DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO INFORMATICA

APRUEBA NORMA DE USO IDENTIFICACIÓN Y AUTENTIFICACIÓN DE SISTEMAS INFORMÁTICOS DEL GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO.

RESOLUCIÓN EXENTA N° 3030

SANTIAGO, 22 DIC 2017

VISTOS:

El Decreto Supremo N° 331/2017 del Ministerio de Interior y Seguridad Pública; las facultades que me concede el Artículo 24 letra ñ) de la Ley N° 19.175, Orgánica Constitucional de Gobierno y Administración Regional; el DFL N° 29 de 2004 del Ministerio de Hacienda, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.834, Estatuto Administrativo; el Decreto N° 83/2005 del Ministerio Secretaría General de la Presidencia sobre seguridad y confidencialidad de los documentos electrónicos; la Resolución N° 1600 de 2008 de la Contraloría General de la República; y

CONSIDERANDO:

1.- Que, el indicador de Seguridad de la Información es un instrumento de control de gestión en las instituciones públicas, para la exitosa implementación de un Sistema de Seguridad de la Información;

2.- Que, es importante considerar los lineamientos que establece la "Política Nacional de CiberSeguridad", la cual señala como esencial dentro de un Sistema de Gestión de la Seguridad de la Información (SGSI), la gestión del riesgo;

3.- Que, la gestión del riesgo permite la identificación de amenazas, valoración y priorización de controles que ayudan a mitigar los mismos, detectados en la institución;

4.- Que, siempre existirá un riesgo residual con el cual hay que convivir como institución, pero es importante establecer el número de controles que mitiguen éstos, hasta el nivel que el riesgo residual sea aceptable.

16177861

5.- Que, es decisivo que cada institución comprenda que el número de controles que decida implementar, será a partir del resultado del perfil de riesgos que cada servicio enfrenta;

6.- Que, un riesgo de seguridad de la información corresponde a una amenaza potencial que podría afectar activos de información, vinculados a los procesos de soporte institucional y/o a los procesos de provisión de Productos Estratégicos (bienes y servicios) establecidos en las definiciones estratégicas institucionales (Formulario A1 DIPRES), y por tanto causar daño a la organización;

7.- Que, los servicios deben determinar cuáles son los riesgos de seguridad que afectan sus productos estratégicos del formulario A1 DIPRES, ello permite priorizar qué controles de la Norma deberán ser implementados para mitigar éstos;

RESUELVO:

1.- DÉJESE sin efecto la Resolución N° 2857 del 30 de diciembre de 2011, que aprobó la Norma de Uso Identificación y Autentificación del Gobierno Regional Metropolitana.

2.- APRUEBASE la Norma de Uso Identificación y Autentificación de Sistemas Informáticos del Gobierno Regional Metropolitano de Santiago.

ANOTESE Y PUBLIQUESE

INTENDENCIA REGION METROPOLITANA
INTENDENTE

JUAN PABLO GOMEZ RAMIREZ
INTENDENTE (S)
REGION METROPOLITANA DE SANTIAGO

IFF/GEP/VGM/MRT/JIG

Distribución:
- Funcionario Gobierno Regional Metropolitano de Santiago
- Honorarios Gobierno Regional Metropolitano de Santiago
- Comité de Seguridad de la Información
- Oficina de Partes

Norma de uso
Identificación y autentificación de Sistemas Informáticos

1 INDICE

1 INDICE 2
2 OBJETIVO 3
3 ALCANCE 3
4 ROLES Y RESPONSABILIDADES 3
5 CONTROL NORMATIVO 4
6 IDENTIFICACION Y AUTENTICACION 5
7 DESARROLLO DE LA NORMA 5
7.1 Administración de la información de autenticación secreta 5
7.2 Uso de la información de autenticación 5
7.3 Sistemas de administración de claves o contraseñas 6
8 REGISTROS DE CONTROL 6
9 MONITOREO 7
10 PROCEDIMIENTOS DE OPERACIÓN 8
11 PROCEDIMIENTO DE OPERACIÓN PARA CAMBIO DE CLAVE SISTEMAS 9
12 DIFUSIÓN 10
13 REVISIÓN 10
14 ANEXOS 11
14.1 Formulario de creación o cambio de autenticación secreta 11
14.2 Formulario solicitud cambio de contraseña 12
15 APROBACIÓN 13
16 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES 14

