



**DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO INFORMATICA**



**APRUEBA POLITICA PARA LA PRIVACIDAD
Y PROTECCIÓN DE LA INFORMACIÓN E
IDENTIFICACIÓN PERSONAL DEL
GOBIERNO REGIONAL METROPOLITANO
DE SANTIAGO.**

RESOLUCIÓN EXENTA N° 3039

SANTIAGO, 22 DIC 2017

VISTOS:

El Decreto Supremo N° 331/2017 del Ministerio de Interior y Seguridad Pública; las facultades que me concede el Artículo 24 letra ñ) de la Ley N° 19.175, Orgánica Constitucional de Gobierno y Administración Regional; 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; el Decreto N° 83/2005 del Ministerio Secretaría General de la Presidencia sobre seguridad y confidencialidad de los documentos electrónicos; la Resolución N° 1600 de 2008 de la Contraloría General de la República; y

CONSIDERANDO:

- 1.- Que, el indicador de Seguridad de la Información es un instrumento de control de gestión en las instituciones públicas, para la exitosa implementación de un Sistema de Seguridad de la Información;
- 2.- Que, es importante considerar los lineamientos que establece la "Política Nacional de CiberSeguridad", la cual señala como esencial dentro de un Sistema de Gestión de la Seguridad de la Información (SGSI), la gestión del riesgo;
- 3.- Que, la gestión del riesgo permite la identificación de amenazas, valoración y priorización de controles que ayudan a mitigar los mismos, detectados en la institución;
- 4.- Que, siempre existirá un riesgo residual con el cual hay que convivir como institución, pero es importante establecer el número de controles que mitiguen éstos, hasta el nivel que el riesgo residual sea aceptable.

JM

16177850



**DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO INFORMATICA**



5.- Que, es decisivo que cada institución comprenda que el número de controles que decida implementar, será a partir del resultado del perfil de riesgos que cada servicio enfrenta;

6.- Que, un riesgo de seguridad de la información corresponde a una amenaza potencial que podría afectar activos de información, vinculados a los procesos de soporte institucional y/o a los procesos de provisión de Productos Estratégicos (bienes y servicios) establecidos en las definiciones estratégicas institucionales (Formulario A1 DIPRES), y por tanto causar daño a la organización;

7.- Que, los servicios deben determinar cuáles son los riesgos de seguridad que afectan sus productos estratégicos del formulario A1 DIPRES, ello permite priorizar qué controles de la Norma deberán ser implementados para mitigar éstos;

RESUELVO:

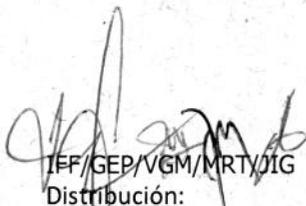
1.- **DÉJESE** sin efecto la Resolución N° 3005 del 29 de noviembre de 2016, que aprobó la Política para la Privacidad y Protección de la Información e Identificación Personal del Gobierno Regional Metropolitana.

2.- **APRUEBASE** la Política para la Privacidad y Protección de la Información e Identificación Personal del Gobierno Regional Metropolitano de Santiago.

ANOTESE Y PUBLIQUESE



**JUAN PABLO GOMEZ RAMIREZ
INTENDENTE (S)
REGION METROPOLITANA DE SANTIAGO**


IFF/GEP/VGM/MRT/JIG
Distribución:

- Funcionario Gobierno Regional Metropolitano de Santiago
- Honorarios Gobierno Regional Metropolitano de Santiago
- Comité de Seguridad de la Información
- Oficina de Partes



GOBIERNO REGIONAL METROPOLITANO – SSI

**POLÍTICA PARA LA PRIVACIDAD Y PROTECCIÓN DE LA
INFORMACIÓN E IDENTIFICACIÓN PERSONAL**

Página 1 de 9

Versión: 03

Código: POL-SSI-006

Fecha: 09/11/2017

Política para la privacidad y protección de la información e identificación personal

