CAIGG

CONSEJO DE AUDITORÍA INTERNA GENERAL DE GOBIERNO

Ministerio Secretaría General de la Presidencia

"Guía GASIC N° 11" - Abril 2025

Guía de Auditoría, Seguridad de la Información y Ciberseguridad N°11

# ADAPTACIÓN AL SECTOR PÚBLICO DEL "REQUISITO TEMÁTICO CIBERSEGURIDAD" DEL IIA

# ÍNDICE

Nota

# PRESENTACIÓN

En cumplimiento con las instrucciones del Presidente de la República, Gabriel Boric Font, sobre fortalecimiento de la Política de Auditoría Interna de Gobierno; el Consejo de Auditoría Interna General de Gobierno, entidad asesora en materias de auditoría interna, control interno, probidad, gestión de riesgos y gobernanza del Supremo Gobierno, presenta a la Red de Auditoría Gubernamental, la GASIC N°11: Adaptación al Sector Público del "Requisito Temático Ciberseguridad" del IIA.

Esta guía forma parte de una iniciativa del Consejo de Auditoría Interna General de Gobierno (CAIGG), orientada a fortalecer las competencias en Seguridad de la Información y Ciberseguridad. Su propósito es proporcionar a los Auditores Internos del Sector Público herramientas e instrumentos que les permitan desarrollar servicios de aseguramiento y asesoramiento alineados con las mejores prácticas y la normativa vigente.

Santiago, abril 2025.

Daniela Caldana Fulss
Auditora General de Gobierno

## Capítulo 1

# OBJETIVO Y ALCANCE DE LA GUÍA

**Objetivo:**

El objetivo de esta Guía es adaptar los contenidos del "Requisito Temáticos Ciberseguridad: Guía de Usuario" del Instituto de Auditores Internos Global (IIA) para que sean aplicables al contexto del Sector Público. Esto se realiza a través contextualizar los contenidos de los requisitos específicos de la Guía de Usuario en el marco normativo vigente y determinar su aporte para alcanzar los requisitos de cumplimiento locales.

Con estas adaptaciones, se pretende promover el uso de mejores prácticas que apoyen alcanzar niveles cada vez mayores de calidad de las auditorías de ciberseguridad que permitan asegurar el cumplimiento normativo y el fortalecimiento de las organizaciones frente al cambiante entorno de amenazas, lo cual contribuye a una gestión más segura y eficiente de los servicios críticos de las entidades del Estado.

**Nota Importante**

En términos estrictos, **Seguridad de la Información y Ciberseguridad** son dos conceptos distintos, aunque relacionados.

La **"Seguridad de la Información"** es la preservación de la Confidencialidad, Integridad y Disponibilidad de la Información en los activos de información, en cualquier medio (incluso, las personas); por otro lado **"Ciberseguridad"** hace referencia exclusiva al ciberespacio y activos digitales.

En esta guía adoptamos el concepto de "Seguridad de la Información y Ciberseguridad", pero para evitar la redundancia y el exceso de texto, utilizaremos los conceptos de "Seguridad de la Información", "Ciberseguridad" o el acrónimo "SIC" como sinónimos para mejorar la comprensión lectora.

**Alcance de la Guía**

Requisito Temático de Ciberseguridad (IIA) - 2024

Los Requisitos Temáticos son un componente esencial y obligatorio del Marco Internacional de Prácticas Profesionales (MIPP) del Instituto de Auditores Internos Global (IIA), que también incluye las Normas Globales de Auditoría Interna y las Guías Globales. El IIA, como organismo normativo de la profesión de auditoría interna, exige estos Requisitos Temáticos obligatorios como complemento de las Normas Globales de Auditoría Interna, que sirven como autoridad para las prácticas requeridas descritas y referenciadas en los Requisitos Temáticos.

Los requisitos temáticos proporcionan una estructura para los temas globales auditados frecuentemente que suelen ser de mayor riesgo y de naturaleza generalizada. Aunque las Normas se aplican a todos los servicios de auditoría interna prestados, un requisito temático debe considerarse como un requisito obligatorio adicional que debe cumplirse cuando ese tema es el objeto de un encargo de auditoría interna. Los requisitos temáticos deben aplicarse, a nivel de entidad u organización, a los temas que tienen un impacto en toda la organización. Los auditores internos deben estar familiarizados con los requisitos temáticos y estar preparados para aplicarlos cuando el tema se incluya en sus planes anuales de auditoría, o si ese tema específico es el objeto de un encargo de auditoría interna. Los elementos de los requisitos temáticos deben ser evaluados al determinar el alcance del encargo. Deben documentarse y conservarse pruebas de que se ha realizado la evaluación y el tratamiento del tema.

***Fuente: Instituto de Auditores Internos Global. https://www.theiia.org***

Cuando un tema de un Requisito Temático se identifica durante el proceso de planificación de auditoría interna basada en riesgos y se incluye en el plan de auditoría, entonces los requisitos descritos en el Requisito Temático deben ser utilizados para evaluar el tema dentro de los compromisos aplicables.

