Subsecretaría de Agricultura

POLÍTICA DE USO ACEPTABLE DE LOS ACTIVOS

Código:	TI-SSI-08
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 modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
25/11/2011	1.0	Rafael Reyes	Se crea política, ya que en la Subsecretaría no existe política que formalice el uso aceptable de activos
28/12/2011	2.0	Rafael Reyes	Se actualiza versión para complementar sobre la copia de activos de información y referenciar la ley 17.3336 de derechos de autor.
13/09/2013	3.0	Cristobal Nef	Se actualizan los campos del Inventario de Activos.
16/12/2013	4.0	Cristobal Nef	Se incluyen los registros de devolución de activos y uso de activos fuera de las dependencias.
15/07/2015	5.0	Daniel Coronado	Actualización de los controles de referencia a la nueva versión de la norma chilena ISO 27001 ver 2013. Se modificaron y/o actualizaron los puntos referentes al llenado de planilla de activos, actividades prohibidas, uso de internet y derechos de autor. Se agregó los puntos de protección contra malware y antivirus, plan de continuidad y baja de activos.
20/12/2017	6.0	Daniel Coronado	Se revisa y modifica los campos según la vigencia del contenido, de acuerdo con 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. 5), "control legal y normativo" (pág. 5), y "Documentos internos de referencia" (pág. 5). Se agregan los controles A.8.3.1, A.8.3.2, y A.8.3.3.

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.

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 reglas claras para el uso de los sistemas, las cuales consisten en:

- Identificar los activos de la Subsecretaría y definir las responsabilidades de protección pertinentes.
- Asegurar que la información recibe el nivel de protección adecuado, según su importancia para la Subsecretaría.
- Prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios.

La finalidad de esto es asegurar la integridad, la confidencialidad y disponibilidad de los activos presentes en la Subsecretaría.

2. Ámbito de ejecución, y alcance

El alcance del "TI-SSI-08 Política de uso aceptable de los activos", aplica para los siguientes procesos de provisión de la Subsecretaría de Agricultura: Informe de Factibilidad para la Construcción, Red Agroclimática Nacional y Transferencias.

La política "TI-SSI-08 Política de uso aceptable de los activos", 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.8 Gestión de Activos,

- A.11 Seguridad Física y Ambiental,
- A.12 Seguridad en la Operativa,
- A.13 Seguridad en las Telecomunicaciones, 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.
- Planilla de Instrumento SSI 2017.

5. Definiciones

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

Sistema de información: Incluye todos los servidores y clientes, infraestructura de red, soporte a sistemas y aplicaciones, datos y demás subsistemas y componentes que pertenecen o son utilizados por

la organización, o que se encuentran bajo responsabilidad de la organización. El uso de un sistema de información también incluye el uso de todos los servicios internos o externos, como el acceso a Internet, correo electrónico, etc.

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.

Procesos críticos: Proceso que afecta de forma directa a la satisfacción del cliente y la eficiencia económica de la organización.

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 objetos 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.8.1.1	Inventario de activos	Los activos asociados a la información y a las instalaciones de procesamiento de la información deben ser identificados y se deben mantener y realizar un inventario de dichos activos.
A.8.1.2	Propiedad de los activos	Los activos que se mantienen en inventario deben pertenecer a un dueño.
A.8.1.3	Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con la información y las instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	Todos los empleados y usuarios de terceras

		partes deben devolver todos los activos pertenecientes a la organización que estén en su poder como consecuencia de la finalización de su relación laboral, contrato o acuerdo.
A.8.3.1	Gestión de los medios removibles	Se deben implementar los procedimientos para la gestión de los medios removibles, de acuerdo al esquema de clasificación adoptado por la organización.
A.8.3.2	Eliminación de los medios:	Se deben eliminar los medios de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales.
A.8.3.3	Transferencia Física de medios	Los medios que contengan información se deben proteger contra accesos no autorizados, uso inadecuado o corrupción durante el transporte.
A.11.2.5	Retiro de Activos	El equipamiento, la información o el software no se debe retirar del local de la organización sin autorización previa.
A.11.2.6	Seguridad del equipamiento y los	Se deben asegurar todos los activos fuera

