POLÍTICA GENERAL
DE SEGURIDAD DE LA INFORMACIÓN

Pol-SSI-05v4.0

Subsecretaría de Transportes

Gobierno de Chile

SUBSECRETARÍA DE TRANSPORTES

Octubre 2018

	Nombre	Cargo	Firma	Fecha
Aprobado por	José Domínguez C.	Subsecretario Transportes		
Revisado por Comité de Seguridad de la Información	Karen Caiceo M.	Presidente Comité Seguridad de la Información		26/12/2018
	Paula Vidal Mohr	Gabinete Subsecretario	Paula Vidal	26/12/2018
	Alvaro Goncalves B.	Encargado Unidad de Gestión de Procesos		
	Mireille Caldichoury O.	Coordinación de Personas		
	Marycela Marquez Marquez	División de Administración y Finanzas		
	María Rojas Zúñiga	División Legal		26/12/2018
	Patricio Echenique G.	Encargado Unidad de Planificación y Control de Gestión		31-12-2018
	Jaime González P.	Encargado Unidad TIC		26/12/2018
Elaborado por	Andrés Fuenzalida V.	Encargado de Seguridad de la Información		26/12/2018

TABLA DE CONTENIDO

Nota de equidad de género:

El uso de un lenguaje que no discrimine ni marque diferencias entre hombres y mujeres ha sido una preocupación en la elaboración de este documento. Sin embargo, y con el fin de evitar la sobrecarga gráfica que supondría utilizar en español o/a para marcar la existencia de ambos sexos, se ha optado por utilizar el masculino genérico, en el entendido de que todas las menciones en tal género representan siempre a todos/as, hombre y mujeres, abarcando claramente ambos sexos.

1. DECLARACIÓN INSTITUCIONAL

La Subsecretaría de Transportes reconoce el valor de la información como un activo fundamental de la organización que necesita ser debidamente protegido, minimizando los riesgos y asegurando la continuidad operacional de sus funciones, tomando en cuenta los tres aspectos fundamentales en la Seguridad de la Información como son: Confidencialidad, Integridad y Disponibilidad de sus activos de información. En este contexto, la Institución asume el compromiso entorno a la gestión de sus activos de información relevantes, que pudieran verse afectados en la conformidad de sus productos y servicios proporcionados a la ciudadanía, a objeto de asegurar su total satisfacción.

Es por ello que esta Subsecretaría, ha decidido utilizar y guiarse por los requisitos establecidos en la Norma NCh-ISO 27001:2013, a fin de mantener y seguir desarrollando las Políticas de Seguridad de la Información al interior de la Institución, garantizando que los procesos que brindan los diferentes servicios a los usuarios, se desarrollen de forma segura y continua.

En consecuencia, este documento presenta los lineamientos necesarios para abarcar cada uno de los ámbitos de acción del Sistema de Seguridad de la Información al interior de la Subsecretaría de Transportes y sus programas dependientes , su documentación y controles asociados.

2. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

2.1 Objetivos Generales

Lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucionales relevantes, asegurando la continuidad operacional de los procesos.

2.2 Objetivos Específicos

- Identificar y catastrar todos los activos de información relevantes que están presentes directa o indirectamente en cada proceso institucional, abarcando tanto los procesos críticos institucionales, como los de soporte.

- Realizar actividades necesarias de análisis de riesgo, según normativas, técnicas y estándares disponibles y aplicables, para diseñar e implantar medidas y controles que permitan mitigar los riegos que sean identificados, sin perder de vista el enfoque de la gestión por procesos instituciones.

- Proteger la información, sus medios de procesamiento, conservación y transmisión del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotaje, violación de la privacidad y otras acciones que pudieran perjudicarlas o ponerla en riesgo.

- Mantener y hacer uso de la estructura y el marco de estándares, políticas y procedimientos en materia de seguridad de la información.

- Minimizar la posibilidad de ocurrencia de hechos contingentes que pudieran interrumpir la operación del negocio y reducir el impacto de los daños a las

instalaciones, medios de almacenamiento, equipos de procesamiento y de comunicación.

- Hacer Uso de/los plan/es de continuidad operacional ante hechos contingentes que interrumpan la operación del negocio.

