1. OBJETIVO

Incorporar la continuidad de la seguridad de la información en los sistemas de gestión de continuidad de negocio del FOSIS y asegurar la disponibilidad de las instalaciones de procesamiento de información**.**

2. ALCANCE

El alcance de esta Política incluye a todos los funcionarios de planta, contrata, prestadores de servicio a honorarios, y a toda persona natural o jurídica que preste servicios al FOSIS y que, a raíz de ello, tenga acceso tanto a dependencias como a equipos tecnológicos que la organización posea, incluyendo los archivos de documentación, las aplicaciones comerciales, bases de datos, aplicaciones desarrolladas internamente, equipos, instalaciones, sistemas y redes.

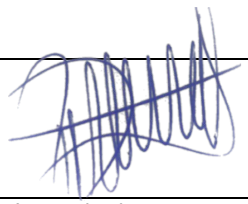
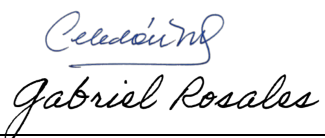
Esta Política abarca todos los procesos operacionales, de apoyo y estratégicos que cuenten con activos de información, los cuales deban ser resguardados en caso de desastres.

Norma NCH-ISO 27001:2013 controles:

- A.17.1.1 Planificación de la continuidad de la seguridad de la información.
- A.17.1.2 Implementación de la continuidad de la seguridad de la información.
- A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- A. 17.2.1 Disponibilidad de las instalaciones de procesamiento de la información.

3. DOCUMENTOS RELACIONADOS

- Política general de seguridad de la información del Fondo de Solidaridad e Inversión Social FOSIS, vigente, y todos sus procedimientos, políticas, instructivos y circulares.
- NCh-ISO 27001 Of2013 – Tecnología de la información -Técnicas de seguridad – Sistema de gestión de la seguridad de la información -Requisitos.

Elaborado por:	Revisado por:	Aprobado por:
Roxana Vercoutere Carter Profesional Depto. Procesos y Mejora Continua Encargada Ciberseguridad (S)	**María José Celedón** Asesora Jurídica Comité de Seguridad de la Información **Gabriel Rosales Villarroel** Jefe de Informática y Telecomunicaciones	**Jaime González Salazar** Encargado de Seguridad de la Información Subdirector de Usuarios (S)
		Jaime Ivan Gonzalez Salazar Firmado digitalmente por Jaime Ivan Gonzalez Salazar Fecha: 2022.07.12 17:08:43 -04'00'
Fecha: 11/07/2022	Fecha:11/07/2022	Fecha: 11/07/2022
Documento Impreso – Copia no controlada sin timbre original		

- DS 83/2004, 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.
- Ley 18.834 Estatuto administrativo.
- NCh ISO 31000:2018 Gestión del riesgo – Directrices
- Ley 18.575 Bases generales de la administración del estado.

4. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
Encargado de Seguridad de la información	• Velar por la implementación de las políticas de seguridad de la información al interior del FOSIS, de su control y de su correcta aplicación; • Coordinar y gestionar la respuesta a incidentes que afecten a los activos de información de la Institución; • Establecer puntos de enlace con los encargados de seguridad de otros organismos públicos y especialistas externos, que permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes; y • Coordinar las acciones del Comité de Seguridad de la Información, correspondientes al Sistema de Seguridad de la Información.
Comité de Seguridad de la información	• Velar por el cumplimiento y actualización de la Política General de Seguridad de la Información, presentando propuesta al director ejecutivo para su aprobación; • Validar, aprobar y difundir al interior del FOSIS las políticas específicas del Sistema de Seguridad de la Información; • Velar por la implementación de los controles de seguridad en el FOSIS; • Gestionar la identificación, evaluación y mitigación de los riesgos que afectan los activos de información y la continuidad de negocio; • Arbitrar conflictos en materia de seguridad de la información y los riesgos asociados y proponer soluciones; • Apoyar el desarrollo de los planes de comunicación, difusión y capacitación en materia de seguridad de la información; • Conocer los incidentes que pudieran afectar a la seguridad de la información al interior de la organización, con el fin de establecer acciones preventivas y correctivas;

