Subsecretaría de Prevención del Delito
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

MINISTERIO DEL INTERIOR Y SEGURIDAD PUBLICA
Oficina de Partes
-7 MAR 2013
TOTALMENTE TRAMITADO
SUBSECRETARIA DE PREVENCION DEL DELITO

MINISTERIO DE HACIENDA
OFICINA DE PARTES
RECIBIDO

MINISTERIO DE HACIENDA
OFICINA DE PARTES
RECEPCIÓN

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		

REFRENDACIÓN

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

CCF/COF/cic
DISTRIBUCIÓN:
1. **Carlos Lobos Medina.** [redacted]
2. Gabinete Subsecretario.
3. División Jurídica.
4. Oficina de Partes.

GABINETE

DENIEGA PARCIALMENTE ENTREGA DE INFORMACIÓN SOLICITADA POR DON CARLOS LOBOS MEDINA, POR CONCURRIR LA CAUSAL DE SECRETO O RESERVA ESTABLECIDA EN EL ARTÍCULO 21 N° 1 DE LA LEYN° 20.285.

RESOLUCIÓN EXENTA N° 207

SANTIAGO, 26 DE FEBRERO DE 2013

HOY SE RESOLVIO LO QUE SIGUE

VISTOS: Los antecedentes adjuntos, lo dispuesto en la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, aprobada por el artículo 1º de la Ley Nº 20.285, de 2008, en adelante, Ley de Transparencia; la Ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado cuyo texto refundido, coordinado y sistematizado fue fijado por el D.F.L. Nº 1/19.653, del 2000, del Ministerio Secretaría General de la Presidencia; la Ley N° 20.502, 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 Decreto Supremo Nº 13, de 2009, del Ministerio Secretaría General de la Presidencia, que aprueba el Reglamento del artículo primero de la Ley Nº 20.285, de 2008; la Resolución Nº 1600, de 30 de octubre de 2008, de Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón; la Instrucción General N° 10 del Consejo para la Transparencia, publicada en el Diario Oficial el 17 de diciembre de 2012; y,

14535959

CONSIDERANDO: 1) Con fecha 06 de febrero de 2013 se recibió la solicitud de acceso a la información Nº AB091W0000093, cuyo tenor literal es el siguiente: *"Estimada(o)s, En el marco de un proyecto de investigación en materias de seguridad de la información y continuidad del negocio, les agradeceríamos nos pudiesen proporcionar la siguiente información: Política de Seguridad de la Información Procedimiento de Gestión de Incidentes Política de Continuidad del Negocio Procedimientos de Análisis del Impacto en el Negocio Planes de Continuidad del Negocio desarrollados Planes de Recuperación de Desastres desarrollados Planilla EXCEL PMG Sistema de Seguridad de la Información (la enviada a Dipres para validación en diciembre 2012 o la más actualizada que posean) En caso de no tener algunos de los documentos y/o archivos solicitados les agradeceríamos especificar claramente ello, de igual forma les solicitamos no enviarnos la información impresa a menos que sea estrictamente necesario. Atento a sus comentarios"*

2) Que de acuerdo a lo dispuesto en el inciso 2° del artículo 10 de la Ley N° 20.285, el acceso a la información comprende el derecho a acceder a la información contenida en actos, resoluciones, actas, expedientes, contratos y acuerdos, así como toda la información elaborada con presupuesto público, cualquiera sea su formato o soporte.

3) Que el artículo 5° del citado cuerpo legal dispone que son públicos los actos y resoluciones de los órganos de la Administración del Estado, sus fundamentos, los documentos que les sirvan de sustento y complemento directo y esencial, y los procedimientos que se utilicen para su dictación; la información elaborada con presupuesto público; y toda otra información que obre en poder de la Administración, cualquiera sea su formato, soporte, fecha de creación, origen, clasificación o procesamiento; a menos que esté sujeta a las excepciones señaladas en la Ley de Transparencia.

4) Que, en lo que respecta a la Política de Seguridad de la Información requerida, la autoridad que suscribe viene en acceder a la entrega completa de la información solicitada, mediante copia de la Resolución Exenta N° 1.400, de 02 de agosto de 2012 de nuestra institución, que Aprueba la Política General de Seguridad de la Información de la Subsecretaría de Prevención del Delito y Anexo.

