GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO

DIVISIÓN DE ADMINISTRACIÓN Y FINANZAS
DEPARTAMENTO DE INFORMÁTICA

DEJA SIN EFECTO LA RESOLUCIÓN EXENTA Nº 2771 DEL 19 DE DICIEMBRE DE 2018 y APRUEBA NUEVA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

RESOLUCIÓN EXENTA N° 1977

SANTIAGO, 27 DIC 2021

VISTOS:

El Acta de proclamación del Gobernador de la Región Metropolitana de Santiago de fecha 09 de julio de 2021, del Tribunal Calificador de Elecciones; lo dispuesto en las letras h) y ñ) del artículo 24 del Decreto con Fuerza de Ley Nº 1-19.175, del Ministerio del Interior y Seguridad Pública, que fija el texto refundido, coordinado, sistematizado y actualizado de la Ley Nº 19.175, Orgánica Constitucional sobre Gobierno y Administración Regional y sus modificaciones; la Ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado; lo establecido en el Art 9°del D.F.L. N° 1/19.653, que fija el texto refundido, coordinado y sistematizado de la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; el Decreto Nº 83/2005 del Ministerio Secretaría General de la Presidencia sobre seguridad y confidencialidad de los documentos electrónicos; el Instructivo Presidencial Nº8/2018 que imparte instrucciones en materia de ciberseguridad; la Resolución Nº2771/2018 que aprueba la Política General de Seguridad de la Información del Gobierno Regional Metropolitano; el memorándum N° 60-A de 25 de noviembre de 2021 del Departamento de Informática; las Resoluciones Nº 7 de 2019 y N° 16 de 2020, ambas de Contraloría General de la República; y

CONSIDERANDO:

1. Que, es importante considerar los lineamientos que establece la Política Nacional de Ciberseguridad, así como el instructivo respecto a esta materia, procurando velar por la protección de redes, plataformas y sistemas informáticos de los órganos de la administración del Estado.

2. Que, siempre existirá un riesgo potencial con el cual hay que convivir como institución, por lo cual se hace necesario contar con un documento base que entregue las directrices necesarias y responsables de mitigar estos riesgos;

3. Que, dado que las amenazas que afectan a la seguridad de la información institucional están en constante evolución, resulta indispensable, contar con una nueva política, actualizada y acorde a los niveles de amenazas que se ciernen actualmente.

4. Que, de esta forma, se hace necesario dejar sin efecto la política de seguridad de la información vigente y aprobar una nueva.

GOBIERNO REGIONAL DE SANTIAGO DEPARTAMENTO JURIDICO REGIÓN METROPOLITANA

5. Que, el objetivo de esta Política es dar orientación y apoyo a la institución respecto de la seguridad de la información, en concordancia con la normativa legal vigente en la materia.

RESUELVO:

1. DÉJESE SIN EFECTO la Resolución Exenta Nº 2771 del 19 de diciembre de 2018, que aprobó la Política General de Seguridad de la Información de este Gobierno Regional.

2. APRUÉBASE la Política General de Seguridad de la Información del Gobierno Regional Metropolitano de Santiago, que se transcribe a continuación:

"POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

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.

GOBIERNO REGIONAL DE SANTIAGO DEPARTAMENTO JURIDICO REGIÓN METROPOLITANA

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.

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.

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.

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 temáticas relacionadas a la seguridad, generación, manejo y resguardo de los activos de información relevantes para la institución, como por ejemplo talleres, charlas, cursos o seminarios
- 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.

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.

GOBIERNO REGIONAL DE SANTIAGO
DEPARTAMENTO JURÍDICO
REGIÓN METROPOLITANA

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.

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 de la Información: 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 de la Información deberá revisar las políticas, normas, planes, procedimientos e instructivos de seguridad de la información a lo menos una vez al año 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.

Es este Comité de Seguridad quien validará a través de la Formalización Externa todas las demás políticas, normas y procedimientos, planes e instructivos mediante su aprobación quedando signado en el Registro de Acta del Comité de Seguridad de la Información, con excepción de esta Política General de la Seguridad de la Información que será validada o formalizada vía Resolución Administrativa del jefe de Servicio.

