DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

RESOLUCION EXENTA Nº 2999

SANTIAGO, 29 NOV 2016

VISTOS:

Las facultades que me confieren el Decreto Supremo Nº 674/2014 del Ministerio del Interior y Seguridad Pública; el artículo 24 letra o) de la Ley Nº 19.175; 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; la Ley N° 18.575 Orgánica Constitucional de Bases Generales de la Administración del Estado; lo dispuesto en la Ley N° 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma; el Decreto N° 181/2002 que aprueba el Reglamento de la Ley N° 19.799; el Decreto Supremo N° 83/2005 del Ministerio Secretaría General de la Presidencia sobre seguridad y confidencialidad de los documentos electrónicos; la Resolución N° 1.600 de 2008 de la Contraloría General de la República; y

CONSIDERANDO:

1.- Que, se hace necesario contar con una normativa adecuada en materia de seguridad de activos de información, la cual vele por su integridad, confidencialidad y disponibilidad,

2.- Que, es afán de este Gobierno Regional dar fiel cumplimiento a la legislación vigente referente a seguridad de la información,

3.- Que, se debe contar con un reglamento disciplinario formal que contenga medidas a tomar en los casos que se vulnere la seguridad de la información, que considere factores como la naturaleza y la gravedad de la transgresión y su impacto en el Servicio.

RESUELVO:

1.- **APRUÉBESE** el **REGLAMENTO SOBRE INFRACCIONES AL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN**, el cual se adjunta y es parte constitutiva de la presente Resolución.

2.- **PUBLÍQUESE** un ejemplar de la presente Resolución en la Intranet Institucional.

ANÓTESE, REGÍSTRESE Y DIFÚNDASE.

INTENDENCIA REGION METROPOLITANA
INTENDENTE

CLAUDIO ORREGO LARRAIN
INTENDENTE
REGION METROPOLITANA DE SANTIAGO

IFF/GEP/MRT/CHM/JGG

Distribución:
Administración Regional
División de Administración y Finanzas
División de Análisis y Control de Gestión
División de Planificación y Desarrollo
Departamento de Gestión Institucional
Departamento de Informática
Oficina de Partes.

15942432

Reglamento sobre Infracciones al SSI

INDICE

1 INTRODUCCIÓN

El objetivo del Sistema de Seguridad de la Información (SSI) es "lograr niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información institucional relevante, con el objeto de asegurar continuidad operacional de los procesos y servicios, a través de un sistema de gestión de seguridad de la información.

Dado que los activos de información son uno de los componentes más importantes de toda organización moderna, requiere junto a los procesos y sistemas que la manejan, ser protegidos convenientemente frente a amenazas que puedan poner en peligro la continuidad de los niveles de servicio, rentabilidad social y conformidad legal, necesarios para alcanzar los objetivos institucionales.
Por otra parte, mediante el Sistema de Seguridad de la Información se busca generar un marco institucional, al establecer políticas, procedimientos y controles en relación a los objetivos estratégicos de la institución, con objeto de controlar el riesgo y mantenerlo por debajo de los estándares establecido por la propia organización.

En este sentido se ha designado a un Encargado de Seguridad de la Información, se crea Comité de Seguridad y se aprueba una Política General de Seguridad Institucional, que expresa adecuadamente el compromiso adquirido.

Para estos efectos, se han aprobado una serie de documentos orientados a implementar adecuadamente los proyectos de interés institucional, entre los cuales se encuentra la Política General de Seguridad de la Información; Normas sobre seguridad informática; Normas de navegación por internet; Norma de acceso físico; Norma de uso de correo electrónico; Norma de uso instalación legal de software; norma de uso identificación y autenticación; normas Outsourcing; Manual de Gestión de Archivos; Manual de Eliminación de Archivos, Norma de Eliminación; Reutilización y Devolución de Activos de Información; Norma de Uso para los Equipos Tecnológicos Portátiles; Norma de Escritorio Limpio; ;Procedimiento de Actualización de Seguridad y Validación de la Data; Procedimiento de Pruebas Funcionales; Instructivo de Autorización y Control para Instalaciones ; Protocolo de Control y Tratamiento de la Seguridad de la Información; Instructivo de Contingencia; Norma de trabajo Remoto ; Política de Dispositivos Móviles; Política de gestión de la capacidad; Política Clasificación de activos; Política Manejo de activos; Política sobre el uso de controles criptográficos; Política para la privacidad y protección de la información e identificación personal; Procedimiento de control de las vulnerabilidades técnicas; y Procedimiento de Gestión de Claves. Así como cualquier documento que tenga que ver con la seguridad de la información.

Este Reglamento aplicará a cualquier política, norma, procedimiento o reglamento posterior a la publicación del mismo y que tenga relación con el Sistema de Seguridad de la Información.

2 ALCANCE

El presente documento permitirá la correcta utilización de los activos provistos por el Gobierno Regional Metropolitano de Santiago, facilitando el manejo, procesamiento, almacenamiento y comunicación de la información conforme a su clasificación.

Esta política es aplicable a todos los funcionarios (planta, contrata, reemplazos y suplencias) personal a honorarios y terceros (proveedores, compra de servicios, etc.), que presten servicios en el Gobierno Regional Metropolitano o el Parque Lo Errazuriz.

