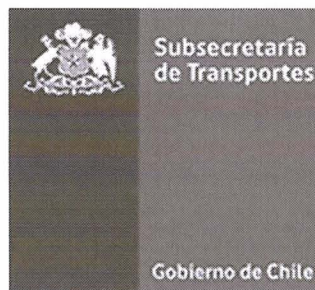


INSTRUCTIVO PARA LA GESTIÓN DE SEGURIDAD EN LOS SERVICIOS DE PROVEEDORES

INS-SSI-15.1 v1.0



SUBSECRETARÍA DE TRANSPORTES

Diciembre 2017

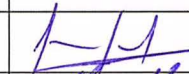

	Nombre	Cargo	Firma	Fecha
Aprobado por	Jaime Gonzalez	Encargado Unidad de TIC		19/12/2017
Elaborado por	Roy Mac Kenney	Encargado de Seguridad de la Información		19/12/2017



TABLA DE CONTENIDO

1. OBJETIVOS DEL INSTRUCTIVO	3
2. CONTEXTO O ÁMBITO DE APLICACIÓN.....	3
3. ROLES Y RESPONSABILIDADES	4
4. MATERIAS QUE ABORDA	4
5. MODO DE OPERACIÓN	4
5.1 CONSIDERACIONES DE SEGURIDAD EN LOS ACUERDOS CON PROVEEDORES	4
5.2 GESTIÓN DE CAMBIOS EN LOS SERVICIOS DE PROVEEDORES	5
6. REGISTROS DE OPERACIÓN Y/O LOGS.....	6
7. EXCEPCIONES AL CUMPLIMIENTO DE ESTE INSTRUCTIVO.....	6
8. GLOSARIO DE TÉRMINOS, DEFINICIONES Y SIGLAS	6
9. HISTORIAL Y CONTROL DE VERSIONES.....	6

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.



**INSTRUCTIVO PARA LA GESTIÓN DE SEGURIDAD
EN LOS SERVICIOS DE PROVEEDORES**

Versión: 1.0
Página: 3 de 6
Fecha: Diciembre 2017

1. OBJETIVOS DEL INSTRUCTIVO

Los objetivos generales del instructivo para la gestión de seguridad en los servicios de proveedores son:

- Cumplir con la Norma Chilena Oficial NCh-ISO 27001:2013.
- Cumplir con la Política General de Seguridad de la Información.
- Cumplir con la Política de Seguridad en la Gestión con Proveedores.
- Implementar y monitorear necesidades de ajustes en los controles de seguridad para la gestión de proveedores.

2. CONTEXTO O ÁMBITO DE APLICACIÓN

El instructivo para la gestión de seguridad en los servicios de proveedores 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 este instructivo 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.15.02.02	Gestión de cambios a los servicios del proveedor

En cuanto al ámbito institucional de aplicación de este instructivo, 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 la 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.

3. ROLES Y RESPONSABILIDADES

- **El Encargado de Seguridad de la Información (ESI)**

- Es responsable de la elaboración del presente instructivo, 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.

- **Contraloría o 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.

4. MATERIAS QUE ABORDA

El presente instructivo aborda aspectos de seguridad en el accionar para la Gestión de Proveedores del Sistema de Seguridad de la Información, en tópicos de:

- Consideraciones de Seguridad en los acuerdos con Proveedores.
- Gestión de cambios a los servicios del proveedor.

5. MODO DE OPERACIÓN

5.1 Consideraciones de Seguridad en los acuerdos con Proveedores

- Se deben integrar los lineamientos de Seguridad establecidos en la Política de Gestión de proveedores, lo que debe quedar consignado por escrito conforme a los formularios y documentos establecidos en el proceso de compras de bienes y servicios.
- Los siguientes aspectos de seguridad de la Información deben ser cubiertos o al menos analizados para su consideración en todo acuerdo con proveedores:
 - Se debe especificar los requisitos mínimos de seguridad a considerar en el desarrollo del trabajo del proveedor cuando éste tenga acceso a la red institucional, Sistemas, Servidores, Bases de Datos e Información de procesos relevantes de la Institución.
 - Declarar los procesos y procedimientos de seguridad que implementará la Subsecretaría para el servicio otorgado, así como también aquellos procesos y procedimientos que se requerirán al proveedor para que los implemente.
 - Previamente establecer los tipos de proveedores y contratos, versus el nivel de acceso que tendrán a la información más relevante de la institución, y cómo se monitoreará el cumplimiento de dichas restricciones.
 - Establecer procesos y ciclos de vida estandarizados para gestionar las relaciones con los proveedores.

