Subsecretaría de Agricultura

POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

Código:	TI-SSI-10
Versión:	4.0
Fecha de la versión:	20-12-2017
Modificado por:	Daniel Coronado
Aprobado por:	Jorge Vega Saavedra
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
25/11/2011	1.0	Rafael Reyes	Al sólo tener procedimientos verbales, se crea esta política.
25/09/2013	2.0	Cristobal Nef	Se eliminó la sección de registro por no ser relevante para el procedimiento.
15/12/2015	3.0	Daniel Coronado	Se actualizan controles de referencias basado en la nueva versión de la NCH ISO 27001.
20/12/2017	4.0	Daniel Coronado	Se revisa y modifica los campos según la vigencia del contenido, de acuerdo a lo existente en la subsecretaría. Se actualizan los datos referentes a la legislación vigente y los requisitos contractuales. Se agregan los campos de "Ámbito de ejecución y alcance" (pág. 4), "control legal y normativo" (pág. 4), y "Documentos de referencia" (pág. 5).

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 definir las directrices para el uso de los sistemas de información del Servicio, para así asegurar la integridad, confidencialidad y disponibilidad de la información de la Subsecretaría de agricultura con entidades ajenas. Las cuales consisten en:

- Establecer los canales de comunicación, para asegurar la seguridad de la información y el software cuando son intercambiados dentro o fuera de la Subsecretaría con entidades ajenas.
- Establecer medidas en los acuerdos, contratos y/o SLA, para la transferencia segura de la información entre la Subsecretaría y terceros.

2. Ámbito de ejecución, y alcance

La política "TI-SSI-10 Política de intercambio de información", 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.

El Dominio abordado en este documento es el A.13 Seguridad en las Telecomunicaciones, de la norma NCH ISO 27001:2013.

3. Control legal y normativo

- 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,
- PNCS. Política Nacional de Ciberseguridad,
- UMyGD. Otras normas Unidad de Modernización y Gobierno Digital y
- Internet Segura – MINEDUC. Internet Segura.

4. Documentos internos de referencia

- TI-SSI-01 Política General de Seguridad de la Información.
- Norma NCH ISO 27002:2013.
- TI-SSI-21 Política de seguridad para proveedores.

5. Definiciones

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

Información: La información está conformada por un grupo de datos, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento. Actualmente la información puede ser de carácter físico (papel, fichas...) o digital (páginas webs, formularios online...).

Proveedor de servicios: Es una entidad que presta servicios a otras entidades. Por lo general, esto se refiere a un negocio que ofrece la suscripción o servicio web a otras empresas o particulares. Ejemplos de estos servicios incluyen: acceso a internet, operador de telefonía móvil, y alojamiento de aplicaciones web.

TI: Tecnologías de la Información.

Contrato: Es un acuerdo legal manifestado en común entre dos o más personas con capacidad (partes del contrato), que se obligan en virtud del mismo, regulando sus relaciones relativas a una determinada finalidad o cosa, y a cuyo cumplimiento pueden compelerse de manera recíproca, si el contrato es bilateral, o compelerse una parte a la otra, si el contrato es unilateral.

6. Roles y responsabilidades

Para cumplir con los objetivos del presente procedimiento, 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.

Funcionario Departamento TI: Responsables 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.

Personal Externo (proveedores de servicios): Responsables 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.

7. Definición respecto a las materias específicas abordadas

Los controles del dominio abordado de la norma NCH ISO 27001:2013 en este documento, es el siguiente:

N° Control	Nombre control NCH ISO 27001:2013	Descripción del control
A.13.2.1	Políticas y procedimientos de Transferencia de información	Las políticas, procedimientos y controles de transferencia formal deben estar en efecto para proteger la transferencia de la información mediante el uso de todos los tipos de instalaciones de comunicación.

A.13.2.2	Acuerdos sobre la transferencia de información:	Los acuerdos deben abarcar la transferencia segura de la información de negocio entre la organización y terceros.

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

7.1. Canales de comunicación electrónica (control de referencia A.13.2.1)

La información de la organización puede ser intercambiada a través de los siguientes canales de comunicación electrónica: correo electrónico, descarga de archivos desde Internet, transferencia de datos por medio de software, teléfonos, equipos de fax, mensajes de texto por teléfonos móviles, soportes móviles y foros o redes sociales.

El Encargado de Seguridad de la Información determina qué canales de comunicación se pueden utilizar para cada tipo de información y las posibles restricciones sobre los permisos para usar dichos canales; es decir, define qué actividades están prohibidas.

Además de los controles establecidos por el "TI-SSI-07 Política para manejo de información clasificada", el Encargado de Seguridad de la información determina controles adicionales para cada tipo de datos y canales de comunicación según los resultados de la evaluación de riesgos.

7.2. Relaciones con entidades externas (control de referencia A.13.2.2)

Entre las entidades externas se incluyen a diversos proveedores de servicios, empresas de mantenimiento de software y hardware, empresas que manejan transacciones o procesamiento de datos, clientes, etc.

Antes de intercambiar información y/o software con cualquier entidad externa, se debe firmar un contrato, el cual es responsabilidad del solicitante interno que requiere el intercambio de información. El contrato puede estar en papel o en formato electrónico (por ejemplo, aceptando los términos y condiciones generales) y debe contener cláusulas que coincidan con la evaluación de riesgos, incluyendo, al menos, las siguientes:

- Método de identificación de la otra parte.
- Autorizaciones para acceder a la información.
- Asegurar la inviolabilidad.
- Estándares técnicos para la transferencia de datos.
- Respuesta a incidentes.
- Etiquetado y manejo de información sensible.

- Derechos de autor.

Los acuerdos con las entidades externas deben ser confeccionados de acuerdo con la TI-SSI-21 Política de seguridad para proveedores.

8. 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.

9. Difusión

La "TI-SSI-10 Política de intercambio de información" 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.

10. 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:

- Cantidad de canales de comunicación utilizados no contemplados por este documento.
- Cantidad de entidades externas con las que se intercambia información sin tener un contrato firmado.
- Cantidad de sistemas de información comercial que intercambian información sin los controles de seguridad especificados.

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