DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO INFORMATICA

APRUEBA POLITICA DE CORREO ELECTRONICO DEL GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO.

RESOLUCIÓN EXENTA N° 3029

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.

16177862

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 Norma de Uso Correo Electrónico del Gobierno Regional Metropolitana.

2.- APRUEBASE la Política de Correo Electrónico 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/NRT/JIG

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

POLITICA DE CORREO ELECTRONICO

1 INDICE

2 OBJETIVO

Ofrecer a los usuarios una guía sobre los requerimientos mínimos que deben ser cumplidos respecto de la política y del uso del correo electrónico institucional que provee el Gobierno Regional Metropolitano de Santiago, como también las implicancias del mal uso.

Es importante mencionar que el uso inapropiado de los recursos dispuestos para los usuarios, expone a la institución a riesgos innecesarios como los virus informáticos, interrupción de las redes y sus sistemas, como también problemas jurídicos tanto nacionales como internacionales.

3 ALCANCE

La Política mencionadas en el presente documento cubren el uso apropiado del correo electrónico que es enviado y recibido desde y hacia el correo electrónico del Gobierno Regional Metropolitano de Santiago y aplica a todos los empleados, proveedores, contratistas, personal que esté vinculado con las firmas que presten servicios al 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 la red del Gobierno Regional Metropolitano de Santiago.

4 ROLES Y RESPONSABILIDADES

El Jefe del Departamento de Informática: será el encargado de aplicar los filtros al servicio de correo que sean necesarios para el cumplimiento de estas normas, así como otros para el resguardo de la comunicación.

El Departamento de Informática: respaldará semanalmente las cuentas de correo sin aviso previo a los usuarios, entendiendo que la información contenida es exclusivamente parte del trabajo habitual.

La infracción a las obligaciones establecidas en el artículo anterior, podrá constituir 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 por el mal uso de esta herramienta.

Los usuarios: Cada usuario será responsable del correcto uso del correo electrónico.

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.13.02.01	Políticas y procedimientos de transferencia de información	Las políticas, procedimientos y controles de transferencia formal deben estar diseñados para proteger la transferencia de la información mediante el uso de todos los tipos de medios de comunicación.
A.13.02.03	Mensajería electrónica	La información involucrada en la mensajería electrónica debe ser debidamente protegida

6 USO ACEPTABLE DEL CORREO ELECTRÓNICO

6.1 Políticas y procedimientos de transferencia

I. El uso de la cuenta de correo electrónico, de las redes y de los sistemas informáticos, proporcionados por El Departamento de Informática, debe guarda relación con el ámbito de competencia del Gobierno Regional Metropolitano de Santiago y tener como finalidad el ejercicio de las funciones propias e inherentes para las cuales el usuario ha sido contratado o se ha convenido su prestación de servicios.

II. Se promueve el buen uso del correo electrónico, de las redes y de los sistemas informáticos, especialmente aquellas prácticas que protejan al sistema de eventuales daños ocasionados por archivos o programas maliciosos.

III. Los usuarios deberán identificar en el correo sus datos (nombre, apellido, unidad), para que el receptor del mensaje identifique con certeza la identidad del remitente y la unidad de su procedencia.

IV. Para efectos de su uso personal, el usuario deberá tener cuentas de correo electrónico distintas a la institucional, utilizando servicios al proporcionado por el Gobierno Regional Metropolitano de Santiago. El uso de este tipo de servicio se encuentra sujeto a la misma normativa descrita en este documento.

V. Toda casilla de correo electrónico está directamente vinculada al funcionario para el cual fue creado, siendo este el responsable implícito del contenido escrito o adjuntado a él.

VI. Los usuarios son los únicos responsables de todas las actividades realizadas en sus cuentas de correo electrónico, debiendo cumplir en todo momento la normativa vigente.

6.2 Transferencia de Información en los correos electrónicos

I. La información intercambiada por este medio deberá restringirse a propósitos institucionales y el Gobierno Regional Metropolitano de Santiago estará facultado para aplicar todas las medidas necesarias para garantizar la estabilidad del servicio y su uso correcto sujeto a la ley vigente.

II. Se considerarán elementos de filtros para el envío de correos con archivos adjuntos, como tamaño máximo autorizado para èl envío.