ROL	RESPONSABILIDAD
	• Generar y proponer proyectos de desarrollo para el cumplimiento de los requisitos técnicos y normativos, dentro del marco presupuestario vigente; y • Informar a la Dirección Ejecutiva, en los intervalos que se convenga, sobre el Sistema de Seguridad de la Información.
Comité de emergencia regional/Central	• Son los responsables operativos de ejecutar las intervenciones estratégicas señaladas en el procedimiento de emergencia y apoyo estratégico FOSIS (PR-GDP-6.4-07), en sus ámbitos de competencias y áreas de desarrollo y de evaluar las gestiones vinculadas al control de la emergencia de acuerdo con los objetivos y alcance definido.
Jefes de Departamento	• Asegurar la aplicación y cumplimiento de las políticas, procedimientos e instructivos de seguridad de la información al interior de cada departamento, subdepartamento, sección o unidad según corresponda. • Velar por la toma de decisiones respecto del activo de información, política o procedimiento relacionado con algún ámbito de seguridad de la información; y • Promover al interior de su equipo de trabajo tanto la denuncia como la respuesta, cuando se solicite, a los incidentes de seguridad de la información.
Usuarios de FOSIS	• Dar cumplimiento a las directrices establecidas en la presente Política, referidas a las acciones permitidas y prohibidas de continuidad operacional; y • Reportar los incidentes de seguridad detectados en el ámbito de la continuidad operacional.

5. POLÍTICA

5.1. Generalidades

Para los efectos de esta Política, los documentos electrónicos constituyen un activo para la entidad que los genera y obtiene. La información que contiene es el resultado de una acción determinada y sustenta la toma de decisiones, por parte de quien la administra y accede a ella.

Este documento no se trata de una descripción técnica de mecanismos de seguridad, sino más bien, del marco en que se debe trabajar tanto a instalación como en la utilización de softwares en equipos y servidores de uso institucional.

5.2. Lineamientos

Ante situaciones de emergencia, desastres u otro tipo de eventos que afecten la operación de la Institución, se debe dar continuidad a la seguridad de la información, manteniendo su aplicación normal en todas las áreas que no hayan sido afectadas por el evento, propiciando su restablecimiento oportuno en las áreas afectadas.

El PR-GDP-6.4-07 Procedimiento de emergencia y apoyo estratégico FOSIS, establece los lineamientos y alcances de la continuidad operacional respecto de sus procesos operacionales, sistemas, aplicaciones y servicios.

Las tareas para la continuidad de la seguridad de la información deben estar alineadas con las establecidas por el Comité de Emergencia del FOSIS[1].

FOSIS establece a través del procedimiento de operación documentada, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante situaciones adversas.

El procedimiento para el contacto con las autoridades y grupos de interés PRSI-06.01.03 es una guía para el contacto con las autoridades pertinentes para cada tipo de evento de seguridad que pueda afectar la continuidad.

Los controles de seguridad de la información que se han implementado deben seguir funcionando durante una situación adversa. Si los controles de seguridad no pueden continuar resguardando la información, se deben establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.

En los casos en que no sea posible mantener la continuidad de la seguridad de la información, en procesos críticos o estratégicos, se deben establecer las acciones para su restablecimiento en el menor plazo posible. Con la finalidad de apoyar en la continuidad de la seguridad de la información, todas las áreas del FOSIS, independiente de la naturaleza de su función, deben tener identificadas en la Matriz de Riesgo aquellas amenazas que pueden afectar la continuidad operacional y la seguridad de la información de sus procesos críticos, además de indicar la forma en que se mitigan los riesgos identificados.

Cada responsable de activos de información[2] del área afectada por una crisis o desastre debe informar a su jefatura directa del estado de los activos de información críticos bajo su responsabilidad y debe apoyar en las acciones para recuperar los activos y dar continuidad al proceso operacional y de seguridad de la información.

---

[1] Componen el comité de emergencia.
Nivel central: jefe de Gabinete, subdirector de Administración y Finanzas, subdirector de Personas, subdirector de Gestión de Programas, Subdirector de Usuarios y Prevencionista de Riesgos
Oficina Regional: director regional, jefe de Administración y Procesos o Finanzas, Encargado de Personas, jefe de Gestión de Programas, Integrante del Comité Paritario

[2] Los activos de información y sus respectivos inventarios se encuentran definidos en el procedimiento para la gestión de activos de información PR-SSI-A.8

Ante una crisis o desastre, el área afectada debe asegurar la continuidad de la seguridad de la información en sus activos, adoptando las medidas necesarias para su aplicación, adecuándose a la contingencia presentada.

5.3. Verificar, revisar y evaluar la continuidad de la seguridad de la información

FOSIS verifica los controles de continuidad de seguridad de la información establecidos e implementados en intervalos regulares a través de auditorías anuales [3]lideradas por el departamento de auditoría interna para poder asegurar que son válidos y eficaces durante situaciones adversas.

