ID 191398

Folio RAEX202601540
23-06-2026

APRUEBA MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) DE LA SUBSECRETARÍA DE ECONOMÍA Y EMPRESAS DE MENOR TAMAÑO; ESTABLECE PROCEDIMIENTO DE ACTUALIZACIÓN Y DEJA SIN EFECTO RESOLUCIONES EXENTAS QUE INDICA.

VISTOS:

Lo dispuesto en el decreto con fuerza de ley N° 1-19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; en la ley N° 21.663, Marco de Ciberseguridad; en la ley N° 21.459 que Establece normas sobre delitos informáticos; en el decreto con fuerza de ley N° 88, de 1953, del Ministerio de Hacienda, que Adopta las medidas que indica en relación con el Ministerio de Economía y Comercio y sus atribuciones y actividades; en el decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, que Aprueba norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos; en la resolución exenta folio RAEX202300204, de 2023, de este origen, que Aprueba nueva política general de seguridad de la información y ciberseguridad de la Subsecretaría de Economía y Empresas de Menor Tamaño; y en la resolución N° 36, de 2024, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón.

CONSIDERANDO:

1. Que la Subsecretaría de Economía y Empresas de Menor Tamaño tiene como misión fundamental el diseño, coordinación y ejecución de políticas de fomento productivo, innovación y emprendimiento, gestionando para ello un alto volumen de información crítica y datos personales de ciudadanos y empresas.

2. Que la seguridad de la información y la ciberseguridad constituyen activos estratégicos imprescindibles para asegurar la continuidad operacional, la fe pública y la protección de los derechos de las personas en el entorno digital.

ID 191398

3. Que la entrada en vigor de la Ley N° 21.663, Marco de Ciberseguridad, impone a los Órganos de la Administración del Estado la obligación de adoptar estándares avanzados de gestión de riesgos, reporte de incidentes y gobernanza de la seguridad.

4. Que esta Subsecretaría ha sido calificada como Operador de Importancia Vital en virtud de lo dispuesto en la Ley Marco de Ciberseguridad N° 21.663, condición que le impone deberes reforzados de ciberresiliencia, incluyendo la obligación legal de implementar y mantener sistemas de gestión de seguridad de la información, realizar auditorías y simulacros periódicos, contar con planes de continuidad operacional probados y reportar incidentes significativos a la Agencia Nacional de Ciberseguridad dentro de los plazos perentorios establecidos por la normativa.

5. Que, dada la naturaleza dinámica de las ciberamenazas y la evolución tecnológica, se hace imperativo transitar desde una política estática hacia un Sistema de Gestión de Seguridad de la Información (SGSI) basado en controles específicos, modulares y auditables, alineados con el estándar internacional ISO/IEC 27002:2022.

6. Que, el Comité de Tecnologías, Seguridad de la Información y Ciberseguridad (CSI) de esta Subsecretaría, en sus sesiones de trabajo, ha revisado técnicamente y validado el nuevo conjunto de políticas, normas y procedimientos propuestos para el fortalecimiento institucional.

7. Que, es necesario formalizar los mecanismos de gobernanza que aseguren que cualquier modificación futura a la normativa interna cuente con los niveles adecuados de revisión técnica y aprobación directiva.

RESUELVO:

ARTÍCULO PRIMERO.- APRUÉBESE el "Manual del Sistema de Gestión de Seguridad de la Información (Versión 2026)" de la Subsecretaría de Economía y Empresas de Menor Tamaño, cuyo objetivo es establecer el marco normativo para proteger la confidencialidad, integridad y disponibilidad de los activos de información institucionales.

ARTÍCULO SEGUNDO.- ESTABLÉCESE que dicho Manual se encuentra conformado por la Política General de Seguridad de la Información y el conjunto de Políticas Específicas, Normas y Procedimientos detallados en el Índice Maestro del SGSI, el cual se encuentra inserto en el numeral 10.2 de la presente resolución que por este acto se aprueba.

ARTÍCULO TERCERO.- ESTABLÉCESE que, con el objeto de mantener la vigencia y efectividad del Sistema de Gestión, cualquier modificación, actualización, derogación o incorporación de nuevos documentos normativos al presente Manual, deberá cumplir con las siguientes condiciones de gobernanza: a) Ser sometida a revisión técnica y aprobación por parte del Comité de Tecnologías, Seguridad de la Información y Ciberseguridad (CSI). b) Contar con la visación técnica del Oficial de Seguridad de la Información (CISO). c) Ser ratificada y oficializada mediante la firma de la Jefatura de Servicio, a través del acto administrativo correspondiente.

