1. OBJETIVO

Asegurar la protección de información en las redes y sus instalaciones de procesamiento de la información de apoyo y mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

2. ALCANCE

Esta política se aplica a todos los funcionarios, servidores públicos a honorarios y terceras partes que tengan derechos de acceso a la información que puedan afectar los activos de información del FOSIS y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

Norma NCh-ISO 27001:2013 Controles:

- 13.01.01 Controles de red
- 13.01.02 Seguridad en los servicios de red
- 13.01.03 Separación de redes
- 13.02.01 Políticas y procedimientos de transferencia de información
- 13.02.02 Acuerdos sobre transferencia de información
- 13.02.03 Mensajería Electrónica
- 13.02.04 Acuerdos de confidencialidad o no divulgación

3. DOCUMENTOS RELACIONADOS

- Política general de seguridad de la información del Fondo de Solidaridad e Inversión Social FOSIS, Vigente, sus políticas, procedimientos e instructivos.
- NCh-ISO 27001:2013 Tecnologías de la información – Técnicas de seguridad – Sistemas de gestión de la 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.
- Ley 20.285 de 2008 sobre acceso a la información pública.
- Ley 17.336 de 2004 sobre de propiedad intelectual
- Ley 19.927 de 2004 modifica código penal y código procesal penal en materia de delitos sobre pornografía infantil.
- Ley 19.799 de 2012 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Ley 19.628 de 1999 sobre protección de la vida privada.
- Ley 19.223 de 1993 sobre figuras penales relativas a la informática.
- Ley 18.168 de 1982, ley general de telecomunicaciones.

4. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
Funcionarios de Planta, Contrata y Honorarios	Cada funcionario es el único responsable de las acciones que se realizan con su cuenta de red institucional. Mantener la confidencialidad de sus contraseñas de acceso a los sistemas FOSIS. Actualizar su clave de acceso a los sistemas FOSIS cuando corresponda. Almacenar la información relevante en carpetas de trabajo creadas directamente en su equipo y/o la nube corporativa[1].
Jefe de Área o Departamento Presidente Nacional ANFFOS Jefe de Bienestar Fiscal Jefe de Auditoría	Solicitar la creación de cuentas genéricas de correo electrónico y listas de distribución. Administración y buen uso de las cuentas genéricas de correo electrónico y listas de distribución solicitadas. Comunicar y mantener informado al Departamento de Informática y

[1] Ver Procedimiento para la gestión de activos de información PR-SSI-A.8

ROL	RESPONSABILIDAD
Directores Regionales Subdirectores	Telecomunicaciones sobre la entrada y salida de personas a las listas de distribución.
Encargado de Seguridad de la Información	Supervisar la implementación y mantener la vigencia de la presente política
Jefe Departamento de Informática y Telecomunicaciones	Implementación de la configuración, monitoreo y controles correspondientes a las redes y los servicios de red del FOSIS. Aprobar o rechazar las solicitudes de permisos especiales de acceso a los servicios de red. Mantener activo todos los registros (LOGS) que las políticas, procedimientos e instructivos indican Mantener respaldo[2] e integridad de los registros. Resguardar que los registros no sobrepasen los límites definidos. Revisar si las solicitudes de nuevos permisos se acogen a los procedimientos vigentes.
Jefe Departamento de Gestión de Personas	Informar contratación, desvinculación, retiro o movilidad del personal de planta, contrata y honorarios, de acuerdo con lo señalado en la política de control de acceso y los procedimientos del área[3].
Proveedores de servicios	**Se debe entregar acceso lógico y físico (dependencias) previa autorización del Jefe del Departamento de Informática y Telecomunicaciones.**

[2] Ver política para el respaldo de información y software. Política-SSI-A-12.03.01

[3] Anexo 1 PR-GDP-6.1-04 Procedimiento para la contratación de cargos de planta y contrata y PR-GDP-6.1-05 Procedimiento para la contratación de cargos a honorarios.

5. POLÍTICA

5.1 Autorización para permitir acceder a redes y servicios de red

Todos los computadores del FOSIS se configuran para acceder a los servicios de red.

