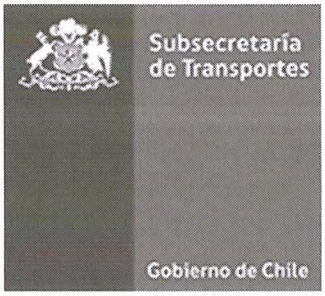
POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

Pol-SSI-10 v2.0



SUBSECRETARÍA DE TRANSPORTES

Noviembre 2017

	Nombre	Cargo	Firma	Fecha
Aprobado por	Matías Schöll	Presidente Comité Seguridad de la Información		23/11/2017
Revisado por Comité de Seguridad de la Información (Quorum mínimo 4 integrantes)	Carola Jorquera	Gabinete Subsecretario		23/11/2017
	Karen Caiceo	Encargada Unidad de Gestión de Procesos		23/11/17
	Mireille Caldichoury	Coordinación de Personas		23/11/17
	Juan Gregorio Flores	Departamento de Contabilidad, Presupuesto y Tesorería		23/11/17
	Patricio Santidrian	División Legal		23/11/2017
	Patricio Echenique	Encargado Unidad de Planificación y Control de Gestión		23/11/2017
	Jaime Gonzalez	Encargado Unidad TIC		23-11-2017
Elaborado por	Roy Mac Kenney	Encargado de Seguridad de la Información		23/11/2017

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 en temas de controles criptográficos para garantizar un uso adecuado y eficaz de la criptografía orientada a proteger la confidencialidad, la autenticidad y/o la integridad de la información.

2. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos generales de la Política de Controles Criptográficos son:

- Cumplir con la Norma Chilena Oficial NCh-ISO 27001:2013.
- Cumplir con la Política General de Seguridad de la Información.
- Reducir los riesgos de confidencialidad, autenticidad o integridad de la información mediante la ayuda de técnicas criptográficas.
- Definir métodos criptográficos de protección de la información crítica o sensible.

3. CONTEXTO O ÁMBITO DE APLICACIÓN

La Política de controles criptográficos 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.10	Dominio: Criptografía
A.10.01.01	Política sobre el uso de controles criptográficos
A.10.01.02	Gestión de claves

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	(5) Subsidios e iniciativas de inversión para	Transporte Público Regional.

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.	la operación y fortalecimiento de los Servicios de Transporte Público.	

4. ROLES Y RESPONSABILIDADES

- **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.
- **El Jefe de la División de Gestión, Tecnologías y Procesos**
  - responsable de la asignación de recursos necesarios tanto de personal como de las herramientas y/o licencias de software necesarias para asegurar la confidencialidad de los activos de información tecnológicos catalogados riesgosos.
- **El Encargado de la Unidad de TIC**
  - responsable de la asignación de funciones al personal de su unidad con el objetivo de asegurar la confidencialidad de los activos de información catalogados riesgosos.
- **El Encargado de Proyectos de la Unidad de TIC**
  - Responsable de velar por que se lleven a cabo los análisis de riesgo de los sistemas de información en operación y en etapas de evaluación, diseño, pruebas e implantación y de la correcta implementación de los métodos de encriptación definidos para su debido resguardo.

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 de controles criptográficos del Sistema de Seguridad de la Información, en tópicos de:

- Requerimientos criptográficos
- Uso de controles criptográficos.
- Gestión de claves criptográficas.

7. LINEAMIENTOS DE CONTROLES CRIPTOGRÁFICOS

7.1 Requerimientos criptográficos

La Subsecretaría velará por la implementación y proponer una postura institucional que regule el uso de controles criptográficos para la protección de la información, sobre su uso, su protección y el ciclo de vida de las claves criptográficas.

Además, procurará que para los nuevos o sistema de información o en su defecto, nuevas versiones de estos, exista una identificación de datos sensibles, y determinará los requerimientos de resguardo y mecanismos de encriptación tanto para su almacenamiento, transporte, validación y control de acceso.

7.2 Protección de claves criptográficas

En caso de requerirse encriptación, se proporcionará una protección adecuada al equipamiento utilizado para generar, almacenar y archivar sus claves privadas, considerándolo crítico o de alto riesgo.

7.3 Protección y uso de firmas digitales avanzadas

Los certificados digitales avanzados se deberán almacenar en equipamiento especializado del tipo HSM (Hardware Security Module).

El acceso físico y lógico al equipo HSM, el enrolamiento de firmas en el mismo y la definición de las entidades firmadoras y su correspondiente firma digital en el Módulo Firmador, se encuentra resguardado por el Encargado Infraestructura de la Unidad de TIC.

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.

Las siguientes son definiciones necesarias para la comprensión de la presente política.

- **Criptografía**: La palabra criptografía proviene del griego "criptos" que significa "oculto" y "grafe" de escritura que alude textualmente a la "escritura oculta". La

criptografía es la ciencia que resguarda documentos y datos que actúa a través del uso de las cifras o códigos para escribir algo secreto en documentos y datos que se aplica a la información que circulan en las redes locales o en internet.

13. HISTORIAL Y CONTROL DE VERSIONES

N° de Versión	Fecha de Aprobación	Resumen de las Modificaciones	Páginas Modificadas	Autor
1	07/2015	Elaboración inicial	Todas	LFV
2	10/2017	Actualización de formato y contenidos según requerimientos PG-SSi 2017.	Todas	RM