1. OBJETIVO

Evitar incumplimientos a las obligaciones legales, estatutarias, normativas o contractuales relacionadas con la Seguridad de la Información y con cualquier requisito de seguridad.
Garantizar que la Seguridad de la Información se implementa y se opera de acuerdo a las políticas y procedimientos vigentes en el IND.

2. ALCANCE

Esta política aplica para todo el personal que trabaje en o para el IND, ya sean funcionarios de planta, a contrata, a honorarios, regidos por el Código del Trabajo, asesores, consultores, practicantes, y otros trabajadores, incluyendo las empresas que presten servicios para el IND. Lo anterior con el fin de garantizar la continuidad operacional y de la Seguridad de la Información de cada una de las etapas de los procesos de provisión vigentes en el IND, de acuerdo a lo establecido en el Formulario de definiciones Estratégicas (A1).

3. MATERIAS ESPECÍFICAS QUE ABORDA

- A.18.01.01 Identificación de la legislación vigente y los requisitos contractuales
- A.18.01.02 Derechos de propiedad intelectual
- A.18.01.03 Protección de los registros
- A.18.01.04 Privacidad y protección de la información de identificación personal
- A.18.02.01 Revisión independiente de la seguridad de la información
- A.18.02.03 Verificación del cumplimiento técnico

4. ROLES Y RESPONSABILIDADES

- Comité de Seguridad de la Información
  - Supervisar la implementación y difusión de las recomendaciones y normas establecidas en la presente política.
- Encargado/a de Seguridad de la Información
  - Mantenerse informado respecto de la legislación y normativas vigentes en temas relacionados con la Seguridad de la Información.
  - Monitorear el avance general de las medidas de control que se desprenden de la presente política.
- Jefatura Departamento Jurídico
  - Apoyar al Sistema de Seguridad de la Información en la actualización de la normativa aplicable al IND en materias de Seguridad de la Información.

- Jefatura Unidad Coordinación Informática
  - Mantener y custodiar pruebas y evidencias de la propiedad de las licencias, discos maestros, manuales, etc.
  - Controlar y revisar periódicamente los equipos para verificar que solo se instale software y productos debidamente licenciados.

5. REVISIÓN Y EVALUACIÓN

La presente Política debe ser objeto de revisión y de evaluación en relación con su correcta aplicación cuando se cumplan dos años de su aprobación, o bien, en forma extraordinaria, cada vez que se presente un evento que propicie un ajuste de las declaraciones establecidas. En ambos casos, estas revisiones y evaluaciones serán realizadas en las sesiones del Comité de Seguridad de la Información.

6. DIFUSIÓN

La presente Política debe ser difundida por medio de su publicación en la sección "Seguridad de la Información" de la intranet institucional.

7. DEFINICIONES

- **Datos personales:** se entiende como tal a la información que incluye datos que pueden utilizarse para identificar a una persona, tal como nombre completo, dirección, número de cedula de identidad, número telefónico y correo electrónico, entre otros.
- **Sistemas críticos:** Sistemas de información que dan soporte a los productos estratégicos.
- **Seguridad de la información:** todas aquellas medidas preventivas y reactivas que permitan resguardar y proteger los activos de información, buscando mantener la confidencialidad, integridad y disponibilidad de los mismos.
- **Ciberseguridad:** conjunto de herramientas, políticas, métodos de gestión, prácticas, y tecnologías que pueden utilizarse para proteger los activos de información de la organización y sus usuarios en el entorno digital, buscando garantizar la disponibilidad, integridad y confidencialidad de la información.
- **Comité de Seguridad de la Información (CSI):** es un cuerpo integrado por representar de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

8. POLITICA

8.1 identificación de los requisitos de legislación y contractuales correspondientes.

La normativa vigente relacionada con el Sistema de Seguridad de la Información deber ser identificada y debidamente difundida dentro del IND, incluyendo lo siguiente:

- Marco normativo aplicable al IND
- Modernización del Estado
- Gobierno Electrónico
- Transparencia y Acceso a la Información Publica
- Estatuto Administrativo
- Propiedad Intelectual

8.2 Derechos de propiedad intelectual

En el correcto cumplimiento de la Ley 17.336 de Propiedad Intelectual y Derechos de Autor, el IND provee los recursos necesarios para el uso de software licenciado, los cuales deben ser adquiridos por proveedores autorizados y confiables, dejando estrictamente prohibido el uso de software que no esté debidamente licenciado. El uso ilegal de software es considerado falta grave, por lo que pueden ser aplicadas las medidas disciplinarias correspondientes a quien se detecte incurriendo en esa falta.

No está permitido duplicar, convertir a otro formato ni descargar grabaciones comerciales (películas, discos, documentales, cortometrajes, etc.); copiar libros, artículos, informes u otros documentos en su totalidad o en parte, que no sean los permitidos por la ley de derecho de autor.

Para mayor detalle, consultar las políticas específicas sobre el "Uso legal de Software" y el "Uso de Internet", disponibles en la intranet institucional, sección "Seguridad de la Información" (SSI).

