



**DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS  
DEPARTAMENTO INFORMÁTICA**



**APRUEBA NORMA DE USO INSTALACIÓN  
LEGAL DE SOFTWARE DEL GOBIERNO  
REGIONAL METROPOLITANO DE  
SANTIAGO.**

**RESOLUCIÓN EXENTA N° 3035**

**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.

*9/16*

*16177955*



**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° 2857 del 30 de diciembre de 2011, que aprobó la Norma de Uso Instalación Legal de Software del Gobierno Regional Metropolitana.

2.- **APRUEBASE** la Norma de Uso Instalación Legal de Software del Gobierno Regional Metropolitano de Santiago..

**ANOTESE Y PUBLIQUESE**



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

IFF/GEP/VGM/MRT/JIS

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**

**NORMA DE USO  
INSTALACIÓN LEGAL DE  
SOFTWARE**

Página 1 de 9

Versión: 03

Código: NOR-SSI-011

Fecha: 25/09/2017

# **NORMA DE USO INSTALACIÓN LEGAL DE SOFTWARE**

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

**000003**



1 INDICE

1 INDICE.....2

2 OBJETIVO.....3

3 ALCANCE.....3

4 ROLES Y RESPONSABILIDADES.....3

5 CONTROL NORMATIVO SSI.....4

6 DESARROLLO DE LA NORMA .....4

6.1 Uso de programas utilitarios .....4

6.2 Control de Software en los sistemas operacionales.....5

6.3 Restricciones sobre las instalaciones de software .....5

6.4 Uso de programas de utilidad privilegiados.....6

7 REGISTRO DE CONTROL.....6

8 DIFUSIÓN.....7

9 REVISIÓN .....7

10 APROBACIÓN .....8

11 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES .....9

	<b>GOBIERNO REGIONAL METROPOLITANO – SSI</b>  <b>NORMA DE USO  INSTALACIÓN LEGAL DE  SOFTWARE</b>	Página 3 de 9
		Versión: 03
		Código: NOR-SSI-011
		Fecha: 25/09/2017

## 2 OBJETIVO

Definir e indicar a los usuarios, sobre los riesgos que implica la instalación de software no autorizado por el Gobierno Regional Metropolitano de Santiago, los cuales exponen a pérdida de información, daño a los recursos disponibles, como también problemas jurídicos tanto nacionales como internacionales, porque son estos software o aplicaciones no autorizadas las que pueden dar pie a vulnerabilidades o bien trasgredir los derechos de propiedad.

## 3 ALCANCE

Las normas mencionadas en el presente documento aplican a todos los funcionarios del Gobierno Regional Metropolitano , proveedores, contratistas, personal que esté vinculado con las firmas que presten servicios al Gobierno Regional Metropolitano o que estén relacionados. Se incluye además, todas las dependencias que son parte de la institución o a quienes transiten por la red digital del Gobierno Regional Metropolitano de manera de evitar la instalación de Programas, software o utilitarios no licenciados para el uso en el Servicio

## 4 ROLES Y RESPONSABILIDADES

El Departamento de Informática será el encargado de velar por el buen uso de los Software disponibles.

Todo usuario deberá ceñirse a usar estrictamente el o los software que el Departamento de Informática establezca o configure en cada dispositivo

El Departamento de Informática revisará periódicamente el quipos computacionales a fin de que no se hayan instalados Software sin autorización, esto mediante software de detección o presencialmente según corresponda

El Departamento de Informática, deberá instalar un software que detecte y prevenga la intrusión de códigos maliciosos, de manera de prevenir toda infección y posterior propagación de códigos maliciosos

	<b>GOBIERNO REGIONAL METROPOLITANO – SSI</b>  <b>NORMA DE USO  INSTALACIÓN LEGAL DE  SOFTWARE</b>	Página 4 de 9
		Versión: 03
		Código: NOR-SSI-011
		Fecha: 25/09/2017

## 5 CONTROL NORMATIVO SSI

La siguiente norma 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.09.04.04	Uso de programas utilitarios privilegiados	Se debiera restringir y controlar estrictamente el uso de los programas utilitarios que pueden estar en capacidad de anular el sistema y los controles de la aplicación.
A.12.05.01	Control del software en sistemas operacionales	Se deben implementar los procedimientos para controlar la instalación de software en los sistemas operacionales.
A.12.06.02	Restricciones sobre la instalación de software	Se deben establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.

## 6 DESARROLLO DE LA NORMA

### 6.1 Uso de programas utilitarios

Cualquier instalación de software o programa utilitario que sea requerido por el usuario y que no se encuentre en la lista de software proporcionado por el Gobierno Regional Metropolitano de Santiago, deberá ser solicitada previamente vía correo electrónico, oficio, memo, u otro, para su posterior evaluación por el Departamento de Informática.

Para la creación y desarrollo de documentos electrónicos del Gobierno Regional Metropolitano de Santiago, los usuarios deberán utilizar software debidamente licenciado.

