Subsecretaría de Prevención del Delito
Ministerio del Interior y Seguridad Pública

Gobierno de Chile

MODIFICA LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN, DE LA SUBSECRETARÍA DE PREVENCIÓN DEL DELITO, APROBADA POR LA RESOLUCIÓN EXENTA N° 1400, DE 2012, DE ESTE ORIGEN, Y SUS MODIFICACIONES, Y APRUEBA TEXTO REFUNDIDO.

MINISTERIO DE HACIENDA
OFICINA DE PARTES

R E C I B I D O

MINISTERIO DE HACIENDA
OFICINA DE PARTES

R E C E P C I Ó N

DEPART. JURÍDICO		
DEP. T. R. Y REGISTRO		
DEPART. CONTABIL.		
SUB. DEP C. CENTRAL		
SUB. DEP. E. CUENTAS		
SUB. DEP. C. P. Y BIENES NAC.		
DEPART. AUDITORIA		
DEPART. V.O.P. U. Y T.		
SUB. DEP. MUNICIP		

R E F R E N D A C I Ó N

REF. POR $ _____
IMPUTAC. _____
ANOT. POR $ _____
IMPUTAC. _____
_____
DEDUC. DTO. _____

MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA
Oficina de Partes
TOTALMENTE TRAMITADO
SUBSECRETARÍA DE PREVENCIÓN DEL DELITO

RESOLUCIÓN EXENTA N° 1696

SANTIAGO, 24 SEP 2019

V I S T O S: Los antecedentes adjuntos; Lo dispuesto en la Ley N° 20.502, del año 2011, del Ministerio del Interior, que "crea el Ministerio del Interior y Seguridad Pública y el Servicio Nacional para la Prevención y Rehabilitación del Consumo de Drogas y Alcohol, y Modifica Diversos Cuerpos Legales"; el literal d) del artículo 2° del Decreto Ley N° 1028, del año 1975, del Ministerio del Interior que "precisa atribuciones y deberes de los Subsecretarios de Estado"; la Resolución Exenta N° 1400, de 2 de agosto de 2012, de la Subsecretaría de Prevención del Delito del Ministerio del Interior y Seguridad Pública, y sus modificaciones; las Resoluciones 6, 7 y 8, de 2019, de la Contraloría General de la República, que fijan normas sobre la exención del trámite de toma de razón; y,

CONSIDERANDO:

1) Que, el artículo 12° de la Ley 20.502, dispone que la Subsecretaría de Prevención del Delito será el órgano de colaboración inmediata del Ministro del Interior y Seguridad Pública en todas aquellas materias relacionadas con la elaboración, coordinación, ejecución y evaluación de políticas destinadas a prevenir la delincuencia, a rehabilitar y a reinsertar socialmente a los infractores de ley, sin perjuicio del ejercicio de las atribuciones que el ministro le delegue, así como del cumplimiento de las tareas que aquél le encargue.

DIVISIÓN JURÍDICA
GABINETE
SUBSECRETARÍA DE PREVENCIÓN DEL DELITO

FRC/ASF/COF/rapb
DISTRIBUCIÓN:
1. División Jurídica y Legislativa
2. División de Adm., Finanzas y Personas
3. Departamento de Planificación, Control y Gestión Institucional
4. Departamento de Informática
5. Departamento de Auditoría Interna
6. Partes y Archivo

1773161

2) Que, de acuerdo a lo dispuesto en el literal d) del artículo 2° del Decreto Ley N° 1028, del año 1975, del Ministerio del Interior, que precisa atribuciones y deberes de los Subsecretarios de Estado, es función de esta Subsecretaria de Estado, impartir instrucciones internas, fiscalizar su aplicación y coordinar la acción de los organismos del sector correspondiente;

3) Que, en este sentido, mediante Resolución Exenta N° 1400, de 2 de agosto del año 2012, de este origen, se estableció la Política de Seguridad de la Información de la Subsecretaría de Prevención del Delito del Ministerio del Interior y Seguridad Pública; acto administrativo que fue posteriormente modificado por las Resoluciones Exentas nros. 1892, de 2 de septiembre del año 2013; 5986, de 14 de septiembre del año 2015; y 1067, de 30 de mayo de 2018, todas de la Subsecretaría de Prevención del Delito;

4) Que, la Política de Seguridad de la Información de esta Subsecretaría, tiene como objetivo establecer el lineamiento institucional referente a la responsabilidad, resguardo y gestión de riesgos de la información, como así también, entregar las directrices generales sobre el acceso, manipulación, procesamiento, transmisión, protección, almacenamiento o cualquier otro tratamiento que se realice sobre los activos de información de la institución. Resulta aplicable a todos los activos de información de la Subsecretaría de Prevención del Delito, considerando sus áreas, departamento, programas, personas, instalaciones, procesos internos, sistemas informáticos, infraestructura tecnológica, redes de comunicación, bases de datos, archivos, datos, documentos físicos, entre otros, así como también a los terceros que mantengan contratos de prestación de servicios con la Institución;