Todos los funcionarios tienen sus cuentas de red debidamente configuradas para acceder a los distintos servicios de red, de acuerdo con su perfil (cargo), el que es informado por el Departamento de Gestión de Personas al momento de ingreso de un nuevo funcionario[4].

En el caso del acceso de proveedores[5], desarrolladores[6] y ejecutores[7] a los que se autoriza acceso a las redes de FOSIS, éstos deben cumplir con lo establecido en las políticas de seguridad de la información y normas internas, el gestor del contrato debe monitorear los accesos mientras dure la relación contractual.

Las solicitudes de permisos especiales o adicionales para utilizar redes o servicios de red deben ser aprobados por la jefatura directa de cada funcionario a través de formulario de solicitud[8] a la Mesa de Ayuda, la cual revisará si se acoge a los procedimientos o instructivos vigentes, de lo contrario, escalará la solicitud al jefe del Departamento de Informática y Telecomunicaciones quién determina si la solicitud no vulnera la Política de Control de accesos[9] del FOSIS, sopesando los criterios de facilidad de operación y protección de la información.

5.2 Controles de seguridad a la red y a los servicios de red[10]

Las conexiones de red y servicios de red del FOSIS están configurados para registrar todas las actividades que se realizan, manteniendo estos registros disponibles por un mes.
Los datos que se registran de los usuarios que utilizan redes o servicios de red de la institución son los siguientes:

- Dirección IP origen
- Nombre del dispositivo origen
- Puertos utilizados
- Dirección IP destino
- URL destino
- Tráfico de red

[4] Anexo 1 PR-GDP-6.1-04 Procedimiento para la contratación de cargos de planta y contrata y PR-GDP-6.1-05 Procedimiento para la contratación de cargos a honorarios.
[5] **Ver política de seguridad de la información para las relaciones con el proveedor. Política 15.1.1**
[6] **Ver política de desarrollo seguro de software y sistemas Política SSI-A-14.2.1**
[7] **Ver política de seguridad de la información para las relaciones con el proveedor. Política 15.1.1**
[8] https://fosis.sharepoint.com/sites/Intranet/SAF/InformaticayTelecomunicaciones/Paginas/Mesa-de-ayuda-Inform%C3%A1tica.aspx
[9] Política-SSI-A-9.1.1 Política de control de acceso
[10] **Ver IT-SDI-09.01.02 Instructivo acceso a redes y servicios de red**

Para minimizar las fallas y dar respuesta oportuna a incidentes, se debe monitorear los servicios de red del FOSIS, alertando a los responsables de manera automática.
Para utilizar servicios de red, todos los usuarios deben iniciar sesión en Active Directory.
Para usuarios que requieren acceso remoto, se aceptarán conexiones VPN autorizadas por el jefe de **I**nformática y Telecomunicaciones.
Todos los usuarios que utilizan servicios de red desde dispositivos móviles deben cumplir con la Política para el uso de dispositivos móviles[11] y la política para el trabajo remoto[12].
Las redes inalámbricas (WIFI), deben cumplir con las siguientes configuraciones:

a) Dos nombres de acceso, una para los usuarios del FOSIS y otra para visitas.
b) Permisos restringidos para las visitas o proveedores externos que solicitan conectarse a la red institucional. Esta conexión es temporal.

Los usuarios con computadores personales[13] que desean utilizar servicios de red en ellos deben ajustarse a los requisitos de la Política para el uso de dispositivos móviles[14].

Queda prohibido que los usuarios accedan a redes o a servicios de redes no permitidos, sin la autorización correspondiente.
El servicio de red de acceso a internet es restringido con un sistema de filtro de contenidos.
Los usuarios tienen prohibición de conectar algún dispositivo que permita compartir acceso a redes o a servicios de red, tales como Router, Switch, o equivalente.
Todo servicio de red que consuma ancho de banda excesivo (transferencia de videos, o archivos de gran tamaño) será restringido, salvo a usuarios que lo requieran para el cumplimiento de sus funciones, en cuyo caso, la jefatura del usuario debe solicitar a la mesa de ayuda el acceso a un servicio en particular.