8.3 Protección de registros

Los registros críticos de los procesos de provisión del IND se deben proteger contra pérdidas, destrucción, falsificación, acceso no autorizado y publicación no autorizada de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales, considerando lo siguiente:

- Definir los registros críticos para la institución y clasificarlos de acuerdo al tipo de registro (de base de datos, de transacciones, de auditoría y operacionales) y a su criticidad en cuanto a confidencialidad, integridad y disponibilidad.
- Tomar las precauciones necesarias para que, en el caso de medios de almacenamiento electrónico, se pueda acceder a los datos por todo el periodo de

retención para protegerlos contra la pérdida debido a cambios en la futura tecnología.

- Seleccionar sistemas de almacenamiento adecuados para que se puedan recuperar los datos en un periodo de tiempo y formato aceptable.
- Dependiendo de las características del medio de almacenamiento, se deben manipular de acuerdo a las indicaciones del fabricante, teniendo en consideración la posibilidad del deterioro de los medios que se utilizan para el almacenamiento de registros.

8.4 Privacidad y protección de información personal identificable

La responsabilidad de manejar información personal identificable y de garantizar el conocimiento de los principios de privacidad se debe abordar de acuerdo con la legislación y las normativas pertinentes. Se deben implementar las medidas técnicas y organizacionales adecuadas para proteger la información personal identificable.

La protección de datos personales se encuentra regulada en diversos instrumentos jurídicos, clasificables en normas generales y sectoriales. La Ley 19.628: “Sobre protección de la vida privada y protección de Datos de Carácter Personal” y la Ley 20.185: “Ley de Transparencia y Acceso a la Información Pública” establecen los procedimientos para el ejercicio del derecho, amparo y la protección de los datos personales.

El IND se compromete a asegurar la privacidad y la protección de la información personal identificable de acuerdo a la legislación y las normativas vigentes y a informar a sus funcionarios sobre cuál es el proceder de la institución en lo que respecta a la obtención, almacenamiento, uso, protección y divulgación de información de carácter personal.

8.4.1 Obtención

La información personal se puede obtener de diversas formas, por ejemplo de manera directa a través del mismo funcionario, proveedor o colaborador; así como otras fuentes permitidas por la ley, como guías telefónicas, bolsas de empleo u otras similares.

8.4.2 Almacenamiento

La información personal debe ser almacenada de manera de proteger su confidencialidad, integridad y disponibilidad, utilizando los mecanismos y herramientas adecuadas según sea el formato en el que se encuentra.

8.4.3 Uso

El IND utiliza la información personal para dar cumplimiento a obligaciones contraídas por convenios, para permitir, adaptar y/o modificar servicios o programas administrados y para el envío de información que pudiera resultar de interés para funcionarios, proveedores y/o colaboradores.

8.4.4 Divulgación

El IND no vende, comparte o divulga los datos personales o información de los funcionarios, proveedores y/o colaboradores, excepto en los casos en que una ley, reglamentación o autoridad judicial así lo requiera o cuando los derechos o propiedad de la institución se vean amenazados.

8.4.5 Protección

El IND utiliza tecnología para proteger la información personal la información personal que se proporciona, mediante políticas de control de acceso y uso de software seguros. El manejo del uso y archivo de expedientes electrónicos y físicos se realiza a través de personal autorizado y capacitado que desarrolla sus funciones dentro de la institución y tiene pleno conocimiento de la presente política.

8.5 Revisión independiente de la seguridad de la información

Se debe revisar, de manera independiente al área de revisión, el enfoque del IND para la gestión de la seguridad de la información y su implementación. Dicha revisión se debe realizar una vez al año o cuando ocurran cambios significativos en la institución.

La revisión al Sistema de Gestión de Seguridad de la Información debe considerar lo siguiente:

- Evaluación del cumplimiento de la normativa de seguridad vigente en el IND.
- Evaluación de oportunidades de mejora y la necesidad de cambios en el enfoque de seguridad.

Los resultados de la revisión independiente se deben registrar en un informe el cual debe ser entregado al Comité de Seguridad de la Información durante los primeros 15 días de diciembre de cada año.

8.6 Verificación del cumplimiento técnico

Los sistemas definidos como críticos se deben revisar anualmente para verificar su cumplimiento con las políticas y normas de seguridad de la información y de ciberseguridad del IND, utilizando herramientas automatizadas que generen informes técnicos para su posterior análisis.

Si se utilizan pruebas de penetración o evaluaciones de vulnerabilidad, se debe tener precaución, pues tales actividades podrían comprometer la seguridad del sistema. Esas pruebas se deben planificar, comunicar y documentar.

Cualquier tipo de revisión de cumplimiento técnico debe ser realizada únicamente por personas autorizadas competentes o personas que estén bajo la supervisión de dichas personas autorizadas.

Aprobaciones

	Nombre	Cargo	Firma
Responsable de Elaboración	Cristian Villalobos Zamora	Encargado PMG Seguridad de la Información	
Responsable de Revisión y Aprobación	Carola Molina Cecchi	Encargada de Seguridad de la Información	

Control de Cambios

Versión	Fecha	Responsable	Descripción
Versión 1	22-06-2017	Cristian Villalobos Z.	Se elabora esta primera versión del presente documento para dar cumplimento al PMG-SSI 2017 y abordar requerimientos internos del IND.
Versión 2	02-07-2018	Cristian Villalobos Z.	Se modifica la difusión de la política y las responsabilidades.
Versión 3	16-05-2019	Cristian Villalobos Z.	Se incorporan los controles A.18.02.01 y A.18.02.03.