

- **USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS**
 - **CONTROL DEL SOFTWARE EN SISTEMAS OPERACIONALES**
- **RESTRICCION SOBRE LA INSTALCION DE SOFTWARE**

NORMA DE USO INSTALACIÓN LEGAL DE SOFTWARE



GOBIERNO REGIONAL
METROPOLITANO DE
SANTIAGO

GOBIERNO REGIONAL METROPOLITANO – SSI

- **USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS**
 - **CONTROL DEL SOFTWARE EN SISTEMAS OPERACIONALES**
- **RESTRICCION SOBRE LA INSTALCION DE SOFTWARE**

Página 2 de 9

Versión: 08/21

A.09.04.04
A.12.05.01
A.12.06.02

Fecha: 23/11/2021

1 INDICE

1	INDICE	2
2	OBJETIVO	3
3	ALCANCE	3
4	ROLES Y RESPONSABILIDADES	3
5	CONTROL NORMATIVO SSI	4
6	DEFINICION Y MODO DE OPERACION.....	4
6.1	Uso de programas utilitario.....	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 OPERACION	7
8	DIFUSIÓN	7
9	REVISIÓN.....	7
10	FORMALIZACION EXTERNA	7
11	REGISTRO DE REVISION Y ACTUALIZACION HISTORICO	8
12	FORMALIZACION.....	9

 <p>GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO</p>	<p align="center">GOBIERNO REGIONAL METROPOLITANO – SSI</p> <ul style="list-style-type: none"> • USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS <ul style="list-style-type: none"> • CONTROL DEL SOFTWARE EN SISTEMAS OPERACIONALES • RESTRICCION SOBRE LA INSTALCION DE SOFTWARE 	Página 3 de 9
		Versión: 08/21
		A.09.04.04 A.12.05.01 A.12.06.02
		Fecha: 23/11/2021

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 softwares que el Departamento de Informática establezca o configure en cada dispositivo

El Departamento de Informática revisará periódicamente el quipo computacional 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

- **USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS**
 - **CONTROL DEL SOFTWARE EN SISTEMAS OPERACIONALES**
- **RESTRICCION SOBRE LA INSTALCION DE SOFTWARE**

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 DEFINICION Y MODO DE OPERACION

6.1 Uso de programas utilitario

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 solicitado 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.

 <p>GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO</p>	<p align="center">GOBIERNO REGIONAL METROPOLITANO – SSI</p> <ul style="list-style-type: none"> • USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS <ul style="list-style-type: none"> • CONTROL DEL SOFTWARE EN SISTEMAS OPERACIONALES • RESTRICCION SOBRE LA INSTALCION DE SOFTWARE 	Página 5 de 9
		Versión: 08/21
		A.09.04.04 A.12.05.01 A.12.06.02
		Fecha: 23/11/2021

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 y distribuido por la unidad 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 de Informática 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 realizan 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.

 <p>GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO</p>	<p align="center">GOBIERNO REGIONAL METROPOLITANO – SSI</p> <ul style="list-style-type: none"> • USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS <ul style="list-style-type: none"> • CONTROL DEL SOFTWARE EN SISTEMAS OPERACIONALES • RESTRICCION SOBRE LA INSTALCION DE SOFTWARE 	Página 6 de 9
		Versión: 08/21
		A.09.04.04 A.12.05.01 A.12.06.02
		Fecha: 23/11/2021

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.

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.

 <p>GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO</p>	<p>GOBIERNO REGIONAL METROPOLITANO – SSI</p> <ul style="list-style-type: none"> • USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS <ul style="list-style-type: none"> • CONTROL DEL SOFTWARE EN SISTEMAS OPERACIONALES • RESTRICCION SOBRE LA INSTALCION DE SOFTWARE 	Página 7 de 9
		Versión: 08/21
		A.09.04.04 A.12.05.01 A.12.06.02
		Fecha: 23/11/2021

7 REGISTRO DE OPERACION

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 anual.

En caso de no haber movimiento en relación a algún control que se pide informar, deberá reportarse de igual manera señalando que no hubo movimiento por lo que no se pudo demostrar con algún medio de verificación durante el respectivo periodo.

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)

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.

10 FORMALIZACION EXTERNA

Mediante el acta fecha 23 de noviembre año 2021, se aprueba por parte del Comité de Seguridad de la Información, la Norma de Uso de Instalación legal de Software.