Este Comité de Seguridad de la Información estará formado por:

- Jefatura División de Administración y Finanzas.
- Jefatura Departamento Jurídico.
- Jefatura Departamento Planificación y Control Institucional.
- Jefatura Departamento de informática
- Jefatura Departamento de Gestión Documental y Activos.

GOBIERNO REGIONAL DE SANTIAGO DEPARTAMENTO JURIDICO REGIÓN METROPOLITANA

- 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.

DEFINICIONES

Política

Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la organización, en ella se contemplan las normas y responsabilidades de cada área, departamento o unidad de la organización. Las políticas deben ser dictadas desde el nivel jerárquico más alto del Servicio con la intención de normar el actuar de los funcionarios alcanzar los objetivos propuestos.

Información

La información es la interpretación que se da a un conjunto de datos, pudiendo residir esta en medios electromagnéticos, físicos o en el conocimiento de las personas. En el caso de la presente política, se entenderá como información a toda forma proveniente de datos relacionados con los procesos emanados del accionar diario de Gobierno Regional Metropolitano, así como antecedentes proporcionados tanto por los usuarios internos como los externos, siempre que sea dentro del contexto del ejercicio de sus funciones y del cumplimiento de sus obligaciones.

Información Pública

Toda aquella información no catalogada como secreta o reservada, tal como lo establece el ordenamiento jurídico vigente

Información Reservada

Son aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva

unidad del órgano a que sean remitidos, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter, cuando la naturaleza misma de la información requiera ser tratada de manera reservada.

Información Secreta
Son aquellos documentos cuyo conocimiento está circunscrito a las autoridades o personas a las que vayan dirigidos y a quienes deban intervenir en su estudio y resolución, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter. Una norma que establece restricciones claras es la ley de datos personales y los Sumarios calificados como tales.

Seguridad de la Información
Es el nivel de confianza que la organización desea tener de su capacidad para preservar la confidencialidad, integridad y disponibilidad de la información. Tiene como objetivo proteger el recurso información de una amplia gama de amenazas, con el fin de asegurar la continuidad del negocio, minimizar el daño y, cumplir su misión y objetivos estratégicos.

Confidencialidad
Es asegurar que la información es accesible sólo para las personas autorizadas para ello.

Integridad
Es salvaguardar la exactitud y totalidad de la información en su procesamiento, transmisión y almacenamiento.

Disponibilidad
Es asegurar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando estos sean requeridos

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 comunicar a todos los empleados y a las parte externas pertinentes un grupo de políticas para l 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 l información a intervalos planificados o si se produce cambios significativos, para asegurar s 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 l información deben ser definidas y asignadas.
A.06.01.02	Segregación de funciones	Se deben segregar las funciones y las áreas d responsabilidad para reducir las oportunidades d

		modificaciones no autorizadas o no intencionales, 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 lo grupos especiales de interés u otros foro especializados en seguridad, así como asociacione de profesionales
A.18.01.01	Identificación de la legislación vigente y los requisitos contractuales	Todos los requisitos estatutarios, regulatorios contractuales pertinentes y el enfoque de l organización para cumplirlos, se deben definir documentar explícitamente, y mantenerlo actualizados para cada sistema de información y par la organización.
A.18.02.01	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de l seguridad de la información y su implementación (e decir, objetivos de control, controles, políticas procesos y procedimientos para seguridad de l información) se debe revisar de maner independiente a intervalos planificados, o cuand ocurran cambios significativos.
A.18.02.02	Cumplimiento con las políticas y normas de seguridad	Las Jefaturas deben revisar con regularidad e cumplimiento del procesamiento de la información los procedimientos de seguridad que están dentro d su área de responsabilidad, de acuerdo con la políticas de seguridad, normas y requisitos d seguridad pertinentes.

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 responsabilidad 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

GOBIERNO REGIONAL DE SANTIAGO DEPARTAMENTO JURÍDICO REGIÓN METROPOLITANA

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.

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.

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.

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.

Revisión Independiente de la Seguridad de la Información

El Gobierno Regional Metropolitano deberá solicitar una revisión independiente.

