



GOBIERNO REGIONAL
METROPOLITANO DE
SANTIAGO

GOBIERNO REGIONAL METROPOLITANO – SSI

Controles NCh-ISO 27001

- **Política de control del acceso**
- **Perímetro de seguridad física**
 - **Controles de acceso físico**
- **Seguridad de oficinas, salas e instalaciones**
 - **Trabajo en áreas seguras**
 - **Áreas de entrega y carga**
- **Ubicación y protección del equipamiento**

Página 1 de 14

Versión: 07/19

A.09.01.01
A.11.01.01
A.11.01.02
A.11.01.03
A.11.01.05
A.11.01.06
A.11.02.01

Fecha: 12/07/2019

Política de Acceso Físico

- Política de control del acceso
- Perímetro de seguridad física
 - Controles de acceso físico
- Seguridad de oficinas, salas e instalaciones
 - Trabajo en áreas seguras
 - Áreas de entrega y carga
- Ubicación y protección del equipamiento

1 INDICE

1	INDICE	2
2	OBJETIVO	3
3	ALCANCE	3
4	ROLES Y RESPONSABILIDADES	4
5	CONTROL NORMATIVO SSI	5
6	DEFINICIONES	6
6.1	Trabajo en áreas seguras	6
6.2	Controles de acceso físico	7
6.3	Seguridad de oficinas, salas e instalaciones	7
6.4	Perímetro de Seguridad física.....	8
6.5	Ubicación y Protección de equipamiento.....	8
6.6	Áreas de entrega y carga	8
7	PERSONAL AUTORIZADO	8
8	ANEXOS	9
8.1	Ingreso de Proveedores.....	9
8.2	Ingreso de proveedores.....	10
9	PERIODICIDAD DE EVALUACION Y REVISIÓN	11
10	DIFUSIÓN	11
11	FORMALIZACION EXTERNA	11
12	REGISTRO DE REVISION Y ACTUALIZACION HISTORICO	12
13	FORMALIZACIÓN INTERNA	14

 <p>GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO</p>	<p>GOBIERNO REGIONAL METROPOLITANO – SSI Controles NCh-ISO 27001</p> <ul style="list-style-type: none"> • Política de control del acceso • Perímetro de seguridad física <ul style="list-style-type: none"> • Controles de acceso físico • Seguridad de oficinas, salas e instalaciones <ul style="list-style-type: none"> • Trabajo en áreas seguras • Áreas de entrega y carga • Ubicación y protección del equipamiento 	Página 3 de 14
		Versión: 07/19
		A.09.01.01 A.11.01.01 A.11.01.02 A.11.01.03 A.11.01.05 A.11.01.06 A.11.02.01
		Fecha: 12/07/2019

2 OBJETIVO

El presente documento tiene por finalidad regular y normar las autorizaciones de los accesos y los desplazamientos del personal y visitas y cualquier otro tipo de personas que ingresen a las instalaciones del Gobierno Regional Metropolitano , específicamente el edificio Institucional , ubicado en calle Bandera N°46 , en la comuna de Santiago.

Además debe establecer normas para garantizar el buen funcionamiento del Datacenter y servicios ofrecidos por el Departamento de Informática.

La aplicación de esta política, buscar evitar el acceso no autorizado ofreciendo, además, controles para auditorias más eficaces, logrando el control total en los accesos en el Gobierno Regional Metropolitano de Santiago, los cuales exponen a la institución a pérdidas de información, daño a los recursos disponibles, como también posibles problemas jurídicos.

