POLÍTICA DE SEGURIDAD EN LA OPERACIÓN Y ADMINISTRACIÓN DE SISTEMAS

Pol-SSI-12 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 de seguridad necesarios en temas de Operación y Administración de plataformas tecnológicas y sistemas de información.

2. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos generales de la Política de Seguridad de Operación y Administración de Sistemas, son:

- Cumplir con la Norma Chilena Oficial NCh-ISO 27001:2013.
- Cumplir con la Política General de Seguridad de la Información.
- Asegurar la correcta operación, administración y funcionamiento de los sistemas de procesamiento de la información y plataformas tecnológicas de soporte.

3. CONTEXTO O ÁMBITO DE APLICACIÓN

La Política de Seguridad en la Operación y Administración de Sistemas 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.12	Dominio: Seguridad de las operaciones
A.12.01.01	Procedimientos de operación documentados
A.12.01.02	Gestión de cambios
A.12.01.03	Gestión de la capacidad
A.12.01.04	Separación de los ambientes de desarrollo, prueba y operacionales
A.12.02.01	Controles contra códigos maliciosos
A.12.03.01	Respaldo de la información
A.12.04.01	Registro de evento
A.12.04.02	Protección de la información de registros
A.12.04.03	Registros del administrador y el operador
A.12.04.04	Sincronización de relojes
A.12.05.01	Instalación del software en sistemas operacionales
A.12.06.01	Gestión de las vulnerabilidades técnicas
A.12.06.02	Restricciones sobre la instalación de software
A.12.07.01	Controles de auditoría de sistemas de información

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.

- **El Jefe de La División de Gestión, Tecnología y Procesos**
  - Es responsable de dar seguimiento a todas las implementaciones de la presente política.

- **El Encargado de la Unidad de TIC**
  - Es responsable de autorizar, gestionar y controlar las implementaciones de la presente política.

- **El Encargado de Infraestructura Tecnológica**
  - Es responsable de mantener actualizados todos los procedimientos e instructivos que le competen de la presente política.

- **Encargado de Proyectos de la Unidad TIC**
  - Es responsable de la generación de los procedimientos para el control del software en producción, control de las vulnerabilidades técnicas, separación de los ambientes de desarrollo, prueba y producción.

- Además, debe asegurar que cada etapa de proyecto considere la generación y actualización de la correspondiente documentación, particularmente las consideraciones de Seguridad de la Información.

- **El Encargado de Servicios de la Unidad TIC**
  - Es responsable de apoyar e impulsar la implementación de los procedimientos sobre las operaciones de infraestructura de TIC y revisar el registro de incidentes que permita dar respuesta oportuna a los usuarios que reporten problemas.

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 Seguridad en la Operación y Administración de Sistemas, en tópicos de:

- Procedimientos de operación documentados.
- Gestión de cambios.
- Gestión de la capacidad.

- Separación de los ambientes de desarrollo, prueba y operacionales.
- Controles contra códigos maliciosos.
- Respaldo de la información.
- Registro de evento.
- Protección de la información de registros.
- Registros del administrador y el operador.
- Sincronización de relojes.
- Instalación del software en sistemas operacionales.
- Gestión de las vulnerabilidades técnicas.
- Restricciones sobre la instalación de software.
- Controles de auditoría de sistemas de información.

7. LINEAMIENTOS DE SEGURIDAD EN LA OPERACIÓN Y ADMINISTRACIÓN DE SISTEMAS

7.1 Procedimientos de producción documentados

- Se debe documentar y actualizar regularmente los instructivos y procedimientos de las actividades en producción. Estos deben estar a disposición de todos los funcionarios de la Unidad de TIC que los necesiten.

7.2 Gestión de cambios en el Ambiente de producción.

Todo cambio a realizar en el ambiente de producción deberá contar con toda la documentación exigida en el respectivo instructivo o procedimiento.

7.3 Gestión de la capacidad de la Infraestructura

Se debe supervisar y adaptar el uso de los recursos y se deben hacer proyecciones de los futuros requisitos de capacidad tecnológica para asegurar el desempeño requerido de los sistemas de información:

- Los requisitos de utilización de recursos de hardware de cada sistema de información deben estar descrito en la documentación del respectivo sistema, considerando la criticidad para el negocio de cada sistema involucrado.
- Los sistemas de información deberán ser monitoreados para garantizar y mejorar la disponibilidad y la eficiencia de los sistemas.
- Las proyecciones sobre los requisitos futuros de capacidad deben considerar los nuevos requisitos del negocio y de los sistemas respecto al procesamiento de información de la organización.
- Se debe considerar un plan de administración de capacidad documentado para los sistemas críticos que están descritos en el plan de continuidad del negocio.