- Sensibilizar y capacitar a los servidores estatales de la Subsecretaría de Transportes y sus programas, acerca de sus responsabilidades para mantener la seguridad de la información y su adecuado uso, estableciendo una cultura organizacional que incorpore el tema de seguridad de la información como un aspecto relevante en los procesos de negocio de la Subsecretaría de Transportes.

3. ALCANCES DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La presente Política será de aplicación obligatoria a toda la Subsecretaría de Transportes y sus programas dependientes, sus procesos, personal, sean de planta, contrata o servidores a honorarios, proveedores y usuarios tanto internos como externos. En este sentido, los incumplimientos que den origen a incidentes que afecten la seguridad de los activos de información, serán objeto de responsabilidad administrativa, en los términos establecidos en el Título V del DFL N°29 de 2005, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo.

Las disposiciones que informan la presente Política de Seguridad de la Información, se sustentan en los requisitos definidos en la Norma NCh-ISO 27001:2013, que regula el aseguramiento, la confidencialidad e integridad de datos y de la información, así como de los sistemas que la procesan, y demás normativa vigente aplicable a este Servicio, que comprende entre otras, el Decreto N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, que aprueba la norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.

En cuanto a las temáticas de protección abordadas, el ámbito de aplicación de esta Política corresponde al (a los) Dominio(s) de Seguridad de la Información y Controles de Seguridad respectivos, detallados a continuación:

Dominios y Controles de Seguridad relacionados	
Nombre Control	**Objetivo del Control**
Dominio: Políticas de Seguridad de la Información	
A.05.01.01	Políticas para la seguridad de la información
A.05.01.02	Revisión de las políticas de seguridad de la información
Dominio: Organización de la Seguridad de la Información	
A.06.01.01	Roles y responsabilidades de la seguridad de la información
A.06.01.02	Segregación de funciones
Dominio: Seguridad de recursos humanos	
A.07.02.01	Responsabilidades de la dirección
A.07.02.02	Concientización, educación y formación en seguridad de la información
Dominio: Administración de Activos	

A.08.01.01	Inventario de activos
Dominio: Control de Acceso	
A.09.01.01	Política de control del acceso
Dominio: Criptografía	
A.10.01.01	Política sobre el uso de controles criptográficos
Dominio: Seguridad Física y del Ambiente	
A.11.01.01	Perímetro de seguridad física
Dominio: Seguridad de las Operaciones	
A.12.01.01	Procedimientos de operación documentados
Dominio: Seguridad de las Comunicaciones	
A.13.01.01	Controles de red
Dominio: Adquisición, desarrollo y mantenimiento del Sistema	
A.14.01.01	Análisis y especificación de requisitos de seguridad de la información
Dominio: Relaciones con los Proveedores	
A.15.01.01	Política de seguridad de la información para las relaciones con el proveedor
Dominio: Administración de incidentes de seguridad de la información	
A.16.01.01	Responsabilidades y procedimientos
Dominio: Aspectos de la Seguridad de la Información en la Administración de la continuidad operacional	
A.17.01.01	Planificación de la continuidad de la Seguridad de la Información
Dominio: Cumplimiento	
A.18.02.01	Revisión independiente de la seguridad de la información
A.18.02.02	Cumplimiento con las políticas y normas de seguridad
A.18.02.03	Verificación del cumplimiento técnico

En cuanto al ámbito institucional de aplicación de esta Política, corresponde a los objetivos y productos estratégicos más abajo singularizados, extraídos de la "FICHA DE DEFINICIONES ESTRATÉGICAS AÑOS 2019 – 2022", la que describe los procesos críticos y los alcances declarados para conformar el Sistema de Gestión de Seguridad de la Información de Subsecretaría de Transporte y sus programas dependientes:

Objetivo, Producto estratégico y Proceso crítico en ámbito de aplicación		
Objetivo Estratégico Subsecretaría de Transporte	Producto Estratégico A1	Proceso crítico protegido
(1) Fortalecer el desarrollo de sistemas y servicios de transportes públicos dignos, accesibles, confiables, expeditos, eficientes, seguros y sustentables.	(1) Regulación que rige el transporte.	Políticas y normas que rigen el transporte.
	(2) Fiscalización y Certificación de los Sistemas de Transporte.	Transporte Público Regional.
	(5) Subsidios e iniciativas de inversión para la operación y	Fiscalización.

