Gobierno de Chile

DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

stgo GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

RESOLUCION EXENTA Nº 2795

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:

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.

3º Que, este Servicio estima pertinente protocolizar en forma precisa el acceso a los Activos de Información existentes y así evitar posibles vulnerabilidades en la Seguridad de la Información.

4° Que, este Servicio considera necesario instruir en forma clara, precisa y eficiente acerca de los procedimientos, procesos y acciones que se deben realizar en el momento que se produzca un incidente relacionado con la Seguridad de la Información.

5° Que, se requiere registrar, catastrar, gestionar y comunicar todos los incidentes de Seguridad de la Información que se produzcan en el Servicio, con la finalidad de poder tomar las medidas correctivas y preventivas para evitar que éstos se produzcan nuevamente.

RESUELVO:

1.- APRUÉBENSE el siguiente Protocolo e Instructivo con el objeto de asegurar, velar, gestionar y fortalecer la Seguridad de la Información del Servicio, los 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:

- Protocolo para el Control y Tratamiento de la Seguridad de la Información.
- Instructivo de Contingencia.

2.- PUBLÍQUESE un ejemplar de la presente Resolución, Protocolo e Instructivo 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.

INSTRUCTIVO DE CONTINGENCIA

1. PROPOSITO

Establecer los procedimientos para manejar los diferentes tipos de incidentes en la seguridad de la información que ocurran en el servicio, con el objetivo de tener un registro y gestión de los mismos.
Las contingencias más comunes que pueden suceder son:

- Fallas del sistema de información y pérdida del servicio.
- Código malicioso.
- Negación del servicio.
- Errores resultantes de data incompleta o inexacta.
- Violaciones de la confidencialidad e integridad.
- Mal uso de los sistemas de información.

2. PLAN DE CONTINGENCIA

En caso de que suceda un incidente relacionado con la Seguridad de la Información se deberán realizar las siguientes etapas:

2.1. Identificación del incidente

En caso de que se produzca un incidente de Seguridad de la Información, se deberá comunicar en forma inmediata con el Encargado de Seguridad del Servicio, quién realizara las coordinaciones internas de la siguiente forma:

a) Cuando se detecte un incidente de seguridad de la información se deberá informar en forma inmediata al Jefe del Departamento de Informática, quién deberá destinar la disponibilidad de personal y los recursos necesaria para poder determinar el Origen del Incidente, el Motivo por el que se produjo y dimensional el impacto del mismo.

b) Se comunicara con el jefe directo de la persona que fue afectada por el incidente para que se encuentre en conocimiento de la situación.

c) Se realizara el registro del incidente por medio de Registro de Incidentes en el que se deberán consignar los siguientes datos: Numero de Incidente, fecha del reporte, fecha del incidente, hora de reporte, nombre de quien reporto, nombre de quien sufrió el incidente, tipo de incidente, descripción del incidente, grado de criticidad, tiempo estimado de solución, tareas a realizar para dar solución, registro de avisos a Jefatura, Encargado de Seguridad, Depto. Gestión de Personas, Depto. De Informática (Debiéndose en estos casos señalar a quién se le informo, la fecha y hora de la comunicación)

2.2. Análisis y gestión del incidente

Cada vez que se produzca un incidente relacionado con la Seguridad de la Información se realizara el análisis de la situación y la gestión del mismo, con el objetivo de poder registrar y aprender de los incidentes que ocurran para que no se repitan y así poder establecer las normas, instructivos y procedimientos necesarios para fortalecer la Seguridad de la Información en el Servicio.

Para lo anterior se deben considerar los siguientes puntos:

a) Uso de evidencia forense en relación a una violación potencial del contrato o el requerimiento regulador o en el caso de una acción legal civil o criminal; por ejemplo, bajo la legislación sobre el mal uso de computadoras o protección de data.

b) Negociación para la compensación de los proveedores del software y servicio.

c) Se deberán controlar formal y cuidadosamente las acciones para la recuperación de las violaciones de la seguridad y para corregir las fallas en el sistema; los procedimientos deberían asegurar que:

- Se acordaran con la dirección los objetivos para la gestión de incidentes en la seguridad de la información, y se deberían asegurar que aquellos responsables de la gestión de incidentes en la seguridad de la información entiendan las prioridades de la organización para el manejo de los incidentes en la seguridad de la información
- Se utilizara la información obtenida de la evaluación de los incidentes en la seguridad de la información para identificar los incidentes recurrentes o de alto impacto.
- Se desarrollaran y seguirán los procedimientos internos cuando se recolecta y presenta evidencia para propósitos de una acción disciplinaria manejada dentro de una organización

2.3. Finalización e informe del incidente

Una vez finalizado el incidente, se realizará un informe respecto al mismo, el que se detallará toda la información relacionada, indicándose las tareas realizadas para su resolución, mejores prácticas posibles de implementar, mejoras a considerar, entre otras.

Este informe será generado por el Departamento de Informática y será enviado a la persona afectada por el incidente, a su jefatura, a los miembros del Comité de Seguridad, Encargado de Seguridad, Departamentos de Gestión de Personas, a los Jefes de División, Administración Regional y Jefe de Servicio, con el objetivo de que tomen conocimiento de la solución del incidente.