RESOLUCION EXENTA Nº FC-F-00812
MAT: APRUEBA POLITICA DE CONTROL DE ACCESO POLITICA-SSI-A-5.15.
SANTIAGO, 2025-12-10

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 Nº 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. 00576-2025 de fecha 02 de diciembre de 2025, enviado por doña Roxana Vercouter Carter, encargada de Ciberseguridad, en el que solicita formalizar mediante un acto administrativo la aprobación de la POLITICA DE CONTROL DE ACCESO, POLITICA-SSI-A-5.15. versión 6 de fecha 01 de diciembre de 2025.
3°.- Que, resulta conveniente establecer mediante una política las medidas para controlar y limitar el acceso a la información, a sus instalaciones de procesamiento de datos e información (Datacenter) y a los procesos implementados con plataforma tecnológica controlada por esta unidad, los cuales deben ser administrados sobre la base de los requisitos de eficiencia, eficacia, ciberseguridad y los que dispone la Ley vigente.
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:

C1.- APRUEBASE la POLITICA DE CONTROL DE ACCESO, POLITICA-SSI-A-5.15. versión 6 de fecha 01 de diciembre de 2025, cuyo texto es el siguiente:

1. OBJETIVO

1.1. Objetivo General

FOSIS, a través de su Comité de Seguridad de la Información **y ciberseguridad**, presenta en este documento la Política de Control de Acceso a las instalaciones físicas y tecnológicas institucionales, **adoptando los principios de Cero Confianza (Zero Trust) para proteger sus activos de información mediante una verificación continua y el principio de menor privilegio.**

Con esta Política, FOSIS, se compromete, a proteger sus activos de información, estableciendo una adecuada gestión del riesgo informático, asegurando el cumplimiento de los requisitos legales, junto a la racionalización del uso de los recursos.

El Departamento de **Tecnologías de la Información y Telecomunicaciones** establece como Política de Control a las medidas para controlar y limitar el acceso a la información, a sus instalaciones de procesamiento de datos e información (Datacenter) y a los procesos implementados con plataforma tecnológica controlada por esta unidad, los cuales deben ser administrados sobre la base de los requisitos de eficiencia, eficacia, ciberseguridad y los que dispone la Ley vigente.

El **Departamento de Tecnologías de la Información y Telecomunicaciones**, provee la plataforma tecnológica que permite a los diferentes actores en la materia, administrar el ciclo de vida de los usuarios, desde la creación de las cuentas, roles y permisos necesarios hasta su cierre por las causales que FOSIS estima necesarias.

1.2. Objetivos específicos

a) Identificar los requerimientos de seguridad de cada una de las aplicaciones.
b) Identificar toda la información relacionada con las aplicaciones.
c) Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de estaciones de trabajo.
d) Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.
e) Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados hacia la seguridad de la información en FOSIS.
f) Establecer los niveles de acceso apropiados a la información de FOSIS, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema y usuario.

2. ALCANCE

Esta política se aplica a todos los funcionarios, servidores públicos a honorarios y terceras partes que tengan derechos de acceso a la información que puedan afectar los activos de información del FOSIS y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información. **El acceso otorgado a proveedores, contratistas y otros terceros está regido por acuerdos contractuales específicos que incluirán cláusulas de seguridad de la información, requisitos de cumplimiento de esta política y la posibilidad de auditorías periódicas.**

Norma NCh-ISO 27001:2023 controles:

- **5.15 control de accesos**
- **5.18 derechos de acceso**
- **6.1 Selección**
- **6.2 Términos y condiciones de empleo**
- **7.5 responsabilidades tras el cese o cambio de empleo**

Esta política rige independientemente del lugar en el trabajador presta sus servicios a la organización, total o parcialmente, e indistintamente de la modalidad de trabajo ya sea “presencial”, “a distancia”, “remoto” u otra, en las condiciones que establezca la legislación vigente, los planteamientos de la Dirección del Trabajo o los Estados de Excepción Constitucional decretados por el Presidente de la República.

Esta política gobierna la seguridad de la información de todos los procesos estratégicos de FOSIS, establecidos en las Definiciones Estratégicas A-1, cubriendo a toda la organización independiente de su ubicación geográfica en el país.