Toda versión impresa de este documento se considera como Copia No Controlada

000003



1 INDICE

1	INDICE.....	2
2	OBJETIVOS.....	3
3	ALCANCE.....	3
4	ROLES Y RESPONSABILIDADES.....	3
5	CONTROL NORMATIVO SSI.....	4
6	REGULACIÓN.....	4
7	DEFINICIONES.....	5
8	APLICACION DE LA POLITICA.....	6
8.1	Datos personales.....	6
8.2	Datos personales destinados para ser usadas por el Servicio.....	6
8.3	Entrega de datos o información a terceros.....	6
8.4	Seguridad de la información.....	6
9	REGISTRO DE CONTROL.....	7
10	DIFUSIÓN.....	7
11	REVISIÓN.....	7
12	APROBACIÓN.....	8
13	REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES.....	9



GOBIERNO REGIONAL METROPOLITANO – SSI

**POLÍTICA PARA LA PRIVACIDAD Y PROTECCIÓN DE LA
INFORMACIÓN E IDENTIFICACIÓN PERSONAL**

Página 3 de 9

Versión: 03

Código: POL-SSI-006

Fecha: 09/11/2017

2 OBJETIVOS

Garantizar el uso apropiado y la protección de los datos e información de carácter personal que pudieran almacenarse en las distintas plataformas, tanto informáticas, como en archivos físicos o digitales, del Gobierno Regional Metropolitano, a través de la implementación de políticas de resguardo, confidencialidad y responsabilidad del uso y registro de información personal, tanto de las autoridades, encargados y jefaturas, como de cada funcionario del servicio.

La protección de datos personales, esta garantiza en la ley 19.628 sobre la vida privada, cuya finalidad es, asegurar a las personas un espacio de control sobre su identidad, y de libre manifestación de su personalidad, considerando la protección sobre la recogida, el almacenamiento, la utilización y la transmisión de los datos personales. Por tanto, es deber de este servicio cumplir con las normativas vigentes, y asegurar el correcto uso de la información considerada personal, confidencial, sensible y privada, en los sistemas de información del Gobierno Regional Metropolitano, sean digitales o físicos.

3 ALCANCE

Lo establecido en esta política, es aplicable a todos los funcionarios del Gobierno Regional Metropolitano de Santiago, no importando su calidad jurídica, estén o no involucrados en el proceso de Seguridad de la Información, y tengan o no participación directa en los sistemas informáticos, sin perjuicio de las responsabilidades específicas de quienes participan de forma directa en los dichos procesos digitales y físicos.

4 ROLES Y RESPONSABILIDADES

Departamento de Informática: será el encargado de proveer de sistemas de seguridad de la información en las plataformas digitales de uso institucional, su correcto resguardo y operatividad, así como también, deberá asegurar la protección a toda la información contenida en medios electrónicos que utilizan los funcionarios del servicio, a través de herramientas informáticas seguras. Asimismo, denunciar conductas incorrectas que transgredan el resguardo de información personal, y vulneren la vida privada de las personas, como también si se detecta alguna conducta en contra de la probidad administrativa, respecto de todos los medios electrónicos que son de su responsabilidad, por ejemplo: celulares institucionales, computadores, Tablet, plataformas digitales, páginas web, etc.

Comité de Seguridad de la información: velará por impulsar medidas de seguridad de la información, difundir y capacitar en torno a las materias de protección de datos personales, y, establecer lineamientos sobre materias relacionadas a seguridad de la información.

Toda versión impresa de este documento se considera como Copia No Controlada

000005



GOBIERNO REGIONAL METROPOLITANO – SSI

POLÍTICA PARA LA PRIVACIDAD Y PROTECCIÓN DE LA INFORMACIÓN E IDENTIFICACIÓN PERSONAL

Página 4 de 9

Versión: 03

Código: POL-SSI-006

Fecha: 09/11/2017

Unidad de Transparencia: Esta unidad será la responsable de subir toda la información digital a la Plataforma de Transparencia.

