DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO INFORMATICA

APRUEBA POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO.

RESOLUCIÓN EXENTA N° 3040

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.

16177944

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° 3163 del 24 de diciembre de 2015, que aprobó la Política General de Seguridad de la Información del Gobierno Regional Metropolitana.

2.- APRUEBASE la Política General de Seguridad de la Información del Gobierno Regional Metropolitana.

ANOTESE Y PUBLIQUESE

INTENDENCIA REGION METROPOLITANA
INTENDENTE

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

IFF/GEP/VGM/MRT/JJG
Distribución:
- Funcionario Gobierno Regional Metropolitano de Santiago
- Honorarios Gobierno Regional Metropolitano de Santiago
- Comité de Seguridad de la Información
- Oficina de Partes

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Versión 9

1 INDICE

2 OBJETIVO

El presente documento corresponde a una sistematización y actualización de las orientaciones estratégicas en materias de seguridad de la información del Gobierno Regional Metropolitano de Santiago.

El Gobierno Regional Metropolitano de Santiago reconoce la importancia de la identificación, clasificación y resguardo de los activos de información, entendiendo como activos de información todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de relevancia para la institución; por lo que se compromete a trabajar en la disminución del nivel de riesgos en el uso, almacenamiento, acceso y distribución de la información, fomentando en todo el personal del Servicio una cultura de seguridad de los activos de información, que involucran el resguardo de su confidencialidad, integridad y disponibilidad.

Esta Política General define los criterios y lineamientos esenciales, en cuanto a la administración, resguardo, custodia y uso de la información y de los bienes asociados a su tratamiento, por lo tanto, se cumplirán los requisitos institucionales, legales o reglamentarios y las obligaciones contractuales en los ámbitos relacionados con la seguridad de la información del servicio.

La Seguridad de la Información es entendida como la prevención de la confidencialidad, integridad, disponibilidad de la información y la protección de ésta, de una amplia gama de amenazas, a fin minimizar el daño, garantizar la continuidad operacional de los procesos institucionales y la entrega de productos y servicios a los usuarios/clientes/beneficiarios.

3 OBJETIVOS ESPECIFICOS

Los objetivos de la gestión de seguridad de la información se han organizado de acuerdo a las categorías de: clasificación y catastro de información, análisis de riesgo y capacitación y difusión al personal.

Es de suma importancia que el inicio de un evento este separado de su autorización y de esta forma evitar posible colusión en el diseño de controles.

3.1 Clasificación y catastro de activos de la información

- Identificar y clasificar los activos de información, según tipo, formato, ubicación, importancia, responsable y procedimiento de manipulación.
- Identificar y etiquetar los activos de información existentes, según la importancia que tienen para la institución.

3.2 Análisis de riesgo

- Identificar y evaluar los riesgos a los que está expuesto el Servicio en de los activos de información e implementar medidas para su control.
- Identificar aquellos activos de información que requieren de una protección adicional.
- Identificar accesos, modificación y utilización de activos sin autorización o detección.

3.3 Capacitación y difusión al personal

Todas las Jefaturas deberán:

- Concientizar y sensibilizar a todo el personal de la relevancia de los activos de información y de la seguridad que deben tener éstos.
- Capacitar a través de talleres, charlas, cursos y seminarios, en temáticas relacionadas a la seguridad, generación, manejo y resguardo de los activos de información relevantes para la institución.
- Proveer de material de apoyo (documentos, manuales y/o textos de referencia) en relación a la seguridad de los activos de información.
- Generar y coordinar instancias de difusión y sensibilización masiva respecto de la importancia de la seguridad de la información en el servicio.
- Publicar toda la documentación relativa a la seguridad de la información, a través de la intranet y/o sitio web institucional.

4 ALCANCE

La presente ***Política General de Seguridad de la Información del Gobierno Regional Metropolitano de Santiago*** es aplicable a la Administración Regional y todas las divisiones, departamentos y unidades que lo conforman y al personal que en éste trabajan.

Asimismo, esta política se complementará con toda aquella documentación que se genere a partir del cumplimiento de la NCh-ISO27001.Of2013 y que sea aprobada por el Comité de Seguridad de la Información del Servicio.

Esta política se matizará y desarrollará en un conjunto de normas, instructivos, estándares y procedimientos, según sea necesario y avance la tecnología o se extienda la información a diferentes plataformas.

5 ROLES Y RESPONSABILIDADES

Es importante que cada documento aprobado por el comité de seguridad de la información dentro de su contenido, determine quienes serán los responsables de cada uno de los procesos de seguridad de la información en un título denominado Roles y Responsabilidades.

El Jefe de Servicio: será el responsable como máxima autoridad de velar por el fiel cumplimiento de todas las políticas y documentos derivados del Sistema de Seguridad de la Información.