Los cambios organizacionales, técnicos de procedimientos y procesos, ya sean en un contexto operacional o de continuidad, pueden dar pie a cambios en los requisitos de continuidad de la seguridad de la información. En tales casos, la continuidad de los procesos, procedimientos y controles para la seguridad de la información se deben revisar contra estos requisitos cambiados.

Se debe verificar la continuidad de la administración de la seguridad de la información de la siguiente forma:

a) el ejercicio y las pruebas de la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información para garantizar que son coherentes con los objetivos de continuidad de la seguridad de la información;
b) el ejercicio y las pruebas del conocimiento y la rutina para operar los procesos, procedimientos y controles de continuidad de la seguridad de la información para garantizar que su desempeño es coherentes con los objetivos de continuidad de la seguridad de la información;
c) revisión de la validez y la efectividad de las medidas de continuidad de la seguridad de la información cuando cambian los sistemas de información, los procesos, los procedimientos y los controles de seguridad de la información, o los procesos y soluciones de administración de administración de continuidad operacional/recuperación ante desastres,

La verificación de los controles de continuidad de la seguridad de la información es distinta de las pruebas y verificación de seguridad de la información y se debe realizar fuera de las pruebas de los cambios. Si es posible, resulta preferible integrar la verificación de los controles de continuidad de la seguridad de la información con las pruebas de recuperación ante desastres.

5.4. Disponibilidad de las instalaciones de procesamiento de la información

Las instalaciones de procesamiento de la información se deben implementar con la suficiente redundancia para cumplir con los requisitos de disponibilidad, para esto, se debe cumplir con lo establecido en la política para el respaldo de información y software[4].

[3] Ver PR-AIN-7.5.1-02 Procedimiento para la elaboración del plan anual de auditoría interna
[4] Política para el respaldo de información y software (POLITICA-SSI-A-12.03.01)

Se deben identificar los requisitos comerciales para la disponibilidad de los sistemas de información, Cuando no se pueda garantizar la disponibilidad a través de la arquitectura de sistemas existente, se deben considerar los componentes o arquitecturas redundantes.

Donde corresponda, se deben probar los sistemas de información redundantes para garantizar que la conmutación por error de un componente a otro funcione adecuadamente, La implementación de redundancias puede introducir riesgos a la integridad o a la confidencialidad de la información y los sistemas de información que se deben considerar al diseñar los sistemas de información[5].

5.5. Denuncias y Notificaciones[6]

El personal del FOSIS, sus proveedores o terceros debe notificar inmediatamente toda debilidad, incidente o evento asociado a actividades no permitidas o malas prácticas de acceso, que pudiera derivar en un posible incumplimiento, uso indebido u otra situación asociada, en el registro para la gestión de incidentes dispuesto en la intranet institucional y su tratamiento se realiza por el encargado de ciberseguridad, de acuerdo con lo establecido en el procedimiento para la gestión de incidentes.

6. DIFUSIÓN

La comunicación de la presente política se efectuará 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 será 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 procederá al término anticipado del contrato, por incumplimiento de obligaciones, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

[5] Ver política de desarrollo seguro de software y sistemas (POLITICA-SSI-A-14.2.1) y Procedimiento para el desarrollo seguro, control de cambios en los sistemas y pruebas de seguridad (PR-SDI-A.14.02.02)

[6] https://fosis.sharepoint.com/sites/Intranet/SAF/InformaticayTelecomunicaciones/Paginas/Registro%20de%20incidentes%20para%20la%20Seguridad%20de%20la%20Informaci%c3%b3n.aspx

8. REVISIÓN Y MEDICIÓN

La presente política deberá ser revisada a lo menos cada tres 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	11/07/2022	Publicación y difusión

FOSIS Ministerio de Desarrollo Social y Familia — Gobierno de Chile	**POLÍTICA DE CONTINUIDAD OPERACIONAL**
	ANEXO ENLACES

1. Política general de seguridad de la información del Fondo de Solidaridad e Inversión Social FOSIS,

1.1. Intranet: https://fosis.sharepoint.com/sites/Intranet/SAF/InformaticayTelecomunicaciones/Seguridad%20de%20la%20informacion/FC-F-00095-APRUEBA%20NUEVA%20POLITICA%20GENERAL%20DE%20SEGURIDAD%20DE%20

1.2. Internet: https://andinoblob.blob.core.windows.net/media/filer_public/ba/15/ba15ce1b-9d25-4950-9b8a-2554fe5a5539/fc-f-00095-aprueba_nueva_politica_general_de_seguridad_de_la_informacion_del_fosis.pdf

