Gobierno de Chile

Política de Seguridad de la Información

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.

Objetivo y Alcance de la Política de Seguridad

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.

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 2015 al 2018, 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.

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.

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.

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.

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 propietario de la información.

- Usuario de información: Persona que solicita acceso para realizar tratamiento sobre la información resguardada por el Administrador de información.

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 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.

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.

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 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.

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.

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.

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.

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.

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.

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.

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 podrán monitorean y supervisan periódicamente su cumplimiento.