



RESOLUCION N° 048
MAT.: APRUEBA POLITICA DE SEGURIDAD DE LA
INFORMACIÓN PARA LAS RELACIONES CON EL
PROVEEDOR.

SANTIAGO, 14-04-2025

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 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 Memorandum FC.MEM. 00160-2025 de fecha 03 de abril de 2025, enviado por doña Roxana Vercouter Carter, encargada de Ciberseguridad, en el que solicita formalizar mediante un acto administrativo la aprobación de la Política de seguridad de la información para las relaciones con el proveedor POLITICA 5.19 versión 4 de fecha 12 de febrero de 2025.
- 3.- Que procede asegurar la protección de los activos del FOSIS a los que tienen acceso de los proveedores y mantener un nivel acordado de seguridad de la información y entrega del servicio, en línea con los acuerdos del proveedor.
- 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 Política de seguridad de la información para las relaciones con el proveedor POLITICA-5.19 versión 4 de fecha 12 de febrero de 2025, cuyo texto es el siguiente:

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON EL PROVEEDOR	Fecha emisión: 23/09/2019
		Versión: 4
	POLÍTICA 5.19	Fecha versión: 12/02/2025

1. OBJETIVO

Asegurar la protección de los activos del FOSIS a los que tienen acceso los proveedores y mantener un nivel acordado de seguridad de la información y entrega del servicio, en línea con los acuerdos del proveedor.

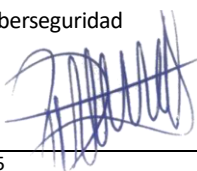

2. ALCANCE


Esta política se aplica a todos los empleados, contratistas y terceros involucrados en las actividades del FOSIS. Incorpora los siguientes controles de la **NCH-ISO 27001:2023**:

- **5.19 Seguridad de la Información en las relaciones con el proveedor**
- **5.20 Abordar la seguridad en los acuerdos con el proveedor.**
- **5.21 Gestión de la seguridad de la información en la Cadena de suministros de tecnologías de la información y comunicación (TIC)**
- **5.22 Seguimiento, revisión y gestión de cambios a los servicios del proveedor**
- **5.23 Seguridad de la información para el uso de servicios en la nube**

3. DOCUMENTOS RELACIONADOS

- [Ley 19.886 de compras públicas y reglamento de bases sobre contratos administrativos de suministro y prestaciones de servicios.](#)
- [Ley 19.628 sobre protección de la vida privada, Ministerio Secretaría General de la Presidencia.](#)
- [Ley 20.285 sobre acceso a la información pública, Ministerio Secretaría General de la Presidencia.](#)
- [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](#)


Elaborado por:	Revisado y Aprobado por:
Roxana Vercoutere Carter Encargada de Ciberseguridad 	Cristian Salomó González Encargado de Seguridad de la Información Subdirector de Usuarios 
Fecha: 12/02/2025	Fecha:
Documento Impreso – Copia no controlada sin timbre original	

 <p>FOSIS Ministerio de Desarrollo Social y Familia</p> <p>Gobierno de Chile</p>	<p>POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON EL PROVEEDOR</p>
	<p>POLÍTICA 5.19</p>

4. ROLES Y RESPONSABILIDADES

ROL	Responsabilidad
Encargado(a) de Seguridad de la Información	Supervisa el cumplimiento de las políticas.
Proveedores, colaboradores y/o Personal externo que presta servicios al FOSIS	Dar estricto cumplimiento a las normas de seguridad descritas en la presente política y en la documentación de seguridad de la información, sin perjuicio de las obligaciones adicionales que se establezcan en su contrato según corresponda a su naturaleza.
Funcionarios(as), planta, contrata, honorarios	Dar cumplimiento estricto de la política y documentación relativa al comportamiento y acceso a los sistemas e información en función del tipo de proveedor y el nivel de acceso. Debe cumplir con todas las políticas y estándares de seguridad de la información del FOSIS.
Encargado(a) Ciberseguridad	Gestiona los incidentes de seguridad de la información relacionados con el incumplimiento de las políticas
Jefe(a) de Tecnologías de la Información y Telecomunicaciones	Asesora a los encargados de compras o gestores del contrato o proyecto sobre los niveles de servicio requeridos para la protección de la seguridad de la información. Incluye cláusulas contractuales relativas a la seguridad de la información y la propiedad intelectual. Cuando corresponda en la formulación de la solicitud de servicios externos debe incorporar los requisitos de seguridad asociados al proceso que se pueden ver afectados. Posteriormente, en el desarrollo de la prestación del servicio debe velar por el cumplimiento de las cláusulas asociadas a materias de seguridad de la información.
Fiscal	Incorporar en las bases y en contratos las cláusulas sobre seguridad de la información y propiedad intelectual pertinentes a la naturaleza del contrato
Unidad de Compras	En la revisión de los requerimientos de compra y posterior elaboración de contrato debe velar porque los requisitos de seguridad se encuentren explicitados en la documentación, además de notificar al proveedor.



