Subsecretaría de Agricultura

POLÍTICA DE CUMPLIMIENTO LEGAL

Código:	TI-SSI-17
Versión:	6.0
Fecha de la versión:	20-12-2017
Creado por:	Daniel Coronado Rojo
Aprobado por:	Jorge Vega Saavedra
Nivel de confidencialidad:	Uso Interno

Historial de Versiones

Fecha	Versión	Creado por	Descripción de la versión
20/08/2013	1.0	Cristobal Nef	Se crea política de cumplimiento legal, para entregar los lineamientos oficiales sobre seguridad de la información.
18/12/2013	2.0	Cristobal Nef	Se Agrega descripción sobre protección de los registros.
04/12/2015	3.0	Daniel Coronado	Se actualiza controles de referencia a la nueva versión 2013 de la ISO 27001. Se modificó los puntos referentes al derecho de propiedad intelectual y al de auditorías de sistemas.
05/10/2016	4.0	Daniel Coronado	Se revisaron y modificaron algunos puntos para cumplir con lo requerido en los controles A.18.1.5 y A.18.2.2
15/12/2016	4.1	Daniel Coronado	Se agregan los apartados de "definiciones", "responsabilidades" y "difusión".
12/06/2017	5.0	Daniel Coronado	Se actualizan los datos referentes a la legislación vigente y los requisitos contractuales. Se agrega el campo de "Ámbito de ejecución, y Alcance". Debido a que es a fin a esta política, se incorpora el control A.18.1.3. Se actualizan los datos referentes a la legislación vigente y los requisitos contractuales. Se agregan los campos de "Alcance y usuarios" (pág. 4), "control legal y normativo" (pág. 6), y "Documentos internos de referencia" (pág. 4).
20/12/2017	6.0	Daniel Coronado	Se agrega control A.18.1.4 (pág. 4 y 8)

Nota de enfoque de género

El uso de un lenguaje que no discrimine ni marque diferencias entre hombres y mujeres ha sido una preocupación en la elaboración de este documento. Sin embargo, y con el fin de evitar la sobrecarga gráfica que supondría el utilizar en español o/a para marcar la existencia de ambos sexos, se ha optado por utilizar el masculino genérico, en el entendido de que todas las menciones en tal género representen siempre a todos/as.

Nota de confidencialidad

Tabla de contenido

Clasificación del Documento

Nivel de Confidencialidad: Uso Interno.
Nota de Confidencialidad: Documento disponible sólo a funcionarios de la Subsecretaría de Agricultura y personal externo autorizado.

1. Objetivo

El objetivo del presente documento es la identificación de los requisitos legales, normativos, contractuales y de otra índole relacionados con la seguridad de la información dentro de la Subsecretaría de Agricultura, como también definir las responsabilidades para su cumplimiento.

2. Ámbito de ejecución, y alcance

La política "TI-SSI-17 Política de cumplimiento legal", se aplica a todos quienes cumplen funciones en la Subsecretaría, ya sea en sus instalaciones o fuera de ellas, tanto a funcionarios, así como también, a personas naturales y jurídicas externas, públicas o privadas que presten servicios en la Subsecretaría o para este y que tengan participación en las actividades descritas en este documento.

El ámbito de ejecución de esta política, son todos los activos de información de la Subsecretaría y aquellos bajo su responsabilidad que estén contemplados en el documento. Su cobertura se extiende a la información impresa y también a aquella almacenada electrónicamente, y transmitida por cualquier soporte o medio. Se debe precisar que el presente alcance aplica para los siguientes procesos de provisión de productos estratégicos de la Subsecretaría de Agricultura: Informe de Factibilidad para la Construcción, Red Agroclimática Nacional y Transferencias.

Los dominios abordados de la norma NCH ISO 27001:2013 en este documento, son los siguiente:

- A.12 Seguridad en la Operativa, y
- A.18 Cumplimiento.

3. Documentos de referencia

- TI-SSI-01 Política General de Seguridad de la información.
- Norma NCH ISO/IEC 27002:2013.

4. Definiciones

A continuación, una definición de los términos claves utilizados en este documento:

TI: Tecnologías de la información.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Contraseñas: Una *contraseña* o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso.

Licencia de Software: Es un contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario (usuario consumidor/usuario profesional o empresa) del programa informático, para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas.

Software Open Source: El software "open source" o libre, son aquellos que no disponen de licencia pagada y permite que el usuario, pueda usar e incluso intervenir libremente en el código fuente.

Auditoria Informática: Es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo institucional, mantiene la integridad de los datos ya que esta lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, cumple con las leyes y regulaciones establecidas.