3 OBJETIVO

El presente Reglamento tiene por objeto establecer los principios y criterios que, de acuerdo con el sistema de seguridad de la información y los documentos asociados al mismo, permitan estimar que una conducta, mediante el uso de las tecnologías de información, pone en riesgo la confidencialidad, integridad y disponibilidad de información de relevancia para la institución.

4 PREREQUISITO

El proceso disciplinario no debe iniciar antes de verificar que ha ocurrido una transgresión a la seguridad de la información.

Para desarrollar la verificación proceda según lo estipulado en la "Política de Gestión de Incidentes de Seguridad".

5 SANCION POSITIVA

El proceso disciplinario puede convertirse en una motivación o incentivo si se definen sanciones positivas para el comportamiento sobresaliente.

Es necesario destacar el buen uso en el Sistema de seguridad de la información e incentivar a los funcionarios a poder denunciar faltas a la seguridad.

6 TÍTULO ÚNICO

ARTÍCULO 1: Se entiende que afectan la Seguridad de la Información los actos u omisiones que puedan poner en riesgo la confidencialidad, integridad, disponibilidad de la información, la continuidad operacional de los procesos institucionales y la entrega de productos y servicios a los usuarios/clientes/beneficiarios.

ARTÍCULO 2: Todo aquel que tome conocimiento de un hecho que pudiere ser irregular, especialmente de aquéllos que contravienen el principio de probidad administrativa regulado por la Ley Nº 18.575, tiene la obligación de ponerlo en conocimiento de su Jefatura directa y/o del Jefe Superior del Servicio.

ARTÍCULO 3: Cualquier funcionario que detecte posibles violaciones de la seguridad de la información deberá informar de inmediato al Encargado de Seguridad, quien, una vez recabados los antecedentes y estimando que puede constituir una conducta o desempeño funcionario reprochable o haber una vulneración de deberes funcionarios, deberá dar cuenta al Jefe del involucrado, para los efectos que se indica en el artículo séptimo o al Jefe Superior del Servicio para los efectos previstos en el artículo noveno, ambos del presente reglamento.

ARTÍCULO 4: Podrán dar origen a la comunicación estipulada en el artículo anterior, y sin que esta enumeración sea taxativa, una o más de las siguientes conductas:

Restringir las conexiones remotas a los recursos de la plataforma tecnológica.

No contar con las aprobaciones requeridas para establecer una conexión remota a los dispositivos de la plataforma tecnológica y no acatar las condiciones de uso establecidas para dichas conexiones.

Establecer conexiones remotas en computadores que no estén previamente identificados o en computadores de uso público, de hoteles o cafés internet, entre otros.

Permitir que otra persona utilice su cuenta de acceso.

No mantener una contraseña de autenticación fuerte.

Modificar las configuraciones de seguridad de los dispositivos móviles institucionales (celulares, notebook, tablet) que les han sido asignados o desinstalar el software provisto con ellos al momento de su entrega.
Instalar programas desde fuentes desconocidas o desde repositorios no oficiales de los dispositivos móviles institucionales.

Almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

Vulnerar las restricciones de acceso a sitios web prohibidos.

En general cualquier conducta que atente o infrinja obligaciones establecidas en las normas, procedimientos, manuales, protocolos y políticas, aprobadas mediante Resolución Exenta Nº 3163 de 24 de diciembre de 2015, de este Servicio, y las Resoluciones Exentas, que la modifiquen, sustituyan o reemplacen.

ARTÍCULO 5: Podrá constituir una violación a la seguridad de la información no guardar secreto en los asuntos que revistan el carácter de reservados en virtud de la ley, del reglamento, de su naturaleza o por instrucciones especiales.

ARTÍCULO 6: También podrá ser considerada una violación a la seguridad de la información el daño, sustracción o pérdida de información o documentos, en forma dolosa o negligente por parte de algún funcionario de esta institución.

ARTÍCULO 7: El Encargado de Seguridad, una vez recabados los antecedentes de acuerdo con lo indicado en el artículo tercero precedente, y estimando que puede constituir una conducta o desempeño funcionario reprochable los hará llegar al Jefe directo del funcionario involucrado, a fin que proceda, si lo estima pertinente, a hacer la anotación de demérito que corresponda.

ARTÍCULO 8: En caso que una determinada situación o conducta pudiera ser constitutiva/o de infracción a las obligaciones o deberes funcionarios deberá ser puesto en conocimiento del Jefe Superior del Servicio, a través del procedimiento antes mencionado, a fin que, si estima que son susceptibles de ser sancionados con una medida disciplinaria, ordene la instrucción de una investigación sumaria o sumario administrativo, que tenga por objeto verificar la existencia de tales hechos y la individualización de los responsables y su participación, todo ello conforme lo establecido en el Título V, de la Ley N° 18.834, sobre Estatuto Administrativo.

7 APROBACIÓN

Elaborado por	Revisado por	Aprobado por
Susana Guzmán Arzic Abogada Departamento Jurídico	**Carlos Hernández A.** Analista Departamento de Informática **José Ignacio Gutiérrez García** Encargado Seguridad de la Información **Carolina Hidalgo M.** Jefa Departamento de Gestión Institucional	**Mayuri Reyes Torres** Presidente Comité de Seguridad

8 Historial de revisiones

Versión	Autor	Cargo	Fecha	Cambio/Revisión