5) Que, como consta de Acta de Reunión, de fecha 30 de agosto de 2019, así como de Resumen Ejecutivo Adjunto, el Comité de Seguridad de la información de esta Subsecretaría decidió modificar y adicionar los aspectos que allí se indican de la precitada Política;

6) Que, por Memorándum N° 51/2019, de fecha 06 de septiembre de 2019, y en el marco del Programa de Mejoramiento de la Gestión, Sistema de Seguridad de la Información PMG SSI 2019, el Jefe del Departamento de Planificación, Control y Gestión Institucional (s) de esta Subsecretaría, solicitó a la División Jurídica y Legislativa la elaboración de una Resolución Exenta que modifique la Política de Seguridad de la Información, con base en la adecuación a la actual Norma NCh.ISO 27.001:2013 y en la Política de Ciberseguridad Nacional definida por el Gobierno;

7) Que, al mismo tiempo, atendida la cantidad de modificaciones efectuadas hasta ahora, resulta aconsejable dictar un texto refundido de la Política en examen;

8) Que, de acuerdo a las consideraciones precedentemente expuestas, se estima pertinente dictar el acto administrativo que sancione las modificaciones y el texto refundido, por tanto

R E S U E L V O

PRIMERO: APRUÉBENSE las modificaciones a la Política General de Seguridad de la Información de la Subsecretaría de Prevención del Delito del Ministerio del Interior y Seguridad Pública, acordadas en reunión del Comité de Seguridad de la Información de esta Subsecretaría, en reunión de fecha 30 de agosto de 2019;

SEGUNDO: Apruébese el siguiente texto refundido de la Política General de la Seguridad de la Información, en su versión final, de acuerdo al texto que consta en la versión 5.0 del documento denominado "Política General de la Seguridad de la Información", Código POL.01, y que se transcribe a continuación:

Política General de Seguridad de la Información

Código del Documento	Versión del Documento
POL.01	5.0

Ministerio del Interior y Seguridad Pública

Subsecretaría de Prevención del Delito

Política General de Seguridad de la Información

Contenido

1 INTRODUCCIÓN

La Subsecretaría de Prevención del Delito, que de acuerdo con lo previsto en la Ley N° 20.502, es el órgano de colaboración inmediata del Ministro del Interior y Seguridad Pública en todas aquellas materias relacionadas con la elaboración, coordinación, ejecución y evaluación de políticas públicas destinadas a prevenir la delincuencia, a rehabilitar y a reinsertar socialmente a los infractores de ley, sin perjuicio del ejercicio de las atribuciones que el Ministro le delegue, así como del cumplimiento de las tareas que aquél le encargue, considera relevante e imprescindible resguardar de manera adecuada y eficientemente la información que posee para el cumplimiento de sus objetivos.

En relación a esto, se declara la necesidad de gestionar la Política General de Seguridad de la Información de la Subsecretaría de Prevención del Delito, esto con la finalidad de identificar, evaluar y controlar los riesgos que pudieran afectar la confidencialidad, integridad y disponibilidad de la información de la Institución.

2 OBJETIVO

La Política General de Seguridad de la Información, tiene como objetivo establecer el lineamiento institucional de la Subsecretaría de Prevención del Delito referente a la responsabilidad, resguardo y gestión de riesgos de la información, como también entregar las directrices generales sobre el acceso, manipulación, procesamiento, transmisión, protección, almacenamiento o cualquier otro tratamiento que se realice sobre los activos de información de la Institución.

3 ALCANCE

Esta Política es aplicable a los principales activos de información que están relacionados a los productos declarados en la ficha de definiciones estratégicas de la Subsecretaría de Prevención del Delito para el período 2018 al 2022 considerando sus áreas, departamentos, programas de gobierno, personas, instalaciones, procesos internos, sistemas informáticos, infraestructura tecnológica, redes de comunicación, bases de datos, archivos y datos, documentos físicos, entre otros, como también es extensible a terceros que mantengan contratos de prestación de servicios con la Institución.

4 ACRÓNIMOS

S.G.S.I.	:	Sistema de Gestión de Seguridad de la Información.
S.S.P.D.	:	Subsecretario(a) de la Subsecretaría de Prevención del Delito.
I.S.O.	:	Organización Internacional de Estándares.
I.E.C.	:	Comisión Electrotécnica Internacional.