Política de seguridad: Conjunto de norma o buenas prácticas, declaradas y aplicadas por una organización, cuyo objetivo es disminuir el riesgo en la realización de actividades o procesos de interés en la organización.

5. Roles y Responsabilidades

Para cumplir con los objetivos de la presente política, se establecen los siguientes roles y responsabilidades:

Encargado de Seguridad de la Información: Funcionario a cargo del desarrollo e implementación de la Política del Sistema de Seguridad para el Servicio, así como también, de velar por la correcta aplicación tanto de esta política, como a su vez, de los instrumentos de apoyo utilizado para ello (Políticas y Procedimientos).

Comité de Seguridad de la Información: Es responsable por la existencia y cumplimiento de las medidas de seguridad de la información acorde con las necesidades de la Subsecretaría, los recursos disponibles y la normativa vigente.

Jefe departamento TI: Responsable de definir los dominios de seguridad, implementar medidas de control para las excepciones de acceso directo desde dominios externos hacia servicios de producción entre otros accesos perimetrales de la red, gestionar y controlar el sistema de gestión de seguridad sobre la protección de los activos de información del servicio, conforme a la normativa vigente y los objetivos estratégicos institucionales.

Unidad de Auditoría Interna: Responsable de revisar y comprobar el cumplimiento de cada una de las medidas establecidas en los documentos que conforman el sistema de seguridad de la información.

Funcionario de la Subsecretaría de Agricultura: Responsable de cumplir con lo establecido en este documento y aplicarlo en su entorno laboral. Tiene la obligación de alertar de manera oportuna y adecuada, a través de canales y procedimientos formalmente establecidos, cualquier situación que pueda poner en riesgo la seguridad de la información.

6. Definición respecto a las materias específicas abordadas

Los controles de los dominios abordados de la norma NCH ISO 27001:2013 en este documento, son los siguientes:

N° Control	Nombre control NCH ISO 27001:2013	Descripción del control
A.12.7.1	Controles de auditoría de sistemas de información	Los requisitos y las actividades de auditoria que involucran sistemas críticos de la subsecretaría, deben planificarse y acordar para minimizar el riesgo de interrupciones en los procesos.
A.18.1.1	Identificación de la legislación vigente y los requisitos contractuales	Los estatutarios, regulatorios y contractuales pertinentes, deben estar referenciados en cada política y procedimiento, pertenecientes al SGSI.
A.18.1.2	Derechos de propiedad intelectual	Los softwares utilizados cumplen con los requerimientos legislativos, regulatorios y contractuales relacionados a los

		derechos de propiedad intelectual.
A.18.1.3	Protección de los registros:	Los registros se deberían proteger contra pérdidas, destrucción, falsificación, acceso no autorizados y publicación no autorizada de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.
A.18.1.4	Privacidad y protección de la información de identificación personal:	Se debe asegurar la privacidad y protección de la información de identificación personal, como se exige en la legislación y regulaciones pertinentes, donde corresponda.
A.18.1.5	Regulación de los controles criptográficos	Se deben utilizar controles criptográficos que cumplen con todos los acuerdos, leyes y regulaciones.
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para

		seguridad de la información) se debe revisar de manera independiente a intervalos planificados, o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Las jefaturas deben revisar con regularidad el cumplimiento del procesamiento de la información y los procedimientos de seguridad que están dentro de su área u departamento.
A.18.2.3	Verificación del cumplimiento técnico	Se deben verificar regularmente los sistemas de información críticos, para velar el cumplimiento de las políticas de seguridad, normas y requisitos de seguridad pertinentes.

A continuación, el desglose de las directrices referente a esta política:

6.1. Conformidad con los requisitos legales.

6.1.1. Identificación de la legislación vigente y los requisitos contractuales (control de referencia A.18.1.1).

El cuadro siguiente detalla todas las obligaciones estatutarias, legales y contractuales de la organización en relación con la seguridad de la información que norman y definen la Política de Seguridad de la Información establecida en el presente documento.