III. número máximo de archivos adjuntos,

IV. elementos criptográficos para proteger la integridad.

V. aplicaciones antivirus y antimalware para la recepción de correos con archivos adjuntos

Todo lo anterior es considerado como "uso aceptable del correo electrónico". Lo que no se ha incluido dentro de este marco, se considera como "uso no aceptable del correo electrónico".

7 USO NO ACEPTABLE DEL CORREO ELECTRÓNICO.

De acuerdo a lo expresado en "uso aceptable del correo electrónico", lo que se presenta a continuación son conductas que caen dentro del ámbito delo uso no aceptable del correo electrónico, siendo un listado "no absoluto".

7.1 Mensajería electrónica

1. Los usuarios deberán mantener bajo reserva la contraseña de acceso de su cuenta de correo electrónico, evitando almacenarla o compartirla para evitar ingresos no autorizados. De ser almacenada en el sistema informático en el que se accede, deberá ser almacenada de manera protegida.

2. Los usuarios tienen prohibido intentar acceder en forma no autorizada a la cuenta de correo electrónico de otro usuario y tratar de tomar su identidad, salvo su expresa autorización.

3. Los usuarios deberán respetar la naturaleza confidencial de los datos que puedan ser de su conocimiento ya sea como parte de su trabajo o por accidente.

4. Los usuarios deberán usar un lenguaje respetuoso en sus mensajes con usuarios internos o externos y estos mensajes de ninguna forma podrán ser de contenido difamatorio, insultante, injurioso, amenazador, ofensivo, obsceno, racista o sexista.

5. Realizar hostigamiento o acoso laboral, sexual, político, o de cualquier otro tipo.

6. Se prohíbe el envío de información con fines de proselitismo político, religioso, u otro de carácter similar.

7. Se prohíbe emitir opiniones personales en foros de discusión, listas temáticas u otras instancias de naturaleza polémica con la cuenta de correo electrónico institucional o de las redes del Gobierno Regional Metropolitano de Santiago.

8. El correo electrónico es vulnerable a modificaciones o accesos no autorizados, por lo que no garantiza el envío seguro y confidencial de la información que la ley establece como secreta o reservada, debiendo el usuario abstenerse de enviarla por dicho medio, salvo que exista causa justificada y se procuren medidas que protejan la seguridad y confidencialidad de la información.

9. Los usuarios deberán abstenerse de enviar/recibir por e-mail contenidos que no tengan relación con el trabajo y que sean de gran tamaño tales como videos, imágenes, archivos de audio (mp3), etc.
10. Está prohibido al usuario el uso de seudónimos u otros sistemas para ocultar su identidad. En todos los mensajes debe estar claramente identificado el origen del mensaje.

11. Está prohibido al usuario enviar mensajes a otro usuario o grupo que no los quieran recibir.

12. La apertura de archivos adjuntos o la ejecución de programas que se reciban vía correo electrónico, constituye acciones que pueden vulnerar la estabilidad, calidad o seguridad de las redes o del sistema informático.

13. Se prohíbe el envío de cualquier tipo de publicidad o aviso comercial, cadenas de correo electrónico, comercialización de productos (compra y venta), pirámides, phishing, donaciones, peticiones de firmas o cualquier asunto que se circunscriba al mal uso del correo electrónico, salvo que se realice con motivo del cumplimiento de las funciones que sean propias.

14. Se prohíbe todo lo que se considere como contenido de naturaleza ilegal (relacionados con hechos delictivos, pudiendo ser terrorismo, piratería, documentos electrónicos con infracción al derecho de autor, pornografía infantil, estafas y otros).

15. El usuario no deberá enviar por correo electrónico documentos que, individualmente o en conjunto, contengan más de 20 megabytes, salvo que el envío por otro medio o dispositivo electrónico, como CD, DVD, pendrive u otro, no sea posible. En todo caso, el usuario puede solicitar al Área de Soporte, la asesoría para determinar la mejor alternativa de compartir estos documentos.

16. Se prohíbe enviar SPAM o correo electrónico masivo no deseado por los destinatarios, salvo que ello fuese excepcional e indispensable para el mejor cumplimiento de sus funciones.

