INSTRUCTIVO DE SEGURIDAD PARA ACCESO A TRAVÉS DE REDES Y ACCESO REMOTO

INS-SSI-09.2 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

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. OBJETIVOS DEL INSTRUCTIVO

El objetivo de este instructivo es establecer el modo de operación y las medidas de seguridad que permitan implementar el acceso seguro a la red de la Institución, incluyendo el acceso remoto, con el fin de proteger la información accesada, procesada o almacenada en los equipos.

- 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 Control de Acceso Lógico.

2. CONTEXTO O ÁMBITO DE APLICACIÓN

Este instructivo aplica a todo acceso a la red de la Institución, incluyendo el acceso remoto. En cuanto a los usuarios, 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.06	Dominio: Organización interna
A.06.02.02	Trabajo remoto
A.09	Dominio: Control de acceso
A.09.01.02	Accesos a las redes y a los servicios de la red
A.09.04.01	Restricción de acceso a la información
A.09.04.02	Procedimientos de inicio de sesión segura
A.09.04.03	Sistema de gestión de contraseñas
A.09.04.04	Uso de programas utilitarios privilegiados
A.09.04.05	Control de acceso al código fuente de los programas

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.	(5) Subsidios e iniciativas de inversión para la operación y fortalecimiento	Transporte Público Regional.

(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.	de los Servicios de Transporte Público.	

3. ROLES Y RESPONSABILIDADES

- **El Encargado de Seguridad de la Información (ESI)**
  - Es responsable de la elaboración y actualización del presente instructivo.
- **Encargado de la Unidad TIC.**
  - Responsable de implementar y mantener las herramientas de apoyo al soporte de usuarios remotos.
- **Jefaturas de áreas.**
  - Velar por el cumplimiento de este instructivo.

4. MATERIAS QUE ABORDA

El presente instructivo aborda actividades de la operación de TIC, considerando las materias de:

- Supuestos generales.
- Accesos a las redes y a los servicios de la red.
- Control de acceso al sistema y aplicaciones.
- Regulaciones generales de seguridad a redes y acceso remoto.
- Condiciones de las telecomunicaciones en acceso remoto.
- Condiciones de equipamiento y cuentas en acceso remoto.
- Uso de programas utilitarios privilegiados.

5. MODO DE OPERACIÓN

A continuación, se describen las actividades a considerar en este instructivo, mismas que buscan implementar los lineamientos de la Política de Control de Acceso Lógico. Cada una de estas actividades, debe quedar debidamente registradas, constituyendo los respectivos registros de operación.

5.1 Supuestos generales.

- La seguridad para el acceso a la información a través de las redes de la Institución, se encuentra regida por la política antes referenciada, siendo un requerimiento indispensable, la adecuada segregación de la red, manteniendo de esta forma, la separación de los distintos servicios y usuarios.

5.2 Accesos a las redes y a los servicios de la red.

- Los usuarios solo deben tener acceso directo a la red, a los sistemas y a los servicios de la red para los que han sido expresamente autorizados, de acuerdo al rol que ejercen en la Institución.

- Este acceso se debe efectuar mediante la solicitud y otorgamiento formal de una cuenta de usuario y su respectiva información de autentificación secreta.

5.3 Control de acceso al sistema y aplicaciones.

- El acceso a la información y a las funciones del sistema de aplicaciones, de acuerdo con la política de control de acceso.
- El acceso a los sistemas y aplicaciones debe estar controlado por el inicio de sesión seguro, en que el usuario de identifica y autentifica mediante una contraseña segura.
- El acceso al código fuente de los programas aplicativos debe estar protegido de accesos no autorizados.

5.4 Regulaciones generales para acceso remoto.

La Institución debe mantener estándares o modelos de seguridad a aplicar en el acceso remoto, considerando lo siguiente:

- Protocolo para la solicitud y autorización del trabajo remoto.
- Se debe firmar NDA (Acuerdo de Confidencialidad) y requerimientos entre las partes para contratos que requieran acceso remoto.
- Protocolo de seguridad para término del servicio que requiere acceso remoto.
- Se debe identificar el usuario que dispondrá de esta modalidad y los permisos de acceso remoto de que dispondrá.
- Protocolo de conexión remota de emergencia para atender requerimientos de soporte e incidencias puntuales.
- Normativas referentes al almacenamiento y recuperación de información institucional fuera de las instalaciones, ya sea en equipos corporativos, personales de funcionarios o dispositivos extraíbles.

5.5 Condiciones para el acceso remoto.

Para controlar el acceso remoto, se deben considerar:

- Toda conexión remota debe ser solicitada, autorizada y registra para posterior control de vigencia. Se evalúa el modelo de conexión, con el objetivo de discriminar el nivel de seguridad necesario a implementar en la conexión.
- Para ello, se utiliza el software definido como el estándar de conexión remota, salvo que el Encargado de la Unidad TIC, indique otro tipo de conexión.
- Los accesos remotos están sujetos a las fechas de inicio y finalización de cada proyecto comprometido por la Institución.
- Se debe utilizar método de conexión segura, con método de identificación y autenticación robusta, mediante AD.
- Las actividades efectuadas por los usuarios remotos deben ser registradas en los respectivos Logs.

5.6 Control, monitoreo y gestión.

- Estas conexiones remotas, deben ser monitoreadas en forma permanente mediante procesos definidos y revisadas periódicamente, en su vigencia.

5.7 Uso de programas utilitarios privilegiados.

- Aplicado a todo software capaz de sobrepasar o anular los controles normales de seguridad, por lo que se debe restringir y controlar su utilización.
- Aplicarán las siguientes consideraciones:

- Usar procedimientos robustos de Control de Acceso para la identificación, autenticación y autorización de los programas de utilidad privilegiado.
- Segregación del acceso de usuarios autorizados a los programas de utilidad privilegiada del software de aplicaciones.
- Limitación del uso de programas de utilidad privilegiada al número mínimo práctico de usuarios de la Unidad de TIC y autorizados;
- Autorización para programas de utilidad de altos privilegios, según cada caso.
- Limitación de la disponibilidad de programas de utilidad privilegiada, es decir, por la duración de un cambio autorizado.
- Registro de uso de los programas de utilidad privilegiada.
- Definición y documentación de los niveles de autorización para los programas de utilidad privilegiada.
- No se debe dejar programas de utilidad privilegiada disponibles a los usuarios que tienen acceso a las aplicaciones de los sistemas donde se requiere la segregación de deberes.

6. REGISTROS DE OPERACIÓN Y/O LOGS

Son registros de operación de este Instructivo:

- Acuerdos NDA para accesos remotos.
- Solicitudes para el acceso remoto.

7. EXCEPCIONES AL CUMPLIMIENTO A 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 SSI-MTT de la intranet institucional.

9. HISTORIAL Y CONTROL DE VERSIONES

N° de Versión	Fecha de Aprobación	Resumen de las Modificaciones	Páginas Modificadas	Autor
1	Dic/2017	Elaboración inicial	Todas	RM