	activos fuera de las instalaciones	de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.
A.12.2.1	Controles contra código malicioso	Se deben implantar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto con los procedimientos adecuados para concientizar a los usuarios.
A.13.2.3	Mensajería electrónica	La información involucrada en la mensajería electrónica debe ser debidamente protegida.
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 (control de referencia A.8.1.3)

7.1. Uso aceptable

Los activos de información solamente pueden ser utilizados a fines de satisfacer necesidades de las actividades con el objetivo de ejecutar tareas vinculadas con la organización.

7.2. Responsabilidad sobre los activos (control de referencia A.8.1.2)

Cada activo de información tiene designado un propietario en el Inventario de activos. El propietario del activo es el responsable de la confidencialidad, integridad y disponibilidad de la información en el activo en cuestión.

7.3. Llenado de planilla Inventario de activos (control de referencia A.8.1.1)

Se debe registrar cada activo, según lo expresado en el documento "TI-PRO-10 Procedimiento de Control de Inventario de Activos".

7.4. Actualización de planilla Inventario de activos

El dueño de cada proceso inventariado en la planilla de Inventario de activos, será responsable de su actualización cuando se adicionen o dejen de estar vigentes los activos de información. Para ello, de manera preventiva al menos 2 veces al año revisará el inventario para verificar dicha información.

7.5. Actividades prohibidas

Está prohibido utilizar los activos de información de manera tal que ocupen innecesariamente capacidad, que disminuya el rendimiento del sistema de información o que presente una amenaza de seguridad. También está prohibido:

- Descargar archivos de imágenes o vídeos que no tienen objetivos de negocios, enviar cadenas de correos electrónicos, jugar juegos, etc.,
- Instalar software en un ordenador local sin el permiso explícito del Jefe Directo y del área de TI. De requerir un software específico, se debe presentar una solicitud al departamento de informática,
- Utilizar aplicaciones Java, controles Active X y otros códigos móviles, excepto cuando esté autorizado por el área TIC,
- Utilizar herramientas criptográficas (encriptado) sobre ordenadores locales, excepto en los casos especificados en la Política para manejo de información clasificada,

- Descargar códigos de programa de soportes externos, y
- Instalar o utilizar dispositivos periféricos como módems, tarjetas de memoria u otros dispositivos para almacenamiento y lectura de datos (por ej., dispositivos USB) sin el permiso explícito del Jefe Directo; el uso en conformidad con la Política para manejo de información clasificada está permitido.

En el caso de ser teléfonos móviles o Smartphones (Android, IOS, entre otros), entregados por el servicio, se prohíbe:

- Instalar aplicaciones de dudosa procedencia o que no estén en "Apple Store", "Play Store" u otros sitios oficiales, además, deben de usarse solo aplicaciones que tengan relación con el servicio,

- No instalar aplicaciones que permitan acceder u habilitar todas las funcionalidades de administrador ("Root"),

- Conectar el teléfono móvil en ordenadores, que no sean de confianza u de la institución. Si se necesita cargar la batería, es preferible que se utilice el cargador de toma corriente, y

- Mantener desactivado el WIFI. Solo se debe activar cuando se va a conectar a una red de confianza u institucional, por lo cual, una vez que ya no necesite de la conexión, se debe desactivar.

7.6. Uso de activos fuera de las instalaciones (controles de referencia A.11.2.5 y A.11.2.6)

Los equipos, la información o software, independientemente de su formato o soporte de almacenamiento, no pueden ser retirados de las instalaciones sin el permiso escrito previo de la Jefatura Directa y del Jefe Departamento TI cuando corresponda a equipos informáticos.