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 de política

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 DESARROLLO DE LA NORMA

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

8 REGISTROS DE CONTROL

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

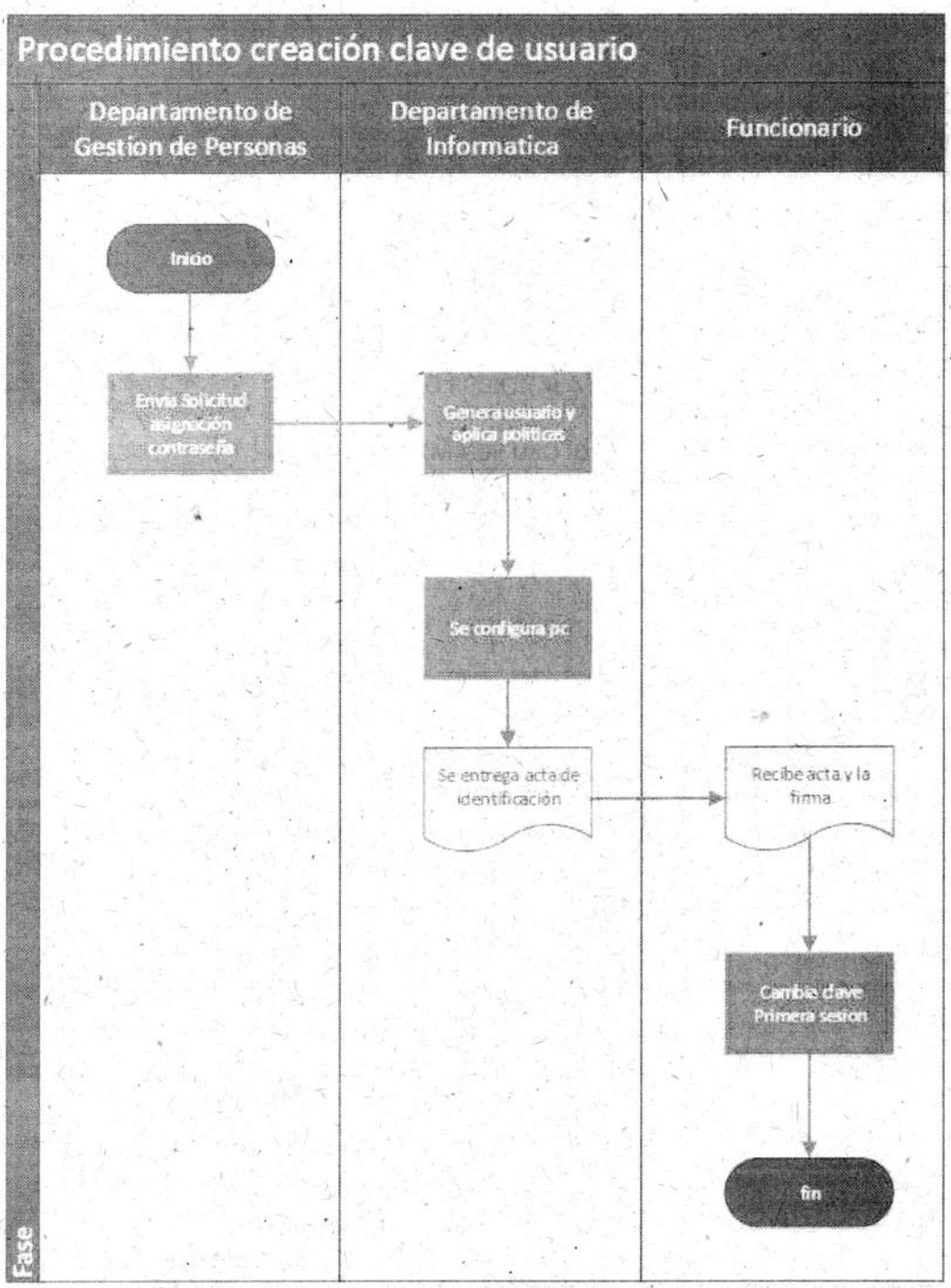
El informe deberá ser enviado al Encargado de Seguridad de manera semestral.