	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON EL PROVEEDOR
	POLÍTICA 5.19

5. POLÍTICA

5.1 Prestación de servicios en FOSIS

El FOSIS prioriza la disponibilidad continua del servicio. Los criterios para priorizar incluyen niveles de servicio, tiempos de respuesta y tiempos de resolución. El departamento solicitante es el responsable, con el apoyo del Departamento de Tecnologías de la Información (TI). Los planes de contingencia deben abordar la disponibilidad del servicio y los datos. El Departamento de TI supervisa la disponibilidad del servicio y gestiona de forma proactiva los incidentes que afectan a la disponibilidad.

Quando se requiere elaborar un contrato particular con proveedores que tienen relación con servicios de tratamiento, manipulación, transmisión o almacenamiento de activos de información, ya sea en formato físico o digital, se deben incorporar cláusulas de seguridad de la información que permitan garantizar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información, tales como: acuerdos de niveles de servicios (SLA), derechos de auditar los procesos involucrados, procedimientos aplicados frente a incidentes de seguridad, cláusulas de confidencialidad y no divulgación de información, como también la extensión de dichos deberes a empresas subcontratadas.

Para efectos de velar por la aplicación de cláusulas de seguridad de la información en los contratos, bases de licitación, tratos directos, actos administrativos o cualquier otro documento formal relacionado a la contratación de servicios de proveedores, es responsabilidad de la persona que cumpla la función de Gestor de Contratos aplicar las modificaciones respectivas a los documentos administrados y elaborados al interior de la Institución con respecto a dicha materia.¹

5.2 Confidencialidad de la información²

Los proveedores que acceden a la información del FOSIS deben firmar acuerdos de confidencialidad. Los acuerdos especifican las responsabilidades, la información cubierta, las medidas de seguridad, los procedimientos de respuesta a incidentes, las extensiones de terceros, la propiedad, los plazos, las sanciones por incumplimiento y la aceptación. Cada departamento del FOSIS solicitante es responsable de estos acuerdos; la estandarización y el almacenamiento seguro son responsabilidad de la Fiscalía del FOSIS.

5.3 Propiedad Intelectual


Todos los proveedores deben cumplir con la política de propiedad intelectual del FOSIS (disponible en el sitio web del FOSIS).

5.4 Intercambio de Información

Las transferencias de datos (electrónicas o físicas) que requieran información personal deben ser realizadas por personal autorizado y con el debido permiso, siguiendo la Ley

¹ Ver instructivo de seguridad de la información para la gestión de proyectos

² Ver política de datos para la privacidad y protección de la información

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON EL PROVEEDOR
	POLÍTICA 5.19

19.628 y las políticas de seguridad del FOSIS pertinentes³. Se deben utilizar las medidas de seguridad adecuadas.

El uso de estos datos debe establecerse en el contrato, y ser autorizado por la autoridad que lo suscribe.

La transmisión de datos de carácter personal, a través de redes de telecomunicaciones se debe realizar cifrando dichos datos o bien utilizando cualquier otro mecanismo autorizado por el **Jefe de TIC** que garantice que la información no sea ininteligible ni manipulada por terceros no autorizados⁴.

En general, debe seguirse lo indicado en la Política para el uso de controles criptográficos y gestión de claves, disponible en la página web del FOSIS.

5.5 Uso apropiado de los recursos informáticos, datos, software, redes, sistemas de comunicación, etc.

El personal externo solo puede utilizar los recursos informáticos proporcionados para las tareas asignadas. El FOSIS se reserva el derecho de monitorear y auditar el uso de los recursos. Los archivos almacenados en la red o en los dispositivos conectados deben cumplir con las políticas de seguridad del FOSIS (incluida la propiedad intelectual, la protección de datos y el antimalware). Los proveedores también deben seguir las políticas generales de seguridad del FOSIS.

5.6 Gestión de equipamiento “Hardware”

Los proveedores son responsables de administrar el equipo proporcionado por el FOSIS: mantener un inventario actualizado, solicitar autorización para reasignaciones (incluido el borrado seguro de datos antes de la transferencia), y devolver todo el equipo al finalizar el contrato.


