



**RESOLUCION EXENTA N° FC-F-00318**  
**MAT: APRUEBA POLÍTICA PARA USO**  
**DE DISPOSITIVOS MÓVILES.**  
**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° 20.530, que crea el Ministerio de Desarrollo Social; Ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado; Ley N° 18.575 de Bases Generales de Administración del Estado; Ley 21.722 de Presupuesto para el año 2025; la Resolución N° 36 de 2025 que fija Normas sobre Exención del Trámite de Toma de Razón 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; 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, los que deberán coordinarse con los que realicen otras reparticiones del Estado.
2. Que, el Memorandum FC.MEM. 00186-2025, de fecha 14 de abril de 2025, enviado por doña Roxana Vercoutere Carter, encargada de Ciberseguridad del FOSIS, en el que solicita formalizar la aprobación de POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES, política-SSI-A-8.1, Versión 3, del 14 de abril de 2025.
3. Que, El objetivo de esta política es Proteger la información contra riesgos introducidos por uso de dispositivos terminales del/la usuario/a y la información almacenada, procesada o accesible a través de los dispositivos.
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, es necesario dictar un acto administrativo aprobatorio del procedimiento referido y sus anexos.

**RESUELVO:**

APRUEBASE la POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES, política-SSI-A-8.1, Versión 3, del 14 de abril de 2025.



	<b>POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES</b>	Fecha emisión: 17/11/2017
	<b>POLÍTICA-SSI-A-8.1</b>	Versión: 3
		Fecha versión: 14/04/2025

**1. OBJETIVO**

Proteger la información contra riesgos introducidos por uso de dispositivos terminales del/la usuario/a y la información almacenada, procesada o accesible a través de los dispositivos.

**2. ALCANCE**

Esta política se aplica a todos los y las funcionarios/as, servidores públicos a honorarios y terceras partes que presten servicios al FOSIS y que en el desarrollo de sus funciones utilicen dispositivos móviles de almacenamiento conectable por puerto USB, Bluetooth u otro medio, debidamente autorizados por FOSIS, tales como discos externos, grabador portátil CD/DVD/BlueRayj tarjetas de memoria portables, pendrive, Tablet, celulares u otro incluyendo el uso de Notebook.

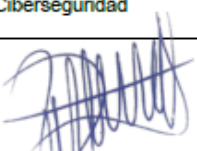

Esta política también está dentro del alcance de la norma NCH-ISO 27001:2023 control 8.1 Dispositivos terminales de usuario/a.

**3. DOCUMENTOS RELACIONADOS**

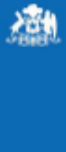
- [Política general de seguridad de la información del Fondo de Solidaridad e Inversión Social FOSIS, vigente, sus políticas, procedimientos e instructivos.](#)
- [NCh-ISO 27001:2023 Seguridad de la Información, Ciberseguridad y protección de la privacidad – Sistema de gestión de Seguridad de la Información- 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
Subdirector/a de Administración Finanzas	- Adquirir los dispositivos móviles autorizados a utilizar por los usuarios,
Jefe/a Departamento de Tecnologías de la Información y Telecomunicaciones	- Definir la configuración de seguridad estándar para los dispositivos móviles. - Efectuar la revisión de los dispositivos móviles que se van a conectar a la red del FOSIS, - Monitorear los dispositivos móviles autorizados a los usuarios que utilizan la red institucional. - Adoptar las medidas necesarias para impedir las violaciones de esta política. - Evaluar, definir y autorizar tanto el uso como la adquisición de dispositivos móviles en el FOSIS.

Elaborado por: Roxana Vercoutere Carter Encargada Ciberseguridad	Aprobado por: Cristian Salomó González Encargado de Seguridad de la Información Subdirector de Usuarios
	
Fecha: 14/04/2025	Fecha: 14/04/2025
Documento Impreso – Copia no controlada sin timbre original	



	<b>POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES</b>
	<b>POLÍTICA-SSI-A-8.1</b>

ROL	RESPONSABILIDAD
Mesa de ayuda	<ul style="list-style-type: none"> <li>- Recoger los informes de fallas de los dispositivos móviles.</li> <li>- Derivar la información de falla a los especialistas adecuados, para su solución.</li> <li>- Registrar cada uno de los reportes de fallas, desde su información hasta el cierre.</li> </ul>
Funcionarios/as de planta, contrata, honorarios y prestadores de servicios	<ul style="list-style-type: none"> <li>- Utilizar correctamente los dispositivos móviles asignados, informando oportunamente cualquier falla o deterioro,</li> <li>- Administrar los datos contenidos en el dispositivo móvil a su cargo, manteniendo el debido resguardo.</li> <li>- Usar de la mejor manera los dispositivos removibles, procurar la protección de los datos institucionales.</li> </ul>
Encargado/a de inventario	<ul style="list-style-type: none"> <li>- Mantener registro actualizado de los dispositivos móviles</li> </ul>

## 5. POLÍTICA

### 5.1. Condiciones de Seguridad

Se prohíbe el uso de dispositivos de almacenamiento removibles conectados a puertos USB, sean estos discos externos, celulares, cámaras u otros afines. Se exceptúan aquellos dispositivos necesarios para la operación, como los son mouse, teclados e impresoras que únicamente posean puerto USB como mecanismo de conexión a la red y también equipos que mediante una solicitud a la mesa de ayuda se autorice su acceso.

En caso de que un usuario/a considere necesario conectar otro dispositivo, debe solicitar autorización al jefe/a Departamento de Tecnologías de la Información y Telecomunicaciones; de ser autorizado su uso, el dispositivo será escaneado automáticamente cada vez que sea conectado a un equipo de la red de FOSIS mediante el antivirus instalado en la máquina. La información que se requiera portar debe ser almacenada en la nube virtual disponible para todos los usuarios.

