1. OBJETIVO

Garantizar la seguridad del trabajo remoto implementando medidas de apoyo a la seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo fuera de las instalaciones del FOSIS.

2. ALCANCE

Es aplicable a todos los usuarios del Fondo de Solidaridad e Inversión Social ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, que en el desarrollo de sus funciones deban realizar trabajo remoto y utilicen computadores de propiedad del FOSIS.

Norma NCh-ISO 27001:2013 control:

- A.6.2.2 Trabajo Remoto

3. DOCUMENTOS RELACIONADOS

- Política general de seguridad de la información del Fondo de Solidaridad e Inversión Social FOSIS, vigente, sus políticas y procedimientos vigentes.
- NCh-ISO 27001 Of2013 – 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.
- Ley 21.220 de 2020 que modifica el código del trabajo en materia de trabajo a distancia del Ministerio del Trabajo y Previsión Social.
- Oficio Circular N°10 de 18 de marzo de 2020, de los Ministerios de Hacienda e Interior, que imparte lineamientos a los Jefes Superiores de Servicio en relación con trabajo remoto, servicios mínimos indispensables, por alerta sanitaria provocada por brote de COVID-19.
- Guías técnicas de la Asociación Chilena de Seguridad para trabajo remoto.

Elaborado por:	Revisado por:	Aprobado por:
Roxana Vercoutere Carter Profesional Depto. Procesos y Mejora Continua **José Ariza Lobos** Encargado de Seguridad Soporte y Operaciones TIC	**Gabriel Rosales Villarroel** Jefe Departamento de Soporte y Operaciones TIC	**Ramón Mellado Quiroz** Encargado de Seguridad de la Información Subdirector de Desarrollo e Innovación
	Gabriel Fernando Rosales Villarroel Firmado digitalmente por Gabriel Fernando Rosales Villarroel Fecha: 2020.04.20 19:12:15 -04'00'	Ramon Luis Mellado Quiroz Firmado digitalmente por Ramon Luis Mellado Quiroz Fecha: 2020.04.20 17:14:01 -04'00'
Fecha: 20/04/2020	Fecha:	Fecha:

4. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
Encargado de Seguridad	Asegurar que se cumplan los requisitos de esta norma para minimizar los riesgos del trabajo remoto.
Subdirector de Administración y Finanzas	Asegurar la seguridad física de las instalaciones, edificios y su entorno. Contar con el inventario físico de todos los equipos FOSIS.
Jefe de Gestión de Personas	Mantener actualizados los perfiles de cargos y la autorización de accesos a los sistemas e información de FOSIS de acuerdo a lo establecido en los procedimientos de contratación de personal de planta y contrata y de contratación a honorarios.
Jefe Departamento de soporte y operaciones TIC	Definir la configuración de seguridad estándar para el trabajo remoto Evaluar, definir y autorizar tanto el uso como la adquisición de computadoras en el FOSIS.
Encargado Ciberseguridad	Es responsable de la seguridad informática del servicio y velar por las medidas de seguridad establecidas para realizar el trabajo remoto.
Funcionarios de planta, contrata, honorarios, consultores externos y prestadores que realicen trabajos en FOSIS	Administrar los datos contenidos en el dispositivo móvil a su cargo, manteniendo el debido resguardo. Registrar la salida de dispositivos móviles y su tiempo de uso en la plataforma dispuesta por la institución Resguardar la confidencialidad, integridad y disponibilidad de la información a la que se accede dentro y fuera de la institución.

5. POLÍTICA

5.1. De la necesidad de acceder a trabajo remoto

Las funciones que realizan algunos trabajadores durante un viaje, o cuando están fuera del lugar habitual de trabajo, sumados a las diferentes modalidades de trabajo remoto implican necesariamente conceder permisos para acceso remoto, es por ello que no se debe descuidar la seguridad y la protección de la información y los datos de la organización.

En este documento, se establecen las condiciones, restricciones, procedimientos y mecanismos operativos necesarios para permitir el acceso remoto con seguridad.

5.2 La seguridad física de las instalaciones, edificios y su entorno.

Los trabajadores deben proteger sus contraseñas de acceso de acuerdo con lo establecido en el procedimiento de gestión de claves, y no compartirlas con nadie, ni siquiera con los miembros de su familia (Política de controles criptográficos y control de claves).

No se deben realizar actividades ilícitas ni vulnerar las políticas de seguridad del FOSIS o utilizar el acceso remoto suministrado para obtener lucro comercial.

La Organización deberá responsabilizarse de proveer la infraestructura computacional necesaria para sus trabajadores, incluyendo en ella toda la configuración necesaria para el correcto desempeño de sus funciones de manera remota.

Cualquier funcionario al que se le autorice el acceso remoto, deben comprometerse a configurar sus dispositivos de tal forma que, al terminar la sesión, se deshabiliten las opciones de acceso remoto.

Debe justificarse la necesidad de acceder a los datos internos o al sistema. Lo anterior, debe ser solicitado a través de la jefatura directa del funcionario por los canales que FOSIS proporciona para ello.

Los datos transmitidos durante una sesión de acceso remoto deben encriptarse (ver política de Política para el uso de controles Criptográficos y Gestión de Claves). Se prohíbe el almacenamiento y procesamiento de los datos en infraestructura externa a la provista por el FOSIS, para esto, la Organización entrega todos los mecanismos de almacenamiento virtual para prevenir la pérdida o manipulación de información en medios locales.

La capacidad de los usuarios de acceso remoto es limitada por el departamento de soporte y operaciones TIC, quién limita a ciertas operaciones y aplica las políticas sobre la eliminación de la autorización, devolución de equipos o cambio de contraseñas, cuando las actividades de trabajo remoto finalizan o dejan de realizarse.

Cada conexión es registrada para asegurar la trazabilidad en caso de un incidente. El acceso no autorizado a estos registros debe ser investigado y atendido de acuerdo con el procedimiento de gestión de incidentes.

5.3 Reglas para eliminar la exposición potencial derivada del uso no autorizado.

Asegurar, controlar y encriptar mediante el uso de firewalls y redes virtuales VPN seguras.
En caso de autorizarse, y por motivos fundados el uso de un dispositivo BYOD[1], el host debe cumplir con los requisitos definidos en la política de configuración de software y hardware de FOSIS.
Los equipos de los usuarios que deban conectarse a la red de la Institución deben contar con un antivirus, el cual debe mantenerse actualizado.
Los usuarios deben aceptar las políticas de la organización al momento de acceder.

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.

[1] Bring Your Own Device , dispositivo propio.

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. 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	17/04/2020	Publicación y difusión