5) Que en cuanto al Procedimiento de Gestión de Incidentes solicitado, es dable señalar, que a la fecha éste procedimiento opera a través de nuestra mesa de ayuda; pero que -sin embargo- no se encuentra documentado formalmente, pues se planea realizar como actividad dentro del denominado Plan de Seguridad año 2013, el cual se está desarrollando.

6) Que, la Subsecretaría de Prevención del Delito es una institución nueva que, en conformidad con lo dispuesto en el DFL N° 3/20.502, de 2011, inició sus actividades con fecha 1 de septiembre de 2011, por tanto los documentos asociados a la Política de Continuidad del Negocio, los Procedimientos de Análisis del Impacto en el Negocio, los Planes de Continuidad del Negocio desarrollados y los Planes de Recuperación de Desastres desarrollados; no se encuentran disponibles pues forman parte

de diversos antecedentes que se encuentran en proceso de análisis -asunto previo- para el desarrollo del "Plan de Continuidad de Negocios" institucional.

7) Que, en lo concerniente a la *"Planilla EXCEL PMG Sistema de Seguridad de la Información (la enviada a Dipres para validación en diciembre 2012 o la más actualizada que posean)"*, se entregará parcialmente la información requerida,

por cuanto y en virtud del artículo 21 N° 1 de la Ley N° 20.285, algunos de los documentos que ella contiene, comprenden información sensible o estratégica, que puede vulnerar o amenazar la seguridad operacional y los procesos de gestión informática de nuestra institución.

8) Que concordante con lo señalado, y de acuerdo a lo dispuesto en el literal e) del artículo 11 de la Ley N° 20.285, se procede a entregar parcialmente la información requerida conforme el principio de divisibilidad, el que prescribe que si un acto administrativo contiene información que puede ser conocida e información que debe denegarse en virtud de causa legal –como ocurre en la especie-, se dará acceso a la primera y no a la segunda.

En ese sentido, y en razón de lo fundado en los considerandos anteriores, se entrega al requirente la siguiente información: 1°) Resumen del Diagnóstico; 2°) Etapa 2- Indicadores; 3°) Etapa 3 y 4- Resumen de Implementación; 4°) Etapa 4- Evaluación; 5°) Etapa 4-Programa Seguimiento; 6°) Etapa 4- Ctrl. y Mejora Continua.

R E S U E L V O:

ARTÍCULO PRIMERO: Deniégase parcialmente la entrega de información requerida por don Carlos Lobos Medina a través de la Solicitud de Acceso a la Información N° AB091W0000093, de 06 de febrero de 2013, por concurrir a su respecto la causal del artículo 21 N° 1 de la Ley N° 20.285.

ARTÍCULO SEGUNDO: Entréguese al solicitante, don Carlos Lobos Medina, copia de los siguientes documentos: 1°) Resolución Exenta N° 1.400, de 02 de agosto de 2012, que Aprueba la Política General de Seguridad de la Información de la Subsecretaría de Prevención del Delito y Anexo; 2°) Resumen del Diagnóstico; 3°) Etapa 2- Indicadores; 4°) Etapa 3 y 4- Resumen de Implementación; 5°) Etapa 4- Evaluación; 6°) Etapa 4-Programa Seguimiento; 7°) Etapa 4- Ctrl. y Mejora Continua.

ARTÍCULO TERCERO: Notifíquese la presente resolución a don Carlos Lobos Medina mediante carta certificada dirigida al domicilio indicado en su presentación.

ARTÍCULO CUARTO: Incorpórese la presente resolución al Índice de actos y documentos calificados como secretos o reservados, una vez que se encuentre a firme, en conformidad a lo dispuesto en la Instrucción General Nº 3, del Consejo para la Transparencia.

