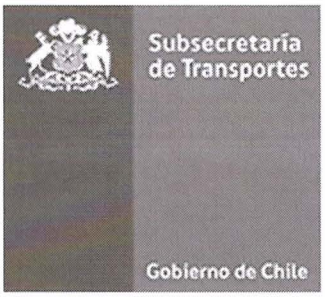
POLÍTICA DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

Pol-SSI-14 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.

Esta política define los lineamientos estratégicos para la Seguridad de la información en los Sistemas de Información, para todas sus modalidades de Desarrollo, Adquisición y mantención.

Los criterios de seguridad deben estar presentes en los desarrollos tanto internos como externos de la Institución, considerándolas en cada una de las etapas de desarrollo incluyendo las etapas de diseño, desarrollo, testing, marcha blanca de producción y producción.

2. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos generales de la Política de Seguridad en los Sistemas de Información son:

- Cumplir con la Norma Chilena Oficial NCh-ISO 27001:2013.
- Cumplir con la Política General de Seguridad de la Información.
- Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información.

3. CONTEXTO O ÁMBITO DE APLICACIÓN

La Política de Seguridad en los Sistemas de 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.14	**Dominio: Adquisición, desarrollo y mantenimiento del sistema**
A.14.01.01	Análisis y especificación de requisitos de seguridad de la información
A.14.01.02	Aseguramiento de servicios de aplicación en redes públicas
A.14.01.03	Protección de las transacciones de servicios de aplicación
A.14.02.01	Política de desarrollo seguro
A.14.02.02	Procedimientos de control de cambios
A.14.02.03	Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación
A.14.02.04	Restricciones en los cambios a los paquetes de software
A.14.02.05	Principios de ingeniería de sistema seguro
A.14.02.06	Entorno de desarrollo seguro
A.14.02.07	Desarrollo tercerizado
A.14.02.08	Prueba de seguridad del sistema
A.14.02.09	Prueba de aprobación del sistema
A.14.03.01	Protección de datos de prueba

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.
  - Además, para efectos de la presente política, deberá definir la lista de sistemas de información clasificados como "críticos" para la Subsecretaría y sus programas.

    Los sistemas clasificados como críticos, pueden ser de desarrollo o empaquetados.

- **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 Encargado de la Unidad de TIC**
  - Es responsable de coordinar la creación de los procedimientos e instructivos correspondientes y de que se cumplan los respectivos requisitos de esta política.

- **Área de Proyectos TIC.**
  - Cumplir con las disposiciones de esta política para todo sistema desarrollado para la Subsecretaría.
  - Mantener vigente conjunto de estándares de diseño que consideran aspectos de seguridad para los nuevos sistemas.

- **Encargado del área de Proyectos de la Unidad de TIC.**
  - Autorizar, validar y documentar los requerimientos funcionales y de seguridad.
  - Tanto para desarrollos externos como consultores, vela por el cumplimiento de los hitos comprometidos.

- **Jefe de Proyectos**
  - Coordina los proyectos desarrollados por el área y los desarrollados por terceros (externos).
  - Recibe levantamiento de los requerimientos del negocio realizados por el analista.
    - Controla y da seguimiento al proyecto en las etapas de desarrollo.
    - Entrega el sistema implementado al usuario solicitante junto al manual de uso respectivo
    - Concluye el proceso con la verificación del usuario solicitante.

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 los Sistemas de Información, en tópicos de:

- Lineamientos generales de seguridad en los Sistemas de Información
- Sistemas Críticos
- Análisis de problemática y evaluación de factibilidad.
- Especificación levantamiento de requerimientos.
- Diseño de proyecto.
- Desarrollo y testing.
- Producción y marcha blanca.
- Adquisición de Sistemas a Terceros.
- Separación de Ambientes y entorno de desarrollo seguro
- Aseguramiento de servicios de aplicación en redes públicas
- Protección de las transacciones de servicios de aplicación
- Procedimientos de control de cambios
- Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación
- Restricciones en los cambios a los paquetes de software
- Principios de ingeniería de sistema seguro
- Prueba de seguridad del sistema
- Prueba de aprobación del sistema
- Protección de datos de prueba

7. LINEAMIENTOS DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN

7.1 Lineamientos generales para los Sistemas de Información

- Se deben establecer y aplicar reglas para el desarrollo de software y sistemas de la Institución.
- Los lineamientos de seguridad de la información deben ser incluidos en los requisitos para los sistemas de información nuevos o las mejoras para los sistemas de información existentes.
- Se deben definir y estandarizar los criterios de seguridad y de calidad a ser considerados durante cada fase del ciclo de desarrollo de los sistemas.
- Todo sistema desarrollado en la Institución debe cumplir con las disposiciones de esta política.
- En el contexto de esta política, se define sistemas críticos como aquellos componentes de software desarrollados interna o externamente, que administran datos sensibles de Institución.
- El desarrollo de trabajo externo debe seguir las mismas etapas definidas en este documento.