Mientras los activos en cuestión permanecen fuera de la Subsecretaría, deben ser controlados por la persona a la que se le concedió el permiso para retirarlo.

7.7. Gestión de medios removibles (control de referencia A.8.3.1)

Evitar la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios.

Se debe implementar procedimientos para la administración de medios extraíbles (CD, pendrives, discos duros...) de acuerdo con el esquema de clasificación adoptado por la Subsecretaría. Se debe considerar:

- Si ya no es necesario, el contenido de cualquier medio reutilizable que será retirado de la Subsecretaría se debe hacer irrecuperable,

- Donde sea necesario y práctico, se debe requerir una autorización para los medios retirados de la Subsecretaría y se debe mantener un registro de tales retiros para poder mantener un seguimiento de auditoría,

- Todos los medios se deben almacenar en un entorno seguro y protegido, de acuerdo con las especificaciones del fabricante,

- Si la confidencialidad o la integridad de los datos son consideraciones importantes, se debe utilizar técnicas de cifrado para proteger los datos de los medios extraíbles,
- Para mitigar el riesgo de que los medios se degraden mientras aún se necesitan los datos almacenados, los datos se deben transferir a medios nuevos antes de que se vuelvan ilegibles,
- Se deben almacenar varias copias de datos valiosos en medios separados para reducir aún más el riesgo accidental de daños o pérdidas de datos,
- Se debe considerar un registro de medios extraíbles para limitar la oportunidad de pérdidas de datos,
- Las unidades de medios extraíbles solo se deben habilitar si existe una razón institucional para ello, y
- Donde exista la necesidad de utilizar medios extraíbles, se debe monitorear la transferencia de información a dichos medios.

7.8. Eliminación de los medios (control de referencia A.8.3.2)

Los medios se deben eliminar de manera segura cuando ya no se necesitan, a través de procedimientos formales. Se debe considerar:

- Los medios que contienen información calificada como restringida se deben almacenar y eliminar de manera segura, es decir, mediante la incineración, o la destrucción o bien a través del borrado de datos para el uso por parte de otra aplicación dentro de la Subsecretaría,
- Deben existir procedimientos en vigencia para identificar los artículos que pueden requerir de una eliminación segura especial,
- Es posible que sea más fácil realizar las disposiciones necesarias para que se recopilen todos los artículos de medios y que se eliminen de manera segura en vez de intentar separar los artículos sensibles,
- Muchas organizaciones ofrecen servicios de retiro y eliminación de medios; se debe tener cuidado al seleccionar a una parte externa adecuada que cuente con la experiencia y los controles necesarios.

La eliminación de los artículos sensibles se debe registrar para mantener un seguimiento de auditoría

7.9. Transferencia física y/o transporte de los medios (control de referencia A.8.3.3)

Los medios que contienen información deben estar protegidos contra el acceso no autorizado, el uso indebido o la corrupción durante el transporte. Se debe considerar:

- Se debe utilizar servicios de transporte o correo confiables,
- Se debe establecer una lista de servicios de correo autorizados con la dirección,
- Se deben desarrollar procedimientos para verificar la identificación de servicios de correo,
- El empaque debe ser suficiente para proteger los contenidos de daños físicos que probablemente ocurran durante el tránsito de acuerdo con las especificaciones del fabricante, por ejemplo, protección contra factores ambientales que puede reducir la efectividad de la restauración de los medios, como la exposición al calor, a la humedad y a los campos electromagnéticos, y
- Se deben mantener registros, identificando el contenido de los medios, la protección aplicada, así como también un registro de las veces en que se transfirió a los custodios en tránsito y un recibo en el lugar del destino.

7.10. Devolución de activos (control de referencia A.8.1.4)

La devolución de activos que han sido asignados a algún funcionario se deberá hacer tanto en el momento de la desvinculación, como en el caso de renovación tecnológica o por desuso de este.