ANÓTESE Y NOTIFÍQUESE

MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA
SUBSECRETARIO

JUAN CRISTÓBAL LIRA IBÁÑEZ
SUBSECRETARIO DE PREVENCIÓN DEL DELITO
MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA

Subsecretaría de Prevención del Delito
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

MINISTERIO DEL INTERIOR Y SEGURIDAD PUBLICA
Oficina de Partes
14 AGO 2012
TOTALMENTE TRAMITADO
SUBSECRETARIA DE PREVENCION DEL DELITO

APRUEBA LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA SUBSECRETARÍA DE PREVENCIÓN DEL DELITO Y ANEXO.

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. _____

RESOLUCION EXENTA N° 1400

SANTIAGO, 02 DE AGOSTO DE 2012

HOY SE RESOLVIO LO QUE SIGUE

VISTO: Los antecedentes adjuntos y lo dipuesto en el literal d) del artículo 2° del Decreto Ley N°1028, de 1975, del Ministerio del Interior que "Precisa atribuciones y deberes de los Subsecretarios de Estado"; la Ley N° 20.502 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"; la Resolución Nº 1600, de 30 de octubre de 2008, de Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón.

CONSIDERANDO: 1) Que tal como lo dispone el artículo 12° de la Ley N°20.502 se crea en el Ministerio del Interior y Seguridad Pública una Subsecretaría de Prevención del Delito, que tiene como función ser el órgano de colaboración inmediata del Ministro 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 la tareas que aquél le encargue.

2) Que esta Subsecretaría requiere contar con una Política General de Seguridad de la Información, la cual tenga por objeto 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 lo activos de información de la Institución.

CCF/CTS/CND/CQF/dcw
DISTRIBUCION:
1. Funcionarios y Asesores de la Subsecretaría de Prevención del Delito.
2. Departamento de Auditoría Interna.
3. Partes y Archivo

GABINETE

3) Que dicha política será aplicable a todos los activos de información de la Subsecretaría de Prevención del Delito, considerando sus áreas, departamentos, programas, 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) Que es facultad de este Subsecretario impartir instrucciones internas de acuerdo a lo dipuesto por el literal d) del artículo 2° del Decreto Ley N°1028, de 1975, del Ministerio del Interior que "Precisa atribuciones y deberes de los Subsecretarios de Estado".

R E S U E L V O:

ARTICULO ÚNICO: **APRUÉBASE**, por las razones ya expresadas, la Política General de Seguridad de la Información de la Subsecretaría de Prevención del Delito del Ministerio del Interior y Seguridad Pública, la cual se incluye como anexo a la presente resolución.

ANÓTESE Y NOTIFÍQUESE

MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA
SUBSECRETARIO
SUBSECRETARIA DE PREVENCIÓN DEL DELITO

JUAN CRISTÓBAL LIRA IBÁÑEZ
SUBSECRETARIO DE PREVENCIÓN DEL DELITO
MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA

Subsecretaria de Prevención del Delito
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

MEMORANDUM DAFP Nº 380/2012

A : **CARLOS QUINTANA FRUGONE**
JEFE DIVISIÓN JURÍDICA

DE : **CARLOS NUÑEZ DUQUE**
JEFE DEPARTAMENTO DE PLANIFICACION Y DESARROLLO

REF. : Solicita elaboración de R.E.

FECHA : Santiago, 26 de julio de 2012

Por medio del presente y junto con saludarle, solicito a usted realizar la elaboración de la Resolución Exenta para la formalización de la **Política de Seguridad de la Información**, según documento adjunto.

Sin otro particular, atentamente,

MINISTERIO DEL INTERIOR Y SEGURIDAD PÚBLICA
DEPTO. DE PLANIFICACION Y DESARROLLO
SUBSECRETARÍA DE PREVENCIÓN DEL DELITO

CARLOS NUÑEZ DUQUE
JEFE DEPARTAMENTO DE PLANIFICACION Y DESARROLLO
SUBSECRETARÍA DE PREVENCIÓN DEL DELITO

/ylr
Distribución:
Depto. Planificación y Desarrollo
Archivo DAFP

13256308

Resumen Ejecutivo

Como parte del marco de trabajo en la implementación de un Sistema de Gestión de Seguridad de la Información a través del PMG SSI (*Programa de Mejoramiento de Gestión del Sistema de Seguridad de la Información*), se hace obligatorio comunicar la necesidad de crear y formalizar una política que permita entregar el marco general de seguridad, como también reflejar el compromiso por parte de la alta dirección de la Institución con respecto a su cumplimiento interno y el apoyar los cambios culturales que puedan requerirse durante su implementación.