5.3 Segmentación de redes

Las redes de comunicación de la institución emplean el protocolo de red IP. Estas están adecuadamente segmentadas, o particionadas, para permitir el establecimiento de puntos de convergencia de los tráficos, los cuales facilitan el control de los datos en tránsito. De esta forma es posible restringir ciertos tipos de tráficos, así como asegurar otros.
Para ello, se establecen como mínimo los perímetros siguientes:

- **DMZ:** esta zona de seguridad está protegida mediante un firewall y tiene como función contener a todos aquellos servidores que exponen información a las redes públicas.
- **Internet:** esta zona de seguridad se delimita por la interconexión con los enlaces de comunicación que permiten el acceso a las redes públicas, como lo es Internet. Debe estar resguardada por un firewall, el cual puede compartir la función de DMZ. Este punto establece la frontera entre lo público y lo privado.

[11] **Política-SSI-A-06.02.01 Política para el uso de dispositivos móviles**
[12] **Política-SSI-A-06.02.02 Política para el trabajo remoto**
[13] **Computadores que no pertenecen al FOSIS**
[14] **Política-SSI-A-06.02.01 Política para el uso de dispositivos móviles**

- **Producción:** este perímetro está destinado a contener aquellos servidores de distintos ámbitos (repositorios, intranet, bases de datos, etc.) que soportan los servicios de procesamiento de información. Estos servidores y/o servicios no pueden estar expuestos a las redes públicas en forma directa, solo a nivel interno. La exposición debe realizarse mediante otro servidor de ambiente DMZ, por ejemplo, mediante arquitecturas de modelo de 3 capas. Debe estar delimitado mediante firewall.
- **Interno:** este perímetro lo componen todas las estaciones de trabajo de los usuarios y aquellos elementos que les prestan servicios complementarios, como impresión, control de acceso, redes inalámbricas, etc. Los usuarios deben estar segregados de acuerdo con el organigrama de la institución. Esta segregación debe estar también reflejada en la estructura jerárquica del Active Directory y debe ser coherente. Los distintos segmentos no pueden comunicarse entre sí y no pueden exponer servicios de ningún tipo, con excepción del que aloja a las impresoras. Debe contar con un firewall para efectos de delimitaciones y control.
- **Desarrollo, pruebas y certificación:** corresponde al perímetro destinado al proceso de construcción de sistemas previo al paso a los entornos de producción o de DMZ. Debe estar delimitado por controles duros de red, como firewall o equivalente y sólo es accesible para quienes tienen relación con los sistemas en alguna de las etapas de construcción. No puede ser expuesto a Internet, no puede alojar sistemas en fase de explotación o producción[15]. Si en alguna situación se requiere exponer un sistema, se puede realizar una excepción, la que deberá tener asociada una duración máxima limitada y documentada.

En FOSIS se protegen los accesos a productivo mediante una red HA-Proxy que permite validar los accesos mediante reglas de enmascaramiento de IP y validación de SSL.

5.4 Seguridad en los perímetros de la red

El FOSIS cuenta con equipos del tipo firewall propios o de terceros que al menos tienen las siguientes funcionalidades[16]:

- Establecer reglas de filtro y navegación para los usuarios internos (LAN)
- Permitir configurar publicaciones de servicios internos hacia internet (DMZ) en forma segura.
- Filtro de correo (Antispam), bloqueo de mensajes no deseados en tiempo real.
- Filtro de Navegación, restricción de accesos WEB de usuarios, de acuerdo con el contenido de los sitios, protección contra sitios maliciosos.
- Filtro antivirus, revisión de tráfico WEB y email de protección perimetral contra spyware, virus y otros.
- Servicio de conectividad remota segura a través de VPN.

[15] **Ver Política-SSI-A-14.2.1 Política de desarrollo seguro de software y sistemas**
[16] **Ver PR-SDI-A.12.02.01 Procedimiento para el control contra el malware**

- Sistema de prevención de intrusos (IPS), que posibilite en tiempo real, identificar, detectar y/o bloquear ataques o actividades sospechosas sobre la red del servicio, complementando los dispositivos de seguridad del firewall.
- Integración con Active Directory, para controlar y agrupar por tipo los diferentes niveles de acceso a Internet por parte de los usuarios.