7.11. Baja de Activos Informáticos

Solo el Jefe del Departamento TI o quién lo subrogue determina si el activo informático cumplió su vida útil o ya no responde eficazmente a las demandas necesarias de la organización, de ser así, es dado de baja para ser reemplazado por uno nuevo. Para esto se notificará a administración, quienes verificarán y requisarán el activo.

7.12. Copias de seguridad

El usuario deber respaldar en la carpeta de red asignada a su área y/o su carpeta personal, toda la información sensible almacenada en su ordenador, como mínimo recomendado, una vez por semana. En los procesos del área T.I. de la Subsecretaría, esta área se encargará de realizar el respaldo de los sistemas utilizados, además de las carpetas compartida de los departamentos y las carpetas de respaldo de los usuarios, para garantizar la operatividad del servicio, ante cualquier incidencia.

7.13. Protección contra malware y virus (control de referencia A.12.2.1)

La subsecretaría debería contar con alguna tecnología, que permita proteger sus sistemas, ante accesos no autorizados, spams o software de carácter malicioso.

Como medidas adicionales, en cada ordenador (sobremesa y portátil), debería contar con algún Antivirus, y un software para evitar el malware (procurando mantenerlos con las últimas actualizaciones), y, además, restringir la instalación -por parte de los funcionarios no pertenecientes al departamento TI- de softwares ajenos a los utilizados en la subsecretaría.

Para asegurar la eficacia de las protecciones antivirus y anti-malware, se debe concientizar a los funcionarios sobre los riesgos del "phishing" y/o de abrir correos electrónicos maliciosos.

7.14. Plan de Continuidad

En caso que un virus y/o malware dañase o comprometiese el funcionamiento correcto del ordenador, el área TI deberá contar con un plan para procurar minimizar los daños que pudiese afectar a la información presente en el equipo.

7.15. Facultados para el uso de sistemas de información

Los usuarios de los sistemas de información solamente pueden acceder a los activos de sistemas de información para los cuales han sido explícitamente autorizados por el propietario del activo.

Los usuarios pueden utilizar los sistemas de información únicamente para las actividades para las cuales han sido autorizados; es decir, para las cuales les han sido otorgados derechos de acceso.

Los usuarios no deben participar en actividades que puedan ser utilizadas para eludir controles de seguridad de los sistemas de información.

7.16. Responsabilidades sobre la cuenta de usuario

El usuario no debe, directa ni indirectamente, permitir que otra persona utilice sus derechos de acceso; es decir, su nombre de usuario; y no debe utilizar el nombre de usuario y/o clave de otra persona. El uso de nombres de usuario grupales está prohibido.

El propietario de la cuenta de usuario es su usuario, que es responsable de su uso y de todas las transacciones realizadas con dicha cuenta de usuario.

7.17. Uso de Internet

Sólo se puede acceder a Internet a través de la red local de la organización asignada a los funcionarios, con la infraestructura y protección de cortafuegos adecuadas. El acceso directo a Internet mediante módems, Internet móvil, red inalámbrica u otros dispositivos de acceso directo a Internet, está prohibido, a excepción de quienes salgan a terreno y tengan asignado un módem inalámbrico.

El área T.I. tiene bloqueado el acceso a determinadas páginas de Internet para usuarios individuales, grupos de usuarios o para todos los empleados de la organización. Si existiese el caso que se tiene bloqueado el acceso a alguna(s) página(s) Web necesaria(s) para el trabajo de un usuario, esta persona puede elevar una petición escrita al área T.I. con copia a su Jefe directo y el Encargado de Seguridad de la Información solicitando autorización para acceder a dicho(s) sitio(s) web. El usuario no debe intentar eludir por su cuenta esa restricción.

El usuario debe considerar a toda la información recibida a través de Internet como no verificada o no confiable. Ese tipo de información puede ser utilizado con fines comerciales solamente después de haber verificado su autenticidad y veracidad.

El usuario es responsable por todas las posibles consecuencias que surjan por el uso no autorizado o inadecuado de servicios o contenidos de Internet.