3. DOCUMENTOS RELACIONADOS

- Política general de seguridad de la información del Fondo de Solidaridad e Inversión Social FOSIS, sus procedimientos instructivos y circulares, Vigente.
- 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.
- Decreto N° 93, de 2006, de la Secretaría General de la Presidencia: Aprueba norma técnica para minimizar la recepción de mensajes electrónicos masivos no deseados, en las casillas electrónicas de los órganos de la Administración del Estado y de sus funcionarios.
- Decreto Supremo N° 1299, Establece nuevas normas que regulan la Red de Conectividad del Estado que administra el Ministerio del Interior y fija los procedimientos, requisitos y estándares tecnológicos para la incorporación a dicha red de instituciones públicas.
- Decreto Supremo N° 5996, Crea Red Interna (INTRANET) del Estado y entrega su implementación, puesta en marcha, administración, coordinación y supervisión al Ministerio del Interior.
- Ley 20.285 regula el principio de transparencia de la función pública y el derecho de acceso a la información de los órganos de la Administración del Estado.
- Ley 19.628 de Protección de vida privada y datos.
- Ley 19.799 Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Ley 19.927 de Delitos de Pornografía Infantil.

4. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
Subdirectores Jefe de Departamento	– Definir los accesos a los datos por parte de los usuarios bajo su cargo, cuidando de mantener una adecuada segregación de funciones.
Jefe **Departamento de Tecnologías de la Información y Telecomunicaciones**	– Disponer los controles y reglas de control de acceso. – Gestionar los derechos de acceso a los medios de procesamiento de información que tenga a su cargo, según lo descrito en esta política.
Jefe de Gestión de Personas	– Solicitar acceso y bajas a sistemas de acuerdo con los requerimientos del cargo.
Funcionarios, Planta, contrata, honorarios	– Conocer y cumplir con esta política y todos los procedimientos relacionados.

5. POLÍTICA

5.1. CONTROL DE DOCUMENTOS

Todos los documentos del FOSIS deben protegerse y controlarse, el procedimiento de operación documentada, entrega las directrices para documentar todos los procesos operativos, garantizando la disponibilidad de la documentación.

Las versiones pertinentes de los documentos aplicables se encuentran disponibles para quienes lo necesiten en intranet, internet (según su pertinencia) y en el repositorio documental y son almacenados y transferidos de acuerdo con el procedimiento antes señalado.

5.2. CONTROL DE ACCESO

5.2.1. Reglas para el control de acceso

Las reglas para el control de acceso están documentadas a través de los diferentes procedimientos de los respectivos activos de información.

5.2.2. Gestión de identidades

Se debe asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información. **Para el acceso a sistemas críticos y, siempre que sea posible, para todo acceso remoto, se requerirá la implementación de autenticación multifactor (MFA/2FA) como capa adicional de seguridad.**

Existen procedimientos formales de inscripción (PR-GDP-6.1-04 Procedimiento para la contratación de cargos de planta y contrata y PR-GDP-6.1-05 Procedimiento contratación honorarios, anexo 1 ficha), y des inscripción (Procedimiento para término de la relación laboral para planta, contrata y a honorarios) de usuarios/as para otorgar y revocar el acceso a todos los sistemas y servicios de información.

El **Departamento de Tecnologías de la Información y Telecomunicaciones** implementa el control de acceso a la plataforma usuaria a partir de la identificación de funcionarios reportados por Departamento

de Gestión de Personas, en lo que se refiere a usuario de red, correo electrónico y telefonía IP. Para lo cual, se requiere conocer las altas y bajas del personal en forma oportuna.

Además de las revisiones por cambio de rol o término de contrato, se realizarán revisiones periódicas y programadas de los derechos de acceso de todos los usuarios, con especial énfasis en las cuentas privilegiadas y el acceso a sistemas críticos. Estas revisiones buscan validar la vigencia, pertinencia y el cumplimiento del principio de menor privilegio de los permisos otorgados.

El acceso de usuarios autorizados a los sistemas **es** determinado por el dueño de la información, para lo cual el **Departamento de Tecnologías de la Información y Telecomunicaciones** habilita para cada sistema un Módulo de Administración de usuarios[1].

La revisión de los derechos de acceso en caso de movilidad del funcionario de planta, contrata u honorario, se regula mediante el Procedimiento de movilidad o promoción interna de los trabajadores FOSIS.