En relación a lo anteriormente expuesto, es que se ha confeccionado el documento "Política General de Seguridad de la Información" que abarca los ámbitos obligatorios a desarrollar y que además se encuentran alineados con estándares internacionales de mejores prácticas a adoptar, como sería el control de acceso a la información, establecer medidas de protección, seguridad y auditoría en los sistemas de información, resguardar la continuidad de los programas estratégicos de la Subsecretaría, velar por la confidencialidad, integridad y disponibilidad de los datos, entre otras que se detallan en su contenido.

La creación de la presente política fue sesionada a través del Comité de Seguridad de la información, y sería la piedra angular que entregará las directrices generales y visión estratégica sobre la seguridad de la información al interior de la Institución, siendo esta aplicable a todo el personal, independiente de su calidad jurídica y que en caso de aplicar podría extenderse a entidades externas relacionadas, como podrían ser proveedores u otras áreas de gobierno, derivando en una estructura de gestión desarrollada a través de políticas, normativas, estándares y procedimientos que apoyan la implementación de controles que buscan mejorar la calidad y seguridad de la información de la Institución.

El cumplimiento de lo establecido en la política será considerado dentro del programa anual de auditoría interna de la Subsecretaría, siendo además sancionable según lo que establece el estatuto administrativo, pudiendo considerar también el marco legal vigente relacionado.

Ministerio del Interior y Seguridad Pública

Subsecretaría de Prevención del Delito

Subsecretaría de Prevención del Delito
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Política General de Seguridad de la Información

1330816R

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, disponibilidad y legalidad 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 todos los activos de información de la Subsecretaría de Prevención del Delito, 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 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, disponibilidad y legalidad 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.
Legalidad	:	Propiedad de la información que apunta a mantener alineada la información como requisito legal para el cumplimiento de la normativa vigente.
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.
Incidente de seguridad	:	Cualquier evento, acción o situación que comprometa el resguardo de las propiedades de la información y/o contravenga la política de seguridad y sus normativas.

6 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

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, disponibilidad o legalidad 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 a 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 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:

- Propietario de información: Persona responsable de una información en particular, como también de su valorización y clasificación.
- Administrador de información: Persona encargada de resguardar la información y administrar las definiciones establecidas por el Dueño de la información.
- Usuario 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 través de un Comité de Seguridad de la Información y/o el Encargado 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 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 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.

6.7 Seguridad Ligada a las Personas

Debido a la importancia que tienen las personas en la Institución, se considera fundamental el gestionar la seguridad de la información aplicada al ciclo de vida de las personas y mientras presten servicios en la organización, por lo mismo se desarrollarán planes orientados a incorporar la cultura de seguridad en los funcionarios y en su quehacer laboral, además de la implementación de otros mecanismos de apoyo a este ámbito, permitiendo entregar un apoyo permanente a la gestión del cambio frente a temas de seguridad de la información en las personas.

6.8 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, u otras condiciones que puedan afectar su confidencialidad, integridad y/o disponibilidad.

6.9 Seguridad en las Comunicaciones y 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 comunicaciones y operaciones relacionados a 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, como también en el manejo de los soportes y la seguridad de la redes tecnológicas, permiten entregar un grado razonable en el resguardo de los activos de información y un cumplimiento adecuado de la política Institucional de seguridad.

La gestión de los servicios entregados por terceros, sobre la cual es requisito obligatorio la supervisión y revisión de los acuerdos de niveles de servicio establecidos, tanto en el ámbito de la calidad como en la seguridad en que son prestados, además de la gestión de cambios entre las partes y sobre todo en los acuerdos de confidencialidad y el intercambio de información con entidades externas a la Subsecretaría de Prevención del Delito, como también áreas internas de la institución, velando en todo momento por preservar la protección y el resguardo de la información.

6.10 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 accesos o manipulación no autorizada.

6.11 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.

6.12 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 situaciones 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 su ocurrencia y para apoyar la mejora continua del sistema de seguridad.

