Norma de uso
Identificación y autentificación de Sistemas Informáticos

1 INDICE

2 OBJETIVO

El acceso a la información de los sistemas del Gobierno Regional Metropolitano de Santiago será solo otorgado a usuarios identificados y autentificados. El Gobierno Regional Metropolitano de Santiago establecerá los procedimientos y controles para otorgar, cambiar y finalizar acceso a los sistemas de información.

Es importante mencionar que el uso inapropiado de los recursos dispuestos para los usuarios, expone a la institución a riesgos innecesarios como los virus informáticos, interrupción de las redes y sus sistemas, como también problemas jurídicos tanto nacionales como internacionales.

3 ALCANCE

Las normas mencionadas en el presente documento cubren el uso apropiado de los sistemas y los métodos de identificación y autentificación del Gobierno Regional Metropolitano de Santiago y aplica a todos los empleados, proveedores, contratistas, personal que esté vinculado con las firmas que presten servicios al Gobierno Regional Metropolitano de Santiago o que estén relacionados. Se incluye, además, todas las dependencias que son parte de la institución o que transite por la red del Gobierno Regional Metropolitano de Santiago

4 ROLES Y RESPONSABILIDADES

Los funcionarios deben comprender sus responsabilidades para salvaguardar los ID´s de identificación (nombre de usuario) y sus contraseñas. Deberá notificar inmediatamente a un supervisor, jefe directo o Departamento de Informática si sospechan que una contraseña u otro sistema credenciales han sido comprometidos.

Los usuarios tienen la obligación de no registrar los identificadores o contraseñas en papel.

Los usuarios no deben almacenar identificadores en un computador de manera desprotegida.

Es absoluta responsabilidad del usuario al terminar su jornada laboral o al no estar frente a su computador debe cerrar su sesión de usuario.

El usuario debe configurar su computador para el uso de protector de pantalla y que este solicite contraseña para iniciar sesión nuevamente.

Está absolutamente prohibido a los usuarios permitir que los sistemas recuerden las contraseñas o identificadores de sistemas. Tampoco deberán incluir el identificador en cualquier proceso de inicio de sesión automatizado. (Ej. Macros)

Los Jefes de Departamento y de Unidad se asegurarán de que su personal cumpla con todas las directrices que figuran en esta política, además notificaran sin demora al Departamento de Informática la Información de las cuentas que deben ser desactivadas, y deberán reportar cualquier sospecha o violaciones compromisos de las credenciales al Departamento de Informática.

El Encargado de seguridad de la información, implementará métodos de autenticación para los sistemas de información en su cuidado, instruyendo a los usuarios en cuanto a su uso.

El Departamento de Informática preparará directrices y normas para las credenciales de usuario, con accesos restringidos según su perfil y aprobará la emisión de las credenciales.

Los desarrolladores de sistemas deben garantizar que sus sistemas soportan los procedimientos y directrices especificadas en este documento normativo

5 CONTROL NORMATIVO

El siguiente procedimiento tiene por finalidad dar cumplimiento a los siguientes controles de la norma NCh-ISO27001.Of2013

Código del Control	Identificación del Control	Requisito de control
A.09.02.04	Gestión de información secreta de autenticación de usuarios	Se debe controlar la asignación de información de autenticación secreta mediante un proceso de gestión formal.
A.09.03.01	Uso de información de autenticación secreta	Se debe exigir a los usuarios el cumplimiento de las prácticas de la organización en el uso de la información de autenticación secreta.
A.09.04.03	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
A.12.01.01	Procedimientos de operación documentados	Los procedimientos de operación se deben documentar, y poner a disposición de todos los usuarios que los necesiten.

6 IDENTIFICACION Y AUTENTICACION

El método específico de autenticación para cada sistema deberá ser proporcional con el nivel de sensibilidad del sistema para tener acceso (es decir, mientras más sensibles sean los sistemas se deberá utilizar métodos de autenticación más fuerte). Varios métodos de autenticación (por ejemplo, uso de la contraseña) puede ser necesaria para la sensibilidad de alta - confidencialidad o de alto riesgo.

7 DEFINICION Y MODO DE OPERACION

7.1 Administración de la información de autenticación secreta

Para todos los sistemas de información, el Departamento de Informática del Gobierno Regional Metropolitano, creará claves de autenticación secreta mediante un proceso de administración formal, previa verificación de identidad, a través del cual se individualizará al usuario, el sistema , derechos de administración sobre el sistema, definiendo si es un usuario normal, uno avanzado o uno con niveles de administrador.

