Subsecretaría de Agricultura

# POLÍTICA DE CONTROL DE ACCESO

| | |
|---|---|
| Código | TI-SSI-02 |
| Versión: | 1.0 |
| Fecha de la versión: | 20-12-2017 |
| Creado por: | Daniel Coronado |
| Aprobado por: | Jorge Vega Saavedra |
| Nivel de confidencialidad: | Uso Interno |

## Historial de modificaciones

| Fecha | Versión | Creado por | Descripción de la modificación |
|---|---|---|---|
| 20-12-2017 | 1.0 | Daniel Coronado | Debido a las mejoras en el formato que deben tener los documentos, la antigua política de control acceso, se dividió en 2, siguiendo los siguientes criterios: El documento antiguo se cambió de política a procedimiento y este documento tendrá el carácter de política, en donde cumplirá con las exigencias del control A.9.1.1 de la norma NCH ISO 27001:2013. |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

**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 del documento

El objetivo del presente documento es definir los lineamientos para el acceso a los diversos sistemas, equipos, instalaciones e información en base a los requerimientos de la Subsecretaría de Agricultura y del Sistema de Seguridad de la Información.

# 2. Ámbito de ejecución, y alcance

La política "TI-SSI-02 Política de control de acceso", 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.

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 los términos claves utilizados en este documento:

**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.

**Perfiles de usuarios:** Un perfil es un entorno personalizado específicamente para un usuario. Contiene configuración del escritorio y de los programas del usuario. Cuando se inicia sesión en un equipo por primera vez, se crea automáticamente un perfil para ese usuario.

**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 siguiente 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 otros 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 la materia específica que abordada

El control del dominio abordado de la norma NCH ISO 27001:2013 en este documento, es el siguiente:

| N° Control | Nombre control NCH ISO 27001 | Definición |
|---|---|---|
| A.9.1.1 | Política de control del acceso | Se debe establecer, documentar y revisar una política de control de acceso basados en los requisitos de negocio y de seguridad de la información. |

A continuación, el desglose de las directrices referente a este control:

## 7.1. Acceso a la información (control de referencia A.9.1.1)

La subsecretaría, para velar por la integridad, confidencialidad y la disponibilidad de la información contenida en sus activos sean sistemas, equipos, software, servidores, instalaciones, entre otros, deberá establecer reglas de acceso para todos los activos que tengan información relevante para el servicio. Las reglas que se deberán establecer, tendrán que tener en cuenta los siguientes puntos:

- Definir tipos de perfiles, delimitando los derechos de acceso acordes las necesidades del trabajo o al rol del funcionario.
- Los derechos de accesos, deben incluir también a las instalaciones en donde se procesa información.
- En el caso de acceso a sistemas y equipos, se deberá incorporar un sistema de autenticación.
- En caso de los perfiles de acceso privilegiados, se debe de asignar solo al personal clave de estos activos.

- Entregar los permisos de acceso solo a los funcionarios de la subsecretaría que hayan sido aprobados por las jefaturas de sus departamentos. En caso del personal externo, deberán tener la venia de su contraparte institucional.
- Se deberá establecer un procedimiento para la asignación de perfiles de acceso.
- Cada cierto tiempo, se deberá revisar los derechos de acceso, para velar que se mantengan según los requerimientos establecidos.
- En caso de desvinculaciones o de modificaciones en los derechos de acceso, deberán ser notificados por medio de un canal establecido.
- En relación a las desvinculaciones, se deberán revocar los permisos de acceso.
- Mantener documentado los perfiles, y las revisiones de los derechos de acceso.

## 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 cada un año.

## 9. Difusión

El "TI-SSI-02 Política de control de acceso" 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 sistemas en donde no se hayan definidos perfiles de acceso.
- Cantidad de perfiles de acceso no acorde con las necesidades de trabajo del usuario
- Cantidad de solicitudes de derechos de acceso que no se hayan realizado según el conducto establecido.

**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