RESOLUCION EXENTA Nº 3163

SANTIAGO, 24 DIC 2015

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, con el objeto de contar con la normativa necesaria en materia de seguridad de activos de información, las cuales velen 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, este Servicio estima necesario la creación y actualización de distintos documentos relativos a seguridad de la información para dar fiel cumplimiento de su implementación,

4.- Que, para lograr lo anterior se abarcarán todo tipo de activos de información, ya sean físicos o tecnológicos, tangibles y no tangibles,

5.- Que el Comité de Seguridad de la Información revisó y actualizó un conjunto de normas, procedimientos y políticas,

RESUELVO:

1.- DEJENSE SIN EFECTO

1.1 Resolución Exenta 1805, del 28 de septiembre del 2011 que aprueba el Plan General de Seguridad de la Información

1.2 Resolución Exenta 2371, del 28 de noviembre del 2011 que aprueba la Política de Clasificación y Manejo de Activos

1568415

1.3 Resolución Exenta 2549, del 19 de diciembre del 2011 que aprueba el Instructivo Correctivo Preventivo

1.4 Resolución Exenta 2621, del 23 de diciembre del 2011 que aprueba la Política y Proceso de Selección de Personal

1.5 Resolución Exenta 2795, del 29 de diciembre del 2011 que aprueba el Protocolo de Control y Tratamiento de la Seguridad de la Información e Instructivo de Contingencia.

1.6 Resolución Exenta 2796, del 29 de diciembre del 2011 que aprueba la Norma de Uso para los Equipos Tecnológicos Portátiles, Procedimiento de Actualización de Seguridad y Validación de Data, Norma de Escritorio Limpio, Norma de Eliminación, Reutilización y Devolución de Activos de Información y el Procedimiento de Pruebas Funcionales.

1.7 Resolución Exenta 2801, del 29 de diciembre del 2011 que aprueba Manual de Gestión de Archivos.

1.8 Resolución Exenta 2857, del 30 de diciembre del 2011 que aprueba Normas Outsourcing, norma de uso Identificación y Autenticación, Norma de uso e Instalación Legal de Software, Norma de Uso Correo Electrónico, Norma de Acceso Físico, Norma de uso Navegación por Internet y Normas de Seguridad Informática.

1.9 Resolución Exenta 2858, del 30 de diciembre del 2011 que aprueba el Instructivo de Autorización y Control para Instalaciones.

1.10 Resolución Exenta 1193, del 26 de junio del 2012 que aprueba el Manual de Procedimientos para Eliminación de Documentos

2.- APRUÉBENSE las siguientes normas, procedimientos, manuales, protocolos y políticas actualizadas con el objeto de asegurar, velar, gestionar y fortalecer la Seguridad de la Información del Servicio, las cuales se adjuntan y son parte constitutiva de la presente Resolución:

2.1 Política General de Seguridad de la Información
2.2 Instructivo Correctivo Preventivo
2.3 Instructivo de Autorización y Control para Instalaciones
2.4 Instructivo de Contingencia
2.5 Manual de Gestión de archivos
2.6 Manual de Eliminación de archivos
2.7 Norma de Acceso físico
2.8 Norma de Eliminación, reutilización y devolución de activos de información.
2.9 Norma de Escritorio Limpio
2.10 Norma de Seguridad Informática
2.11 Norma de Uso de Correo Electrónico
2.12 Norma de Uso Identificación y autentificación

2.13 Norma de Uso Instalación legal de software
2.14 Norma de Uso Navegación por Internet
2.15 Norma de Uso Outsourcing
2.16 Norma de Uso para los Equipos Tecnológicos Portátiles
2.17 Política de Clasificación y Manejo de Activos de Información
2.18 Política y Proceso de Selección de Personal
2.19 Procedimiento de Actualización de Seguridad y Validación de Data
2.20 Procedimiento de Prueba Funcionales
2.21 Protocolo de Control y Tratamiento de la seguridad de la información

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

ANÓTESE, REGÍSTRESE Y COMUNÍQUESE.

INTENDENCIA REGION METROPOLITANA
INTENDENTE

CLAUDIO ORREGO LARRAIN
INTENDENTE
REGION METROPOLITANA DE SANTIAGO

MEL/RZE/MRT/CCM/JGG

Distribución:
Administración Regional
División de Administración y Finanzas
Departamento de Gestión Institucional
Departamento de Informática
Unidad de Auditoría Interna
Oficina de Partes.

DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Versión 6
11.12.2015

1.- DECLARACIÓN INSTITUCIONAL

El presente documento corresponde a una sistematización y actualización de las orientaciones estratégicas en materias de seguridad de la información del Gobierno Regional Metropolitano de Santiago.

La Política General de Seguridad de la Información será revisada integralmente al menos una vez al año y aprobada por el Comité de Seguridad de la Información del Servicio.