ID 191398

ARTÍCULO CUARTO.- DÉJANSE SIN EFECTO, a contar de la fecha de la presente resolución, la Resolución Exenta Folio RAEX202300204, de fecha 15 de febrero de 2023, y su modificación contenida en la Resolución Exenta Folio RAEX202402618, de fecha 13 de agosto de 2024, así como cualquier otra instrucción interna previa que contravenga las disposiciones contenidas en el Manual que aquí se aprueba.

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

Subsecretaría de Economía y Empresas de Menor Tamaño

1. Declaración Institucional

La información es un activo estratégico fundamental para la Subsecretaría de Economía y Empresas de Menor Tamaño. Nuestra capacidad para fomentar la inversión, apoyar a las MiPymes y gestionar los registros públicos depende íntegramente de la disponibilidad, integridad y confidencialidad de nuestros datos y sistemas.

En el actual escenario digital, donde las ciberamenazas son cada vez más sofisticadas y frecuentes, la protección de la información deja de ser una opción técnica para convertirse en una obligación de Estado.

En virtud de lo anterior, y conscientes de nuestra calificación como **Operador de Importancia Vital** bajo la Ley N° 21.663 (Ley Marco de Ciberseguridad), la Alta Dirección declara su compromiso irrestricto con el fortalecimiento de nuestra ciberresiliencia.

Para materializar este compromiso, la Subsecretaría establece, implementa y mantiene un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con los estándares internacionales **NCh-ISO 27001** y los controles de la norma **ISO/IEC 27002:2022**.

2. Objetivo General

El objetivo principal de esta Política es proteger los activos de información de la Subsecretaría frente a amenazas internas y externas, deliberadas o accidentales, con el fin de:

2.1 **Garantizar la Continuidad Operacional:** Asegurar que los servicios críticos que prestamos a la ciudadanía y a las empresas se mantengan disponibles incluso ante incidentes adversos o crisis.

2.2 **Proteger la Confidencialidad:** Resguardar rigurosamente los datos personales de los ciudadanos, la información estratégica del fomento productivo y los antecedentes reservados, evitando fugas o accesos no autorizados.

2.3 **Asegurar la Integridad:** Garantizar que la información contenida en nuestros registros y sistemas sea precisa, completa y no haya sido alterada sin autorización.

2.4 **Cumplimiento Legal:** Asegurar el cumplimiento estricto de la legislación vigente, en particular la Ley Marco de Ciberseguridad (21.663), la Ley de Delitos Informáticos (21.459) y la Ley de Protección de la Vida Privada (19.628).

3. Pilares Estratégicos del SGSI

3.1 **Gestión de Riesgos:** La seguridad no es un estado, sino un proceso. Toda decisión estará basadas en una evaluación permanente de los riesgos que afectan a nuestros activos.

3.2 **Responsabilidad Compartida:** La seguridad de la información es responsabilidad de todos y todas. Cada funcionario/a, prestador de servicios y proveedor externo es un eslabón clave en la cadena de defensa y debe cumplir con las normas establecidas.

3.3 **Mejora Continua:** Se establece un compromiso a revisar y mejorar sistemáticamente el SGSI, aprendiendo de los incidentes y adaptándose a los cambios tecnológicos y normativos.

4. Alcance y ámbito de aplicación

El Sistema de Gestión de Seguridad de la Información (SGSI) de la Subsecretaría de Economía y Empresas de Menor Tamaño se establece con un alcance integral, transversal e indivisible, aplicable a todos los procesos de negocio, estratégicos y de apoyo de la institución.

Su ámbito de aplicación se define bajo las siguientes dimensiones:

4.1 **Alcance Subjetivo (Personas y Entidades):** Las presentes políticas y normas son de cumplimiento obligatorio e inexcusable para:

- **Funcionarios y Personal Interno:** La totalidad de las personas que desempeñan funciones en la Subsecretaría, cualquiera sea su calidad jurídica de contratación (Planta, Contrata, Código del Trabajo u Honorarios), estamento o jerarquía, incluyendo a las altas autoridades y jefaturas.
- **Colaboradores Transitorios:** Alumnos en práctica, pasantes, personal en comisión de servicio y reemplazos temporales.
- **Terceras Partes y Cadena de Suministro:** Todos los proveedores, contratistas, consultores y socios estratégicos que, en virtud de un vínculo contractual o convenio, tengan acceso físico o lógico a los activos de información, redes o instalaciones de la institución.

