1. OBJETIVO

Establecer las normas para el acceso a la información para los funcionarios, servidores públicos a honorarios de FOSIS y terceras partes, adoptando las medidas de apoyo a la seguridad para gestionar los riesgos asociados.

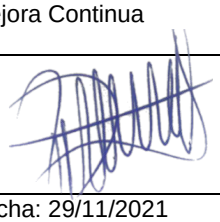
2. ALCANCE

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:

- 9.1.1 Política de control de accesos
- 9.2.2 Gestión de los derechos acceso asignados a usuarios
- 9.2.5 Revisión de los derechos de acceso de los usuarios
- 9.2.6 Retirada o adaptación de los derechos de acceso
- 7.1.1 Investigación de antecedentes
- 7.1.2 Términos y condiciones de contratación
- 7.3.1 Cese o cambio de puesto de trabajo
- 6.2.1 Política de dispositivos móviles

3. DOCUMENTOS RELACIONADOS

- Política general de seguridad de la información del Fondo de Solidaridad e Inversión Social FOSIS**, sus procedimientos instructivos y circulares, Vigente.**
- NCh-ISO 27001:2013 – Tecnología de la información -Técnicas de seguridad – Sistema 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.
- Decreto N° 93, de 2006, de la Secretaría General de la Presidencia: Aprueba norma técnica para minimizar la recepción de mensajes electrónicos masivos no deseados, en las casillas electrónicas de los órganos de la Administración del Estado y de sus funcionarios.

Elaborado por:	Revisado por:	Aprobado por:
Roxana Vercoutere Carter Profesional Depto. Procesos y Mejora Continua	**Gonzalo Calderón** Jefe Departamento de Procesos y Mejora Continua	**Jaime González Salazar** Encargado de Seguridad de la Información **Subdirector de Usuarios (S)**
		
Fecha: 29/11/2021	Fecha: 29/11/2021	Fecha:29/11/2021
Documento Impreso – Copia no controlada sin timbre original		

- Decreto Supremo N° 1299, Establece nuevas normas que regulan la Red de Conectividad del Estado que administra el Ministerio del Interior y fija los procedimientos, requisitos y estándares tecnológicos para la incorporación a dicha red de instituciones públicas.
- Decreto Supremo N° 5996, Crea Red Interna (INTRANET) del Estado y entrega su implementación, puesta en marcha, administración, coordinación y supervisión al Ministerio del Interior, Trámite extraordinario de urgencia.
- Ley 20.285 regula el principio de transparencia de la función pública y el derecho de acceso a la información de los órganos de la Administración del Estado.
- Ley 19.628 de Protección de vida privada y datos.
- Ley 19.223 de Delitos informáticos.
- Ley 19.799 Sobre documentos electrónicos, firma electrónica y
- servicios de certificación de dicha firma.
- Ley 19.927 de Delitos de Pornografía Infantil.

4. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
Jefe de Departamento	Definir los accesos a los datos por parte de los usuarios bajo su cargo, cuidando de mantener una adecuada segregación de funciones.
Jefe Departamento de **Informática y Telecomunicaciones**	Disponer los controles y reglas de control de acceso. Gestionar los derechos de acceso a los medios de procesamiento de información que tenga a su cargo, según lo descrito en esta política.
Jefe de Gestión de Personas	Solicitar acceso **y bajas** a sistemas de acuerdo con los requerimientos del cargo.
Funcionarios, Planta, contrata, honorarios	Conocer y cumplir con esta política y todos los procedimientos relacionados.

5. POLÍTICA

5.1 CONTROL DE DOCUMENTOS

Todos los documentos del FOSIS deben protegerse y controlarse. Para lograr este objetivo, las acciones necesarias a implementar son las señaladas en el PR-SGC-4.2.3-01 Procedimiento Elaboración, Emisión y Control de Documentos, vigente del sistema de gestión de la calidad.
Las versiones pertinentes de los documentos aplicables se encuentran disponibles para quienes lo necesiten y son almacenados y transferidos de acuerdo con el procedimiento antes señalado.

5.2 CONTROL DE ACCESO

5.2.1 Reglas para el control de acceso

Las reglas para el control de acceso están documentadas a través de los diferentes procedimientos de los respectivos activos de información.

5.2.2 Gestión de identidades

Se debe asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información.

