DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

RESOLUCION EXENTA Nº 2796

SANTIAGO, 29 DIC 2011

VISTOS:

Las facultades que me confieren el Decreto Supremo Nº 591/2011 del Ministerio del Interior y Seguridad Pública; el artículo 24 letra o) de la Ley Nº 19.175, Orgánica Constitucional de Gobierno y Administración Regional; el D.F.L. Nº 1/19.653, de 2.000, del Ministerio Secretaria General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; la Resolución Nº 1600, de la Contraloría General de la República; el DFL Nº 1/19.175, que fijó el texto refundido, coordinado, sistematizado y actualizado de la ley Nº 19.175, Orgánica Constitucional sobre Gobierno y Administración Regional; y

CONSIDERANDO:

1º 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.

3º 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 y procedimientos 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, la que entrará en vigencia a partir de la fecha de su total tramitación:

- Norma de Uso para los Equipos Tecnológicos Portátiles.
- Norma de Escritorio Limpio.
- Norma de Eliminación, Reutilización y Devolución de Activos de Información.
- Procedimiento de Actualización de Seguridad y Validación de la Data.
- Procedimiento de Pruebas Funcionales

11955484

2.- PUBLÍQUESE un ejemplar de la presente Resolución, Normas y Procedimientos adjuntos 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/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.

NORMA DE ESCRITORIO LIMPIO

1. PROPÓSITO

El presente documento tiene por finalidad proteger toda la información institucional que pudiere estar accesible en los puestos de trabajo asignados a los usuarios internos del Servicio, que se considere importante para el logro de la misión y objetivos institucionales, independiente de la forma en que dicha información esté almacenada o contenida.

2. ÁMBITO ESPECÍFICO

El usuario estará obligado a proteger tantos sus artículos personales como los del Servicio y más aún, toda la información institucional que de él dependa y/o utilice.

3. SITUACIONES ESPECÍFICAS

A continuación se detallan y explican las situaciones a tener en cuenta para velar por la seguridad en nuestros puestos de trabajo.

Situación	Norma
Datos Propios del usuario	• Guardar agendas, celulares, organizadores y laptops en un cajón bajo llave, o quitarlos del escritorio durante períodos de tiempo extendidos, incluyendo la noche. • Cerrar maletines y gabinetes cuando se aleja del escritorio por periodos extendidos de tiempo. • Mantener todos los efectos personales en un maletín o gabinete cerrado dedicado a los mismos.
Elementos de Acceso	• Llevar consigo los dispositivos, y bloquear con clave los teléfonos y otros dispositivos móviles. • Nunca dejar tarjetas de control de acceso ni llaves; siempre portarlas. • Notificar inmediatamente al personal de seguridad si se pierden tarjetas de control de acceso o llaves.
Herramientas de Tecnologías de la Información	• Cerrar aplicaciones y bloquear el equipo cuando se aleje de su escritorio. • No dejar medios portátiles como pendrives conectados. • Apagar la computadora al alejarse por períodos prolongados de tiempo. • Nunca escribir las contraseñas en notas autoadhesivas ni tratar de esconderlas en la oficina. • Quitar impresiones antes de dejar el lugar. • Destruir impresiones con datos sensibles una vez utilizados. • Borrar archivos de memorias e impresoras.

Configuración de los espacios de trabajo	• Los escritorios deben posicionarse de forma que el material sensible no sea visible desde ventanas o pasillos. • Posicionar el monitor de forma que la información sea visible sólo para el usuario del puesto de trabajo. • Borrar pizarrones; si se necesita guardar datos, utilizar medios electrónicos. • Configurar el computador para que el protector de pantalla se active pasado los 5 minutos de espera, y que solicite clave de usuario.
Fuera del Escritorio	• No usar estanterías para guardar carpetas con información sensible. Etiquetar estas carpetas con nombres clave y cerrar con llave. • Ordenar carpetas en gabinetes para que las menos sensibles queden al frente y las más sensibles detrás. • Mantener los gabinetes de archivos cerrados con llave. No dejar las llaves en sus cerraduras. • Triturar el papel antes de arrojarlo. • Cerrar con llave la oficina al alejarse por períodos prolongados de tiempo.
Especies Valorados	• Todas las especies valoradas (Cheques, Vales Vista, Depósitos a Plazo, etc.) en caso de que el usuario se aleje o abandone su puesto de trabajo, deberán ser guardadas en la caja fuerte destinada para tales efectos. • Las facturas deberán ser guardadas en sus archivadores respectivos y en un estante ubicado en una oficina independiente con acceso restringido.

Para evitar violaciones de seguridad en nuestros puestos de trabajo se implementarán las siguientes medidas de seguridad informática:

a) Se configurarán todas las cuentas de usuarios para que a partir de las 22:00 sean deshabilitadas y así evitar la posibilidad de ingreso de terceros

b) Será responsabilidad de cada usuario estar atento a las impresiones que pudiéramos hacer en impresoras que no se encuentren conectadas a nuestros PCs de manera local y que están fuera de nuestra vista. De esta forma evitaremos la perdida de información.

4. LEYES, REGULACIONES Y POLÍTICAS.

Todos los usuarios deberán acatar y regirse por las leyes, regulaciones y políticas vigentes para Seguridad de la Información, suscritas y a las que se adhiera el Gobierno Regional Metropolitano de Santiago.

Asimismo, la presente norma será revisada y actualizada, en caso que así lo amerite, al menos una vez año.