FOSIS
Ministerio de Desarrollo Social y Familia

Gobierno de Chile

RESOLUCION EXENTA Nº FC-F-00757
MAT: APRUEBA NUEVA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DEL FONDO DE SOLIDARIDAD E INVERSIÓN SOCIAL.
SANTIAGO, **21-11-2023**

VISTOS:

Lo dispuesto en la Ley Nº 18.989, en particular en su Título II sobre el Fondo de Solidaridad e Inversión Social; en la Ley N° 18.575 Orgánica Constitucional de Bases Generales de la Administración del Estado; en la 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 Resolución Nº 7, de 2019 que fija Normas sobre Exención del Trámite de Toma de Razón; en el Decreto N°7 del 19 de mayo de 2023, publicado en el Diario oficial con fecha 17 de agosto de 2023 y en el Decreto Supremo N° 15, de 28 de abril de 2022, del Ministerio de Desarrollo Social y Familia que nombra a don Nicolás Navarrete Hernández en el cargo de Director Ejecutivo del Fondo de Solidaridad e Inversión Social.

CONSIDERANDO:

1. Que existe la obligación para los organismos de la Administración del Estado, de aprobar una política tendiente a resguardar los activos de información que sean manejados por cada Servicio.

2. Que, con este objeto, cada Servicio se ve en la obligación de conformar un Comité de Seguridad de la Información **y ciberseguridad,** el cual está encargado de la definición de las políticas y la verificación del cumplimiento de las normas y las buenas prácticas relacionadas con la seguridad de la información **y ciberseguridad** y de los activos de información que les pertenecen.

3. Que, en el ejercicio de sus funciones, el Comité de Seguridad de la Información **y ciberseguridad** de FOSIS ha definido la nueva política general de seguridad de la información **y ciberseguridad** que debe implementarse en el Servicio, según da cuenta el acta del referido Comité, de fecha 4 de octubre de 2023, cuya copia se adjunta.

4. Que, el Decreto N°7 del 19 de mayo de 2023, publicado en el Diario oficial con fecha 17 de agosto de 2023, que establece la Norma Técnica de seguridad de la información y ciberseguridad conforme La ley N°21.180, dispone en su artículo 3°, que los órganos de la Administración del Estado deberán generar e implementar una Política de Seguridad de la Información y Ciberseguridad.

5. Que, dicha Política debe tener como objetivo, establecer las directrices generales en materia de seguridad de la información y ciberseguridad dentro del órgano, además de velar por la seguridad de los componentes de software y hardware, de los sistemas informáticos y de los datos o información que almacenan, procesan e interoperan. Asimismo, deberá contener la visión estratégica del respectivo órgano de la Administración del Estado respecto de la seguridad de la información y ciberseguridad. Además de velar por la preservación, confidencialidad, integridad y disponibilidad de la información, considerando estándares de seguridad de la información y la privacidad como parte del diseño inicial.

6. Que, debido a lo anterior, el **Subdirector de Usuarios (S)** y encargado de seguridad de la información del FOSIS solicita, mediante memorándum N° MEM.00414, de 8 de noviembre de 2023, adjunto, la aprobación de la nueva política de seguridad de la información y ciberseguridad sancionada por el Comité de Seguridad de la información y Ciberseguridad, cuyo texto se consigna en la parte resolutiva del presente acto administrativo.

7. Que, no existiendo observaciones al texto propuesto, corresponde aprobarlo mediante el presente acto administrativo y dejar sin efecto, la anterior Política General de Seguridad de la información del FOSIS, cuya aprobación se formalizó a través de la Resolución Exenta N° FC-F-00095, de 20 de abril de 2021.

RESUELVO:

1° APRUÉBESE la nueva política general de seguridad de la información y ciberseguridad del Fondo de Solidaridad e Inversión Social, FOSIS, cuyo texto es el siguiente:

FOSIS Ministerio de Desarrollo Social y Familia – Gobierno de Chile	**POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD**	Fecha emisión: 29/09/2011 Versión: **8**
	POLÍTICA-SSI-A 5	Fecha versión: **31/10/2023**

Introducción

El Fondo de Solidaridad e Inversión Social – FOSIS-, es un servicio público, con personalidad jurídica y patrimonio propio, funcionalmente descentralizado, regulado por el título II de la Ley N.º 18.989, cuya finalidad es financiar en todo o parte planes, programas, proyectos y actividades especiales de desarrollo social, los que deberán coordinarse con los que realicen otras reparticiones del Estado.

Su 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*"**.

