Subsecretaría de Agricultura

POLÍTICA PARA MANEJO DE INFORMACIÓN CLASIFICADA

Código:	TI-SSI-07
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	En vista a la necesidad de normar la información clasificada, la Subsecretaría de Agricultura crea esta política
29/07/2015	2.0	Daniel Coronado	Modificación en los niveles de confidencialidad. Actualización controles referenciados a la nueva versión de la norma ISO 27001.
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 "Ámbito de ejecución, y Alcance" (pág. 4), "control legal y normativo" (pág. 4), y "Documentos de referencia" (pág. 5). Se remueve el control A.8.3.1.

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 presente en la Subsecretaría, en el objetivo del presente documento es establecer directrices y reglas para:

- Clasificar la información, según el grado de confidencialidad que disponga, evitando así accesos no autorizados,
- Establecer un correcto manejo y utilización de la información presente en los activos de las Subsecretaría, y
- Garantizar la protección de la información utilizada en la Subsecretaría a un nivel adecuado.

2. Ámbito de ejecución, y alcance

La política "TI-SSI-07 Política para manejo de información clasificada", 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.8 Gestión de Activos,
- A.9 Control de Acceso, y
- A.13 Seguridad en las Telecomunicaciones.

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.
- Planilla de Instrumentos SSI 2017.
- Norma NCH ISO 27002:2013.

5. Definiciones

A continuación, una definición de un término clave utilizado en este documento:

Información: La información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Activo: Información o bienes que tiene valor para la Subsecretaría. El servicio incluye diferentes tipos de activos: activos relacionados con el entorno (edificios, instalaciones, equipamiento) y personal, activos relacionados con los sistemas de tecnologías de información (equipos, software, comunicaciones), activos relacionados con la información (datos, soporte), activos relacionados con las funcionalidades de la organización (productos, servicios) y activos intangibles (credibilidad, conocimiento acumulado).

Activos de información: En el contexto de esta Política, el término activos de información se aplica a los sistemas de información y demás información o equipos, incluyendo documentos en papel, teléfonos móviles, ordenadores portátiles, soportes de almacenamiento de datos, etc.

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

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.

Documento electrónico: Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

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

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.

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.8.2.1	Clasificación de la información	La información debe ser clasificada en términos de requisitos legales, criticidad y sensibilidad para la

		divulgación o modificación sin autorización.
A.8.2.2	Etiquetado de la información	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo al esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos	Se deben desarrollar e implementar los procedimientos para el manejo de activos, de acuerdo al esquema de clasificación de información adoptado por la organización.
A.9.4.1	Restricción del acceso a la información:	Se debe restringir el acceso a la información y a las funciones del sistema de aplicaciones, de acuerdo con la política de control de acceso.
A.13.2.3	Mensajería electrónica	La información involucrada en la mensajería electrónica debe ser debidamente protegida.

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

7.1. Pasos y responsabilidades

Los pasos y responsabilidades para la gestión de la información deberán ser los siguientes:

Nombre del paso	*Responsabilidad*
1. Ingreso del activo de información en el Inventario de activos	Propietario del activo
2. Clasificación de la información	Propietario del activo
3. Etiquetado de la información	Propietario del activo
4. Manejo de la información	Personas que poseen derechos de acceso de acuerdo con esta Política

Si la información clasificada proviene de afuera de la organización, el propietario del activo debe ser el responsable de su clasificación según las reglas establecidas en esta Política, y esta persona se convertirá en el propietario de ese activo de información.

7.2. Clasificación de la información (control de referencia A.8.2.1)

7.2.1. *Criterios de clasificación*

El nivel de confidencialidad deberá ser determinado de acuerdo a los siguientes criterios:

- Valor de la información: según las consecuencias evaluadas durante la evaluación de riesgos.
- Sensibilidad y grado crítico de la información: según el mayor riesgo calculado para cada elemento de información durante la evaluación de riesgos.
- Obligaciones legales y contractuales: según la Lista de obligaciones estatutarias, legales y contractuales.

7.2.2. *Niveles de confidencialidad*

Toda la información deberá ser clasificada en niveles de confidencialidad.

Nivel de confidencialidad	*Etiquetado*	*Criterios de clasificación*	*Restricción de acceso*
Pública	(sin etiquetar)	Hacer pública la información no puede dañar a la Subsecretaría de ninguna forma	La información está disponible para todo el público

Uso interno	USO INTERNO	El acceso no autorizado a la información podría ocasionar daños y/o inconvenientes menores a la Subsecretaría	La información está disponible para todos los funcionarios y terceros seleccionados
Restringida	RESTRINGIDA	El acceso no autorizado a la información podría dañar considerablemente el servicio y/o la reputación de la Subsecretaría	La información está disponible solamente para un grupo específico de funcionarios y de terceros autorizados (condición excepcional amparada en la Ley 20.285, artículo 21).

La regla básica es utilizar el nivel de confidencialidad más bajo garantizando un adecuado nivel de protección para evitar gastos de protección innecesarios.

7.2.3. *Lista de personas autorizadas*

La información clasificada como "Restringida" deberá de estar acompañada de una Lista de personas autorizadas en la que el propietario de la información específica los nombres o los cargos de las personas que tienen derechos de acceso para esa información.

La misma regla aplica para el nivel de confidencialidad "Uso interno" si las personas externas a la organización tendrán acceso a esos documentos.

7.2.4. *Reclasificación*

Los propietarios de activos deberán revisar el nivel confidencialidad de sus activos de información cada [tres años] y deben evaluar si se puede cambiar dicho nivel. Si es posible, deberían bajarlo.