Existen procedimientos formales de inscripción (PR-GDP-6.1-04 Procedimiento para la contratación de cargos de planta y contrata y PR-GDP-6.1-05 Procedimiento contratación honorarios, anexo 1 ficha), y des inscripción (PR-GDP-6.2 1-09 Procedimiento para término de la relación laboral para planta y contrata y PR-GDP 6.2 1-10 Procedimiento término de la relación laboral para el personal a honorarios) de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.

La revisión de los derechos de acceso en caso de movilidad del funcionario de planta, contrata u honorario, se regula mediante el PR-GDP-6.2.1-01 Procedimiento de movilidad o promoción interna de los trabajadores FOSIS.

5.2.3 Responsabilidad de los usuarios

Todos los funcionarios o terceros que tengan acceso a los activos de información del FOSIS deben conocer y cumplir con el uso de esta política específica **y toda la normativa vigente**[1], donde se dictan pautas sobre derechos y deberes con respecto al uso adecuado de los activos de información.

[1] **Ver toda la normativa disponible en intranet**
https://fosis.sharepoint.com/sites/Intranet/SAF/InformaticayTelecomunicaciones/Seguridad%20de%20la%20informacion/Forms/AllItems.aspx

5.2.4 Control de Acceso a la Red

Las conexiones no seguras a los servicios de red pueden afectar a toda la institución, por lo tanto, se controla el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios no comprometan la seguridad de estos.

Las reglas de acceso a la red a través de los puertos estarán basadas en la premisa "todo está restringido, a menos que este expresamente permitido".

5.2.4.1 Política de utilización de los servicios de red

Todos los usuarios internos y externos deben cumplir el procedimiento para la activación y desactivación de derechos de acceso a las redes, el cual comprende:

- El control del acceso a los servicios de red tanto internos como externos.
- La identificación de las redes y servicios de red a los cuales se permite el acceso.
- La aplicación de normas y procedimientos de autorización de acceso entre redes.

5.2.4.2 Autenticación de usuarios para conexiones externas

El Departamento de **Informática y telecomunicaciones** contempla como servicios de conexiones externas SSL, VPN y primarios para funcionarios cualquiera sea su calidad (planta, contrata y honorarios), que requieran conexión remota a la red de datos institucional. Este servicio también puede ser accedido a proveedores con expresa autorización de un funcionario responsable de este acceso.

5.2.4.3 Identificación de equipos en la Red

El Departamento de **Informática y telecomunicaciones** controla e identifica los equipos conectados a su red, mediante el uso de controladores de dominio, asignación manual de rango de IP, clave de seguridad para la conexión WIFI. Además, identifica los equipos de acuerdo con el nombre de usuario asignado como el siguiente modelo ejemplo: FC_rvercoutere, para identificar la región y el usuario responsable del equipo.

5.2.4.4 Protección de los puertos de configuración y diagnóstico remoto

Los puertos que permitan realizar mantenimiento y soporte remoto a los equipos de red, servidores y equipos de usuario final, está restringido a los administradores de red o servidores.

Los usuarios finales de toda la institución deben permitir tomar el control remoto de sus equipos para el Departamento de **Informática y telecomunicaciones**, teniendo en cuenta no tener archivos con información sensible a la vista ni desatender el equipo mientras que se tenga el control del equipo por un tercero.

5.2.4.5 Separación de redes

El Departamento de **Informática y telecomunicaciones** utiliza dispositivos de seguridad —firewalls, para controlar el acceso de una red a otra.

La segmentación se realiza en equipos de enrutamiento mediante la configuración de lista de control de acceso y configuraciones de VLAN en los equipos de comunicaciones layer 3 de acuerdo con el PR -SDI.A.13.01.03 Procedimiento para la segregación de redes.

5.2.4.6 Control de conexión de las redes

La seguridad para las conexiones WiFi es WPA2 o superior.
Dentro de la red de datos institucional se restringe el acceso a:

- Servicios de escritorio remoto a través de internet.
- Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de esta.

5.2.4.7 Control de enrutamiento de red

El Departamento de **Informática y telecomunicaciones** provee a través de sus ISP (Proveedor de Servicio de Internet) el servicio de internet institucional y es el único servicio de internet autorizado.
El uso de internet está regulado por perfilamiento de navegación definido en la institución.

