativas aplicables en sus operaciones. Esto incluye la gestión de acceso a la información sensible, el cifrado de datos y la implementación de medidas de privacidad que cumplan con estándares legales como el GDPR en Europa o la Ley de Protección de Datos Personales en Chile. Además, es fundamental contar con un equipo de cumplimiento regulatorio que revise regularmente la alineación de las políticas de seguridad con los requerimientos legales y que capacite a los empleados en prácticas seguras y conformes a la ley.

**1.2 Rol de la Auditoría en la Verificación del Cumplimiento**

Desde el lado de la auditoría, la verificación del cumplimiento legal y regulatorio se realiza mediante auditorías periódicas que evalúan la adherencia de la organización a las normativas establecidas. Los auditores revisan si los controles y políticas cumplen con las disposiciones legales, identificando posibles deficiencias y emitiendo recomendaciones para fortalecer el marco de cumplimiento. Esta función es esencial para evitar incumplimientos que puedan derivar en sanciones y para garantizar una adecuada gestión de riesgos legales y regulatorios, consolidando así un entorno seguro y alineado con las mejores prácticas de la industria.

# Modelo de Madurez

|  |  |
| --- | --- |
| NIVEL 1 [Impredecible y reactivo]: La actividad se completa, pero a menudo se retrasa y supera el presupuesto. | 1. Identificar y evaluar todos los posibles requisitos de cumplimiento relacionados con SIC y su impacto en las actividades de la organización en áreas como flujo de datos, privacidad, controles internos, informes financieros, regulaciones específicas de la industria, propiedad intelectual, normativa sectorial.   2. Identificar los requisitos legales, estatutarios, regulatorios y contractuales relevantes para la seguridad de la información.  3. Mantener un registro global, armonizado e integrado, de los requisitos de cumplimiento externo para la empresa.  3.1 Mantener actualizados los requisitos documentados. |
| NIVEL 2 [Gestionado a nivel de proceso]: Las actividades se planifican, ejecutan, miden y controlan. | 1. Formalizar políticas y procesos de seguridad de la información que tengan como finalidad determinar los requerimientos de cumplimiento.  1.1 Clasificar la información y otros activos asociados como parte del proceso de establecimiento de requisitos de seguridad de la información.  2. Asignar la responsabilidad de identificar y supervisar los cambios en los requisitos legales, regulatorios y otros requisitos contractuales externos, relevantes para el uso de recursos de TI y el procesamiento de la información dentro de las operaciones.  3. Diseñar, implementar o cambiar los controles de seguridad de la información tomando en cuenta los requisitos externos. |
| NIVEL 3 [Proactivo antes que reactivo]: Los estándares de toda la organización brindan orientación a través de proyectos, programas y carteras. | 1. Realizar evaluaciones de riesgos de seguridad de la información y determinar actividades de tratamiento de riesgos de seguridad de la información tomando en cuenta los requisitos externos.  1.1 Evaluar el impacto de los requisitos legales y regulatorios relacionados con SIC y tecnologías de la información sobre contratos con terceros relacionados con las operaciones de ciberseguridad, proveedores de servicio y otros socios comerciales de negocios  1.2 Definir las consecuencias del incumplimiento.  2. Determinar procesos y responsabilidades relacionados con la seguridad de la información tomando en cuenta los requisitos externos.  3. Determinar los requisitos contractuales de los proveedores relevantes para la organización y el alcance de suministro de productos y servicios.  4. Obtener asesoría independiente cuando corresponda, sobre los cambios en la legislación, regulaciones y estándares vigentes.  5. Revisar y ajustar continuamente las políticas, principios, estándares, procedimientos y metodologías para que sean eficaces en garantizar el cumplimiento necesario y abordar el riesgo empresarial.   5.1 Usar expertos internos y externos, cuando sea necesario.  6. Comunicar los requisitos nuevos y modificados a todo el personal relevante.  7. Evaluar periódicamente los procesos y actividades del negocio y de la función de SIC para asegurar el cumplimiento de las obligaciones relevantes (normativas, legislativas, de derecho consuetudinario, contractuales), las politicas internas, las normas y directrices profesionales. |
| NIVEL 4 [Gestionado Cuantitativamente]: La organización está basada en datos con objetivos cuantitativos de mejora del desempeño que son predecibles | 1. Revisar regularmente los requisitos legales, estatutarios, regulatorios y contractuales para mantenerse actualizados con los cambios y para identificar nueva legislación.  2. Revisar regularmente los patrones recurrentes de fallos de cumplimiento y evaluar las lecciones aprendidas.  3. Establecer metas y objetivos que permitan asegurar el éxito para el proceso de análisis y gestión del cumplimiento y medir el desempeño del proceso en relación con estos objetivos. |
| 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 las políticas, estándares, procedimientos, metodologías y sus procesos y actividades asociadas con base en la revisión y las lecciones aprendidas. |