6.13 Gestión de la Continuidad de Negocio

Los productos estratégicos, tales como el programa de servicio de orientación e información, el programa de atención a víctimas del delito o el programa denuncia seguro, entre otros, 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 de la Institución, los que a través de la gestión de riesgos, el análisis de impacto, el desarrollo de estrategias y los planes de prueba y mejora principalmente, permiten garantizar razonablemente la operación de los productos estratégicos de la Institución.

6.14 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, 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 que monitorean y supervisan periódicamente el cumplimiento de estas.

7 ROLES Y RESPONSABILIDADES

7.1 Subsecretario 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 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 aplicabilidad bajo el marco de la política, supervisar la implementación de normativas, identificar y evaluar acciones correctivas, aprobar metodologías de gestión de riesgos y seguridad, identificar cambios significativos que pudieran generar riesgos, proponer soluciones de controles de seguridad, establecer medios para concientizar y capacitar al personal, arbitrar conflictos relacionados a la seguridad, evaluar la información recibida del monitoreo y de los incidentes de seguridad y 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 de Seguridad de la Información

Responsable de coordinar actividades de gestión de seguridad, en donde sus funciones claves son de alinear la debida respuesta y priorización al tratamiento de incidentes y riesgos vinculados a los activos de información de los procesos institucionales, 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 Auditoría Interna

Responsable del monitoreo y seguimiento la implantación del SGSI, reportando de manera periódica al S.S.P.D., declarando que el equipo de Auditoría Interna se encuentra facultado y autorizado para evaluar de manera anual o cuando estime conveniente el cumplimiento de la Política de Seguridad de la Información, como también de todas aquellas normativas y controles que de ella se desprendan.

7.5 Funcionarios 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, disponibilidad o legalidad 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.2009 y NCh ISO/IEC 27002 Of.2009, 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 deberá establecer una metodología para la gestión de riesgos de la información y su tratamiento de control, la cual se encontrará documentada y aprobada por el Comité de Seguridad de la Información, que también a su vez deberá ser 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 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 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 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 una adecuado lineamiento con la misión y objetivos de la Institución.

11 CONTROL DOCUMENTAL

11.1 Control de Aprobación

Nombre	Cargo	Actividad	Fecha	Firma
Ariel Severino Fuentes	Coordinador Unidad de Proyectos, Tecnología e Innovación	Creación del documento	18/07/12	
Carlos Núñez Duque	Jefe Departamento Planificación y Desarrollo	Revisión del documento	18/07/12	
Claudio Toledo Sepúlveda	Jefe División Administración, Finanzas y Personas	Revisión del documento	18/07/12	
Carlos Quintana Frugone	Jefe División Jurídica	Revisión del documento	19/07/12	
Carlos Charme Fuentes	Jefe Gabinete Subsecretario	Revisión del documento	19/07/12	
Cristóbal Lira Ibáñez	Subsecretario de Prevención del Delito	Aprobación del documento	26/07/2	

11.2 Control de Cambios

Versión	Cambio	Responsable
1.0	Aprobación y difusión del documento.	Cristobal Lira

11.3 Publicación y Difusión

• Jefes de División • Jefes de Departamento • Archivo DAFP • Archivo Gabinete

12 ANEXOS

No aplica.

<< FIN DEL DOCUMENTO >>

Nombre de la Institución:	SUBSECRETARIA DE PREVENCION DEL DELITO	
	Requisitos Técnicos	Fecha
Revisiones regulares del SSI	Revisión 1	
	Revisión 2	
	Revisión n	
Indicadores y metas	Revisión de indicadores y metas	
	Establecimiento de medidas de mejora	
	Aprobación CSI o Dirección	
Inventario de activos y riesgos	Actualización del inventario de activos	
	Incorporación a gestión de riesgos institucional	

Nombre de la Institución: SUBSECRETARIA DE PREVENCION DEL DELITO

Requisitos Técnicos		Medios de verificación (adjuntar)
Evaluación de los resultados del Plan General	Revisión del % de cumplimiento logrado, por parte del CSI	
	Revisión de los resultados de las actividades desarrolladas y la efectividad en la mitigación de riesgos	
	Identificación de riesgos persistentes y otras debilidades, y su análisis de causa	
	Recomendaciones de mejora, que consideren medidas correctivas y preventivas	
Difusión de los resultados de la implementación		