***Fuente: Requisito Temático de Ciberseguridad - IIA.***

El Requisito Temático de ciberseguridad utiliza la definición de NIST para la ciberseguridad, que es "La protección de la información y los sistemas de información contra el acceso no autorizado, uso, divulgación, interrupción, modificación o destrucción con el fin de proporcionar confidencialidad, integridad y disponibilidad". Para soportar este objetivo, el Requisito Temático se divide en tres requisitos específicos que podremos revisar en la tabla a continuación:

| *Gobernanza* | *Gestión de Riesgos* | *Controles* |
|---|---|---|
| Objetivos y estrategias básicos de ciberseguridad claramente definidos que respalden los objetivos, políticas y procedimientos de la organización. | Procesos para identificar, analizar, gestionar y supervisar las ciberamenazas, incluido un proceso para escalar los ciberriesgos con prontitud. | Procesos de control establecidos por la dirección y evaluados periódicamente para mitigar el ciberriesgo. |

Estos temas se abren a su vez en una serie de ítems verificables que se basan en los marcos de mejores prácticas líderes en el sector: NIST CSF 2.0, NIST SP 800-53 y COBIT 2019.

El Requisito Temático se complementa con una serie de **Consideraciones** para cada uno de los temas. Las Consideraciones se pueden utilizar como ayuda para la evaluación de los requisitos temáticos, son ilustrativas, pero no obligatorias, además, su aplicabilidad depende del contexto.

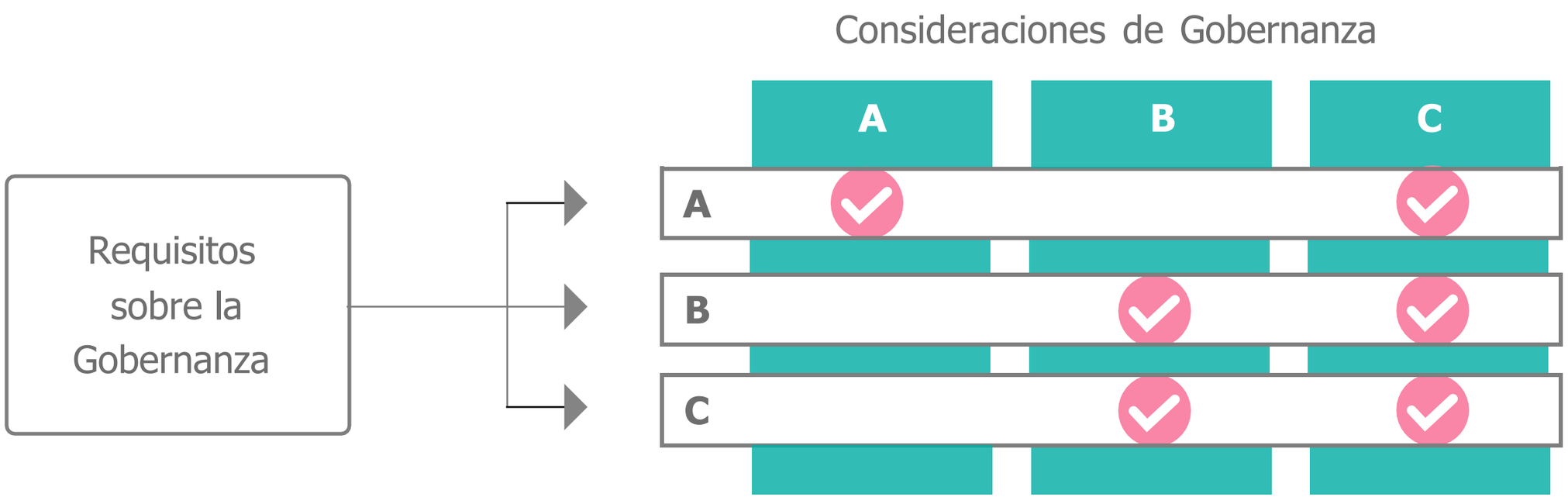


*Ilustración 1 Ejemplo Aplicabilidad Consideraciones en los requisitos*

Cuando se trate de la comparativa entre el marco normativo vigente y el Requisito Temático, esta GASIC "Adaptación al Sector Público del "Requisito Temático Ciberseguridad" del IIA." utilizara los requisitos específicos, y las consideraciones serán utilizadas sólo como información adicional para mantener su carácter de voluntario.

Capítulo 2

# ADAPTACIÓN AL MARCO NORMATIVO Y REGLAMENTARIO LOCAL

# 2. AJUSTE AL MARCO NORMATIVO Y REGLAMENTARIO LOCAL

La adaptación del *Requisito Temático de Ciberseguridad* del IIA implicó considerar leyes y regulaciones específicas de Chile, tales como la Ley N° 19.880 sobre Bases de los Procedimientos Administrativos, la Ley de Protección de Datos Personales y cualquier normativa vigente que regule directa o indirectamente la ciberseguridad dentro del sector público. El objetivo del ajuste es comprender de que forma la guía contribuye a desarrollar de mejor forma los requisitos expresados en estas normas.

Estas referencias ayudan a que los auditores internos trabajen dentro del marco legal aplicable y estén preparados para evaluar la conformidad de las entidades gubernamentales con las obligaciones regulatorias locales. Adicionalmente, es importante que el marco normativo incorporado refleje las necesidades específicas del sector público, tales como la rendición de cuentas hacia la Contraloría General de la República y la gestión de los datos de los ciudadanos de forma segura y transparente. Esta guía no aborda las necesidades particulares de cada componente del Sistema Público, el alcance se mantiene dentro del margen de la guía y las referencias normativas generales.

**Resultados:**

01

**Marco de referencias normativas y reglamentarias aplicables al sector público chileno:**

Documento que incluya una caracterización de las leyes y regulaciones pertinentes, en materias de ciberseguridad y protección de dato. Este informe permitirá comprender los requisitos de cumplimiento en materias de ciberseguridad y seguridad de la información. Desde un primer levantamiento inicial, se seleccionará un subconjunto de referencias normativas más relevantes para el desarrollo del marco de referencia y se obtendrán sus principales requisitos para desarrollar el segundo entregable de este punto.

