

	GOBIERNO REGIONAL METROPOLITANO – SSI PROTOCOLO DE CONTROL Y TRATAMIENTO DE SEGURIDAD DE LA INFORMACION	Página 1 de 11
		Versión: 04
		Código: PROT-SSI-001
		Fecha: 2/08/2018

PROTOCOLO DE CONTROL Y TRATAMIENTO DE SEGURIDAD DE LA INFORMACION

	GOBIERNO REGIONAL METROPOLITANO – SSI PROTOCOLO DE CONTROL Y TRATAMIENTO DE SEGURIDAD DE LA INFORMACION	Página 2 de 11
		Versión: 04
		Código: PROT-SSI-001
		Fecha: 2/08/2018

1 INDICE

1	INDICE	2
2	OBJETIVO	3
3	ALCANCE	3
4	ROLES Y RESPONSABILIDADES	3
5	CONTROL NORMATIVO SSI	4
6	DEFINICIONES Y MODO DE OPERACION.....	4
6.1	Acuerdos	4
6.2	Acceso físico a medios de procesamiento de información	5
6.3	Acceso lógico desde la red Institucional del Gobierno Regional Metropolitano.....	6
6.4	Acceso lógico a la red Institucional del Servicio.....	7
6.5	Acuerdo de Protección de activos.....	8
6.6	Supervisión y revisión	9
7	REGISTRO DE OPERACION.....	9
8	DIFUSIÓN	9
9	REVISIÓN.....	9
10	APROBACIÓN.....	10
11	REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES.....	11

	GOBIERNO REGIONAL METROPOLITANO – SSI PROTOCOLO DE CONTROL Y TRATAMIENTO DE SEGURIDAD DE LA INFORMACION	Página 3 de 11
		Versión: 04
		Código: PROT-SSI-001
		Fecha: 2/08/2018

2 OBJETIVO

El presente documento tiene por finalidad definir y normar los métodos o procedimientos de acceso para el desarrollo de actividades con terceros, de modo de considerar y establecer mecanismos y reglas de protección a la información y al equipamiento tecnológico del Gobierno Regional Metropolitano. Dadas las actuales condiciones de avance en materia de tecnologías de información y comunicación, es que se deben definir los resguardos y garantías que permitan establecer acuerdos de confiabilidad en el desarrollo de actividades por terceros, en cualquiera de sus formas posibles y, ante la necesidad de otorgar permisos de acceso a información institucional, equipos de procesamiento de información o red interna de comunicación del Servicio se deben utilizar las definiciones del presente documento

3 ALCANCE

El presente documento se debe considerar para todo tipo de trabajo que involucre acceso a la información de la Institución, así como facilitar cualquier tipo de acceso a equipamiento de éste en cualquiera de sus formas. Se deben utilizar las normativas que aquí se definen, de modo de asegurar la protección e integridad de la información como de los equipos de procesamiento de información del Servicio.

4 ROLES Y RESPONSABILIDADES

Departamento de Informática

El departamento de Informática dará los permisos y accesos necesarios para personal externo, pertenecientes a proveedores que prestan servicios dentro de las dependencias del Gobierno Regional Metropolitano

A su vez el Departamento de Informática designará a un funcionario de la unidad de soporte para que acompañe al personal externo a cualquiera de las dependencias del Gobierno Regional Metropolitano, en especial a las de acceso restringido.

Departamento de Servicios Generales

EL departamento de Servicios generales deberá identificar, registrar y anunciar las visitas técnicas de proveedores, a fin de poder coordinar con el Departamento de Informática.

 GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO	GOBIERNO REGIONAL METROPOLITANO – SSI PROTOCOLO DE CONTROL Y TRATAMIENTO DE SEGURIDAD DE LA INFORMACION	Página 4 de 11
		Versión: 04
		Código: PROT-SSI-001
		Fecha: 2/08/2018

Los proveedores

Los proveedores deberán ceñirse a estos protocolos de manera de estar de acuerdo con los procedimientos que aquí se describen, de manera de reducir probables riesgos en equipos ajenos a su negocio.

5 CONTROL NORMATIVO SSI

El siguiente procedimiento 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.15.01.01	Política de seguridad de la información para las relaciones con el proveedor	Se deben acordar y documentar, junto con el proveedor, los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso del proveedor a los activos de la organización.
A.15.02.01	Supervisión y revisión de los servicios del proveedor	Las organizaciones deben supervisar, revisar y auditar la entrega del servicio.