	fortalecimiento de los Servicios de Transporte Público. (6) Planificación, diseño y desarrollo de los Sistemas de Transporte de personas y de carga.	Planificación de los Sistemas de Transporte Urbano.
(2) Mejorar el desarrollo de sistemas y servicios de transporte de bienes y servicios que impacten positivamente en el crecimiento y desarrollo económico del país.	(1) Regulación que rige el Transporte. (6) Planificación, diseño y desarrollo de los Sistemas de Transporte de personas y de carga	Políticas y normas que rigen el transporte. Planificación de los Sistemas de Transporte Urbano.
(3) Fomentar y fiscalizar el uso de medios de transporte de baja o cero emisión que contribuyan a la prevención de accidentes, a la reducción de víctimas fatales y a reducir la congestión vehicular.	(1) Regulación que rige el Transporte. (2) Fiscalización y Certificación de los Sistemas de Transporte. (4) Información, difusión y atención a la Ciudadanía en materias de transporte.	Políticas y normas que rigen el transporte. Fiscalización. Información y atención a la ciudadanía en materias de transporte.
(4) Desarrollar políticas, normativas y regulación de sistemas y servicios de transportes, fiscalización y seguridad vial, con enfoque de género y accesibilidad universal.	(1) Regulación que rige el Transporte. (2) Fiscalización y Certificación de los Sistemas de Transporte. (3) Monitoreo y Control de Tránsito.	Políticas y normas que rigen el transporte. Fiscalización.
(5) Diseñar sistemas y servicios de transportes que respondan a las principales necesidades de movilidad de las personas, priorizando los modos más eficientes y sustentables, y mejorando la convivencia vial considerando el enfoque de género y la accesibilidad universal.	(1) Regulación que rige el Transporte. (2) Fiscalización y Certificación de los Sistemas de Transporte. (3) Monitoreo y Control de Tránsito. (5) Subsidios e iniciativas de inversión para la operación y fortalecimiento de los Servicios de Transporte Público. (6) Planificación, diseño y desarrollo de los Sistemas de Transporte de personas y de carga	Políticas y normas que rigen el transporte. Transporte Público Regional. Fiscalización. Planificación de los Sistemas de Transporte Urbano.
(6) Desarrollar y mantener una gestión institucional eficiente, eficaz, transparente, innovadora y cercana a la ciudadanía, a través del mejoramiento	(1) Regulación que rige el Transporte. (2) Fiscalización y Certificación de los Sistemas de Transporte.	Políticas y normas que rigen el transporte. Transporte Público Regional.

continuo y la automatización de los procesos claves de la Subsecretaría de Transportes	(3) Monitoreo y Control de Tránsito. (4) Información, difusión y atención a la Ciudadanía en materias de transporte. (5) Subsidios e iniciativas de inversión para la operación y fortalecimiento de los Servicios de Transporte Público. (6) Planificación, diseño y desarrollo de los Sistemas de Transporte de personas y de carga	Fiscalización. Planificación de los Sistemas de Transporte Urbano. Información y atención a la ciudadanía en materias de transporte.

4. ROLES Y RESPONSABILIDADES

La estructura de roles para el Sistema de Gestión de Seguridad de la Información - SGSI, estará constituida de la siguiente manera:

Responsable	Rol	Funciones
Subsecretario(a) de Transportes	Liderar la definición e implementación de la Política de Seguridad de la Información.	▪ Generación de lineamientos y criterios generales. ▪ Aprobación de políticas institucionales. ▪ Evaluación del funcionamiento y efectividad del SGSI a intervalos planificados. ▪ Asignación de recursos según las necesidades para la gestión de la seguridad de la información.
Comité de Seguridad de la Información (CSI SUBTRANS)	Coordinar los avances en la implementación y funcionamiento de las políticas y procedimientos.	▪ Responsable de la implementación y mantención del SGSI institucional. ▪ Revisión periódica del SGSI, en particular de las responsabilidades del Encargado de Seguridad de la Información y sus Contrapartes, y los Responsables de Dominios. ▪ Monitorear el avance general de la implementación de los planes de continuidad del servicio. ▪ Reportar periódicamente al Subsecretario(a) de Transportes respecto de las oportunidades de mejora, los incidentes relevantes y su gestión.
Encargado de Seguridad de la Información	Responsable de cautelar un adecuado resguardo y	▪ Actuar como asesor del Jefe del Servicio en las materias relativas a seguridad de la información. ▪ Diseñar e implementar políticas, normas y

