Subsecretaría de Agricultura

POLÍTICA DE SEGURIDAD PARA PROVEEDORES

Código:	TI-SSI-21
Versión:	2.0
Fecha de la versión:	20-12-2017
Creado por:	Daniel Coronado Rojo
Aprobado por:	Jorge Vega Saavedra
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
07-12-2016	1.0	Daniel Coronado	Para dar cumplimiento con la implementación del control A.15.1.1, se crea esta política.
20-12-2017	2.0	Daniel Coronado	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. 4), y "Documentos internos 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

La información contenida en este documento es de propiedad de la Subsecretaría de Agricultura y debe ser tratada de acuerdo a su nivel de confidencialidad, establecida en la "TI-SSI-07 Política para manejo de información clasificada". El uso no autorizado de la información contenida en este documento podrá ser sancionado de conformidad con la ley chilena. Si usted ha recibido este documento por error, le pedimos eliminarlo y avisar inmediatamente a la Subsecretaría de Agricultura.

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 de este documento es entregar las reglas básicas de seguridad de la información para la relación con los proveedores, con el fin de:

- Evitar malentendidos entre la subsecretaría y el proveedor respecto a las obligaciones de ambas partes para cumplir requisitos relevantes de seguridad de la información, tanto durante el SLA como también en su finalización.
- Reducir los incidentes de seguridad de la información, que pudiese provocar el personal de la entidad proveedora, con los activos de información de la Subsecretaría de Agricultura.
- Reducir los incidentes de indisponibilidad y de vulnerabilidad del servicio provisto por un tercero.

2. Ámbito de ejecución, y alcance

La política "TI-SSI-21 Política de seguridad para proveedores", 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 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 siguientes:

- A.7 Seguridad ligado a los Recursos Humanos,
- A.8 Gestión de Activos, y
- A.15 Relaciones con el Proveedor.

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-21 Política del sistema de seguridad de la información.
- Cláusulas de seguridad para proveedores.

5. Definiciones

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

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.

Propietario de la información: Es el que genera, mantiene y utiliza la información, siendo responsable de ella, y de los procesos que la manipulan, sean estos manuales, mecánicos o eléctricos.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información: también puede involucrar otras propiedades como autenticidad, responsabilidad, no-repudios y confiabilidad.

Confidencialidad: Propiedad de la información de no ponerse 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.

6. Roles y Responsabilidades

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

Jefe del Servicio: Responsable de aprobar: la política de seguridad de la información, y de designar al encargado de seguridad de la información, además, se encarga de formalizar la aprobación o el termino de los contratos que se tengan con los proveedores.

Encargado de Seguridad de la Información: Funcionario designado por el Jefe de Servicio, con el fin de tener a su cargo el desarrollo e implementación de la Política del Sistema de Seguridad para el Servicio, así como también, 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.

Funcionarios Departamento de Compras y Contrataciones: El Departamento de Compras y Contrataciones se encargan del abastecimiento y la compra de bienes y servicios para la Subsecretaria de Agricultura, siendo, además, responsables de la elaboración de los contratos.

Funcionario Abogado Sección Jurídica: Responsables de visar los contratos, antes de ser enviados para su formalización.

Jefe Departamento de Compras y Contrataciones: Responsable de preservar y guardar todos los contratos con los proveedores, designa además al funcionario quien será propietario de dicho acuerdo.

Jefe Departamento TI: Funcionario 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 (contraparte y/o responsable del contrato, incluida jefaturas): 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.

7. 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.7.1.1	Selección	Se debe verificar los antecedentes de proveedor.
A.7.2.2	Concientización, educación y formación en seguridad de la información:	Todos los funcionarios de la subsecretaría, y en donde sea pertinente los contratistas, deben recibir formación adecuada en

		concientización y actualizaciones regulares en políticas y procedimientos organizacionales, pertinentes para su función laboral.
A.8.1.4	Devolución de activos	Los activos se deberán devolver al momento de finalizar el contrato.
A.15.1.1	Política de seguridad de la información para las relaciones con los proveedores	Se deben acordar y documentar, junto con el proveedor, los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso del proveedor a los activos de la organización.
A.15.1.2	Abordar la seguridad dentro de los acuerdos con los proveedores	Todos los requisitos de seguridad de la información pertinente, deben ser definidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización.
A.15.2.1	Supervisión y revisión de los servicios del proveedor	La subsecretaría debe supervisar y auditar la entrega del servicio por parte del proveedor.
A.15.2.2	Gestión de cambios a los servicios del proveedor:	La subsecretaría debe gestionar los cambios que presentara o que fuera necesario realizar al servicio provisto por el proveedor.