7.3. Etiquetado de la información (control de referencia A.8.2.2)

Los niveles de confidencialidad tendrán que ser etiquetados de la siguiente forma:

- **Documentos en papel**: Se deberá indica el nivel de confidencialidad en la esquina superior derecha de cada página del documento; también se indica en la portada o en el sobre que contiene dicho documento, como también en la carpeta de archivo en la que se guarda el documento.
- **Documentos electrónicos**: Se deberá indica el nivel de confidencialidad en la esquina superior derecha de cada página del documento.
- **Sistemas de información**: el nivel de confidencialidad en aplicaciones y bases de datos debe ser indicado en la pantalla de acceso al sistema, como también en la esquina superior derecha de cada pantalla consecutiva que muestra información confidencial.
- **Correo electrónico**: Se indicará el nivel de confidencialidad en la primera línea del cuerpo del correo electrónico.

- **Soporte de almacenamiento electrónico** (discos, tarjetas de memoria, etc.): Se debe indicar el nivel de confidencialidad sobre la superficie de cada soporte.
- **Información transmitida oralmente**: El nivel de confidencialidad de la información confidencial que se transmite a través de una comunicación cara a cara, por teléfono o por alguna otra vía de comunicación debe ser comunicado antes que la información propiamente dicha.

7.4. Manejo de información clasificada (controles de referencia A.8.2.3, A.9.4.1 y A.13.2.3)

Todas las personas que tengan acceso a información clasificada deberán seguir las reglas enumeradas en el siguiente cuadro. El Encargado de Seguridad de la Información deberá activar acciones disciplinarias cada vez que se no se cumplan las reglas o si la información se transmite a personas no autorizadas. Cada incidente relacionado con el manejo de información clasificada debe ser reportado de acuerdo con el Procedimiento para gestión de incidentes.

Los activos de información podrán ser llevados fuera de las instalaciones solamente con autorización, de acuerdo a lo establecido en la TI-SSI-08 Política de uso aceptable de los activos.

El método para borrado y destrucción segura de soportes está establecido en el documento TI-PRO-01 Procedimientos de operación documentados.

	Uso interno	***Restringida***
Documentos en papel	• Sólo las personas autorizadas pueden tener acceso. • Si es enviado fuera de la organización, el documento debe ser enviado por correo certificado o libro de partes. • Los documentos sólo pueden ser guardados en habitaciones sin acceso público. • Los documentos deben ser retirados constantemente de impresoras y máquinas de fax.	• El documento debe ser almacenado en un gabinete con llave. • Los documentos pueden ser transferidos dentro y fuera de la organización solamente en un sobre cerrado. • Si es enviado fuera de la organización, el documento debe ser enviado con acuse de recibo. • Los documentos deben ser retirados inmediatamente de impresoras y máquinas de fax. • Solamente el propietario del documento puede copiarlo. • Solamente el propietario del documento puede destruirlo.
Documentos electrónicos	• Sólo las personas autorizadas pueden tener acceso. Cuando se	• Sólo las personas con autorización para este documento pueden acceder a la parte del sistema de

	intercambian archivos a través de servicios como FTP, mensajería instantánea, etc., deben estar protegidos con clave. • El acceso a los sistemas de información en los que están almacenados los documentos debe estar protegido por una clave segura. • La pantalla en la que se muestra el documento debe bloquearse automáticamente luego de 10 minutos de inactividad.	información en el que está guardado el documento. • Cuando se intercambian archivos a través de servicios como FTP, mensajería instantánea, etc., deben estar encriptados. • Solamente el propietario del documento puede borrarlo.
Sistemas de información	• Sólo las personas autorizadas pueden tener acceso. • El acceso al sistema de información debe estar protegido por una clave segura. • La pantalla debe bloquearse automáticamente luego de 10 minutos de inactividad. • El sistema de información puede estar ubicado solamente en habitaciones con acceso físico controlado.	• Los usuarios deben finalizar la sesión en el sistema de información si abandonan temporal o permanentemente su lugar de trabajo. • Los datos deben ser borrados solamente con un algoritmo que garantice un borrado seguro.

Correo electrónico	• Sólo las personas autorizadas pueden tener acceso. • El remitente debe verificar cuidadosamente el destinatario. • Aplican todas las reglas mencionadas para "Sistemas de información".	• El correo electrónico debe estar encriptado si se envía fuera de la organización.
Soportes de almacenamiento electrónico	• Sólo las personas autorizadas pueden tener acceso. • Los soportes o archivos deben estar protegidos con clave. • Si es enviado fuera de la organización, el soporte debe ser enviado por correo certificado. • El soporte solamente puede ser guardado en habitaciones con acceso físico controlado.	• Los soportes y archivos deben estar encriptados. • El soporte debe ser almacenado en un gabinete con llave. • Si es enviado fuera de la organización, el soporte debe ser enviado con acuse de recibo. • Sólo el propietario del soporte puede borrar sus datos o destruirlo.
Información transmitida oralmente	• Sólo las personas autorizadas pueden tener acceso a la información. • Las personas no autorizadas no deben estar presentes en la habitación cuando se comunica la información.	• La habitación debe tener aislamiento acústico. • La conversación no debe ser grabada.

*Los controles se implementan acumulativamente; es decir, los controles para cualquier nivel de confidencialidad conllevan los controles definidos para los niveles inferiores: si se establecen controles más estrictos para un nivel de confidencialidad mayor, sólo se implementan esos controles.

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-07 Política para manejo de información clasificada" 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 el acceso no autorizado a la información.
- Cantidad de activos de información clasificados con un nivel de confidencialidad inadecuado.

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