APRUEBA POLITICA DE ACCESO FISICO. DEL GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO.

RESOLUCIÓN EXENTA N° 3031

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.

16177860

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 Política de Acceso Físico del Gobierno Regional Metropolitana.

2.- DÉJESE sin efecto la Resolución N° 3163 del 24 de diciembre de 2015, que aprobó la Política de Acceso Físico del Gobierno Regional Metropolitana.

3.- APRUEBASE la Política de Acceso Físico del Gobierno Regional Metropolitano de Santiago.

ANOTESE Y PUBLIQUESE

INTENDENCIA REGION METROPOLITANA DE SANTIAGO
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

Política de Acceso Físico

1 INDICE

1 INDICE 2
2 OBJETIVO 3
3 ALCANCE 3
4 ROLES Y RESPONSABILIDADES 3
5 CONTROL NORMATIVO SSI 4
6 ACCESO A LAS INSTALACIONES 5
6.1 Trabajo en áreas seguras 5
6.2 Controles de acceso físico 6
6.3 Seguridad de oficinas, salas e instalaciones 6
6.4 Perímetro de Seguridad física 7
6.5 Ubicación y Protección de equipamiento 7
6.6 Áreas de entrega y carga 7
7 PERSONAL AUTORIZADO 7
8 REGISTRO DE CONTROL 8
9 APLICACIÓN 8
10 REVISIÓN 8
11 DIFUSIÓN 9
12 ANEXOS 9
12.1 Ingreso de Proveedores 9
12.2 Ingreso de proveedores 10
13 APROBACIÓN 11
14 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES 12

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

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.

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.

6 ACCESO A LAS INSTALACIONES

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 Nº 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.
- Los registros de acceso de las tarjetas de acceso magnéticas o claves 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 pórtico 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.

- 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.

8 REGISTRO DE CONTROL

El Departamento de Informática y el Departamento de Servicios Generales deberán emitir un informe que dé cuenta de:

- A.09.01.01 Informe Resolución Política de Control de acceso
- A.11.01.01 Informe de registros de accesos a Perímetros de Seguridad Física
- A.11.01.02 Informe de accesos de visitas con porte de tarjetas asignadas.
- A.11.01.03 Informe de Asignación de Tarjetas de acceso
- A.11.01.05 Informe de Seguridad de instalaciones con accesos restringidos solo a personal autorizado (Datacenter y racks de Comunicaciones)
- A.11.01.06 Informe del uso de áreas de entrega y carga
- A.11.02.01 Informe de Ubicación y acceso limitado a Sala de Servidores

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)

9 APLICACIÓN

La infracción a las obligaciones establecidas en el artículo anterior, podrá construir una violación al principio de probidad administrativa, y será sancionada en conformidad a lo dispuesto en la Ley N° 18.834, sobre Estatuto Administrativo. Lo anterior es sin perjuicio de la responsabilidad civil o penal que corresponda.

El Departamento de Informática velará por el cumplimiento de estas políticas, resguardando los intereses del Gobierno Regional Metropolitano de Santiago.

El Departamento de Informática no se hará responsable por incidentes producidos por el no cumplimiento de estas políticas de seguridad.

10 REVISIÓN

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

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 ANEXOS

12.1 Ingreso de Proveedores

INGRESO DE PROVEDORES A LAS DEPENDENCIAS DEL GORE /2017.-

fecha	Hora de ingreso	Hora de egreso	Nombre / Apellidos	Cedula de identidad	PATENTE	OBSERVACIONES

12.2 Ingreso de proveedores

stgo

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

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

OBSERVACIONES:
Reparacion ascensor

13 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 **Carolina Hidalgo M.** Jefa Departamento de Gestión Institucional	**Mayuri Reyes Torres** Presidente Comité de Seguridad

14 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES

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. • 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. • Agrega anexos proveedores

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