Subsecretaría de Agricultura

POLÍTICA DE CLAVES

Código:	TI-SSI-04
Versión:	3.0
Fecha de la versión:	20-12-2017
Creado por:	Daniel Coronado
Aprobado por:	Jorge Vega Saavedra
Nivel de confidencialidad:	Uno Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
25-11-2011	1.0	Rafael Reyes	En base a que la Subsecretaría no contaba con este procedimiento formal, sólo instructivo verbal, se procede a crear esta política.
05-08-2015	2.0	Daniel Coronado	Actualización de la política, en base a la versión 2013 de la NCH 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. 5), "Documentos de referencia" (pág. 5), y "Periodicidad de evaluación y revisión de la política" (pág. 8).

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

- Preservar y cuidar la información presente en sistemas informáticos, estaciones de trabajo, por medio de claves de autentificación asignados a los funcionarios y/o personal autorizado,
- Garantizar la gestión y utilización seguras de las claves de autentificación, y.
- Establecer reglas para el cumplimiento de las medidas establecidas en el uso de claves de autentificación seguras.

2. Ámbito de ejecución, y alcance

La política "TI-SSI-04 Política de claves", 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 la Subsecretaría de Agricultura: Informe de Factibilidad para la Construcción, Red Agroclimática Nacional y Transferencias

El Dominio abordado en este documento es el A.9 "Control de Acceso", 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 de referencia

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

5. Definiciones

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

Clave/contraseña: Una clave es una combinación de letras y/o números que brinda, a quien lo conoce, la posibilidad de acceder a un recurso. La clave/contraseña sirve como protección y como mecanismo de seguridad: aquellas personas que no conocen la clave, no pueden acceder al recurso en cuestión.

Criptografía: Proceso de tomar un mensaje no cifrado (texto plano), aplicarle una función matemática (algoritmo de cifrado con una clave) y producir un mensaje encriptado (texto codificado)

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

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 del dominio abordado 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.9.2.1	Registro y cancelación de registro de usuario	Se debe implementar un proceso de registro y cancelación de registro de usuario para habilitar los derechos de acceso.
A.9.2.4	Gestión de información secreta de autenticación de usuarios	Se debe controlar la asignación de información de autenticación secreta mediante un proceso de gestión formal.
A.9.3.1	Uso de información de autenticación secreta	Se debe controlar la asignación de información de autenticación secreta mediante un proceso de gestión formal.
A.9.4.2	Procedimientos de inicio de sesión seguro	Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones debe ser controlado por un procedimiento de inicio de sesión seguro.
A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad

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

7.1. Asignación y cancelación de nombre de usuario en los sistemas (control de referencia A.9.2.1)

El Departamento T.I. velará que cada usuario tenga un nombre o identificador único en cada uno de los sistemas de la Subsecretaría de Agricultura, y la creación de este identificador será derivado de sus nombres y apellidos o el RUT. Con esta medida se pretende evitar confusiones o duplicidad de identificadores.

El Departamento T.I. también deberá revocar el identificador del usuario, cuando este se desvincule o haya sido solicitado por la jefatura de su departamento.

7.2. Obligaciones de los Usuarios (controles de referencia A.9.2.4, A.9.3.1)

Los usuarios deben aplicar buenas prácticas de seguridad en cuanto a la elección y uso de claves:

- No se deben revelar las claves a otras personas, incluyendo cargos directivos y los administradores del sistema.
- No se debe llevar un registro de las claves, a menos que un método seguro haya sido aprobado por el Comité de seguridad de la información (CSI).
- Las claves generadas por el usuario no deben ser distribuidas por ningún medio (oral, escrito, electrónico, etc.); las claves deben ser cambiadas si existen indicios de que puedan estar en riesgo las mismas claves o el sistema (en ese caso, se debe informar un incidente de seguridad).
- Se deben escoger claves seguras de la siguiente forma:
    - utilizando al menos ocho caracteres;
    - utilizando al menos un carácter numérico;
    - utilizando al menos un carácter alfabético en mayúscula y uno en minúscula;
    - una clave no debe ser una palabra que se encuentre en el diccionario, en un dialecto o jerga de ningún idioma; como tampoco ninguna de estas palabras escritas hacia atrás;
    - las claves no deben estar relacionadas con datos personales (por ej., fecha de nacimiento, domicilio, nombre de un familiar, etc.);
    - no se deben usar nuevamente las últimas tres claves.
- Se deben cambiar las claves cada 3 meses.
- Se deben cambiar las claves en el primer ingreso al sistema.
- Las claves no deben ser almacenadas en un sistema de registro automatizado (por ej., macros o explorador).
- No se deben utilizar las mismas claves personales para fines privados y para fines comerciales.

7.3. Gestión de la clave del usuario (control de referencia A.9.3.1, A.9.4.2 y A.9.4.3)

Cuando se asignan y utilizan claves de usuarios, se deben seguir las siguientes reglas:

- Los usuarios tienen la obligación de mantener sus claves en forma confidencial.
- Cada usuario puede utilizar solamente su propio nombre de usuario asignado de forma exclusiva.
- Cada usuario debe tener la posibilidad de escoger su propia clave, en los casos corresponda.
- Las claves utilizadas para el primer acceso al sistema deben ser exclusivas y seguras, según lo establecido precedentemente.
- Las claves de primer acceso deben ser comunicadas al usuario de forma segura, y se debe verificar previamente la identidad del usuario.
- El sistema de gestión de claves debe requerir que el usuario modifique la clave de primer acceso cuando ingrese al sistema por primera vez.
- El sistema de gestión de claves debe requerir que el usuario escoja contraseñas seguras.
- El sistema de gestión de claves debe requerir que los usuarios cambien sus claves cada tres meses.

- Si el usuario solicita una nueva clave, el sistema de gestión de claves debe determinar la identidad del usuario mediante un correo electrónico desde su cuenta de correo electrónico Ministerial.
- La contraseña no debe ser visible en la pantalla durante el inicio de sesión.
- Si un usuario ingresa una clave incorrecta tres veces consecutivas, el sistema debe bloquear la cuenta de usuario en cuestión.
- Las claves creadas por el fabricante del software o hardware deben ser cambiadas durante la instalación inicial.
- Los archivos que contienen claves deben ser guardados en forma separada de los datos de sistema de la aplicación.

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-04 Política de Claves" 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 indebido de claves por personas no autorizadas.
- Cantidad de incidentes relacionados con el manejo inadecuado de claves.

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