Una revisión independiente es necesaria para asegurar la idoneidad, adecuación y efectividad continua del enfoque de la organización para administrar la seguridad de la información. La revisión debería incluir la evaluación de oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluidos los objetivos de política y control.

Dicha revisión la deberían realizar personas independientes del área bajo revisión, es decir, la función de un especialista independiente o una organización externa que se

GOBIERNO REGIONAL DE SANTIAGO
DEPARTAMENTO JURIDICO
REGIÓN METROPOLITANA

especialice en dichas previsiones. Las personas que realizan estas revisiones deberían contar con las habilidades y experiencia adecuada.

El Servicio deberá registrar y considerar las sugerencias hechas por los revisores independientes con el fin de tomar las medidas correctivas y aplicarlas.

Se deberá hacer a lo menos una revisión Independiente. Para esto se podrá considerar realizarla a comienzos del año respecto de los controles e informes presentados en el periodo anterior.

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.

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:

1. Instructivo correctivo y preventivo contra fallas de energía y otras fallas de servicio
2. Manual de gestión de archivos
3. Norma de acceso a la Red
4. Norma de Eliminación de Activos
5. Norma de la Seguridad de la información para la Gestión de Proyectos
6. Norma de Outsourcing
7. Norma de Trabajo Remoto
8. Norma de uso identificación y autentificación
9. Norma de uso de instalación legal de software
10. Norma de reutilización y devolución de activos
11. Plan de Continuidad
12. Plan de emergencia Institucional
13. Política clasificación de activos
14. Política de acceso físico
15. Política de correo electrónico e Internet
16. Política de Derechos de propiedad Intelectual
17. Política de desarrollos de sistemas
18. Política de dispositivos móviles
19. Política de escritorios y pantallas limpias
20. Política de gestión de incidentes de seguridad
21. Política de gestión de la capacidad
22. Política Gestión de Personas
23. Política de la seguridad informática
24. Política de respaldo de la información
25. Política general de seguridad de la información
26. Política gestión de claves
27. Política manejo de activos
28. Política sobre el uso de controles criptográficos
29. Procedimiento de control de las vulnerabilidades técnicas
30. Procedimiento de Controles de Auditoria de Sistemas de Información

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.

GOBIERNO REGIONAL DE SANTIAGO
DEPARTAMENTO JURIDICO
REGIÓN METROPOLITANA

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.

FORMALIZACION EXTERNA

Mediante el acta fecha 23 de noviembre año 2021, se aprueba por parte del Comité de Seguridad de la Información, la Política general de seguridad de la información.

REGISTRO DE REVISION Y ACTUALIZACION HISTORICO

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 modificación acápite "formato d las políticas"**
03	Carlos Hernández Pablo Fuentes	8-9	18-11-10	**Modificación participantes Comit de Seguridad de la información**
04	Carlos Hernández	8	02-12-10	**Incorporación Política d Seguridad Informática**
05	Carlos Hernández	1-3-4-5	11-12-15	**Modificación objetivos de l gestión de seguridad de l información, análisis del riesgc Norma ISO que aplica seguimiento y control**
06	Carlos Hernández	todas	11-12-15	**Precisiones solicitadas por la Re de Expertos por Norma ISO 27.00**
07	Carlos Hernández	todas	10-07-17	**Modificación de documento par cumplimiento a directrices de l red de expertos SSI.** • **Se incorpora control normativo SS** **Se incorpora registro de control**
08	Carlos Hernández	todas	18-10-17	**Modificación de Formato, s agrega índice, Revisión, Difusión. Se modifican la**
09	Mauricio Marín V	9,10,11	23-11-17	**Se incorporan los siguiente subtítulos:** **8.1 Segregación de deberes.** **8.2 Identificación de la legislació vigente** **8.3 Cumplimiento con las política y normas de seguridad** **9 Política y documentos para l Seguridad de la Información**