Nombre de la Institución: **SUBSECRETARIA DE PREVENCION DEL DELITO**

Nombre del indicador	Fórmula de cálculo	Fecha de inicio de la medición	Frecuencia de la medición	Efectiva a Agosto de 2012	Efectiva a Octubre de 2012	Efectiva a Diciembre de 2012	Meta	Medios de verificación	Supuestos	Notas
Responsabilidad sobre la SI en la organización.	(N° de contratos elaborados que contienen clausulas de seguridad de la información I/total de contratos elaborados)*100	30/09/2013	Trimestral	0%	0%	0%	70%	Contratos que contengan clausulas de SI		La elaboración de contratos abarca tanto contratos de personal en calidad de planta, contrata y honorarios de la subsecretaria de Prevención del Delito.
Existencia de control de accesos a usuarios	(N° de sistemas de información de la SPD/N°Total de estandares de perfiles)*100	30/09/2013	Trimestral	0%	0%	0%	80%	Informe de perfiles de accesos establecidos. Informe de dotación actualizado.		Por estandar de perfil se entiende una matriz que detalla los derechos de acceso del usuario sobre el sistema.
Porcentaje de procesos de cambio que se han realizado conforme a la normativa existente al respecto, en relación al total de cambios solicitados	(N°de de procesos de cambio que se han realizado conforme a la normativa existente/total de cambios solicitados)*100	30/09/2013	Trimestral	0%	0%	0%	70%	Informe deprocesos de cambio que se han realizado conforme a la normativa existente		
Porcentaje de incidentes de seguridad que reciben tratamiento de acuerdo al plan de continuidad de negocio establecido en el sistema de Seguridad de la información en año t	(N° incidentes de seguridad que reciben tratamiento de acuerdo al plan de continuidad de negocio establecido en el sistema de Seguridad de la información en año t/N° total de incidentes)*100	30/09/2013	Trimestral	0%	0%	0%	70%	Informe de gestión de incidentes de seguridad de la información		
Porcentaje de riesgos de seguridad de la información a los que se les ha aplicado los controles de seguridad en forma completa y satisfactoria.	(N°de riesgos de seguridad de la información a los que se les ha aplicado los controles de seguridad en forma completa y satisfactoria/ N° Total de riesgos de seguridad de la información)*100	30/09/2013	Trimestral	0%	0%	0%	50%	Informe de gestión en el tratamiento de riesgos de información		

(1) Adaptado de: "INSTRUCCIONES PARA LA FORMULACIÓN PRESUPUESTARIA. FORMULARIO H. INDICADORES DE DESEMPEÑO AÑO 2011". Disponible en http://www.dipres.gob.cl/572/articles-36282_doc_pdf3.pdf (30 de Marzo de 2012)

