POLÍTICA DE SEGURIDAD
EN LA GESTIÓN CON PROVEEDORES

Pol-SSI-15 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		27/12/2017
	Mireille Caldichoury	Coordinación de Personas		27/12/2017
	Juan Gregorio Flores	Departamento de Contabilidad, Presupuesto y Tesorería		
	Patricio Santidrian	División Legal		27/12/2017
	Patricio Echenique	Encargado Unidad de Planificación y Control de Gestión		27/12/2017
	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 en temas de protección de la seguridad de la información en la gestión con proveedores de la Institución.

2. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos generales de la Política de Seguridad en la Gestión de Proveedores, son:

- Cumplir con la Norma Chilena Oficial NCh-ISO 27001:2013.
- Cumplir con la Política General de Seguridad de la Información.
- Implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros.
- Gestionar la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados de manera segura para satisfacer todos los requerimientos acordados con terceros.

3. CONTEXTO O ÁMBITO DE APLICACIÓN

La Política de Seguridad en la Gestión de Proveedores se aplica a todo Funcionario que le corresponda establecer acuerdos con proveedores, que tengan acceso a los sistemas y/o activos de información de la Institución. Para efectos de esta política, el término "proveedores", incluye proveedores de servicios, recursos humanos externos contratados, y consultores externos.

Internamente puede involucrar 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.15	Dominio: Relaciones con el proveedor
A.15.01.01	Política de seguridad de la información para las relaciones con el proveedor
A.15.01.02	Abordar la seguridad dentro de los acuerdos del proveedor
A.15.01.03	Cadena de suministro de tecnologías de la información y comunicaciones
A.15.02.01	Supervisión y revisión de los servicios del proveedor
A.15.02.02	Gestión de cambios a los servicios del proveedor

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 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.

- **Encargado de Unidad TIC**
  - Cuando corresponda en la formulación de la solicitud de servicios externos deben incorporar los requisitos de seguridad asociados al proceso que se pueden ver afectados. Posteriormente, en el desarrollo de la prestación del servicio debe velar por el cumplimiento de las cláusulas asociadas a materias de seguridad de la información.

- **Jefes de División**
  - En la formulación de la solicitud de servicios externos deben incorporar los requisitos de seguridad asociados al proceso que se pueden ver afectados. Posteriormente, en

el desarrollo de la prestación del servicio debe velar por el cumplimiento de las cláusulas asociadas a materias de seguridad de la información.

- **Unidad de Compras y Contrataciones**
  - En la revisión de los requerimientos de compra y posterior elaboración de contrato debe velar porque los requisitos de seguridad se encuentren explicitados en la documentación, además de notificar al proveedor.

- **Auditoría Interna**
  - En la revisión de los requerimientos de compra y posterior elaboración de contrato debe velar porque los requisitos de seguridad se encuentren explicitados en la documentación.

- **Proveedores**
  - Conocer las políticas de seguridad de la información y sus procedimientos asociados con respecto a terceros.

- **Unidad de Logística de DAF**
  - Cuando corresponda, coordinar los accesos al proveedor externo a las dependencias. Controlando el tiempo y vigencia del acceso.

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 Gestión de Proveedores del Sistema de Seguridad de la Información, en tópicos de:

- Lineamientos de seguridad de la información para las relaciones con el proveedor.
- Abordar la seguridad dentro de los acuerdos del proveedor.
- Cadena de suministro de tecnologías de la información y comunicaciones.
- Supervisión y revisión de los servicios del proveedor.
- Gestión de cambios a los servicios del proveedor.

7. LINEAMIENTOS

7.1 Lineamientos de seguridad de la información para las relaciones con el proveedor

- El personal externo que desarrolle trabajos para la Subsecretaría deberá cumplir con las políticas de seguridad institucionales.
- El Jefe de División y/o Unidad, cada vez que formule un requerimiento de contratación de servicio debe especificar los requisitos mínimos de seguridad cuando:
  - Durante el desarrollo del trabajo del proveedor deba tener acceso a recursos institucionales e información de procesos relevantes de la Subsecretaría
  - si corresponde, se debe definir y gestionar en el tiempo los accesos del proveedor externo a las dependencias necesarias para el servicio.
- El personal externo que tenga acceso a información deberá considerar que dicha información, por omisión, tiene el carácter de confidencial. Sólo se podrá considerar como información no confidencial aquella información a la que haya tenido acceso a través de los medios de difusión pública de información dispuestos para tal efecto
- Todos los proveedores de servicios que impliquen el acceso (tanto privilegiado como no privilegiado) a los sistemas de información de la Subsecretaría que se realicen mediante el uso de infraestructura TIC independientemente del lugar en el que se presten, deberán considerar las normativas de Seguridad de la Información de la Subsecretaría, particularmente en cuanto a los controles y cuidados con el acceso lógico y al procedimiento de gestión de incidentes.

7.2 Abordar la seguridad dentro de los acuerdos del proveedor

- Los proveedores sólo podrán desarrollar las actividades cubiertas bajo el correspondiente contrato de prestación de servicios, acuerdo complementario, acuerdo de confidencialidad u otro documento que formalice la prestación del servicio, estableciendo los niveles de servicio previamente acordados, estableciendo los principios de propiedad intelectual y el uso adecuado de los recursos de la Institución, especialmente en lo referido a los controles de acceso físico y lógico
- Cualquier tipo de intercambio de información que se produzca con la empresa proveedora se entenderá que ha sido realizado dentro del marco establecido por el

contrato de prestación de servicios, acuerdo complementario, acuerdo de confidencialidad u otro documento que formalice la prestación del servicio, de modo que dicha información no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados a dicho documento.

7.3 Cadena de suministro de tecnologías de la información y comunicaciones

- Los acuerdos con los proveedores deben incluir en sus requisitos los controles de mitigación que permitan abordar los riesgos de seguridad de la información, asociados a la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.

7.4 Supervisión y revisión de los servicios del proveedor

- Los servicios contratados a proveedores deben ser monitoreados, revisados y auditados en su cumplimiento, pudiendo existir sanciones por incumplimientos, previamente acordadas por contrato, acuerdo complementario o bases de licitación de convenio marco.
- Se debe establecer la periodicidad de tales revisiones.

7.5 Gestión de cambios a los servicios del proveedor

- Se deben administrar los cambios en la provisión de servicios que realizan los proveedores haciendo mantención y ajustes a las políticas de seguridad de la información relacionadas, los instructivos y controles específicos, referidos al tenor del servicio otorgado.
- Se debería, en tales casos, ponderar la criticidad de la información afectada, así como los sistemas y procesos involucrados para determinar la necesidad de un proceso de reevaluación de riesgos.
- La empresa proveedora proporcionará los nombres de las personas, las funciones y responsabilidades asociados al servicio provisto, e informará de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación. Estas designaciones podrían ser sometidas a verificaciones de antecedentes y pueden ser vetadas por la Subsecretaría, sin explicación alguna, requiriendo del cambio de la persona.

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	12/2017	Elaboración inicial	Todas	RM