Cuando los dispositivos móviles son utilizados fuera de las oficinas de FOSIS, la información contenida en estos debe permanecer cifrada mediante la herramienta BitLocker disponible en las máquinas con Windows.

En el caso de cifrado de la información, la clave debe estar debidamente resguardada, empleando un protocolo seguro, a través de la nube virtual


### 5.2. Utilización del dispositivo móvil.

El uso de un dispositivo móvil debe ser expresamente solicitado por el área usuaria, autorizado y asignado por el Departamento de Tecnologías de la Información y Telecomunicaciones.

Previo a su utilización, el dispositivo será revisado automáticamente por el antivirus, según el estándar de revisión de dispositivos móviles.

La entrega del dispositivo móvil debe ser efectuada formalmente en regiones por el encargado de informática regional y/o jefe de administración y finanzas/procesos y en el nivel central por el Departamento de Tecnologías de la Información y Telecomunicaciones



	<b>POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES</b>
	<b>POLÍTICA-SSI-A-8.1</b>

### 5.3. Manejo de dispositivo móvil por parte del/la usuario/a.

El dispositivo móvil debe estar siempre bajo la supervisión del/a usuario/a al que le fue asignado. El uso del dispositivo móvil es de exclusiva responsabilidad del/la usuario/a, el que debe tomar las medidas adecuadas para el almacenamiento y resguardo necesario, con el objetivo de evitar los riesgos de pérdida, daño o acceso no autorizado.

Cualquier incidente con el dispositivo, falla o malfuncionamiento, debe ser informado de inmediato a al Departamento de Tecnologías de la Información y Telecomunicaciones mediante la mesa de ayuda.

Todos/as los y las usuarios/as deben conocer los requisitos y procedimientos de seguridad para la protección de dispositivos de los/as usuarios/as, así como sus responsabilidades en la aplicación de dichas medidas de seguridad.

Se instruye a los/as usuarios/as que:

- a) cerrar las sesiones activas y terminar los servicios cuando ya no sean necesarios;
- b) proteger dispositivos terminales de los usuarios del uso no autorizado con un control físico (por ejemplo, bloqueo con llave o cerraduras especiales) y un control lógico (por ejemplo, acceso con contraseña) cuando no se utilicen; no dejar desatendidos dispositivos que transportan información importante, sensible o crítica para el FOSIS;
- c) usar dispositivos con especial atención en lugares públicos, oficinas abiertas, lugares de reunión y otras zonas no protegidas (por ejemplo, evitar la lectura de información confidencial si la gente puede leer por detrás, usar filtros de pantalla de privacidad);
- d) proteger físicamente dispositivos terminales de usuarios contra robo (por ejemplo, en autos y otros medios de transporte, habitaciones de hotel, centros de conferencias y lugares de reunión).

### 5.4. Manejo de dispositivo móvil por parte de terceros.


Terceras personas no están autorizados a utilizar dispositivos móviles institucionales.

### 5.5. Uso de dispositivos personales.

Cuando se usan de dispositivos personales, además de orientaciones dadas en este control, se debe considerar lo siguiente:

- a) separación del uso personal y profesional de dispositivos, incluyendo el uso de software para apoyar dicha separación y proteger los datos profesionales en un dispositivo privado;
- b) proporcionar acceso a información de FOSIS solo después que los usuarios hayan reconocido sus obligaciones (protección física, actualización de "software", otro), renunciando a la propiedad de datos de la FOSIS, permitiendo el borrado remoto de datos por parte de FOSIS en caso de robo o pérdida del dispositivo o cuando ya no se esté autorizado a usar el servicio. En estos casos, se debe tener en cuenta la legislación de protección de la información personal;
- c) evitar conflictos relativos a los derechos de propiedad intelectual desarrollados en equipos de propiedad privada políticas y procedimientos específicos del tema;
- d) acceder a equipos de propiedad privada (para verificar la seguridad de la máquina o investigación), que puede ser impedido por la legislación;



	<b>POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES</b>
	<b>POLÍTICA-SSI-A-8.1</b>

**5.6. Conexiones inalámbricas.**

FOSIS establece protocolos para:

- a) la configuración de las conexiones inalámbricas en los dispositivos desactivando los protocolos vulnerables;
- b) la utilización de conexiones inalámbricas o por cable con un ancho de banda adecuado de acuerdo con políticas específicas del tema (por ejemplo, porque se necesitan copias de seguridad o actualizaciones de "software").

**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 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 debe ser revisada a lo menos cada dos años o cuando ocurran cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad

**9. CONTROL DE VERSIONES**

Versión	Fecha de Aprobación	Motivo del Cambio
1	17/11/2017	Publicación difusión
2	11/09/2019	Actualizar referencia a la política general de seguridad de la información. Actualizar los documentos de referencia. Incorporar rol de Mesa de ayuda. Adecuarlas responsabilidades de los encargados de informática regionales
3	14/04/2025	Actualiza a normativa vigente



**ANÓTESE, COMUNÍQUESE Y PUBLÍQUESE.**

---

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

**NNH/PMD/CSG/RVC/JDG/GRV/FMZ/JSU**

**ANEXOS: SI CORRESPONDE**

**DISTRIBUCIÓN**

- OFICINA DE PARTES
- DIRECTORES REGIONALES
- SUBDIRECTORES
- JEFES DE DEPARTAMENTO
- DIRECCIÓN EJECUTIVA

Fecha de Emisión: 2025-05-19 (12:23)

Válido  
indefinidamente

Código Verificación:



Nicolas Navarrete Hernandez  
Director Ejecutivo  
FOSIS

**Documento firmado con FIRMAGOB**

Verifique la validez de este documento escaneando el código QR.