1. OBJETIVO

Asegurar la protección de los activos de 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 funcionarios, servidores públicos a honorarios y terceras partes que participen en actividades desarrolladas para FOSIS.
NCh-ISO 27001:2013 Control:

- 15.1.1 Política de seguridad de la información para las relaciones con el proveedor.
- 15.1.2 Abordar la seguridad dentro de los acuerdos con el proveedor.
- **15.1.3 Cadena de suministros de tecnologías de la información y comunicaciones**
- 15.2.1 Supervisión y revisión de los servicios del proveedor.
- **15.2.2 Gestión de cambios a los servicios del proveedor**

3. DOCUMENTOS RELACIONADOS

- Ley 19.886 de compras púbicas 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.
- NCh-ISO 9001:2015 Sistema de Gestión de la Calidad – Requisitos.
- NCh ISO 27001:2013 Tecnologías de la Información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información Requisitos.
- NCh ISO 31000: 2018 Gestión del Riesgo – Directrices.
- Política general de seguridad de la información vigente, **sus políticas, procedimientos, instructivos y toda la documentación difundida**

Elaborado por:	Revisado por:	Aprobado por:
Roxana Vercoutere Carter **Armando Guajardo San Martín** Profesionales Departamento de Procesos y Mejora Continua	**María José Celedón Muñoz** Asesor Jurídico Comité de Seguridad de la Información	**Ramón Mellado Quiroz** Encargado de Seguridad de la Información Subdirector de Desarrollo e Innovación
Fecha: 17/08/2020	Fecha: 17/08/2020	Fecha: 17/08/2020

4. ROLES Y RESPONSABILIDADES

ROL	Responsabilidad
Encargado de Seguridad de la Información	Velar por el cumplimiento de la presente política.
Proveedores y/o colaboradores	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.
Personal externo que presta servicios a FOSIS	Dar estricto cumplimiento a las normas de seguridad descritas en la presente política y en la documentación de seguridad de la información.
Funcionarios, planta, contrata, honorarios	Dar estricto cumplimiento en cuanto a las reglas adecuadas sobre el compromiso y el comportamiento en base al tipo de proveedor y el nivel de acceso del proveedor a los sistemas y la información de la organización, lo anterior, sin perjuicio del cumplimiento de las normas y políticas de seguridad de la información a que debe dar cumplimiento todo el personal interno del FOSIS.
Secretario técnico comité de seguridad de la información	Gestionar los incidentes de seguridad de la información relacionados a incumplimientos de la presente política.
Jefe de Informática	**Asesorar a los gestores de compra en los niveles de servicio necesarios para asegurar la protección de los activos de 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

5. POLÍTICA

5.1 Prestación de servicios en FOSIS

La Institución considera relevante mantener la disponibilidad permanente de los servicios relacionados con Tecnología, considerándose como criterios: el nivel de servicio, la entrega continua del mismo, los tiempos de respuesta de atención para su entrega, los tiempos de resolución de problemas, entre otros, los que son aplicados por el área respectiva que solicita el servicio y asesorados por el departamento de **informática** de la Institución.

Por otra parte, el área requirente del servicio, en conjunto con el departamento de **informática** deben verificar la existencia de planes de contingencia para efectos de validar que estos cumplen de buena forma con el criterio de disponibilidad del servicio y de los datos.

Para el caso de servicios asociados a tecnología y sistemas, es responsabilidad del departamento de **informática** incorporar en su control de monitoreo la disponibilidad de los servicios tecnológicos, plataformas de infraestructura y los sistemas de información que son entregados por el proveedor, con la finalidad de medir los niveles

del servicio y gestionar de manera oportuna cualquier incidente que pueda afectar el principio de disponibilidad.

En la medida que el área requirente necesite información detallada del servicio o sus equipos, podrá solicitar a **informática** un informe técnico sobre la disponibilidad del servicio, incluyendo el rendimiento de estos.

Cuando 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.

5.2 Confidencialidad de la información

En los casos en que se requiere entregar información a proveedores, o que producto de la prestación del servicio debe acceder a información de la Institución, se deben aplicar acuerdos de confidencialidad y no divulgación entre FOSIS y los proveedores reflejándose en los respectivos contratos, los que deben dar cuenta de los responsables, la información en cuestión, las medidas mínimas de seguridad aplicadas, la forma de proceder frente a incidentes, la extensión del acuerdo a terceros subcontratados, la propiedad de los productos desarrollados, el tiempo de vigencia del acuerdo, las sanciones frente a su incumplimiento y su aceptación formal. La aplicación de los acuerdos de confidencialidad es responsabilidad de cada área requirente, sin embargo, su redacción estandarizada y el resguardado de los acuerdos ya formalizados es responsabilidad de la Fiscalía del FOSIS.

5.3 Propiedad Intelectual

Todos los proveedores y/o colaboradores deben dar cumplimiento a la política de propiedad intelectual del Servicio, disponible en la página web del FOSIS.

