Subsecretaría de Agricultura

POLÍTICA DE PANTALLA Y ESCRITORIO LIMPIOS

Código:	TI-SSI-05
Versión:	4.0
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	Actualmente la Subsecretaría no contaba con una política que defina pantalla y escritorios limpios, razón que se crea esta política.
30-07-2013	2.0	Cristobal Nef	Se agrega párrafo sobre consumo de alimentos en los puestos de trabajo.
09-07-2015	3.0	Daniel Coronado	Actualizaciones controles de referencia a la nueva versión de la NCH ISO 27001. Se agrega párrafo sobre protección de estación de trabajo móvil.
20-12-2017	4.0	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. 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

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:

- Definir reglas para evitar el acceso no autorizado a la información en los puestos de trabajo, como también en las instalaciones y a los equipos compartidos.
- Establecer medidas para evitar daños en el equipamiento y en las instalaciones, o en cualquier medio que contenga información.
- Establecer reglas para evitar pérdidas de información en los puestos de trabajos, equipamientos y en las instalaciones.

2. Ámbito de ejecución, y alcance

La política "TI-SSI-05 Política de pantalla y escritorio limpios", 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.

Los dominios abordados de la norma NCH ISO 27001:2013 en este documento, son los siguiente:

- A.9 "Control de Acceso", y
- A.11 "Seguridad Física y Ambiental".

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. InternetSegura.

4. Documentos de referencia

- TI-SSI-01 Política General de Seguridad de la Información.
- TI-SSI-07 Política para manejo de información clasificada.
- Norma NCH ISO 27002:2013.

5. Definiciones

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

Documento: Es una carta, diploma o escrito (formato físico o digital) que ilustra acerca de un hecho, situación, o circunstancia.

Clave de acceso: Palabra o clave utilizada para confirmar una identidad en un sistema remoto y evitar que una persona pueda usurpar la identidad de otra.

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.

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 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: Son responsables 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.9.4.2	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.11.2.1	Ubicación y protección del equipamiento:	El equipamiento se debe ubicar y proteger para reducir los riesgos provocados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.
A.11.2.8	Equipo de usuario desatendido	Los usuarios se deben asegurar de que a los equipos desatendidos se les da protección apropiada.
A.11.2.9	Política de escritorio y pantalla limpios:	Se debe adoptar una política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de la información.

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

Cabe destacar toda la información clasificada como "Restringida", de acuerdo a lo establecido en la "TI-SSI-07 Política para manejo de información clasificada", es considerada sensible para este documento.

7.1. Protección del puesto de trabajo (control de referencia A.11.2.9)

7.1.1. Política de escritorio limpio (control de referencia A.11.2.1)

Para preservar la integridad, la confidencialidad y la disponibilidad de la información, presentes en documentos en papel o en equipos informático, en la Circular N°004 del 20 de diciembre de 2017, se recomienda a los funcionarios de la Subsecretaria de Agricultura, cumplir con las siguientes prácticas de escritorio limpio:

- No consumir alimentos como: bebida, café, té u otro líquido que pudiere derramarse en el equipamiento informático o en su escritorio, dañando la información ahí dispuesta.
- No fumar en las cercanías del equipamiento informático y otros bienes.
- Se recomienda que las áreas de trabajo, llámese esto a los escritorios asignados a cada funcionario, estén libres de objetos, artículos y líquidos que no tengan relación a la debida realización de su función diaria.

Haciendo referencia a lo anteriormente mencionado, los funcionarios deben cumplir con las siguientes instrucciones oficiales.

- Si la persona autorizada no se encuentra en su puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos (pendrives, cd, discos externos, etc.), etiquetados como sensibles, deben ser retirados del escritorio o de otros lugares (impresoras, equipos de fax, fotocopiadoras, etc.) para evitar el acceso no autorizado a los mismos.
- Este tipo de documentos y soportes deben ser archivados de forma segura, de acuerdo a lo establecido en la Política para manejo de información clasificada.

7.1.2. Política de pantalla limpia (control de referencia A.9.4.2 y A.11.2.8)

Si la persona autorizada no se encuentra en su puesto de trabajo, se debe quitar toda la información sensible de la pantalla, y se debe denegar el acceso a todos los sistemas para los cuales la persona tiene autorización.

En el caso de una ausencia corta (mínima de 10 minutos), los equipos deben contar con un bloqueado de pantalla con una clave. Si la persona se ausenta por un período más prolongado (superior a 30 minutos), la estación de trabajo deberá entrar en modo suspensión. Si la estación de trabajo del funcionario es un portátil, deberá estar además protegida con un candado físico con llave, para evitar un posible robo, hurto o retiro no autorizado.

7.2. Protección de instalaciones y equipos compartidos (control de referencia A.9.4.2 y A.11.2.9)

Los documentos que contienen información sensible deben ser retirados inmediatamente de las impresoras, equipos de fax y fotocopiadoras.

El uso no autorizado de impresoras, fotocopiadoras, escáneres y demás equipamiento compartido para copiado se deberá evitar asignando una clave a cada usuario de la Subsecretaría.

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-05 Política de pantalla y escritorio limpios" 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 acceso no autorizado a información en escritorios, impresoras, fotocopiadoras, equipos de fax, puestos de trabajo, etc.

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