3 ALCANCE

La Política se aplica a todos los accesos restringidos que contenga el Gobierno Regional Metropolitano de Santiago, aplicando a todos los empleados, proveedores, contratistas, personal que esté vinculado con las firmas que presten servicios a Gobierno Regional Metropolitano de Santiago o que estén relacionados. Se incluye, además, todas las dependencias que son parte de la institución o que transite por las dependencias del Gobierno Regional Metropolitano

 GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO	GOBIERNO REGIONAL METROPOLITANO – SSI Controles NCh-ISO 27001 <ul style="list-style-type: none"> • Política de control del acceso • Perímetro de seguridad física <ul style="list-style-type: none"> • Controles de acceso físico • Seguridad de oficinas, salas e instalaciones <ul style="list-style-type: none"> • Trabajo en áreas seguras • Áreas de entrega y carga • Ubicación y protección del equipamiento 	Página 4 de 14
		Versión: 07/19
		A.09.01.01 A.11.01.01 A.11.01.02 A.11.01.03 A.11.01.05 A.11.01.06 A.11.02.01
		Fecha: 12/07/2019

4 ROLES Y RESPONSABILIDADES

El Departamento de Informática será el encargado de evaluar y conceder los permisos de acceso a las tarjetas magnéticas. Así como la administración del sistema de acceso y el control de los roles de acceso.

El Departamento de informática del Gobierno Regional Metropolitano de Santiago, es el responsable de la seguridad de los datos en la red y sus equipos, con el fin de ejecutar a cabalidad la tarea de mantener la infraestructura de la red.

- Política de control del acceso
- Perímetro de seguridad física
 - Controles de acceso físico
- Seguridad de oficinas, salas e instalaciones
 - Trabajo en áreas seguras
 - Áreas de entrega y carga
- Ubicación y protección del equipamiento

5 CONTROL NORMATIVO SSI

La siguiente política 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.09.01.01	Política de control del acceso	Se debe establecer, documentar y revisar la política de control de acceso en base a los requisitos de negocio y de seguridad de la información.
A.11.01.01	Perímetro de seguridad física	Se debe definir y utilizar perímetros de seguridad para proteger las áreas que contienen ya sea información sensible o crítica y las instalaciones de procesamiento de información.
A.11.01.02	Controles de acceso físico	Las áreas seguras deben estar protegidas por controles de entrada apropiados que aseguren que sólo se permite el acceso a personal autorizado.
A.11.01.03	Seguridad de oficinas, salas e instalaciones	Se debe diseñar y aplicar elementos de la seguridad física en oficinas, salas e instalaciones.
A.11.01.05	Trabajo en áreas seguras	Se debe definir acceso físico a zonas restringidas en las cuales solo podrá acceder personal autorizado
A.11.01.06	Áreas de entrega y carga.	Se deben controlar los puntos de acceso tales como áreas de entrega y de carga y otros puntos donde las personas no autorizadas puedan acceder a las instalaciones y, si es posible, aislarlas de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.02.01	Ubicación y protección del equipamiento	El equipamiento se debe ubicar y proteger para reducir los riesgos provocados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.

	GOBIERNO REGIONAL METROPOLITANO – SSI Controles NCh-ISO 27001 <ul style="list-style-type: none"> • Política de control del acceso • Perímetro de seguridad física <ul style="list-style-type: none"> • Controles de acceso físico • Seguridad de oficinas, salas e instalaciones <ul style="list-style-type: none"> • Trabajo en áreas seguras • Áreas de entrega y carga • Ubicación y protección del equipamiento 	Página 6 de 14
		Versión: 07/19
		A.09.01.01 A.11.01.01 A.11.01.02 A.11.01.03 A.11.01.05 A.11.01.06 A.11.02.01
		Fecha: 12/07/2019