GOBIERNO REGIONAL DE SANTIAGO
DEPARTAMENTO JURÍDICO
REGIÓN METROPOLITANA

10	Mauricio Marin V.	12	23-04-2018	**Se agrega en Registro de Control e siguiente párrafo: En caso de n haber movimiento en relación algún control que se pide informa deberá reportarse de igual maner señalando que no hub movimiento por lo que no se pud demostrar con algún medio d verificación durante el respectiv periodo.**
11	Mauricio Marin V.	10,11,12	06-06-2018	**Se agrega Control 18.2.1 Respect de la revisión independiente de l Seguridad de la Información**
12	Mauricio Marin V.	todas	13/06/2018	**Comité de Seguridad hace revisió de documento para el año 2018,**
13	Mauricio Marin V.	5, 7, 15	2/11/2018	**Se agrega párrafo respecto de lo roles del Comité de Seguridad Se cambia título 6 de definiciones Se Modifica el título 11 d "Registro de Control" po "Registro de Operación" Se Modifica el título 13 po "Periodicidad de Evaluación Revisión"**
13	Mauricio Marin V.	todas	16/11/2018	**Comité de Seguridad hace revisió del documento**
14	Matias Benitez	Todas	08-07-2019	**Se cambia pie de página.**
15	Matias Benitez.	Todas	12-07-2019	**Comité de la seguridad de l información revisa y aprueb Política general de seguridad de l información año 2019.**

GOBIERNO REGIONAL DE SANTIAGO * DEPARTAMENTO JURIDICO * REGIÓN METROPOLITANA

16	Carlos Hernández	14,17	15-11-2021	**Se quita de último párrafo de 9.3 l siguiente "y otra a mediados d año para ver sugerencias correcciones a los informe finales.** **Se agrega documento "Program de concientización sobr seguridad de la información"** **Se agrega capítulo 1 formalización externa**
17	**Carlos Hernández**	**todas**	**23-11-2021**	**Comité SSI revisa y aprueba añ 2021.**

16. FORMALIZACIÓN INTERNA

	José Ignacio Gutiérrez G. Encargado de Seguridad SSL	
	Paulo Mendoza Encargado Unidad de Soporte	
Carlos Hernández A. **Analista Departamento de Informática**		**Mayuri Reyes T.** Presidente Comité de Seguridad
	Carolina Hidalgo M. Jefa Departamento Planificación y Control Institucional	

GOBIERNO REGIONAL DE SANTIAGO * DEPARTAMENTO JURIDICO * REGION METROPOLITANA

3. **DIFÚNDASE** el presente acto, mediante su remisión por correo electrónico a todos los funcionarios y prestadores de servicio de este Gobierno Regional;

4. **PUBLÍQUESE** un ejemplar en la intranet institucional.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

GOBIERNO REGIONAL METROPOLITANO DE SANTIAGO ★ GOBERNADOR ★

CLAUDIO ORREGO LARRAÍN
GOBERNADOR REGIONAL
REGIÓN METROPOLITANA DE SANTIAGO

JMSM/MRT/JGG/HVV/PDG

Distribución:
- Administración Regional;
- División de Administración y Finanzas
- Departamento de Informática;
- Encargado de Seguridad de la Información (Jefe Departamento de Informática)
- Oficina de Partes

ID DOC

GOBIERNO REGIONAL DE SANTIAGO ★ DEPARTAMENTO JURÍDICO ★ REGIÓN METROPOLITANA

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

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.

GOBIERNO REGIONAL DE SANTIAGO DEPARTAMENTO JURIDICO REGION METROPOLITANA

000021

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 temáticas relacionadas a la seguridad, generación, manejo y resguardo de los activos de información relevantes para la institución, como por ejemplo talleres, charlas, cursos o seminarios
- 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 de la Información: 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 de la Información deberá revisar las políticas, normas, planes, procedimientos e instructivos de seguridad de la información a lo menos una vez al año 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.

Es este Comité de Seguridad quien validará a través de la Formalización Externa todas las demás políticas, normas y procedimientos, planes e instructivos mediante su aprobación quedando signado en el Registro de Acta del Comité de Seguridad de la Información, con excepción de esta Política General de la Seguridad de la Información que será validada o formalizada vía Resolución Administrativa del jefe de Servicio.