El funcionario, deberá considerar lo siguiente:

Los Usuarios no podrán instalar software en los equipos computacionales de la red del Gobierno Regional Metropolitano de Santiago sin la debida aprobación del Departamento de Informática.

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

000006

	<b>GOBIERNO REGIONAL METROPOLITANO – SSI</b>  <b>NORMA DE USO</b> <b>INSTALACIÓN LEGAL DE</b> <b>SOFTWARE</b>	Página 5 de 9
		Versión: 03
		Código: NOR-SSI-011
		Fecha: 25/09/2017

## 6.2 Control de Software en los sistemas operacionales

El software que no ha sido facilitado por el Gobierno Regional Metropolitano de Santiago, deberá ser solicitado al Departamento de Informática. Posteriormente de su autorización, deberá ser analizado por el área de seguridad y distribuido por el área de soporte.

El Departamento de Informática será el encargado de obtener el licenciamiento de las aplicaciones solicitadas y evaluación en busca de conflictos de compatibilidad y estabilidad del sistema, para luego realizar la instalación y distribución, según corresponda.

Será este Departamento quien además deberá guardar y llevar el registro de la cantidad de licencias usadas y de las disponibles, a fin de proveerlas de acuerdo al número de funcionarios del Gobierno Regional Metropolitano

Las actualizaciones de software proporcionados por el Gobierno Regional Metropolitano de Santiago, se realiza de forma centralizada y automatizada, por lo que el usuario no deberá realizar esta operación, salvo una solicitud expresa de la Unidad de Informática.

En el caso de los Software de Antivirus, su actualización será centralizada, es decir, cada máquina se actualizará en forma automatizada y apuntando directamente al servidor antivirus de manera de no congestionar la salida a Internet. Lo propio sucederá con la actualización de productos Microsoft como Sistema Operativos y herramientas o programas utilitarios de oficina, los que apuntarán a un Servidor que dispondrá de todas las actualizaciones vigentes por parte de Microsoft aplicando todos los parches ofrecidos para eliminar o reducir debilidades .

Los sistemas que dejen de ser actualizados por parte del proveedor deberían ser considerados como riesgosos por lo tanto se sugiere su actualización a versiones superiores o mejoradas previa prueba de funcionalidad con los procesos actuales del Servicio.

## 6.3 Restricciones sobre las instalaciones de software

Conforme a lo descrito a la normativa vigente:

El Departamento de Informática controlará la instalación de software no debidamente licenciado por el Gobierno Regional Metropolitano de Santiago, evitando el mal uso de la infraestructura disponible. Lo descrito anteriormente, se realiza con el fin de proporcionar información para el caso de revisiones y auditorias que requiera la organización.

El Departamento de Informática creará GPO para controlar la instalación de Software no autorizados, de manera que los usuarios no puedan instalar programas o utilitarios sin autorización, para esto se considerará el principio de menores privilegios.

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

000007

	<b>GOBIERNO REGIONAL METROPOLITANO – SSI</b>  <b>NORMA DE USO</b> <b>INSTALACIÓN LEGAL DE</b> <b>SOFTWARE</b>	Página 6 de 9
		Versión: 03
		Código: NOR-SSI-011
		Fecha: 25/09/2017

El Departamento de Informática, a través de su unidad de Soporte, hará levantamientos permanentes de todas las máquinas de manera de revisar que todo software instalado esté debidamente licenciado, para esto se usará una herramienta partner de Microsoft que hará un escáner remoto a todo equipo conectado a la LAN del GORE y que será totalmente transparente e invisible para los usuarios. En el caso de detectar algún software no autorizado, se procederá a consultar la necesidad de este para luego establecer su regularización y de esta manera cumplir con lo establecido de evitar instalaciones no autorizadas.

#### 6.4 Uso de programas de utilidad privilegiados

El Departamento de Informática deberá revisar todos los equipos computacionales de los usuarios de manera de prevenir el uso de programas de utilidad privilegiados evitando que puedan modificar o anular los sistemas operativos y los controles de operación.

El uso y acceso a estos programas utilitarios privilegiados debe ser autorizado sólo a los administradores de sistema, técnicos o analistas informáticos que por la naturaleza de sus funciones requieran acceso.

Para esto la Unidad de soporte restringirá los privilegios de los usuarios en los computadores, eliminando o deshabilitando todos los programas de utilidad innecesarios para los usuarios y negando el acceso de estos a los sistemas donde se requiere una segregación de derechos de uso.

En caso de necesitarse el uso de unos de estos programas de utilidad privilegiados, su uso quedará restringido a los administradores del sistema mediante una clave autorizada por el Departamento de Informática.