02

**Matriz de correspondencia entre la guía del IIA y las referencias normativas aplicables:**

Matriz que relacione los requisitos de la guía del Instituto de Auditores Internos Global (IIA) con las normativas y leyes chilenas relevantes. Este documento facilitará la identificación de cómo cada requisito del IIA se alinea con las regulaciones locales, proporcionando un detalle de las áreas de intersección donde se alcanza el cumplimiento y la contribución de la guía en temáticas que no se encuentran abordadas en la normativa nacional vigente.

Capítulo 3

# SECCIÓN 1: GOBIERNO DE CIBERSEGURIDAD

# 3. SECCIÓN 1: GOBIERNO DE CIBERSEGURIDAD

El Requisito Temático de Ciberseguridad indica que el gobierno de ciberseguridad es el responsable de que las políticas y procedimientos de ciberseguridad se encuentren correctamente definidos y actualizados. Además, sugiere la alineación con algunos marcos reconocidos como NIST y COBIT, lo que debiera garantizar un entorno seguro.

## APORTE DE LA GUÍA A LOS REQUISITOS DEL MARCO LEGAL VIGENTE:

### Establecimiento y Actualización de Políticas y Procedimientos:

El documento enfatiza la necesidad de que las organizaciones desarrollen y mantengan políticas y procedimientos de gestión de riesgos de ciberseguridad, basándose en marcos ampliamente adoptados como NIST o COBIT.

"Se establecen y actualizan periódicamente las políticas y procedimientos relacionados con los procesos de gestión de riesgos de ciberseguridad, incluida la promoción de prácticas que refuercen el entorno de control basadas en marcos ampliamente adoptados (NIST, COBIT y otros)."

### Definición Clara de Funciones y Responsabilidades:

Se destaca la importancia de asignar roles y responsabilidades específicas en materia de ciberseguridad, asegurando que las personas encargadas posean las competencias necesarias.

"Las funciones y responsabilidades que soportan los objetivos de ciberseguridad de la organización están claramente establecidas y esas funciones son desempeñadas por personas con los conocimientos, habilidades y capacidades necesarias."

### Comunicación Periódica al Consejo:

Se establece la obligación de informar regularmente al consejo sobre las actualizaciones en objetivos, estrategias, riesgos y controles de ciberseguridad.

"Las actualizaciones de los objetivos, estrategias, riesgos y controles de mitigación en materia de ciberseguridad se comunican periódicamente al consejo."

### Compromiso de las Partes Interesadas:

Se resalta la necesidad de involucrar a diversas partes interesadas, tanto internas como externas, en la discusión y mejora de los procesos de gestión de riesgos de ciberseguridad.

"Las partes interesadas relevantes (por ejemplo, el liderazgo, las operaciones, los proveedores estratégicos y otros) se comprometen a debatir la mejor manera de establecer y mejorar los procesos de gestión de riesgos de ciberseguridad."

### Asignación de Recursos Necesarios:

Se subraya la importancia de identificar y comunicar al consejo los recursos necesarios para una gestión efectiva de la ciberseguridad, incluyendo liderazgo, presupuesto, talento, hardware, software y formación.

"Se comunican al consejo los recursos necesarios (como liderazgo, presupuesto, talento, hardware, software y formación) para ejecutar eficazmente los procesos de gestión de riesgos de ciberseguridad."

En el Requisito Temático del IIA se destacan incluyen puntos de énfasis, como:

- **Estructura de Gobernanza**
- **Planificación Estratégica y Coordinación**
- **Monitoreo y Evaluación de Desempeño**
- **Alineación con Estándares Internacionales**
- **Gestión de Riesgos**
- **Integración de Tecnologías Emergentes**
- **Cultura Organizacional y Conciencia**

## APORTE DE ESTA GUÍA A CADA REQUISITO DE CUMPLIMIENTO EN EL ALCANCE:

**LEY 19.628**

En su aporte a la Ley 19.628 que regula la protección de datos personales y el derecho a la privacidad, la guía menciona un enfoque de Gobierno el cual incluye la asignación de responsabilidades, capacitación de los funcionarios y la comunicación constante de estrategias y políticas de ciberseguridad al consejo directivo. Todo esto contribuye y refuerza el cumplimiento y la supervisión de la ley, ya que incluye la estructura de ciberseguridad para el manejo de datos sensibles y el derecho a la vida privada.

**LEY 21.633**

La Ley 21.663 define principios de seguridad y privacidad, junto con responsabilidades concretas, como la asignación de un delegado de ciberseguridad, tal como se especifica en el artículo 8.
La Guía Requisito Temático ahonda en las operaciones al requerir la realización de auditorías periódicas para mantener actualizadas políticas y procedimientos, comunicar de manera regular las estrategias de ciberseguridad al consejo, y la formación de personal capacitado. Estas medidas aseguran la supervisión y alineación de las pautas de gobernanza establecidas por la Ley, incorporando procedimientos como la evaluación de riesgos y la renovación de estrategias fundamentadas en normas reconocidas, como NIST, COBIT u otros.

**LEY 21.459**

La Ley 21.459 define normas sobre delitos informáticos y abarca el tratamiento correcto de los datos y dispositivos. La Guía fortalece los requisitos de la ley al proporcionar directrices sobre cómo monitorear el cumplimiento y fomentar las responsabilidades dentro de las organizaciones. Además, promueve la difusión de estrategias de ciberseguridad, garantizando que los objetivos establecidos por la Ley se apliquen de forma eficaz.