Deberá asignar las personas con responsabilidades de seguridad de la información estos podrán delegar sus tareas de seguridad a otros. Sin embargo, seguirán siendo responsables y deberán determinar que cualquier tarea delegada se haya realizado correctamente.

Departamento de Informática: quienes desempeñan funciones relativas a la ***Seguridad de la Información*** y otras de administración relacionadas, serán quienes la administren, la divulguen y la hagan conocida de todos los funcionarios del Servicio

El Comité de Seguridad: será en quienes recae la revisión de la Política General de Seguridad, de manera de asegurar la continuidad operacional de los procesos institucionales y la entrega de productos y servicios a los usuarios, clientes o beneficiarios.

El Comité de Seguridad deberá revisar las políticas de seguridad de la información a intervalos planificados o si se producen cambios significativos, para asegurar su conveniencia, suficiencia y eficacia continua y firmar un Acta de revisión de las Políticas para dar conformidad a todas y cada una de ellas.

Este Comité estará formado por:

- Jefatura División de Administración y Finanzas.
- Jefatura Departamento Jurídico.
- Jefatura Departamento de Gestión institucional.
- Jefatura Departamento de informática
- Jefatura Departamento de Gestión Documental.
- Jefatura Departamento de Servicios Generales
- Jefatura Departamento de Gestión de Personas
- Encargado /a Unidad de Transparencia
- Prevencionista de Riesgo

Encargado de Seguridad del Servicio, será quien esté presente en el desarrollo y la implementación de la Política Seguridad de la Información, además deberá:

- Coordinar la respuesta a incidentes computacionales y otros que afecten a los distintos activos de información institucionales.
- Coordinar y supervisar la implementación de las acciones tendientes a resguardar la seguridad de la información del Servicio.
- Asegurar que los activos de información reciban un nivel de protección adecuado para garantizar su resguardo ante eventuales amenazas.
- Coordinar con el Comité de Seguridad de la Información la respuesta a incidentes que afecten a los activos de información institucionales.
- informar al Comité de Seguridad de la información en relación a los avances, incidentes u otras situaciones que afecten a los activos de información.
- Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes

Funcionarios del Gobierno Regional Metropolitano: la responsabilidad de la seguridad de la información es de todo el personal del Servicio, lo que no obsta a que cada funcionario o usuario asuma su parte de responsabilidad respecto a los medios que utiliza, según los puntos que se indican en esta política.

6 CONTROL NORMATIVO SSI

El siguiente procedimiento tiene por finalidad dar cumplimiento a los siguientes controles de la política NCh-ISO27001.Of2013

Código del Control	Identificación del Control	Requisito de control
A.05.01.01	Políticas para la seguridad de la información	La Dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grupo de políticas para la seguridad de la información.
A.05.01.02	Revisión de las políticas de seguridad de la información	Se deben revisar las políticas de seguridad de la información a intervalos planificados o si se producen cambios significativos, para asegurar su conveniencia, suficiencia y eficacia continuas
A.06.01.01	Roles y responsabilidades de la seguridad de la información	Todas las responsabilidades de la seguridad de la información deben ser definidas y asignadas.
A.06.01.02	Segregación de funciones	Se deben segregar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos de la organización.
A.06.01.04	Contacto con grupos especiales de interés.	Se deben mantener contactos apropiados con los grupos especiales de interés u otros foros especializados en seguridad, así como asociaciones de profesionales
A.18.01.01	Identificación de la legislación vigente y los requisitos contractuales	Todos los requisitos estatutarios, regulatorios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben definir y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.02.02	Cumplimiento con las políticas y normas de seguridad	Las Jefaturas deben revisar con regularidad el cumplimiento del procesamiento de la información y los procedimientos de seguridad que están dentro de su área de responsabilidad, de acuerdo con las políticas de seguridad, normas y requisitos de seguridad pertinentes.

7 COMPROMISOS INSTITUCIONALES

- La información es un bien valioso para el Servicio, que debe ser administrada bajo los más altos estándares de seguridad.
- Se reconoce la seguridad de la información como un atributo necesario en los servicios ofrecidos por el Servicio.
- La información es considerada como un recurso imprescindible para la gestión y operación del negocio.
- La seguridad de la información, es responsable de todos, independiente del cargo que se desempeñe.
- La información es clasificada de acuerdo a criterios de valoración en relación a la importancia que posee para el Servicio.
- La información de la organización sólo puede ser accedida por personas o entidades externas, según la clasificación que se haya hecho de ella en las situaciones y formas expresamente establecidas en las normas vigentes y con controles que garanticen su protección.
- La organización declara su decisión de cumplir con la normativa y legislación vigente en relación a aspectos de reserva y privacidad de la información.
- Todo Funcionario, proveedor o personal externo que preste sus servicios debe acceder exclusivamente a la información que, de acuerdo a su clasificación, le sea autorizada para lo cual se tendrá en consideración las tareas que deban cumplir.
- Todo funcionario tiene la obligación de notificar cualquier actividad o situación que afecte la seguridad de los activos de información.
- El servicio reconoce que la sensibilización, capacitación y entrenamiento a su personal en las materias de seguridad de la información son tareas prioritarias.