5 DEFINICIONES

Seguridad de la Información	:	Conjunto de procesos, metodologías, políticas, normativas, estándares, procedimientos, controles, software, hardware, y otros elementos necesarios para mantener la confidencialidad, integridad y disponibilidad de la información.
Activo de información	:	Recurso del sistema de información como personas, instalaciones, procesos, archivos digitales, documentos físicos, base de datos, intangibles e información en general, entre otros, necesario para que la Institución funcione correctamente y alcance los objetivos propuestos.
Tratamiento de información	:	Actividad de creación, digitación, transmisión, procesamiento, almacenamiento, modificación, eliminación, consulta, o cualquier otra acción que diga relación con manipulación de información.
Proceso	:	Conjunto de actividades o eventos que se realizan de manera estructurada o alternativa con el fin de cumplir un objetivo determinado.
Confidencialidad	:	Propiedad de la información que apunta a que el acceso a la información, sólo pueda ser realizado por personas, sistemas o entidades autorizadas para hacerlo.
Integridad	:	Propiedad de la información que apunta a mantener la exactitud y totalidad de la información, como también los métodos y mecanismos de tratamiento en general.
Disponibilidad	:	Propiedad de la información que apunta a que los usuarios autorizados, tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
No repudio	:	Propiedad de la información que apunta a la prevención de la negación del envío y recepción de un mensaje de datos y manipulación de la información en general.
Sistema de información	:	Uno o más computadores, software asociado, hardware y periféricos, terminales, procesos físicos, medios de transferencia, bases de datos, entre otros, que forman un todo autónomo capaz de realizar tratamiento de información.
Riesgo de información	:	Cualquier acción o situación que podría afectar las propiedades de la información y a su vez ocasionar resultados no esperados para la Institución.
Evento de seguridad	:	Ocurrencia anómala de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o a la falla de controles establecidos, pudiendo ser desconocida y que podría afectar la seguridad de niveles menores a moderados, tales como violaciones a la política, instalación no autorizada de software, accesos denegados a un servidor, etc. y en ningún caso afectando la continuidad operacional.

Incidente de seguridad	:	Materialización de algún riesgo significativo conocido o desconocido para la Institución, o también se entenderá como tal la sumatoria de eventos de seguridad relacionados que afecten de manera considerable al Organismo, tales como acciones que afecten de manera negativa la imagen Institucional; desastres naturales menores que inhabiliten temporalmente las instalaciones de procesamiento; fallas tecnológicas críticas que interrumpan temporalmente la continuidad de las operaciones, entre otros.

6 POLÍTICAS DE SEGURIDAD

6.1 Principio de Constitucionalidad y Legislación

La Política de Seguridad de la Información deberá mantener un lineamiento acorde a las directrices definidas por la Institución, siempre considerando el marco constitucional y legislativo vigente en nuestro país, particularmente lo referido a los derechos y libertades de las personas y otras leyes aplicables al campo de la información y la tecnología.

6.2 Seguridad de la Información en la Institución

Se declara que todo activo de información que sea propio a realizar su tratamiento por personas, sistemas o cualquier otra entidad al interior de la Subsecretaría de Prevención del Delito o por terceros, deberán implementar los mecanismos necesarios para resguardar la confidencialidad, integridad y disponibilidad de la información, permitiendo controlar los riesgos inherentes a los cuales por su naturaleza pueda verse expuesta.

6.3 Implementación de Seguridad de la Información

La implementación se llevará a cabo de manera continua a través de un proceso de mejora en la seguridad, el cual deberá considerar prioritariamente la información de mayor valor para la Institución, abarcando los programas de gobierno y productos estratégicos, y posteriormente extendiéndose a los procesos y áreas de soporte de la Subsecretaría de Prevención del Delito.

6.4 Responsabilidad de las Personas

Toda persona, ya sea funcionario(a) o personal externo a la Institución y que tenga acceso a información de esta, será responsable de mantener el resguardo adecuado de la seguridad de los datos, para lo cual se destinará la siguiente clasificación de tipos de usuarios(as):

- Propietario(a) de información: Persona responsable de una información en particular, como también de su valorización y clasificación.
- Administrador(a) de información: Persona encargada de resguardar la información y administrar las definiciones establecidas por el propietario de la información.
- Usuario(a) de información: Persona que solicita acceso para realizar tratamiento sobre la información resguardada por el Administrador de información.

6.5 Organización de la Seguridad

La Subsecretaría de Prevención del Delito mantendrá una adecuada organización relacionada a la seguridad de la información, para lo cual gestionará a través de un Comité de Seguridad de la Información y/o el Encargado(a) de Seguridad de la Información, normativas, estándares, procedimientos o cualquier otro mecanismo de control que ayuden a mejorar el S.G.S.I. de la Institución.

La facultad que mantiene tanto el Comité como el Encargado(a) de Seguridad de la Información para dictaminar marcos de trabajo de seguridad, contempla también la relación con entidades externas a la Institución y/o terceros que presten servicios de cualquier índole a la Subsecretaría de Prevención del Delito.

6.6 Seguridad Ligada a las Personas

Debido a la importancia que tienen las personas en la Institución, se considera fundamental gestionar la seguridad de la información aplicada al ciclo de vida de las personas y mientras presten servicios para la organización, por lo mismo se incorporarán términos legales de

confidencialidad y responsabilidades de seguridad en los contratos y descripciones de cargos, adicionalmente se desarrollarán planes orientados a incorporar la cultura de seguridad en los funcionarios(as) y en su quehacer laboral, en conjunto con otros mecanismos complementarios a este ámbito, permitiendo entregar un apoyo permanente a la gestión del cambio frente a temas de seguridad de la información en las personas.