## 7 REGISTRO DE CONTROL

El Departamento de Informática deberá emitir un informe que dé cuenta de:

- A.09.04.04 Informe de configuración de equipos con privilegios restringidos
- A.12.05.01 Informe de actualizaciones de sistemas operacionales
- A.12.06.02 informe de Implementación de GPO Software Restriction Policies

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)

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

**000008**

 SERVICIO DE TRANSPARENCIA Y GESTIÓN SANTIAGO	<b>GOBIERNO REGIONAL METROPOLITANO – SSI</b>  <b>NORMA DE USO INSTALACIÓN LEGAL DE SOFTWARE</b>	Página 7 de 9
		Versión: 03
		Código: NOR-SSI-011
		Fecha: 25/09/2017

## 8 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.

## 9 REVISIÓN

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



GOBIERNO REGIONAL METROPOLITANO – SSI

**NORMA DE USO  
INSTALACIÓN LEGAL DE  
SOFTWARE**

Página 8 de 9

Versión: 03

Código: NOR-SSI-011

Fecha: 25/09/2017

10 APROBACIÓN

Elaborado por

Revisado por

Aprobado por

**Carlos Hernández A.**  
Analista Departamento de  
Informática

**José Ignacio Gutiérrez G.**  
Encargado de Seguridad SSI

**Paulo Mendoza R.**  
Encargado Unidad de Soporte

**Mayuri Reyes Torres**  
Presidente Comité de Seguridad

**Carolina Hidalgo M.**  
Jefa Departamento de  
Gestión Institucional

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

000010

	<b>GOBIERNO REGIONAL METROPOLITANO – SSI</b>  <b>NORMA DE USO  INSTALACIÓN LEGAL DE  SOFTWARE</b>	Página 9 de 9
		Versión: 03
		Código: NOR-SSI-011
		Fecha: 25/09/2017

## 11 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES

Versión	Autor	Página o Secciones	Fecha Modificación	Motivo
01	Carlos Hernández	todas	09-11-11	Creación Documento
02	Carlos Hernández	todas	10-07-17	Modificación de documento para cumplimiento a directrices de la red de expertos SSI. <ul style="list-style-type: none"> <li>• Se incorpora control normativo SSI</li> <li>• Se incorpora registro de control</li> </ul>
03	Mauricio Marín	todas	25-09-17	Modificación de Formato, se agrega índice, Revisión, Difusión.

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

000011

## **Acta de Reunión Comité de Seguridad de la Información**

### **Asistentes:**

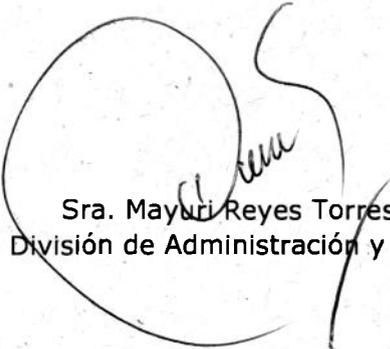
- Sra. Mayuri Reyes Torres - Jefa División de Administración y Finanzas
- Srta. Carolina Hidalgo Mandujano – Jefa Departamento de Gestión Institucional
- Sra. Valentina Guerra Monsalve - Jefa Departamento Jurídico
- Sra. María Macarena Miranda Nuñez - Jefa Departamento de Gestión Documental
- Sr. José 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

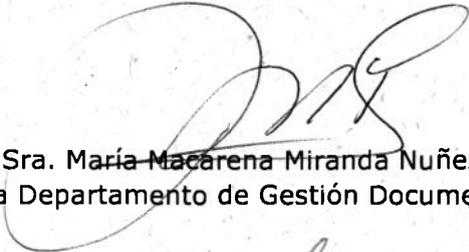
- Norma de Uso Navegación por Internet
  - Norma de Uso para los Equipos Tecnológicos Portátiles
  - Norma de Reutilización y Devolución de Activos
  - Plan de Emergencia Institucional
  - Política de Clasificación de Activos
  - Política de Acceso físico
  - Política de Correo Electrónico
  - Política 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 periodo 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.

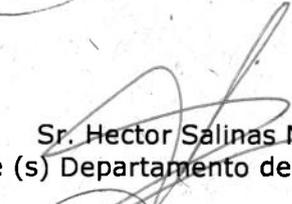
**Aprueban:**

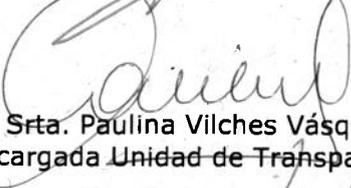
  
Sra. Mayuri Reyes Torres  
Jefa División de Administración y Finanzas

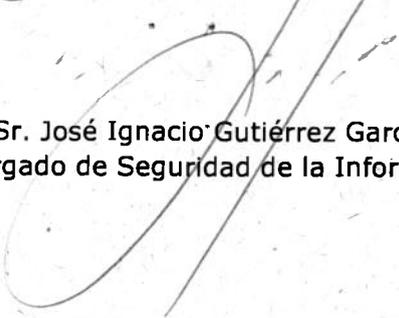
  
Srta. Carolina Hidalgo Mandujano  
Jefa Departamento de Gestión Institucional

  
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