6 DEFINICIONES Y MODO DE OPERACION

6.1 Acuerdos

Toda solicitud de acceso a información, equipos de procesamiento de información o red interna de datos por parte de personas externas al Servicio, debe ser solicitada, elevada y canalizada formalmente al encargado de seguridad del Gobierno Regional Metropolitano. En esta se deben especificar los siguientes puntos:

- Motivo del acceso.
- Método requerido.
- Período para el cual se requiere de acceso.
- Horarios en los que se efectúa el acceso.
- Periodicidad.
- Tipo de información o tipo de acceso requerido.
- Responsable de la solicitud de tercero.
- Contraparte interna del Gobierno Regional Metropolitano para el acceso.

Con esta información el encargado de seguridad deberá solicitar antecedentes a la contraparte interna del Gobierno Regional Metropolitano, quien deberá responder formalmente en no más de 15 días hábiles, el ámbito de intervención interno de la solicitud, siendo como mínimo los siguientes:

	GOBIERNO REGIONAL METROPOLITANO – SSI PROTOCOLO DE CONTROL Y TRATAMIENTO DE SEGURIDAD DE LA INFORMACION	Página 5 de 11
		Versión: 04
		Código: PROT-SSI-001
		Fecha: 2/08/2018

- Identificación de las áreas o unidades de procesamiento interna responsables de la información o de orientación que originan el motivo de la solicitud.
- Análisis del valor o criticidad de la información solicitada (Extremo-Alto-Medio-Bajo).
- Definición de intereses involucrados que puedan ser afectados por la solicitud.

Una vez recibidos los antecedentes, el Encargado de Seguridad podrá conformar un comité de evaluación que estará integrado como mínimo por el Encargado de Unidad responsable de la información, Jefatura del Departamento de Informática, Analista del Departamento de Informática y Abogado del Departamento Jurídico, quienes deberán desarrollar un informe de evaluación de solicitud en el ámbito de seguridad de la información y de las disposiciones legales que afectan o involucran en la petición.

De acuerdo a esto, el Encargado de Seguridad procederá a autorizar o rechazar la solicitud, fundamentando la decisión.

Lo anterior con el fin de acordar y documentar las solicitudes de acceso a la información a fin de mitigar los riesgos asociados al acceso de personal externo a los activos de la institución


Al aceptar una solicitud conforme al punto anterior, se debe establecer claramente el tipo de acceso requerido, el cual debe normarse de acuerdo a uno de los siguientes enfoques:

6.2 Acceso físico a medios de procesamiento de información

El acceso al Servicio o a alguna de sus dependencias estará representado en una o más personas las que deberán portar una credencial de visita solo para el piso y lugar correspondiente al desarrollo de sus funciones.

Se evaluará la posibilidad de otorgar una credencial permanente en caso que el acceso sea mayor a 1 mes. El Departamento de Informática en conjunto con el Encargado de Unidad responsable de la información realizará:

- a) Acta de recepción de los bienes inventariarles involucrados para uso del tercero en el Gobierno Regional Metropolitano.
- b) La creación de usuario-clave válido en concordancia con los requerimientos estipulados en la solicitud de acceso.
- c) Evaluación de activos comprometidos, solo en caso que el acceso no

	GOBIERNO REGIONAL METROPOLITANO – SSI PROTOCOLO DE CONTROL Y TRATAMIENTO DE SEGURIDAD DE LA INFORMACION	Página 6 de 11
		Versión: 04
		Código: PROT-SSI-001
		Fecha: 2/08/2018

sea solo lectura. Se deberá identificar uno a uno los datos a los cuales el tercero tendrá acceso a carga o modificación donde finalmente se enunciarán todos los resultados (reportes, cálculos) a los que se podría ver afectada la integridad de la información.

d) Descripción de los servicios de información disponibles para el tercero.

e) Método de monitoreo o seguimiento de las actividades realizadas por el tercero. Donde dicho monitoreo debe tener una frecuencia semanal de envío al encargado de seguridad quien registrara las actividades.


f) Definición de un método específico de protección de la integridad de la información. Esto como mínimo debe considerar el respaldo diario o la previa validación de información cargada por un funcionario responsable del Gobierno Regional Metropolitano, entre otros, los que deben ser definidos de acuerdo a la índole de la intervención del tercero.

Todo acceso otorgado bajo este tipo de requerimiento debe estar enmarcado dentro de la Política de Acceso Físico a Oficinas e Instalaciones del Gobierno Regional Metropolitano.