5.2.3. Registro y Monitoreo de Eventos de Acceso

Todos los accesos a sistemas y recursos, así como los intentos de acceso (exitosos y fallidos), deben ser registrados, monitoreados y almacenados de forma centralizada. Los registros deben incluir, como mínimo, la identidad del usuario, la fecha y hora, el sistema o recurso accedido, el tipo de operación realizada y la dirección IP de origen. Dichos registros serán retenidos conforme a los requisitos legales y las políticas internas de retención de información, siendo utilizados para la detección de incidentes de seguridad, análisis forense y auditorías.

5.2.4. Responsabilidad de los usuarios

Todos los funcionarios o terceros que tengan acceso a los activos de información del FOSIS deben conocer y cumplir con el uso de esta política específica y toda la normativa vigente[2], donde se dictan pautas sobre derechos y deberes con respecto al uso adecuado de los activos de información.

5.2.5. Control de Acceso a la Red institucional

Las conexiones no seguras a los servicios de red pueden afectar a toda la institución, por lo tanto, se controla el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios no comprometan la seguridad de estos.

Las reglas de acceso a la red a través de los puertos están basadas en la premisa “todo está restringido, a menos que este expresamente permitido”.

5.2.5.1. Procedimientos para la utilización de los servicios de red

El Departamento de Tecnologías de la Información y Telecomunicaciones, debe establecer procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenden:

- El control del acceso a los servicios de red tanto internos como externos.
- La identificación de las redes y servicios de red a los cuales se permite el acceso.

---

[1] **Los dueños de sistemas se encuentran registrados en el inventario de sistemas.**

[2] Ver toda la normativa disponible en intranet

- La aplicación de normas y procedimientos de autorización de acceso entre redes.

5.2.5.2. Autenticación de usuarios para conexiones externas

El **Departamento de Tecnologías de la Información y Telecomunicaciones** contempla como servicios de conexiones externas SSL, VPN y primarios para funcionarios cualquiera sea su calidad (planta, contrata y honorarios), que requieran conexión remota a la red de datos institucional. Este servicio también puede ser accedido a proveedores con expresa autorización de un funcionario responsable de este acceso. Para las conexiones externas es necesario seguir las instrucciones de la política para el trabajo remoto. **Se priorizará la implementación de autenticación multifactor (MFA/2FA) para todas las conexiones externas a la red institucional**

5.2.5.3. Identificación de equipos en la Red

El **Departamento de Tecnologías de la Información y Telecomunicaciones** controla e identifica los equipos conectados a su red, mediante el uso de controladores de dominio, asignación manual de rango de IP, clave de seguridad para la conexión WIFI. Además, identifica los equipos de acuerdo con el nombre de usuario asignado como el siguiente modelo ejemplo: fc_rvercoutere, para identificar la región y el usuario responsable del equipo.

5.2.5.4. Protección de los puertos de configuración y diagnóstico remoto

Los puertos que permitan realizar mantenimiento y soporte remoto a los equipos de red, servidores y equipos de usuario final, está restringido a los administradores de red o servidores.

Los usuarios finales de toda la institución deben permitir tomar el control remoto de sus equipos para el Departamento de Tecnologías de la Información y Telecomunicaciones, teniendo en cuenta no tener archivos con información sensible a la vista ni desatender el equipo mientras que se tenga el control del equipo por un tercero[3].

5.2.5.5. Separación de redes

El Departamento de Tecnologías de la Información y Telecomunicaciones utiliza dispositivos de seguridad —firewalls, para controlar el acceso de una red a otra.
La segmentación se realiza en equipos de enrutamiento mediante la configuración de lista de control de acceso y configuraciones de VLAN en los equipos de comunicaciones layer 3 de acuerdo con el Procedimiento para la segregación de redes.

5.2.5.6. Control de conexión de las redes

La seguridad para las conexiones WiFi es WPA2 o superior.
Dentro de la red de datos institucional se restringe el acceso a:

- Servicios de escritorio remoto a través de internet.
- Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de esta.

5.2.5.7. Control de enrutamiento de red

El Departamento de Tecnologías de la Información y Telecomunicaciones provee a través de sus ISP (Proveedor de Servicio de Internet) el servicio de internet institucional y es el único servicio de internet autorizado.

El uso de internet está regulado por perfilamiento de navegación definido en la institución.