(ESI SUBTRANS)	protección de los activos de información en la institución.	procedimientos de seguridad de la información, mantener el control de su implementación y velar por su correcta aplicación. ▪ Detectar y comprender las necesidades de la organización en materia de seguridad de la información, e instar para su incorporación de manera coherente a la estrategia institucional. ▪ Promover iniciativas y proyectos que aumentan la seguridad de la información, liderar proyectos de securitización, definir y publicar políticas de seguridad. ▪ Asesorar en forma permanente y cercana a las distintas áreas de la Subsecretaría de Transportes y programas dependientes en temas relacionados con seguridad y conducir al correcto cumplimiento de los estándares de seguridad definidos. ▪ Comunicar al Subsecretario en forma oportuna, sobre las materias en que se requiera su apoyo y a través de ello lograr alinear al personal de la Subsecretaría de Transportes y programas dependientes, en torno a las políticas y procedimiento de seguridad de la información ▪ Preparar instrucciones para la seguridad de los activos de información, respecto al uso seguro del correo electrónico, la asignación de identificadores, uso de redes y servicios de red ▪ Coordinar equipos de trabajo abocados a temas de seguridad de la información compuestos por diferentes estamentos del servicio.
Contrapartes del Encargado de Seguridad de la Información de los Programas de la Subsecretaría de Transportes (Contrapartes ESI Programas SUBTRANS)	Encargados de la implementación de la Política de Seguridad de la Información en los programas dependientes de la Subsecretaría de Transportes	▪ Asesorar al Encargado de Seguridad de la Información, así como al Comité de Seguridad de la Información, en materias relativas a la seguridad de los activos de información. • Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de la institución, para proponer su aprobación al Comité de Seguridad de la Información. • Tener a su cargo, el control de la implementación de las políticas, velando por su correcta aplicación. • Coordinar las respuestas de los programas ante incidentes que afecten a los activos de información institucionales.

		• Establecer en coordinación con el Encargado de Seguridad de la Información, puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad. • Proponer al Encargado de Seguridad de la Información y al Comité de Seguridad de la Información, la clasificación y procedimientos del caso para el procesamiento de los activos de información al interior de los programas. • Preparar instrucciones para la seguridad de los activos de información, respecto al uso seguro del correo electrónico, la asignación de identificadores, uso de redes y servicios de red al interior de los programas. ▪ Detectar y comprender las necesidades de la organización y sus programas en materia de seguridad de la información, e instar para su incorporación de manera coherente a la estrategia institucional. ▪ Comunicar al Subsecretario en forma oportuna sobre las materias en que se requiera su apoyo y a través de ello lograr alinear al personal de la institución en torno a las políticas y procedimiento de seguridad de la información.
Auditoría Interna (AI)	Aseguramiento del Sistema de Gestión de Seguridad de la Información (SGSI)	• Asegurar que el proceso de monitoreo y revisión de los controles de riesgos, se realicen en conformidad a las políticas, instructivos y documentación complementaria del Sistema de Gestión de Seguridad de la Información Institucional. ▪ Retroalimentar sobre el cumplimiento de las recomendaciones y compromisos de los diferentes responsables que intervienen en el SGSI de la Subsecretaría de Transportes y programas dependientes.
Jefaturas y Responsables de programas de la Subsecretaría de Transportes	Implementar las Políticas y procedimientos emanados del SGSI	• Promover y dar cumplimiento a lo establecido en la presente Política y en las que la complementen y aplicarlo en su entorno laboral, a través de los procedimientos e instrucciones que se determinen en el marco del SGSI. • Alertar de manera oportuna y adecuada al CSI, cualquier situación que atente contra lo establecido en esta Política o pueda poner en riesgo la continuidad de los procesos.
Servidores Estatales de la Subsecretaría de Transportes	Colaboradores en la implementación y dar cumplimiento a las	• Dar cumplimiento a lo establecido en la presente Política y en las que la complementen, además de aplicarlo en su entorno laboral, a través de los

	normas y procedimientos que emanan de la Política de la Seguridad de la Información	procedimientos e instructivos que se determinen en el marco del SGSI. • Alertar de manera oportuna y adecuada a la jefatura directa, con copia al CSI, cualquier situación que atente contra lo establecido en esta Política o pueda poner en riesgo la continuidad de los procesos. • Implementar las medidas de prevención en las relaciones con los respectivos usuarios externos, especialmente en lo que diga relación con la confidencialidad de los datos que se determinen en el marco del SGSI. ▪ Debida reserva respecto de los datos que tomen conocimiento en el ejercicio de sus funciones.