17. Se prohíbe utilizar los servidores de correo electrónico para retransmitir correos sin el permiso expreso de la autoridad correspondiente, debiendo cumplir la normativa vigente.

18. Se prohíbe la utilización de servidores de correos distintos a los utilizados por el Gobierno Regional Metropolitano de Santiago para el envío o recepción de documentos electrónicos propios de la institución. El Gobierno Regional Metropolitano de Santiago no dará soporte de servicios de correo electrónico que no sean los propios (ejemplo: gmail, yahoo, terra, etc.)

19. El uso de este listado de contactos difundidos por los sistemas de la institución, es solo para consultas y de uso exclusivo dentro del Gobierno Regional Metropolitano de Santiago. Está prohibido difundir cualquier listado (ej. Correos, teléfonos, y otro tipo de información pública) por cualquier medio electrónico o impreso para propósitos que no sean de uso institucional.

20. El Departamento de Informática no realizará respaldos de los correos ni de las carpetas locales de los usuarios, por lo que será de responsabilidad de éstos hacerlo. El usuario podrá solicitar al área de Soporte, que se respalden dichos correos, utilizando algún procedimiento automatizado y asignar los recursos de almacenamiento según correspondan, previa autorización del jefe del solicitante.

8 PROCEDIMIENTO DE ACTUALIZACIÓN ANTIVIRUS

8.1 Control contra códigos maliciosos

El Gobierno Regional Metropolitano cuenta con un sistema de protección antivirus a través de un software ESET EndPoint, diseñado para actuar en ambientes corporativos y que permite una completa protección a los equipos.

El servidor localizará todos los equipos disponibles en la Red e instalará individualmente a través de toda la red del Gobierno Regional Metropolitano mediante un paquete de instalación descargado desde el Servidor de antivirus en el cual se alojarán las respectivas versiones, sean de 32 o 64 bits.
Una vez copiado el paquete de instalación, éste se auto ejecutará y luego de un reinicio de la maquina quedará listo y protegida contra cualquier intrusión.

Las cuentas son en este caso serán los diferentes equipos a través de la red , siendo identificados por el servidor por el nombre de equipo y su respectiva dirección IP.

La actualización se hace de manera automática a través del mismo software que apuntará la última actualización existente en el servidor de antivirus, para finalmente actualizar la base da datos del antivirus.
Esta herramienta, nos permitirá reconocer cualquier dispositivo que sea conectado al computador y poder escanearlo automáticamente evitando así intrusiones indeseadas.

Respecto del correo electrónico, este sistema de protección antivirus escaneara todos los archivos adjuntos, dejando pasar todo aquello que no represente un peligro o vulnerabilidad para los sistemas informáticos del Gobierno Regional Metropolitano, manteniendo lis sistemas libres de riesgos.
El sistema de antivirus tiene un protocolo de cifrado de información que funciona por un lado con la contraseña de usuario y la contraseña del buzón. La primera verifica la identidad del usuario y la segunda el contenido del correo.

9 REGISTRO DE CONTROL

El Departamento de Informática deberá emitir un informe que dé cuenta de las solicitudes recibidas para:

- A.13.02.01 Informe de sistemas de seguridad en la transferencia de información mediante correo electrónico.
- A.13.02.03 Informe de Aplicaciones de Seguridad y filtros al correo electrónico para mensajería segura.

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)

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 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 el mismo estime conveniente, en cuanto a su funcionamiento y correcta aplicación en la Institución.

12 APROBACIÓN

Elaborado por	Revisado por	Aprobado por
Carlos Hernández A. Analista Departamento de Informática	**José Ignacio Gutiérrez G.** Encargado de Seguridad SSI **Paulo Mendoza** Encargado Unidad de Soporte **Carolina Hidalgo M.** Jefa Departamento de Gestión Institucional	**Mayuri Reyes Torres** Presidente Comité de Seguridad

13 REGISTRO DE HISTORIAL DE VERSIONES O MODIFICACIONES

Versión	Autor	Paginas o secciones	Fecha Modificación	Motivo
01	Carlos Hernández	todas	22-11-2011	Creación
02	Carlos Hernández	todas	29-06-2017	Se cambia formato y se actualiza documento
03	Mauricio Marín	4,9	28-09-2017	• Se incorpora control normativo SSI • Se incorpora registro de control

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