1. OBJETIVOS ESTRATÉGICOS DE LA ORGANIZACIÓN

Para el período, el FOSIS ha definido los siguientes objetivos estratégicos a través del formulario A-1:

- **Desarrollar estrategias de intervención inclusivas que generen oportunidades para el bienestar económico, social y territorial de personas, familias y comunidades.**
- **Instalar una instancia de pilotaje y co-diseño de programas orientados a personas y grupos de alta vulnerabilidad social, mediante un proceso de escalamiento de proyectos de innovación social, que entregue soluciones ajustadas a las necesidades programáticas del Estado.**
- **Mejorar en forma continua nuestra oferta programática con pertinencia territorial y con foco en la cohesión social, habilidades y capacidades de las poblaciones objetivo.**
- **Instalar un modelo de alianzas colaborativas, que permita la movilización de capacidades y recursos, para robustecer la respuesta a la vulnerabilidad de usuarios y usuarias.**
- **Desarrollar las capacidades necesarias para la modernización y transformación digital, teniendo como focos la interoperabilidad de datos con otros organismos del Estado, las necesidades institucionales y el mejoramiento e innovación en los servicios y programas dirigidos a usuarios y usuarias.**

De acuerdo con lo señalado, FOSIS, a través de su Comité de Seguridad de la Información y Ciberseguridad, presenta en este documento las características mínimas obligatorias de seguridad de la información y confidencialidad, integridad y disponibilidad para la organización y coordinación institucional a fin de gestionar adecuadamente la administración de la información (recopilación, procesamiento, almacenamiento y distribución) en consistencia con los principios rectores de la política general de seguridad de la información y ciberseguridad. Para los efectos de esta política, los documentos electrónicos institucionales constituyen un activo de información y son tratados de acuerdo con la relevancia institucional. Con lo cual, se compromete a todo nivel, a proteger sus activos de información, estableciendo una adecuada gestión del riesgo, asegurando cumplimiento de requisitos legales, aplicando una estrategia de seguridad basada en las mejores prácticas y controles sobre estos recursos con el fin de protegerlos de las amenazas.

El Comité de Seguridad de la Información y Ciberseguridad, sesionará mensualmente, o ante la convocatoria de algunos de sus miembros que fundadamente invoquen alguna situación de emergencia o relevante para FOSIS, con el objeto de revisar los mecanismos de gestión para la prevención de delitos y riesgos operacionales, lo que implicaría de ser necesario el desarrollo de políticas, procedimientos, guías o protocolos adicionales.

FOSIS
Ministerio de Desarrollo Social y Familia
Gobierno de Chile

1. Declaración de intención de la Dirección Ejecutiva

El FOSIS, debido a la sensibilidad de la información que maneja referente a los usuarios/as, tiene la obligación de disponer todos los medios y recursos necesarios para proteger la información que administra, y resguardar la tecnología usada para su procesamiento, estableciendo los controles que ayuden a disminuir o mitigar las amenazas internas o externas. Lo anterior, con el fin de asegurar la confidencialidad de los datos, resguardar integridad, disponibilidad, legalidad y confiabilidad de la información. Además, se busca garantizar la continuidad de los sistemas de información, para asegurar el eficiente cumplimiento de sus objetivos estratégicos.

2. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

- Promover en el FOSIS una cultura que se oriente hacia la Seguridad de la Información.
- Comprometer a todas las autoridades del FOSIS en la difusión, consolidación y cumplimiento de esta Política.
- Implementar las medidas de seguridad, en consideración a los recursos y las partidas presupuestarias disponibles.
- Mantener las políticas y procedimientos actualizados, con el fin de asegurar su vigencia y eficacia.
- Promover prácticas que aseguren la continuidad de las funciones del FOSIS, de acuerdo con lo definido en las políticas de seguridad establecida.

3. OBJETIVOS DE LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

1. Objetivos Generales

Establecer las directrices generales en materia de seguridad de la información y ciberseguridad dentro del FOSIS, además de velar por la seguridad de los componentes de software y hardware, de los sistemas informáticos y de los datos o información que almacenan, procesan e interoperan.

Velar por la preservación, confidencialidad, integridad y disponibilidad de la información, considerando estándares de seguridad de la información y la privacidad como parte del diseño inicial.

2. Objetivos Específicos

- Identificar, clasificar y asignar los activos de información de la Institución, al objeto de lograr niveles satisfactorios de integridad, confidencialidad y disponibilidad.
- Prevenir, controlar, y/o mitigar los riesgos de Seguridad de la Información y **ciberseguridad**, identificando las vulnerabilidades y amenazas que enfrentan los activos de información, con el fin de garantizar la continuidad del negocio.
- Establecer normas, políticas y procedimientos que permitan proteger los activos de información del FOSIS.
- **Establecer un marco de trabajo para las autoridades y directivos que permita controlar el funcionamiento de la seguridad de la información y ciberseguridad dentro de la organización.**
- **Asignar las responsabilidades en relación con seguridad de la información y ciberseguridad.**
- **Promover la segregación de funciones.**
- **Establecer los mecanismos de coordinación con los contactos y encargados apropiados.**
- **Promover comunicación y contactos con comunidades y grupos asociadas a la seguridad de la información para fortalecer la comunidad interna tanto técnica como profesional.**
- **Favorecer la integración de la seguridad de la información en la gestión de los proyectos institucionales, sin importar la naturaleza del proyecto.**

4. ROLES Y RESPONSABILIDADES

Asignación de Roles y Responsabilidades sobre la Seguridad de la Información y la ciberseguridad

A continuación, se detallan la autoridad y responsabilidades de quienes participan en la administración, implementación y evaluación de la Política de Seguridad de la Información y ciberseguridad en FOSIS, la que debe estar en directa relación con la orgánica y funcionalidades descritas en la constitución del Comité de Seguridad de la Información y Ciberseguridad:

Cada uno de los roles indicados a continuación es responsable de la resolución inmediata de los incidentes de seguridad que afecten sus áreas de responsabilidad.