**LEY 19.799**

La Ley 19.799 regula la utilización de la firma electrónica y la validez de documentos digitales, pero no trata sobre cómo las distintas entidades deben administrar la seguridad digital. La Guía proporciona directrices sobre cómo las organizaciones deben definir políticas y procedimientos relacionados con la gestión de riesgos de ciberseguridad, además de funciones y obligaciones para resguardar documentos y firmas digitales. Por ejemplo, requerir la supervisión de los sistemas que gestionan información electrónica para asegurar su fiabilidad y prevenir alteraciones no permitidas.

Matriz de Correspondencia: Gobierno, Evaluación y Valoración del Gobierno de la Ciberseguridad.

| | Descripción de Requisitos | Ley 19.628 | Ley 21.663 | Ley 21.459 | Ley 19.799 | Recomendaciones |
|---|---|---|---|---|---|---|
| A | Se establecen y actualizan periódicamente políticas y procedimientos en relación con los procesos de gestión de riesgos de ciberseguridad, incluida la promoción de prácticas que refuercen el entorno de control basadas en marcos ampliamente adoptados. (NIST, COBIT y otros). | | | El cumplimiento de estas obligaciones exige la implementación de protocolos y estándares establecidos por la Agencia, y estándares particulares de ciberseguridad en conformidad a la regulación sectorial respectiva.<br><br>El objetivo de estos protocolos es la prevención y gestión de riesgos de ciberseguridad, así como la contención y mitigación del impacto que los incidentes pueden tener sobre la continuidad operacional del servicio o la confidencialidad e integridad de la información, de las redes o de los sistemas informáticos (Art. 7). | | Adopción de marcos como NIST y COBIT.<br>Así como otra documentación relevante para la gestión de ciberseguridad:<br><br>1. Documentación clara, concisa, coherente y actualizada, idealmente a medida que se identifican nuevos riesgos de ciberseguridad y al menos una vez al año.<br><br>2. Procedimientos relacionados con la identificación, análisis, resolución y notificación de brechas u otras pérdidas de datos sensibles.<br><br>3. Documentación sobre cómo la dirección o gerencia operativa garantiza que las políticas y procedimientos son suficientes para respaldar las operaciones de ciberseguridad. |
| B | Las funciones y responsabilidades que soportan los objetivos de ciberseguridad de la organización están claramente establecidas y son desempeñadas por personas con los conocimientos, habilidades y capacidades necesarias. | El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los posibles daños (Art. 11). | Designar un delegado de ciberseguridad, quien actuará como contraparte de la Agencia le informará a la autoridad, jefatura o jefe superior del órgano o servicio de Administración del Estado o a los directores, gerentes, administradores o ejecutivos principales, según lo definan las instituciones privadas (Art.8 i). | | Emplear personal calificado para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados (Art. 17.c). | Deben ser personas debidamente capacitadas.<br><br>E incluir una estructura de informes que garantice que la ciberseguridad se informa a un nivel de la organización que tenga suficiente visibilidad para lograr el apoyo de la organización (Apéndice A "Consideraciones para cada requisito de gobierno" letra B). |

| | | | | | | |
|---|---|---|---|---|---|---|
| C | Se han establecido políticas y procedimientos de gestión de riesgos de ciberseguridad que se actualizan periódicamente, incluida la promoción de prácticas que refuerzan los procesos de gestión de riesgos de ciberseguridad basados en marcos de gestión de riesgos ampliamente adoptados, guías autorizadas u otras mejores prácticas. | | Las instituciones obligadas por la presente ley deberán aplicar de manera permanente las medidas para prevenir, reportar y resolver incidentes de ciberseguridad.<br><br>Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso. | | | Establecer políticas y procedimientos de gestión de riesgos de ciberseguridad que se mantengan actualizadas. El proceso que la organización utiliza para actualizar periódicamente las políticas relacionadas con la gestión de riesgos de ciberseguridad puede incluir:<br><br>1. Revisión y aprobación anual de las políticas y procedimientos. |

Matriz de Correspondencia: Gobierno, Evaluación y Valoración del Gobierno de la Ciberseguridad.

| | Descripción de Requisitos | Ley 19.628 | Ley 21.663 | Ley 21.459 | Ley 19.799 | Recomendaciones |
|---|---|---|---|---|---|---|
| C | | | El cumplimiento de estas obligaciones exige la debida implementación de los protocolos y estándares establecidos por la Agencia, así como de los estándares particulares de ciberseguridad dictados de conformidad a la regulación sectorial respectiva (Art.8 i). | | | 2. Comprensión de cómo la organización garantiza el cumplimiento de sus políticas de gestión de riesgos y la manera en que se forma al personal en la ejecución de las políticas y procedimientos.<br><br>A. Comprensión de qué marcos o directrices autorizadas utiliza la dirección o gerencia operativa para gestionar los riesgos de ciberseguridad (NIST, COBIT y otros) y la forma en que la organización confirma la adhesión a los marcos elegidos.<br>consejo y las pone en práctica, comunicando al consejo el estado de los cambios. |
| D | La rendición de cuentas y la responsabilidad, con respecto a la gestión de los riesgos de ciberseguridad, están establecidas y se ha identificado a una persona o equipo que supervisa y comunica periódicamente cómo se están gestionando los riesgos de ciberseguridad, incluidas las necesidades de recursos para mitigar los riesgos y la identificación de riesgos de ciberseguridad emergentes que no se habían identificado previamente. | | | | | |
| E | Se establece un proceso para elevar rápidamente cualquier riesgo de ciberseguridad (emergente o previamente identificado) que alcance niveles inaceptables sobre la base de las directrices de gestión de riesgos establecidas por la organización o para cumplir con los requisitos legales y/o reglamentarios aplicables. | | Adoptar de forma oportuna y expedita las medidas necesarias para reducir el impacto y la propagación de un incidente de ciberseguridad, incluida la restricción de uso o el acceso a sistemas informáticos, si fuera necesario (Art. 8.e). | | | Definir niveles de riesgo, tales como alto, moderado, bajo, incluyendo una explicación detallada para cada nivel de riesgo y procedimientos para elevar cada categoría de riesgo. |