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)

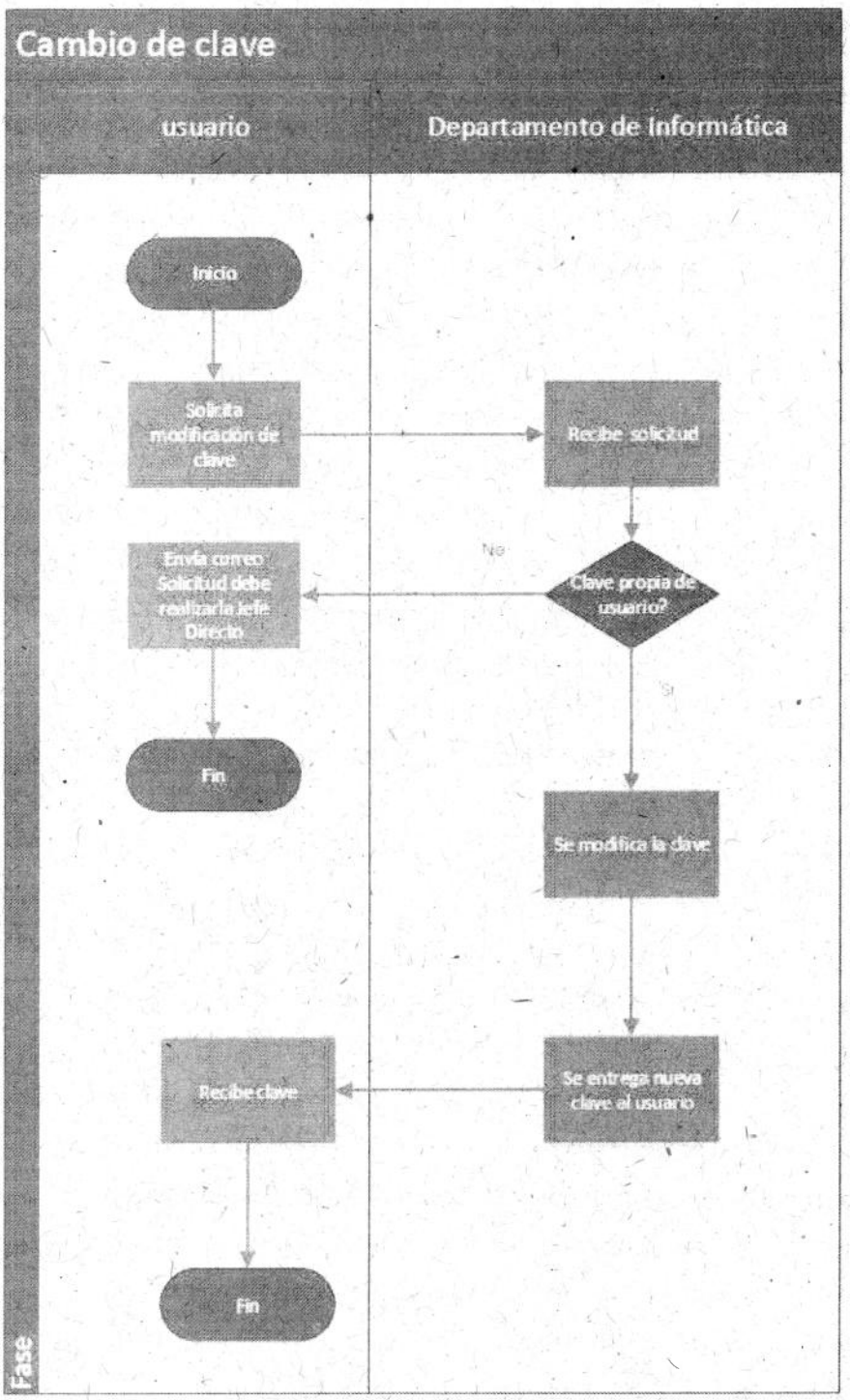
9 MONITOREO

El Departamento de Informática controlará la identificación y autentificación de los usuarios de los sistemas informáticos provistos por el Gobierno Regional Metropolitano de Santiago, evitando el mal uso de la infraestructura disponible.
Lo descrito anteriormente, se realiza con el fin de proporcionar información para el caso de revisiones.

10 PROCEDIMIENTOS DE OPERACIÓN



11 PROCEDIMIENTO DE OPERACIÓN PARA CAMBIO DE CLAVE SISTEMAS



12 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.

13 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.