A continuación, el desglose de las directrices referente a esta política (control de referencia A.15.1.1):

7.1. Identificación de riesgos

Los riesgos de seguridad relacionados con proveedores se identifican durante el proceso de evaluación de riesgos, según se define en la metodología de evaluación y tratamiento de riesgos. Durante la evaluación de riesgos, se debe tener especial cuidado para identificar riesgos relacionados con tecnología de la información y comunicación, como también riesgos relacionados con la cadena de suministro de productos.

El Encargado de Seguridad de la Información decide si también es necesario evaluar los riesgos relacionados con proveedores específicos.

7.2. Selección (control de referencia A.7.1.1)

El departamento de compras y contrataciones debe realizar verificaciones de antecedentes de determinados proveedores, por medio de herramientas como el registro oficial de proveedores del estado, y en caso que sea necesario, determinará otros métodos que deben aplicarse (Por ejemplo, historial crediticio, antecedentes legales, comportamientos anteriores...).

7.3. Abordar la seguridad dentro de los acuerdos del proveedor (control de referencia A.15.1.2), en el contrato

El Encargado de seguridad de la información es responsable de decidir qué cláusulas de seguridad se incluirán en el contrato con el proveedor. Esta decisión debe estar basada en los resultados de la evaluación y tratamiento de riesgos; sin embargo, las cláusulas que establecen la confidencialidad y la devolución de activos una vez finalizado el acuerdo son obligatorias. Además, los contratos deben garantizar la entrega confiable de productos y servicios, que es sumamente importante con proveedor de servicios de la nube.

En el anexo cláusulas de seguridad para proveedores se incluye una lista de cláusulas sugeridas.

El Encargado de seguridad de la información decidirá si los empleados del proveedor deberán firmar las declaraciones de confidencialidad cuando trabajen para la Subsecretaría de Agricultura.

La jefatura del departamento responsable del servicio contratado, decidirá quién será el administrador o la contraparte técnica de cada contrato; es decir, quién será responsable de un determinado proveedor.

7.4. Concientización, educación y formación en seguridad de la información (control de referencia A.7.2.2)

El administrador o la contraparte técnica del contrato decide qué empleados del proveedor necesita concienciación y capacitación sobre seguridad.

El Jefe del departamento TI o quien lo subrogue es responsable de suministrar toda la capacitación y de realizar la concienciación a esos empleados.

7.5. Supervisión y revisión de los servicios del proveedor (control de referencia A.15.2.1)

El administrador o la contraparte técnica debe revisar y controlar periódicamente el nivel de los servicios y cumplimiento de las cláusulas de seguridad de parte de los proveedores y los informes y registros generados por ellos, como también deben realizarles una auditoría al menos una vez al año.
Todos los incidentes de seguridad relacionados con el trabajo del proveedor deben ser elevados inmediatamente al Encargado de Seguridad de la Información.

7.6. Gestión de cambios a los servicios del proveedor (control de referencia A.15.2.2) o finalización del servicio

El administrador o la contraparte técnica del contrato puede proponer cambios o la finalización del contrato, si no se ha cumplido con las cláusulas estipuladas en el mismo, siendo el Jefe del Servicio quién tomará la decisión final. En caso de realizarse cambios, y sólo si es necesario, el Encargado de Seguridad de la información, realizará una nueva evaluación de riesgos, antes de que se acepten los cambios.

7.7. Eliminación de derecho de acceso, y devolución de activos (control de referencia A.8.1.4)

Cuando se modifica o finaliza un contrato, se deben eliminar los derechos de acceso para los empleados del proveedor.

Además, cuando se cambia o finaliza un contrato, el propietario del contrato debe asegurarse de que todo el equipamiento, software o información en formato electrónico o papel sea devuelto.

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-21 Política de seguridad para proveedores" deberá ser difundida -según lo expresado en la Política del Sistema 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 e importancia de incidentes que surgen por actividades de proveedores.
- Cantidad de contratos en los que no está definido el propietario del contrato.

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