Matriz de Correspondencia: Gobierno, Evaluación y Valoración del Gobierno de la Ciberseguridad.

| | Descripción de Requisitos | Ley 19.628 | Ley 21.663 | Ley 21.459 | Ley 19.799 | Recomendaciones |
|---|---|---|---|---|---|---|
| F | La gestión de riesgos de ciberseguridad incluye la coordinación entre la seguridad de la información, el departamento jurídico, el de cumplimiento y otros directivos para identificar y cumplir todas las obligaciones legales y contractuales, como leyes y reglamentos. Tanto el estado del cumplimiento como del incumplimiento de los requisitos aplicables se comunica periódicamente dentro de la organización. | | | | | |
| G | Se establece un proceso para identificar y gestionar los riesgos de ciberseguridad relacionados con terceros. Los vendedores, proveedores y otros proveedores de procesos y/o servicios externalizados están obligados contractualmente a implantar controles de ciberseguridad eficaces que protejan adecuadamente la confidencialidad, integridad y disponibilidad de los sistemas y datos de la organización a los que tienen accesos terceros. | | Implementar un sistema de gestión de seguridad de la información continuo con el fin de determinar aquellos riesgos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y la continuidad operacional del servicio. Este sistema deberá permitir evaluar tanto la probabilidad como el potencial impacto de un incidente de ciberseguridad (Art. 8.a).<br><br>Realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos y sistemas para detectar acciones o programas informáticos que comprometan la ciberseguridad y comunicar la información relativa a dichas acciones o programas al CSIRT Nacional, en la forma que determine el reglamento (Art. 8.d ). | Acceso ilícito.<br>El que, sin autorización o excediendo la autorización que posea y superando barreras de seguridad, acceda a un sistema informático será castigado con la pena de presidio menor en su grado mínimo o multa de once a veinte unidades tributarias mensuales.<br>Si el acceso fuere realizado con el ánimo de apoderarse o usar la información contenida en el sistema informático, se aplicará la pena de presidio menor en sus grados mínimos a medio. Igual pena se aplica a quien divulgue la información a la cual se accedió de manera ilícita, si no fuese obtenida por éste (Art. 2).<br><br>Interceptación ilícita.<br>El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos, será castigado con la pena de presidio menor en su grado medio.<br>El que, sin contar con la debida autorización, capte, por medios técnicos, datos contenidos en sistemas informáticos a través de las emisiones electromagnéticas provenientes de éstos, será castigado con la pena de presidio menor en sus grados medio a máximo (Art.3). | | Verificar que los controles de ciberseguridad del proveedor se revisan antes de iniciar una relación comercial y que los contratos incluyen el derecho a revisiones periódicas a lo largo de la relación. Incluir la obtención y el análisis del informe de controles de la organización de servicios del tercero y la verificación de que la organización ha documentado su revisión del informe SOC, que debe incluir la garantía de que se han aplicado las consideraciones de control del usuario.<br>Comprender el enfoque de la dirección o gerencia operativa para determinar si los terceros tienen un entorno de control adecuado que se corresponda con los controles de la organización. |

Matriz de Correspondencia: Gobierno, Evaluación y Valoración del Gobierno de la Ciberseguridad.

