POLÍTICA DE CONTROL DE ACCESO LÓGICO

Pol-SSI-09 v3.0

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 necesarios en temas de control de acceso lógico, postulando que todo usuario interno de la institución deberá poseer una cuenta de usuario personal, que actuará como una credencial que lo identifique unívocamente, y que le permitirá tener acceso a los recursos de la red corporativa de la Subsecretaría de Transportes.

Para todo sistema computacional de la organización, el usuario deberá señalar quién es (identificación), y luego deberá comprobar que es quien dice ser (autenticación) para recién autorizar sus acciones (autorización).

2. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos generales de la Política de Control de Acceso Lógico son:

- Cumplir con la Norma Chilena Oficial NCh-ISO 27001:2013.
- Cumplir con la Política General de Seguridad de la Información.
- Definir el acceso a los sistemas institucionales.
- Definir la composición que tienen las credenciales de acceso.
- Controlar el acceso a los Sistemas y a la Información de la Subsecretaría y sus Programas.
- Prevenir acceso no autorizado a los Sistemas de Información.
- Proteger adecuadamente la red y los servicios de red de la Institución.

3. CONTEXTO O ÁMBITO DE APLICACIÓN

La Política de Control de Acceso Lógico 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.09	Dominio: Control de Acceso
A.09.01.01	Política de control del acceso
A.09.01.02	Accesos a las redes y a los servicios de la red
A.09.02.01	Registro y cancelación de registro de usuario
A.09.02.02	Asignación de acceso de usuario
A.09.02.03	Gestión de derechos de acceso privilegiados
A.09.02.04	Gestión de información secreta de autenticación de usuarios
A.09.02.05	Revisión de los derechos de acceso de usuario

A.09.02.06	Eliminación o ajuste de los derechos de acceso
A.09.03.01	Uso de información de autenticación secreta
A.09.04.01	Restricción de acceso a la información
A.09.04.02	Procedimiento de inicio de sesión seguro
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 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 de seguridad.
- **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.

- **El Encargado Infraestructura Tecnológica**
  - Responsable de la implementación de accesos y contraseñas de acuerdo a las normas establecidas en la presente política. Además de establecer los controles necesarios de acceso a la red y a servicios de red.
- **Encargado de Servicios TIC**
  - Deberá verificar que los usuarios estén cumpliendo la presente política cuando sea necesario.
- **Todo usuario de activos tecnológicos**
  - Cumplir la presente política.

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 Control de Acceso Lógico del Sistema de Seguridad de la Información, en tópicos de:

- Lineamientos generales de control del acceso
- Accesos a las redes y a los servicios de la red
- Registro y cancelación de registro de usuario
- Gestión de asignación de acceso de usuarios
- Gestión de derechos de acceso privilegiados
- Gestión de información secreta de autenticación de usuarios
- Revisión de los derechos de acceso de usuario
- Eliminación o ajuste de los derechos de acceso
- Uso de información de autenticación secreta
- Restricción de acceso a la información
- Procedimiento de inicio de sesión seguro
- Sistema de gestión de contraseñas
- Uso de programas utilitarios privilegiados
- Control de acceso al código fuente de los programas.

7. LINEAMIENTOS DE CONTROL DE ACCESO LÓGICO

7.1 Lineamientos generales de control del acceso

- Las reglas de acceso a la red estarán basadas en el principio de Negación por Omisión: "todo está restringido, a menos que esté expresamente permitido".
- Las reglas específicas para el control de acceso, estarán documentadas a través de los diferentes procedimientos de control de acceso a los recursos tecnológicos correspondientes.
- Se establecerá, documentará y revisará los lineamientos de control de accesos en base a las necesidades de seguridad y de servicio de la institución.

7.2 Accesos a las redes y a los servicios de la red

- El acceso a redes desde y hacia afuera de la Institución cumplirá con los lineamientos de "Responsabilidad de los Usuarios" y adicionalmente se utilizarán métodos como autenticación de protocolo de enrutamiento, rutas estáticas, traducción de direcciones y listas de control de acceso.
- Se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán, al menos:
  - Controlar el acceso a los servicios de red tanto internos como externos.
  - Identificar las redes y servicios de red a los cuales se permite el acceso.
  - Establecer normas, controles y procedimientos de administración para proteger el acceso a la red de datos de la institución.