Por su parte, considerando los dominios en materia de Seguridad de la Información, se establecen para la Subsecretaría de Transportes y sus programas dependientes, las siguientes responsabilidades por dominio:

Dominios NCh-ISO 27001		
N° Dominio	Nombre de Dominio ISO	Responsable de Dominio ISO
1	Políticas de seguridad de la información	Subsecretario de Transportes
2	Organización de la seguridad de la información	Encargado de Seguridad de la Información
3	Seguridad de recursos humanos	Jefatura de Coordinación de Personas de la Subsecretaría de Transportes
4	Administración de activos	Jefatura de División de Administración y Finanzas de la Subsecretaría de Transportes
5	Control de acceso lógico	Jefatura de Unidad de Tecnología de la Información y las Comunicaciones de la Subsecretaría de Transportes
6	Criptografía	Jefatura de Unidad de Tecnología de la Información y las Comunicaciones de la Subsecretaría de Transportes
7	Seguridad física y ambiental	Jefatura de División de Administración y Finanzas de la Subsecretaría de Transportes
8	Seguridad de las operaciones	Jefatura de Unidad de Tecnología de la Información y las Comunicaciones de la Subsecretaría de Transportes
9	Seguridad en las comunicaciones	Jefatura de Unidad de Tecnología de la Información y las Comunicaciones de la Subsecretaría de Transportes
10	Adquisición, desarrollo y mantenimiento de sistemas	Jefatura de Unidad de Tecnología de la Información y las Comunicaciones de la Subsecretaría de Transportes
11	Relaciones con los proveedores	Jefatura de División de Administración y Finanzas de la Subsecretaría de Transportes

12	Administración de incidentes de seguridad de la información	Jefatura de Unidad de Tecnología de la Información y las Comunicaciones de la Subsecretaría de Transportes
13	Aspectos de la seguridad de la información de la administración de la continuidad operacional	Comité de Seguridad de la Información de la Subsecretaría de Transportes
14	Cumplimiento	Encargado de Seguridad de la Información

Los Responsables de Dominio, deberán supervigilar el cumplimiento de las Políticas e Instructivos de Seguridad de la Información, así como de toda documentación que el Sistema de Gestión de Seguridad de la Información de la Subsecretaría de Transportes genere a partir de su implementación, además de permitir y facilitar el camino para la implantación y control de la Seguridad de la Información al interior de la organización.

5. MARCO NORMATIVO

El marco jurídico referido a los Sistemas de Gestión de Seguridad de la Información (SGSI), se encuentra publicado en el portal del CSIRT del Ministerio del Interior https://www.csirt.gob.cl/decretos.html y comprende:

- Decretos que regulan la Seguridad de la Información y Ciberseguridad:
  - Decreto Supremo N° 5996, de 1999, del Ministerio de Interior, que crea red interna del Estado y entrega su implementación, puesta en marcha, administración, coordinación y supervisión al Ministerio del Interior.
  - Decreto Supremo N° 1299, de 2004, del Ministerio del Interior, que establece nuevas normas que regulan la red de conectividad del estado que administra el Ministerio del Interior y fija los procedimientos, requisitos y estándares tecnológicos para la incorporación a dicha red de instituciones públicas.
  - Decreto Supremo N°1, de 2016, del Ministerio Secretaría General de la Presidencia, que crea comisión asesora presidencial denominada Comité de Ministros para el Desarrollo Digital
  - Decreto Supremo 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.
  - Decreto Supremo N°93, de 2006, el Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los órganos de la Administración del Estado y sus funcionarios.
  - Decreto N° 181, de 2002, del Ministerio de Economía, Fomento y Reconstrucción, Subsecretaría de Economía, Fomento y Reconstrucción, que aprueba reglamento de la ley N° 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.