4.2 **Alcance Objetivo (Activos de Información):** La protección se extiende a la información en todas sus formas, soportes y estados:

- **Información Digital:** Bases de datos, sistemas de gestión, correos electrónicos, archivos ofimáticos, código fuente, registros de auditoría (logs) y certificados digitales.
- **Información Física:** Documentación en papel, expedientes administrativos, contratos, resoluciones, medios de almacenamiento extraíbles y archivos en custodia.
- **Infraestructura Tecnológica:** Todo el hardware (servidores, estaciones de trabajo, dispositivos móviles), redes de comunicaciones, equipos de seguridad perimetral y la infraestructura crítica de soporte del Centro de Datos (climatización y energía).

- **Activos Intangibles:** Propiedad intelectual, imagen institucional, conocimientos técnicos (know-how) y la reputación de la Subsecretaría.

4.3 **Alcance Territorial y Entornos de Trabajo:** Las normas de seguridad rigen independientemente de la ubicación geográfica del activo o del usuario:

- **Instalaciones Físicas:** Edificio del Nivel Central, todas las Secretarías Regionales Ministeriales (SEREMIAS) a lo largo del país, bodegas y archivos externos.
- **Entornos de Teletrabajo y Movilidad:** Espacios de trabajo remotos y dispositivos móviles en tránsito, desde los cuales se acceda a los servicios institucionales.
- **Infraestructura en la Nube:** Servicios de procesamiento o almacenamiento de datos propios o contratados a terceros (Cloud Computing) que gestionen información institucional.

4.4 **Alcance en el Ciclo de Vida:** Las medidas de seguridad deberán aplicarse de manera continua durante todas las etapas del ciclo de vida de la información: desde su generación, captura o recepción; durante su clasificación, procesamiento, almacenamiento y transmisión; hasta su disposición final, archivo histórico o destrucción segura.

5. Gestión de Activos de Información

Para garantizar una protección eficaz y eficiente, la Subsecretaría debe conocer qué activos posee, cuál es su valor y dónde se encuentran.

5.1 **Inventario de Activos:** La Subsecretaría mantendrá un Inventario Oficial de Activos de Información actualizado, que incluya todos los recursos necesarios para la operación institucional (datos, software, hardware, servicios y personas).

- Es obligación de cada Jefatura de División y Departamento declarar los activos bajo su responsabilidad y reportar cualquier alta, baja o modificación a la Unidad de Tecnologías de la Información y Comunicaciones (UTIC) y al Oficial de Seguridad de la Información (CISO).
- Se prestará especial atención a la identificación de los Activos de Información Críticos, definidos como aquellos indispensables para la provisión de los servicios esenciales de la institución en su calidad de Operador de Importancia Vital.

5.2 **Propiedad del Activo:** Todo activo de información debe tener asignado un **"Propietario del Activo"**.

- El Propietario es la autoridad o jefatura responsable de asegurar que la información sea clasificada adecuadamente y de autorizar los accesos a la misma.
- La responsabilidad sobre el activo acompaña al cargo, no a la persona, y persiste durante todo el ciclo de vida del activo.

5.3 **Clasificación de la Información:** Para aplicar los niveles de seguridad adecuados, la información institucional se clasificará en uno de los siguientes niveles, según el impacto que causaría su divulgación no autorizada:

- **Pública:** Información destinada a ser conocida por la ciudadanía.
- **Interna:** Información de uso exclusivo para las operaciones de la Subsecretaría, cuya divulgación pública no está autorizada pero cuyo impacto es bajo (ej. directorios telefónicos, manuales internos, actas rutinarias).

- **Reservada / Confidencial:** Información crítica protegida por ley o estrategia, cuya divulgación causaría un daño grave a la institución, a terceros o a la seguridad nacional (ej. Datos Personales Sensibles, Estrategias Legales, Claves de Acceso, Información Financiera no pública).

5.4 **Etiquetado y Manipulación:** Todos los activos de información deberán ser etiquetados (visual o digitalmente) de acuerdo con su clasificación, para alertar a los usuarios sobre los cuidados que deben tener en su manipulación, transmisión y almacenamiento. Está estrictamente prohibido procesar información clasificada como "Reservada" en sistemas o medios no autorizados (como correos personales o nubes públicas no corporativas).

5.5 **Devolución de Activos:** Al término de la relación contractual o cambio de funciones, todo funcionario o tercero debe devolver todos los activos institucionales (equipos y datos) que estén en su poder. La retención indebida de información institucional será constitutiva de falta grave y podrá ser perseguida legalmente.

6. Gestión del Riesgo

La Subsecretaría de Economía y Empresas de Menor Tamaño reconoce que la seguridad absoluta es inalcanzable. Por tanto, el modelo de protección se basa en una Gestión de Riesgos sistemática, estructurada y alineada con la norma ISO/IEC 27005 y la Ley Marco de Ciberseguridad.

