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 ACCESO FÍSICO

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

Introducción

Propósito. El propósito de esta política es establecer normas para garantizar el buen funcionamiento del Datacenter y servicios ofrecidos por el Departamento de Informática.

La aplicación de esta política, buscar evitar el acceso no autorizado ofreciendo además, controles para las auditorías más eficaces, logrando el control total en los accesos en el Gobierno Regional Metropolitano de Santiago, los cuales exponen a la institución a perdidas de información, daño a los recursos disponibles, como también problemas jurídicos tanto nacionales como internacionales.

Alcance

La política se aplica a todos los accesos restringidos que contenga el Gobierno Regional Metropolitano de Santiago, aplicando a todos los empleados, proveedores, contratistas, personal que esté vinculado con las firmas que presten servicios a 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 GORE.

Política

Ésta política especifica controles para reducir los riesgos asociados a la seguridad de la información asociados al control de acceso físico a las instalaciones.

Acceso a las instalaciones

- Todos los sistemas de seguridad física deben cumplir con todas las regulaciones aplicables como tal, pero no están limitados a los normas de construcción y prevención de incendios
- Todo acceso físico a las personas será restringido, debiéndose gestionar y documentar
- Todas las instalaciones de TI deberían estar físicamente protegidas en proporción a la criticidad o importancia de su función en el Gobierno Regional Metropolitano de Santiago
- Todo acceso a las instalaciones de TI, sólo se concederán al personal designado por el Departamento de Informática del Gobierno Regional Metropolitano de Santiago y contratistas, cuyas responsabilidades de trabajo requieran el acceso a dicha instalación
- El proceso para la obtención de las credenciales, tarjetas de acceso magnético o claves de acceso a instalaciones de TI deberán incluir la aprobación del Jefe del Departamento de Informática de Gobierno Regional Metropolitano de Santiago
- Las tarjetas de acceso magnético o claves de acceso no deben ser compartidas o cedidas a otros
- Las tarjetas de acceso magnético o claves de acceso que ya no sean necesarios o ya cumplieron su función, deberán ser devueltos a el Departamento de Informática del Gobierno Regional Metropolitano de Santiago. Las tarjetas no deberán ser reasignadas a otra persona sin pasar por el proceso de re enrolamiento

- La pérdida o robo de las tarjetas de acceso magnéticas o claves deberán ser reportados a El Departamento de Informática del Gobierno Regional Metropolitano de Santiago

- Los registros de acceso de las tarjetas de acceso magnéticas o claves deberán conservarse para mantener una revisión de los accesos y rutinas realizadas basados en la criticidad de los recursos que se protegen

- El Departamento de Informática del Gobierno Regional Metropolitano de Santiago, en colaboración con el área de personal, serán los encargados de recuperar y eliminar los accesos a los lugares restringidos de las personas que sean desvinculadas ó que por cambios en el contrato, cambien sus roles operativos

- Los visitantes deberán ser escoltados en el acceso a las zonas controladas por las instalaciones TI del Gobierno Regional Metropolitano de Santiago

- El Departamento de Informática, se encargará de revisar periódicamente los privilegios y derechos de acceso de las tarjetas de acceso magnético o claves para eliminar las de las personas que ya no requieran de éstos privilegios

- Las señaleticas para el acceso a las salas y locaciones restringidas deberá ser simple, sin embargo, deberá informar de forma simple la importancia de la ubicación

- Cualquier uso de las instalaciones de TI deberá contar con la aprobación del Departamento de informática del Gobierno Regional Metropolitano de Santiago.

- El personal autorizado debe tener las (24) horas de libre acceso a las instalaciones criticas de TI

Personal Autorizado

El acceso al Datacenter y racks de redes TI estarán restringidos sólo a los administradores de sistema TI y Jefe del Departamento de Informática. Los otros accesos a personal de servicios, Oficiales de seguridad y otros actores, estarán restringidos y, según sea necesario, se solicitará a la jefatura correspondiente para gestionar con el Jefe del Departamento de Informática dichos privilegios. Cualquier otro tipo de personal, deberá ingresar acompañado a las instalaciones.

Responsabilidades

El Departamento de Informática del Gobierno Regional Metropolitano de Santiago es el responsable de la seguridad de los datos en la red y sus equipos, con el fin de ejecutar a cabalidad la tarea de mantener la infraestructura de la red.

Aplicación de las políticas de acceso físico

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 velará por el cumplimiento de estas políticas, resguardando los intereses del Gobierno Regional Metropolitano de Santiago.

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

Difusión

Se mantendrá publicada dentro de la intranet del Gobierno Regional Metropolitano de Santiago, las normas de uso y políticas de seguridad establecidas en el presente reglamento.

Anexos

Historial de revisiones

VERSIÓN	ELABORADO	REVISADO	APROBADO	AUTORIZADO	FECHA

Este documento de origen electrónico, una vez impreso, pasa a ser copia no controlada y puede estar obsoleto. Para la versión vigente ir a Intranet.