---

[3] **Ver política de pantallas y escritorios limpios en intranet**

5.2.6.Control de Acceso al Sistema Operativo

5.2.6.1. Registro de inicio seguro

El acceso a los sistemas operativos está regulado por el procedimiento de inicio de sesión segura.

5.2.6.2. Gestión de contraseñas

La asignación de contraseñas se controla a través del procedimiento para la administración de contraseñas

5.2.6.3. Uso de utilitarios del sistema

El uso de utilitarios licenciados del sistema está restringido a usuarios administradores.

En el controlador de dominio, se define una política que no permite la instalación de software y cambios de configuración del sistema. Ningún usuario final tiene privilegios de usuario administrador.

Todo software que se utilice en la institución debe cumplir con los licenciamientos correspondientes del proveedor y contratos de mantención de al menos las actualizaciones de solución de problemas de seguridad. Los equipos computacionales contemplan una instalación de software estándar descrito en la normativa de Utilización de equipos personales e Instalación legal de software publicadas en la Intranet. En estas, se establece una política a nivel de controlador de dominio o sistema equivalente para la gestión centralizada de autenticación e identidad, que no permite la instalación de software y cambios de configuración del sistema, salvo que se trate de personal autorizado del Departamento de Tecnologías de la Información y Telecomunicaciones.

Ningún usuario final, debe tener privilegios de usuario administrador en ningún equipo o dispositivo.

5.2.6.4. Limitación de tiempo de conexión

El Departamento de Tecnologías de la Información y Telecomunicaciones, no limita el tiempo de conexión, ni establece restricciones en la jornada laboral.

5.2.6.5. Control de acceso a la información

El Departamento de Tecnologías de la Información y Telecomunicaciones, identifica según los niveles de clasificación de información[4] cuáles sistemas considera sensibles y que deben gestionarse desde ambientes tecnológicos aislados e independientes.

5.2.7.Computación Móvil y Trabajo Remoto[5]

Teniendo en cuenta las ventajas de la computación móvil y el trabajo remoto, así mismo el nivel de exposición a amenazas que pongan en riesgo la seguridad de la información institucional, a continuación, se establecen directrices que permiten regular el uso de la computación móvil y trabajo remoto.

[4] Ver procedimiento para la gestión de activos de información

[5] Ver política para el trabajo remoto

5.2.7.1. Computación y comunicaciones móviles[6]

Se entiende como dispositivos de cómputo y comunicación móviles institucionales, todos aquellos que permitan tener acceso y almacenar información institucional, desde lugares diferentes a las instalaciones.

El uso de equipos de cómputo y dispositivos de almacenamiento móviles está restringido únicamente a los provistos por la institución y contempla las siguientes directrices:

- Uso de usuario y contraseña para acceso al mismo.
- Uso de software antivirus provisto por el **Departamento de Tecnologías de la Información y Telecomunicaciones.**
- Restricción de privilegios administrativos para los usuarios.
- Uso de software licenciado y provisto por **el Departamento de Tecnologías de la Información y Telecomunicaciones.**
- Realización de copias de seguridad periódicas.
- Permanecer siempre cerca del dispositivo.
- No dejar desatendidos los equipos.
- No llamar la atención al portar equipos móviles.
- No identificar el dispositivo con distintivos del **Departamento de Tecnologías de la Información y Telecomunicaciones.**
- No colocar datos de contacto técnico en el dispositivo.
- Mantener cifrada la información clasificada de acuerdo con la política de gestión de claves.
- No conectarse a redes WIFI-públicas.
- Mantener apagado el Bluetooth o cualquier otra tecnología inalámbrica que exista o llegara a existir.
- Informar de inmediato al **Departamento de Tecnologías de la Información y Telecomunicaciones**, sobre la pérdida o hurto del dispositivo para proceder al bloqueo del usuario.
- Para dispositivos de comunicación móvil (telefonía celular) institucionales se aplicarán los controles antes mencionados y los detallados a continuación:
    - Activar la clave del teléfono, para acceso a la agenda telefónica, mensajes de texto, llamadas entrantes, salientes, perdidas. Archivos de voz, imagen y videos.
    - No hablar de temas confidenciales cerca de personas que no requieran conocer dicha información.