6.7 Gestión de Activos de Información

Para hacer más eficiente el proceso de implementación del S.G.S.I., la Institución desarrolla estrategias focalizadas de trabajo para optimizar el uso de los recursos de seguridad, por lo mismo se establecen métodos para la identificación, clasificación y valorización de los activos de información, considerando también la asignación de responsabilidades sobre su tratamiento, permitiendo mantener claramente identificación sobre los activos de información relevante para la Institución y mantener mecanismos acordes para el control de los riesgos de información.

6.8 Seguridad en el Acceso a la Información

La Institución considera fundamental controlar el acceso a los activos de información para mantener su confidencialidad principalmente, por tanto los archivos digitales, documentos electrónicos, bases de datos, software y aplicativos, entre otros, son componentes esenciales para lograr el cumplimiento de los objetivos de la Institución, por lo mismo y en relación a este principio es que los sistemas de información del organismo cuentan con medidas de control que son adecuadas para mantener el resguardo de la información, considerando normativas de acceso, gestionando cuentas de usuarios autorizados, estableciendo responsabilidades por parte de las personas, controlando el ingreso a las redes de comunicación y equipos computacionales, como también aplicando mecanismos de protección de acceso sobre las aplicaciones y la información de la Institución, tratando de evitar en todo momento que pueda verse afectada por el acceso o la manipulación no autorizada.

6.9 Criptografía

Los controles criptográficos tienen como objetivo principal proteger y garantizar la confidencialidad, integridad y no repudio de la información, mediante el uso de técnicas especializadas. Debido al importante volumen de información que genera e intercambia la Subsecretaría de Prevención del Delito a través de sus diferentes sistemas y servicios tecnológicos en general, se hace necesaria la aplicación de mecanismos criptográficos que permitan robustecer estas actividades.

El uso de cifrado para proteger la información sensible que se intercambia a través de medios magnéticos y/o dispositivos de almacenamiento masivo, líneas de comunicación directa como correo electrónico y enlaces dedicados, es de vital importancia; asimismo, el resguardo de las claves de acceso a sus diferentes sistemas de información, sobre todo cuando se trata de sistemas publicados en la Internet. Todo ello deberá ser definido mediante una evaluación de riesgo con la cual se pueda identificar el nivel de protección requerida según sea el caso.

La Institución deberá contar con una política que contribuya a la implementación de controles criptográficos al interior de la organización y sus procesos, tales como la definición de roles y responsabilidades en cada fase de la implementación de estos controles y procedimientos formales para su efectiva aplicación; tomando en consideración también las regulaciones, mejores prácticas y restricciones nacionales que pudiesen aplicar en el uso de cada técnica adoptada.

6.10 Seguridad Física y Ambiental

Los activos de información físicos, tales como centros de atención o denuncia, oficinas administrativas, áreas de procesamiento de información, equipos tecnológicos y de soporte, información en medios físicos, entre otros, son base para el cumplimiento de los objetivos de la Institución, por lo mismo se mantendrán normativas, controles y otros mecanismos que resguarden la seguridad de las instalaciones y ambientes de trabajo, el acceso a las áreas, el manejo de los documentos, los mecanismos físicos para el tratamiento de la información, el hardware que da soporte a los procesos, entre muchos otros, permitiendo garantizar la protección de los activos de información frente a amenazas físicas, ambientales y naturales.

6.11 Seguridad de las Operaciones

Gran parte de la información que se manipula en la Institución se encuentra en formato digital, por lo mismo se considera de vital necesidad gestionar los riesgos asociados a las operaciones de los activos de información, el definir responsabilidades y segregación de funciones, documentar las operaciones en el tratamiento de información, establecer criterios de calidad para la aceptación de los sistemas de información, administrar planes de respaldo, implementar mecanismos de monitoreo y supervisión de los eventos de la plataforma tecnológica incluyendo también las vulnerabilidades y amenazas que pudiesen impactar de forma negativa sobre la Institución; todo esto permite mantener un nivel de seguridad aceptable con respecto al resguardo de los activos de información.

6.12 Seguridad de las Comunicaciones

Un aspecto fundamental que debe ser gestionado dentro del ambiente tecnológico es la seguridad en las telecomunicaciones. Para ello se hace imperativa la implementación de controles y mecanismos que resguarden y protejan las redes tecnológicas de la Institución tanto en el perímetro interno como en el externo; además de contar con estándares y procedimientos que permitan llevar a cabo de manera controlada y segura, las funciones de intercambio de información de la Subsecretaría de Prevención del Delito con partes externas. Entendiendo así también la existencia mínima de acuerdos de nivel de servicio donde se garantice la confidencialidad y secreto de la información, además del resguardo de la mensajería electrónica y cualquier otro mecanismo de intercambio de información que sea definido en la Institución.