Por otra parte, el Departamento de Informática y Telecomunicaciones, gestiona, a través de recursos propios o de terceros, las siguientes tareas en orden de mantener la Seguridad Perimetral en permanente operación:

- Resumen de incidentes y requerimientos en un mes[17].
- Principales eventos de seguridad detectados, criticidad, origen de estos y recomendaciones.
- Análisis de upgrades y parches para la plataforma administrada.
- Monitoreo y Reportes de Uptime general de componentes.
- Registro de Conexiones denegadas.
- Registro y Reportes de Bloqueo de sitios Web no autorizados.
- Registro y Reportes de sitios Web más visitados.
- Registro y Reportes de Ranking de los usuarios con mayor actividad en el acceso bajo supervisión.
- Registro y Reportes de Eventos ocurridos en el firewall y en el acceso bajo supervisión durante el período

5.5 Acuerdos de servicios de red

Entre la documentación que el Departamento de Informática y Telecomunicaciones genera y mantiene permanentemente actualizada en la respectiva carpeta de red está la lista de los Servicios de Red, incluyendo en esta, los mecanismos de seguridad empleados para otorgar el servicio en forma segura, los niveles de servicio y reportes que son solicitados a través de contratos o bien solicitados por FOSIS, tales como reportes comprometidos en los CDC (Convenios de Desempeño Colectivo) o PMG (Programa de Mejoramiento de Gestión).

5.6 Regulaciones para el correo electrónico

a) Sólo el personal interno, o externo que es formalmente autorizado, puede hacer uso del sistema de correo electrónico.
b) Se puede dar uso personal a este servicio, siempre que no interfiera con las actividades formales de la institución, que no se sostengan actividades comerciales personales y que no comprometa a la institución.
c) La creación de casillas de correo se rige de acuerdo con los procedimientos de contratación[18] emanados de la subdirección de personas al momento del ingreso al servicio.
d) Toda casilla debe estar asociada a una persona, sistema o servidor específico.

[17] **Ver PR-SSI-A-16.1 Procedimiento para gestionar incidentes de seguridad de la información**

[18] Anexo 1 PR-GDP-6.1-04 Procedimiento para la contratación de cargos de planta y contrata y PR-GDP-6.1-05 Procedimiento para la contratación de cargos a honorarios.

e) Se permiten listas de distribución solo para la recepción de correos.
f) Sólo se permite el uso del software cliente de correo electrónico establecido como estándar para el servicio de correo electrónico institucional.
g) El correo electrónico tiene una forma estándar y capacidad limitada de espacio de almacenamiento para cada usuario de correo. Las excepciones son autorizadas por el jefe del Departamento de Informática y Telecomunicaciones.
h) Se debe utilizar el estándar institucional de pie de firma para los correos[19]**.**
i) Se debe habilitar respuesta automatizada sólo para períodos de ausencia autorizadas por el Servicio.
j) En caso de que la comunicación lo amerite, por su contenido o por el cargo de los participantes, el correo electrónico debe generarse firmado digitalmente y/o cifrado.
k) Es responsabilidad del usuario revisar y eliminar mensajes de correo detectados como SPAM por la plataforma central de seguridad del correo electrónico y avisar a la mesa de ayuda.
l) Los buzones de correo electrónico institucional deben utilizarse tomando todas las medidas de seguridad, en especial cuando se remita información restringida de la institución. Cualquier archivo con información confidencial, debe remitirse con algún tipo de encriptación y/o clave de seguridad o password de cierta complejidad, que inhiba el acceso por parte de personas no autorizadas.
m) Bajo ninguna circunstancia el correo electrónico institucional puede ser utilizado para difamar, insultar, hostigar, ni acosar, ya sea al personal interno, externo, ni a la Institución.

5.7 Regulación de seguridad para mensajería y transferencia de información

Deben existir controles formales para la transferencia de información en las redes de datos de la institución con el fin de evitar actos no autorizados como intercepción, copia, modificación, ruteo incorrecto y destrucción.
Deben existir mecanismos de protección de dichas comunicaciones:

- Sistemas antivirus y antimalware para correo electrónico.
- Uso de cifrado para transacciones que lo ameriten.