7.2 Sistemas Críticos

El Encargado de la Unidad de TIC debe elaborar y mantener una lista de Sistemas de Información y proponer al Comité de Seguridad de la Información una lista acotada de sistemas clasificados como críticos. El Comité (CSI) podrá modificar dicha lista y finalmente aprobarla.

7.3 Análisis de problemática y evaluación de factibilidad.

- Como parte de la fase de evaluación se debe clarificar la problemática actual referida a la seguridad de la información, que debe ser cubierta por el nuevo sistema.
- En el estudio de factibilidad, se debe considerar el aspecto de seguridad, en cuanto al nivel de criticidad del sistema y de los controles que se debieran predefinir.
- La información relacionada a servicios de aplicación que pasan por redes públicas debe ser protegida de la actividad fraudulenta, disputas contractuales, y su divulgación o modificación no autorizada.

7.4 Especificación levantamiento de requerimientos.

- El diseño e implantación de los sistemas de información que sustentan los procesos de negocio pueden ser cruciales para la seguridad, por tanto, los requisitos de seguridad deberían ser identificados y consensuados previamente a su desarrollo y/o implantación.
- Se deben recolectar los requerimientos de los usuarios para realizar el documento inicial para el desarrollo de este. En esta etapa es indispensable la participación del jefe de proyecto y usuario solicitante.
- Los requerimientos son autorizados formalmente por el Encargado de Proyectos de la Unidad de TIC.

7.5 Diseño de proyecto.

- En el diseño de un proyecto, se deben considerar aspectos de seguridad para el diseño de la presentación, el diseño de arquitectura, el diseño de Base de datos y la lógica del sistema.
- El Encargado de Proyectos coordinará la participación del Jefe de proyecto, del que realizará la mantención de la base de datos y del que realiza la labor de entregar soporte de las aplicaciones para realizar los aportes necesarios para realizar el proyecto, este debe ser finalizado con el levantamiento final de los requerimientos que debe quedar formalizado.

7.6 Desarrollo y testing.

- Existe prohibición de:
  - Escribir o modificar código auto-copiante o cualquier otro tipo de código malicioso (virus y gusanos) usando infraestructura de la institución.
  - Incluir funciones u operaciones no documentadas o no autorizadas en los programas.
  - Modificar programas sin que quede registrado o documentado el cambio.
- La generación de código fuente debe quedar en el repositorio correspondiente para tener la trazabilidad de las modificaciones.
- El acceso a código fuente de los distintos sistemas debe estar protegido para acceder solo con las contraseñas asignadas.
- Para consultores externos se le debe dar acceso al código solo en el periodo que dure el proyecto.
- La empresa externa que trabaje con códigos de sistemas críticos debe firmar una carta de confidencialidad.
- Debe existir un repositorio único y controlado de código fuente de la Institución.

- El desarrollo de los sistemas se realiza en un ambiente local, utilizando los datos de la base de datos de desarrollo.
- El Encargado de Servicios TIC es responsable de mantener los ambientes locales (estaciones de trabajo de desarrollo) libres de fuentes de virus, troyanos, gusanos y otros que pudieran comprometer el desarrollo.
- El desarrollo se basa en el documento de levantamiento de requerimiento.
- Las pruebas del sistema deben incluir:
  - pruebas de integración (instalación, almacenamiento, configuración, seguridad, recuperación ante errores),
  - pruebas funcionales
  - Pruebas de rendimiento.

  Los resultados de las pruebas deben quedar registrados, almacenados y respaldados.
- El control de acceso usado en el ambiente de testing debe ser tan estricto como el usado en el ambiente de producción.
- El usuario solicitante accede al ambiente de testing y solo tienen acceso a lectura de la información.
- Los sistemas críticos deben incluir la validación de los datos de entrada, para asegurar un correcto procesamiento.
- Los sistemas críticos deben incluir controles de validación de los datos de salida, para asegurar que el procesamiento ejecutado haya sido correcto.
- Los sistemas críticos que interactúen con otros deben incluir controles para asegurar la integridad de los mensajes intercambiados.

7.7 Producción y marcha blanca.

- El paso a producción del proyecto es autorizado por el usuario solicitante cuando termina el testing.
- Según el proyecto, se define el tiempo de la marcha blanca.
- Se deben revisar y auditar los controles de seguridad definidos en la etapa de diseño.
- El equipo de desarrollo debe revisar y auditar sus propios sistemas ("testing interno") antes de pasar a la etapa de pruebas formales.
- El equipo externo de pruebas ("testing externo"), debe revisar y auditar los controles de seguridad, según las especificaciones generadas en la etapa de diseño.
- Si hay modificaciones al proyecto se debe comenzar el ciclo nuevamente, comenzando con el levantamiento de requerimientos.
- Todo traspaso a producción se debe hacer durante períodos de baja carga de trabajo del usuario final del sistema, debidamente coordinados con el área dueña del sistema.