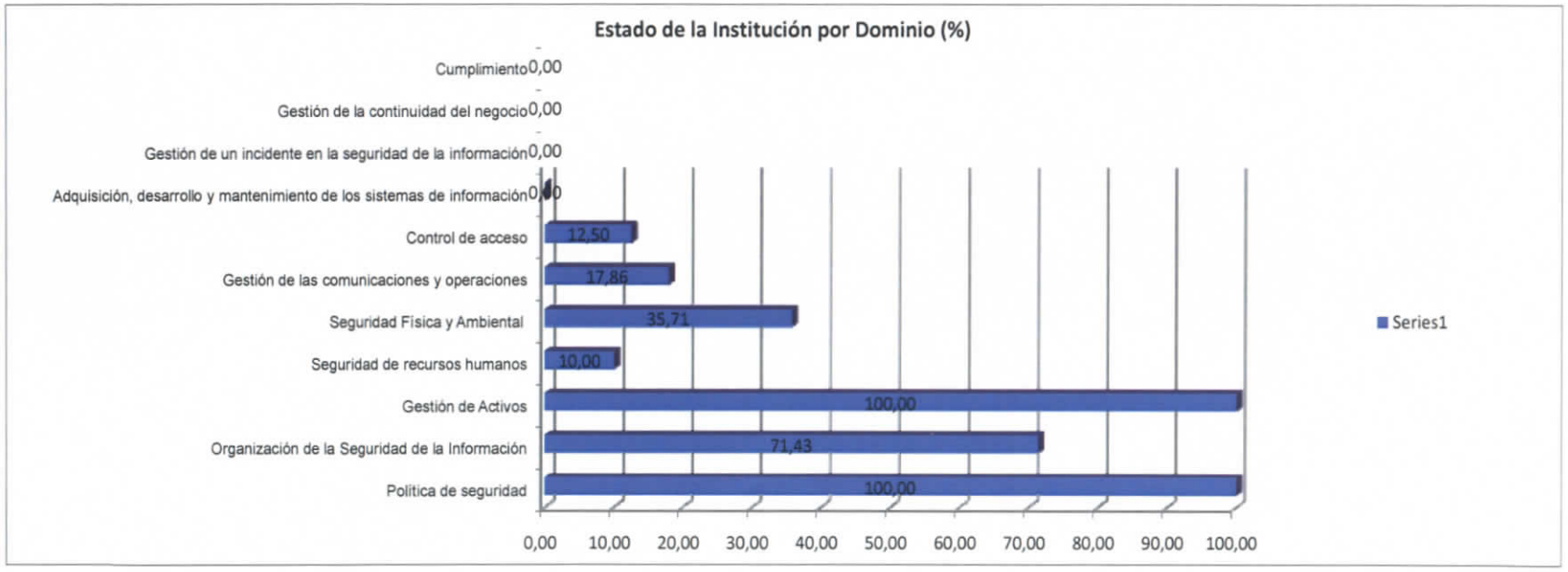
(2) "Indicadores de gestión en los servicios públicos. Serie Guía Metodológica. Santiago de Chile, junio de 1996". Dirección de Presupuestos, citado en "SISTEMA INTEGRAL DE INFORMACIÓN Y ATENCIÓN CIUDADANA, SIAC. GUÍA METODOLÓGICA 2010". Disponible en: http://siac.msgg.gob.cl/uploads/f15be81f87_guia_final[1].pdf (30 de Marzo de 2012)

Nombre de la Institución: SUBSECRETARIA DE PREVENCION DEL DELITO

Requisitos Técnicos			
Recomendaciones y medidas de mejoramiento	Compromisos	Plazo	Responsable

PMG/MEI -SSI: RESUMEN - DIAGNOSTICO

DOMINIO	% CUMPLIMIENTO	COBERTURA
Política de seguridad	100,00	83,33
Organización de la Seguridad de la Información	71,43	58,33
Gestión de Activos	100,00	11,11
Seguridad de recursos humanos	10,00	83,33
Seguridad Física y Ambiental	35,71	70,00
Gestión de las comunicaciones y operaciones	17,86	65,12
Control de acceso	12,50	57,14
Adquisición, desarrollo y mantenimiento de los sistemas de información	0,00	42,11
Gestión de un incidente en la seguridad de la información	0,00	100,00
Gestión de la continuidad del negocio	0,00	50,00
Cumplimiento	0,00	40,00
ESTADO DE LA INSTITUCION (DIAGNOSTICO)	**31,59**	



PMG/MEI - SSI: RESUMEN - IMPLEMENTACIÓN

DOMINIO	% CUMPLIMIENTO	COBERTURA
Política de seguridad	100,00	83,33
Organización de la Seguridad de la Información	71,43	58,33
Gestión de Activos	100,00	11,11
Seguridad de recursos humanos	10,00	83,33
Seguridad Física y Ambiental	35,71	70,00
Gestión de las comunicaciones y operaciones	19,23	65,12
Control de acceso	12,50	57,14
Adquisición, desarrollo y mantenimiento de los sistemas de información	0,00	42,11
Gestión de un incidente en la seguridad de la información	0,00	100,00
Gestión de la continuidad del negocio	0,00	50,00
Cumplimiento	0,00	40,00
ESTADO DE LA INSTITUCION (IMPLEMENTACION)	**31,72**