Las autenticaciones secretas temporales serán creadas por defecto en la instalación inicial del sistema, y será una clave estándar, la cual deberá ser cambiada cuando el usuario inicie su próxima sesión. El usuario deberá confirmar el ingreso de su autenticación secreta, digitando dos veces su nueva autentificación secreta. Una vez cambiada la autenticación secreta deberá ingresar con su nombre de usuario y su nueva clave para de esta manera verificar la identidad del usuario en el sistema. Una vez realizado esto, deberá firmar un documento que identifica el cambio de la clave estándar por su nueva autenticación secreta.

Con lo anteriormente descrito, el usuario ya estará en condiciones de acceder al sistema con su propia clave.

7.2 Uso de la información de autenticación

A los funcionarios, cualquiera sea su calidad jurídica, se les hará firmar un documento que declare que las claves son personales e intransferibles.
La clave deberá tener una longitud mínima, y no podrán basarse en nombres de hijos o familiares fáciles de adivinar. La clave deberá cambiarse si se sospecha que esta ha sido comprometida o vulnerada.

Las claves temporales deberán ser cambiadas en el primer inicio de sesión

7.3 Sistemas de administración de claves o contraseñas

Los usuarios deberán ser forzados al uso de claves secretas o contraseñas, de manera de mantener su información resguardada

El Departamento de Informática les permitirá a los usuarios cada cierto tiempo cambiar sus propias contraseñas, permitiéndoles confirmar las nuevas claves y evitar errores de digitación.

El sistema deberá mantener un registro para evitar claves o contraseñas utilizadas con anterioridad.

Todos estos procedimientos deberán quedar documentados y a disposición de los funcionarios en cualquier momento.

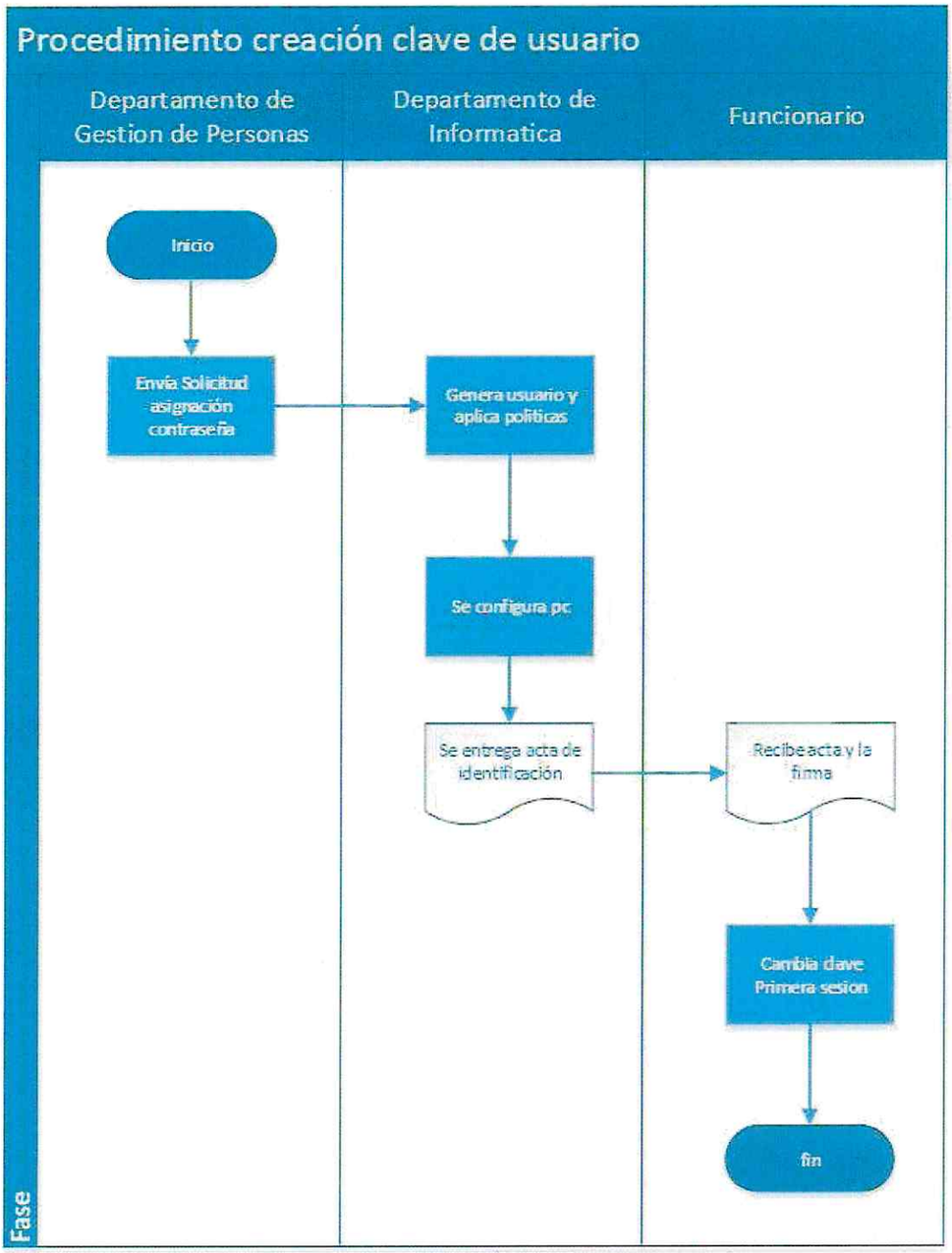
7.4 Solicitud de cambio de autentificación secreta