5.2.7.2. Trabajo remoto

Teniendo en cuenta las ventajas de la computación móvil y el trabajo remoto, como así mismo, el nivel de exposición a amenazas que pongan en riesgo la seguridad de la información institucional al utilizar estos medios, se establecen directrices orientadas a regular el uso de la computación móvil y trabajo remoto a través de la política para el trabajo remoto[7] y que son de responsabilidad de los funcionarios usuarios de la plataforma institucional.

5.2.7.3. Tiempo de inactividad de la sesión

Después de cinco (5) minutos de inactividad del sistema, se considerará tiempo muerto y se bloqueará la sesión automáticamente, sin cerrar las aplicaciones que se encuentren abiertas.

---

[6] Ver también: Política de uso de dispositivos móviles, Política de trabajo remoto

[7] Política para el trabajo remoto.

Los usuarios deben bloquear sus sesiones, cuando abandonen temporalmente su puesto de trabajo (Tecla Windows + L) y apagar los equipos al finalizar la jornada laboral o cuando se ausenten por más de dos (2) horas.

Téngase presente que si se están desarrollando trabajos remotos que requieran el acceso al equipo, éste podrá quedar encendido, pero debidamente bloqueado su acceso.

5.2.7.4. Sesiones en múltiples dispositivos

Los sistemas WEB del FOSIS permiten el acceso desde múltiples dispositivos simultáneamente.

Para asegurar un adecuado control de sesiones, es imperativo que los usuarios mantengan activa únicamente una sesión a la vez. Por tanto, se requiere que los usuarios cierren sesión en el dispositivo que dejan de utilizar, garantizando así un uso responsable de los recursos.

5.2.7.5. Alistamiento de sistemas sensibles

El Departamento de Tecnologías de la Información y Telecomunicaciones identifica según los niveles de clasificación de información, o por definición legal, o a requerimiento de otra unidad debidamente fundado, cuáles son los sistemas sensibles y que deben gestionarse desde ambientes tecnológicos aislados e independientes, con requerimientos de seguridad de la información robustos y resilientes, propios del tratamiento de infraestructura crítica o equipamiento de misión crítica.

Al aislar estos sistemas, se prevé que el intercambio de la información con otras fuentes de datos sea seguro, ya que no se permite duplicar información en otros sistemas, siguiendo las directrices de fuentes únicas de datos.

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

9. TABLA DE MODIFICACIONES

Versión	Fecha de Aprobación	Motivo del Cambio
1	17/11/2017	Puesta en marcha de la política
2	06/09/2019	Actualiza logo Actualiza objetivo y alcance Actualiza normativa (Res. Política general de seguridad de la información) Actualiza Roles y responsabilidades (Jefe TIC, ahora Jefe de Soporte y Operaciones TIC)
3	29/11/2021	Actualiza cargo jefe de informática y telecomunicaciones Actualiza normativa vigente
4	29/06/2022	Actualiza ítems 5.1, 5.4.2.4
5	19/06/2023	Actualiza objetivo Actualiza alcance Agrega ítems 5.2.6.3 y 5.2.6.4
6	**01/12/2025**	**Actualiza normativa vigente** **Actualización de controles de acceso: inclusión de MFA, revisión periódica, monitoreo de eventos, principios Zero Trust, gestión de terceros y referencia a clasificación de información. |**

ANOTESE, COMUNIQUESE Y PUBLIQUESE.

_____

NICOLAS NAVARRETE HERNANDEZ
DIRECTOR EJECUTIVO
FONDO DE SOLIDARIDAD E INVERSIÓN SOCIAL

ANEXOS: MEMORANDUM FC.MEM. 00576-2025, POLITICA DE CONTROL DE ACCESO PDF FIRMADO.

VISADORES:
Marco Antonio Leal Ruiz
Francisco Andrés Molina Zapata
Roxana Vercoutere Carter
Jaime Gonzalez Salazar
Pablo Alfonso Meza Donoso

DISTRIBUCIÓN EXTERNA:
1.- Subdirección de Usuarios. POLITICA-SSI-A.5.15.
2.- Oficina de Partes.

Fecha de Emisión: 2025-12-10 (13:01)

Válido indefinidamente

Código Verificación:

DOCUMENTO FIRMADO ELECTRÓNICAMENTE
FOSIS

Nicolas Navarrete Hernandez
Director Ejecutivo
FOSIS

Documento firmado con FIRMAGOB
Verifique la validez de este documento escaneando el código QR.