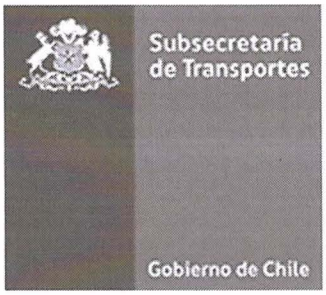
POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Pol-SSI-06 v1.0



SUBSECRETARÍA DE TRANSPORTES

Diciembre 2017

	Nombre	Cargo	Firma	Fecha
Aprobado por	Matías Schöll	Presidente Comité Seguridad de la Información		27/12/2017
Revisado por Comité de Seguridad de la Información (Quorum mínimo 4 integrantes)	Carola Jorquera	Gabinete Subsecretario		27/12/2017
	Karen Caiceo	Encargada Unidad de Gestión de Procesos		27/12/17
	Mireille Caldichoury	Coordinación de Personas		27/12/2017
	Juan Gregorio Flores	Departamento de Contabilidad, Presupuesto y Tesorería		
	Patricio Santidrian	División Legal		27/12/17
	Patricio Echenique	Encargado Unidad de Planificación y Control de Gestión		27/12/17
	Jaime Gonzalez	Encargado Unidad TIC		27/12/2017
Elaborado por	Roy Mac Kenney	Encargado de Seguridad de la Información		27/12/2017

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 se compromete a mantener políticas en el ámbito de la seguridad de la información, con el fin de asegurar que sus procesos brinden servicios a la comunidad y tengan la debida continuidad operacional que se requiere.

Este documento presenta los lineamientos necesarios que permiten establecer la gobernabilidad de la seguridad de la información, como parte fundamental de los objetivos y actividades de la institución.

2. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos generales de la Política de Organización de la Seguridad de la Información, son:

- Cumplir con la Norma Chilena Oficial NCh-ISO 27001:2013.
- Cumplir con la Política General de Seguridad de la Información
- Establecer un esquema directivo de gestión para iniciar y controlar la implementación y operativa de la seguridad de la información.
- Garantizar la seguridad de la información en el uso de recursos de informática móvil y remota.

3. CONTEXTO O ÁMBITO DE APLICACIÓN

La Política de Organización de la Seguridad de la Información se aplica a todo el personal de la Subsecretaría de Transportes y sus Programas dependientes sean de planta, contrata o a honorarios, y externos que presten servicios a ella, e involucra a las visitas y a todos sus instalaciones, recursos y activos de información.

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	
A.06	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
A.06.01.03	Contacto con autoridades
A.06.01.04	Contacto con grupos especiales de interés
A.06.01.05	Seguridad de la información en la gestión de proyecto
A.06.02.01	Política de dispositivos móviles
A.06.02.02	Trabajo remoto

En cuanto al ámbito institucional de aplicación de esta política, corresponde a los siguientes objetivos y productos estratégicos del formulario A1 relacionados con procesos críticos que corresponden al alcance declarado del Sistema de Seguridad de la Información de SUBSECRETARÍA DE TRANSPORTE:

Objetivo, Producto estratégico y Proceso crítico en ámbito de aplicación		
Objetivo Estratégico SUBSECRETARÍA DE TRANSPORTE	Producto Estratégico A1	Proceso crítico protegido
(1) Disminuir fallecidos por accidentes de tránsito. (2) Desarrollar planes y estudios que permiten definir políticas y normativas en los temas relevantes a transporte de carga.	(1) Regulación que rige el transporte	Políticas y normas que rigen el transporte.
(3) Mejorar las condiciones para la operación e integración del Transporte Público a través de infraestructura prioritaria, con foco inicial en la mejora de los tiempos de viaje. (4) Diseñar sistemas de transportes que respondan a las principales necesidades multimodales de las personas, priorizando los modos más eficientes y sustentables y mejorando la convivencia de usuarios de los distintos modos. (6) Velar por la accesibilidad, calidad, seguridad e impacto ambiental que entregan los servicios de transporte terrestre y otros modos.	(5) Subsidios e iniciativas de inversión para la operación y fortalecimiento de los Servicios de Transporte Público.	Transporte Público Regional.

4. ROLES Y RESPONSABILIDADES

- **El Jefe de Servicio**
  - Es el responsable institucional del debido resguardo de la Seguridad de la Información y que por tanto es quien oficializa la presente estructura de gobernabilidad.