8 PROTECCIÓN DE LA INFORMACIÓN

En el Gobierno Regional Metropolitano de Santiago se reconoce expresamente la importancia de la información y de los sistemas de información, así como de la necesidad de su protección, por constituir un activo estratégico y vital, hasta el punto de poder llegar a poner en peligro la continuidad del Servicio, o al menos suponer daños muy importantes, si se produjera una pérdida irreversible de determinados datos.

8.1 Segregación de deberes.

Para segregar las funciones o deberes, el Servicio debería considerar controles como el monitoreo de actividades y supervisión de redes y sistemas con el fin de evitar el uso indebido no autorizado, no intencional de los activos de la organización.

Cada funcionario sólo podrá realizar las tareas y acceder a los datos necesarios que se requieran para cumplir su cometido, es decir se considerará el principio del llamado "mínimo privilegio" para evitar accesos no autorizados, segregando así los perfiles de los usuarios de acuerdo a sus funciones y limitando los accesos con derechos normales, avanzados o de administrador según corresponda.

8.2 Identificación de la legislación vigente

Los accesos y usos de la información, por tanto, estarán en línea con lo que se indica en la presente política y en las leyes, decretos, normas, instructivos, estándares y procedimientos relativos a la seguridad de la información.

El siguiente corresponde al listado de la normativa vigente relacionada con el SSI:

- Ley N°19.553, febrero 1998. Concede asignación de modernización y otros beneficios que indica. Ministerio de Hacienda.
- Decreto N°475. Reglamento Ley 19.553 para la aplicación del incremento por Desempeño institucional del artículo 6° de la Ley y sus modificaciones.
- Ley N°20.212, agosto de 2007. Modifica las leyes N° 19.553, N° 19.882, y otros cuerpos legales, con el objeto de incentivar el desempeño de los funcionarios públicos. Ministerio de Hacienda.
- Ley N°19.799, abril de 2002. Sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma. Ministerio de Economía.
- DS N°181. Reglamento Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.
- Instructivo Presidencial Nº 05, mayo de 2001: Define el concepto de Gobierno Electrónico. Contiene la mayor parte de las instrucciones referidas al desarrollo de Gobierno Electrónico en Chile.
- Instructivo Presidencial Nº 06, junio de 2004: Imparte instrucciones sobre la implementación de la firma electrónica en los actos, contratos y cualquier tipo de documento en la administración del Estado, para dotar así de un mayor grado de seguridad a las actuaciones gubernamentales que tienen lugar por medio de documentos electrónicos y dar un mayor grado de certeza respecto de las personas que suscriben tales documentos.
- DS N°158. Modifica D.S. N° 81 sobre norma técnica para la interoperabilidad de los documentos electrónicos.
- DS N°83. Norma técnica para los órganos de la Administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos.

• DS N°93. Norma técnica para minimizar la recepción de mensajes electrónicos masivos no deseados en las casillas electrónicas de los órganos de la Administración del Estado y de sus funcionarios.
• DS N°14, 27 de febrero de 2014, Ministerio de Economía, Fomento y Turismo. Modifica Decreto Nº 181 de 2002.
• Ley Nº 20.285, agosto de 2008. Regula el principio de transparencia de la función pública y el derecho de acceso a la información de los órganos de la administración del Estado. Ministerio Secretaría General de la Presidencia.
• Instrucción General N°2, mayo de 2009, del Consejo para la Transparencia: Designación de Enlaces con el Consejo para la Transparencia.
• Instrucción General N°3, mayo de 2009, del Consejo para la Transparencia: Índice de Actos o Documentos calificados como secretos o reservados.
• Instructivo Presidencial N°08, diciembre de 2006: Imparte instrucciones sobre Transparencia Activa y Publicidad de la Información de la Administración del Estado.
• Circular Nº3, enero de 2007: Detalla las medidas específicas que deben adoptar los servicios y dispone los materiales necesarios para facilitar la implementación del instructivo presidencial sobre transparencia activa y publicidad de la información de la Administración del Estado.
• Ley Nº 19.880, mayo de 2003: Establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado. Ministerio Secretaría General de la Presidencia.
• Instructivo Presidencial N°4, junio de 2003: Imparte instrucciones sobre aplicación de la Ley de Bases de Procedimientos Administrativos.
• Ley N° 19.628, agosto de 1999. Sobre protección de la vida privada y datos personales. Ministerio Secretaría General de la Presidencia.
• Ley Nº 17.336, octubre de 1970: Sobre propiedad intelectual. Ministerio de Educación Pública.
• Ley Nº 19.223, junio de 1993: Sobre delitos informáticos. Ministerio de Justicia.
• Ley Nº 19.927, enero de 2004: Sobre delitos de pornografía infantil. Ministerio de Justicia.
• Guía Metodológica del Sistema Gobierno Electrónico.
• Guía Metodológica del Sistema Seguridad de la Información.