El Gobierno Regional Metropolitano de Santiago reconoce la importancia de la identificación, clasificación y resguardo de los activos de información, entendiendo como activos de información todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de relevancia para la institución; por lo que se compromete a trabajar en la disminución del nivel de riesgos en el uso, almacenamiento, acceso y distribución de la información, fomentando en todo el personal del Servicio una cultura de seguridad de los activos de información, que involucran el resguardo de su confidencialidad, integridad y disponibilidad.

Esta Política General define los criterios y lineamientos esenciales, en cuanto a la administración, resguardo, custodia y uso de la información y de los bienes asociados a su tratamiento, por lo tanto se cumplirán los requisitos institucionales, legales o reglamentarios y las obligaciones contractuales en los ámbitos relacionados con la seguridad de la información del servicio.

La Seguridad de la Información es entendida como la prevención de la confidencialidad, integridad, disponibilidad de la información y la protección de ésta, de una amplia gama de amenazas, a fin minimizar el daño, garantizar la continuidad operacional de los procesos institucionales y la entrega de productos y servicios a los usuarios/clientes/beneficiarios.

2.- COMPROMISOS INSTITUCIONALES

- La información es un bien valioso para el Servicio, que debe ser administrada bajo los más altos estándares de seguridad.
- Se reconoce la seguridad de la información como un atributo necesario en los servicios ofrecidos por el Servicio.
- La información es considerada como un recurso imprescindible para la gestión y operación del negocio.
- La seguridad de la información, es responsable de todos, independiente del cargo que se desempeñe.
- La información es clasificada de acuerdo a criterios de valoración en relación a la importancia que posee para el Servicio.
- La información de la organización sólo puede ser accedida por personas o entidades externas, según la clasificación que se haya hecho de ella en las situaciones y formas expresamente establecidas en las normas vigentes y con controles que garanticen su protección.
- La organización declara su decisión de cumplir con la normativa y legislación vigente en relación a aspectos de reserva y privacidad de la información.
- Todo empleado, proveedor o personal externo que preste sus servicios debe acceder exclusivamente a la información que, de acuerdo a su clasificación, le sea autorizada para lo cual se tendrá en consideración las tareas que deban cumplir.
- Todo empleado tiene la obligación de notificar cualquier actividad o situación que afecte la seguridad de los activos de información.
- El servicio reconoce que la sensibilización, capacitación y entrenamiento a su personal en las materias de seguridad de la información son tareas prioritarias.

3.- ALCANCE

La presente ***Política General de Seguridad de la Información del Gobierno Regional Metropolitano de Santiago*** es aplicable a la Administración Regional y todas las divisiones, departamentos y unidades que lo conforman y al personal que en éste trabajan.

Asimismo, esta política se aplica a la clasificación y manejo de la información; uso de internet y correcto electrónico;

4.- OBJETIVOS DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos de la gestión de seguridad de la información se han organizado de acuerdo a las categorías de: clasificación y catastro de información, análisis de riesgo y capacitación y difusión al personal.

Es de suma importancia que el inicio de un evento este separado de su autorización y de esta forma evitar posible colusión en el diseño de controles.

CLASIFICACIÓN Y CATASTRO DE ACTIVOS DE INFORMACIÓN

- Identificar y clasificar con un inventario detallado los activos de información, según tipo, formato, ubicación, importancia, responsable y procedimiento de manipulación.
- Identificar y etiquetar los activos de información existentes, según la importancia que tienen para la institución.

ANÁLISIS DE RIESGO

- Identificar y evaluar los riesgos a los que está expuesto el Servicio en de los activos de información e implementar medidas para su control.
- Identificar aquellos activos de información que requieren de una protección adicional.
- Identificar accesos, modificación y utilización de activos sin autorización o detección.

CAPACITACIÓN Y DIFUSIÓN AL PERSONAL

- Concientizar y sensibilizar a todo el personal de la relevancia de los activos de información y de la seguridad que deben tener éstos.
- Capacitar a través de talleres, charlas, cursos y seminarios, en temáticas relacionadas a la seguridad, generación, manejo y resguardo de los activos de información relevantes para la institución.
- Proveer de material de apoyo (documentos, manuales y/o textos de referencia) en relación a la seguridad de los activos de información.
- Generar y coordinar instancias de difusión y sensibilización masiva respecto de la importancia de la seguridad de la información en el servicio.
- Publicar toda la documentación relativa a la seguridad de la información, a través de la intranet y/o sitio web institucional.

5.- PROTECCIÓN DE LA INFROMACIÓN

En el Gobierno Regional Metropolitano de Santiago se reconoce expresamente la importancia de la información y de los sistemas de información, así como de la necesidad de su protección, por constituir un activo estratégico y vital, hasta el punto de poder llegar a poner en peligro la continuidad del Servicio, o al menos suponer daños muy importantes, si se produjera una pérdida irreversible de determinados datos.