- D.S. N°14/2014. MODIFICA DECRETO Nº 181, DE 2002, QUE APRUEBA REGLAMENTO DE LA LEY 19.799 SOBRE DOCUMENTOS ELECTRÓNICOS, FIRMA ELECTRÓNICA Y LA CERTIFICACIÓN DE DICHA FIRMA, Y DEROGA LOS DECRETOS QUE INDICA,
- D.S. N°83/2004. Norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos,
- D.S. N°93/2006. Norma técnica busca minimizar reducción de correos electrónicos masivos en el estado y sus funcionarios,
- D.S. N°1/2015. APRUEBA NORMA TÉCNICA SOBRE SISTEMAS Y SITIOS WEB DE LOS ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO,
- Ley N°17.336/2004. Ley sobre propiedad intelectual,
- Ley N°19.223/1993. Ley sobre figuras penales relativas a la informática,
- Ley N°19.628/1999. Ley sobre protección de la vida privada,
- Ley N°19.799/2002. Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma,
- Ley N°19.927/2004. Ley modifica códigos penales en materia de delitos sobre pornografía infantil,
- Ley N°19.880/2003. Ley sobre procedimientos administrativos que rigen los actos de los órganos del Estado,
- Ley N°20.285/2008. Ley sobre acceso a la información pública,
- Ley N° 19.496. Ley de Protección del Consumidor, N° 19.496, Artículo 28B,
- D.F.L. N°5200/1929. Ley sobre la creación de la dirección de Bibliotecas Archivos y Museos,
- PNCS. Política Nacional de Ciberseguridad,
- UMyGD. Otras normas Unidad de Modernización y Gobierno Digital y
- Internet Segura – MINEDUC. Internet Segura.

6.1.2. Derechos de propiedad intelectual (control de referencia A.18.1.2).

La Subsecretaria de Agricultura trabaja alineadamente con la Ley N°17.336, sobre Propiedad Intelectual, por lo que todos sus funcionarios (Planta, Contrata u Honorarios) siempre deben respetar los siguientes apartados:

- En caso de elaborar reportes, informes, presentaciones o memos, en donde se utilicen textos u citas de forma completa o parcial, que estén presente en libros, reportes u otros documentos con derecho de propiedad intelectual, se debe mencionar la fuente de estos escritos, para no cometer plagio u apropiación ilícita,
- Los Softwares que se utilicen en el servicio, deben de estar al día con su respectiva licencia o el acuerdo reglamentario que se tenga establecido. Si el funcionario desea hacer uso de algún tipo de software que no se encuentre instalado y licenciado por parte del equipo TI., puede hacer la solicitud de compra a través de su jefatura directa, sin embargo, esto no autoriza al uso de licencias ilegales y
- En relación a lo anterior, no se puede usar los activos TI para descargar música, libros u películas, sobre todo aquellos que no hayan sido adquiridos legalmente.

6.1.3. Softwares Utilizados

La Subsecretaria de Agricultura debe trabajar con software y plataformas de empresas reconocidas a nivel mundial y nacional, además, de contar con el debido soporte en actualizaciones o escalamiento de fallas con dichos softwares.

Se debe mantener un registro de los softwares licenciados que se utilizan en la Subsecretaría de Agricultura.

Los softwares "Open Source" que sean ocupados, deben contar con el debido respaldo internacional, además, de disponer actualizaciones constantes, para solventar posibles fallas o bugs que pudieran presentar.

Se debe mantener una lista del software "Open Source" que se utilice en la Subsecretaría.

6.1.4. Uso de Softwares de carácter no convencional

Los softwares, plataformas y/o programas utilitarios que permiten ejecutar acciones no convencionales y que requiere de un nivel técnico experto en su utilización, deberá ser usados solo por las áreas técnicas de la Subsecretaría, y los propósitos para su uso deben ser conocidos y estar autorizados por el Jefe del Departamento de TI.

6.1.5. Protección de los registros (control de referencia A.18.1.3).

Los registros, bases de datos y repositorios importantes, se deben proteger contra pérdida, destrucción y falsificaciones, además de prevenir los accesos que no sean autorizados.

La protección de los registros debe ser de acuerdo con los requisitos estatuarios, regulatorios y contractuales.

6.1.6. Protección y privacidad de la información personal (control de referencia A.18.1.4)

Se debe asegurar la protección y privacidad de los datos personales, de acuerdo a la legislación, cláusulas contractuales, y regulaciones pertinentes.

6.1.7. Uso de los Medios de Procesamiento de Información.

Los medios de procesamiento de información (PC, celulares, etc.) pertenecen a la institución, sin embargo, los responsables de velar por el correcto uso de estos son los propios funcionarios.

Será considerado un acto incorrecto de un medio de procesamiento de información:

- Instalar Software ilegal (sin licencia) aun cuando este sea para usos laborales,
- Utilizar el PC para descargas que no sean para usos laborales (Música, Videos, Películas, etc.),
- Descargar Material Pornográfico de cualquier índole,
- Espiar la red interna con fines personales,
- Utilizar el dispositivo celular para realizar llamadas personales y

- Utilizar aplicaciones para desbloquear todos los accesos de administrador del Smartphone ("Root").

6.1.8. Regulación de los controles criptográficos (control de referencia A.18.1.5)

Cada funcionario de la Subsecretaría de Agricultura tiene el derecho de escoger sus contraseñas en los diversos sistemas que utilice para su trabajo, sin embargo, el Sistema de Seguridad de la Información de la institución, le sugiere el uso de contraseñas robustas para cuidar la confidencialidad, disponibilidad e integridad.