6.3 Acceso lógico desde la red Institucional del Gobierno Regional Metropolitano.

El Departamento de informática en conjunto con el Encargado de Unidad responsable de la información realizará:

- a) La creación de usuario-clave válido en concordancia con los requerimientos estipulados en la solicitud de acceso.
- b) Declaración del o los sistemas a los que se concederá el acceso.
- c) Para cada uno de los sistemas involucrados de debe proporcionar:
 - Evaluación de activos comprometidos sólo en caso que el acceso no sea solo lectura. Se deberá identificar uno a uno los datos a los cuales el tercero tendrá acceso a carga o modificación donde finalmente se enunciarán todos los resultantes (reportes, cálculos) a los que se podría ver afectada la integridad de la información.
 - Descripción de los servicios de información disponibles para el tercero.

	GOBIERNO REGIONAL METROPOLITANO – SSI PROTOCOLO DE CONTROL Y TRATAMIENTO DE SEGURIDAD DE LA INFORMACION	Página 7 de 11
		Versión: 04
		Código: PROT-SSI-001
		Fecha: 2/08/2018

- Método de monitoreo o seguimiento de las actividades realizadas por el tercero. Donde dicho monitoreo debe tener una frecuencia semanal de envío al encargado de seguridad quien registrará las actividades.
- Definición de un método específico de protección de la integridad de la información. Esto como mínimo debe considerar el respaldo diario o la previa validación de información cargada por un funcionario responsable del Gobierno Regional Metropolitano, entre otros, los que deben ser definidos de acuerdo a la índole de la intervención del tercero.
- Fundamentar las razones en términos de beneficios y riesgos de los accesos otorgados.

Todo acceso otorgado bajo este tipo de requerimiento debe estar enmarcado dentro de la Política de Acceso Físico a Oficinas e Instalaciones del Gobierno Regional Metropolitano.

6.4 Acceso lógico a la red Institucional del Servicio

Solo estará permitido para esta modalidad el uso de Web-Services donde se deberá aplicar:

a) La creación de usuario-clave válido en concordancia con los requerimientos estipulados en la solicitud de acceso.

b) Evaluación de activos comprometidos, sólo en caso que el acceso no sea sólo lectura. Se deberá identificar uno a uno los datos de los cuales el tercero tendrá acceso a carga o modificación donde finalmente se enunciarán todos los resultantes (reportes, cálculos) a los que se podría ver afectada la integridad de la información.

c) Descripción de los servicios de información disponibles para el tercero.

d) Método de monitoreo o seguimiento de las actividades realizadas por el tercero. Donde dicho monitoreo debe tener una frecuencia semanal de envío al Encargado de Seguridad o quien éste defina, el cual registrará las actividades como mecanismo de control.

e) Definición de un método específico de protección de la integridad de los activos de información. Esto como mínimo debe considerar el respaldo diario o la previa validación de información cargada por un funcionario responsable del Gobierno Regional Metropolitano, entre otros, los que deben ser definidos de acuerdo a la índole de la intervención del tercero.

f) Fundamentar las razones en términos de beneficios y riesgos de los accesos otorgados.

Todo acceso otorgado bajo este tipo de requerimiento debe estar enmarcado dentro de la Política de Acceso Físico a Oficinas e Instalaciones del Gobierno Regional Metropolitano.


 GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO	GOBIERNO REGIONAL METROPOLITANO – SSI PROTOCOLO DE CONTROL Y TRATAMIENTO DE SEGURIDAD DE LA INFORMACION	Página 8 de 11
		Versión: 04
		Código: PROT-SSI-001
		Fecha: 2/08/2018

6.5 Acuerdo de Protección de activos

Se deberá establecer con el tercero un acuerdo formal de protección a la información el que será vinculado, de acuerdo a la índole del tercero, a través de un oficio si es con otro servicio público o del contrato si corresponde a un prestador de servicios, el que debe incluir las siguientes cláusulas de protección mínimas:

- a) Se realizará un monitoreo o seguimiento de las actividades realizadas por el tercero, el que tendrá una evaluación periódica y permitirá evaluar si se cumplen las solicitudes de acceso autorizadas pudiendo detectar anomalías de acceso, carga errónea de información o cualquier actividad que pudiera afectar la información o equipamiento del Gobierno Regional Metropolitano lo que ocasionará la revocación inmediata de los permisos otorgados, desencadenando las acciones legales que se estimen pertinentes.
- b) No se permitirá en ningún caso extraer información no especificada en la solicitud de acceso como tampoco realizar divulgación, venta o copia de ésta.
- c) No se podrán realizar instalaciones o desinstalaciones de software de cualquier tipo sin previa autorización escrita por la jefatura del Departamento de Informática.
- d) El tercero declara conocer la Política de Seguridad de la Información del Gobierno Regional Metropolitano.
- e) Se deberá enviar mensualmente al Encargado de Seguridad o quien éste defina y, si no aplica el período, al menos una vez, el detalle de actividades realizadas identificando usuario, fecha, información intervenida o alcanzada y resultados obtenidos.

El mantenimiento del equipamiento de procesamiento de información será única y exclusivamente mantenido por personal del Departamento de Informática del Gobierno Regional Metropolitano. Estará estrictamente prohibido conectar computadores portátiles o cualquier dispositivo de procesamiento de propiedad del tercero a la red de datos del Gobierno Regional Metropolitano, sin contar con una autorización por escrito emitida por el Departamento de Informática.

	GOBIERNO REGIONAL METROPOLITANO – SSI PROTOCOLO DE CONTROL Y TRATAMIENTO DE SEGURIDAD DE LA INFORMACION	Página 9 de 11
		Versión: 04
		Código: PROT-SSI-001
		Fecha: 2/08/2018

6.6 Supervisión y revisión

El Gobierno Regional Metropolitano deberá disponer de una contraparte técnica la cual estará encargada de monitorear y revisar los servicios del proveedor, garantizando de esta forma que los acuerdos se respeten y que los incidentes y problemas generados se gestionen correctamente.

La contraparte técnica del proveedor deberá tener las competencias suficientes así como las habilidades y recursos técnicos para monitorear, revisar o auditar los requisitos técnicos en el control de la Seguridad de la Información.

7 REGISTRO DE OPERACION

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

- A.15.01.01 Informe de solicitudes de acceso privilegiado de proveedores
- A.15.02.01 Informe de supervisión a accesos privilegiados

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

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.



GOBIERNO REGIONAL
METROPOLITANO DE
SANTIAGO

GOBIERNO REGIONAL METROPOLITANO – SSI

PROTOCOLO DE CONTROL Y TRATAMIENTO DE SEGURIDAD
DE LA INFORMACION


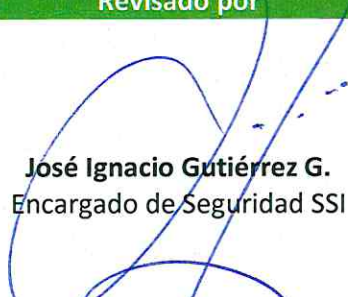
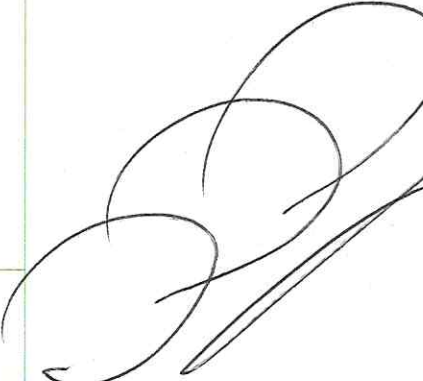

Página 10 de 11


Versión: 04

Código: PROT-SSI-001

Fecha: 2/08/2018

10 APROBACIÓN

Elaborado por	Revisado por	Aprobado por
 Carlos Hernández A. Analista Departamento de Informática	 José Ignacio Gutiérrez G. Encargado de Seguridad SSI	 Alejandro Segura B. Presidente Comité de Seguridad
	 Carolina Hidalgo M. Jefa Departamento Planificación y Control Institucional	

 GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO	GOBIERNO REGIONAL METROPOLITANO – SSI PROTOCOLO DE CONTROL Y TRATAMIENTO DE SEGURIDAD DE LA INFORMACION	Página 11 de 11
		Versión: 04
		Código: PROT-SSI-001
		Fecha: 2/08/2018

11 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES

Versión	Autor	Página o Secciones	Fecha Modificación	Motivo
01	Carlos Hernández	todas	11-08-16	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	15-09-17	Modificación de Formato, se agrega índice, Revisión, Difusión.
04	Mauricio Marín V.	9	2-08-2018	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 Definiciones y Modo de Operación. Se cambia título 7 por Registro de Operación