Sin perjuicio de lo anterior, cada rol tiene las siguientes responsabilidades específicas a su cargo:

ROL	RESPONSABILIDADES
Director/a Ejecutivo/a	• Aprobar y comunicar la Política de Seguridad de la Información y Ciberseguridad. • Supervigilar que las estrategias definidas por el Comité, para el control asociado a los activos de información, estén en concordancia con las políticas institucionales de seguridad de la información y los objetivos del servicio. • Proveer los recursos necesarios para la ejecución de esta política.

ROL	RESPONSABILIDADES
Subdirectores/as **Directores Regionales**	• Apoyar y promover la Política de Seguridad de la información dentro del FOSIS, mediante la difusión, educación y concientización sobre la Políticas y otras medidas de seguridad. • Cumplir con los requerimientos que el Comité Seguridad de la Información y Ciberseguridad efectúe a las unidades. • Construir las directrices de mapas de procesos a implementar en sus unidades a cargo.
Fiscal	• Asesorar al Comité en materias jurídicas relacionadas con la implementación de la Política de Seguridad de la Información y Ciberseguridad y evaluar la legalidad de los actos que de ésta demande. • Asegurar la incorporación de los requisitos jurídicos del Sistema de Seguridad de la información y Ciberseguridad, en las diferentes celebraciones de contratos y servicios. • Efectuar el control jurídico de los actos administrativos que realizan las unidades organizacionales dependientes del FOSIS. • Revisar e informar las investigaciones internas que se instruyan por orden del Director Ejecutivo.
Jefe de Auditoría Interna	• Asesorar al Comité de Seguridad de la Información y ciberseguridad en lo relativo a las auditorías internas del Sistema de Seguridad de la Información y Ciberseguridad. • Realizar auditorías internas anuales en materias de Seguridad de la Información y ciberseguridad de acuerdo con requerimiento del Comité de Seguridad de la información y Ciberseguridad. • Proponer aspectos de mejora a los hallazgos encontrados en las auditorias e informarlas al Director/a Ejecutivo/a y al comité de Seguridad de la información y Ciberseguridad. • Realizar el seguimiento de las medidas preventivas y correctivas emanadas de los hallazgos detectados en los informes de auditoria realizados a la materia de Seguridad de la Información y ciberseguridad.
Jefes/as de Departamento o unidad	• Implementar las políticas de Seguridad de la Información. • Velar por el cumplimiento de las políticas, normativas y procedimientos por parte de sus equipos.
Jefe de Comunicaciones	• Indicar a los Encargados de comunicaciones regionales difundir la política de seguridad • Difundir los temas relevantes en materias de seguridad a terceros y entidades externas relevantes. • A través de Comunicación Interna Difundir de las políticas de seguridad de la información al interior de FOSIS. • Difundir a todo el personal FOSIS la Política de

ROL	RESPONSABILIDADES
	Seguridad de la Información y Ciberseguridad vigente
Jefe de Control de Gestión	• Realizar el monitoreo permanente de la operación de los controles del sistema de seguridad de la información y ciberseguridad.
Jefe/a de Desarrollo Organizacional	• En el proceso de Inducción Informar y notificar al personal que ingrese a FOSIS sobre sus obligaciones respecto del cumplimiento de la Política General de Seguridad de la Información y ciberseguridad y de todas las normas, procedimientos y prácticas aplicadas en la institución. • Avisar oportunamente a la Unidad responsable de Ciberseguridad en el caso de movilidad interna o traslado para la modificación de las funciones de un funcionario de planta, contrata u honorarios, para realizar un análisis de los derechos de accesos a la información actual que posee el usuario en cuestión y se retiran permisos de acceso a la información o se otorgarán nuevos derechos propios de la función asumida, según requiera su Jefatura. • Ejecutar tareas de capacitación continuas al personal de FOSIS en materias de Seguridad de la Información. • Definir y coordinar un Plan de Capacitación y Sensibilización en temas de Seguridad de la Información, el cual se estructura en base a requerimientos del encargado de seguridad.
Jefe/a de Gestión de Personas	• Informar a través de mail a la Unidad responsable de Ciberseguridad sobre el personal contratado, a efecto de protocolizar, identificar o designar el perfil de usuario del personal ingresado. • Informar una vez al mes a través de reporte ingreso o cese de funcionarios al encargado/a de Ciberseguridad acerca de creación o eliminación de cuentas de correo institucionales. • Las normas y política expresadas en esta resolución, se consideran parte integrante y se adjuntarán a las resoluciones de nombramiento o contrataciones de personal, de planta, a contrata o prestadores de servicio honorarios.
Jefe Servicios Generales y Prevención de Riesgos	• Administrar, cuidar y controlar tanto los bienes muebles, inmuebles, así como también el acceso y vigilancia de personas externas a la institución. • Coordinar con el responsable de Ciberseguridad y el Departamento de Administración, revisar el reporte el ingreso, desvinculación o cambios del personal, para resguardar o recuperar la información de bienes que se encuentran a su cargo y los privilegios de acceso de información.
Jefe/a Tecnologías de la información y	• Cumplir con los procedimientos relativos a los dominios de control de acceso, adquisición, desarrollo y