5.4 Intercambio de Información

Toda salida de información que contenga datos de carácter personal (tanto en soportes informáticos como en papel o por correo electrónico) sólo puede ser realizada por personal autorizado y con el debido permiso, cumpliendo con la Ley 19.628 sobre protección de la vida privada **y lo establecido en la política de seguridad en las telecomunicaciones.**

Si el tratamiento de datos de carácter personal se llevase a cabo fuera de las instalaciones del FOSIS, dicho tratamiento debe ser autorizado expresamente por el dueño o responsable de la información y, en todo caso, debe garantizarse el nivel de seguridad correspondiente al tipo de información tratado[1]. **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 que garantice que la información no sea inteligible ni manipulada por terceros[2].

En general, deberá 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.

Los recursos que el FOSIS pone a disposición del personal externo, independientemente del tipo que sean (informáticos, datos, software, redes, sistemas de comunicación, etc.), están disponibles exclusivamente para cumplir las obligaciones y propósito de la operativa para la que fueron proporcionados, y de acuerdo con su uso natural. El FOSIS se reserva el derecho de implementar mecanismos de control y auditoría que verifiquen el uso apropiado de estos recursos.

Cualquier archivo introducido en la red de FOSIS o en cualquier equipo conectado a ella a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, debe cumplir los requisitos establecidos en las políticas de seguridad del FOSIS y, en especial, las referidas a propiedad intelectual[3], protección de datos de carácter personal y control de malware[4].

En general, los proveedores deberán cumplir con lo señalado en las políticas de seguridad del FOSIS, disponible en la página web del FOSIS.

5.6 Gestión de equipamiento "Hardware"

Los proveedores de servicios deben asegurarse de que todos los equipos proporcionados por FOSIS para la prestación de servicios, independientemente del tipo que sean, se gestionan apropiadamente. Para ello deben cumplir con lo siguiente:

- El proveedor debe mantener una relación actualizada de equipos proporcionados por el FOSIS y usuarios de dichos activos, o responsables asociados en caso de que los activos no sean de uso unipersonal. Dicha relación puede ser requerida por el FOSIS en cualquier momento.
- Siempre que un proveedor quiera reasignar algún equipo entregado por el FOSIS, a otro miembro de su equipo, debe devolver temporalmente dicho activo a personal del FOSIS para que se puedan llevar a cabo los procedimientos de borrado seguro necesarios, de forma previa a su reasignación[5].

[1] **PR-SSI-8 Procedimiento para gestión de activos de información**

[2] **Política A.10.1.1 Política para uso de controles criptográficos y gestión de claves**

[3] **Política A.18.1.2 Política de propiedad intelectual**

[4] **PR-A.12.02.01 Procedimiento para el control de malware**

[5] **PR-SSI-A-11.2.7 Procedimiento de seguridad en la reutilización o descarte de equipos**

- En caso de que un proveedor cese en la prestación del servicio, debe devolver al FOSIS todos los activos recibidos, tal y como establecen los correspondientes contratos de prestación de servicios.

5.7 Cadena de suministros de tecnologías de la información y comunicaciones

Los acuerdos con los proveedores deben incluir los requisitos para abordar los riesgos de seguridad de la información asociados a los servicios de la tecnología de la información y las comunicaciones y la cadena de suministros del producto considerando:

- **Para los servicios de tecnologías de información y comunicaciones, que los proveedores apliquen las mejores prácticas de seguridad, en toda la cadena de suministro de servicios y productos que son entregados a FOSIS**
- **Implementación de procesos de seguimiento y monitoreo para validar la entrega de información, servicios y productos que se adhieren a los requisitos de seguridad.**
- **Identificar componentes de productos y servicios que son críticos para el mantenimiento y funcionalidad, por lo tanto, requieren de un mayor control.**
- **Tener la seguridad que los servicios o productos son entregados de acuerdo con lo que se espera, sin inconvenientes o situaciones inesperadas.**
- **Implementación de procesos para la gestión de tecnologías de información y comunicaciones, el ciclo de vida de los componentes y sus riesgos asociados.**

5.8 Gestión de cambios a los servicios del proveedor

Se deben gestionar los cambios al suministro de los servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles al considerar la criticidad de la información del servicio, los sistemas y procesos involucrados y la reevaluación de los riesgos considerando los siguientes aspectos:

- **Cambios en los acuerdos con los proveedores.**
- **Los cambios para poner en práctica mejoras en los servicios ofrecidos, desarrollo de nuevas aplicaciones y sistemas, modificación o mejoras en las políticas y procedimientos de FOSIS o cambios o nuevos controles para mitigar incidentes de seguridad o mejoras en la seguridad.**
- **Cambios en los servicios de proveedores para poner en práctica mejoras en los servicios de telecomunicaciones, uso de nuevas tecnologías, cambios de versiones de productos o nuevas versiones, nuevas herramientas de desarrollo y ambientes, cambios físicos en instalaciones de FOSIS, cambios de proveedores y subcontratación de otros proveedores.**

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.
- 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 FOSIS[6].

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 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	30/09/2019	Primera versión política
2	06/12/2019	Incorpora responsabilidad del Fiscal y del encargado de seguridad de la información
3	**17/08/2020**	**- Actualiza objetivo** **- Amplía alcance** **- Actualiza de departamento de soporte y operaciones TIC a Departamento de Informática** **- Incorpora 5.7 y 5.8**

[6] **Oficio circular 0398/26-09-2019. Imparte instrucciones sobre observancia de la política de seguridad de la información del FOSIS**