6.13 Seguridad en la Adquisición, Desarrollo y Mantención de Sistemas de Información

La Institución cuenta con sistemas de información que dan soporte a los procesos internos y programas estratégicos de la Subsecretaría de Prevención del Delito, con lo cual permite entregar una mayor calidad y seguridad en la ejecución de las actividades y optimizar el uso de los recursos informáticos, sin embargo la incorporación de nuevas tecnologías en la organización también incorpora riesgos que son propios de esta, por lo mismo la institución mantiene mecanismos que permitan controlar estos riesgos a través de normativas y estándares base de requerimientos de seguridad, metodologías y procesos formales para la construcción de sistemas, implementación de controles criptográficos, como también actividades de aseguramiento de software.

Por otra parte, los sistemas de información que se encuentran en producción cuentan con medidas de control que permitan resguardar adecuadamente los archivos de sistema y la información sobre la cual se realiza tratamiento, normativas y herramientas de gestión de cambios y de configuración, son acciones que ayudan al cumplimiento de esta política y en el logro de los objetivos de la Institución.

6.14 Relaciones con el Proveedor

Con el fin de dar continuidad de forma segura a la entrega de los servicios o productos prestados por proveedores externos, específicamente aquellos asociados al tratamiento de información, es fundamental garantizar que el proveedor cuente al menos con el mismo estándar de mecanismos y controles de seguridad definidos por la Institución; en consecuencia, los proveedores deberán estar en conocimiento de las políticas de seguridad de la Subsecretaría y garantizar su cumplimiento.

Previamente a la contratación del servicio, se deberán ejecutar acciones que permitan identificar las amenazas potenciales a las cuales pudiese estar expuesta la Institución. En base a lo anterior, será importante priorizar que el futuro proveedor de servicios cuente con certificaciones vigentes en el ámbito de seguridad de la información.

Dentro del contrato de servicio, se deberán definir los requisitos de seguridad de la información que contribuyan a delimitar las responsabilidades de cada proveedor para con esto proteger a la Institución de los riesgos asociados a los componentes tecnológicos y activos de información involucrados en el ciclo de vida del servicio a prestar. Así también, indicar el derecho que tendrá la Institución de solicitarle al proveedor las evidencias que avalen la puesta en práctica de sus estándares y niveles adecuados en aspectos de seguridad. Se deberán incluir los acuerdos de nivel de servicio que garantizarán la disponibilidad permanente del servicio entregado por el proveedor y los acuerdos de confidencialidad y no divulgación de la información entre las partes.

La Institución podrá realizar inspecciones o visitas a las instalaciones del proveedor para constatar las condiciones del servicio, particularmente en los casos de prestación de servicios de almacenamiento y resguardo de información; asimismo, será la responsable de realizar el monitoreo de la disponibilidad de los servicios tecnológicos, plataforma y sistemas de información entregados por el proveedor. Los aspectos anteriores deberán quedar formalizados en el contrato de servicio.

6.15 Gestión de Incidentes de Seguridad

La retroalimentación de parte de las personas y entidades es base para mejorar el control interno de la Institución, por lo mismo se desarrollan canales de comunicación para la notificación de eventos, debilidades y oportunidades de mejora en el S.G.S.I., como también se establecen equipos de respuesta frente a eventuales incidentes que puedan afectar la seguridad de la información, considerando el análisis y aprendizaje de los efectos generados por dichas situaciones e implementando mecanismos que permitan prevenir o detectar su ocurrencia, además de minimizar su impacto y/o probabilidad, apoyando la mejora continua del sistema de seguridad.

En relación a los canales de comunicación para la notificación de incidentes vinculados al ámbito tecnológico, es deber del Encargado de Ciberseguridad de la Institución, reportar al Centro de Coordinación de Entidades de Gobierno C-SIRT mediante los medios o canales establecidos, cualquier incidente de Ciberseguridad que se presente, ponga en riesgo o impacte de forma negativa los activos de información o plataformas tecnológicas de la Subsecretaría.

6.16 Gestión de la Continuidad de Negocio

Los productos estratégicos son la cadena de valor de la Subsecretaría de Prevención del Delito, por lo mismo se deben implementar los mecanismos necesarios para mantener su continuidad operacional frente a situaciones que pudieran afectar prioritariamente su disponibilidad, donde la infraestructura, la tecnología, los procesos, las personas y la información son la base fundamental sobre la cual se centran los planes de continuidad de negocio, los que a

través de la gestión de riesgos, el análisis de impacto, el desarrollo de estrategias y los planes de contingencia y recuperación, permiten garantizar razonablemente la operación de los productos estratégicos de la Institución.

6.17 Gestión del Cumplimiento Normativo

El marco regulatorio, legislativo y constitucional de nuestro país representa los límites de aplicabilidad de esta política, como también obliga el cumplimiento de la normativa vigente relacionada a la información y la tecnología, leyes relacionadas a la propiedad intelectual, el manejo de datos personales, los documentos electrónicos y la firma digital, los delitos penales asociados a la tecnología y los sistemas de información, o sobre las comunicaciones y su privacidad, la política nacional de ciberseguridad, entre otras, así como también el marco normativo interno de seguridad de la información, son considerados relevantes para la Institución, por lo mismo se mantienen herramientas de auditoría en los sistemas de información y un adecuado control a través de entidades independientes y objetivas podrán monitorean y supervisan periódicamente su cumplimiento.