Para el cambio de clave de un funcionario cuando este no esté presente , o se vea imposibilitado de hacerlo personalmente, deberá ser solicitado por su jefatura directa mediante correo electrónico el que debe ser respaldado además con la solicitud formal del cambio de clave mediante el formulario Solicitud Cambio de Contraseña

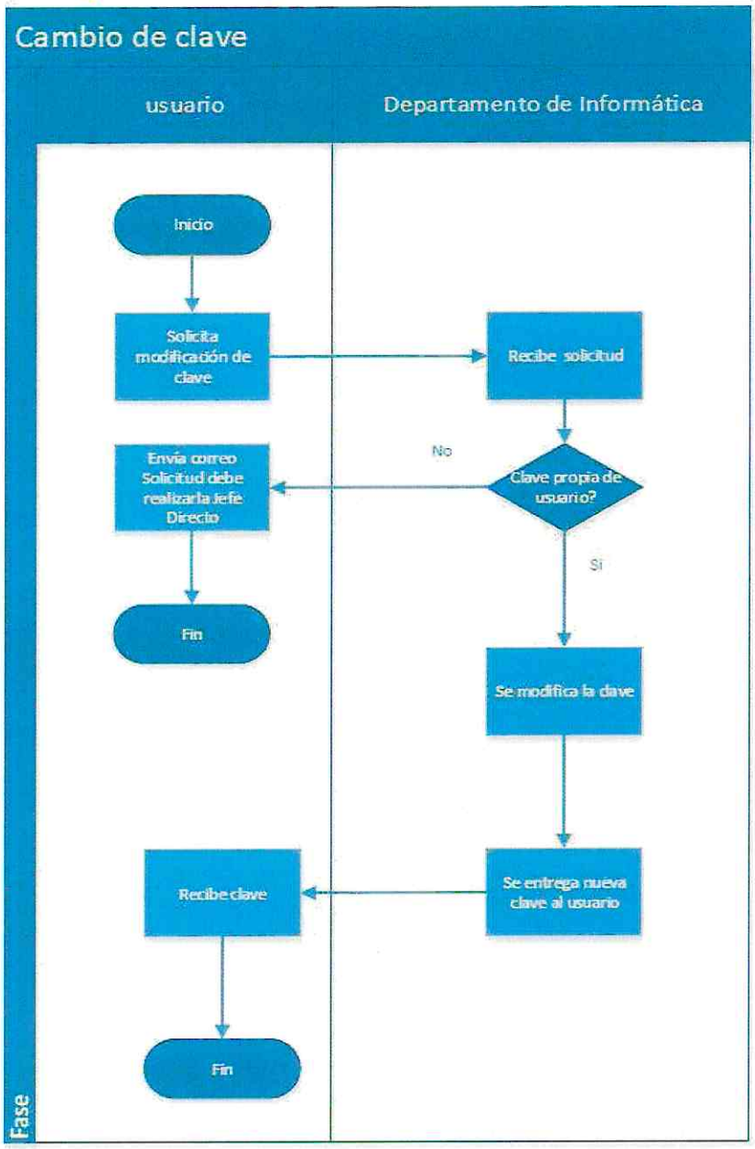
7.5 Procedimientos Documentados

Todos estos procedimientos, así como las demás Políticas, reglamentos, y normas deberán quedar documentados de manera electrónica en la Intranet del Servicio, quedando a disposición de todos los usuarios para cuando ellos lo requieran.

