Gobierno de Chile

DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

stgo 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 USO PARA LOS EQUIPOS TECNOLÓGICOS PÓRTATILES

1. PROPOSITO

El presente documento tiene por finalidad normar el uso de equipos portátiles de propiedad del Gobierno Regional Metropolitano de Santiago, con el objetivo de evitar los riesgos asociados a la seguridad de información.

Los computadores móviles son una herramienta esencial para el negocio, en los que se mantiene, usa y almacena información critica para el Servicio, ya que permiten revisar, modificar y generar documentos en cualquier momento, lugar y horario.

En la actualidad también son utilizados como equipos tecnológicos portátiles los teléfonos celulares y/o smartphones, ya que nos permiten tener acceso a nuestros correos electrónicos y documentos en cualquier momento o lugar.

Dada la portabilidad que nos entregan estos equipos se pueden generar ciertas vulnerabilidades a la seguridad de la información, tales como: robo, pérdida y/o daño físico del equipo, corrupción de datos, copia no autorizada de información, mal uso de la información almacenada en el equipo, entre otras.

Este documento detalla de forma específica las políticas de seguridad que aplican al equipamiento portátil entregado por el Gobierno Regional Metropolitano de Santiago.

2. SEGURIDAD Y CONTROL FÍSICO DE LOS EQUIPOS TECNOLÓGICOS PORTATILES

La seguridad física del equipo móvil facilitado por el Gobierno Regional Metropolitano de Santiago, es de responsabilidad de la persona a la que se le asigna, y será quien deberá responder en caso de daños o hurto, debiendo estar alerta ante posibles riesgos.

El funcionario responsable del equipo tecnológico portátil, deberá mantener bajo su cuidado y resguardo el equipo asignado. Deberá tener especial cuidado en lugares públicos. Tenga presente que este tipo de equipamiento puede ser robado con gran facilidad y que su extravío es muy común.

Si por algún motivo debe dejar temporalmente su equipo tecnológico portátil en alguna oficina, sala de reuniones, habitaciones de hoteles, aunque sea por un corto período, utilice cables de seguridad para equipos móviles o algún dispositivo con similares características para amarrar o trabar en algún sitio que lo permita de forma segura. Deberá implementar y configurar el bloqueo automático del equipo y una contraseña de seguridad para su desbloqueo

Cuando no sea necesario utilizar el equipo portátil deberá ser guardado en un lugar seguro, no dejándolo a la vista o en un vehículo para evitar hurtos.

Si el equipo es robado o extraviado, se deberá notificar inmediatamente al Departamento de Informática y realizar la correspondiente denuncia en Carabineros, entregando la información relativa al equipo.

Deberá realizar en forma periódica respaldo de la información almacenada en los equipos tecnológicos portátiles, se recomienda que para los computadores portátiles este respaldo sea a lo menos cada 15 días y para los celulares y/o smartphones sea 1 vez al mes

3. PROTECCIÓN CONTRA VIRUS EN LOS COMPUTADORES PORTATILES

Los virus son la mayor amenaza para los equipos portátiles y para la información en ellos almacenada, si no se tienen las precauciones necesarias. La aplicación del antivirus debe ser actualizada a lo menos una vez al mes. La forma más fácil de hacer este procedimiento, es, conectando el equipo a la red del Gobierno Regional Metropolitano de Santiago, el cuál actualizará automáticamente el equipo portátil. Si existe algún problema, contacte al Departamento de Informática y notifique el problema.

Los archivos adjuntos en los correos son una fuente de virus de computadores. Evite abrir cualquier archive adjunto en caso de que este se encuentre en un correo electrónico de una dirección que no conozca.

Cada vez que descargue algún archivo a su equipo portátil, utilice siempre la aplicación de antivirus para revisar su contenido. Normalmente el antivirus automáticamente revisa cualquier tipo de archivo. Si desea realizar un escaneo de archivos manual o tiene dudas, podrá preguntar al Departamento de Informática.

Para reportar cualquier incidente de seguridad (ya sea virus, spam u otros) deberá comunicarse con el Departamento de Informática para minimizar los daños. No reenvíe archivos desde su computador si sospecha que éste pueda estar infectado.

Si el equipo presenta problemas de virus, se deberá notificar inmediatamente al Departamento de Informática con la finalidad de que pueda tomar las medidas correspondientes para solucionar el incidente.

4. CONTROLES PARA ACCESO NO AUTORIZADO A LOS EQUIPOS

Deberá utilizar la aplicación de encriptación de datos que posee el equipo portátil entregado por el Gobierno Regional Metropolitano de Santiago, asegurándose de elegir una contraseña de largo razonable y que no sea común. Contáctese con el Departamento de Informática para obtener información relacionada con la encriptación en el equipo portátil. Si el equipo portátil es robado o extraviado, la encriptación provee de una protección extremadamente segura contra accesos no autorizado a la información.

Su identificación con la que ingresa dentro de la red del Servicio debe mantenerla a resguardo debido ya que pone en peligro la información la Red. Deberá abstenerse de compartir dicha contraseña.

Los equipos portátiles asignados por el Gobierno Regional Metropolitano de Santiago son de uso exclusivo del personal, debiendo evitar el uso por familiares y/o amigos.

Evite dejar el equipo portátil con la sesión abierta. Siempre apague, bloquee (teclas Windows + L) o active el protector de pantalla con contraseña después de utilizar activamente el equipo.

5. OTROS CONTROLES DE SEGURIDAD PARA LOS EQUIPOS PORTATILES

5.1. Software no autorizado

No se permitirá instalar, descargar o usar software que no se encuentre autorizado por el Gobierno Regional Metropolitano de Santiago. El software no autorizado puede introducir serias vulnerabilidades de seguridad dentro del Servicio, afectando el trabajo de todo el personal de la Institución. Está estrictamente prohibida la instalación y utilización de aplicaciones de hackeo, crackeo, gestores de descargas u otros que no sean afines a las labores habituales del personal.

5.2. Software no licenciado

Se realizará un control minucioso y detallado de las licencias de software instalado en los equipos computacionales del Servicio. La mayoría del software que sea específicamente identificado como "freeware" o "de dominio público", puede ser instalado y/o usado si la licencia ha sido previamente autorizada explícitamente por la Unidad de Desarrollo y no contravenga el punto anterior. Las aplicaciones shareware o de prueba deben ser eliminadas o licenciadas una vez terminado el período de prueba.

6. MATERIAL NO AUTORIZADO

Se prohíbe y será sancionado todo lo que se considere como contenido de naturaleza ilegal (relacionados con hechos delictivos tales como terrorismo, piratería, documentos electrónicos con infracción al derecho de autor, pornografía infantil, estafas o temas adversos en general).

7. LEYES, REGULACIONES Y POLÍTICAS

Para el uso de equipos computacionales y la utilización del software instalado en ellos, el Servicio reconoce, y en todas sus funciones se rige por la normativa legal vigente en lo relacionado con propiedad intelectual, derechos de autor y seguridad de la información, siendo ésta parte integral de la Política General de Seguridad de la Información del Servicio.

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