DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

RESOLUCION EXENTA N° 2857

SANTIAGO, 30 DIC 2011

VISTOS:

Las facultades que me confieren el Decreto Supremo N° 591/2011 del Ministerio del Interior y Seguridad Pública; el artículo 24 letra o) de la Ley N° 19.175, Orgánica Constitucional de Gobierno y Administración Regional; el D.F.L. N° 1/19.653, de 2.000, del Ministerio Secretaria General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; la Resolución N° 1600, de la Contraloría General de la República; el DFL N° 1/19.175, que fijó el texto refundido, coordinado, sistematizado y actualizado de la ley N° 19.175, Orgánica Constitucional sobre Gobierno y Administración Regional; y

CONSIDERANDO:

1° Que, con el objeto de contar con un sistema de gestión de seguridad de la información que permita lograr niveles adecuados de integridad, confidencialidad y disponibilidad para todos los activos de información institucional, de manera de asegurar la continuidad operacional de los procesos institucionales y la entrega de productos y servicios a los usuarios/clientes/beneficiarios.

2° Que, es afán de este Gobierno Regional, responder a distintos requerimientos, y en particular, lo referente a seguridad de la información.

3° Que, este Servicio estima pertinente crear normas y procedimientos para asegurar y velar por la Seguridad de los Activos de Información.

4° Que, este Servicio considera necesario abarcar todos los Activos de Información, no realizando diferencias entre Activos Físicos y Tecnológicos.

5° Que, debido al valor de la información de este Servicio se requiere fijar normas especificas para evitar vulnerabilidades en la Seguridad de la Información.

RESUELVO:

1.- APRUÉBENSE las siguientes normas con el objeto de asegurar, velar, gestionar y fortalecer la Seguridad de la Información del Servicio, las cuáles se adjuntan y son parte constitutiva de la presente Resolución:

- Norma de Acceso Físico
- Norma de Seguridad Informática
- Norma de Uso Navegación por Internet
- Norma de Uso Correo Electrónico

GOBIERNO REGIONAL DE SANTIAGO
DEPARTAMENTO JURIDICO
REGION METROPOLITANA

- Norma de Uso Instalación Legal de Software
- Norma de Uso Identificación y Autentificación
- Norma de Uso Outsourcing

2.- PUBLÍQUESE un ejemplar de la presente Resolución y los documento citados anteriormente en el Banner de Seguridad de la Información de la Intranet Institucional.

ANÓTESE, REGÍSTRESE Y COMUNÍQUESE.