| | Descripción de Requisitos | Ley 19.628 | Ley 21.663 | Ley 21.459 | Ley 19.799 | Recomendaciones |
|---|---|---|---|---|---|---|
| H | Las políticas y procesos relacionados con la clasificación, conservación, destrucción y encriptación de datos se diseñan adecuadamente y se despliegan con eficacia para proporcionar un enfoque sistemático que garantice un registro completo y preciso de los datos y proteja la confidencialidad y privacidad de la información sensible. de ciberseguridad eficaces que protejan adecuadamente la confidencialidad, integridad y disponibilidad de los sistemas y datos de la organización a los que tienen accesos terceros. | Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo (Art.7).<br><br>La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal.(Art. 23) Los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado (Art.6). | | Ataque a la integridad de los datos informáticos. El que indebidamente altere, dañe o suprima datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño grave al titular de estos mismos (Art.4).<br><br>Receptación de datos informáticos. El que conociendo su origen o no pudiendo menos que comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas descritas en los artículos 2°, 3° y 5°, sufrirá la pena asignada a los respectivos delitos, rebajada en un grado (Art.6). | | Establecer políticas y procesos relacionados con la clasificación, conservación, destrucción y encriptación de datos. Se recomienda que las políticas y procedimientos respecto a el tratamiento de datos considere:<br><br>4. Cifrado<br>5. Gestión de acceso/identidad.<br><br>6. Quién prepara, revisa y actualiza la documentación, que idealmente debería incluir personal jurídico y de cumplimiento para garantizar la conformidad con la normativa aplicable.<br><br>7. Cómo realiza la organización la clasificación de información para garantizar que los datos confidenciales y privados se han identificado y tienen el nivel de protección adecuado, como la limitación del acceso de los usuarios.<br><br>8. Cómo revisa periódicamente la organización el proceso utilizado para clasificar los datos y si el proceso sigue respaldando los objetivos de ciberseguridad de la organización y cumpliendo las políticas de la organización y la normativa aplicable. |
| I | Se establece un proceso de comunicación de los riesgos operativos de ciberseguridad para garantizar el conocimiento por parte de la dirección y los empleados. Todos los problemas, diferencias, deficiencias o fallos de control se comunican al consejo de administración y a la dirección o gerencia operativa, y el estado de las medidas correctoras se supervisa estrechamente y se notifica. Los incumplimientos de las políticas de ciberseguridad se identifican, investigan, notifican y corrigen a su debido tiempo. | | Deber de reportar. Todas las instituciones públicas y privadas del artículo 4° tendrán la obligación de reportar al CSIRT Nacional ciberataques e incidentes que puedan tener efectos significativos en términos del artículo 27, tan pronto les sea posible y conforme siguiente esquema. (Art.9) Informar a los potenciales afectados y si lo requiere a la Agencia, sobre los incidentes que pudieran comprometer gravemente su información, redes o sistemas informáticos, especialmente cuando involucren datos personales y no exista otra disposición legal; o sea necesario para prevenir la ocurrencia de nuevos incidentes (Art. 8.g). | Ataque a la integridad de los datos informáticos. El que indebidamente altere, dañe o suprima datos informáticos, será castigado con presidio menor en su grado medio, siempre que con ello se cause un daño grave al titular de estos mismos (Art.4).<br><br>Receptación de datos informáticos. El que conociendo su origen o no pudiendo menos que comercialice, transfiera o almacene con fin ilícito datos informáticos, como las conductas descritas en los artículos 2°, 3° y 5°, sufrirá la pena asignada a los respectivos delitos, rebajada en un grado (Art.6). | | El proceso de comunicación de los riesgos operativos de ciberseguridad a la dirección o gerencia operativa ya los empleados. Lo ideal sería que esta comunicación se incluyera en la formación periódica sobre ciberseguridad. (al menos una vez al año). Comprender el proceso de la dirección o gerencia operativa para comunicar las actualizaciones sobre la remediación existente de los problemas de ciberseguridad junto con las fechas de finalización previstas. Verificar que el incumplimiento se supervisa de cerca y se proporcionan actualizaciones al consejo y a la alta dirección. |

Capítulo 4

# SECCIÓN 2: CONTROLES DE CIBERSEGURIDAD

# 4. CONTROLES DE CIBERSEGURIDAD

En cuanto a los controles de ciberseguridad, la guía establece la importancia de que cada organización cuente con la asignación de recursos necesarios para potenciar la efectividad de los controles, asegurando que estos promuevan el cumplimiento de los objetivos de ciberseguridad y la resolución de problemas. Se deben considerar controles para verificar la información del personal, existencia de políticas robustas y la integración de ciberseguridad tanto en el ciclo de vida de sistemas como en el hardware, adicionalmente se menciona la importancia de integrar la seguridad de las redes, los servicios de comunicación, administración de dispositivos y seguridad física e infraestructura crítica dentro de los controles de ciberseguridad. Adicionalmente la implementación de estos controles debe garantizar que la dirección este informada sobre posibles riesgos y oportunidades de mejora.

**Revisión Sistemática de Controles:**

**01**

El requisito enfatiza la importancia de revisar periódicamente la efectividad de los controles de ciberseguridad.

"Los controles de ciberseguridad implementados deben ser revisados de manera sistemática para asegurar su eficacia frente a las amenazas y riesgos emergentes"

**Valoración Basada en Métricas:**

**02**

Insiste en utilizar métricas claras y cuantificables para valorar la efectividad de los controles.

"Es esencial establecer métricas de desempeño/rendimiento clave (KPIs) para medir la efectividad de los controles y optimizar su aplicación en función de los resultados obtenidos"

**Auditorías Regulares de los Controles:**

**03**

Incluye la realización de auditorías internas y externas para garantizar que los controles cumplan con los estándares.

"Se deben realizar auditorías periódicas de los controles implementados, asegurando la alineación con estándares internacionales y la mejora continua"

**Alineación con Marcos Normativos:**

**04**

Subraya la necesidad de que los controles estén alineados con normativas y estándares internacionales reconocidos.

"Los procesos de control de la ciberseguridad deben estar alineados con estándares como ISO/IEC 27002, garantizando la cobertura de áreas clave y cumplimiento normativo"

**Documentación de Evaluaciones:**

**05**

Se exige documentar todas las evaluaciones de control para permitir el seguimiento y la trazabilidad.

"Las evaluaciones de control deben documentarse meticulosamente para proporcionar trazabilidad, facilitar auditorías y respaldar la toma de decisiones"

**Adopción de Enfoques Basados en Riesgos:**

**06**

Destaca la importancia de priorizar controles en función del impacto y la probabilidad de los riesgos identificados.

