Subsecretaría de Agricultura

POLÍTICA SOBRE COMPUTACIÓN MÓVIL Y TELE-TRABAJO

Código:	TI-SSI-06
Versión:	3.0
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
25-11-2011	1.0	Rafael Reyes	Se crea esta política, debido a que la Subsecretaría de Agricultura no contaba con un apolítica que ampare el uso de tecnologías móviles y tele-trabajo.
15-12-2015	2.0	Daniel Coronado	Se actualizan los controles de referencia a la nueva versión de la ISO 27001. Se realizan otras modificaciones en el punto de "Tele Trabajo" y en la ubicación del registro de los memos.
20-12-2017	3.0	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 "Alcance y usuarios" (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

Para garantizar que la integridad, la disponibilidad y la confidencialidad de la información que esté presente en todo sistema de información de la Subsecretaría, el objetivo del presente documento es:

- Definir las reglas básicas necesarias, para la protección de la información contenidas en los activos de información, que estén ubicados fuera de las instalaciones del Servicio,
- Definir las medidas necesarias para evitar el acceso no autorizado a equipos con procesamiento de información de la Subsecretaría, por parte de terceros y/o funcionarios no autorizados, que estén ubicados fuera de las instalaciones de la Subsecretaría, y
- Establecer las reglas para la autorizar el trabajo de forma remota.

2. Ámbito de ejecución, y alcance

La política "TI-SSI-06 Política sobre computación móvil y tele-trabajo", 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 siguiente:

- A.6 Aspectos organizativos de la Seguridad de la Información,
- A.11 Seguridad Física y Ambiental, y
- A.18 Cumplimiento.

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 de referencia

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

5. Definición

A continuación, una definición de los términos clave utilizado en este documento:

Virtual Private Network (VPN): Es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar estas redes para que sus empleados, desde sus casas, hoteles, etc., puedan acceder a recursos corporativos que, de otro modo, no podrían.

Activo de Información: Los activos de información son todos los elementos para la producción, el procesamiento, la emisión, el almacenaje, la comunicación, la visualización, los encargados y la recuperación de la información que tiene un elevado valor para la organización. Pueden clasificarse en personas, sistemas y datos.

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:

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 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.

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.6.2.1	Política de dispositivos móviles:	Se debe adoptar una política y medidas de apoyo a la seguridad para gestionar los riesgos introducidos al usar dispositivos móviles.
A.6.2.2	Trabajo Remoto	Se debe implementar una política, y medidas de apoyo a la seguridad para

		proteger la información a la que se accede, procesa o almacena en los lugares de trabajo remoto.
A.11.2.6	Seguridad del equipamiento y los activos fuera de las instalaciones	Se deben asegurar todos los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.
A.18.1.2	Derechos de propiedad intelectual	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y al uso de productos de software patentados.

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

7.1. Computación móvil

7.1.1. Introducción

Entre los equipos de computación móvil se incluyen todo tipo de ordenadores portátiles, teléfonos móviles, tarjetas de memoria y demás equipamiento móvil utilizado para almacenamiento y procesamiento de datos.

El equipamiento mencionado precedentemente puede ser llevado fuera de las instalaciones solamente con autorización, de acuerdo a lo establecido en la Política de uso aceptable de los activos y en el Inventario de activos.

7.1.2. Reglas básicas (control de referencia A.6.2.1, y A.11.2.6)

Se debe tener especial cuidado cuando los equipos de computación móvil se encuentran en vehículos (incluyendo automóviles), espacios públicos, habitaciones de hotel, salas de reunión, centros de conferencias y demás áreas no protegidas exteriores a las instalaciones de la organización.

Los funcionarios que se lleven equipos de computación móvil fuera de las instalaciones deberán cumplir las siguientes reglas:

- El equipamiento de computación móvil que contenga información importante, sensible o crítica no debe ser desatendido y, en lo posible, debe quedar resguardado bajo llave o se deben utilizar trabas especiales para asegurarlo.
- Cuando se utiliza equipamiento de computación móvil en lugares públicos, el usuario deberá tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- Las actualizaciones de parches y demás configuraciones del sistema son realizadas por el Departamento T.I. de la Subsecretaría.
- Las protecciones contra códigos maliciosos se instalan y actualiza por el Departamento T.I. de la Subsecretaría.
- La conexión a redes de comunicación y el intercambio de datos debe reflejar la sensibilidad de los datos y se realiza por el Departamento T.I. El usuario que necesite entrar a redes ajenas a la Subsecretaría informará previamente al á Departamento T.I. para su análisis de autorización.
- La protección de datos sensibles debe ser implementada de acuerdo con la Política para manejo de información clasificada.
- En el caso que el equipamiento de computación móvil sea desatendido, se deben aplicar las reglas para equipamiento de usuario desatendido, de acuerdo a la Política de uso aceptable de los equipos.

El Jefe Departamento T.I. es el responsable de la capacitación y concienciación de las personas que utilizan equipamiento de computación móvil fuera de las instalaciones de la organización.

7.2. Tele-trabajo (control de referencia A.6.2.2 y A.18.1.2)

Tele-trabajo significa que los equipos de información y comunicación se utilizan para permitir que los empleados realicen su trabajo fuera de la organización. El tele-trabajo incluye el uso de teléfonos móviles fuera de las instalaciones de la organización.

El tele-trabajo debe ser autorizado por el Encargado de seguridad de la información mediante un memo de autorización.

El Jefe Departamento TI o quien lo subrogue, deberá garantizar lo siguiente:

- Proteger del equipamiento de computación móvil, de acuerdo a lo indicado en el punto anterior.
- Evitar el acceso no autorizado de personas que viven o trabajan en la ubicación donde se realiza la actividad de tele-trabajo.
- Configurar adecuadamente la red local utilizada para conectarse a la Internet.
- Protección de los derechos de propiedad intelectual de la organización, tanto por el software como por otros contenidos que puedan estar protegidos por derechos de propiedad intelectual.
- Proceso de devolución de datos y equipamiento en caso de finalización del empleo.
- Niveles mínimos de configuración de la instalación donde se realizarán las actividades de tele-trabajo.
- Asignación de credenciales VPN.
- Tipos de actividades permitidas y prohibidas.

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

El "TI-SSI-06 Política sobre computación móvil y tele-trabajo" 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 incidentes relacionados con llevar equipamiento de computación móvil fuera de las instalaciones de la organización sin autorización.
- Cantidad de incidentes relacionados con el acceso no autorizado a equipamiento de computación móvil fuera de las instalaciones de la organización.

Creado por:

Ingeniero Proyectos TI
Daniel Coronado Roi

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