7 ROLES Y RESPONSABILIDADES

7.1 Subsecretario(a) de la Institución

Responsable de liderar la implantación y mejora continua del S.G.S.I., en donde sus funciones claves son de aprobar políticas y validar el proceso de gestión de Seguridad de la Información, como también de aprobar las estrategias y mecanismos de control para el tratamiento de riesgos, además de colocar a disposición los recursos necesarios para su ejecución.

7.2 Comité de Seguridad de la Información

Responsable de gestionar la Política de Seguridad de la Información, en donde sus funciones claves son de asegurar que las actividades sean ejecutadas en conformidad con la política de seguridad de la información, definir y aprobar la implementación de normas vinculados a la política de seguridad de la información, identificar y evaluar las acciones correctivas para dar solución a las observaciones de auditoría, aprobar las metodologías y procesos relacionados a la evaluación del riesgo y la seguridad de la información, identificar cambios significativos que pudieran generar riesgos en el procesamiento de la información, proponer soluciones y evaluar la idoneidad y coordinación en la implementación de los controles de seguridad de información, establecer medios para la concientización y capacitación del personal en temas de seguridad de la información, arbitrar conflictos en materia relacionada a la seguridad de la información, sus riesgos y soluciones, evaluar la información recibida de los incidentes de seguridad de la información, emitiendo recomendaciones para su prevención, detección y corrección, como también reportar a la Alta Dirección, respecto a oportunidades de mejora en el S.G.S.I., así como de los incidentes relevantes y su solución.

7.3 Encargado(a) de Seguridad de la Información

Responsable de asesorar al Jefe(a) de Servicio y coordinar actividades de gestión de seguridad relativas a la información, en donde sus funciones claves son de proponer políticas y normativa a la Alta Dirección y al Comité de Seguridad de la Información para su aprobación y velar por su correcta aplicación, coordinar la respuesta a incidentes de seguridad que afecten a los activos de información que dan soporte a los procesos institucionales, establecer puntos de enlace con encargados(as) de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias en materia de seguridad de la información, gestionar la creación y/o aprobación de estándares y procedimientos documentados operativos de seguridad para el tratamiento de los activos de información, proponer al responsable por omisión de los

documentos electrónicos de esta Subsecretaría conforme al artículo 14° del Decreto Supremo N° 83 de 2004 emitida por el Ministerio Secretaría General de la Presidencia, formular los planes de contingencia para asegurar la continuidad de las operaciones críticas de esta Subsecretaría, conforme al artículo 35 del Artículo primero del Decreto Supremo N° 83 de 2004 emitida por el Ministerio Secretaría General de la Presidencia, monitorear el avance general de la implementación de las estrategias de control y tratamiento de riesgos, como también mantener la coordinación con otras unidades del Servicio para apoyar los objetivos de seguridad.

7.4 Auditoria Interna

Otorgar aseguramiento a la Dirección sobre el cumplimiento de la Política de Seguridad de la Información, a través de las actividades de auditoría que se encuentren programadas o le sean encomendadas.

7.5 Supervisores de Cumplimiento de Seguridad de la información

Los jefes de sección, departamento, programa, división, servicio y todo aquel funcionario que tenga personal bajo su cargo, serán los responsables de garantizar el cumplimiento de la Política de Seguridad de la Información y sus normativas dentro de los procesos correspondientes a su Unidad, en cuanto a:

- Promover dentro de su equipo de trabajo, el uso intransferible de sus credenciales (usuario y contraseña) de acceso a los distintos aplicativos y/o herramientas de la Institución, así como la custodia y resguardo de las mismas.

- Garantizar la manipulación adecuada de documentos en los escritorios de trabajo, pudiendo llevar a cabo como referencia las siguientes acciones:

  - Asegurarse de que cada integrante de su equipo de trabajo cuente con los muebles adecuados para el almacenamiento seguro de sus documentos sensibles y confidenciales. De existir alguno que no cuente con los mismos, deberá solicitarlos al Departamento de Administración.
  - Distribuir recordatorios en las áreas clave del recinto de trabajo de manera tal que los funcionarios o asesores recuerden seguir con las Normas *del escritorio despejado y de la manipulación de documentos en los escritorios de trabajo.*
  - Realizar revisiones rápidas y frecuentes al recinto de trabajo, las cuales le permitan asegurarse de que los funcionarios o asesores están cumpliendo con la *Norma del escritorio despejado*. Asimismo, según el volumen de la información confidencial, secreta y/o sensible que maneja la jefatura, designar al azar y forma frecuente, a uno o más funcionarios que contribuyan al control y despeje de las áreas, siendo esto parte de sus funciones laborales correspondientes al período designado.
  - Motivar la generación de documentos en formato electrónico antes de documentos impresos, de manera tal que solo se imprima el material estrictamente necesario en la jefatura; por ende, los funcionarios o asesores tengan que resguardar o custodiar una menor cantidad de información impresa.