"Los controles de ciberseguridad deben priorizarse con base en el análisis de riesgos, maximizando la mitigación de impactos significativos"

En la guía de la IIA se destacan puntos de énfasis, tales como:

- **Auditorías Periódicas de los Controles de Ciberseguridad**
- **Mecanismos de Medición y Evaluación**
- **Revisión de Controles Frente a Nuevas Amenazas**
- **Integración con Sistemas de Gestión de Riesgos**
- **Evaluación de Controles Internos y Externos**
- **Capacitación y Sensibilización Sobre Controles**

Matriz de Correspondencia: Controles, Evaluación y Valoración de los Procesos de Control de la Ciberseguridad.

| | *Descripción de Requisitos* | *Ley 19.628* | *Ley 21.663* | *Ley 21.459* | *Ley 19.799* | *Recomendaciones* |
|---|---|---|---|---|---|---|
| *A* | Prioriza los controles de ciberseguridad y garantiza que el presupuesto y los recursos relacionados (como personal, software, herramientas y otros) se asignan para maximizar los beneficios esperados. | | | | | |
| *B* | Garantiza que los controles de ciberseguridad funcionen de forma que promuevan la consecución de los objetivos de ciberseguridad de la organización y la resolución oportuna de los problemas. | | | | | |
| *C* | Proporciona formación suficiente al personal responsable de las operaciones de ciberseguridad. | | Contar con programas de capacitación, formación y educación continua de sus trabajadores y colaboradores, que incluyan campañas de ciberhigiene (Art. 8.h). | | | Se recomienda incluir:<br><br>El proceso de la dirección o gerencia operativa para evaluar las necesidades de formación del personal de ciberseguridad dentro de la organización y cómo se asignan los recursos para impartir la formación adecuada y garantizar que se comprenden y gestionan las nuevas amenazas a la ciberseguridad.<br>Comprender cómo se asegura la dirección o gerencia operativa de que los empleados tienen suficiente formación en ciberseguridad, que puede incluir eventos de formación en directo, instrucción grabada o realización de módulos de formación. |
| *D* | Ha desarrollado políticas y procedimientos suficientes para gestionar todos los aspectos de las operaciones de ciberseguridad y los controles relacionados. | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| *E* | Garantiza que la dirección o gerencia operativa disponga de los recursos necesarios para mantenerse informada sobre los problemas de ciberseguridad emergentes de las nuevas tecnologías, identificar oportunidades para mejorar las operaciones y comprender cómo pueden desplegarse mejor los esfuerzos de ciberseguridad para incidir en metas y objetivos organizativos más amplios. | | | | La acreditación es el procedimiento en virtud del cual el prestador de servicios de certificación demuestra a la Entidad Acreditadora que cuenta con las instalaciones, sistemas, programas y recursos humanos necesarios para otorgar los certificados en los términos establecidos en la ley y en el reglamento, permitiendo su inscripción en el registro señalado en el artículo 18 (Art. 17). | El proceso de la organización para formar al equipo directivo responsable de operaciones y controles de ciberseguridad para reconocer las tendencias emergentes y proporcionar a sus equipos un liderazgo estratégico.<br>Comprender cómo identifica la organización las oportunidades de aumentar las capacidades de la dirección para apoyar la concienciación sobre los problemas emergentes, como la participación en la formación y la educación profesional continua. |

Matriz de Correspondencia: Controles, Evaluación y Valoración de los Procesos de Control de la Ciberseguridad.

| | Descripción de Requisitos | Ley 19.628 | Ley 21.663 | Ley 21.459 | Ley 19.799 | Recomendaciones |
|---|---|---|---|---|---|---|
| F | Integra adecuadamente la ciberseguridad en el ciclo de vida de desarrollo de sistemas para aplicaciones empresariales, incluidos los programas informáticos y las aplicaciones adquiridas o desarrolladas a medida. | | Implementar un sistema de gestión de seguridad de la información continuo con el fin de determinar aquellos riesgos que puedan afectar la seguridad de las redes, sistemas informáticos y datos, y la continuidad operacional del servicio. Este sistema deberá permitir evaluar tanto la probabilidad como el potencial impacto de un incidente de ciberseguridad (Art. 8.a ). | | | |
| G | Ha incluido la ciberseguridad en la gestión del hardware (como portátiles, ordenadores de sobremesa, dispositivos móviles). | | | | | |
| H | Ha implantado controles eficaces en relación con el soporte de hardware de producción, como la configuración, la aplicación de parches, el soporte de la gestión de acceso de usuarios y la supervisión de la disponibilidad y el rendimiento. La organización ha evaluado tanto la adecuación del diseño como la eficacia operativa de estos controles. | | | | | |
| I | Optimiza los controles relacionados con la red en lo que respecta a su segmentación, el uso y la colocación de cortafuegos, las conexiones limitadas a redes y/o sistemas externos y el uso de tecnologías preventivas y detectivas, como los sistemas de detección/prevención de intrusiones. | | Realizar continuamente operaciones de revisión, ejercicios, simulacros y análisis de las redes, sistemas informáticos y sistemas para detectar acciones o programas informáticos que comprometan la ciberseguridad y comunicar la información relativa a dichas acciones o programas al CSIRT Nacional, en la forma que determine el reglamento (Art. 8.d). | | | Revisar cómo utiliza la organización los cortafuegos, incluyendo dónde están ubicados y el proceso utilizado para revisar, analizar y restringir el acceso a la red, evitando el acceso no autorizado. Revisar cómo utiliza la organización los sistemas de detección/prevención de intrusiones para prevenir, detectar y recuperarse de ataques de ciberseguridad. |

Matriz de Correspondencia: Controles, Evaluación y Valoración de los Procesos de Control de la Ciberseguridad.