7.4 Separación de los ambientes de desarrollo, prueba y producción

- Se debe definir y documentar un procedimiento o instructivo de paso a producción, que detalle las reglas de transferencia de software desde un estado de desarrollo al productivo.
- Se deben probar los cambios a los sistemas y aplicaciones en un entorno de pruebas o etapas antes de aplicarlos a los sistemas que están en producción.

7.8 Protección de Registro de Eventos de Seguridad

- Se deberá proteger contra posibles alteraciones y accesos no autorizados la información de los registros de eventos.
- Dichos registros deben poder utilizarse para consultas posteriores o auditorías.

7.9 Registros del administrador y operador

- Las actividades del administrador y del operador del sistema se deberán registrar y los registros se deberían proteger y revisar de manera regular.
- Se debe utilizar un sistema de detección de intrusión (IDS) que se administre fuera del control de los administradores del sistema y de la red para monitorear el cumplimiento de las actividades de administración de redes.

7.10 Sincronización de relojes

- Se debe mantener sincronizado los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la Subsecretaría de Transportes o de un dominio de seguridad con una fuente de tiempo de referencia única.

7.11 Control de instalación de software en entorno operacional

Se debe implementar los procedimientos para controlar la instalación de software en los sistemas en producción, considerando a lo menos:

a) La actualización del software en producción, las aplicaciones, y las bibliotecas de programas deben ser realizadas solo por administradores experimentados y con la debida autorización por parte del Encargado de Infraestructura.

b) Los sistemas en producción solo deben contener código ejecutable aprobado por el Coordinador del Área de Proyectos, y no código en desarrollo ni compiladores.

c) Cada sistema en producción debe tener documentado en los procedimientos de implementación, la lista de archivos y carpetas que serán pasados al ambiente de producción.

d) Las aplicaciones y el software en producción deben ser implementados después de realizar las pruebas pertinentes.

7.12 Control de las vulnerabilidades técnicas

El Personal de Infraestructura debe tener conocimiento de las vulnerabilidades técnicas de los sistemas de información de manera preventiva e informar al Encargado de Seguridad de la Información y al Encargado de la Unidad de TIC. La exposición a esas vulnerabilidades se debe evaluar y se deben tomar las medidas correspondientes para minimizar el riesgo asociado, considerando lo siguiente:

a) Mantener un inventario de activos de información debidamente actualizado y vigente. es la base para la gestión eficaz de las vulnerabilidades técnicas.

b) Se deben documentar todos contactos técnicos con la información necesaria para apoyar la gestión de vulnerabilidades técnicas, las que incluyen a proveedores de software, números de versión y las personas responsables por el software.

c) Se debe documentar un instructivo para responder a las vulnerabilidades técnicas encontradas en la gestión de riesgos del inventario de activos de información.

7.13 Restricción sobre la instalación de software por parte de usuarios

- Sólo personal autorizado de la Unidad de TIC puede instalar software en las estaciones de trabajo de los usuarios.

7.14 Controles de auditoría de sistemas de información

- Las auditorías a los sistemas de información deben ser acordadas con la Unidad de TIC previamente a su ejecución, y el alcance debe ser acordado y controlado.
- Las pruebas de auditoría deben limitarse al acceso de sólo lectura al software y los datos.
- Las pruebas de auditoría que, de acuerdo al análisis previo, puedan afectar a la disponibilidad de los sistemas de información, se deben ejecutar fuera de horas de oficina.
- Todos los accesos en las pruebas de auditoría deben ser monitoreados y con los registros de eventos debidamente habilitados y configurados para producir un rastro de referencia.

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.

- **Clúster**: Corresponde a un conjunto de computadores que están unidos entre ellos comportándose como si fuesen un solo equipo.
- **ID de usuario**: Se refiere al identificador único de un usuario.
- **IDS**: Sistema de Detección de Intrusos (en inglés - Intrusion Detection System).
- **Malware**: Es la abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.
- **Networking**: Concepto utilizado para referirse a actividades de configuración y administración redes informáticas, switch, routers y relacionados.
- **Registro (Log)**: Cada elemento de un sistema de información genera una serie de registros de eventos del tipo "Error", "Advertencia" e "Información".
- **Sistema de Información**: Un sistema de información (SI) es un conjunto de elementos de Hardware y Software orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior. Todos estos elementos interactúan para procesar los datos (incluidos los procesos manuales y automáticos) y dan lugar a información más elaborada.
- **Storage**: Corresponde al lugar físico donde se almacena la información.

13. HISTORIAL Y CONTROL DE VERSIONES

N° de Versión	Fecha de Aprobación	Resumen de las Modificaciones	Páginas Modificadas	Autor
1	07/2016	Elaboración inicial. Lineamientos a controles NCh-ISO 27001:2013	0	07/07/2016
2	10/2017	Actualización de formato y contenidos según requerimientos PG-SSi 2017.	Todas	RM