Subsecretaría de Agricultura

POLÍTICA ACCESO Y SEGURIDAD FÍSICA

Código:	TI-SSI-14
Versión:	4.0
Fecha de la versión:	20-12-2017
Creado por:	Daniel Coronado Rojo
Aprobado por:	Jorge Vega Saavedra
Nivel de confidencialidad:	Interno

Historial de Versiones

Fecha	Versión	Creado por	Descripción de la versión
14/12/2012	1.0	Cristobal Nef	Documento que entrega los lineamientos sobre el control de acceso y seguridad física para los funcionarios de la Subsecretaría de Agricultura.
30/07/2013	2.0	Cristobal Nef	Se agregan párrafos 6 y 7 sobre Elementos de Soporte y Seguridad en el Cableado
15/12/2016	3.0	Daniel Coronado	Se actualiza referencias a la nueva versión de la norma ISO 27001; se amplía el alcance de cobertura a las oficinas regionales.
20/12/2017	4.0	Daniel Coronado	Se actualizan los documentos de referencia. Se agrega el campo de "Alcance y usuarios". 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).

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

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 **6**

7.1. PERÍMETROS DE SEGURIDAD FÍSICA, Y CONTROL DE ACCESO FÍSICO (CONTROLES DE REFERENCIA A.11.1.1 Y A.11.1.2) 8

7.1.1. Nivel central *8*

7.1.2. Nivel Regional *8*

7.2. ASEGURAR SEGURIDAD DE OFICINAS, SALAS E INSTALACIONES (CONTROLES DE REFERENCIA A.11.1.3 Y A.11.1.5). 9

7.2.1. Data Center. *9*

7.2.2. Oficinas. *9*

7.3. ÁREAS DE ENTREGA Y CARGA (CONTROL DE REFERENCIA A.11.1.6). 9

7.4. ELEMENTOS DE SOPORTE (CONTROL DE REFERENCIA A.11.2.2) 9

7.5. SEGURIDAD EN EL CABLEADO (CONTROL DE REFERENCIA A.11.2.3) 10

8. PERIODICIDAD DE EVALUACIÓN Y REVISIÓN DE LA POLÍTICA **10**

9. DIFUSIÓN **10**

10. VALIDEZ Y GESTIÓN DE DOCUMENTOS. **11**

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 de este documento es entregar los lineamientos sobre el control de acceso y seguridad física en la Subsecretaría de Agricultura para:

- Evitar incidentes relacionados con los accesos no autorizados a las instalaciones, estaciones de trabajo y lugares físicos con equipos de procesamiento de información,
- Evitar los incidentes relacionados a fallas energéticas, de conectividad alámbrica, o de otra índole que afecte la integridad de los equipos de procesamiento de información, y
- Disponer de elementos de soporte, para reducir al mínimo la indisponibilidad de los activos de información.

2. Ámbito de ejecución, y alcance

La política "TI-SSI-14 Política de acceso y seguridad física", 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.11 Seguridad Física y Ambiental, 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 ISO NCH 27002:2013.

5. Definiciones

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

Incidente de Seguridad: Situación adversa que pone en riesgo un proceso.

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

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

Control de Acceso: El control de acceso consiste en la verificación de si una entidad (una persona, vehículo, ordenador, etc....) solicitando acceso a un recurso tiene los derechos necesarios para hacerlo.

Data Center: La data center o centro de datos o **centro** de procesamiento de **datos** (CPD) es aquella ubicación en donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

UPS: Sistema de alimentación ininterrumpida (**SAI**), en inglés uninterruptible power supply (**UPS**), es un dispositivo que, gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados.

Canaleta: Las canaletas son tubos metálicos o plásticos que conectados de forma correcta proporcionan al cable una mayor protección en contra de interferencias electromagnéticas originadas por los diferentes motores eléctricos.

Externo (personal): Empresa externa que brinda un servicio a la Subsecretaría.

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.

Jefe Departamento Administración: Responsable de definir e implementar las medidas de control de acceso a las instalaciones de la institución, gestionar y controlar que todas las instalaciones del edificio a nivel central, como también las oficinas regionales (Seremias), funcionen en condiciones adecuadas.

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 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.11.1.1	Perímetro de seguridad física	Se define un perímetro de seguridad, para proteger las áreas que contienen

		información sensible o crítica, y las instalaciones de procesamiento de información.
A.11.1.2	Controles de ingreso físico	Las áreas o zonas seguras deben protegerse por un control de ingreso.
A.11.1.3	Asegurar Seguridad de oficinas, salas e instalaciones:	La subsecretaría debe disponer de un sistema de seguridad física en oficinas salas e instalaciones.
A.11.1.5	Trabajo en áreas seguras	Se deben diseñar y aplicar procedimientos para trabajar en áreas seguras.
A.11.1.6	Áreas de entrega y carga	Debe existir un nexo entre las entidades externas y la subsecretaría, para controlar u aislar el ingreso a las áreas u instalaciones de procesamiento de información.
A.11.2.2	Elementos de soporte	Se debe proteger el equipamiento frente a cortes de luz y otras interrupciones causadas por fallas en los elementos de soporte.
A.11.2.3	Seguridad en el cableado	Se debe proteger contra la interceptación, interferencia o daños

		el cableado usado para energía y telecomunicaciones.

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

7.1. Perímetros de Seguridad física, y control de acceso físico (controles de referencia A.11.1.1 y A.11.1.2)

El perímetro de seguridad de la Subsecretaría está clasificado en dos grandes grupos: Nivel Central y Nivel Regional. Para proteger las instalaciones de acceso no autorizados, se deberá aplicar las siguientes medidas:

7.1.1. Nivel central

En la entrada del nivel central, debe existir un funcionario, que tendrá que administrar el ingreso de las personas externas a la Institución. Las personas externas a quienes se les haya autorizado en ingreso, se les deberá entregar una tarjeta de acceso para visitas (que tendrán que regresar cuando se retiren), registrando la entrada y salida.

En cada piso perteneciente a la subsecretaría de Agricultura, se debe contar con barreras física de acceso.

Para complementar el control de acceso, se deberá disponer de algún sistema de vigilancia.

En cuanto a la Tarjeta de Acceso:

Todo funcionario del nivel central de la Subsecretaría tendrá que disponer de una tarjeta de acceso y es su deber llevarla en un lugar visible, para facilitar la identificación de las personas externas a la Institución.

Si un funcionario identifica a una persona externa que no lleva su tarjeta de acceso a la vista, debe reportarlo al Departamento de Administración, quienes se encargarán de tomar las medidas que correspondan.

7.1.2. Nivel Regional

En caso de las regiones, debe existir un funcionario a cargo de la administración del ingreso y salida de personas externas a la oficina regional, registrando la entrada y salida.

Para complementar el control de acceso, se deberá disponer de algún sistema de vigilancia.

7.2. Asegurar Seguridad de oficinas, salas e instalaciones (controles de referencia A.11.1.3 y A.11.1.5).

7.2.1. Data Center.

La Subsecretaría cuenta con dos centros de datos (data center), ubicados en el nivel central. El principal se encuentra en el séptimo piso del edificio (en las dependencias de ODEPA), mientras que el otro, está en el quinto piso, en el área de administración de la Subsecretaría. Por lo cual, para preservar la seguridad de los "data center", se debe controlar el acceso, por medio de las siguientes medidas:

- Los accesos a los "data center" deben estar acotados solo a funcionarios autorizados. En el caso del personal externo y del resto de los funcionarios, solo podrán acceder acompañados.
- El acceso a los "data center", debe estar protegido por medio de barreras físicas.
- El acceso a los "data center", deben de estar siempre bajo vigilancia.

7.2.2. Oficinas.

Las oficinas de la Subsecretaría deben estar ubicadas tras una barrera de acceso, para evitar accesos no autorizados, además los lugares donde se almacena información crítica (archivadores, oficinas de superiores), se deben proteger en estanterías u oficinas de almacenaje de acceso restringido solo al personal autorizado, cuidando así la confidencialidad, integridad y disponibilidad de los activos de Información.

7.3. Áreas de entrega y carga (control de referencia A.11.1.6).

La Subsecretaría debe contar con una oficina de partes o alguna entidad que sea el nexo entre las partes externas y el servicio. A nivel central se debe ubicar en el primer piso, en la entrada del edificio, para facilitar el control del acceso público, en cambio a nivel regional, debe estar cerca de la entrada de la Seremia.

En el caso de adquisiciones del servicio, los proveedores tendrán que ser recibidos por un funcionario, quien deberá solicitar la información de la empresa y realizar el contacto con el responsable correspondiente.

7.4. Elementos de soporte (control de referencia A.11.2.2)

La Subsecretaría deberá procurar mantener sus tableros eléctricos en buen estado y con la capacidad necesaria para cubrir la demanda energética del servicio, para así evitar incidencias.

Los computadores del personal clave, deberán contar con una unidad de fuente de energía ininterrumpidas (UPS). Los "data center" deben también disponer de UPS para evitar caídas espontáneas, además, el "data center" principal, deberá contar con un soporte eléctrico de emergencia, para preservar la continuidad de los servicios, en caso de corte de luz. En caso de altas temperaturas o principio de incendio, se debe disponer de un sistema de enfriamiento y un sistema extintor de incendios.

Las instalaciones deben disponer de un sistema de iluminación de emergencia que se activen en cada ocasión que se produzcan cortes de energía.

Para ayudar en la prevención de posibles cortes de energía, se debe contratar alguna empresa reparaciones (distinta al proveedor de electricidad).

7.5. Seguridad en el Cableado (control de referencia A.11.2.3)

Las instalaciones eléctricas, datos y telefonía se tienen que proteger. Para no producir interferencias electromagnéticas en el cableado que recorren los distintos pisos y oficinas, deben de estar debidamente separadas.

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

La "TI-SSI-14 Política de acceso y seguridad física" 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:

- Accesos físicos no autorizados.
- Robos o alguna otra pérdida de los activos 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

Jefe Departamento de Administración
Claudio Yañez Gajardo

Aprobado por:

SUBSECRETARIA DE AGRICULTURA
JEFE DIVISION ADMINISTRATIVA

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