6 DEFINICIONES

6.1 Trabajo en áreas seguras

- Los sistemas de seguridad física deben cumplir con todas las regulaciones aplicables como tal, pero no están limitadas a las normas de construcción y prevención de incendios.
- Cualquier uso de las instalaciones de TI deberá contar con la aprobación del Departamento de Informática del Gobierno Regional Metropolitano de Santiago.
- El personal autorizado debe tener las (24) horas de libre acceso a las instalaciones críticas de TI.
- Toda persona, sea funcionario o personal externo que transite por las distintas dependencias del GORE deberá portar su tarjeta de identificación, la que le permitirá abrir solo las puertas para las cuales ha sido autorizada.
- Toda persona que concurra de visita el Servicio deberá acreditarse en la recepción de calle Bandera N° 46, donde la empresa de seguridad asignara una tarjeta de visita diseñada para la apertura de puertas sólo del piso donde justifica su destino, previo confirmación con el funcionarios que viene a visitar
- El proceso para la obtención de las credenciales, tarjetas de acceso magnéticas o claves de acceso a instalaciones de TI deberán incluir la aprobación del Jefe del Departamento de Informática del Gobierno Regional Metropolitano de Santiago.
- Las tarjetas de acceso magnéticas o claves de acceso no deben ser compartidas o cedidas a terceros.
- Las tarjetas de acceso magnético o claves de acceso que ya no sean necesarios o ya cumplieron su función, deberán ser devueltas al Departamento de Informática del Gobierno Regional Metropolitano de Santiago. Las tarjetas no deberán ser reasignadas a otra persona sin pasar por el proceso de re enrolamiento.
- La pérdida o robo de las tarjetas de acceso magnéticas o claves deberán ser reportados al Departamento de Informática del Gobierno Regional Metropolitano de Santiago.

Toda versión impresa de este documento se considera como copia no controlada.

 <p>GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO</p>	<p>GOBIERNO REGIONAL METROPOLITANO – SSI Controles NCh-ISO 27001</p> <ul style="list-style-type: none"> • Política de control del acceso • Perímetro de seguridad física <ul style="list-style-type: none"> • Controles de acceso físico • Seguridad de oficinas, salas e instalaciones <ul style="list-style-type: none"> • Trabajo en áreas seguras • Áreas de entrega y carga • Ubicación y protección del equipamiento 	Página 7 de 14
		Versión: 07/19
		A.09.01.01 A.11.01.01 A.11.01.02 A.11.01.03 A.11.01.05 A.11.01.06 A.11.02.01
		Fecha: 12/07/2019

- Los registros de acceso de las tarjetas de acceso magnético o clave deberán conservarse para mantener una revisión de los accesos y rutinas realizadas basadas en la criticidad de los recursos que se protegen.
- El Departamento de informática del Gobierno Regional Metropolitano de Santiago, en colaboración con el área de personal, serán los encargados de recuperar y eliminar los accesos a los lugares restringidos de las personas que sean desvinculadas o que por cambios en el contrato cambien sus roles operativos.
- En casos de emergencias, será el encargado de emergencia de cada piso quien tendrá la obligación de desbloquear las puertas de acceso. De igual manera la jefatura del Departamento de Informática realizara el desbloqueo por software a cada pórtilco de acuerdo a lo establecido en el Plan de Emergencia
- El Departamento de Informática, se encargará de revisar periódicamente los privilegios y derechos de acceso de las tarjetas de acceso magnético o claves para eliminar las de las personas que ya no requieran de estos privilegios.
- Las señaléticas para el acceso a las salas locaciones restringidas deberá ser simple, sin embargo, deberá informar de forma simple la importancia de la ubicación.

6.2 Controles de acceso físico

- Todo acceso físico al edificio y dependencias del Gobierno Regional Metropolitano estará restringido, y solo se realizará tras la obtención y mediante de una tarjeta magnética vía solicitud al Departamento de Gestión de Personas, así como también el ingreso de visitas será consignado y autorizado por el funcionario a quien visita . Se le otorgará una tarjeta magnética con acceso solo al piso que visite

6.3 Seguridad de oficinas, salas e instalaciones

- Para poder acceder a un piso y sus oficinas, será necesario el porte de una tarjeta magnética consignada con los respectivos privilegios de controles acceso físico, según sea funcionario, proveedor externo o simple visita
- Todas las instalaciones de TI deberían estar físicamente protegidas en proporción a la criticidad o importancia de su función en el Gobierno Regional Metropolitano de Santiago.

Toda versión impresa de este documento se considera como copia no controlada.