ROL	RESPONSABILIDADES
telecomunicaciones	mantenimiento de los sistemas de información y gestión de las comunicaciones y operaciones. • Gestionar los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la institución.
Encargado de Transformación Digital	• Gestionar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases. • Proponer mejoras en función de nuevas tecnologías que ayuden al objeto de la política de Seguridad de la Información y ciberseguridad. • Desarrollar políticas, estándares, procesos y directrices para asegurar la seguridad física y electrónica de sistemas automatizados. Asegurar que la política y los estándares de administración de seguridad son adecuados para el propósito, están actualizados y están implementados correctamente.
Comité de Seguridad de la información y ciberseguridad	• Proponer las definiciones estratégicas, lineamientos y prioridades, así como también los recursos e insumos, que permitan orientar y focalizar las políticas, planes, programas e iniciativas en materias de Seguridad de la Información y ciberseguridad. • Definir roles y las responsabilidades de todo el personal involucrado, incluyendo además colaboradores y terceras personas en materia de Seguridad de la información y ciberseguridad. • Evaluar y seleccionar materias a incorporar en la Política de Seguridad de la Información y ciberseguridad. • Impulsar y proponer al director ejecutivo las políticas y directrices definidas en materia de seguridad de la información y ciberseguridad. • Apoyar y promover la seguridad de la información y ciberseguridad dentro de FOSIS, mediante la difusión, educación y concientización sobre las Políticas y otras medidas de seguridad. • Coordinar, supervisar y monitorear la implementación de las Políticas y procedimientos de la seguridad de la información y ciberseguridad. • Coordinar los esfuerzos con los diferentes centros de responsabilidad y todos los grupos interés que tengan responsabilidades sobre la seguridad de la información y ciberseguridad. • Analizar, evaluar y priorizar las estrategias de tratamiento de riegos en la Seguridad de la Información y ciberseguridad. • Asegurar la protección de los activos de información. • Reportar al director ejecutivo, el resultado de la implementación de la Política, de los Riesgos, y de las medidas de administración de la Seguridad de la

ROL	RESPONSABILIDADES
	Información y ciberseguridad. • Aprobar los aspectos operativos de la implementación del Sistema de Gestión de Seguridad de la Información. • Definir los mecanismos a través de los cuales se implementará el alcance de la Política General de Seguridad. • Delimitar las responsabilidades de todo el personal involucrado, incluyendo además colaboradores y terceras partes. • Sesionar periódicamente, o cuando fuese necesario, conforme a la planificación anual definida por el Comité y comunicada según las instancias establecidas. • Gestionar la actualización de las Políticas tanto General como Específicas. • Gestionar la actualización de los Procedimientos, Guías, Protocolos y todos los documentos auxiliares que fueren necesarios para el mejor despliegue, comprensión y aplicabilidad de las directrices.
Encargado/a de Seguridad de la Información	• Velar por el desarrollo del marco normativo y los requerimientos necesarios para garantizar la protección de la información y los medios donde esta reside, sujeto a las políticas de la organización. • Organizar y presidir las actividades del Comité de Seguridad de la información y Ciberseguridad. • Ser el nexo entre el Comité Directivo y el Comité de Seguridad de la Información y Ciberseguridad. • Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior de la institución y el control de su implementación, velando por su correcta aplicación. • Supervisar el monitoreo del avance general de la implementación de las estrategias de control y tratamiento de riesgos. • Gestionar la coordinación con otros departamentos y direcciones regionales para apoyar los objetivos de seguridad. • Supervisar el establecimiento de puntos de enlace con los encargados de seguridad de otros servicios públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinente.
Secretario/a técnico del Comité de Seguridad de la Información y Ciberseguridad	• Asesorar al Encargado de Seguridad de la Información en materias técnicas de seguridad. • Gestionar las soluciones a los incidentes de Seguridad de la Información que afecten los activos de la información institucional. • Monitorear el avance de cada una de las etapas de la implementación de la política de Seguridad de la Información, reportando periódicamente al encargado de Seguridad de la Información.
Propietarios y/o responsables de los activos de	• Gestionar los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología

ROL	RESPONSABILIDADES
información	de la institución. • Gestionar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases. • Definir niveles de seguridad y establecer roles y perfiles de cada uno de los actores de los procesos estratégicos.
Encargado de Ciberseguridad (Titular y Subrogante)	• Ser el responsable de la seguridad informática en el servicio. • Proponer al Comité las debidas respuestas y posible priorización de medidas de tratamiento de incidentes y riesgos vinculados a los activos de información de los procesos institucionales y sus objetivos. • Coordinar las actividades relativas a la seguridad de la información con el Comité. • Coordinar con las distintas unidades del Servicio las acciones tendientes a cumplir y apoyar los objetivos de seguridad de la información y ciberseguridad. • Mantener historial de versiones de las Políticas institucionales en la materia. • Revisar nuevas propuestas y proveer asesoramiento especializado en temas e implicaciones de seguridad. • Monitorear la aplicación y el cumplimiento de procedimientos de administración de seguridad y revisar sistemas de información para detectar infracciones reales o potenciales en la seguridad. Asegurar que todas las infracciones de seguridad identificadas se investigan rápidamente y en profundidad y que cualquier cambio al sistema requerido para mantener la seguridad sea implementado. Asegurar que los registros de seguridad son precisos y están completos y que las solicitudes de soporte se abordan de conformidad con los estándares y procedimientos establecidos. Contribuir a la creación y el mantenimiento de políticas, estándares, procedimientos y documentación de seguridad. • Mantener los procesos de administración de la seguridad y comprobar que todas las solicitudes de soporte sean tratadas conforme a procedimientos acordados. Proveer orientación para definir derechos y privilegios de acceso. Investigar las infracciones de seguridad de conformidad con procedimientos establecidos, recomendar acciones requeridas y soportar/hacer seguimiento para asegurar que sean implementadas. • Investigar infracciones de seguridad menores conforme a los procedimientos establecidos. Asistir a los usuarios en la definición de sus derechos y privilegios de acceso. Ejecutar tareas de administración de seguridad no estándares y resolver asuntos relacionados con la administración de la seguridad. • Recibir y responder a solicitudes rutinarias de soporte

ROL	RESPONSABILIDADES
	en materia de seguridad. Mantener registros y asesorar a las personas relevantes sobre las acciones tomadas. Asistir con la investigación y resolución de asuntos relacionados con los controles de acceso y los sistemas de seguridad. • Ejecutar tareas simples de administración de seguridad. Mantener documentación y registros relevantes. • Promover buenas prácticas en el funcionamiento del Equipo de Respuesta frente a Incidentes Informáticos (CSIRT). • Promover planes de capacitación, entrenamiento, difusión y educación en el marco de los objetivos planteados por el Comité.
Encargado de los activos de Información	• Identificar y Clasificar los activos de información • Gestionar los riesgos y niveles de seguridad asociados • Custodiar, proteger o almacenar la información y activos, vinculados a determinado proceso Institucional. • Definir el acceso a los activos de información y velar por su cumplimiento.
Todo el personal del FOSIS	• Conocer y cumplir la Política de Seguridad de la Información y Ciberseguridad vigente, entendiendo en ésta la General y Específicas. • Utilizar adecuadamente los activos de información a su cargo. • Utilizar adecuadamente la plataforma tecnológica, servicios informáticos, equipamiento y dispositivos institucionales.

5. ALCANCE DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

5.1 Alcance General

Esta política se aplica a todos los funcionarios y prestadores de servicios a honorarios y terceras partes que tengan o no una relación directa o indirecta de acceso a la información que pueda afectar los activos de información del FOSIS. También se aplica a cualesquiera de sus relaciones con terceros que impliquen el acceso a sus datos, utilización de sus recursos o a la administración y control de sus sistemas de información y debe ser conocida y cumplida por todos.

Esta política rige independientemente del lugar en el que el funcionario o prestador de servicios a honorarios presta sus servicios a la organización, total o parcialmente, e indistintamente de la modalidad de trabajo ya sea "presencial", "remota", "teletrabajo" u otra, en las condiciones que establezca la legislación vigente, Contraloría General de la

República 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 del FOSIS, establecidos en el documento institucional denominado Definiciones Estratégicas A-1, cubriendo a toda la organización independiente de su ubicación geográfica en el país.

La Política General de Seguridad de la Información del Fondo de Solidaridad e Inversión Social se establece considerando las disposiciones legales vigentes, para gestionar adecuadamente la Seguridad de la Información y Ciberseguridad.

Por lo anterior, la información que genera y gestiona el FOSIS constituye un activo clave para asegurar la continuidad del negocio, por lo cual la Seguridad de la Información es una herramienta para responder por su integridad, disponibilidad y confidencialidad.

5.2 **Definición de Activos de Información**

Son aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información valiosa para el FOSIS, y se distinguen tres niveles:

1. La información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.).
2. Los equipos, sistemas e infraestructura que soportan esta información.
3. Las personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

5.3 **Definición de Seguridad de la Información**

El Fondo de Solidaridad e Inversión Social concibe la ciberseguridad y la seguridad de la información como el conjunto de acciones, políticas, medidas preventivas y reactivas destinadas a la prevención, mitigación, manejo, respuesta y estudio de las amenazas y riesgos de incidentes de seguridad, a la reducción de sus efectos y el daño causado; antes, durante y después de su ocurrencia; respecto de los activos y activos de información y la continuidad del servicio, con el fin de proteger, preservar y restablecer la confidencialidad, integridad y disponibilidad de aquellos y de las plataformas electrónicas, aumentando su resiliencia en el tiempo. (1)

6. **MARCO GENERAL DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD**

6.1 **Aspectos Generales**

La Política General de Seguridad de la Información y Ciberseguridad se elabora respetando la legislación vigente, compatibilizándola además con las prácticas sugeridas en la NCh ISO 27001.