7.6 PROCEDIMIENTOS DE OPERACION PARA CREACION CLAVE DE USUARIO A TRAVES DE DIAGRAMAS DE FLUJOS



8 Procedimiento de operación para cambio de clave sistemas a traves de diagrama de flujos



9 REGISTROS DE OPERACION

El Departamento de Informática deberá emitir un informe que dé cuenta de las solicitudes recibidas para:

- A.09.02.04 Informe de creación y mantención de usuarios
- A.09.03.01 Informe de usuarios con recepción de clave secreta conforme
- A.09.04.03 Informe de cambio de claves al inicio de la primera sesión, haciendo hincapié en Sistema de gestión de claves de calidad
- A.12.01.01 Informe de publicación de procedimientos en Intranet

El informe deberá ser enviado al Encargado de Seguridad de manera anual.

En caso de no haber movimiento en relación a algún control que se pide informar, deberá reportarse de igual manera señalando que no hubo movimiento por lo que no se pudo demostrar con algún medio de verificación durante el respectivo periodo.

Todo documento deberá venir formalizado por quienes sean responsables del proceso (Debe contener logo del Servicio, fecha de creación, nombre, cargo y firma del responsable)

10 DIFUSIÓN

El presente documento será difundido a través de correo electrónico a todo el personal del Servicio, así como también una copia de éste será publicada en la intranet Institucional.

11 REVISIÓN

La siguiente Norma será revisada, evaluada y/o actualizada según corresponda una vez al año por el Comité de Seguridad de la Información o cuando el mismo estime conveniente, en cuanto a su funcionamiento y correcta aplicación en la Institución.

12 ANEXOS

12.1 Formulario de creación o cambio de autenticación secreta

DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

ACTA DE ENTREGA DE IDENTIFICACIÓN

Acta de entrega de Identificación

IDENTIFICACIÓN DE FUNCIONARIO

Nombre de Funcionario:_____ RUN:_____

Departamento:_____ Fecha de Entrega:__/__/_____

Nombre de Usuario:_____

Clave de acceso:_____

Mediante el presente la persona anteriormente individualizada toma conocimiento según lo establecido en la Política Gestión de Claves de este Gobierno Regional. Que deberá hacer cambio de la clave entregada en el siguiente inicio de sesión, que esta tendrá una duración de tres meses, que pasado este tiempo deberá crear nueva contraseña la cual no puede ser igual a las ultimas diez utilizadas, deberá ser alfanumérica, deberá tener una longitud mínima de ocho caracteres, deberá considerar el uso de mayúsculas y minúsculas, además de caracteres especiales.

_____
FIRMA FUNCIONARIO

12.2 Formulario solicitud cambio de contraseña

DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

SOLICITUD CAMBIO DE CONTRASEÑA

DATOS SOLICITANTE

Nombre de Funcionario:_____ RUN:_____

Departamento:_____ Fecha de Solicitud:__/__/_____

Mediante el presente la persona anteriormente individualizada, solicita al Departamento de Informática gestionar el cambio de contraseña para el funcionario sr(a)_____.

De acuerdo a lo establecido en la Politica Gestión de Claves de este Gobierno Regional.

_____
FIRMA SOLICITANTE

12 APROBACIÓN

Elaborado por	Revisado por	Aprobado por
Carlos Hernández A. Analista Departamento de Informática	**José Ignacio Gutiérrez G.** Encargado de Seguridad SSI **Paulo Mendoza R.** Encargado Unidad de Soporte **Carolina Hidalgo M.** Jefa Departamento Planificación y Control Institucional	**Alejandro Segura B.** Presidente Comité de Seguridad

14 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES

Versión	Autor	Página o secciones	Fecha Modificación	Motivo
01	Carlos Hernández	todas	Agosto 2011	Creación
02	Carlos Hernández	todas	Diciembre 2016	• Cambio diseño • Se incorpora periodicidad de evaluación • Se incorpora periodicidad de revisión • Se incorpora Roles y responsabilidades
03	Mauricio Marín	todas	24/10/ 2017	Actualización y Modificación de documento para cumplimiento a directrices de la red de expertos SSI. • Se incorpora control normativo SSI • Se incorpora registro de control • Agrega anexos de creación modificación clave de usuarios • Agrega flujogramas de procedimientos de
04	Mauricio Marin V.	6	1/08/2018	Se agrega en Registro de Control el siguiente párrafo: En caso de no haber movimiento en relación a algún control que se pide informar, deberá reportarse de igual manera señalando que no hubo movimiento por lo que no se pudo demostrar con algún medio de verificación durante el respectivo periodo.

04	Mauricio Marin	6	1/08/2018	Se agrega el subtítulo de Procedimientos Documentados Se cambia título 7 por Definición y Modo de Operación Se cambia título 8 por Registro de Operación.