- **El Comité de Seguridad de la Información (CSI)**

  En concordancia con la resolución que aprueba este comité, se identifican las siguientes funciones relacionadas con esta temática:
  - Supervisar la implementación de la presente política.

- **El Encargado de Seguridad de la Información (ESI)**
  - Es responsable de la elaboración de la presente política, de su actualización y velar por el cumplimiento de sus disposiciones.

- **Los responsables de activos de información**
  - Deben clasificar la información en el inventario de Activos de Información según el grado de criticidad, de documentar y mantener actualizada la clasificación, además de definir los usuarios con permisos de acceso a la información de acuerdo a las funciones y competencias.

- **Todos los funcionarios de la Subsecretaría de Transportes**
  - Deben asegurarse de conocer, cumplir y hacer cumplir la Política de Seguridad de la Información.

5. MARCO NORMATIVO

El Marco Jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior https://www.csirt.gob.cl/decretos.html.

- Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad:
  - Decreto Supremo N° 1299, de 2004, del Ministerio del Interior.
  - Decreto Supremo N° 5996, de 1999, del Ministerio de Interior.
  - Decreto Supremo N°1, de 2015, del Ministerio Secretaría General de la Presidencia.
  - Decreto Supremo N°83, de 2004, del Ministerio Secretaría General de la Presidencia.
  - Decreto Supremo N°93, de 2006, el Ministerio Secretaría General de la Presidencia.

- Leyes relacionadas
  - Ley N°20.285/2008 Ley sobre acceso a la información pública
  - Ley N°17.336/2004 Ley sobre propiedad intelectual
  - Ley N°19.927/2004 Ley modifica códigos penales en materia de delitos sobre pornografía infantil
  - Ley N°19.880/2003 Ley que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado
  - Ley N°19.799/2002 Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma
  - Ley N°19.628/1999 Ley sobre protección de la vida privada
  - Ley N°19.223/1993 Ley sobre figuras penales relativas a la informática

- Instructivo de Gabinete Presidencial Nro. 1 de 2017, que instruye la implementación de la Política Nacional de CiberSeguridad (PNCS).

6. MATERIAS QUE ABORDA

La presente política aborda lineamientos para la Organización de la Seguridad de la Información, en tópicos de:

- Roles y responsabilidades de la seguridad de la información
- Segregación de funciones y usuarios
- Contacto con autoridades
- Contacto con grupos especiales de interés
- Seguridad de la información en la gestión de proyecto
- Protección de dispositivos móviles
- Trabajo remoto.

7. LINEAMIENTOS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

7.1 Asignación de roles y responsabilidades de la seguridad de la información

Como Estructura de Gobernabilidad para la Seguridad de la Información, la Subsecretaría de Transportes cuenta con una estructura que permite mantener la gestión de mejora continua de la Seguridad de la Información mediante los roles del Jefe de Servicio, como responsable institucional quien conforma y designa mediante Resolución Exenta un Comité de Seguridad de la Información (CSI) y un Encargado de Seguridad de la Información (CSI), según lo norma el Decreto Supremo N° 83 de 2004.

En forma complementaria, en la Política General de Seguridad de la Información, se definen los siguientes Roles y Responsabilidades:

- Jefe de Servicio
- Comité de Seguridad de la Información (CSI)
- Encargado de Seguridad de la Información (ESI)
- Unidad de Planificación y Control de Gestión
- Responsables de los activos de información
- Funcionarios de la Subsecretaría de Transportes

7.2 Segregación de funciones

Se deben segregar las funciones y las áreas de responsabilidad para evitar potenciales conflictos de intereses, con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la institución.

7.3 Segregación de usuarios.

Los usuarios deben ser segregados mediante perfiles de usuario que deben ser definidos en consecuencia a las descripciones de cargo y contener los mínimos accesos a los sistemas de información para llevar a cabo sus funciones.

Estos perfiles serán gestionados por el Área de Infraestructura de la Unidad de TIC, mediante Active Directory (la gestión de permisos incluye administración del equipo, acceso a Sistemas, acceso a sitios web, etc.).

El Encargado de Proyectos de la unidad de TIC debe elaborar y mantener actualizado el Instructivo de Roles de Usuarios respecto a cada Sistema de Información en producción. Además, previo al paso a producción de un sistema nuevo o modificado, debe emitir una nueva versión del Instructivo con la actualización de los roles de cada cargo en el sistema nuevo o modificado.

