INSTRUCTIVO DE GESTIÓN DE CUENTAS DE USUARIOS

INS-SSI-09.1 v1.0

SUBSECRETARÍA DE TRANSPORTES

Diciembre 2017

	Nombre	Cargo	Firma	Fecha
Aprobado por	Jaime Gonzalez	Encargado de Unidad de TIC		18/12/2017
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

Los objetivos generales del Instructivo de gestión de Incidentes y debilidades de Seguridad de la Información,

- 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.
- Definir el mecanismo de gestión de cuentas en el proceso de identificación y autenticación del control de acceso lógico a los sistemas institucionales.

2. CONTEXTO O ÁMBITO DE APLICACIÓN

Este instructivo para la Gestión de Cuentas de 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.09	Dominio: Control de 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.09.04.03	Sistema de gestión de contraseñas

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 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 del presente instructivo, de su actualización y velar por el cumplimiento de sus disposiciones.
- **El Encargado de la Unidad de TIC**
  - Es responsable de coordinar el cumplimiento del presente instructivo y de que se cumplan los requisitos de la política de Control de Acceso.
- **El Encargado Infraestructura Tecnológica**
  - Responsable de la implementación de accesos y contraseñas de acuerdo a las normas establecidas en la política de Control de Acceso. 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 el instructivo cuando sea necesario.
- **Todo usuario de activos tecnológicos**
  - Cumplir el presente instructivo.

4. MATERIAS QUE ABORDA

El presente instructivo aborda las actividades de Gestión de Cuentas de Usuarios, en tópicos de:

- Accesos a las redes y a los servicios de la red.
- Gestión de cuentas y derechos de acceso.
- AMB (Alta, Modificación, Baja) de cuentas 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.
- Gestión de contraseñas y su sistema de control
- Restricción de acceso a la información.

5. MODO DE OPERACIÓN

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

- Implementando criterio de negación por omisión, los usuarios solo podrán acceder a la red de la institución y con ello a los servicios de red, si cuentan con autorización específica.

- Para la gestión de acceso a las redes y sus servicios, se debe mantener
  - Repositorio central que mapea roles o grupos y las redes y los servicios de red a los que se tiene derecho de acceso.
  - Instructivo de autorización para determinar a quién se le permite acceder a qué redes y servicios con redes.
  - Controles y procedimientos de administración para proteger el acceso a las conexiones de red y a los servicios de red.
  - Catastro de los mecanismos alternativos y sus medios de control de seguridad, que se utilizan para acceder a las redes y a los servicios con redes. Considera, entre otros, VPN, red inalámbrica, acceso remoto a escritorios.
  - Monitoreo del uso de servicios de red.

5.2 Gestión de Cuentas y Privilegios

- Para el control de acceso a los sistemas de información se requiere verificar las siguientes reglas:
  - Todo acceso a equipos o sistemas sea con la identificación y autenticación del usuario que requiere.
  - Todo acceso a un sistema de información se encuentra prohibido, salvo que se autorice expresamente.
  - Ningún equipo o sistema debe quedar desatendido, exponiendo información sensible a personas no autorizadas.
- Active Directory es para la Subsecretaría de Transporte la plataforma para la asignación o revocación de derechos de acceso que se asignan a las cuentas de usuarios.
- En el protocolo de gestión de derechos, se debe considerar que:
  - Se debe autorizar los permisos de acceso por el propietario del sistema de información o servicio, consistente con la Política de Control de Acceso Lógico.
  - El uso de un único identificador de usuario.
  - La comprobación de que el usuario tiene autorización del propietario del sistema y de que el nivel de acceso concedido es adecuado.
  - La declaración y firma del usuario sobre la aceptación de sus derechos de acceso.
  - El mantenimiento de un registro formal de todas las personas registradas para el uso del servicio.
  - Los privilegios finales, se deben asignar una vez verificadas las condiciones y antecedentes estipulados para cada caso.
  - Verificar periódicamente
    - La correlación entre los derechos de acceso de los usuarios y la actualización de sus roles, contratos o cargo de trabajo.
    - Los derechos de acceso con los propietarios de los sistemas de información o servicios TI.

5.3 AMB de Cuentas de Usuarios

- Solicitud de AMB de cuenta:

- Coordinación de Personas solicita mediante mail a la mesa de ayuda.

  Los datos obligatorios para la AMB de cuenta son:

  - Nombre completo / Calidad funcionaria
  - RUT
  - Departamento de desempeño
  - Región - Cuando corresponde.
  - Fecha de Baja de la cuenta – Cuando corresponde.
  - Modificación solicitada – Cuando corresponde.

- Posteriormente, la jefatura directa del usuario solicita mediante mail a la mesa de ayuda.
  - Informa Cargo – Cuando corresponde.
  - Tipo de permiso en sistemas
  - Teléfono (Anexo)
  - Asignación de activos de información

- Procesar la solicitud:
  - El personal de la mesa de ayuda registra la solicitud en el Sistema de Gestión de Tickets y envía la solicitud al Encargado de Infraestructura, el cual valida que la información esté completa y según el tipo de cuenta se reenvía la solicitud al ingeniero de sistemas correspondiente.
- AMB Cuenta Active Directory (AD):
  - El ingeniero de sistemas correspondiente ejecuta la AMB de la cuenta solicitada.
  - En caso de creación completa los datos solicitados por la consola "Active Directory Users and Computers" a la unidad organizacional (OU) determinada por el departamento de desempeño del funcionario. Si la cuenta creada requiere de asociación de correo electrónico se debe ejecutar el protocolo de Configuración de cuentas de correo electrónico.
- AMB Cuenta de Acceso a Sistemas:
  - El ingeniero de sistemas correspondiente, en el servidor LDAP ejecuta la AMB de la cuenta.