5.2.5 Control de Acceso al Sistema Operativo

5.2.5.1 Registro de inicio seguro

El acceso a los sistemas operativos está regulado por el procedimiento PR-SSI: 9.4.2-01

5.2.5.2 Gestión de contraseñas

La asignación de contraseñas se controla a través del procedimiento PR-SSI: 9.4.3-01

5.2.5.3 Uso de utilitarios del sistema

El uso de utilitarios licenciados del sistema está restringido a usuarios administradores.
En el controlador de dominio, se define una política que no permite la instalación de software y cambios de configuración del sistema. Ningún usuario final tiene privilegios de usuario administrador.

5.2.5.4 Limitación de tiempo de conexión

El Departamento de **Informática y Telecomunicaciones**, no limita el tiempo de conexión, ni establece restricciones en la jornada laboral.

5.2.5.5 Control de acceso a la información

El Departamento de **Informática y Telecomunicaciones,** identifica según los niveles de clasificación de información cuáles sistemas considera sensibles y que deben gestionarse desde ambientes tecnológicos aislados e independientes.

5.2.6 Computación Móvil y Trabajo Remoto

Teniendo en cuenta las ventajas de la computación móvil y el trabajo remoto, así mismo el nivel de exposición a amenazas que pongan en riesgo la seguridad de la información institucional, a continuación, se establecen directrices que permiten regular el uso de la computación móvil y trabajo remoto.

5.2.6.1 Computación y comunicaciones móviles[2]

Se entiende como dispositivos de cómputo y comunicación móviles **institucionales**, todos aquellos que permitan tener acceso y almacenar información institucional, desde lugares diferentes a las instalaciones.

El uso de equipos de cómputo y dispositivos de almacenamiento móviles está restringido únicamente a los provistos por la institución y contempla las siguientes directrices:

- Uso de usuario y contraseña para acceso al mismo.
- Uso de software antivirus provisto por el Departamento de **Informática y Telecomunicaciones.**
- Restricción de privilegios administrativos para los usuarios.
- Uso de software licenciado y provisto por el Departamento de **Informática y Telecomunicaciones.**
- Realización de copias de seguridad periódicas.
- Permanecer siempre cerca del dispositivo.
- No dejar desatendidos los equipos.
- No llamar la atención al portar equipos móviles.
- No identificar el dispositivo con distintivos del Departamento de **Informática y Telecomunicaciones**.
- No colocar datos de contacto técnico en el dispositivo.
- Mantener cifrada la información clasificada.
- No conectarse a redes WIFI-públicas.
- Mantener apagado el Bluetooth o cualquier otra tecnología inalámbrica que exista o llegara a existir.
- Informar de inmediato al Departamento de **Informática y Telecomunicaciones,** sobre la pérdida o hurto del dispositivo para proceder al bloqueo del usuario.
- Para dispositivos de comunicación móvil (telefonía celular) institucionales se aplicarán los controles antes mencionados y los detallados a continuación:
    - Activar la clave del teléfono, para acceso a la agenda telefónica, mensajes de texto, llamadas entrantes, salientes, perdidas. Archivos de voz, imagen y videos.
    - No hablar de temas confidenciales cerca de personas que no requieran conocer dicha información.

5.2.6.2 Trabajo remoto

El trabajo remoto **está regulado por la política para el trabajo remoto[3]**.

6. DIFUSIÓN

[2] **Ver también: Política de uso de dispositivos móviles, Política de trabajo remoto**

[3] **Política SSI-A-6.02.02 Política para el trabajo remoto**
https://fosis.sharepoint.com/sites/Intranet/SAF/InformaticayTelecomunicaciones/Seguridad%20de%20la%20informacion/A.06.02.02%20Pol%C3%ADtica%20para%20el%20trabajo%20remoto.pdf

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.

7. SANCIONES

El incumplimiento de las obligaciones emanadas de esta política y todos sus procedimientos asociados es 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 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. TABLA DE MODIFICACIONES

Versión	Fecha de Aprobación	Motivo del Cambio
1	17/11/2017	Puesta en marcha de la política
2	06/09/2019	Actualiza logo Actualiza objetivo y alcance Actualiza normativa (Res. Política general de seguridad de la información) Actualiza Roles y responsabilidades (Jefe TIC, ahora Jefe de Soporte y Operaciones TIC)
3	**29/11/2021**	**Actualiza cargo jefe de informática y telecomunicaciones** **Actualiza normativa vigente**