DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO INFORMATICA

APRUEBA NORMA DE ACCESO A LA RED DEL GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO.

RESOLUCIÓN EXENTA N° 3025

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.

16177870

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.- APRUEBASE la Norma de Acceso a la Red del Gobierno Regional Metropolitano de Santiago.

ANOTESE Y PUBLIQUESE

INTENDENCIA REGION METROPOLITANA
INTENDENTE

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

IFF/GEP/VGM/MRT/JLG

Distribución:
- Funcionario Gobierno Regional Metropolitano de Santiago
- Honorarios Gobierno Regional Metropolitano de Santiago
- Comité de Seguridad de la Información
- Oficina de Partes

Norma de Acceso a la Red

1 INDICE

1 INDICE 2
2 OBJETIVO 3
3 ALCANCE 3
4 ROLES Y RESPONSABILIDADES 3
5 CONTROL NORMATIVO SSI 4
6 APLICACIÓN 5
6.1 Acceso a la Red 5
6.2 Mecanismos de seguridad física a áreas TI 5
7 Controles de Red 6
8 Seguridad de los servicios de redes 7
9 SEGREGACIÓN DE REDES 7
10 REGISTRO DE CONTROL 8
11 REVISIÓN 8
12 DIFUSIÓN 8
13 APROBACIÓN 9
14 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES 10

2 OBJETIVO

Establecer normas para garantizar el buen funcionamiento de las redes del Gobierno Regional Metropolitano y los servicios ofrecidos por el Departamento de Informática.

La aplicación de esta norma, buscar evitar el acceso no autorizado a la red digital del Gobierno Regional Metropolitano y está orientado a validar, verificar y proveer acceso lógico a la información, a las aplicaciones, bases de datos y servicios en general, logrando el control total en los accesos a la Red, los cuales exponen a la institución a pérdidas de activos de información, daño a los recursos disponibles.

3 ALCANCE

La Norma se aplica 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 y que por sus funciones deban hacer uso de la Red digital del GORE o de su área local de conexión . Se incluyen, además, todas las dependencias que son parte de la institución o que tengan acceso a la red digital del Gobierno Regional Metropolitano.

4 ROLES Y RESPONSABILIDADES

El Departamento de Informática será el encargado de evaluar y conceder los permisos de acceso a la red del Servicio, así como la administración del sistema de acceso y el control de los roles de acceso a la misma

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.

El Departamento de Personal deberá informar las altas y las bajas de personal a modo de mantener actualizado el registro de usuarios

Todos los usuarios deberán regirse por todo lo establecido en esta norma, quedándoles estrictamente prohibido el uso de la red para fines personales. Deberán tomar todos los resguardos necesarios que el Departamento de Informática ha puesto su disposición.
No podrán conectar a la red otros equipos que no sean los del Servicio. Si necesita usar un equipo distinto a los provistos por el Servicio, será menester del Departamento de Informática su autorización previo chequeo del equipo y que este cumpla con las normas básicas de seguridad.

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.09.01.02	Accesos a las Redes y a los servicios de la red	Los usuarios sólo deben tener acceso directo a a la red y a los servicios de la red para los cuales han sido autorizados.
A.13.01.01	Controles de red	Las redes se deben gestionar y controlar para proteger la información en los sistemas y aplicaciones.
A.13.01.02	Seguridad de los servicios de la red	Los mecanismos de seguridad, los niveles de servicio y los requisitos de la gestión de todos los servicios de red se deben identificar e incluir en los acuerdos de servicios de red, ya sea que estos servicios son prestados dentro de la organización o por terceros.
A.13.01.03	Separación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en redes.

6 APLICACIÓN

6.1 Acceso a la Red

- Todo acceso a la Red se hará mediante la creación de una cuenta de usuario autorizada previamente por el Departamento de Gestión de personas. Esta cuenta de usuario será autenticada mediante una clave secreta que se validará en el Active Directory del Dominio del Gobierno Regional Metropolitano

- Toda la Red deberá estar físicamente protegidas en proporción a la criticidad o importancia de su función en el Gobierno Regional Metropolitano de Santiago.

- Los accesos a los distintos servidores o áreas serán permitidos de acuerdo a los privilegios otorgados a cada usuario de acuerdo lo establezca el Departamento de Informática del Gobierno Regional Metropolitano.

6.2 Mecanismos de seguridad física a áreas TI

- Todo acceso a las instalaciones de TI, 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.

- 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 devueltos 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 basados 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.

- 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.

- Cualquier uso de las instalaciones de TI deberá contar con la aprobación del Departamento de Informática del Gobierno Regional Metropolitano de Santiago.

- Todo dispositivo o equipo personal deberá contar con la autorización del Departamento de Informática para poder conectarse a la Red del Servicio previa revisión y escaneo del mismo a manera de evitar intrusiones de virus y propagación de este por la Red

7 Controles de Red

La administración de la red corresponderá al Departamento de Informática del Gobierno regional Metropolitano.

El personal autorizado debe tener libre acceso a las instalaciones críticas de TI las 24 horas del día.

El Departamento de Informática deberá velar por la protección contra interceptación, interferencia o daños en la red. La red deberá ser monitoreada con el fin de evitar accesos inadecuados o posibles ataques o intrusiones.

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 Seguridad de los servicios de redes

El Gobierno Regional Metropolitano, deberá disponer de soluciones de seguridad de redes administradas como firewalls y sistemas de detección de intrusos, con el fin de proteger la red Institucional.

El Departamento de Informática deberá monitorear de manera constante los servicios de red con el fin de asegurar un UpTime lo más cercano al 100%. Así mismo el Servicio debería garantizar que los proveedores de servicios de red implementen estas medidas.

Las funciones de seguridad de los servicios de red pueden ser:

- con aplicación de tecnología para la seguridad de los servicios de redes, como la autenticación, el cifrado y los controles de conexión de redes;
- parámetros técnicos necesarios para la conexión segura con los servicios de red de acuerdo con la seguridad y las reglas de conexión de redes;
- los procedimientos para el uso de servicios de redes para restringir el acceso a los servicios de red o aplicaciones, donde corresponda.

9 SEGREGACIÓN DE REDES

La red institucional, deberá ser segmentada en redes perimetrales con el fin de administrar la seguridad del Servicio.

De requerirlo, la red misma deberá ser segregada en diferentes niveles de acceso con el fin de evitar ataques tanto internos como externos.

L segregación deberá a lo menos contar con una LAN para los usuarios, una DMZ para Servidores y una red perimetral para los accesos WiFi.

Los accesos de confianza podrían generarse mediante grupos de accesos validados en Active Directory con privilegios según las funciones de cada usuario

10 REGISTRO DE CONTROL

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

- A.09.01.02 Informe de usuarios Autenticados a través de Active Directory para acceso a la Red.
- A.13.01.01 Informe de controles de red implementados en la institución.
- A.13.01.02 Informe de Seguridad de los servicios de red implementados en la institución.
- A.13.01.03 Informe de segregación de redes implementadas en la institución.

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)

11 REVISIÓN

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

12 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.

13 APROBACIÓN

Elaborado por	Revisado por	Aprobado por
Mauricio Marín Vera Analista Departamento de Informática	**José Ignacio Gutiérrez G.** Encargado de Seguridad SSI **Carlos Hernández A.** Analista Departamento de Informática **Carolina Hidalgo M.** Jefa Departamento de Gestión Institucional	**Mayuli Reyes Torres** Presidente Comité de Seguridad

14. REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES

Versión	Autor	Página o Secciones	Fecha Modificación	Motivo
01	Mauricio Marín	todas	29-09-17	Creación

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