La elaboración de contraseñas robustas, y su constante actualización por parte de los funcionarios, permitirá mitigar el riesgo de sufrir pérdidas o modificaciones no autorizadas a los activos de información que manejan.

El Departamento TI, que juega un rol clave en la administración de los sistemas y medios de procesamiento de información, posee un estricto control criptográfico que incluye la creación de claves robustas (letras mayúsculas, letras minúsculas, números y caracteres especiales) y una actualización constante dependiendo del medio.

6.2. Revisiones de la política de seguridad y de la conformidad técnica.

6.2.1. Cumplimiento con las políticas y normas de seguridad (control de referencia A.18.2.2).

Todos los Jefes o personas que tengan a cargo personal, deben velar por respetar la Política de Seguridad de la Información, y porque se lleven a cabo las buenas practicas que involucra todo el sistema.

Cualquier incidente o mala práctica detectada por la Jefatura, debe ser informado al encargado de Seguridad para poder hacer el análisis de mejora e incluirlo en una futura auditoria del Sistema.

6.2.2. Verificación del cumplimiento técnico (control de referencia A.18.2.3).

El Departamento TI debe realizar constante monitoreo de sus sistemas y medios de procesamiento de información, de las redes internas y de los enlaces de datos, con objetivo de detectar posibles fallas y evitar incidentes.

6.3. Revisiones al sistema de seguridad de la información (control de referencia A.12.7.1 y A.18.2.1).

6.3.1. Auditorias

El Sistema de Seguridad de la Información de la Subsecretaria de Agricultura, está en base a la Norma NCH ISO 27001 ver 2013, norma de gestión basada en procesos, por lo que su aplicación (es decir, los objetivos de control, los controles, las políticas, los manuales, los procesos y procedimientos) debe ser revisada. Para esto que se debe incluir la realización de auditorías por parte de la Unidad de Auditoria (o por un ente auditor externo), para lograr completar el ciclo de gestión del Sistema.

El Encargado de seguridad debe planificar las auditorías que se deberá realizar en el año, haciendo el enfoque que estas no pueden ser realizadas por las mismas personas que realizan las actividades auditadas.

6.3.2. Protección de las herramientas de auditoria de sistemas.

La Subsecretaría de Agricultura, tiene la obligación de proteger el acceso a todos los elementos que se utilicen en las Auditorias de los Sistemas, separándolos de los elementos normales de trabajo. Se debe velar por:

Evitar los accesos no autorizados:

- Proteger las instalaciones de procesamiento de información, de los accesos no autorizados (lógico y físico).

Velar por la continuidad de los servicios:

- Mantener Respaldos de la información digital contenidas en los servidores críticos.
- Preservar la continuidad operativa ante incidentes (corte de luz, problemas de temperatura en el entorno, incendios, entre otros)

6.3.3. Historial de Reportes de Auditoría

Todos los reportes u informes digitales de las auditorías realizadas, con sus respectivas observaciones y recomendaciones de mejora, deben ser almacenadas en un repositorio digital, siendo accedidos solo por el personal que el encargado de seguridad estime conveniente.

7. Periodicidad de evaluación y revisión de la política

El propietario de este documento es el Jefe Departamento TI, quien deberá verificar la vigencia del contenido, por lo menos una vez al año. Si el documento necesita ser modificado y/o debe realizarse alguna actualización, tendrá que ser notificado al resto de los miembros del Comité de Seguridad de la Información.

La periodicidad de evaluación del documento debe hacerse al menos una vez al año.

8. Difusión

La "TI-SSI-17 Política de cumplimiento legal" deberá ser difundida -según lo expresado en la Política General de Seguridad de la información- por medio de la intranet institucional, o por vía circular o por decreto, y/o vía correo electrónico según sea pertinente, asegurándose una completa cobertura.

9. Validez y gestión de documentos

Este documento es válido desde el 20-12-2017.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Abuso considerable en contra de los derechos de propiedad intelectual.
- Mal uso reiterado de los medios de procesamiento de información.
- Cantidad de auditorías de seguridad de la información se han realizado en el periodo.

Creado por:

Ingeniero Proyectos TI
Daniel Coronado Rojo

Validado por:

SUBSECRETARIA DE AGRICULTURA
JEFE DEPTO TECNOLOGIAS DE LA INFORMACION

Jefe Departamento TI
Rafael Reyes Cuevas

Aprobado por:

SUBSECRETARIA DE AGRICULTURA
JEFE DIVISION ADMINISTRATIVA

Encargado de Seguridad de la Información
Jefe División Administrativa
Jorge Vega Saavedra