Se debe informar en el registro de incidentes de seguridad cualquier detección de falla, uso o acceso malintencionado de información, para evitar responsabilidades del usuario que comprometan al Servicio, por difamación, acoso, imitación, spam, u otros actos reñidos con la moral, buenas costumbres o legalidad[20]**.** Se debe integrar a los lineamientos de uso aceptable de las instalaciones y tecnologías de comunicación.

[19] Disponible en intranet en el espacio de imagen corporativa
[20] Ver PR-SSI-A-16.1 Procedimiento para gestionar incidentes de seguridad de la información

5.8 Acuerdos de confidencialidad o no divulgación

FOSIS considera los siguientes elementos para identificar los requisitos de confidencialidad o para los acuerdos de no divulgación en el intercambio de información[21]:

- Individualización de las partes.
- Identificar y definir claramente la información que se protege.
- Establecer la duración de los acuerdos, incluidos los casos donde es posible que sea necesario mantener la confidencialidad de manera extendida.
- Acciones necesarias al terminar un acuerdo.
- Responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada.
- Propiedad de la información, secretos legales o administrativos y propiedad intelectual y cómo esto se relaciona con la protección de información confidencial[22].
- El uso permitido de la información confidencial y los derechos del firmante para utilizar dicha información.
- Derechos para auditar y monitorear actividades que involucran información confidencial.
- Notificar e informar la divulgación no autorizada o la fuga de información confidencial. Condiciones para la información que se va a regresar o destruir al término del acuerdo.
- Medidas esperadas que se toman en caso de un incumplimiento del acuerdo.

5.9 Prohibiciones

Queda prohibido, el uso del correo electrónico institucional, para llevar a cabo alguna de las siguientes acciones:

a) Envío de cadenas de cualquier tipo.
b) Envío de información confidencial de la Institución, a terceros no autorizados.
c) Publicar cualquier tipo de avisos comerciales.
d) Envío de cualquier mensaje o publicación que contravenga las normas éticas y principios de la Institución, así como también, la legislación vigente.
e) Envío de cualquier tipo de Spam o correo masivo.
f) Cualquier intento de suplantación.
g) Cualquier tipo de comunicado interno o externo que contenga material obsceno, ofensivo, pornográfico, xenófobo, homofóbico, transfóbico, racista o cualquier otro tipo de mensaje de carácter discriminatorio, que pueda dañar la integridad o el honor de las personas.
h) Publicar hipervínculos direccionados a sitios alusivos al ítem anterior.
i) Apertura de correos externos, cuyos emisores o contenidos sean de dudoso origen o desconocidos.
j) Queda prohibido, el uso del acceso a Internet, para lo siguiente:

[21] **Ver IT-SSI-A.18.01.01 Identificación de la legislación vigente, PR-SDI-18.1.3-01 Procedimiento para la protección de los registros, Política-SSI-A-18.01.02 Política de propiedad intelectual**
[22] **Ver Política-SSI-A-18.01.02 Política de propiedad intelectual**

a. **Bajar películas, música y juegos.**
b. **Acceder a sitios de internet que contravengan las normas éticas y principios de la Institución, así como también, la legislación vigente.**
c. **Publicar en redes sociales o sitios de internet, cualquier tipo de información que pueda afectar la seguridad, operación, imagen y reputación de la Institución.**
d. **Acceder y/o almacenar contenidos de connotación pornográfica u otros similares que contenga material obsceno, ofensivo, xenófobo, homofóbico, transfóbico, racista, o cualquier otro tipo de connotación de carácter discriminatorio o delictivo.**

6. DIFUSIÓN

La comunicación de la presente política se efectúa de manera que el contenido de la documentación es 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.

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. TABLA DE MODIFICACIONES

Versión	Fecha de Aprobación	Motivo del Cambio
1	30/09/2019	Aprueba política

Versión	**Fecha de Aprobación**	**Motivo del Cambio**
2	11/08/2021	Modifica cargo jefe de Informática y Telecomunicaciones Incorpora referencias de procedimientos, instructivos y políticas.
3	**21/12/2021**	**Incorpora ítem 5.9 prohibiciones**