La Dirección Ejecutiva del FOSIS se compromete a realizar las acciones que estén a su alcance para garantizar la continuidad operativa de manera de hacer frente a las interrupciones de las actividades institucionales y proteger los procesos críticos de los efectos de complicaciones importantes o paralizaciones en los sistemas de información y asegurar su oportuna reanudación.

6.2 **Aprobación de la Política**

La política general de seguridad de la información es aprobada por el/la Director/a Ejecutivo/a del Fondo de Solidaridad e Inversión Social, reflejando claramente su compromiso, apoyo e interés en el desarrollo de una cultura de Seguridad de la Información y ciberseguridad en el FOSIS.

6.3 **Difusión de las políticas de seguridad de la información**

El mecanismo de difusión de la Política es a través de la Intranet, circulares informativas, correos electrónicos masivos o cualquier otro medio que el Comité de Seguridad de la Información y Ciberseguridad estime pertinente, procurando apoyar la sensibilización con infografías que faciliten la comprensión de esta por todos los usuarios en general.

Para la difusión de las políticas que tengan relación con terceros que presten servicios a la institución, ésta se realiza a través de la página web a cargo del Departamento de Comunicaciones de la institución.

[1] Decreto Número 7/2023 “Establece norma técnica de seguridad de la información y ciberseguridad Conforme la ley N°21.180”, Artículo 2 Definición 3.

6.4 **Revisión de la Política**

La Política se considera vigente desde la fecha de su aprobación por parte del Director/a Ejecutivo/a, documento que será revisado y actualizado cada dos años o cuando el Comité de Seguridad de la Información y Ciberseguridad lo determine, o toda vez que se produzca un cambio significativo que modifique el nivel de riesgo presente de FOSIS.

La Política debe ser revisada por el Comité de Seguridad de la Información y Ciberseguridad. No obstante, aquello, la unidad de Ciberseguridad promoverá la revisión permanente de esta Política y generará las propuestas de actualización que sean necesarias, con el objetivo de apoyar el ciclo de mejora continua del SGSIyC.

Entre los cambios que hacen necesaria la revisión de las políticas, se debe destacar:

- **Cambios en las leyes o reglamentos que afecten a FOSIS**
- **Incorporación o modificaciones relevantes de procesos críticos de FOSIS**

- **Cambios significativos al soporte tecnológico.**
- **Modificaciones en la estructura de la organización.**
- **Cambios significativos en los niveles de riesgo a que se expone la información.**
- **Cambios relevantes en las Definiciones Estratégicas.**
- **Ajustes necesarios producto de Estados de Excepción Constitucional.**
- **Ajustes necesarios para proteger las infraestructuras críticas.**

6.5 **Evaluación del Cumplimiento de la Política**

Todos/as los/as Subdirectores/as, Directores/as Regionales, Jefes/as de Departamento y Unidades son responsables de la implementación de las políticas de Seguridad de la Información y Ciberseguridad, dentro de sus áreas de responsabilidad, así como del cumplimiento de las políticas, normativas y procedimientos por parte de sus equipos.

El FOSIS debe realizar auditorías internas anuales al Sistema de Seguridad de la Información para verificar el cumplimiento de las políticas, normas y procedimientos de Seguridad de la Información.

El incumplimiento de la Política General de Seguridad de la Información tiene como resultado la aplicación de sanciones acordes a la magnitud y características del aspecto no cumplido independiente de su calidad contractual (planta, contrata, honorarios y/o colaborador externo).

El Comité determinará la metodología y los alcances que estime necesarios para cumplir los objetivos estratégicos de revisión y cumplimiento de las políticas y su mejora continua.

6.6 **Control de documentos**

Los documentos requeridos por el Sistema de Gestión de la Seguridad de la Información y Ciberseguridad (SGSIyC) deben protegerse y controlarse. Con este objetivo, las acciones necesarias a implementar son:

- **Revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente.**
- **Registrar los cambios o actualizaciones de los documentos una vez que son aprobados por el Comité de y Seguridad de la información y ciberseguridad.**
- **Se debe controlar el uso no intencionado de documentos obsoletos.**
- **En caso de mantenerse los documentos por cualquier propósito, éstos deben tener una adecuada identificación a efecto de diferenciarse de los vigentes.**

Las versiones pertinentes de los documentos aplicables se encuentran disponibles para quienes lo necesiten y son almacenados y transferidos de acuerdo con los procedimientos aplicables a su clasificación.