Este Comité de Seguridad de la Información estará formado por:

- Jefatura División de Administración y Finanzas.
- Jefatura Departamento Jurídico.
- Jefatura Departamento Planificación y Control Institucional.
- Jefatura Departamento de informática
- Jefatura Departamento de Gestión Documental y Activos.
- 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:

000024

GOBIERNO REGIONAL DE SANTIAGO DEPARTAMENTO JURIDICO REGIÓN METROPOLITANA

- 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 DEFINICIONES

6.1 Política

Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la organización, en ella se contemplan las normas y responsabilidades de cada área, departamento o unidad de la organización. Las políticas deben ser dictadas desde el nivel jerárquico más alto del Servicio con la intención de normar el actuar de los funcionarios alcanzar los objetivos propuestos.

6.2 Información

La información es la interpretación que se da a un conjunto de datos, pudiendo residir esta en medios electromagnéticos, físicos o en el conocimiento de las personas. En el caso de la presente política, se entenderá como información a toda forma proveniente de datos relacionados con los procesos emanados del accionar diario de Gobierno Regional Metropolitano, así como antecedentes proporcionados tanto por los usuarios internos como los externos, siempre que sea dentro del contexto del ejercicio de sus funciones y del cumplimiento de sus obligaciones.

GOBIERNO REGIONAL DE SANTIAGO DEPARTAMENTO JURIDICO REGION METROPOLITANA

6.3 Información Pública

Toda aquella información no catalogada como secreta o reservada, tal como lo establece el ordenamiento jurídico vigente

6.4 Información Reservada

Son aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano a que sean remitidos, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter, cuando la naturaleza misma de la información requiera ser tratada de manera reservada.

6.5 Información Secreta

Son aquellos documentos cuyo conocimiento está circunscrito a las autoridades o personas a las que vayan dirigidos y a quienes deban intervenir en su estudio y resolución, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter. Una norma que establece restricciones claras es la ley de datos personales y los Sumarios calificados como tales.

6.6 Seguridad de la Información

Es el nivel de confianza que la organización desea tener de su capacidad para preservar la confidencialidad, integridad y disponibilidad de la información. Tiene como objetivo proteger el recurso información de una amplia gama de amenazas, con el fin de asegurar la continuidad del negocio, minimizar el daño y, cumplir su misión y objetivos estratégicos.

6.7 Confidencialidad

Es asegurar que la información es accesible sólo para las personas autorizadas para ello.

6.8 Integridad

Es salvaguardar la exactitud y totalidad de la información en su procesamiento, transmisión y almacenamiento.

6.9 Disponibilidad

Es asegurar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando estos sean requeridos

7 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.18.02.01	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se debe

		revisar de manera independiente a intervalos planificados, o cuando ocurran cambios significativos.
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.

8 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 responsabilidad 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.

9 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.

9.1 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.

9.2 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.

9.3 Revisión Independiente de la Seguridad de la Información

El Gobierno Regional Metropolitano deberá solicitar una revisión independiente.

Una revisión independiente es necesaria para asegurar la idoneidad, adecuación y efectividad continua del enfoque de la organización para administrar la seguridad de la información. La revisión debería incluir la evaluación de oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluidos los objetivos de política y control.

Dicha revisión la deberían realizar personas independientes del área bajo revisión, es decir, la función de un especialista independiente o una organización externa que se especialice en dichas previsiones. Las personas que realizan estas revisiones deberían contar con las habilidades y experiencia adecuada.

El Servicio deberá registrar y considerar las sugerencias hechas por los revisores independientes con el fin de tomar las medidas correctivas y aplicarlas.

Se deberá hacer a lo menos una revisión Independiente. Para esto se podrá considerar realizarla a comienzos del año respecto de los controles e informes presentados en el periodo anterior.

9.4 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.

10 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:

1. Instructivo correctivo y preventivo contra fallas de energía y otras fallas de servicio
2. Manual de gestión de archivos
3. Norma de acceso a la Red
4. Norma de Eliminación de Activos
5. Norma de la Seguridad de la información para la Gestión de Proyectos
6. Norma de Outsourcing
7. Norma de Trabajo Remoto
8. Norma de uso identificación y autentificación
9. Norma de uso de instalación legal de software
10. Norma de reutilización y devolución de activos
11. Plan de Continuidad
12. Plan de emergencia Institucional
13. Política clasificación de activos
14. Política de acceso físico
15. Política de correo electrónico e Internet
16. Política de Derechos de propiedad Intelectual
17. Política de desarrollos de sistemas
18. Política de dispositivos móviles
19. Política de escritorios y pantallas limpias
20. Política de gestión de incidentes de seguridad
21. Política de gestión de la capacidad
22. Política Gestión de Personas
23. Política de la seguridad informática
24. Política de respaldo de la información
25. Política general de seguridad de la información
26. Política gestión de claves