Departamento Gestión de personas: será responsable de dar a conocer de toda la documentación en lo relativo a la privacidad y protección de la información personal.

Departamento de Gestión Documental: será responsable por el envío de correos con documentos que pudieran tener información sensible.

Funcionarios: todo funcionario es responsable de la información que almacena, administra y difunde, sea o no, relativa a sus funciones, propias o de terceros, debiendo asegurar que, su uso, se rija a la normativa vigente. También, de informar, cuando corresponda, si presencia conductas inapropiadas o incoherentes a las políticas de seguridad de la información y la probidad administrativa. Además, deberá ser responsable de los documentos personales, que no dicen relación con sus funciones, que almacene en medios digitales o físicos.

5 CONTROL NORMATIVO SSI

El siguiente procedimiento tiene por finalidad dar cumplimiento a los siguientes controles de la política NCh-ISO27001.Of2013

Código del Control	Identificación del Control	Requisito de control
A.18.01.04	Privacidad y protección de la información de identificación personal	Se debe asegurar la privacidad y protección de la información de identificación personal, como se exige en la legislación y regulaciones pertinentes.

6 REGULACIÓN

La Política para la Privacidad y Protección de la Información e Identificación Personal se complementará con todos los instrumentos sobre Seguridad de la Información emitidos por el Gobierno Regional Metropolitano de Santiago, y toda aquella normativa legal relacionada vigente.

Esta política será impulsada por el Comité de Seguridad de la Información, y su cumplimiento estará regulado por el **Reglamento sobre Infracciones al Sistema de Seguridad de la Información**, sin perjuicio, de las sanciones emanadas del procedimiento administrativo correspondiente.

Toda versión impresa de este documento se considera como Copia No Controlada

000006

	GOBIERNO REGIONAL METROPOLITANO – SSI POLÍTICA PARA LA PRIVACIDAD Y PROTECCIÓN DE LA INFORMACIÓN E IDENTIFICACIÓN PERSONAL	Página 5 de 9
		Versión: 03
		Código: POL-SSI-006
		Fecha: 09/11/2017

7 DEFINICIONES

Dato Personal: cualquier información de personas naturales, que permita identificar al titular, ya sea información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo. Es decir, todo antecedente que permita identificar directa o indirectamente a una persona, ya sea a través de uno o varios elementos específicos, tales como: características de su identidad física, económica, cultural, etc. como por ejemplo: dirección, teléfono, rut, etc. Para estos efectos, se entenderá además como dato personal, todo antecedente almacenado en los sistemas digitales y físicos, de cada persona, que no tengan directa relación con la función que desempeñan.

Dato Sensible: o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

Seguridad de la Información: 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. Es decir, las medidas, instrumentos, herramientas o políticas implementadas para asegurar el resguardo de la información personal.

Comunicación o transmisión de datos: dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.

Uso de Datos: cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

Almacenamiento de datos: la conservación o custodia de datos en un registro, o cualquier instrumento automatizado o no.

Documentos personales: se entenderá en esta política, documentos de carácter personal, que cada funcionario almacene en cualquier medio digital o físico, que no tenga relación con lo laboral, del cual tiene propiedad, y es responsable. Lo anterior, sin perjuicio de que su contenido pueda estar sujeto a normas de probidad administrativa.

Funcionarios: personas contratadas por el Gobierno Regional Metropolitano de Santiago, indistintamente su calidad jurídica, que haga uso de la información del servicio, y sus medios electrónicos, sin perjuicio de la aplicabilidad legal de la responsabilidad administrativa cuando corresponda.