# 3. Preguntas de Auditoría para Asegurar el Cumplimiento de Requerimientos Legales y Regulatorios

|  |
| --- |
| 3.1 Temática: Identificación y actualización de requisitos de cumplimiento |
| Para asegurar el cumplimiento de requerimientos legales y regulatorios, las prácticas de auditoría se enfocan en realizar revisiones sistemáticas y exhaustivas de los procesos, políticas y controles implementados por la organización. Estas auditorías buscan evaluar la conformidad con las leyes y normativas aplicables, identificar posibles brechas y áreas de mejora, y garantizar que se tomen medidas correctivas adecuadas.  Entre las prácticas de auditoría se incluye la revisión de documentos y registros para verificar que la organización cuenta con políticas y procedimientos claros y actualizados, que se ajusten a los marcos legales y regulatorios vigentes. Además, se evalúa si se han asignado roles y responsabilidades específicas para el cumplimiento normativo.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existe una lista de los posibles requisitos legales, estatutarios, regulatorios y contractuales relevantes en las actividades de SIC? * ¿Existe una lista de fuentes confiables y actualizadas de la cual recopilar información? * ¿Existe un encargado definido dentro de la organización que realice esta actividad? * ¿Se han realizado jornadas que informen a toda la organización sobre la relevancia de comprender los requisitos de cumplimiento en materias de SIC y las posibles consecuencias de fallar? * ¿Se mantiene un proceso formalizado para identificar los requisitos legales, estatutarios, regulatorios y contractuales relevantes para la seguridad de la información? * ¿Este proceso está documentado y existe registros formales, aprobados, comunicados y almacenados? * ¿Se mantiene un proceso formalizado para identificar los requisitos legales, estatutarios, regulatorios y contractuales relevantes para la seguridad de la información? ¿Está documentado este proceso? * ¿Los documentos contienen información detallada de cada requisito? * ¿Se mantienen documentos actualizados y aprobadas por la dirección?   ¿Existen actas o entrega de información a la organización a través de canales formales que demuestre que los documentos han sido aprobados por la dirección? |

|  |
| --- |
| **3.2 Temática: Análisis de riesgo e impacto del incumplimiento** |
| |  | | --- | | ℹ Estas prácticas de auditoría se desarrollan con más profundidad en los controles: Dirigir la Gestión de Riesgos, Evaluar la Gestión de Riesgos, Monitorear la Gestión de Riesgos del Dominio de Gobernanza de SIC y los controles del Proceso de Gestión de Riesgos. |   Por un lado, el análisis de riesgo permite identificar las áreas de la organización que podrían ser vulnerables o estar en mayor riesgo de incumplimiento de los requisitos legales y regulatorios y, por el otro lado, el análisis de impacto determina las consecuencias que podría tener el incumplimiento de los requerimientos legales y regulatorios en la organización. Al comprender los riesgos y el impacto, la organización puede priorizar las acciones y medidas de seguridad necesarias para mitigar los riesgos identificados y evitar posibles sanciones y pérdidas.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existen evaluaciones de impacto y de las consecuencias del incumplimiento de las regulaciones legales relacionados con SIC? * ¿Se incluye los riesgos e impactos externos como contratos con terceros relacionados con las operaciones de ciberseguridad, proveedores de servicio y otros socios comerciales de negocios? * ¿Existe documentación que demuestre que los riesgos, impactos y daños organizacionales del no cumplimiento de los requisitos de SIC han sido comunicados a la dirección y son conocidos? * Verifique la existencia de documentación formal, en lo posible con evidencia de que ha sido recibida por un miembro de la dirección o comité relevante. * ¿Existen evidencias de que se han implementado medidas de que se han tratado los riesgos identificados? |