27. Política manejo de activos
28. Política sobre el uso de controles criptográficos
29. Procedimiento de control de las vulnerabilidades técnicas
30. Procedimiento de Controles de Auditoria de Sistemas de Información
31. Programa de concientización sobre seguridad de la información
32. Protocolo y control de tratamiento de SSI

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 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.

13 FORMALIZACION EXTERNA

Mediante el acta fecha 23 de noviembre año 2021, se aprueba por parte del Comité de Seguridad de la Información, la Política general de seguridad de la información.

14 REGISTRO DE REVISION Y ACTUALIZACION HISTORICO

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
10	Mauricio Marin V.	12	23-04-2018	Se agrega en Registro de Control el siguiente párrafo: 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.
11	Mauricio Marin V.	10,11,12	06-06-2018	Se agrega Control 18.2.1 Respecto de la revisión independiente de la Seguridad de la Información
12	Mauricio Marin V.	todas	13/06/2018	Comité de Seguridad hace revisión de documento para el año 2018,
13	Mauricio Marin V.	5, 7, 15	2/11/2018	Se agrega párrafo respecto de los roles del Comité de Seguridad Se cambia título 6 de definiciones Se Modifica el título 11 de "Registro de Control" por "Registro de Operación" Se Modifica el título 13 por "Periodicidad de Evaluación y Revisión"
13	Mauricio Marin V.	todas	16/11/2018	Comité de Seguridad hace revisión del documento

14	Matias Benitez	Todas	08-07-2019	Se cambia pie de página.
15	Matias Benitez.	Todas	12-07-2019	Comité de la seguridad de la información revisa y aprueba Política general de seguridad de la información año 2019.
16	Carlos Hernández	14,17	15-11-2021	Se quita de último párrafo de 9.3 lo siguiente "y otra a mediados de año para ver sugerencias y correcciones a los informes finales. Se agrega documento "Programa de concientización sobre seguridad de la información" Se agrega capítulo 13 formalización externa
17	Carlos Hernández	todas	23-11-2021	Comité SSI revisa y aprueba año 2021.

16.FORMALIZACIÓN INTERNA

Elaborado por	Revisado por	Aprobado por

José Ignacio Gutiérrez G.
Encargado de Seguridad SSI

Carlos Hernández A.
Analista Departamento de Informática

Paulo Mendoza
Encargado Unidad de Soporte

Mayuri Reyes T.
Presidente Comité de Seguridad

Carolina Hidalgo M.
Jefa Departamento Planificación y Control Institucional

stg	**ACTA DE REUNION** **COMITÉ DE SEGURIDAD DE LA INFORMACION**	Página 1 de 3 Fecha 23/11/ 2021

ACTA DE REUNION Comité de Seguridad de la Información

Objetivo	Situación SSI año 2021
Fecha y Hora	23-11-2021, 15:00
Lugar	Sala de Reunión 2° Piso

PUNTOS DE LA REUNION

1. Bienvenida
2. Actualización de Documentos
3. Vulnerabilidades año 2021
4. 67 vulnerabilidades detectadas en sitios y páginas webs
    a. Caída de Switch piso 5 - 13 de septiembre 2021
    b. Caída de Switch piso 1 - 27 de septiembre 2021
5. Envío Correo Phishing
6. Protectores de Pantalla
7. Capacitación SSI
8. Mejoras
    a. Switch
    b. GTD Ancho Banda
9. SGD, 0 Papel
10. Eliminación Activos
11. Necesidades Tecnológicas