FOSIS
Ministerio de Desarrollo Social y Familia

Gobierno de Chile

6.7 **Autorización para las Instalaciones de procesamiento de información**

Los procesos licitatorios para la adquisición e instalación de nuevos recursos y servicios tecnológicos son visados por el encargado de Ciberseguridad, y deben estar acordes a los lineamientos de seguridad establecidas por la Política General y las Políticas Específicas vigentes. En caso de no estar alineados con estos instrumentos normativos se debe iniciar un proceso ante el Comité de Seguridad de la Información y ciberseguridad tendiente a compatibilizar la nueva tecnología en las Políticas vigentes mediante presentación de informe fundado técnica, jurídica y económicamente.

Además, el encargado de Ciberseguridad evaluará, negará o autorizará, el uso de servidores de procesamiento de información, equipamiento personal en las dependencias, e infraestructura tecnológica de FOSIS.

6.8 **Contacto con Grupos Especiales de Interés**

Los encargados de Seguridad de la Información y Ciberseguridad deben coordinar los conocimientos y experiencias que han adquirido a FOSIS, con el fin de brindar asesoría en la toma de decisiones en materia de seguridad de la información. Asimismo, podrán asociarse y hacerse asesorar por otros organismos y establecer convenios de cooperación nacionales e internacionales.

6.9 **Confidencialidad de la Información** (2)

Los contratos o convenios de cooperación o servicios suscritos con terceras partes y que involucren los activos de información, deben contar con cláusulas de confidencialidad o no divulgación, debidamente validadas por Fiscalía.

6.10 **Partes Externas**

6.10.1 **Relación con terceros** (3)

FOSIS establece e implementa los mecanismos de control necesarios para la seguridad de los activos de información, en sus relaciones con personal externo que le provean de bienes o servicios. Los funcionarios responsables de la supervisión o fiscalización de contratos, convenios o acuerdos o con personal externo, deben garantizar el cumplimiento de la Política General de Seguridad de la Información y ciberseguridad por parte de éstos.

Todo contrato, convenio o acuerdo con personal externo debe tener claramente definidas las exigencias y los distintos niveles de servicios (uso, intercambio, procesamiento, etc.), en términos de seguridad de la información, requisito que se contemplará como un numeral de las especificaciones técnicas.

FOSIS, antes de permitir el acceso a la información e instalaciones de procesamiento, debe asegurarse de la identificación de los riesgos asociados y de la implementación de las medidas apropiadas para la disposición de la información.

FOSIS debe exigir, al momento del contrato o inicio de operaciones del servicio, la suscripción de un acuerdo de confidencialidad entre FOSIS y la empresa proveedora, al igual que uno entre FOSIS y cada uno de los trabajadores de la empresa contratada que tengan participación directa en los servicios prestados o tomen conocimientos de datos institucionales independientemente de si éstos son considerados públicos, reservados o secretos.

La Política de Seguridad de la Información y ciberseguridad, busca establecer y formalizar las tareas, funciones y responsabilidades sobre los procesos de tratamiento de información, incluyendo la recopilación, el desarrollo de sus procesos, procesamiento, almacenamiento y distribución de la información, lo que permitirá gestionar y controlar adecuadamente la seguridad de la información y la ciberseguridad al interior de la organización, de manera de lograr una adhesión y compromiso a todo nivel.

7. TRABAJO REMOTO O TELETRABAJO (4-5)

Por la complejidad y transversalidad del concepto FOSIS cuenta con una política específica y las medidas que apoyen la seguridad para proteger la información a la que se accede, procesa o almacena en los sitios de trabajo remoto y de teletrabajo.

En esta política, en tanto no se especifique algún normativa específica o legislación jerárquicamente superior que lo reemplace, se establecen las condiciones y las restricciones del uso del trabajo remoto o del teletrabajo. Se deben considerar los siguientes asuntos donde se considere aplicable y lo permita la ley vigente o los Estados de Excepción Constitucional decretados por el Presidente de la República:

[2] política de datos para la privacidad y protección de la información

[3] política de seguridad de la información para las relaciones con el proveedor

[4] Política para el trabajo remoto

[5] Resolución Exenta N°FC-P-00262 Aprueba protocolo para la implementación de la modalidad de teletrabajo en el FOSIS, 02-05-2023.

- **la seguridad física existente del sitio de teletrabajo, considerando la seguridad física del edificio y del entorno local;**
- **el entorno de teletrabajo físico propuesto;**
- **los requisitos de seguridad para las comunicaciones, considerando la necesidad de contar con acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se accederá y que se traspasará por el enlace de comunicaciones y la sensibilidad del sistema interno;**
- **la provisión de acceso a un escritorio virtual que evite el procesamiento y el almacenamiento de información en equipos de propiedad privada;**

- **la amenaza del acceso no autorizado a la información o a los recursos de parte de otras personas que utilizan el recinto, es decir, la familia y los amigos;**
- **el uso de redes domésticas y los requisitos o restricciones en la configuración de los servicios de redes inalámbricas;**
- **las políticas y procedimientos para evitar disputas en cuanto a los derechos de propiedad intelectual desarrollados en equipos de propiedad privada;**
- **acceso a equipos de propiedad privada (para verificar la seguridad de la máquina durante una investigación), lo que se puede evitar por legislación;**
- **acuerdos de licenciamiento de software que pueden hacer que las organizaciones se hagan responsables del software de cliente en estaciones de trabajo de propiedad privada de empleados o de usuarios externos;**
- **requisitos de protección de malware**
- **requisitos de protección en su firewall (cortafuegos).**