6.1 **Enfoque Preventivo y Basado en Riesgo:** Las decisiones de inversión en seguridad, implementación de controles y asignación de recursos no serán arbitrarias, sino que responderán directamente a los resultados de las evaluaciones de riesgo. Se priorizará la protección de aquellos activos cuya vulneración implique un mayor impacto en la continuidad de los servicios esenciales, la privacidad de las personas y la fe pública.

6.2 **Metodología Oficial:** El CISO mantendrá una Metodología de Gestión de Riesgos formalmente aprobada, que permita:

- **Identificar** las amenazas y vulnerabilidades que afectan a los activos.
- **Analizar** la probabilidad de ocurrencia y el impacto potencial.
- **Evaluar** el nivel de riesgo resultante.
- **Tratar** el riesgo mediante la implementación de controles (del Anexo A de la norma ISO 27001).

6.3 **Apetito de Riesgo y Criterios de Aceptación:** La Subsecretaría define su riesgo bajo el principio de **"Tolerancia Mínima"** para sus Servicios Esenciales:

- **Riesgos Críticos y Altos:** Son **INACEPTABLES**. Deben ser tratados de inmediato mediante planes de acción correctiva urgentes para reducir su nivel a parámetros tolerables. La Jefatura del Servicio o la Alta dirección no autorizará la operación de sistemas nuevos que presenten este nivel de riesgo residual.
- **Riesgos Medios:** Deben ser gestionados y reducidos en un plazo razonable. Su aceptación temporal requiere la autorización formal del Propietario del Activo y del CISO.
- **Riesgos Bajos:** Pueden ser aceptados si el costo del control supera el beneficio de la protección, bajo monitoreo continuo.

6.4 **Opciones de Tratamiento:** Frente a un riesgo identificado, la Subsecretaría adoptará alguna de las siguientes acciones:

- **Reducir (Mitigar):** Implementar controles de seguridad (políticas, software, hardware) para bajar el riesgo.
- **Transferir (Compartir):** Derivar el riesgo a terceros (ej. contratación de seguros de ciberseguridad o proveedores especializados con cláusulas de responsabilidad).
- **Evitar (Eliminar):** Descontinuar la actividad, proceso o sistema que genera el riesgo.
- **Aceptar:** Asumir el riesgo de manera consciente y formal.

Está prohibido aceptar riesgos que comprometan la legalidad vigente o la continuidad de servicios catalogados como vitales por la ley.

6.5 **Evaluación Continua (Seguridad desde el Diseño):** La evaluación de riesgos no es un evento anual, es un requisito continuo:

- **Proyectos Nuevos:** Todo nuevo proyecto tecnológico o modificación significativa (Control de Cambios) debe someterse a una evaluación de riesgos de seguridad y privacidad antes de su paso a producción.
- **Cambios del Entorno:** Se re-evaluarán los riesgos ante cambios legislativos, nuevas amenazas detectadas por el CSIRT Nacional o cambios en la infraestructura.

7. Marco de Referencia normativo

El diseño, implementación y operación del Sistema de Gestión de Seguridad de la Información (SGSI) de la Subsecretaría se fundamenta en el estricto cumplimiento del siguiente marco jurídico y técnico:

7.1 **Marco Legal:**

- **Ley N° 21.663 (Ley Marco de Ciberseguridad):** Establece la institucionalidad, los principios y las obligaciones para los Operadores de Importancia Vital y Servicios Esenciales.
- **Ley N° 21.459 (Sobre Delitos Informáticos):** Tipifica y sanciona figuras como el acceso ilícito, la interceptación, el ataque a la integridad de los datos y el fraude informático.
- **Ley N° 19.628 (Sobre Protección de la Vida Privada):** Regula el tratamiento de datos personales y sensibles en poder de la administración pública.
- **Ley N° 19.799 (Sobre Documentos Electrónicos y Firma Electrónica):** Otorga validez legal a los documentos y firmas digitales.
- **Ley N° 20.285 (Sobre Acceso a la Información Pública):** Regula la transparencia activa y pasiva, y sus excepciones (causales de secreto o reserva).

7.2 **Marco Reglamentario y Administrativo:**

- **Decreto Supremo N° 83 (2005) del MINSEGPRES:** Aprueba la norma técnica sobre seguridad y confidencialidad de los documentos electrónicos para órganos de la Administración del Estado.
- **Instructivos Presidenciales de Ciberseguridad:** Lineamientos impartidos por el Gobierno para la ciberseguridad en el Estado.
- **Resoluciones y Oficios de la Contraloría General de la República:** Jurisprudencia administrativa relativa al control, uso de recursos TIC y probidad administrativa.