Aprobación los siguientes documentos

1. **Instructivo correctivo y preventivo contra fallas de energía y otras fallas de servicio**
2. **Manual de gestión de archivos**
3. **Norma de acceso a la Red**
4. **Norma de Eliminación de Activos**
5. **Norma de la Seguridad de la información para la Gestión de Proyectos**
6. **Norma de Outsourcing**
7. **Norma de Trabajo Remoto**
8. **Norma de uso identificación y autentificación**
9. **Norma de uso de instalación legal de software**
10. **Norma de reutilización y devolución de activos**
11. **Plan de Continuidad**
12. **Plan de emergencia Institucional**
13. **Política clasificación de activos**
14. **Política de acceso físico**
15. **Política de correo electrónico e Internet**
16. **Política de Derechos de propiedad Intelectual**
17. **Política de desarrollos de sistemas**

000039

18. Política de dispositivos móviles
19. Política de escritorios y pantallas limpias
20. Política de gestión de incidentes de seguridad
21. Política de gestión de la capacidad
22. Política Gestión de Personas
23. Política de la seguridad informática
24. Política de respaldo de la información
25. Política general de seguridad de la información
26. Política gestión de claves
27. Política manejo de activos
28. Política sobre el uso de controles criptográficos
29. Procedimiento de control de las vulnerabilidades técnicas
30. Procedimiento de Controles de Auditoria de Sistemas de Información
31. Programa de concientización sobre seguridad de la información
32. Protocolo y control de tratamiento de SSI

DESARROLLO DE LA PRESENTACION

José Ignacio da la bienvenida y explica brevemente que es el SSI y las funciones del comité

Se da detalle al comité respecto a las vulnerabilidades CSIRT y las caídas de los switch

Claudio Muñoz y Mayuri Reyes, solicitan al comité la revisión de funcionamiento de cámaras de seguridad del Gore. Debido a problemas que existen actualmente

José Ignacio informa que esta demora se ha debido a que se necesita realizar una revisión inicial de todas las cámaras y su funcionamiento.

Se detallan las mejoras tecnológicas a realizar con carácter de importancia

- Cambios en los switch
- Importancia de dejar el sistema de cámaras en un circuito cerrado fuera de la red

Se recalca la importa de incluir SSI en la inducción a nuevos funcionarios

Se menciona a comité que se enviara cazabobos y que de ahí se realizara una capacitación a quienes caigan en él.

Se establece que el cambio de contraseñas debiera ser cada 6 meses de forma obligatoria empezando con un cambio masivo en marzo. Aplicándose tanto en AD como en sistemas.

Comité solicita que los mensajes de los protectores de pantalla sean un poco más "Rudos" refiriéndose a la gravedad de lo que podría ocasionar una vulneración importante de sistemas

Silvana Torres entrega información

- Acerca del expurgo de documentos
- 2022 se enviará soporte en papel a archivo nacional
- Se está digitalizando documentación antigua
- Menciona que para todo envío a archivo nacional o eliminación debe haber un testigo que vise la correcta digitalización de documentos, transformación digital 21808

José Ignacio retoma la palabra e indica al comité la importancia dentro de todo el proceso de 0 papel de contar con una cloud de respaldo para toda la gran cantidad de archivos que se está generando

Explica que se continuara siempre con el respaldo en cintas. Indica que se necesita realizar respaldo en cintas como parte de SSI

Se aprueban políticas y documentación SSI

Carolina Hidalgo solicita curso de ciberseguridad a comité y participantes

stg	**ACTA DE ASISTENTES COMITÉ DE SEGURIDAD DE LA INFORMACION**	Página 1 de 1 Fecha 23/11/ 2021

N°	NOMBRE	DEPARTAMENTO O UNIDAD	FIRMA
01	José Ignacio Gutiérrez	Departamento de Informática	
02	Mayuri Reyes T.	División Administración y Finanzas	
03	Héctor Valladares	Departamento Jurídico	
04	Carolina Hidalgo	Departamento Planificación y Control Institucional	
05	Silvana Torres	Departamento de Gestión Documental y Activos	
06	Claudio Muñoz	Departamento de Servicios Generales	
07	Paulo Serrano	Departamento de Gestión de Personas	
08	Luz Magaly Nuñez	Unidad de Transparencia	
	Ariel Lagos	Prevencionista de Riesgo	
10	VIRGINIA SAAVEDRA	DAF	
11			
12			
13			

000042

DEPARTAMENTO JURIDICO