5.7 Cadena de suministros de tecnologías de la información y comunicaciones

Los acuerdos con los proveedores deben abordar los riesgos de seguridad de la información dentro de la cadena de **cualquier suministro que mantenga información**. Esto incluye:

- Implementar las mejores prácticas de seguridad en toda la cadena de suministro
- Monitorear y validar que los servicios y productos cumplan con los requisitos de seguridad
- Identificación de componentes críticos que requieren un control mejorado
- Garantizar que los servicios y productos funcionen como se espera
- Gestión del ciclo de vida de las TIC y los riesgos asociados

³ Ver Política de seguridad en las telecomunicaciones, política de datos para la privacidad y protección de la información

⁴ Política para uso de controles criptográficos y gestión de claves

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON EL PROVEEDOR
	POLÍTICA 5.19

5.7.1 Gestión de la cadena de suministros TIC

Abordar la seguridad de la información en la cadena de suministro de las TIC implica:

- Definición de requisitos de seguridad para adquisiciones⁵
- Exigir a los proveedores que propaguen los requisitos de seguridad a los subcontratistas
- Exigir a los proveedores de productos que aborden las prácticas de seguridad dentro de su cadena de suministro
- Obtención de información sobre los componentes del software
- Obtener información sobre las funciones y configuraciones de seguridad implementadas
- Validar el cumplimiento de la seguridad a través de métodos como pruebas de penetración y certificaciones de seguridad de terceros.
- Identificación y documentación de componentes críticos
- Garantizar la trazabilidad de los componentes
- Garantizar la funcionalidad del producto
- Verificación de la autenticidad mediante métodos tales como etiquetas anti-manipulación y hashes criptográficos
- Establecer procedimientos de intercambio de información
- Gestión del ciclo de vida de los componentes de las TIC y de los riesgos de seguridad relacionados.

5.8 Gestión de cambios a los servicios del proveedor, monitoreo y revisión


Se deben **supervisar, revisar, evaluar y gestionar regularmente los cambios en prácticas o de seguridad de información de proveedores y la prestación de servicios.**

Revisar y gestionar periódicamente los cambios en las prácticas de los proveedores y la prestación de servicios. El proceso debe incluir:

- Monitoreo del rendimiento del servicio
- Gestión de cambios en los servicios (mejoras, nuevas aplicaciones, actualizaciones de políticas, resolución de incidencias)
- Monitoreo de cambios en los servicios del proveedor (cambios en la red, actualizaciones tecnológicas, etc.)
- Revisión de informes de servicio
- Celebración de reuniones periódicas
- Realización de auditorías (incluidas auditorías independientes cuando estén disponibles)
- Informes sobre incidentes de seguridad
- Respuesta y gestión de incidencias
- Abordaje de vulnerabilidades
- Asegurar que el proveedor mantenga una adecuada capacidad de servicio y planificación de continuidad.

5.9 Seguridad de la Información para uso de servicios en la nube

⁵ [Ver manual de procedimiento de adquisiciones, del sistema de compras y contrataciones públicas del FOSIS](#)

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON EL PROVEEDOR
	POLÍTICA 5.19

El FOSIS establece políticas específicas sobre uso de servicios en la nube a todas las partes interesadas establecidas en el contrato. La gestión de riesgos está a cargo del departamento de TI. La responsabilidad es compartida, y en el contrato – o instrumento que establezca los términos del servicio - se especifica:

- Requisitos de seguridad
- Criterios de selección
- Responsabilidades
- Funciones de seguridad controladas
- Acceso a capacidades de seguridad
- Controles de seguridad aplicados
- Procedimientos de gestión de incidencias
- Procesos de seguimiento y revisión

6. DIFUSIÓN

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

- Publicación en la intranet del FOSIS
- Correo informativo.
- Publicación en la página web del FOSIS.

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 FOSIS⁶.

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	30/09/2019	Primera versión política
2	06/12/2019	Incorpora responsabilidad del Fiscal y del encargado de seguridad de la información

⁶. Circular que Imparte instrucciones sobre observancia de la política de seguridad de la información del FOSIS

	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON EL PROVEEDOR
	POLÍTICA 5.19

Versión	Fecha de Aprobación	Motivo del Cambio
3	17/08/2020	<ul style="list-style-type: none"> - Actualiza objetivo - Amplía alcance - Actualiza de departamento de soporte y operaciones TIC a Departamento de Informática - Incorpora 5.7 y 5.8
4	12/02/2025	- Actualiza normativa vigente (ISO 27001:2023)

ANOTESE, COMUNIQUESE Y PUBLIQUESE.

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

Distribución.

- 1.- Subdirección de Usuarios. POLITICA 5.19
- 2.- Oficina de Partes.

Fecha de Emisión: 2025-04-14 (12:05)

Válido
indefinidamente

Código Verificación:



Nicolas Navarrete Hernandez
Director Ejecutivo
FOSIS

Documento firmado con FIRMAGOB

Verifique la validez de este documento escaneando el código QR.