7.4 Segregación de Roles del personal de la Unidad de TIC

El Encargado de la Unidad de TIC, junto a Coordinación de Personas debe elaborar y mantener actualizada las respectivas descripciones de cargos de la Unidad de TIC.

Además, debe velar por que los roles de los cargos de La Unidad de TIC sean segregados funcionalmente con el propósito de reducir las modificaciones no-autorizadas o mal uso no-intencional de los activos de Información de la Subsecretaría.

7.5 Contacto con autoridades

Se deben mantener contactos apropiados con autoridades pertinentes, particularmente para gestión y coordinación institucional ante incidentes de envergadura o situaciones que puedan tener connotación nacional.

Así, el Comité de Seguridad de la Información, debe mantener la debida coordinación con otras instancias organizacionales para desarrollar estrategias comunes de la institución en estas materias.

El Encargado de Seguridad de la Información, deba establecer puntos de enlaces 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 pertinente.

7.6 Contacto con grupos especiales de interés

Entre otras actividades, el Encargado de Seguridad de la Información, deberá liderar el contacto con grupos o foros de seguridad especializados y asociaciones profesionales en temas de seguridad de la información.

7.7 Seguridad de la información en la gestión de proyecto

Se deber contemplar la seguridad de la información en la gestión de proyectos, de manera independiente al tipo de proyecto a desarrollar por la institución.

7.8 Política de dispositivos móviles

Se deben establecer lineamientos institucionales de seguridad, adecuados para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones.

7.9 Trabajo remoto

Se desarrollará e implantará lineamientos de seguridad para proteger la información accedida, procesada o almacenada desde ubicaciones distintas a las oficinas institucionales.

8. PERIODO DE REVISIÓN

La Subsecretaría debe establecer una revisión independiente la cual asegure la idoneidad, adecuación y efectividad continua del enfoque para administrar la seguridad de la información. Dicha revisión la deberían realizar personas independientes del área bajo revisión o una organización externa que se especialice. Los resultados de la revisión independiente se deberían registrar e informar a la dirección que inició esta revisión y mantener estos registros.

Esta política de Seguridad debe ser revisadas cada 3 años como máximo, para mantener al día su vigencia.

9. EVALUACIÓN DE CUMPLIMIENTO

La revisión del cumplimiento de esta Política se efectuará anualmente por el Encargado de Seguridad de la Información. Adicionalmente, según lo requiera un caso particular, podría requerirse una revisión de cumplimiento por Auditoría ministerial, auditoría interna, jefaturas de cada Unidad o el Comité de Seguridad de la Información, atendiendo necesidades de cambios, para garantizar su idoneidad, adecuación y efectividad.

10. EXCEPCIONES AL CUMPLIMIENTO DE ESTA POLÍTICA

Frente a casos especiales, el Comité de Seguridad de la Información podrá establecer condiciones puntuales de excepción en el cumplimiento de las directrices de esta Política de Seguridad de la Información, siempre que no infrinja la legislación vigente ni afecte

directrices de otras Políticas. Toda excepción debe ser documentada y se le debe efectuar seguimiento, generando un proceso de revisión de la misma, para determinar si amerita una nueva directriz particular o un cambio en otra ya existente.

11. MECANISMO DE DIFUSIÓN

La Subsecretaría de Transportes difundirá ésta y todas las políticas de seguridad mediante un conjunto de actividades planificadas, que tienen como objetivo dar a conocer y sensibilizar a los funcionarios internos y externos, que realicen trabajos para la institución, a través de la publicación en secciones destinadas a la Seguridad de la Información en sitios web internos de la institución, difusión mediante correo electrónico, y como parte de los procesos de inducción del personal nuevo y de los contratos acordados con terceros. Frente a un cambio se notificará por el correo institucional al personal relacionado.

12. GLOSARIO DE TÉRMINOS, DEFINICIONES Y SIGLAS

El completo glosario de términos y siglas utilizados en los documentos del Sistema de Gestión de Seguridad de la Información de la Subsecretaría de Transporte, se encuentran integrados en el Estándar de Seguridad "Glosario Términos de SSI-MTT", ubicado en la sección "Políticas de Seguridad de la Información" de la intranet institucional.

13. HISTORIAL Y CONTROL DE VERSIONES

N° de Versión	Fecha de Aprobación	Resumen de las Modificaciones	Páginas Modificadas	Autor
1	11/2017	Creación del documentos y contenidos según requerimientos PG-SSi 2017.	Todas	RM