7.18. Correo electrónico y otros métodos de intercambio de mensajes (control de referencia A.13.2.3)

Entre los métodos de intercambio de mensajes, aparte del correo electrónico, se puede incluir la descarga de archivos desde Internet, la transferencia de datos por medio de chats, teléfonos, equipos de fax, el envío de mensajes de texto por teléfonos móviles, soportes móviles y foros o redes sociales.

De acuerdo con la Política de intercambio, como también con la Política para manejo de información clasificada, el área T.I. determina el canal de comunicación que se puede utilizar para cada tipo de dato, como también las posibles restricciones sobre quién tiene permiso para utilizar los canales; es decir, define qué actividades están prohibidas.

Los usuarios solamente pueden enviar mensajes que contengan información veraz. Está prohibido enviar materiales perturbadores, desagradables, sexualmente explícitos, groseros, difamatorios o cualquier otro contenido inaceptable o ilegal. Los usuarios no deben enviar mensajes basura a personas con las cuales no se ha establecido relación con la función de la Subsecretaría de Agricultura o a personas que no solicitaron ese tipo de información.

Si un usuario recibe un correo electrónico basura, debe eliminarlo.

Si se envía un mensaje con una marca de confidencialidad, el usuario debe protegerlo de acuerdo con lo establecido en la Política para manejo de información clasificada.

El usuario debe guardar todos los mensajes que contienen datos importantes para los negocios de la organización utilizando el método especificado por el área T.I.

Cada correo electrónico debe incluir una exención de responsabilidad, salvo los mensajes enviados a través de los sistemas de comunicación determinados por el área T.I. Si un usuario envía un mensaje a través de un sistema de intercambio de mensajes (redes sociales, foros, etc.), debe declarar sin ambigüedades que no representa el punto de vista de la organización.

7.19. Derechos de autor (control de referencia A.18.1.2)

La Subsecretaría de Agricultura, por medio de esta política, indica que respeta la ley de derechos de autor indicada en la sección de "Documentos de referencia", por lo tanto, existe la instrucción que ni los Administradores de sistema ó usuarios de los sistemas de la Subsecretaría no deben instalar software "pirateado" ni realizar copias no autorizadas del software que pertenece a la organización, excepto en los casos permitidos por ley, por el fabricante o por el área T.I.

Los usuarios no deben copiar software ni otros materiales originales de otras fuentes, y son responsables por todas las consecuencias que pudieran surgir bajo la ley de propiedad intelectual.

7.20. Supervisión del uso de sistemas de información y comunicación

Todos los datos creados, almacenados, enviados o recibidos a través del sistema de información, o de otro sistema de comunicación, de la organización, incluyendo diversas aplicaciones, correo electrónico, Internet, fax, etc., independientemente de si es personal o no, se considera propiedad de la Subsecretaría de Agricultura.

Los usuarios aceptan que personas autorizadas en la organización puedan acceder a todos los datos de ese tipo y que el acceso de dichas personas no será considerado una violación de privacidad del usuario.

La organización puede utilizar herramientas especializadas para identificar y bloquear métodos prohibidos de comunicación y para filtrar contenidos prohibidos.

7.21. Incidencias

Cada funcionario, proveedor o tercero que esté en contacto con datos y/o sistemas de la Subsecretaría de Agricultura debe reportar toda debilidad del sistema, incidente o evento que pudiera derivar en un posible incidente, de acuerdo con lo establecido en el Procedimiento para gestión de incidentes.

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-08 Política de uso aceptable de los activos" 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 uso inadecuado o no autorizado de los activos de información.
- Cantidad de incidentes relacionados con inadecuados programas de capacitación o de concienciación de empleados sobre el uso aceptable del activo de información.

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 ... JEFE DIVISION ADMINISTRATIVA

Encargado de Seguridad de la Información
Jefe División Administrativa

Jorge Vega Saavedra