2. PR-GDP-6.4-07 Procedimiento de emergencia y apoyo estratégico FOSIS

2.1. Intranet: https://fosis.sharepoint.com/sites/Intranet/SAF/InformaticayTelecomunicaciones/Seguridad%20de%20la%20informacion/PR-GDP-6.4-07%20Protocolo%20Emergencia.pdf

2.2. Internet: https://qsmfosis.caschile.cl/documentos/archivos/862/PR-GDP-6.4-07%20Protocolo%20de%20Emergencia%20V1.pdf

3. PR-SSI-A-12.1.1 procedimiento de operación documentada

3.1. Intranet https://fosis.sharepoint.com/sites/Intranet/SAF/InformaticayTelecomunicaciones/Seguridad%20de%20la%20informacion/A.12.1.1%20Procedimiento%20de%20Operaci%C3%B3n%20Documentada%20V.3.pdf

4. Procedimiento para el contacto con las autoridades y grupos de interés PRSI-06.01.03

4.1. Intranet: https://fosis.sharepoint.com/sites/Intranet/SAF/InformaticayTelecomunicaciones/Seguridad%20de%20la%20informacion/A.6.1.3-4%20Procedimiento%20para%20el%20contacto%20con%20autoridades%20y%20grupos%20especiales%20de%20inter%C3%A9s%20V.4.pdf

4.2. Anexo listado autoridades intranet https://fosis.sharepoint.com/sites/Intranet/SAF/InformaticayTelecomunicaciones/Seguridad%20de%20la%20informacion/A.06.01.03%20Anexo%201%20Listado%20de%20autoridades.pdf

5. Procedimiento para la gestión de activos de información PR-SSI-A.8

5.1. Intranet https://fosis.sharepoint.com/sites/Intranet/SAF/InformaticayTelecomunicaciones/Seguridad%20de%20la%20informacion/PR-SSI-8.%20Procedimiento%20para%20gesti%C3%B3n%20de%20activos%20de%20informaci%C3%B3n%20V.5.pdf

6. PR-AIN-7.5.1-02 Procedimiento para la elaboración del plan anual de auditoría interna

6.1. Intranet: https://fosis.sharepoint.com/sites/Intranet/SAF/InformaticayTelecomunicaciones/Seguridad%20de%20la%20informacion/PR-AIN-7%205%201-02%20Elaboraci%C3%B3n%20del%20Plan%20anual%20de%20Auditor%C3%ADa%20Interna%20V13.doc.pdf

7. Política para el respaldo de información y software POLITICA-SSI-A-12.03.01

7.1. Intranet: https://fosis.sharepoint.com/sites/Intranet/SAF/InformaticayTelecomunicaciones/Seguridad%20de%2

0la%20informacion/A120301%20Pol%C3%ADtica%20de%20Respaldo%20de%20Informaci%C3%B3n%20y%20Software.pdf

7.2. Internet: https://fosisstorage.blob.core.windows.net/pdfs/A.12_Poli%CC%81tica_de_Respaldo_de_Informacio%CC%81n_y_Software.pdf

8. Procedimiento para el desarrollo seguro, control de cambios en los sistemas y pruebas de seguridad PR-SDI-A.14.02.02

8.1. Intranet: https://fosis.sharepoint.com/sites/Intranet/SAF/InformaticayTelecomunicaciones/Seguridad%20de%20la%20informacion/A.14.02.02%20ProcedimientoDesarrollo%20Seguro.pdf

9. Ver política de desarrollo seguro de software y sistemas POLITICA-SSI-A-14.2.1

9.1. Intranet: https://fosis.sharepoint.com/sites/Intranet/SAF/InformaticayTelecomunicaciones/Seguridad%20de%20la%20informacion/POL%C3%8DTICA%20DE%20DESARROLLO%20SEGURO%20DE%20SOFTWARE%20Y%20SISTEMAS%20%20V.3.pdf

9.2. Internet: https://andinoblob.blob.core.windows.net/media/filer_public/bf/91/bf91bd17-e121-4867-b418-c188e7b04a47/a1421_politica_de_desarrollo_seguro_de_software_y_sistemas__v3.pdf

10. Registro de incidentes https://fosis.sharepoint.com/sites/Intranet/SAF/InformaticayTelecomunicaciones/Paginas/Registro%20de%20incidentes%20para%20la%20Seguridad%20de%20la%20Informaci%c3%b3n.aspx