7.3 **Estándares Técnicos Internacionales:**

- **NCh-ISO/IEC 27001:** Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de Seguridad de la Información - Requisitos.
- **ISO/IEC 27002:2022:** Seguridad de la Información, Ciberseguridad y Protección de la Privacidad - Controles de Seguridad de la Información.
- **ISO/IEC 27005:** Gestión del Riesgo de Seguridad de la Información.

7.4 **Actualización Dinámica:** Se entenderá que todas las referencias a las normas citadas incluyen sus futuras modificaciones, reglamentos complementarios y cualquier nueva legislación que las reemplace o complemente, asegurando así que el SGSI se mantenga siempre alineado con la legalidad vigente.

8. Roles y Responsabilidades

La seguridad de la información no es responsabilidad exclusiva de un área técnica, sino una función transversal que involucra a toda la estructura organizacional de la Subsecretaría. Se definen los siguientes roles y responsabilidades clave:

8.1 **Jefe/a del Servicio:** Es la máxima autoridad y responsable final del SGSI ante la ley. Sus responsabilidades son:

- Liderar el compromiso institucional con la seguridad de la información.
- Asignar los recursos financieros, técnicos y humanos necesarios para la operación y mejora del SGSI.
- Designar formalmente al Oficial de Seguridad de la Información (CISO).
- Ser o asignar la representación legal ante la Agencia Nacional de Ciberseguridad en calidad de Operador de Importancia Vital.

8.2 **Comité de Tecnologías, Seguridad de la Información y Ciberseguridad (CSI):** Sus funciones son:

- Aprobar las políticas, normas y procedimientos del SGSI (incluyendo este Manual).
- Validar la evaluación de riesgos y aceptar los riesgos residuales que excedan el nivel operativo.
- Priorizar los proyectos de inversión en seguridad.
- Sesionar periódicamente para revisar el desempeño del SGSI y el estado de los incidentes relevantes.

8.3 **Oficial de Seguridad de la Información (CISO):** Rol estratégico e independiente de la operación de TI, encargado de la gestión del SGSI. Sus responsabilidades son:

- Asesorar a la Alta Dirección y al Comité en materias de ciberseguridad y riesgos.
- Mantener actualizado el marco normativo.
- Supervisar el cumplimiento de las políticas por parte de todas las áreas (incluyendo TI y Proveedores).
- Coordinar la respuesta ante incidentes de seguridad y actuar como enlace con el CSIRT Nacional.
- Gestionar el programa de concientización y capacitación.

8.4 **Jefatura de la Unidad de TIC (UTIC):** Responsable de la implementación técnica de los controles. Sus funciones son:

- Configurar y mantener segura la infraestructura tecnológica (servidores, redes, aplicaciones) siguiendo los lineamientos del CISO.
- Ejecutar los respaldos de información y las pruebas de recuperación.
- Gestionar la aplicación de parches de seguridad y la remediación de vulnerabilidades técnicas.
- Asegurar que los desarrollos de software (internos o externos) cumplan con los requisitos de seguridad desde el diseño.

8.5 **Propietarios de la Información:** Corresponde a los Jefes de División, Departamento o Unidad de Negocio. Son responsables de:

- Identificar y clasificar la información y los procesos críticos bajo su cargo.
- Definir quién debe tener acceso a su información (autorizar altas) y solicitar la revocación de accesos cuando ya no sean necesarios (bajas).
- Aceptar los riesgos operativos asociados a sus procesos de negocio, dentro de los límites tolerables definidos por la institución.

8.6 **Funcionarios y Usuarios:** Sus obligaciones son:

- Conocer y cumplir las políticas y normas de seguridad establecidas.
- Proteger sus credenciales de acceso (contraseñas) y no compartirlas en ninguna circunstancia.
- Reportar inmediatamente cualquier evento sospechoso o incidente de seguridad a la Mesa de Ayuda o al CISO.
- Utilizar los activos tecnológicos exclusivamente para fines laborales y de manera ética.

8.7 **Auditoría Interna:** Rol de aseguramiento independiente.

- Evaluar periódicamente, mediante auditorías programadas, que el SGSI cumple con la normativa ISO 27001, la legislación vigente y las propias políticas de la institución.
- Verificar que los controles declarados están efectivamente implementados y operando.

9. Principios de la Política

9.1 **Principio de constitucionalidad y legalidad**: La presente política, se deberá interpretar de manera tal que su aplicación concilie con las normas constitucionales y legales vigentes, referidas a los derechos y libertades de las personas.

9.2 **Principio de confidencialidad, integridad y disponibilidad de la información y ciberseguridad:** Se deberá garantizar y mantener la confidencialidad, integridad y disponibilidad de toda la información y datos, a los que se tenga acceso en los sistemas de información y servicios de redes.