INTENDENCIA REGION METROPOLITANA
INTENDENTA

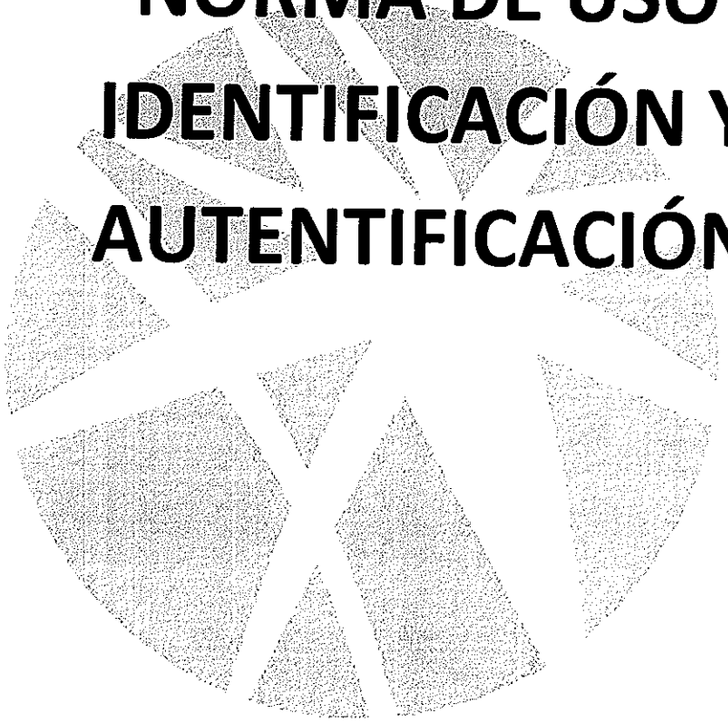
CECILIA PEREZ JARA
INTENDENTA
REGIÓN METROPOLITANA DE SANTIAGO

PUM/RAH/FRW/PSL/JGG/sbq

Distribución:
Gabinete Intendencia
Administración Regional
División de Análisis y Control de la Gestión
División de Planificación y Desarrollo
División de Administración y Finanzas
Departamento Jurídico
Unidad de Auditoría Interna
Unidad de Control Interno y Rendición de Cuentas
Unidad Regional de Asuntos Internacionales
Departamento de Gestión Institucional
Departamento de Gestión de Personas
Departamento de Gestión Documental
Departamento de Gestión de Abastecimiento
Departamento de Presupuesto y Contabilidad
Departamento de Servicios Generales
Departamento de Informática
Unidad de Desarrollo
Unidad de Soporte
Departamento de Control de Proyectos de Infraestructura y Obras Viales
Departamento de Actividades de Cultura, Deporte y Seguridad
Departamento de Transferencias de Capital
Departamento de Adquisición de Activos no Financieros
Departamento de Preinversión y Proyectos
Departamento de Planificación
Oficina de Partes.

GOBIERNO REGIONAL DE SANTIAGO
DEPARTAMENTO JURIDICO
REGION METROPOLITANA

NORMA DE USO IDENTIFICACIÓN Y AUTENTIFICACIÓN



GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

Introducción

Propósito. 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.

Alcance

Las políticas 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.

Identificación y autentificación

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.

Procedimientos y directrices:

i. Cada sistema debe incorporar la autenticación de usuario y la identificación para garantizar que el acceso no se concederá a personas no autorizadas. Los usuarios no tendrán el acceso a los recursos de información del Gobierno Regional Metropolitano de Santiago Gobierno Regional Metropolitano de Santiago sin identificarse y autenticarse en ellos.

ii. El Departamento de informática creara un sistema de bloqueo de usuario tras intentos fallidos en las contraseñas de los mismos, el cual solo será quitado tras solicitud formal por parte de la jefatura.

iii. Las contraseñas solo serán cambiadas por el departamento de informática tras una solicitud formal por parte de la jefatura correspondiente al usuario.

iv. La asignación de los identificadores o contraseñas se hará mediante un proceso formal de gestión, en que el jefe directo del usuario será el responsable de la respectiva solicitud.

v. El personal de informática deberá crear la cuenta y permitir en su inicio de sesión al usuario cambiar su contraseña.

vi. La contraseña asignada por el Departamento de Informática solo será entregada al Usuario Final.

vii. Esta contraseña nunca será enviada por correo electrónico o será dejada al usuario final en algún papel sino solamente será entregada por palabra. El usuario firmara un acta de entrega del identificador o contraseña.

viii. Las contraseñas o identificadores deberán tener una longitud mínima de ocho caracteres; no deberán ser fáciles de recordar; deben contener letras, mayúsculas, dígitos, y caracteres de puntuación; no estarán basados en cosas obvias o de fácil deducción a partir de datos relacionados con el usuario, por ejemplo, nombres, números telefónicos, cédula de identidad, fecha de nacimiento; estén libres de caracteres idénticos consecutivos o grupos completamente numéricos o alfabéticos; tampoco deben ser palabras del diccionario o nombres comunes;

ix. No se deberán colocar contraseñas que ya se hayan usado anteriormente.

x. Los usuarios a quienes se haya asignado privilegios especiales deberán cambiar sus contraseñas con una frecuencia no superior a 3 meses.

xi. Los usuarios no deberán mantener la misma contraseña para las distintas plataformas usadas en el servicio.

xii. Los usuarios que dispongan de un firmador electrónico como e-token, certificado de firma electrónica o sistemas biométricos deberán hacer uso de él logeandose en los sistemas que permitan el uso de estos.

modificación de las cuentas de usuario y credenciales de autenticación.

xiii. Las cuentas de usuario deben cumplir con las siguientes directrices:

a. Permitir sólo un usuario por cada cuenta. Los identificadores de usuario no deben ser compartidos. (Nombre de usuario, ID´s).

b. Nunca se debe activar/habilitar una cuenta de invitado. Eliminar todas las cuentas que se crea de forma predeterminada por el sistema, a menos que sea absolutamente necesario, aprobado por el administrador de la red.

c. No utilizar cuentas fáciles de predecir, nombres genéricos como:

- Anónimo
- Invitado
- Admin
- FTP
- Telnet
- Usuario
- Test
- otros

xiv. Las cuentas que están presentes por defecto en la instalación inicial del sistema, se deberán eliminar o cambiar de nombre a menos que sea técnicamente requerida por el sistema, debiendo dar aviso para tomar el resguardo necesario.

xv. Para las labores especificas que requieran cuentas de acceso (ya sea para algún funcionario o contratista), se deberán desactivar inmediatamente después del término de su utilización.

xvi. Las cuentas deben ser desactivadas inmediatamente después del término de una labor específica que sea ejecutada por un empleado o contratista.

xvii. Las cuentas no utilizadas serán desactivadas. Para esto se deberá generar una calendarización, que se ejecute al menos una vez al mes.

xviii. Las cuentas de los contratistas y los trabajadores temporales debe expirar en la final de su contrato.

xix. Las cuentas de administrador deben cumplir con las siguientes directrices:

a. Los nombres de las cuentas de administración deben ser cambiadas con una frecuencia que no dificulte la administración de los sistemas, dificultando a los atacantes adivinar los nombres de estas cuentas.

b. Cada persona que tiene una necesidad legítima de usar los privilegios de administración, debe tener su propia cuenta administrativa que se utilizará para llevar a cabo funciones. El uso de la cuenta de administrador principal para cada uno del sistema debe delimitarse a un grupo limitado de usuarios y a situaciones de emergencia. Esto protegerá a la cuenta de administrador principal y proporcionando una pista de auditoría de las actividades administrativas.

c. Todas las cuentas con privilegios de administrador deben tener contraseñas fuertes u otros métodos alternativos de autenticación robusta.

d. Otros métodos de autenticación de contraseñas distintas de contraseñas (por ejemplo, sistemas biométricos, tarjetas inteligentes, tokens, otros), deben ser aprobados por El Departamento de Informática del Gobierno Regional Metropolitano de Santiago.

xx. La información de las credenciales de la cuenta (por ejemplo, identificadores de usuario, contraseñas) que se almacenan en los dispositivos deben ser encriptadas.

a. Para evitar ataques de fuerza bruta, una función de bloqueo de intrusos debe ser implementado en cada sistema, suspendiendo temporalmente la cuenta después de tres intentos de inicio de sesión no válido. La reactivación de las cuentas bloqueadas deberá realizarse de forma manual por un administrador de sistema de seguridad.

xxi. El Gobierno Regional Metropolitano de Santiago restringirá el acceso a los datos de autenticación. Los datos de autenticación deberán ser protegidos con controles de acceso y encriptación para evitar que personas no autorizadas logren obtención de los datos.

Roles y Responsabilidades:

i. Los empleados 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 ha sido comprometido.

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

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

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

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

vi. Esta 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)

vii. Los supervisores y jefes de áreas 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 las cuentas que deben ser desactivadas, y deberán reportar cualquier sospecha o violaciones compromisos de las credenciales al Departamento de Informática.

viii. El área de Seguridad y/o los encargados de la seguridad de la información, implementaran métodos de autenticación para los sistemas de información en su cuidado, instruyendo a los usuarios en cuanto a su uso.

ix. El Sistema de Información de Seguridad preparará directrices y las normas para las credenciales de usuario, realizar revisiones de cumplimiento, y aprobar la emisión de las credenciales de administrador.

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

Monitoreo

Conforme a lo descrito a la normativa vigente:

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 y auditorias que requiera la organización.

Aplicación de las políticas de instalación legal de software

La infracción a las obligaciones establecidas en el artículo anterior, podrá constituir una violación al principio de probidad administrativa, y será sancionada en conformidad a lo dispuesto en la Ley N° 18.834, sobre Estatuto Administrativo. Lo anterior es sin perjuicio de la responsabilidad civil o penal que corresponda.

El Departamento de Informática del Gobierno Regional Metropolitano de Santiago, revisará y aprobará las aplicaciones que sean solicitadas para el cumplimiento de estas políticas y a su vez, la compatibilidad con la plataforma.

El Departamento de Informática no se hará responsable por incidentes producidos por el no cumplimiento de estas políticas de seguridad.

Historial de revisiones

VERSIÓN	ELABORADO	REVISADO	APROBADO	AUTORIZADO	FECHA