 <p>GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO</p>	<p>GOBIERNO REGIONAL METROPOLITANO – SSI</p> <p>Controles NCh-ISO 27001</p> <ul style="list-style-type: none"> • Política de control del acceso • Perímetro de seguridad física <ul style="list-style-type: none"> • Controles de acceso físico • Seguridad de oficinas, salas e instalaciones <ul style="list-style-type: none"> • Trabajo en áreas seguras • Áreas de entrega y carga • Ubicación y protección del equipamiento 	Página 8 de 14
		Versión: 07/19
		A.09.01.01 A.11.01.01 A.11.01.02 A.11.01.03 A.11.01.05 A.11.01.06 A.11.02.01
		Fecha: 12/07/2019

- El Departamento de Informática junto con el Departamento de Gestión de las Personas, asignaran las tarjetas de acceso segregando los roles de control de acceso según sea la naturaleza de la solicitud

6.4 Perímetro de Seguridad física

- Todo acceso a las instalaciones de TI estará delimitado por un perímetro definido y solo se concederán al personal designado por el Departamento de Informática del Gobierno Regional Metropolitano de Santiago y contratistas, cuyas responsabilidades de trabajo requieran el acceso a dicha instalación.

6.5 Ubicación y Protección de equipamiento

- Todo el equipamiento relacionado con el procesamiento de la información como Servidores y Racks de comunicaciones debe estar ubicado en un sector aparte, delimitado físicamente, con acceso restringido solo a personal del Departamento de Informática y a proveedores externos autorizados, los que no podrán estar solos en dicho sitio sino que acompañados de un funcionario del Departamento de Informática de manera de reducir los riesgos por accesos no autorizados

6.6 Áreas de entrega y carga

- El acceso a la entrega y carga desde fuera del edificio, será restringido a personal debidamente identificado y autorizado. Las puertas externas serán aseguradas cuando se abran las puertas internas. El material que ingrese se inspeccionado para evitar posibles amenazas artes que sean ingresados a su lugar de utilización. Deberán segregarse físicamente los envíos entrantes y salientes

7 PERSONAL AUTORIZADO

El acceso al Datacenter y racks de redes TI estarán restringidos solo a los administradores de sistema TI y Jefe del Departamento de informática. Los otros accesos a personal de servicios, oficiales de seguridad y otros actores, estarán restringidos y, según sea necesario, se solicitará a la jefatura correspondiente para gestionar con el Jefe del Departamento de Informática dichos privilegios. Cualquier otro tipo de personal, deberá ingresar acompañado a las instalaciones.

Toda versión impresa de este documento se considera como copia no controlada.



GOBIERNO REGIONAL
METROPOLITANO DE
SANTIAGO

GOBIERNO REGIONAL METROPOLITANO – SSI

Controles NCh-ISO 27001

- Política de control del acceso
- Perímetro de seguridad física
 - Controles de acceso físico
- Seguridad de oficinas, salas e instalaciones
 - Trabajo en áreas seguras
 - Áreas de entrega y carga
- Ubicación y protección del equipamiento

Página 10 de 14

Versión: 07/19

A.09.01.01
A.11.01.01
A.11.01.02
A.11.01.03
A.11.01.05
A.11.01.06
A.11.02.01

Fecha: 12/07/2019

8.2 Ingreso de proveedores



GOBIERNO REGIONAL
METROPOLITANO DE
SANTIAGO

EMPRESA ASENSORES SCHINDLERS FECHA:					
Nº	HORA DE INGRESO	NOMBRE / APELLIDOS	C.IDENTIDAD	CARGO	HORA DE EGRESO

PERSONAL EXTERNO A LA DOTACION Y EDIFICIO					
Nº	HORA DE INGRESO	NOMBRE / APELLIDOS	C.IDENTIDAD	CARGO	HORA DE EGRESO
1					

OBSERVACIONES:					
Reparacion ascensor					

Toda versión impresa de este documento se considera como copia no controlada.

 <p>GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO</p>	<p>GOBIERNO REGIONAL METROPOLITANO – SSI Controles NCh-ISO 27001</p> <ul style="list-style-type: none"> • Política de control del acceso • Perímetro de seguridad física <ul style="list-style-type: none"> • Controles de acceso físico • Seguridad de oficinas, salas e instalaciones <ul style="list-style-type: none"> • Trabajo en áreas seguras • Áreas de entrega y carga • Ubicación y protección del equipamiento 	Página 11 de 14
		Versión: 07/19
		A.09.01.01 A.11.01.01 A.11.01.02 A.11.01.03 A.11.01.05 A.11.01.06 A.11.02.01
		Fecha: 12/07/2019

9 PERIODICIDAD DE EVALUACION Y REVISIÓN

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

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 FORMALIZACION EXTERNA

Mediante el acta fecha 12 de julio año 2019, se aprueba por parte del Comité de Seguridad de la Información, la Política de acceso físico.