9.3 **Principio del buen uso de los recursos institucionales:** El uso de los sistemas de comunicaciones electrónicas debe enmarcarse en el ámbito de competencia de la institución, teniendo como finalidad el ejercicio de las funciones propias e inherentes para las cuales el usuario ha sido nombrado o se ha convenido su prestación de servicios.

9.4 **Principio para obtención de pruebas en procesos de investigación:** Con motivo de una investigación se podrá autorizar la ejecución, en determinados sistemas de información o en servidores de la institución, tendiente a obtener información necesaria de tal forma que se garantice la menor afectación a la privacidad de los/as funcionarios/as.

9.5 **Principio de responsabilidad por uso malicioso:** La apertura de archivos adjuntos o la ejecución de programas que se reciban por medios electrónicos, constituyen acciones que pueden vulnerar la estabilidad, calidad, seguridad de las redes o de sistemas de información institucional.

9.6 **Principio de acciones especiales de seguridad de la información y ciberseguridad:** El personal autorizado de la Unidad de Tecnologías de Información y Comunicaciones (UTIC) podrá restringir, bloquear o cancelar el acceso de un usuario a los servicios tecnológicos o a otro servicio o sistema informático, siempre que dicha acción de seguridad sea indispensable y aprobada por el Comité de Tecnologías, Seguridad de la Información y Ciberseguridad, bajo hechos fundados o bajo la existencia de requerimientos legales o judiciales.

10. Políticas Específicas y Estructura Documental

Para garantizar una implementación efectiva de los controles de seguridad, el SGSI se estructura en niveles jerárquicos de documentación, los cuales son de conocimiento y cumplimiento obligatorio según corresponda al rol del funcionario.

10.1 **Arquitectura del Manual del SGSI:** El marco normativo se descompone en:

- **Nivel Estratégico (Política General):** El presente documento, que define la postura institucional, el apetito de riesgo y las responsabilidades de alto nivel.
- **Nivel Táctico (Políticas Específicas y Normas):** Documentos que regulan dominios concretos de seguridad (ej. Control de Acceso, Teletrabajo, Criptografía). Estos documentos detallan el "qué" se debe cumplir.
- **Nivel Operativo (Procedimientos e Instructivos):** Guías técnicas paso a paso que describen "cómo" ejecutar una tarea de seguridad (ej. Procedimiento de Alta de Usuarios, Instructivo de Configuración de Firewall).
- **Nivel de Evidencia (Registros):** Logs, formularios, actas y tickets que demuestran el cumplimiento de lo anterior.

10.2 **Catálogo Oficial (Índice Maestro del SGSI):** Las Políticas Específicas que componen el Manual del SGSI son aquellas listadas en la tabla a continuación:

- Controles Organizacionales (Serie 5.x)
- Controles de Personas (Serie 6.x)
- Controles Físicos (Serie 7.x)
- Controles Tecnológicos (Serie 8.x)

ID 191398

Código	Nombre del Documento
Dominio 5	**Controles Organizacionales**
5.1	Políticas de seguridad de la información
5.2	Funciones y responsabilidades en seguridad de la información
5.3	Segregación de funciones
5.4	Responsabilidades de la dirección
5.5	Contacto con autoridades
5.6	Contacto con grupos de interés especiales
5.7	Inteligencia de amenazas
5.8	Seguridad de la información en la gestión de proyectos
5.9	Inventario de información y otros activos asociados
5.10	Uso aceptable de la información y otros activos asociados
5.11	Devolución de activos
5.12	Clasificación de la información
5.13	Etiquetado de la información
5.14	Transferencia de información
5.15	Control de acceso
5.16	Gestión de la identidad
5.17	Información de autenticación
5.18	Derechos de acceso
5.19	Seguridad de la información en las relaciones con proveedores
5.20	Abordar la seguridad de la información en acuerdos con proveedores
5.21	Gestión de la seguridad en la cadena de suministro TIC
5.22	Monitoreo, revisión y gestión de cambios de servicios de proveedores
5.23	Seguridad de la información para el uso de servicios en la nube
5.24	Planificación y preparación de la gestión de incidentes
5.25	Evaluación y decisión sobre los eventos de seguridad
5.26	Respuesta a incidentes de seguridad de la información
5.27	Aprendizaje de los incidentes de seguridad de la información
5.28	Recolección de evidencia
5.29	Seguridad de la información durante la interrupción
5.30	Preparación de TI para la continuidad del servicio
5.31	Requisitos legales, estatutarios, reglamentarios y contractuales
5.32	Derechos de propiedad intelectual
5.33	Protección de los registros
5.34	Privacidad y protección de la información de identificación personal (PII)
5.35	Revisión independiente de la seguridad de la información
5.36	Cumplimiento de las políticas y normas de seguridad