- Leyes relacionadas
  - Ley N°20.285 de 2008, del Ministerio Secretaría General de la Presidencia, sobre sobre acceso a la información pública
  - Ley N°17.336 de 2004, del Ministerio de Educación Pública, sobre propiedad intelectual

- Ley N°19.880 de 2003, del Ministerio Secretaría General de la Presidencia, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado
- Ley N°19.799 de 2002, del Ministerio de Economía, Fomento y Reconstrucción, Subsecretaría de Economía, Fomento y Reconstrucción, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma
- Ley N°19.628 de 1999, del Ministerio Secretaría de la Presidencia, sobre protección de la vida privada
- Ley N°19.223 de 1993, del Ministerio de Justicia, que tipifica figuras penales relativas a la informática

- Instructivo de Gabinete Presidencial Nro. 8 de 2018, que instruye la implementación de la Política Nacional de CiberSeguridad (PNCS).

6. LINEAMIENTOS PARA LAS POLITICAS DE SEGURIDAD DE LA INFORMACIÓN

El marco general, la gestión de Políticas de Seguridad de la Información en la Subsecretaría de Transportes se sustenta en los siguientes lineamientos:

- **Definición de Seguridad de la Información**: Según lo señalado por la Norma NCh-ISO 27001:2013, se entiende por seguridad de la información al proceso de mejoramiento continuo que se sostiene por un conjunto de medidas preventivas, tecnológicas, organizativas, legales, entre otras, que tienen como objetivo mantener una adecuada protección de la integridad, confidencialidad y disponibilidad de los activos de información de la Subsecretaría de Transportes.

- **Sistema de Gestión de Seguridad de la Información**: Es un proceso continuo de gestión conformado por un debido análisis y gestión de riesgos, para asegurar la continuidad operacional del servicio, minimizar impactos adversos y preservar la seguridad de la información en la Subsecretaría de Transportes cumpliendo con los Objetivos de las Políticas de Seguridad.

- **Gestión de Riesgos de Seguridad de la Información**: Corresponde a la protección de los activos de información institucionales, que incorpora actividades como; a) realizar inventario de activos de información, b) analizar su exposición a amenazas de seguridad de la información y c) mitigar los riesgos encontrados implementando los controles de la norma NCh-ISO 27001:2013. Así mismo, se debe integrar la seguridad de la información en los métodos de administración de proyectos, abordando los riesgos como parte de sus objetivos, permitiendo así la integración de controles de seguridad de la información.

- **Lineamientos en tópicos de seguridad específicos**: Existirá un conjunto de políticas, instructivos y otros documentos normativos, alineadas a los siguientes tópicos de seguridad de la información que corresponden a los dominios o áreas de control necesarios de gestionar:

  - Un conjunto de Políticas de Seguridad de la información, destinadas a dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del servicio, las leyes y regulaciones.

- Una estructura Organizacional para la Gobernabilidad de la Seguridad de la Información, con el objetivo de establecer un esquema directivo de gestión para la implementación y operación de la seguridad de la información en la Subsecretaría de Transporte y sus programas dependientes.

- Seguridad ligada a la gestión del recurso humano, con el fin de formalizar la necesidad de educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación contractual, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.

- Gestión de Activos de información, con el objetivo de identificar y mantener un conocimiento actualizado de los activos en la organización y definir las responsabilidades para una protección adecuada de sus riesgos.

- Mantener adecuados controles de acceso lógico para regular la visibilidad y uso de la información y las instalaciones utilizadas para su procesamiento mediante un sistema de restricciones y excepciones de acceso, como base de todo sistema de seguridad informática.

- Establecer uso de sistemas y técnicas criptográficas para la protección de la información en base al riesgo asociado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

- Fortalecer la seguridad física y del ambiente, destinada a impedir accesos físicos no autorizados, daños e interferencia a las unidades de negocios y de la información de la institución.

- Garantizar la seguridad de las operaciones para una la correcta instalación de procesamiento de la información.

- Garantizar la seguridad de las comunicaciones para la protección de las redes y medios de comunicación.

- Resguardar la seguridad en la adquisición, desarrollo y mantenimiento de los sistemas de seguridad de la información. Orientado a garantizar la incorporación temprana de medidas de seguridad en los sistemas de información, abordando su adquisición o desarrollo, implementación y su mantenimiento.