8.3 Cumplimiento con las políticas y normas de seguridad

Las jefaturas deberán revisar regularmente el cumplimiento y apego a las Políticas de Seguridad de la Información, fomentar la difusión de éstas de forma periódica, se promoverá la formación en seguridad entre funcionarios y colaboradores en previsión de la comisión de errores, omisiones, fraudes o delitos y tratando de detectar la posible existencia de anomalías lo antes posible.

Algunos de los riesgos frente a los que las jefaturas deberán establecer controles adecuados y razonables, tanto preventivos, como de detección y correctivos son: errores y omisiones, sabotajes, vandalismo, espionaje, trasgresión de la privacidad y tráfico de datos, acciones de otros agentes externos no autorizados, y cualesquiera otros que puedan influir en que la información no sea exacta, completa, en definitiva, integra, o no esté disponible dentro del tiempo fijado.

Las jefaturas deberán verificar que se cumplan los requisitos de seguridad de la información establecidos en las Políticas de Seguridad del Gobierno Regional Metropolitano y si se encontrare algún incumplimiento, deberán identificar las causas e identificar e implementar las acciones correctivas necesarias y cerciorarse si han sido efectivas.

9 Política y documentos para la Seguridad de la Información

Con el fin de establecer el enfoque de la organización para administrar sus objetivos de seguridad de la información, el Gobierno Regional Metropolitano ha definido mediante el Comité de Seguridad de la Información un conjunto de políticas, normas, instructivos y otros procedimientos para asegurar la seguridad de la información. Estas son:

- Instructivo correctivo preventivo
- Manual de gestión de archivos
- Norma de acceso a la Red
- Norma de Eliminación de Activos
- Norma de la Seguridad de la información para la Gestión de Proyectos
- Norma de Outsourcing
- Norma de Trabajo Remoto
- Norma de uso identificación y autentificación
- Norma de uso de instalación legal de software
- 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 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 general de seguridad 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 y control de tratamiento de SSI
- Reglamento sobre infracciones al SSI

10 REGISTRO DE CONTROL

El Departamento de Informática deberá emitir un informe que dé cuenta de las acciones realizadas para:

- A.05.01.01 Informe Resolución aprobatoria de Políticas y documentos.
- A.05.01.02 Informe Acta de Revisión Política General de la información
- A.06.01.01 Informe de roles y responsabilidades definidas y asignadas.
- A.06.01.02 Informe de sistemas de implementación de segregación de deberes.
- A.06.01.04 Informe de resolución Encargado de Seguridad con función descrita en control ISO A.06.01.04
- A.18.01.01 Informe de inclusión de legislación vigente en Política General de Seguridad.
- A.18.02.02 Informe de detección de irregularidades por parte de jefaturas.

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 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 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.

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** 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	10-10-10	Creación Documento
02	Carlos Hernández Pablo Fuentes	1-3-9	02-11-10	Incorporación concepto seguridad en los activos de información y modificación acápite "formato de las políticas"
03	Carlos Hernández Pablo Fuentes	8-9	18-11-10	Modificación participantes Comité de Seguridad de la información
04	Carlos Hernández	8	02-12-10	Incorporación Política de Seguridad Informática
05	Carlos Hernández	1-3-4-5	11-12-15	Modificación objetivos de la gestión de seguridad de la información, análisis del riesgo, Norma ISO que aplica, seguimiento y control
06	Carlos Hernández Paulo Serrano L	todas	11-12-15	Precisiones solicitadas por la Red de Expertos por Norma ISO 27.002
07	Carlos Hernández	todas	10-07-17	Modificación de documento para cumplimiento a directrices de la red de expertos SSI. • Se incorpora control normativo SSI Se incorpora registro de control
08	Carlos Hernández	todas	18-10-17	Modificación de Formato, se agrega índice, Revisión, Difusión. Se modifican las responsabilidades
09	Mauricio Marín V	9,10,11	23-11-17	Se incorporan los siguientes subtítulos: 8.1 Segregación de deberes. 8.2 Identificación de la legislación vigente 8.3 Cumplimiento con las políticas y normas de seguridad 9 Política y documentos para la Seguridad de la Información

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