**DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS**
**DEPARTAMENTO INFORMATICA**

**APRUEBA REGLAMENTO SOBRE INFRACCIONES AL SSI DEL GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO.**

**RESOLUCIÓN EXENTA N°** 3037

**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.

16177853

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° 2999 del 29 de noviembre de 2016, que aprobó el Reglamento sobre Infracciones al Sistema de Seguridad de la Información del Gobierno Regional Metropolitana.

**2.- APRUEBASE** el Reglamento sobre Infracciones al SSI del Gobierno Regional Metropolitano de Santiago.

**ANOTESE Y PUBLIQUESE**

INTENDENCIA REGION METROPOLITANA
INTENDENTE

**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

# Reglamento sobre Infracciones al SSI

# 1 INDICE

1 INDICE ..... 2
2 OBJETIVO ..... 3
3 OBJETIVO ESPECIFICO ..... 3
4 ALCANCE ..... 4
5 ROLES Y RESPONSABILIDADES ..... 4
6 PREREQUISITO ..... 4
7 SANCION POSITIVA ..... 5
8 CONTROL NORMATIVO SSI ..... 5
9 TÍTULO ÚNICO ..... 5
10 REGISTRO DE CONTROL ..... 7
11 DIFUSIÓN ..... 7
12 REVISIÓN ..... 7
13 APROBACIÓN ..... 8
14 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES ..... 9

## 2 OBJETIVO

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.

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

## 3 OBJETIVO ESPECIFICO

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 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.

Este reglamento 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.

## 5 ROLES Y RESPONSABILIDADES

El Encargado de Seguridad deberá evaluar y solicitar a la Jefatura pertinente cualquier procedimiento de sanción en caso de existir una infracción.

Las Jefaturas deberán ser responsables de detectar posibles fallas en la Seguridad de la Información e informarlas al Encargado de Seguridad a la brevedad.

Cada usuario será responsable de velar por la seguridad de los activos del servicio y denunciar alguna falta o mal procedimiento según indiquen las Políticas, Normas u otros documentos aprobados por el Servicio en materia de Seguridad de la Información.

Las denuncias podrán realizarse mediante el botón de "DENUNCIA" que se ha incorporado en la Intranet institucional o directamente en el link http://intranet.gobiernosantiago.cl/denuncias.

## 6 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".**

## 7 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.

## 8 CONTROL NORMATIVO SSI

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

| Código del Control | Identificación del Control | Requisito de control |
|---|---|---|
| A.07.02.03 | Proceso disciplinario | Debe existir un proceso disciplinario formal y sabido por los empleados para tomar acciones en contra de los empleados que han cometido una infracción a la seguridad de la información. |

## 9 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, instructivos y políticas, aprobadas por el Comité de Seguridad de este Servicio.

**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.

## 10 REGISTRO DE CONTROL

El Encargado de Seguridad del Servicio deberá emitir un informe que dé cuenta de las solicitudes recibidas para:

- A.07.02.03 Informe de Procesos disciplinarios realizados a raíz de denuncias o infracciones detectadas a la Seguridad de la Información

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)

## 11 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.

## 12 REVISIÓN

El siguiente reglamento será revisado, evaluado y/o actualizado 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.

## 13 APROBACIÓN

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

## 14 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES

| Versión | Autor | Página o Secciones | Fecha Modificación | Motivo |
|---|---|---|---|---|
| 01 | Susana Guzmán | todas | 09-11-16 | Creación Documento |
| 02 | Carlos Hernández | todas | 01-08-17 | Modificación de documento para cumplimiento a directrices de la red de expertos SSI.<br>• Se modifica diseño del documento<br>• Se incorpora control normativo SSI<br>• Se incorpora registro de control |

# 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 Autentificación

- 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