7.8 Separación de Ambientes

- Se debe mantener, al menos 3, entornos de trabajo: desarrollo, test y producción.
  - Separación de red: segmentos de red, distintos IP.
  - Separación de la base de datos.
  - Separación de roles. Los roles en los distintos ambientes
    - Desarrollo: Solo el equipo del Proyecto
    - Testing: contará con un Encargado de transferencia a testing designado por el Encargado de la Unidad de TIC.

  - Producción: El encargado de Infraestructura de la Unidad de TIC.
- A no ser que sea bajo circunstancias excepcionales y con la autorización escrita del usuario responsable, no se deberían realizar pruebas en los sistemas productivos.
- Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema no deberán estar accesibles desde los sistemas operacionales cuando no sea necesario.
- Los usuarios deben utilizar distintos perfiles de usuario para los sistemas operacionales y de prueba y se deberán mostrar menús para mostrar mensajes de identificación adecuados para reducir el riesgo de errores.
- Toda modificación de software crítico por parches o módulos adicionales, debe ser analizado previamente en los ambientes de desarrollo y prueba.
- Se debe planificar detalladamente las etapas de paso a producción, incluyendo respaldos, recursos, conjunto de pruebas pre y post-instalación, criterio de aceptación del cambio y un plan de vuelta atrás.

7.9 Adquisición de Sistemas a Terceros

- Se debe establecer un acuerdo previo y formal con instituciones o empresas externas, que resguarde la propiedad intelectual (de la Institución cuando sea un desarrollo tercerizado) y asegure los niveles de confidencialidad de la información manejada en el proyecto.
- Se debe diferenciar entre el encargado de establecer y autorizar los acuerdos con terceros, de los que deban auditar su cumplimiento.
- El proceso de adquisición del sistema debe ser formal y cumplir con las disposiciones de seguridad descritas en esta política.

7.10 Separación de Ambientes y entorno de desarrollo seguro.

- Un entorno de desarrollo seguro incluye a las personas, procesos y tecnologías asociadas con el desarrollo e integración de sistemas.
- Se deben establecer entornos de desarrollo seguro, considerando aspectos de riesgo y en parte, los siguientes elementos:
  - La sensibilidad de los datos que el sistema procesará, almacenará y transmitirá.
  - El grado de externalización y confiabilidad asociado al proyecto de desarrollo.
  - Control del acceso al entorno de desarrollo.
  - Control sobre el movimiento de datos desde y hacia el entorno.

7.11 Aseguramiento de servicios de aplicación en redes públicas.

La información relacionada a servicios de aplicación que pasan por redes públicas debe ser protegida de la actividad fraudulenta, disputas contractuales, y su divulgación o modificación no autorizada.

7.12 Protección de las transacciones de servicios de aplicación.

La información implicada en transacciones de servicio de aplicación se debe proteger para evitar la transmisión incompleta, la omisión de envío, la alteración no autorizada, la duplicación o repetición no autorizada del mensaje.

7.13 Procedimientos de control de cambios

En el ciclo de vida de desarrollo se deberían hacer uso de procedimientos formales de control de cambios.

7.14 Revisión técnica de los cambios en la plataforma de operación

Cuando se cambien las plataformas de operación, se deben revisar y poner a prueba las aplicaciones críticas del negocio para asegurar que no hay impacto adverso en las operaciones o en la seguridad de la organización.

7.15 Restricciones en los cambios a los paquetes de software

Se deberían evitar modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían controlar estrictamente.

7.16 Principios de ingeniería de sistema seguro

Se deben establecer, documentar, mantener y aplicar los principios para los sistemas seguros de ingeniería para todos los esfuerzos de implementación del sistema de información.

7.17 Pruebas de seguridad

Se deben efectuar pruebas de funcionalidad en aspectos seguridad del sistema durante la etapa del desarrollo. Además, se debe establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones.

7.18 Protección de datos de prueba

- Los datos de pruebas se deben seleccionar cuidadosamente, proteger y controlar. El objetivo es garantizar la protección de los datos que se utilizan para procesos de pruebas.
- Se debe evitar la exposición de datos sensibles en entornos de prueba.
- Para proteger los datos de prueba se deberían establecer normas y procedimientos que contemplen prohibir el uso de bases de datos operativas.
- En caso contrario se deberían despersonalizar los datos antes de su uso y aplicar idénticos procedimientos de control de acceso que en la base de producción.

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