|  |
| --- |
| 3.3 Temática: Revisión periódica de los requerimientos en los procesos de la organización |
| El panorama legal y regulatorio está en constante evolución. La revisión periódica garantiza que la organización esté preparada para hacer frente a nuevos desafíos y cambios en los requisitos, permitiendo una adaptación rápida y efectiva.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existen procesos que estén documentados y que detallen los requerimientos legales y regulatorios de SIC que los afecten? * Revise si existe una interfaz documentada entre procesos y requisitos regulatorios al interior del proceso, del macro proceso o detalladas en las actividades. * Evalué la pertinencia de los requerimientos de cumplimiento asociados y si están o no actualizados. * ¿Existe un responsable que se encargue de revisar los procesos del negocio constantemente? * ¿Existe un perfil de cargo con responsabilidades, tareas y funciones claramente definidos? * ¿Se mide el éxito de este responsable según su capacidad de mantener los requerimientos de cumplimiento SIC correctamente actualizados? * ¿Existen registros o evidencias de que se realizan revisiones periódicas a los procesos para asegurar el cumplimiento de las obligaciones legales y regulatorias? * ¿Existe un registro de no conformidades, opciones de mejora y opiniones de los auditores formal, documentado y recibido por una autoridad organizacional? |

|  |
| --- |
| 3.4 Temática: Mejora continua de los procesos de identificación y cumplimiento |
| La mejora continua busca optimizar los métodos y enfoques utilizados para identificar los requisitos legales relevantes y asegurarse de que la organización cumpla con ellos de manera efectiva y oportuna.  Este levantamiento puede incluir análisis específicos tales como:   * ¿Existen objetivos y metas establecidas para el análisis y gestión del cumplimiento de las políticas SIC aplicadas? * ¿Los objetivos y metas establecidas son claros, medibles, alcanzables? * ¿Los objetivos y metas recopilan las nuevas necesidades que nacen de requisitos de cumplimiento actualizados o agregados? * ¿Los objetivos y metas se han definido considerando la matriz de riesgos de la organización? * ¿Los objetivos buscan mejorar aquellos procesos y dar cumplimiento pleno a aquellos requisitos de SIC que representan un mayor riesgo potencial de no cumplimiento? * ¿Existe un proceso de recolección, tratamiento y análisis de datos que entregue información respecto a la evaluación del cumplimiento de los requisitos legales y regulatorios? * ¿Se recopilan datos periódicamente y estos se mantienen actualizados y seguros para su posterior tratamiento? * ¿Los datos recopilados se mantienen seguros y restringidos para que no puedan ser modificados sin autorización? * ¿Se han realizado pruebas técnicas sobre las bases de datos o instrumentos de ofimática para asegurar su integridad, disponibilidad y confidencialidad? * ¿Existe una segregación de funciones adecuada para determinar quién puede acceder a los datos de mejora? * ¿Existe un proceso formalizado de mejora continua, innovación y de gestión del cambio implementada en la organización? ¿Se utilizan los análisis de datos, lecciones aprendidas o un análisis de brechas y oportunidades dentro de este proceso? * ¿Existen registros que respalden que se hayan realizado cambios dentro de los procesos de identificación, evaluación e implementación de los requisitos legales y regulatorios? |