- Asegurar la protección de los activos de información en la relación con proveedores de la Institución.

- Gestionar adecuadamente potenciales incidentes de seguridad de la información, minimizando sus impactos y evitando su recurrencia.

- Preservar los aspectos de seguridad de la información en la gestión de continuidad del negocio.

- Velar por el cumplimiento e impedir infracciones y violaciones a las disposiciones legales, reglamentarias, estatutarias o contractuales vigentes, que digan relación con los requisitos de seguridad de la información.

7. MONITOREO Y REVISIÓN

A lo menos una vez al año, el Comité de Seguridad de la Información (CSI), debe evaluar el cumplimiento de la Política General de Seguridad de la Información, considerando los cambios que puedan surgir en el curso del período y que podrían afectar el enfoque de la organización, y la gestión de la seguridad de la información, incluyendo cambios al ambiente de la organización, disponibilidad de los recursos, condiciones contractuales, reguladoras, y legales, así como cambio al ambiente técnico.

Para ello se deben considerar aspectos como:

- Retroalimentación de las partes interesadas,
- Resultados de las revisiones efectuadas por terceras partes,
- Estado de acciones preventivas y correctivas,
- Cambios en los procesos institucionales, nueva legislación, tecnología, etc.,
- Alertas ante amenazas y vulnerabilidades,
- Información relacionada a incidentes de seguridad,
- Recomendaciones provistas por autoridades relevantes,
- Medición de los indicadores del Sistema.

Por lo tanto, se deberá revisar el estado del Sistema de Gestión de Seguridad de la Información, a lo menos cada tres años mediante auditorías internas o externas.

8. EXCEPCIONES AL CUMPLIMIENTO DE ESTA POLÍTICA

Frente a casos particulares como conflictos en materias de seguridad y/o situaciones de riesgo que afecten a los activos de información, el Comité de Seguridad de la Información podrá establecer condiciones puntuales de excepcionalidad en el cumplimiento de las directrices de esta Política, siempre que no infrinja la legislación vigente, ni afecte las directrices de otras políticas. Toda excepción, deberá ser documentada y monitoreada, generando un proceso de revisión de la misma, para determinar si amerita nuevas directrices particulares o cambio en otras existentes.

9. MECANISMO DE DIFUSIÓN

Todas las políticas deberán ser informadas mediante un conjunto de actividades planificadas como: publicaciones en sitios web internos y externos de la organización, difusión periódica mediante correo electrónico, en los procesos de inducción del personal nuevo y a través de los contratos por servicios de terceros. En caso de existir ajustes en las políticas, procedimientos y/o instructivos, estas se deberán notificar a los interesados, por medio de correo institucional.

10. GLOSARIO DE TÉRMINOS, DEFINICIONES Y SIGLAS

Las definiciones relacionadas con el SGSI institucional, se encontraran disponibles en el documento denominado "Estándar de Seguridad – Glosario de Términos de SSI-MTT" publicado en la sección "Políticas de Seguridad de la Información" del sitio web interno de la Subsecretaría de Transportes, bajo la dirección http://www.intranet.mtt.cl/centro-documentacion/552.

11. HISTORIAL Y CONTROL DE VERSIONES

N° de Versión	Fecha de Aprobación	Resumen de las Modificaciones	Páginas Modificadas	Autor
0	12/2010	Elaboración inicial	Todas	XM
1.0	06/2011	Actualización de Política	2-3-4-5	HBD
1.1	10/2011	Actualización Políticas	2	LFG
2.0	06/2014	Actualización de la Política	Todas	LFV
2.2	12/2015	Adecuación de responsabilidades y a controles de NCh-ISO 27001:2013 (A.06.01.01, A.06.01.05, A.18.02.01, A.18.02.02)	Todas	RMK
3.0	10/2017	Actualización de la Política a nuevos requerimientos de formato y contenidos.	Todas	RMK
4.0	10/2018	Actualización de la Política en los siguientes tópicos: - Objetivos Generales y Específicos; - Ámbito institucional de aplicación; - Roles y Responsabilidades; - Incorporación de Responsables de Dominios ISO; - Lineamientos para las Políticas SSI; y - Monitoreo y Revisión;	Todas	AFV