Las pautas y disposiciones que se deben incluir son (6)

- **la provisión de equipos idóneos y muebles de almacenamiento para las actividades de teletrabajo, donde no se permite el uso de equipos de propiedad privada que no estén bajo el control de la organización;**
- **una definición del trabajo permitido, las horas de trabajo, la clasificación de información que se puede tener y los sistemas y servicios internos que se autoriza al teletrabajador a acceder;**
- **la provisión de equipos de comunicación idóneos, incluidos los métodos para proteger el acceso remoto;**
- **seguridad física;**
- **normas y orientación sobre el acceso a familiares y visitas a los equipos y a la información;**
- **la provisión de soporte y mantenimiento de hardware y software;**
- **la provisión de seguros;**
- **los procedimientos para el respaldo y la continuidad en el negocio;**
- **auditoría y monitoreo de seguridad;**
- **revocación de autoridad y derechos de acceso y la devolución de los equipos cuando concluyen las actividades de teletrabajo.**

De manera obligatoria se deben incorporar las recomendaciones y buenas prácticas sugeridas por el CSIRT de Gobierno.

En tanto no se disponga de una legislación para el sector público, a efectos de las políticas en las que se integre el concepto de "trabajo remoto" o "teletrabajo" se asumirán las siguientes definiciones, basadas en la Ley N°21.220:

7.1 **Trabajo remoto:**

Es trabajo a distancia aquel en el que el trabajador presta sus servicios, total o parcialmente, desde su domicilio u otro lugar o lugares distintos de los establecimientos o instalaciones de FOSIS.

7.2 **Teletrabajo:**

FOSIS
Ministerio de Desarrollo Social y Familia
Gobierno de Chile

Se denomina teletrabajo si los servicios son prestados mediante la utilización de medios tecnológicos, informáticos o de telecomunicaciones o si tales servicios deben reportarse mediante estos medios.

8. **CONTROL DE VERSIONES**

[6] Se deben considerar también las pautas establecidas en la Resolución Exenta N°FC-P-00262 que aprueba protocolo para la implementación de la modalidad de teletrabajo en el FOSIS, 02-05-2023.

Versión	Fecha de aprobación	Motivo del cambio
1	29/09/2011	• Aprueba Política General. • Decisión del Director Ejecutivo.
2	30/12/2011	• Actualiza formato. • Deja sin efecto resolución anterior.
3	25/10/2016	• Actualiza Política. • Actualiza controles de acuerdo con la versión 2013 de la norma.
4	5/10/2017	• Incorpora roles y responsabilidades. • Incorpora control de cambios.
5	30/05/2019	• Actualiza las definiciones estratégicas. • Actualización de Revisor y Aprobador del documento. • Incorpora al encargado de ciberseguridad entre los responsables • Actualiza medios de difusión
6	05/11/2019	• Delega difusión a Comunicaciones Internas y Departamento de Comunicaciones • Incorporación del Departamento de Soporte y Operaciones TIC y Departamento de Transformación Digital. • Incorporación Comunicaciones Internas y Departamento de Comunicaciones.
7	**16/03/2021**	• **Actualiza definiciones estratégicas** • **Actualiza cargo jefe de Informática y telecomunicaciones**
8	**31/10/2023**	**Actualiza política completa respecto del Decreto N°7/2023 que establece Norma técnica de seguridad de la información y Ciberseguridad conforma la ley 21.180.**

2° DÉJESE SIN EFECTO, la Resolución Exenta N° FC-F-00095, de 20 de abril de 2021, que aprobó la anterior Política General de Seguridad de la Información del Fondo de Solidaridad e Inversión Social.

ANÓTESE, COMUNÍQUESE Y PUBLÍQUESE.

Nicolás Navarrete Hernández

Firmado digitalmente por Nicolás Navarrete Hernández
Fecha: 2023.11.21 11:53:04 -03'00'

NICOLAS NAVARRETE HERNANDEZ
DIRECTOR EJECUTIVO
FONDO DE SOLIDARIDAD E INVERSIÓN SOCIAL

NNH/PMD/FMZ/JGS/RVC/MJCM
ANEXOS: SI CORRESPONDE
DISTRIBUCIÓN
DIRECCIÓN EJECUTIVA (1)

SUBDIRECCIÓN DE USUARIOS (1)

SUBDIRECCIÓN DE GESTIÓN DE PROGRAMAS (1)

SUBDIRECCIÓN DE PERSONAS (1)

SUBDIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS (1)

FISCALÍA (1)

AUDITORÍA INTERNA (1)

DIRECTORES REGIONALES (1)

OFICINA DE PARTES (1)

RESPONSABLE UNIDAD SOLICITANTE: **ROXANA VERCOUTERE CARTER**