Toda versión impresa de este documento se considera como Copia No Controlada

000007

	GOBIERNO REGIONAL METROPOLITANO – SSI POLÍTICA PARA LA PRIVACIDAD Y PROTECCIÓN DE LA INFORMACIÓN E IDENTIFICACIÓN PERSONAL	Página 6 de 9
		Versión: 03
		Código: POL-SSI-006
		Fecha: 09/11/2017

8 APLICACION DE LA POLITICA

8.1 Datos personales

El Gobierno Regional Metropolitano, en cumplimiento con la normativa vigente, en particular la Ley 19.628, sobre la protección de la vida privada y protección de los datos, garantizará su confidencialidad tanto a los funcionarios, cualquiera sea su calidad jurídica, proveedores y contratistas, que toda información personal entregada al servicio no será utilizada sin su consentimiento y que solo usará esta información para fines propios de la gestión administrativa del Servicio.

8.2 Datos personales destinados para ser usadas por el Servicio

Respecto de quienes hagan uso de las plataformas digitales del Gobierno Regional Metropolitano, a través de los formularios electrónicos de nuestro sitio web y en los campos que se indique para la postulación electrónica, como quienes aplican de forma presencial mediante formularios físicos y suministran información personal como: nombre, Rut, correo electrónico, número telefónico, etc., lo hacen de manera libre y voluntaria y facilitan sus datos personales para que sean usados para la postulación de proyectos propios del Servicio.

En este sentido, el Gobierno Regional Metropolitano, establece que no utiliza sistemas automáticos de recolección de cookies

De esta forma, el Servicio asegurará la máxima reserva y protección de datos personales, comprometiéndose a no entregar información personal alguna.

8.3 Entrega de datos o información a terceros

El Gobierno Regional Metropolitano, en virtud de lo antes expuesto, no compartirá información con terceros y solo podrá entregarse en razón de un mandato legal o una orden emanada de los tribunales de Justicia que así lo establezcan.

8.4 Seguridad de la información

El Gobierno Regional Metropolitano, ha establecido y adoptado los niveles de seguridad pertinentes para la protección de datos personales tal como lo establece la legislación vigente y ha instalado todos los medios tecnológicos para evitar la pérdida de información, mal uso, modificación, acceso no autorizado y robo de información personal facilitado por los usuarios.

De esta forma se da cumplimiento a lo dispuesto en la Ley.

	GOBIERNO REGIONAL METROPOLITANO – SSI POLÍTICA PARA LA PRIVACIDAD Y PROTECCIÓN DE LA INFORMACIÓN E IDENTIFICACIÓN PERSONAL	Página 7 de 9
		Versión: 03
		Código: POL-SSI-006
		Fecha: 09/11/2017

9 REGISTRO DE CONTROL

El Departamento de Gestión de Personas y la Unidad de Transparencia deberán emitir un informe que dé cuenta de lo siguiente:

- A.18.01.04 informe de resguardo para la privacidad y protección de la información de identificación personal

El informe deberá ser enviado al Encargado de Seguridad de manera semestral.

Todo documento deberá venir formalizado por quienes sean responsables del proceso (Debe contener logo del Servicio, fecha de creación, nombre, cargo y firma del responsable)

10 DIFUSIÓN

El presente documento será difundido a través de correo electrónico a todo el personal del Servicio, así como también una copia de éste será publicada en la intranet Institucional.

11 REVISIÓN

La siguiente Política será revisada, evaluada y/o actualizada según corresponda una vez al año por el Comité de Seguridad de la Información o cuando el mismo estime conveniente, en cuanto a su funcionamiento y correcta aplicación en la Institución.



GOBIERNO REGIONAL METROPOLITANO – SSI

**POLÍTICA PARA LA PRIVACIDAD Y PROTECCIÓN DE LA
INFORMACIÓN E IDENTIFICACIÓN PERSONAL**

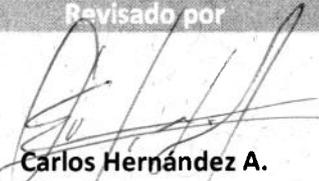
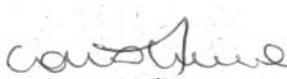
Página 8 de 9