7.3 Registro y cancelación de registro de usuario

- Se mantendrán protocolos de registro (alta) y cancelación (baja) de usuarios con objeto de habilitar la asignación de derechos de acceso.

7.4 Gestión de asignación de acceso de usuarios

- Se deben establecer procedimientos que controlen la asignación y revocación de derechos de acceso o privilegios de acceso a los servicios y sistemas de la Subsecretaría de Transportes y sus Programas.
- Se establecerán los procedimientos de registro, modificación y borrado de usuario.

7.5 Gestión de derechos de acceso privilegiados

- La asignación y uso de derechos de acceso con privilegios especiales o de administrador, debe ser restringido y controlado, dado su alto riesgo en la continuidad operacional de las plataformas tecnológicas.

7.6 Gestión de información secreta de autenticación de usuarios

- La asignación de información confidencial, como parte de la autenticación del usuario, debe ser controlada mediante un proceso de gestión seguro y auditable.

7.7 Revisión de los derechos de acceso de usuario

- Los propietarios de los activos deben poder revisar los derechos de acceso asignados o en curso, de todos los usuarios de los sistemas o plataformas a su cargo.

7.8 Eliminación o ajuste de los derechos de acceso

- Se deben retirar los derechos de acceso a la información y a las instalaciones del procesamiento de información para todos los funcionarios, proveedores o usuarios de terceros, a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio.
- Al momento del cese de labores de un funcionario del área Tecnologías de Información se deberá modificar contraseñas de los equipos de producción y accesos remotos.

7.9 Uso contraseñas y de cualquier información de autenticación secreta

- Se exige a los usuarios el uso de las mejores prácticas de seguridad en el uso y protección de información confidencial de sus contraseñas e información adicional usada para la autenticación.

7.10 Restricción de acceso a la información

- Se debe controlar el acceso de los usuarios y personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, según rol y perfil de cada uno.

7.11 Procedimiento de inicio de sesión seguro

- Cuando sea requerido por la política de control de accesos se debe controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on.

7.12 Sistema de gestión de contraseñas

- Emplear un identificador formal de autenticación único, con una estructura definida y contraseñas configuradas con mayúsculas y minúsculas, con dígitos, y con al menos 8 caracteres.
- La contraseña asignada a una nueva cuenta de usuario, debe crearse expirada, de modo de obligar a ser cambiada por éste durante su primera conexión.
- Las contraseñas son confidenciales, personales e intransferibles y no deben ser enviadas por email, ni por ningún otro tipo de formulario electrónico.
- Las contraseñas de equipamiento y sistemas en producción se deben modificar cada tres meses.
- Las contraseñas de usuarios de la red corporativa caducan cada tres meses.
- Las contraseñas de Equipos y Sistemas en producción se deben almacenar en sobres cerrados, en un área segura, y se debe informar y copiar a la Jefatura respectiva.

7.13 Uso de programas utilitarios privilegiados

- Se debe restringir y controlar estrechamente el uso de los Software Utilitarios que poseen la capacidad de sobrepasar (anular o evitar) los controles de acceso a los sistemas y aplicaciones. Debe existir un procedimiento de identificación, autorización y autenticación para este tipo de Software, además, se debe asegurar que:
  - Exista una segregación entre los Sistemas en Producción y los softwares utilitarios
  - Existe un límite en el uso de softwares utilitarios a un número mínimo y práctico de funcionarios autorizados expresamente por el Encargado de la Unidad de TIC.
  - Debe existir una lista de los softwares de estas características permitidos en la Subsecretaría, a la que sólo el Encargado de Operaciones y Superiores pueden tener acceso.

7.14 Control de acceso al código fuente de los programas.

- Se debe restringir el acceso al código fuente de las aplicaciones software.

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.