



Subsecretaría de Agricultura

## POLÍTICA DE SEGREGACIÓN DE RESPONSABILIDADES

Código:	TI-SSI-20
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
17/10/2013	1.0	Cristobal Nef Gatica	Se crea Política de Segregación de responsabilidades.
10/08/2015	2.0	Daniel Coronado	Modificaciones y Actualizaciones en los controles de referencia y en los procesos y activos presentes en esta política.
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). Se quitan los controles A.6.2.1, A.8.2.1, A.8.2.2, A.8.3.1, A.8.2.3 y A.13.2.3.

### 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.

### Nota de confidencialidad

La información contenida en este documento es de propiedad de la Subsecretaría de Agricultura y debe ser tratada de acuerdo a su nivel de confidencialidad, establecida en la "TI-SSI-07 Política para manejo de información clasificada". El uso no autorizado de la información contenida en este documento podrá ser sancionado de conformidad con la ley chilena. Si usted ha recibido este documento por error, le pedimos eliminarlo y avisar inmediatamente a la Subsecretaría de Agricultura.

## Tabla de Contenido

1.	OBJETIVO .....	4
2.	ÁMBITO DE EJECUCIÓN, Y ALCANCE .....	4
3.	CONTROL LEGAL Y NORMATIVO .....	4
4.	DOCUMENTOS DE REFERENCIA .....	5
5.	DEFINICIONES.....	5
6.	ROLES Y RESPONSABILIDADES .....	6
7.	DEFINICIÓN RESPECTO A LAS MATERIAS ESPECÍFICAS ABORDADAS .....	7
7.1.	SISTEMAS Y EQUIPOS DE INFORMACIÓN (CONTROL DE REFERENCIA A.6.1.2). .....	7
7.1.1.	<i>Responsables de los sistemas definidos por proceso (control de referencia A.9.4.1) .....</i>	8
7.1.1.1.	<i>Red Agroclimática Nacional (RAN). .....</i>	8
7.1.1.2.	<i>IFC. ....</i>	8
7.1.1.3.	<i>Transferencias de Fondos de la Subsecretaría.....</i>	8
7.1.2.	<i>Responsables de los sistemas utilizados a nivel del servicio.....</i>	8
7.1.2.1.	<i>Sistema Office 365. ....</i>	8
8.	PERIODICIDAD DE EVALUACIÓN Y REVISIÓN DE LA POLÍTICA .....	9
9.	DIFUSIÓN .....	9
10.	VALIDEZ Y GESTIÓN DE DOCUMENTOS.....	9

## 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 establecer unas pautas para la segregación de responsabilidades para:

- Establecer alcance en las responsabilidades respecto aspectos tecnológicos, mediante segregaciones de funciones.
- Restringir los accesos a los sistemas de información que no sean acordes con las responsabilidades de los funcionarios y/o externos.
- Mitigar los riesgos asociados a modificaciones no autorizadas, por parte de un funcionario en particular u tercero.

## 2. Ámbito de ejecución, y alcance

La política "TI-SSI-20 Política de segregación de responsabilidades", 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.6 Aspectos organizativos de la Seguridad de la Información, y
- A.9 Control de Acceso.

## 3. Control legal y normativo

- D.S. N°14/2014. MODIFICA DECRETO N° 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. Definiciones

A continuación, una definición de un término clave utilizado 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.

**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.

**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.

**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.

**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 Departamento TI:** Es responsable de administrar los sistemas de información, incluidos los perfiles de usuarios con sus privilegios, además de cumplir con lo establecido en este documento y aplicarlo en su entorno laboral.

**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.6.1.2	Segregación de funciones	Se deben segregar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos de 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 continuación, el desglose de las directrices referente a esta política:

### 7.1. Sistemas y Equipos de Información (control de referencia A.6.1.2).

El Departamento T.I. de la Subsecretaría de Agricultura posee la administración general de los Servidores, la administración de los Sistemas de Información asociados a medios informáticos y los equipos informáticos.

La organización de los sistemas y los equipos se han segregado, de manera de disminuir la responsabilidad de los funcionarios.

Los Sistemas de información y los equipos que abarca esta política, son aquellos que se encuentran dentro del alcance de los procesos críticos de la Institución. Estos son los siguientes:

- Web Agromet

- Sistema Twitter
- Plataforma Digital UNIBOX
- Sistema Office 365
- Disco Unidad de Transferencia

Estos pueden ser Internos (alojamiento en los servidores Minagri), como también externos (alojamiento externo).

#### **7.1.1. Responsables de los sistemas definidos por proceso (control de referencia A.9.4.1)**

Los responsables de los sistemas están segregados por proceso.

##### **7.1.1.1. Red Agroclimática Nacional (RAN).**

El sistema Web RAN Agromet, es una plataforma web, utilizada para realizar:

- Visualizaciones los datos climatológicos entregados por las estaciones meteorológicas automáticas (EMA), ubicadas a lo largo del país. El Departamento TI tiene la responsabilidad de ir agregando y/o quitando las EMA de la base de datos del portal RAN.
- Publicaciones de noticias e información ligada al Riesgo Agroclimático, la utilización de esta plataforma está asociada al personal de la Unidad de Emergencias Agrícolas.

Por otro lado, el sistema *Twitter*, es un sistema externo utilizado también por la Unidad de Emergencias Agrícolas, donde ellos administran la cuenta que es utilizada para la difusión de información.

##### **7.1.1.2. IFC.**

El sistema Unibox es una herramienta BPM, que permite el trabajo mediante flujos de trabajo, asignando tareas y la realizando las mismas. Dentro de esta herramienta, existen distintos perfiles de usuario, todos con diversos roles y permisos, sin embargo, la administración general del sistema está a cargo del Departamento T.I.

##### **7.1.1.3. Transferencias de Fondos de la Subsecretaría.**

El Disco Unidad de Transferencias es una unidad alojada en el servidor interno "File Server", en donde se encuentran carpetas, documentos y archivos utilizados por el departamento asociado a este proceso. El Departamento TI tiene la responsabilidad de agregar o quitar el derecho de acceso del funcionario, con previa notificación de la jefatura de este.

#### **7.1.2. Responsables de los sistemas utilizados a nivel del servicio.**

##### **7.1.2.1. Sistema Office 365.**

El Sistema Office 365, es el proveedor de servicios para intercambio de información digital y correo electrónico utilizado en todos los procesos de la subsecretaría. La administración de este sistema está a cargo del Departamento T.I.



## 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-20 Política de segregación de responsabilidades" deberá ser difundida -según lo expresado en la Política del Sistema 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:

- Sistemas nuevos en la Subsecretaria de Agricultura.
- Procesos críticos de la Subsecretaria de Agricultura.

Creado por:



Ingeniero Proyectos TI  
Daniel Coronado Rojo

Validado por:



Jefe Departamento TI  
Rafael Reyes Cuevas



Aprobado por:

  
Encargado de Seguridad de la Información  
Jefe División Administrativa  
Jorge Vega Saavedra