Los accesos y usos de la información, por tanto, estarán en línea con lo que se indica en la presente política y en las leyes, decretos, normas, instructivos, estándares y procedimientos relativos a la seguridad de la información, en especial los siguientes:

- Decretos Supremos N° 77/2004; N° 81/2004 ; N° 83/2004; N° 93/2006: N° 100/2006; N° 158/2007;
- Leyes N° 17.336/2004; N° 19.223/1993; N° 19.628/1999; N° 19.799/2002; N° 19.927/2004; N° 20.285/2008;
- Instrucciones I.P. N° 5/2001; I.P. N° 6/2008; I.P. N° 8/2008;
- Norma Chilena 27.001 (Nch-ISO 27001,Of 2013).

En la práctica se generarán las instancias para que se pueda establecer la separación de funciones y revisión independiente de las operaciones o transacciones realizadas cuando sea necesario, a partir de los registros, de quién ha hecho qué, cuándo y desde dónde.

En previsión de la comisión de errores, omisiones, fraudes o delitos, y tratando de detectar la posible existencia de anomalías lo antes posible, se fomentará la difusión de información y se promoverá la formación en seguridad entre empleados y colaboradores.

Algunos de los riesgos frente a los que se deberán establecer controles adecuados y razonables, tanto preventivos, como de detección y correctivos son: errores y omisiones, sabotajes, vandalismo, espionaje industrial, trasgresión de la privacidad y tráfico de datos, acciones de otros agentes externos no autorizados, y cualesquiera otros que puedan influir en que la información no sea exacta, completa, en definitiva integra, o no esté disponible dentro del tiempo fijado.

Se establecerán los medios necesarios y adecuados para la protección de personas, datos, programas, equipos, instalaciones, documentación y otros soportes que contengan información, y en general de cualquier activo del Gobierno Regional Metropolitano de Santiago.

En el caso de baja del empleado o contratado deberá entregar llaves, tarjetas de acceso, material del Servicio, equipos y cualquier tipo de información, y se eliminarán o bloquearán sus códigos de usuario de acceso a los sistemas; en el caso de baja disciplinaria, y si hubiera sospecha, se analizará si ha podido obtener copias, en papel o en otro soporte, de información clasificada, o haber introducido variaciones no autorizadas a programas de computador

6.- RESPONSABILIDADES

La responsabilidad de la seguridad de la información es de todo el personal del Servicio, lo que no obsta a que cada funcionario o usuario asuma su parte de responsabilidad respecto a los medios que utiliza, según los puntos que se indican en esta política.

Quienes desempeñan funciones relativas a la ***Seguridad de la Información*** y otras de administración relacionadas, serán quienes administren la seguridad.

7.- SEGUIMIENTO Y CONTROL

Deberán realizarse periódicamente, a lo menos una vez cada 3 años o cada vez que se requiera, evaluaciones de riesgos y, en función de las debilidades detectadas, se elaborarán los planes de tratamiento que incorporarán los reforzamientos de controles. Asimismo, se realizarán de auditorías externas cada 3 años de cumplimiento y aseguramiento de los estándares de seguridad.

La revisión de la seguridad, si bien ésta ha de ser una inquietud de todos, recaerá en las funciones tanto al Comité de Seguridad de la Información como del Encargado de Seguridad del Servicio.

Esta política se matizará y desarrollará en un conjunto de normas, instructivos, estándares y procedimientos, según sea necesario y avance la tecnología o se extienda la información a diferentes plataformas.

8.- CONTROL DE VERSIONES

N° Revisión	Fecha Elaboración	Fecha Aprobación	Motivo de Revisión	Páginas Modificadas	Autor
1	10.10.10		Creación Política General de Seguridad	Todas	PFF/CHA
2	02.11.10		Incorporación concepto seguridad en los activos de información y modificación acápite "formato de las políticas"	1-3,9	PFF/CHA
3	18.11.10		Modificación participantes Comité de Seguridad de la información	8-9	PFF
4	02.12.10	10.12.10	Incorporación Política de Seguridad Informática	8	CHA
5	28.09.11		Precisiones solicitadas por la Red de Expertos por Norma ISO 27.002	Todas	PSL
6	11.12.2015		Modificación objetivos de la gestión de seguridad de la información, análisis del riesgo, Norma ISO que aplica y Seguimiento y control	1-3-4-5	CHA

HOJA DE REVISIÓN

FECHA	OBSERVACIONES	ENCARGADO DE SEGURIDAD	FIRMA
21-12-15	REVISAR AÑO 2016	JOSE IGNACIO GUTIERREZ	

HOJA DE ACTUALIZACIÓN

FECHA	HOJAS MODIFICADAS	ENCARGADO DE SEGURIDAD	FIRMA
22-12-2015	1-3-4-5	JOSE IGNACIO GUTIERREZ	