Versión: 03

Código: POL-SSI-006

Fecha: 09/11/2017

12 APROBACIÓN

Elaborado por	Revisado por	Aprobado por
 <p>Paulina Vilches Vásquez Encargada de Transparencia</p>	 <p>Carlos Hernández A. Analista Departamento de Informática</p>	 <p>Mayuri Reyes Torres Presidente Comité de Seguridad</p>
	 <p>Carolina Hidalgo M. Jefa Departamento de Gestión Institucional</p>	

Toda versión impresa de este documento se considera como Copia No Controlada

000010



GOBIERNO REGIONAL METROPOLITANO – SSI

**POLÍTICA PARA LA PRIVACIDAD Y PROTECCIÓN DE LA
INFORMACIÓN E IDENTIFICACIÓN PERSONAL**

Página 9 de 9

Versión: 03

Código: POL-SSI-006

Fecha: 09/11/2017

13- REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES

Versión	Autor	Página o Secciones	Fecha Modificación	Motivo
01	Paulina Vilches	todas	11-08.16	Creación Documento
02	Carlos Hernández	4 y 7	10-07-17	Modificación de documento para cumplimiento a directrices de la red de expertos SSI. <ul style="list-style-type: none">• Se incorpora control normativo SSI• Se incorpora registro de control
03	Mauricio Marín	6	09/11/2017	Se incorpora aplicación de la política

Toda versión impresa de este documento se considera como Copia No Controlada

000011

Acta de Reunión Comité de Seguridad de la Información

Asistentes:

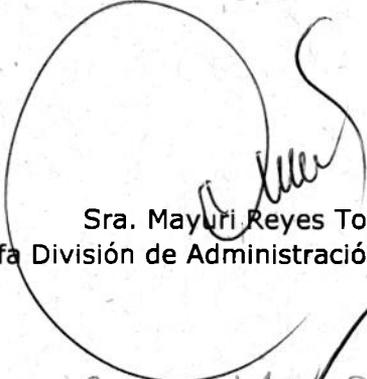
- Sra. Mayuri Reyes Torres - Jefa División de Administración y Finanzas
- Srta. Carolina Hidalgo Mandujano – Jefa Departamento de Gestión Institucional
- Sra. Valentina Guerra Monsalve - Jefa Departamento Jurídico
- Sra. María Macarena Miranda Nuñez - Jefa Departamento de Gestión Documental
- Sr. José Ignacio Gutiérrez - Encargado de Seguridad de la información
- Sr. Hector Salinas Murúa – Jefe (s) Departamento de Informática
- Sr. Carlos Hernández Arancibia – Analista Departamento de Informática
- Sr. Mauricio Marín Vera – Analista Departamento de Informática
- Srta. Paulina Vilches Vásquez– Encargada Unidad de Transparencia
- Sr. Juan Catalán Farías – Depto. Servicios Generales
- Sr. Ariel Lagos Vásquez – Prevencionista de Riesgos

Tabla:

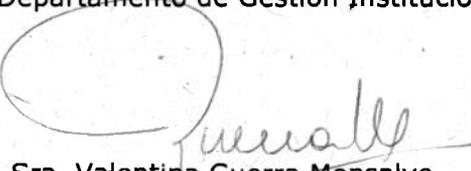
1. Se ratifica al Jefe del Departamento de Informática como Encargado de Seguridad de la Información.
2. Se acuerda incorporación a este Comité de los siguientes funcionarios:
 - a. Jefe Departamento de Servicios Generales
 - b. Jefe Departamento de Gestión de Personas
 - c. Prevencionista de Riesgos Institucional
3. Se revisa y evalúa la correcta ejecución de los contratos de mantenimiento del Gobierno Regional Metropolitano (GORE RM).
4. Se revisan y validan por parte de este Comité los siguientes documentos:
 - Política General de Seguridad de la Información
 - Resolución Encargado de Seguridad de la Información
 - Resolución de nombramiento Comité de Seguridad de la Información
 - Instructivo Correctivo Preventivo
 - Manual de Gestión de Archivos
 - Norma de Acceso a la Red
 - Norma de Eliminación de Activos
 - Norma de Seguridad de la Información para la Gestión de Proyectos
 - Norma de Uso Outsourcing
 - Norma de Trabajo Remoto
 - Norma de Uso Instalación Legal de Software
 - Norma de Uso Identificación y Autenticación