- Política de control del acceso
- Perímetro de seguridad física
 - Controles de acceso físico
- Seguridad de oficinas, salas e instalaciones
 - Trabajo en áreas seguras
 - Áreas de entrega y carga
- Ubicación y protección del equipamiento

12 REGISTRO DE REVISION Y ACTUALIZACION HISTORICO

Versión	Autor	Página o Secciones	Fecha Modificación	Motivo
01	Carlos Hernández	todas	01-11-2011	Creación
02	José Gutiérrez G	todas	01-11-2012	Revisión Comité de Seguridad
03	Carlos Hernández	todas	10-08-17	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
04	Mauricio Marín	6,9,10	12-10-17	Se complementa información en el punto 6.1 Trabajo en áreas seguras. <ul style="list-style-type: none"> • Agrega anexos proveedores
05	Mauricio Marin V	todas	01/08/2018	Se cambia código interno de NOR-SSI-007 por POL-SSI-016 Se agrega el siguiente párrafo en el punto 8 Registro de Control 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” Se cambia título 8 por “Registro de Operaciones” SE cambia título 9 por “ Periodicidad de evaluación y revisión



GOBIERNO REGIONAL
METROPOLITANO DE
SANTIAGO

GOBIERNO REGIONAL METROPOLITANO – SSI

Controles NCh-ISO 27001

- **Política de control del acceso**
- **Perímetro de seguridad física**
 - **Controles de acceso físico**
- **Seguridad de oficinas, salas e instalaciones**
 - **Trabajo en áreas seguras**
 - **Áreas de entrega y carga**
- **Ubicación y protección del equipamiento**

Página 13 de 14

Versión: 07/19

A.09.01.01
A.11.01.01
A.11.01.02
A.11.01.03
A.11.01.05
A.11.01.06
A.11.02.01

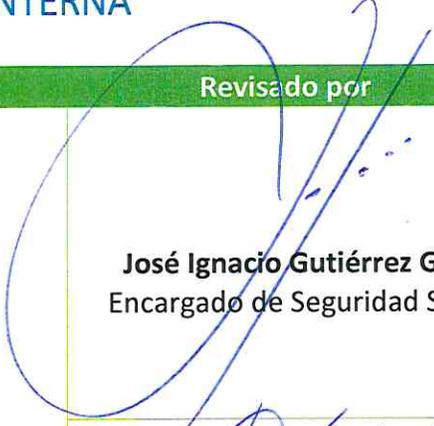
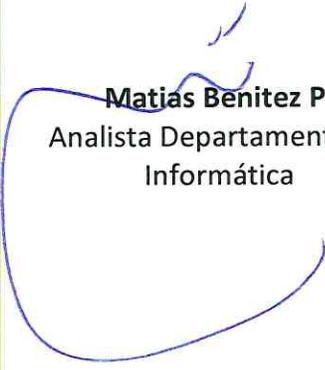
Fecha: 12/07/2019

06	Mauricio Marin	todas	16/11/18	Comité de Seguridad revisa y aprueba documento para el año 2018.
07	Matias Benitez.	Todas	12-07-2019	Comité de la seguridad de la información revisa y aprueba Política de acceso físico año 2019.

- Política de control del acceso
- Perímetro de seguridad física
 - Controles de acceso físico
- Seguridad de oficinas, salas e instalaciones
 - Trabajo en áreas seguras
 - Áreas de entrega y carga
- Ubicación y protección del equipamiento

- A.09.01.01
- A.11.01.01
- A.11.01.02
- A.11.01.03
- A.11.01.05
- A.11.01.06
- A.11.02.01

13 FORMALIZACIÓN INTERNA

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