| | Descripción de Requisitos | Ley 19.628 | Ley 21.663 | Ley 21.459 | Ley 19.799 | Recomendaciones |
|---|---|---|---|---|---|---|
| J | Ha implantado controles eficaces en torno a los servicios comunes de comunicación de escritorio, como el correo electrónico, los navegadores de Internet, las videoconferencias, la mensajería y los protocolos de intercambio de archivos. | | | | | |
| K | Ha implantado controles adecuados de prestación de servicios para garantizar que las siguientes áreas están integradas con la supervisión de la ciberseguridad: gestión de cambios, servicio/ayuda y administración de dispositivos de usuario final. | | | | | |
| L | Ha implantado controles de seguridad física adecuados para proteger de ataques los centros de información de alto riesgo (como centros de datos, centros de operaciones de red y centros de operaciones de seguridad). | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| M | Ha implantado controles de respuesta a incidentes y de recuperación. | | Informar a los potenciales afectados y a la Agencia sobre la ocurrencia de incidentes que pueden comprometer su información o redes y sistemas informáticos, especialmente cuando involucren datos personales y no exista otra disposición legal; o sea necesario para prevenir la ocurrencia de nuevos incidentes o para gestionar uno (Art. 8.g).<br><br>Deber de reportar. Todas las instituciones públicas y privadas señaladas en el artículo 4° tendrán la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos en los términos del artículo 27, tan pronto sea posible (Art.9).<br><br>Elaborar e implementar planes de continuidad operacional y ciberseguridad, los que deben certificarse en conformidad al artículo 28, y revisarse de forma periódica con una frecuencia mínima de dos años. (Art. 8.c) | | | Se recomienda incluir:<br><br>1. Un plan documentado que se revisa y actualiza a medida que las operaciones de la organización cambian con el tiempo.<br><br>2. Pruebas periódicas y comunicación de los resultados a la dirección o gerencia operativa.<br><br>3. Determinar si los problemas detectados en las pruebas se solucionan a tiempo. |

## APORTE DE LA GUÍA A CADA REQUISITO DE CUMPLIMIENTO EN EL ALCANCE:

En cuanto a los controles de ciberseguridad, la guía establece la importancia de que cada organización cuente con la asignación de recursos necesarios para potenciar la efectividad de los controles, asegurando que estos promuevan el cumplimiento de los objetivos de ciberseguridad y la resolución de problemas. Se deben considerar controles para verificar la información del personal, existencia de políticas robustas y la integración de ciberseguridad tanto en le ciclo de vida de sistemas como en el hardware, adicionalmente se menciona la importancia de integrar la seguridad de las redes, los servicios de comunicación, administración de dispositivos y seguridad física e infraestructura crítica dentro de los controles de ciberseguridad. Adicionalmente la implementación de estos controles debe garantizar que la dirección este informada sobre posibles riesgos y oportunidades de mejora.

## APORTE DE LA GUÍA A CADA REQUISITO DE CUMPLIMIENTO EN EL ALCANCE:

**LEY 19.628**

La ley 19.628 define principios generales acerca de la protección de datos, sin embargo, la Guía Requisito Temático de Ciberseguridad aporta controles específicos y operativos que se deben implementar para mitigar riesgos. Se hace énfasis en implementar controles de seguridad en áreas específicas como el ciclo de vida del desarrollo de software, gestión de hardware y protección de la red, lo cual es fundamental para asegurar que los datos sensibles no sean vulnerables a accesos no autorizados o perdidas de integridad. Estos controles contribuyen a la ley como capas adicionales de defensa, respondiendo a amenazas cibernéticas con soluciones técnicas precisas y alineadas con estándares de ciberseguridad.

**LEY 21.633**

Esta ley exige la implementación de medidas pertinentes para mitigar incidentes de ciberseguridad, además de la certificación de sus planes de continuidad. La guía complementa estos requisitos al detallar controles de seguridad básicos como el cifrado, la segmentación de la red y la integración de la ciberseguridad en el desarrollo de software. Todo esto permite a las organizaciones poder alinearse de mejor manera a los estándares legales e internacionales, mejorando así su capacidad para enfrentar posibles ciberataques.

**LEY 21.459**

La guía Requisito Temático de ciberseguridad complementa la ley 21.459, ya que, proporciona un marco práctico y detallado para la implementación y evaluación de los procesos de ciberseguridad. Mientras que la ley establece las bases legales para castigar el delito informático, la guía presenta un enfoque estructurado para asegurar que las organizaciones estén en mejores condiciones para cumplir con la ley y que adopten las mejores prácticas para proteger sus activos de información y administrar los riesgos de ciberseguridad.

**LEY 19.799**

La ley posiciona a la firma electrónica como un método seguro de autenticación, sin embargo, en ella no se detallan controles técnicos para su protección. La Guía Requisitos temáticos de ciberseguridad complementa esto sugiriendo la implementación de controles de ciberseguridad que garanticen el presupuesto necesario para alcanzar los objetivos de ciberseguridad de la organización, junto con esto se indica la importancia del desarrollo de políticas y procedimientos para gestionar las operaciones y controles. Además del deber de incluir la ciberseguridad tanto en la gestión de hardware, como en la red, el perímetro físico y las operaciones, como, por ejemplo, técnicas de cifrado robusto, la implementación de MFA y la protección de claves criptográficas utilizadas en las firmas digitales. Estas medidas mejoran la seguridad de los documentos electrónicos, garantizando que no sean alterados ni utilizados indebidamente y otorgando un mayor sustento a la ley.