5.4 Gestión de derechos de acceso privilegiados

- La gestión de cuentas con acceso de alto privilegio, debe considerar:
  - Mantener actualizado un listado de usuarios y su relación con cuentas de altos privilegios de los sistemas y plataformas más críticas.
  - Dichos accesos se deben asignar bajo una precisa necesidad de negocio, a usuarios capacitados y por un plazo definido y acotado.
  - Estos permisos se deben asignar en forma independiente de las cuentas normales que pueda requerir el mismo usuario, para otras funciones.

- Se debe auditar periódicamente la asignación, real necesidad y uso de las cuentas en curso.
- Se debe maximizar la protección de claves de acceso, especialmente frente a cambios de personal o rotación de funciones.

5.5 Protección de passwords e información secreta de autenticación de usuarios

- El debido cuidado de las claves de acceso o passwords utilizadas en los procesos de Control de Acceso, debe considerar:
  - Toda password inicial debe ser segura y ser entregada -a su vez- de manera segura y debe ser cambiada por el usuario en su primer uso.
  - No deben mantenerse passwords por omisión o de fabricante en los sistemas.
  - Todas las contraseñas de usuarios deben ser cambiadas cada 60 días como máximo.

5.6 Revisión de los derechos de acceso de usuario

- Se deben revisar periódicamente los derechos de acceso asignados, considerando los siguientes aspectos:
  - Los derechos de accesos se deben revisar a intervalos regulares y después de cualquier cambio de rol o empleo, donde se debiesen eliminar o reasignar.
  - Se debe garantizar que no se han obtenido privilegios superiores no autorizados.
  - Se debe monitorear los cambios a las cuentas más relevantes, en particular las con altos con privilegios para su revisión periódica.

5.7 Eliminación o ajuste de los derechos de acceso

- La gestión de eliminación o ajuste de los derechos de acceso, debe considerar:
  - Que se verifica la eliminación o bloqueo de los derechos de acceso de los usuarios que cambian de rol o abandonan la institución, tanto por acceso físicos como lógicos.
  - Se comprueba periódicamente la vigencia de las cuentas de usuarios en todo su ciclo de vida.
  - Dependiendo del caso, la eliminación o el ajuste puede integrar la eliminación, la revocación o el reemplazo de claves, tarjetas de identificación o suscripciones.
  - Se debe ajustar también la documentación que identifica la modificación de los derechos de acceso de los usuarios.

5.8 Gestión de contraseñas y su sistema de control

- Se usará Active Directory para la gestión cuentas y contraseñas de usuarios de la red de la Subsecretaría de Transporte, considerando:
  - Que el nivel de acceso para passwords y otras consultas son de uso estrictamente personal e intransferible.
  - El usuario es responsable de mantener actualizada la información confidencialidad de autenticación.

- Las passwords deben ser cambiadas de acuerdo al estándar de control de acceso lógico establecido por la Institución.

- Las contraseñas de dispositivos TI, podrían requerir algún tratamiento especial, las que serán administradas de acuerdo con las mejores prácticas definidas para la gestión de tales dispositivos, lo que debe quedar documentado.
- Se controlarán los intentos de acceso fallidos a los sistemas de información y/o equipos, así como también el intento de uso indebido de privilegios, siendo necesario bloquearlo ante la detección de estos hechos.
  - De producirse este bloqueo, se debe establecer como proceso obligatorio, el desbloqueo ante la petición e identificación positiva del usuario en cuestión, previo al análisis de la posible violación a la seguridad.

5.9 Restricción de acceso a la información

- Las restricciones al acceso se deberían basar en requisitos de aplicación de negocios individuales y de acuerdo con la política de control de acceso definida.
- Se debería considerar lo siguiente para poder apoyar los requisitos de restricción de acceso:
  - Proporcionar menús para controlar el acceso a las funciones del sistema de aplicación.
  - Controlar los datos a los que un usuario en particular puede acceder;
  - Controlar los derechos de acceso de los usuarios, es decir, de lectura, escritura, eliminación y ejecución;
  - Controlar los derechos de acceso de otras aplicaciones;
  - Limitar la información contenida en la producción;
  - Proporcionar controles de acceso físicos o lógicos para el aislamiento de aplicaciones sensibles, datos o sistemas de aplicación.

6. REGISTROS DE OPERACIÓN Y/O LOGS

Son registros de operación de este Instructivo:

- Mail a la mesa de ayuda con solicitudes AMD

7. EXCEPCIONES AL CUMPLIMIENTO DEL PRESENTE 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 procedimiento, siempre que no infrinja las políticas internas existentes. Toda excepción debe ser documentada y monitoreada, generando un proceso de revisión del procedimiento, 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

N° de Versión	Fecha de Aprobación	Resumen de las Modificaciones	Páginas Modificadas	Autor
0	11/2017	Creación	Todas	RM
1	12/2017	Creación	Todas	RM