ID 191398

5.37	Procedimientos operativos documentados
Dominio 6	**Controles de Personas**
6.1	Selección
6.2	Términos y condiciones del empleo
6.3	Concientización, educación y formación en seguridad
6.4	Proceso disciplinario
6.5	Responsabilidades después de la terminación o cambio de empleo
6.6	Acuerdos de confidencialidad o de no divulgación
6.7	Trabajo a distancia
6.8	Reporte de eventos de seguridad de la información
Dominio 7	**Controles Físicos**
7.1	Perímetros de seguridad física
7.2	Controles de entrada física
7.3	Asegurar oficinas, salas e instalaciones
7.4	Monitoreo de la seguridad física
7.5	Protección contra amenazas físicas y ambientales
7.6	Trabajo en áreas seguras
7.7	Escritorio y pantallas limpias
7.8	Ubicación y protección de los equipos
7.9	Seguridad de los activos fuera de las instalaciones
7.10	Medios de almacenamiento
7.11	Servicios públicos (Suministros)
7.12	Seguridad del cableado
7.13	Mantenimiento del equipamiento
7.14	Eliminación segura o reutilización de activos
Dominio 8	**Controles Tecnológicos**
8.1	Dispositivos terminales del usuario
8.2	Derechos de acceso privilegiado
8.3	Restricción de acceso a la información
8.4	Acceso al código fuente
8.5	Autenticación segura
8.6	Gestión de la capacidad
8.7	Protección contra malware
8.8	Gestión de vulnerabilidades técnicas
8.9	Gestión de la configuración
8.10	Borrado de la información
8.11	Enmascaramiento de datos
8.12	Prevención de la fuga de datos

ID 191398

8.13	Respaldo de información
8.14	Redundancia de las instalaciones de tratamiento de información
8.15	Registro (Logging)
8.16	Actividades de supervisión
8.17	Sincronización de relojes
8.18	Uso de programas de utilidad privilegiados
8.19	Instalación de software en sistemas operativos
8.20	Seguridad de las redes
8.21	Seguridad de los servicios de red
8.22	Segregación de redes
8.23	Filtrado Web
8.24	Uso de criptografía
8.25	Ciclo de vida de desarrollo seguro
8.26	Requisitos de seguridad de las aplicaciones
8.27	Principios de arquitectura e ingeniería de sistemas seguros
8.28	Codificación segura
8.29	Pruebas de seguridad en el desarrollo y la aceptación
8.30	Desarrollo externalizado
8.31	Separación de ambientes de desarrollo, prueba y producción
8.32	Gestión de cambios
8.33	Información de prueba
8.34	Protección de sistemas durante pruebas de auditoría

10.3 **Ciclo de Vida y Aprobación:** Todas las políticas específicas y normas deben seguir un ciclo de vida formal:

- **Elaboración/Actualización:** A cargo del Oficial de Seguridad de la Información (CISO) o las áreas técnicas competentes.
- **Validación:** Revisión técnica por el Comité de Tecnologías, Seguridad de la Información y Ciberseguridad (CSI).
- **Aprobación:** Formalización mediante acto administrativo de la Jefatura de Servicio.
- **Revisión:** Todos los documentos deberán ser revisados, como mínimo, una vez al año o ante cambios significativos en el entorno tecnológico o legal, para asegurar su vigencia.

10.4 **Disponibilidad y Difusión:** Para garantizar el acceso oportuno a la normativa vigente, la Subsecretaría dispone de un Repositorio Oficial. Es responsabilidad de cada funcionario consultar las versiones vigentes en los canales oficiales antes de ejecutar procedimientos críticos. El desconocimiento de estas normas, estando debidamente publicadas, no exime de su cumplimiento.

- **Ubicación Digital:** Intranet Institucional > Unidad de Gestión Estratégica > Seguridad de la Información.
- **Sitio Web de Referencia:** http://ssi.economia.cl

11. Incumplimiento y Sanciones

El cumplimiento de las normas de seguridad de la información es una obligación inherente al desempeño de la función pública y a la ejecución de contratos con el Estado. La ignorancia de estas normas no excusa su incumplimiento.

La violación de las disposiciones señaladas en el SGSI y sus documentos complementarios dará lugar a las responsabilidades y sanciones que se detallan a continuación:

11.1 **Responsabilidad Administrativa:** Para el personal de planta y a contrata, la seguridad de la información se considera parte integrante de los deberes funcionarios de probidad, obediencia y custodia de bienes públicos.