- Implementar controles a fin de garantizar de forma segura y eficiente el proceso de destrucción de documentos, tales como:

  - Enviar constantemente comunicaciones electrónicas a todos los funcionarios o asesores que conforman su equipo de trabajo, instando al cumplimiento de lo indicado en la sección *4.3 De la destrucción eficaz de documentos*, contenida en la *Norma de*

seguridad física y ambiental para las instalaciones y áreas internas, disponible en la Intranet de la Subsecretaría de Prevención del Delito.

- Distribuir recordatorios en las áreas clave del recinto de trabajo de manera tal que los funcionarios o asesores recuerden destruir todo aquel documento físico que no sea requerido para su uso.

- Velar por que el personal a su cargo porte en un lugar visible el carnet que lo identifica como empleado de la Institución.

- Motivar a que los funcionarios o asesores bajo su supervisión bloqueen su estación de trabajo antes de dejarla desatendida. Asimismo, promover el correcto apagado de sus equipos al culminar la jornada de trabajo.

- Participar en el proceso de sensibilización frecuente y continua sobre los aspectos de seguridad de la información dentro de su equipo de trabajo.

- Promover dentro de su equipo de trabajo la implementación de compañía guiada en el caso de la visita y de esta manera evitar que ésta se extienda a lugares que no correspondan. Asimismo, motivar el desarrollo de un ambiente de pertenencia en el área física que ocupan conjuntamente con los funcionarios o asesores que conforman su equipo de trabajo de manera tal que estos contribuyan con el avistamiento y notificación al encargado de la recepción, de personas desconocidas transitando en el interior de cualquiera de las áreas de su servicio.

Adicionalmente, deberá contribuir y promover el cumplimiento de todos los aspectos contenidos en la *Norma de seguridad física y ambiental para las instalaciones y áreas internas*, que no hayan sido resaltadas anteriormente. Esta Norma se encuentra publicada en la intranet de la Institución.

Finalmente, deben informar sobre incidentes de seguridad o acciones que transgredan los objetivos declarados o que puedan atentar contra los criterios básicos de la información de la Institución.

7.6 Funcionarios(as), Asesores(as) y Terceros Relacionados

Responsable de dar cumplimiento a la Política de Seguridad de la Información y sus normativas, además del deber de informar sobre incidentes de seguridad o acciones que transgredan los objetivos declarados o que puedan afectar la confidencialidad, integridad y disponibilidad de la información de la Institución.

8 METODOLOGÍAS DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

8.1 Metodología de Gestión de Seguridad

La Institución adoptará para todo efecto lo dictado en la norma estándar NCh ISO/IEC 27001 Of.2013 y NCh ISO/IEC 27002 Of.2013; sin embargo, para ámbitos específicos y de contribuir de mejor manera a esta política, se considerarán otras normativas existentes relacionadas a las anteriores, constituyéndose en la base fundamental de todo el marco de gobernabilidad del Sistema de Gestión de Seguridad de la Información.

8.2 Metodología de Gestión de Riesgos

La Institución adopta la metodología establecida por la Dirección de Presupuestos o Red de expertos designada para la gestión de riesgos de la información y su tratamiento de control, la cual se encuentra documentada a través de la Guía Metodológica emitida por dichos Organismos, siendo consistente y alineada con lo establecido en las mejores prácticas de gestión de riesgo.

9 OBSERVANCIA DE POLÍTICAS, NORMATIVAS, ESTÁNDARES Y PROCEDIMIENTOS

9.1 Responsabilidad por Incumplimiento

Todo incumplimiento de las políticas, normativas, estándares y/o procedimientos de seguridad, esto bajo el marco de la normativa legal vigente y/o el Estatuto Administrativo según corresponda, por parte de cualquier servidor(a) que se desempeñe en la Institución será evaluado por el Comité de Seguridad de la Información quién deberá informar del hecho al S.S.P.D. para que determine de ser procedente la instrucción de un proceso disciplinario.

10 DIFUSIÓN Y REVISIÓN

10.1 Difusión de la Política

La difusión de esta política se realizará mediante correo electrónico a todo el personal de la Subsecretaría de Prevención del Delito y terceros relacionados contractualmente, además su versión digitalizada quedará a disposición en el sitio Web interno y externo de la Institución para facilitar su acceso y conocimiento.

10.2 Revisión de la Política

La revisión formal de esta política se realizará a lo menos cada 3 años desde la fecha de su publicación por el Comité de Seguridad de la Información; sin embargo, bajo circunstancias que estimen conveniente, la política será revisada a intervalos menores según sea necesario para mantener un adecuado lineamiento con la misión y objetivos de la Institución.

10.3 Revisión de Cumplimiento de la Política

El Departamento de Auditoría Interna de la Institución tendrá la responsabilidad de llevar a cabo el aseguramiento de aspectos generales en relación al cumplimiento de esta política, el cual se desarrollará de manera anual como parte del programa de actividades de auditoría que sean realizadas en las diferentes áreas del Organismo.