- **USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS**
 - **CONTROL DEL SOFTWARE EN SISTEMAS OPERACIONALES**
- **RESTRICCION SOBRE LA INSTALCION DE SOFTWARE**

11 REGISTRO DE REVISION Y ACTUALIZACION HISTORICO

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"> • Se incorpora control normativo SSI • Se incorpora registro de control
03	Mauricio Marín	todas	25-09-17	Modificación de Formato, se agrega índice, Revisión, Difusión.
04	Mauricio Marín V.	4 , 6	1/08/2018	Se agrega en Registro de Control el siguiente párrafo. En caso de no haber movimiento en relación a algún control que se pide informar, deberá reportarse de igual manera señalando que no hubo movimiento por lo que no se pudo demostrar con algún medio de verificación durante el respectivo periodo. Se cambia título 6 por Definición y Modo de Operación Se cambia título 7 por Registro de Operación
05	Matias Benitez	Todas	08-07-2019	Se cambia pie de página.
06	Matias Benitez.	Todas	12-07-2019	Comité SSI revisa y aprueba año 2019.
07	Carlos Hernández	7	15-11-2021	Se agrega capítulo 10 formalización externa Se actualiza índice
08	Carlos Hernández	Todas	23-11-2021	Comité SSI revisa y aprueba año 2021.



GOBIERNO REGIONAL
METROPOLITANO DE
SANTIAGO

GOBIERNO REGIONAL METROPOLITANO – SSI

- USO DE PROGRAMAS UTILITARIOS PRIVILEGIADOS
 - CONTROL DEL SOFTWARE EN SISTEMAS OPERACIONALES
- RESTRICCION SOBRE LA INSTALCION DE SOFTWARE

Página 9 de 9

Versión: 08/21

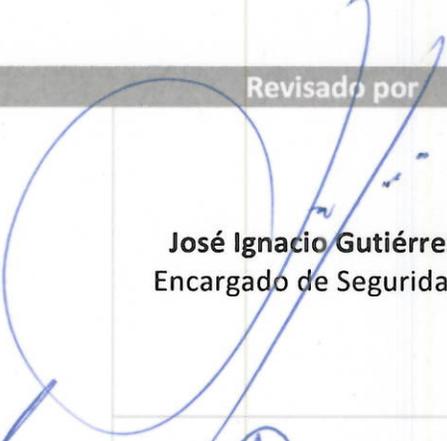
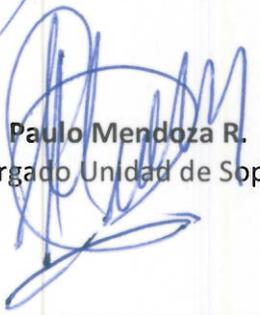
A.09.04.04

A.12.05.01

A.12.06.02

Fecha: 23/11/2021

12 FORMALIZACION

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 T. Presidente Comité de Seguridad
	 Carolina Hidalgo M. Jefa Departamento Planificación y Control Institucional	



GOBIERNO REGIONAL
METROPOLITANO DE
SANTIAGO

**ACTA DE REUNION
COMITÉ DE SEGURIDAD DE LA
INFORMACION**

Página 1 de 3

Fecha 23/11/ 2021

ACTA DE REUNION: Comité de Seguridad de la Información

Objetivo	Situación SSI año 2021
Fecha y Hora	23-11-2021, 15:00
Lugar	Sala de Reunión 2° Piso

PUNTOS DE LA REUNION

1. Bienvenida
2. Actualización de Documentos
3. Vulnerabilidades año 2021
4. 67 vulnerabilidades detectadas en sitios y páginas webs
 - a. Caída de Switch piso 5 - 13 de septiembre 2021
 - b. Caída de Switch piso 1 - 27 de septiembre 2021
5. Envío Correo Phishing
6. Protectores de Pantalla
7. Capacitación SSI
8. Mejoras
 - a. Switch
 - b. GTD Ancho Banda
9. SGD, 0 Papel
10. Eliminación Activos
11. Necesidades Tecnológicas