- **Mecanismo:** Toda infracción detectada será investigada mediante el correspondiente Sumario Administrativo o Investigación Sumaria, instruido por la autoridad competente.
- **Sanciones:** De comprobarse la responsabilidad administrativa, se aplicarán las medidas disciplinarias establecidas en la Ley N° 18.834 (Estatuto Administrativo).

11.2 **Responsabilidad Contractual (Honorarios y Proveedores):** Para el personal a honorarios y las empresas proveedoras externas, el cumplimiento de estas políticas es una obligación contractual esencial.

- **Personal a Honorarios:** El incumplimiento grave o reiterado de las normas de seguridad facultará a la Subsecretaría para poner término anticipado al contrato de prestación de servicios, sin derecho a indemnización alguna.
- **Proveedores y Contratistas:** En caso de infracción por parte de una empresa externa (ej. Desarrollo de Software, Soporte, Datacenter), se aplicarán las medidas estipuladas en las Bases de Licitación y el Contrato respectivo, incluyendo:
    - Cobro de multas por incumplimiento de Niveles de Servicio (SLA).
    - Ejecución de las Boletas de Garantía de Fiel Cumplimiento.
    - Término anticipado del contrato y reporte al Registro de Proveedores de Mercado Público.

11.3 **Responsabilidad Penal (Ley de Delitos Informáticos):** Sin perjuicio de las sanciones administrativas o contractuales descritas anteriormente, las conductas que revistan el carácter de delito serán perseguidas penalmente conforme a la Ley N° 21.459.

- **Obligación de Denuncia:** Todo funcionario público tiene la obligación legal de denunciar ante el Ministerio Público o las policías cualquier hecho que pueda constituir un delito informático.
- **Delitos Tipificados:** Se perseguirá activamente a quienes incurran en conductas tales como:
    - Acceso ilícito a sistemas informáticos (hacking).
    - Interceptación o captura de datos.
    - Falsificación informática (alteración de registros).
    - Sabotaje informático (borrado o destrucción de datos).
    - Fraude informático.
    - Abuso de dispositivos (uso de malware).

ID 191398

11.4 **Responsabilidad Civil** La Subsecretaría se reserva el derecho de ejercer las acciones civiles necesarias para perseguir la reparación e indemnización de los perjuicios materiales y morales causados al patrimonio institucional por el actuar doloso o culposo de funcionarios o terceros.

11.5 **Deber de Reporte** Constituye una falta grave la ocultación deliberada de un incidente de seguridad. Todo funcionario o tercero que tome conocimiento de una vulnerabilidad, brecha o violación a estas políticas, tiene la obligación inmediata de reportarlo al Oficial de Seguridad de la Información (CISO) o a través de los canales oficiales de denuncia. La omisión de este reporte será sancionada conforme a las normas de responsabilidad administrativa.

ARTÍCULO QUINTO: Instrúyese a todas las Jefaturas de División, Departamento y Unidad la difusión obligatoria de estas normas entre el personal a su cargo, así como velar por su estricto cumplimiento. El incumplimiento de las disposiciones de seguridad de la información podrá dar lugar a las responsabilidades y sanciones administrativas que correspondan, conforme al Estatuto Administrativo.

ARTÍCULO SEXTO: Publíquese la presente Resolución en la Intranet institucional y, según corresponda en virtud de las normas de transparencia activa, en el sitio web institucional, para conocimiento de todos los funcionarios y usuarios.

ANÓTESE, PUBLÍQUESE EN LA INTRANET DE LA SUBSECRETARÍA Y COMUNÍQUESE

KARLFRANZ KOEHLER DUNCKER
SUBSECRETARIO DE ECONOMÍA Y EMPRESAS DE MENOR TAMAÑO

DISTRIBUCIÓN

- Gabinete de Ministro de Economía, Fomento y Turismo
- Auditoría Ministerial
- Unidad de Gestión Estratégica
- Unidad de Comunicaciones
- Gabinete Subsecretario de Economía y Empresas de Menor Tamaño
- Secretarías Regionales Ministeriales
- Unidad de Auditoría Interna
- Unidad de Control de Gestión
- División de Empresas de Menor Tamaño
- División de Asociatividad y Cooperativas
- División Política Comercial e Industrial
- División Jurídica
- División Fomento, Inversión e Industria
- División Competencia y Mejora Regulatoria
- División de Desarrollo Productivo Sostenible
- Departamento Administrativo
- Unidad de Gestión y Desarrollo de Personas
- Oficina de Partes
- Archivo Seguridad de la Información y Ciberseguridad

Información de firma electrónica:	
Firmantes	KARLFRANZ KOEHLER DUNCKER
Fecha de firma	23-06-2026
Código de verificación	705528
URL de verificación	https://tramites.economia.gob.cl