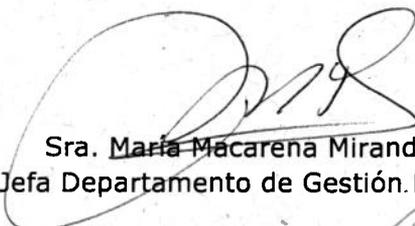
- Norma de Uso Navegación por Internet
 - Norma de Uso para los Equipos Tecnológicos Portátiles
 - Norma de Reutilización y Devolución de Activos
 - Plan de Emergencia Institucional
 - Política de Clasificación de Activos
 - Política de Acceso físico
 - Política de Correo Electrónico
 - Política de Desarrollos de Sistemas
 - Política de Dispositivos Móviles
 - Política de Escritorios y Pantallas Limpias
 - Política de Gestión de Incidentes de Seguridad
 - Política de Gestión de la capacidad
 - Política de la Seguridad Informática
 - Política de Respaldo de la Información
 - Política Gestión de Claves
 - Política Manejo de Activos
 - Política para la Privacidad y Protección de la Información e Identificación Personal
 - Política sobre el Uso de Controles Criptográficos
 - Política y Proceso de Selección de Personal
 - Procedimiento de Control de las Vulnerabilidades Técnicas
 - Protocolo de Control y Tratamiento de SSI
 - Reglamento sobre Infracciones al SSI
5. Se toma conocimiento y valida el informe "Procesamiento y Confidencialidad de los Activos de Información", elaborado por el Encargado del Seguridad de la Información, el cual da cuenta de la no ocurrencia de incidentes de seguridad durante el período 2017.
6. Se informa por parte del Encargado de Seguridad de la Información respecto de la participación en distintas instancias en materias relativas al Sistema de Seguridad de la Información:
- Exposición para el Sector Público de Expertos en materia de Seguridad informática (Subsecretaría del Interior)
 - Reunión bipartita GORE RM-Red de Expertos
 - Jornada de Capacitación Indicador SSI (Ministerio Secretaría General de la Presidencia)
7. Se dan a conocer por parte del Encargado de Seguridad de la información las medidas de difusión del Sistema de Seguridad de la Información a través de:
- Correo electrónico a todo el personal.
 - Banner corporativo en Intranet Institucional.
8. Se acuerda que el Comité de Seguridad tenga una próxima sesión durante el primer semestre del próximo año para evaluar lo reportado durante 2017 y revisar los compromisos 2018.

Aprueban:

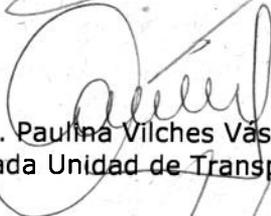

Sra. Mayuri Reyes Torres
Jefa División de Administración y Finanzas

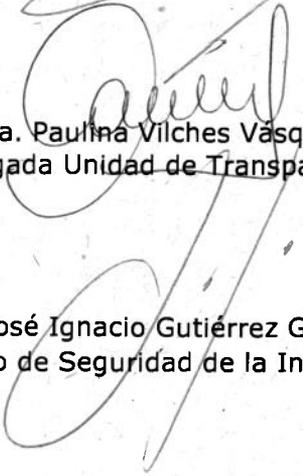

Srta. Carolina Hidalgo Mandujano
Jefa Departamento de Gestión Institucional


Sra. Valentina Guerra Monsalve
Jefa Departamento Jurídico


Sra. María Macarena Miranda Nuñez
Jefa Departamento de Gestión Documental


Sr. Hector Salinas Murúa
Jefe (s) Departamento de Informática


Srta. Paulina Vilches Vásquez
Encargada Unidad de Transparencia


Sr. José Ignacio Gutiérrez García
Encargado de Seguridad de la Información