- Establecer perfiles de riesgo de los proveedores, según su vinculación con la información más sensible de la institución.
- Controles de precisión y nivel de detalles para garantizar la integridad de la información o el procesamiento de información que entrega cualquiera de las partes
- Documentar el tipo de obligaciones y controles de seguridad aplicables a los proveedores para proteger la información, según su relación contractual con la institución.
- Establecer protocolos de gestión, coordinación y escalamientos frente a incidentes, contingencias y desastres, con los proveedores, incluidas las responsabilidades de la institución y sus proveedores.
- Resiliencia y, en caso de ser necesario, disposiciones de recuperación y contingencia para garantizar la disponibilidad de la información o el procesamiento de información proporcionado por cualquiera de las partes;
- Capacitación de concientización para el personal de la organización que interactúa con el personal de los proveedores en cuanto a las reglas adecuadas sobre el compromiso y el comportamiento en base al tipo de proveedor y el nivel de acceso del proveedor a los sistemas y la información de la organización;
- Las condiciones sobre los controles y requisitos de seguridad de la información se documentarán en un acuerdo firmado por ambas partes;
- Administración de las transiciones necesarias de información, instalaciones de procesamiento de información y cualquier otra cosa que se deba mover y, garantizando que se mantiene la seguridad de la información a través de todo el período de transición.
- Se deben firmar acuerdos de confidencialidad (NDA), nivel de servicio (SLA); protocolos de ajuste o modificación del servicio, condiciones excepcionales de término del acuerdo y sanciones o multas en casos de incumplimientos, con el fin de formalizar el ciclo de vida de la relación.

5.2 Gestión de cambios en los Servicios de Proveedores

- Se deberían administrar los cambios a la provisión de servicios de parte de los proveedores, considerando aspectos modificados como:
 - Condiciones de acuerdo con el proveedor.
 - Cambios realizados por la institución.
 - Desarrollo de cualquier nueva aplicación y sistemas.
 - Modificaciones o actualizaciones de las políticas, procedimientos o instructivos de la institución.
 - Ajustes en los controles para resolver incidentes de seguridad de la información y mejorar la seguridad.
 - Cambios en los servicios o condiciones de la relación del proveedor:
 - Cambios y mejoras en las redes.
 - Uso de nuevas tecnologías
 - Adopción de nuevos productos o nuevas versiones.
 - Nuevas herramientas y entornos de desarrollo.
 - Cambios en la ubicación física de las instalaciones de servicios.
 - Cambio de proveedores.
 - Subcontratación a otro proveedor.



INSTRUCTIVO PARA LA GESTIÓN DE SEGURIDAD EN LOS SERVICIOS DE PROVEEDORES

Versión: 1.0
Página: 6 de 6
Fecha: Diciembre 2017

6. REGISTROS DE OPERACIÓN Y/O LOGS

Son registros de operación de este Instructivo:

- Acuerdos de servicio que incluyan condiciones de seguridad de la información.
- NDA
- SLA

7. EXCEPCIONES AL CUMPLIMIENTO DE ESTE INSTRUCTIVO

Frente a casos de especiales, el Jefe de la Unidad de Informática de la Subsecretaría evaluará la situación y podrá establecer condiciones puntuales de excepción en el cumplimiento del presente instructivo, siempre que no infrinja las políticas internas existentes. Toda excepción debe ser documentada y monitoreada, generando un proceso de revisión del instructivo, para determinar si se deben efectuar actualizaciones en las condiciones de operación particular.

8. 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.

9. HISTORIAL Y CONTROL DE VERSIONES

Nº de Versión	Fecha de Aprobación	Resumen de las Modificaciones	Páginas Modificadas	Autor
1	12/2017	Elaboración inicial	Todas	RM