Aprobación los siguientes documentos

1. **Instructivo correctivo y preventivo contra fallas de energía y otras fallas de servicio**
2. **Manual de gestión de archivos**
3. **Norma de acceso a la Red**
4. **Norma de Eliminación de Activos**
5. **Norma de la Seguridad de la información para la Gestión de Proyectos**
6. **Norma de Outsourcing**
7. **Norma de Trabajo Remoto**
8. **Norma de uso identificación y autenticación**
9. **Norma de uso de instalación legal de software**
10. **Norma de reutilización y devolución de activos**
11. **Plan de Continuidad**
12. **Plan de emergencia Institucional**
13. **Política clasificación de activos**
14. **Política de acceso físico**
15. **Política de correo electrónico e Internet**
16. **Política de Derechos de propiedad Intelectual**
17. **Política de desarrollos de sistemas**

18. Política de dispositivos móviles
19. Política de escritorios y pantallas limpias
20. Política de gestión de incidentes de seguridad
21. Política de gestión de la capacidad
22. Política Gestión de Personas
23. Política de la seguridad informática
24. Política de respaldo de la información
25. Política general de seguridad de la información
26. Política gestión de claves
27. Política manejo de activos
28. Política sobre el uso de controles criptográficos
29. Procedimiento de control de las vulnerabilidades técnicas
30. Procedimiento de Controles de Auditoria de Sistemas de Información
31. Programa de concientización sobre seguridad de la información
32. Protocolo y control de tratamiento de SSI

DESARROLLO DE LA PRESENTACION

José Ignacio da la bienvenida y explica brevemente que es el SSI y las funciones del comité

Se da detalle al comité respecto a las vulnerabilidades CSIRT y las caídas de los switch

Claudio Muñoz y Mayuri Reyes, solicitan al comité la revisión de funcionamiento de cámaras de seguridad del Gore. Debido a problemas que existen actualmente

José Ignacio informa que esta demora se ha debido a que se necesita realizar una revisión inicial de todas las cámaras y su funcionamiento.

Se detallan las mejoras tecnológicas a realizar con carácter de importancia

- Cambios en los switch
- Importancia de dejar el sistema de cámaras en un circuito cerrado fuera de la red

Se recalca la importa de incluir SSI en la inducción a nuevos funcionarios

Se menciona a comité que se enviara cazabobos y que de ahí se realizara una capacitación a quienes caigan en él.

Se establece que el cambio de contraseñas debiera ser cada 6 meses de forma obligatoria empezando con un cambio masivo en marzo. Aplicándose tanto en AD como en sistemas.

Comité solicita que los mensajes de los protectores de pantalla sean un poco más “Rudos” refiriéndose a la gravedad de lo que podría ocasionar una vulneración importante de sistemas

Silvana Torres entrega información

- **Acerca del expurgo de documentos**
- **2022 se enviará soporte en papel a archivo nacional**
- **Se está digitalizando documentación antigua**
- **Menciona que para todo envío a archivo nacional o eliminación debe haber un testigo que vise la correcta digitalización de documentos, transformación digital 21808**

José Ignacio retoma la palabra e indica al comité la importancia dentro de todo el proceso de 0 papel de contar con una cloud de respaldo para toda la gran cantidad de archivos que se está generando

Explica que se continuara siempre con el respaldo en cintas. Indica que se necesita realizar respaldo en cintas como parte de SSI

Se aprueban políticas y documentación SSI

Carolina Hidalgo solicita curso de ciberseguridad a comité y participantes



GOBIERNO REGIONAL
METROPOLITANO DE
SANTIAGO

ACTA DE ASISTENTES
COMITÉ DE SEGURIDAD DE LA
INFORMACION

Página 1 de 1

Fecha 23/11/ 2021

N°	NOMBRE	DEPARTAMENTO O UNIDAD	FIRMA
01	José Ignacio Gutiérrez	Departamento de Informática	
02	Mayuri Reyes T.	División Administración y Finanzas	
03	Héctor Valladares	Departamento Jurídico	
04	Carolina Hidalgo	Departamento Planificación y Control Institucional	
05	Silvana Torres	Departamento de Gestión Documental y Activos	
06	Claudio Muñoz	Departamento de Servicios Generales	
07	Paulo Serrano	Departamento de Gestión de Personas	
08	Luz Magaly Nuñez	Unidad de Transparencia	
09	Ariel Lagos	Prevencionista de Riesgo	
10	VIRGINIA SAAVEDRA	IAF	
11			
12			
13			