14 ANEXOS

14.1 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

14.2 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

15 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 de Gestión Institucional	**Mayuri Reyes Torres** Presidente Comité de Seguridad

16 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 • Se incorpora Difusión
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 procedimientos

Acta de Reunión
Comité de Seguridad de la Información

Asistentes:

- Sra. Mayuri Reyes Torres - Jefa División de Administración y Finanzas
- Srta. Carolina Hidalgo Mandujano – Jefa Departamento de Gestión Institucional
- Sra. Valentina Guerra Monsalve - Jefa Departamento Jurídico
- Sra. María Macarena Miranda Nuñez - Jefa Departamento de Gestión Documental
- Sr. José Ignacio Gutiérrez - Encargado de Seguridad de la información
- Sr. Hector Salinas Murúa – Jefe (s) Departamento de Informática
- Sr. Carlos Hernández Arancibia – Analista Departamento de Informática
- Sr. Mauricio Marín Vera – Analista Departamento de Informática
- Srta. Paulina Vilches Vásquez– Encargada Unidad de Transparencia
- Sr. Juan Catalán Farías – Depto. Servicios Generales
- Sr. Ariel Lagos Vásquez – Prevencionista de Riesgos

Tabla:

1. Se ratifica al Jefe del Departamento de Informática como Encargado de Seguridad de la Información.

2. Se acuerda incorporación a este Comité de los siguientes funcionarios:
   a. Jefe Departamento de Servicios Generales
   b. Jefe Departamento de Gestión de Personas
   c. Prevencionista de Riesgos Institucional

3. Se revisa y evalúa la correcta ejecución de los contratos de mantenimiento del Gobierno Regional Metropolitano (GORE RM).

4. Se revisan y validan por parte de este Comité los siguientes documentos:

   - Política General de Seguridad de la Información
   - Resolución Encargado de Seguridad de la Información
   - Resolución de nombramiento Comité de Seguridad de la Información
   - Instructivo Correctivo Preventivo
   - Manual de Gestión de Archivos
   - Norma de Acceso a la Red
   - Norma de Eliminación de Activos
   - Norma de Seguridad de la Información para la Gestión de Proyectos
   - Norma de Uso Outsourcing
   - Norma de Trabajo Remoto
   - Norma de Uso Instalación Legal de Software
   - Norma de Uso Identificación y Autentificación

- Norma de Uso Navegación por Internet
- Norma de Uso para los Equipos Tecnológicos Portátiles
- Norma de Reutilización y Devolución de Activos
- Plan de Emergencia Institucional
- Política de Clasificación de Activos
- Política de Acceso físico
- Política de Correo Electrónico
- Política de Desarrollos de Sistemas
- Política de Dispositivos Móviles
- Política de Escritorios y Pantallas Limpias
- Política de Gestión de Incidentes de Seguridad
- Política de Gestión de la capacidad
- Política de la Seguridad Informática
- Política de Respaldo de la Información
- Política Gestión de Claves
- Política Manejo de Activos
- Política para la Privacidad y Protección de la Información e Identificación Personal
- Política sobre el Uso de Controles Criptográficos
- Política y Proceso de Selección de Personal
- Procedimiento de Control de las Vulnerabilidades Técnicas
- Protocolo de Control y Tratamiento de SSI
- Reglamento sobre Infracciones al SSI

5. Se toma conocimiento y valida el informe "Procesamiento y Confidencialidad de los Activos de Información", elaborado por el Encargado del Seguridad de la Información, el cual da cuenta de la no ocurrencia de incidentes de seguridad durante el período 2017.

6. Se informa por parte del Encargado de Seguridad de la Información respecto de la participación en distintas instancias en materias relativas al Sistema de Seguridad de la Información:

   - Exposición para el Sector Público de Expertos en materia de Seguridad informática (Subsecretaría del Interior)
   - Reunión bipartita GORE RM-Red de Expertos
   - Jornada de Capacitación Indicador SSI (Ministerio Secretaría General de la Presidencia)

7. Se dan a conocer por parte del Encargado de Seguridad de la información las medidas de difusión del Sistema de Seguridad de la Información a través de:

   - Correo electrónico a todo el personal.
   - Banner corporativo en Intranet Institucional.

8. Se acuerda que el Comité de Seguridad tenga una próxima sesión durante el primer semestre del próximo año para evaluar lo reportado durante 2017 y revisar los compromisos 2018.

Aprueban:

Sra. Mayuri Reyes Torres
Jefa División de Administración y Finanzas

Srta. Carolina Hidalgo Mandujano
Jefa Departamento de Gestión Institucional

Sra. Valentina Guerra Monsalve
Jefa Departamento Jurídico

Sra. Maria Macarena Miranda Nuñez
Jefa Departamento de Gestión Documental

Sr. Hector Salinas Murúa
Jefe (s) Departamento de Informática

Srta. Paulina Vilches Vásquez
Encargada Unidad de Transparencia

Sr. José Ignacio Gutiérrez García
Encargado de Seguridad de la Información