10.4 Revisión de la documentación derivada de la Política

Toda norma, estándar o procedimiento derivado del cumplimiento de la Política General de Seguridad de la Información de la Institución, será actualizado cuando el propietario del procedimiento así lo considere en base a la implementación de algún cambio relacionado con la estructura organizativa o en la definición estratégica de la Subsecretaría, en los procesos de negocio propios de cada área o en la plataforma tecnológica que soporta estos procesos, cambios en el marco regulatorio aplicable a la Institución y ante la ocurrencia de incidentes graves que afecten a la Institución debido a la falta de efectividad de algún control.

La difusión de los documentos derivados de las directrices de la Política se deberá realizar cada vez que surja alguna necesidad de cambio en cualquiera de estos, mediante correo electrónico entre las partes interesadas y su versión digitalizada quedará a disposición en el sitio Web interno de la Institución para facilitar su acceso y conocimiento.

11 CONTROL DOCUMENTAL

11.1 Control de Revisión

Nombre	Cargo	Actividad	Firma
Natalia Huenchul Llebul	Encargado de Seguridad de la Información.	Creación del documento	
Dominique Díaz Rohde	Encargada PMG Seguridad de la Información.	Revisión del documento	
Ariel Severino Fuentes	Jefe Sección de Informática.	Revisión del documento	
Mauricio Toro Rojas	Jefe Departamento Gestión de Personas.	Revisión del documento	
Juan Salazar Lorca	Jefe Departamento de Administración.	Revisión del documento	
María Fernanda Román Castellano	Jefa División de Administración, Finanzas y Personas.	Revisión del documento	

11.2 Control de Aprobación

Nombre	Cargo	Fecha	Firma
Katherine Martorell Awad	Subsecretaria de Prevención del Delito.	05-09-2019	

11.3 Control de Cambios

Versión	Cambio	Fecha	Aprobador
1.0	Aprobación y difusión del documento.	02.08.2012	Cristobal Lira Ibáñez
2.0	Incorporación de términos legales y responsabilidad en el punto 6.7 Seguridad Ligada a las Personas. Revocación de reportar monitoreo en el punto 7.2 al Comité de Seguridad de la Información. Adecuación de nuevas funciones en el rol 7.3 Encargado(a) de Seguridad de la Información. Modificación en el punto 5 de definición de incidente de seguridad e incorporación de evento de seguridad. Modificación en las políticas 6.12 de Gestión de Incidentes de Seguridad. Se incorpora el punto 10.3 que hace referencia a la revisión del cumplimiento de la política.	02.09.2013	Cristóbal Lira Ibáñez
3.0	Se modifica alcance para ser ajustado a las definiciones estratégicas establecidas en la ficha A1. Se elimina de la política el atributo de legalidad de la información, ajustando propiedades a lo establecido por la Dirección de Presupuesto. Se modifica la metodología ISO/IEC 27.001:2009 que apoya el sistema de gestión por su nueva versión ISO/IEC 27.001:2013.	25.08.2015	Antonio Frey Valdés
4.0	Se incorpora como parte de la política de cumplimiento normativo los aspectos de ciberseguridad en el punto 6.14. Se adecúa documento para dar cumplimiento a los aspectos de equidad de género.	26.04.2018	Katherine Martorell Awad

5.0	Incorporación de nueva definición de "No Repudio" en la sección 5. Se incorpora como parte de la política de cumplimiento normativo los aspectos relacionados con criptografía y relaciones con proveedores de servicios en las secciones 6.9 y 6.14 respectivamente. Incorporación del nuevo rol Supervisores de Cumplimiento de Seguridad de la Información en el punto 7.5. Reorganización de la estructura de la sección 6. Políticas de Seguridad, garantizando la inclusión de los controles normativos adecuados a la versión ISO/IEC 27001:2013. Se separa la política Seguridad en las Comunicaciones y Operaciones, constituyendo así los puntos 6.11 Seguridad en las Operaciones y 6.12. Seguridad en las Comunicaciones. Modificación de la sección 6.15 Gestión de incidentes de seguridad, incorporando la ejecución de reportes al C-SIRT de Interior. Se incorpora la sección 10.4 Revisión de la documentación derivada de la Política, los aspectos relacionados con la actualización y difusión de las normas, estándares y procedimientos derivados de las directrices definidas en el presente documento.	05-09-2019	Katherine Martorell Awad

11.4 Publicación y Difusión

Listado de Distribución

- Intranet de la Subsecretaría de Prevención del Delito.
- Correo electrónico a todos(as) los(as) usuarios(as) del servicio.

TERCERO: Dejese sin efecto la Resolución Exenta N° 1400, de 2 de agosto del año 2012, de este origen y sus modificaciones.

ANÓTESE Y COMUNÍQUESE

KATHERINE MARTORELL AWAD
SUBSECRETARIA DE PREVENCIÓN DEL DELITO
MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA