



RESOLUCION EXENTA N° FC-F-00321
MAT: APRUEBA POLITICA DE
PANTALLAS Y ESCRITORIOS LIMPIOS.
POLITICA-SSI-A-7.7.
SANTIAGO, 19-05-2025

VISTOS:

Lo dispuesto en la Ley N° 18.989, en su Título II sobre el Fondo de Solidaridad e Inversión Social; Ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado; En la Ley 21.180 de Transformación digital del Estado; Ley N° 18.575 de Bases Generales de Administración del Estado; Ley 21.722 de Presupuestos del sector público para el año 2025; la Resolución N° 36/2024 que fija Normas sobre Exención del Trámite de Toma de Razón y Resolución N°8 que modifica la Resolución N°36/2024 ambas de la Contraloría General de la República; en el Decreto Supremo N° 15/2022, del Ministerio de Desarrollo Social y Familia, que nombra a persona que indica en el cargo de Director Ejecutivo del Fondo de Solidaridad e Inversión Social; y demás antecedentes tenidos a la vista.

CONSIDERANDO:

1°.- Que, El Fondo de Solidaridad e Inversión Social – FOSIS, es un Servicio Público funcionalmente descentralizado, con personalidad jurídica y patrimonio propio, regulado por el Título II de la Ley 18.989, cuya misión es contribuir a la superación de la pobreza y vulnerabilidad social a través de estrategias que fortalezcan la cohesión social, las habilidades y capacidades de personas, familias y comunidades, con pertinencia territorial y enfoque de género y su finalidad es financiar en todo o en parte planes, programas, proyectos y actividades especiales de desarrollo social.
 2°.- El Memorándum FC.MEM. 00215-2025 de fecha 30 de abril de 2025, enviado por doña Roxana Vercoutare Carter, encargada de Ciberseguridad, en el que solicita formalizar mediante un acto administrativo la aprobación de la POLITICA DE PANTALLAS Y ESCRITORIOS LIMPIOS, POLITICA-SSI-A-7.7 versión 3 de fecha 23 de abril de 2025.
 3°.- Que resulta necesario para el FOSIS establecer normas para el uso seguro de información en los puestos de trabajo de todos los funcionarios y servidores a honorarios o terceros que se relacionen con FOSIS con la finalidad de proteger los activos de información tanto físicos como virtuales y asegurar que los equipos no supervisados cuenten con la protección adecuada.
 4°.- Que, en virtud del principio de formalidad que rige los actos de la Administración establecido en el artículo 3 de la Ley N° 19.880, corresponde dictar un acto administrativo aprobatorio.

RESUELVO:

APRUEBASE la POLITICA DE PANTALLAS Y ESCRITORIOS LIMPIOS, POLITICA-SSI-A-7.7 versión 3 de fecha 23 de abril de 2025, cuyo texto es el siguiente:



	POLÍTICA DE PANTALLAS Y ESCRITORIOS LIMPIOS	Fecha emisión: 17/11/2017
	POLÍTICA-SSI-A-7.7	Versión: 3
		Fecha versión: 23/04/2025

1. OBJETIVO

Establecer normas para el uso seguro de información en los puestos de trabajo de todos los funcionarios de FOSIS, con la finalidad de proteger los activos de información tanto físicos como virtuales y asegurar que los equipos no supervisados cuenten con la protección adecuada.

2. ALCANCE

Esta política se aplica a todos los funcionarios, servidores públicos a honorarios y terceras partes, que presten servicios para el FOSIS y que en el desarrollo de sus funciones utilizan equipos, pantallas y escritorios donde se procese información, o papeles y medios de almacenamiento móviles.

Esta política está dentro del alcance de la norma NCH-ISO 27001:2023 control:

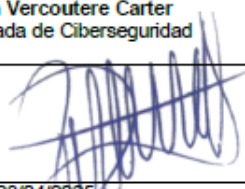
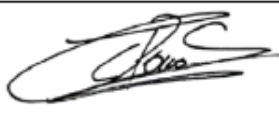
- 7.7 Escritorio despejado y pantalla limpia

3. DOCUMENTOS RELACIONADOS

- [Política general de seguridad de la información del Fondo de Solidaridad e Inversión Social FOSIS, vigente, sus políticas, procedimientos e instructivos.](#)
- [NCh-ISO 27001:2023 Seguridad de la Información, Ciberseguridad y protección de la privacidad – Sistema de gestión de Seguridad de la Información- Requisitos, Decreto N° 83, de 2004, de la Secretaría General de la Presidencia: Aprueba norma técnica para los órganos de la Administración del Estado, sobre seguridad y confidencialidad del documento electrónico.](#)

4. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
Encargado de Seguridad de la Información	Determinar los requisitos de Seguridad respecto a cómo tratar la información, junto con velar la correcta aplicación de la presente política.
Jefe de Tecnologías de la Información y las Telecomunicaciones	Implementar las directrices de seguridad definidas en esta política para el manejo y protección de la información.
Funcionarios, Planta, contrata, honorarios	Proteger tanto sus artículos personales como los del Servicio y más aún, toda la información institucional que maneja y/o utiliza.

Elaborado por: Roxana Vercoutere Carter Encargada de Ciberseguridad	Revisado y Aprobado por: Cristian Salomó González Encargado de Seguridad de la Información Subdirector de Usuarios
	
Fecha: 23/04/2025	Fecha: 30.04.2025
Documento Impreso – Copia no controlada sin timbre original	



5. POLÍTICA

El propósito de esta política es reducir riesgos de acceso no autorizado, pérdida y daño de información en escritorios, pantallas y otros lugares accesibles durante y fuera del horario de trabajo.

Toda vez que un usuario/a se ausenta de su lugar de trabajo, junto con bloquear su equipo (tecla **Windows + L**), debe guardar en lugar seguro cualquier documento, y/o dispositivo que contenga información de su responsabilidad, como la nube de office 365 en caso de información digital.

Al finalizar la jornada de trabajo, el usuario debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno, además desconectarse de los computadores centrales, servidores y estaciones de trabajo de oficina cuando la sesión es finalizada, es decir, debe apagar el equipo.

Si el usuario/a está ubicado cerca de zonas de atención de público, al ausentarse de su lugar de trabajo debe guardar también los documentos y medios que contengan información de uso interno.

Todos los funcionarios/as deben tener en cuenta las siguientes directrices:

- a) guardar bajo llave información sensible o crítica (por ejemplo, en papel o en medios de almacenamiento electrónico) (idealmente en una caja fuerte, armario u otra forma de mobiliario de seguridad) cuando no se necesite, especialmente cuando la oficina esté desocupada;
- b) proteger dispositivos de puntos finales de usuarios¹ de seguridad mediante cerraduras con llave u otros medios cuando no se usen o estén desatendidos;
- c) todos los usuarios/as que tengan asignados computadores o dispositivos móviles deben protegerlos del uso no autorizado o robo mediante un candado con llave o un control equivalente, además de considerar los cuidados establecidos en el instructivo para el retiro de activos y seguridad fuera de las instalaciones.
- d) dejar los dispositivos terminales del usuario desconectados o protegidos con un mecanismo de bloqueo de pantalla y teclado controlado por un mecanismo de autenticación del usuario cuando estén desatendidos. Todos los computadores y sistemas deben estar configurados con una función de tiempo de espera o de cierre de sesión automático;
- e) se debe evitar el uso no autorizado de fotocopiadoras u otro tipo de tecnologías de reproducción (ej. escáneres, cámaras digitales). Los documentos que contienen información sensible se deben extraer inmediatamente de las impresoras².
- f) se deben recoger las salidas de las impresoras o dispositivos multifunción de forma inmediata.
- g) almacenar de forma segura los documentos y medios de almacenamiento extraíbles que contengan información sensible y cuando ya no se necesiten, desecharlos

¹ Los dispositivos de punto final son los equipos que permiten a los usuarios conectarse a una red informática. Son componentes esenciales de las redes de computación modernas. Algunos ejemplos de dispositivos de punto final son: Computadoras de escritorio, Computadoras portátiles, Tabletas, Teléfonos inteligentes, Impresoras, Terminales de punto de venta (POS), Dispositivos del Internet de las cosas (IoT).

² Ejemplo Información Sensible: Información sobre proyectos específicos, presupuestos y recursos asignados que pueden ser sensibles en términos de planificación y ejecución, Información identificable de beneficiarios como nombres, direcciones, números de identificación y detalles de contacto.



	POLÍTICA DE PANTALLAS Y ESCRITORIOS LIMPIOS
	POLÍTICA-SSI-A-7.7

mediante mecanismos de eliminación seguros³ según lo descrito en el 5.1 de la política;

- h) establecer normas y orientaciones para la configuración de ventanas emergentes en pantallas (por ejemplo, desactivar las nuevas ventanas emergentes del correo electrónico y mensajería, si es posible, durante presentaciones, pantallas compartidas o en una zona pública);
- i) borrar la información sensible o crítica de pizarras y otros tipos de pantalla cuando ya no sea necesaria.

5.1. Borrado seguro y destrucción de la información

Para finalizar el ciclo de vida de la información desde el enfoque de la seguridad, es indispensable cubrir un aspecto de suma importancia: la destrucción de la información.

5.1.1. Métodos de destrucción de la información⁴

Los medios eficaces que evitan completamente la recuperación de los datos contenidos en los dispositivos de almacenamiento son: la desmagnetización, la destrucción y la sobreescritura en la totalidad del área de almacenamiento de la información.

5.1.1.1. Desmagnetización

La desmagnetización consiste en la exposición de los soportes de almacenamiento a un potente campo magnético, proceso que elimina los datos almacenados en el dispositivo.

Este método es válido para la destrucción de datos de los dispositivos magnéticos, como, por ejemplo, los discos duros, disquetes, cintas magnéticas de backup, etc.

Cada dispositivo, según su tamaño, forma y el tipo de soporte magnético de que se trate, necesita de una potencia específica para asegurar la completa polarización de todas las partículas.

5.1.1.2. Destrucción física

Desintegración, pulverización, fusión e incineración: son métodos diseñados para destruir por completo los medios de almacenamiento. Estos métodos suelen llevarse a cabo en una destructora de metal o en una planta de incineración autorizada, con las capacidades específicas para realizar estas actividades de manera eficaz, segura y sin peligro.

Trituración: las trituradoras de papel se pueden utilizar para destruir los medios de almacenamiento flexibles. El tamaño del fragmento de la basura debe ser lo suficientemente pequeño para que haya una seguridad razonable en proporción a la confidencialidad de los datos que no pueden ser reconstruidos. Los medios ópticos de almacenamiento (CD, DVD, magnetoópticos) deben ser destruidos por pulverización, trituración de corte transversal o incineración. Cuando el material se desintegra o desmenuza, todos los residuos se reducen a cuadrados de cinco milímetros (5mm) de lado.

Como todo proceso de destrucción física, su correcta realización implica la imposibilidad de recuperación posterior por ningún medio conocido.

³ Los mecanismos de eliminación segura de información incluyen la sobreescritura, la desmagnetización, la destrucción física, el cifrado y la destrucción electromagnética.

⁴ [Ver Instructivo de eliminación de documentos del Fondo de Solidaridad e Inversión Social](#)



	POLÍTICA DE PANTALLAS Y ESCRITORIOS LIMPIOS
	POLÍTICA-SSI-A-7.7

En el caso de los discos duros se debe asegurar que los platos internos del disco han sido destruidos eficazmente, no sólo la cubierta externa.

5.1.1.3. Sobreescritura

La sobreescritura consiste en la escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento. Para asegurar la completa destrucción de los datos se debe escribir la totalidad de la superficie de almacenamiento.

La sobreescritura se realiza accediendo al contenido de los dispositivos y modificando los valores almacenados, por lo que no se puede utilizar en aquellos que están dañados ni en los que no son regrabables, como los CD y DVD.

5.1.2. Documentación de las operaciones de borrado realizadas:

- Al seleccionar una herramienta de borrado, elegir aquella que permita la obtención de un documento que identifique claramente que el proceso de borrado se ha realizado, detallando cuándo y cómo ha sido realizado
- En el caso de que la destrucción lógica no se realice correctamente por fallo del dispositivo, este hecho debe documentarse claramente y utilizar métodos de destrucción física de dicho soporte, asegurando que se realice de forma respetuosa con el medio ambiente.

6. DIFUSIÓN

La comunicación de la presente política se efectúa de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, mediante los siguientes canales:

- Publicación en la intranet de FOSIS
- Correo informativo.

7. SANCIONES


El incumplimiento de las obligaciones emanadas de esta Política y todos sus procedimientos asociados es sancionado en los términos de las leyes vigentes y aplicables bajo el Estatuto Administrativo para los funcionarios del FOSIS. Cuando el incumplimiento se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de esta política, se procede al término anticipado del contrato, por incumplimiento de obligaciones, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

8. REVISIÓN Y MEDICIÓN

La presente política deberá ser revisada al menos cada dos años o cuando ocurran cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad.

9. TABLA DE MODIFICACIONES

Versión	Motivo del Cambio	Fecha de aprobación
1	Puesta en marcha de la primera versión de la norma	17/11/2017
2	Actualiza logo Modifica objetivo Amplía alcance Actualización de Referencias Actualización nombres departamentos Incorpora punto 7 sanciones	06/09/2019
3	Actualiza a norma ISO 27001:2023	23/04/2025

La Seguridad de la Información y la Transformación Digital del FOSIS son tareas de todas y todos 



ANÓTESE, COMUNÍQUESE Y PUBLÍQUESE.

**NICOLAS NAVARRETE HERNANDEZ
DIRECTOR EJECUTIVO
FONDO DE SOLIDARIDAD E INVERSIÓN SOCIAL**

NNH/PMD/CSG/RVC/FMZ/MLR

ANEXOS: SI CORRESPONDE

DISTRIBUCIÓN

DISTRIBUCIÓN.

1. SUBDIRECCIÓN DE USUARIOS. POLITICA-SSI-A-7.7
2. SUBDIRECTORES
3. DIRECTORES REGIONALES
4. JEFES DE DEPARTAMENTO
5. COMUNICACIONES INTERNAS
6. OFICINA DE PARTES.

Fecha de Emisión: 2025-05-19 (16:18)

Válido
indefinidamente

Código Verificación:



Nicolas Navarrete Hernandez
Director Ejecutivo
FOSIS

Documento firmado con FIRMAGOB

Verifique la validez de este documento escaneando el código QR.