NNH/PMD/OPO/GRV/CSG/RVC/FMZ/MLR

RESOLUCION N° 0114

MAT.: APRUEBA POLITICA PARA EL TRABAJO REMOTO.

SANTIAGO, 28-11-2024

VISTOS

Lo dispuesto en la Ley N° 18.989, en su Título II sobre el Fondo de Solidaridad e Inversión Social; Ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado; En la Ley 21.180 de Transformación digital del Estado; Ley N° 18.575 de Bases Generales de Administración del Estado; Ley 21.640 de Presupuesto para el año 2024; la Resolución Nº 7/2019 que fija Normas sobre Exención del Trámite de Toma de Razón de la Contraloría General de la República; en el Decreto Supremo N° 15/2022, del Ministerio de Desarrollo Social y Familia, que nombra a persona que indica en el cargo de Director Ejecutivo del Fondo de Solidaridad e Inversión Social; y demás antecedentes tenidos a la vista.

CONSIDERANDO

1°.- Que, El Fondo de Solidaridad e Inversión Social – FOSIS, es un Servicio Público funcionalmente descentralizado, con personalidad jurídica y patrimonio propio, regulado por el Título II de la Ley 18.989, cuya misión es contribuir a la superación de la pobreza y vulnerabilidad social a través de estrategias que fortalezcan la cohesión social, las habilidades y capacidades de personas, familias y comunidades, con pertinencia territorial y enfoque de género y su finalidad es financiar en todo o en parte planes, programas, proyectos y actividades especiales de desarrollo social.

2.- El Memorándum FC.MEM. 00382-2024 de fecha 30 de octubre de 2024, enviado por doña Roxana Vercoutere Carter, encargada de Ciberseguridad del FOSIS en el que solicita formalizar mediante un acto administrativo la aprobación de la política para el trabajo remoto, Política-SSI-A-6.7 Versión 2 del 24 de octubre de 2024, adjuntando una copia firmada.

3.- Que resulta necesario garantizar la seguridad del trabajo en forma remota, implementando medidas de seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo fuera de las instalaciones FOSIS.

4.- Que, en virtud del principio de formalidad que rige los actos de la Administración establecido en el artículo 3 de la Ley N° 19.880, es necesario dictar un acto administrativo aprobatorio respectivo.

RESUELVO

APRUEBASE la política para el trabajo remoto Política-SSI-A-6.7 Versión 2 del 24 de octubre de 2024, y cuyo texto es el siguiente:

FOSIS Ministerio de Desarrollo Social y Familia — Gobierno de Chile	**POLÍTICA PARA EL TRABAJO REMOTO**	Fecha emisión: 17/04/2020
		Versión: 2
	POLÍTICA-SSI-A-6.7	**Fecha versión: 24/10/2024**

1. OBJETIVO

Garantizar la seguridad del trabajo en forma remota, implementando medidas de 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

Esta política se aplica a todos los trabajadores y terceras partes que tengan o no una relación directa o indirecta de acceso a la información que pueda afectar los activos de información del FOSIS También se aplica a cualesquiera de sus relaciones con terceros que impliquen el acceso a sus datos, utilización de sus recursos o a la administración y control de sus sistemas de información.

Esta política rige independientemente del lugar en el trabajador presta sus servicios a la Institución, total o parcialmente, e indistintamente de la modalidad de trabajo ya sea “presencial”, “a distancia”, “teletrabajo” u otra, en las condiciones que establezca la legislación vigente, los planteamientos de la Dirección del Trabajo o los Estados de Excepción Constitucional decretados por el Presidente de la República.

Esta política gobierna la seguridad de la información de todos los procesos estratégicos de FOSIS, establecidos en el documento denominado Definiciones Estratégicas o equivalente, cubriendo a toda la Institución independiente de su ubicación geográfica en el país (Chile Continental, Chile Insular o la Antártica Chilena).

Norma NCh-ISO 27001:2023 control:

- **A 6.7 Trabajo a distancia**
- **A.7.6 Trabajo en áreas seguras**
- **A 7.9 Seguridad fuera de las instalaciones**

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 Of2023 – Seguridad de la Información, Ciberseguridad y Protección de la Privacidad – Sistemas de gestión de la seguridad de la información -Requisitos.
- 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.
- Ley 21.220 de 2020 que modifica el código del trabajo en materia de trabajo a distancia.

- Circular IF 463 27 de marzo de 2024 Deroga instrucciones dictadas con motivo de la alerta sanitaria por coronavirus 2019-NCOV
- Guías técnicas de la Asociación Chilena de Seguridad para trabajo remoto.
- Recomendaciones psicológicas en teletrabajo
- Instructivo Marcación remota

Elaborado por: **Roxana Vercoutere Carter** **Encargada de Ciberseguridad**	**Revisado por:** **Gabriel Rosales Villarroel** **Jefe Departamento de Tecnologías de la Información y Telecomunicaciones**	**Aprobado por:** **Cristian Salomó González** **Encargado de Seguridad de la Información** **Subdirector de Usuarios**
		
Fecha: 24/10/2024	Fecha:	Fecha:
Documento Impreso – Copia no controlada sin timbre original		

4. ROLES Y RESPONSABILIDADES

ROL	RESPONSABILIDAD
Encargado de Seguridad	Asegurar que se cumplan los requisitos de esta política para minimizar los riesgos del trabajo a distancia.
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 con lo establecido en los procedimientos de contratación de personal de planta y contrata y de contratación a honorarios.
Jefe Departamento de Tecnologías de la información y Telecomunicaciones	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	Velar por las medidas de seguridad establecidas para realizar el trabajo a distancia.
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. Definiciones Estratégicas

FOSIS, a través de su comité de seguridad de la información, establece las características mínimas obligatorias de seguridad de la información, confidencialidad, integridad y disponibilidad, para abordar el trabajo a distancia y teletrabajo.

Es trabajo a distancia o remoto aquel en el que el trabajador presta sus servicios, total o parcialmente, desde su domicilio u otro lugar o lugares distintos de los establecimientos, instalaciones o faenas.

Se denomina teletrabajo si los servicios son prestados mediante la utilización de medios tecnológicos, informáticos o de telecomunicaciones o si tales servicios deben reportarse mediante esos medios.

En este contexto FOSIS incorpora esta modalidad de trabajo bajo la ley vigente[1] e introduce consideraciones de ciberseguridad para que estas labores se desempeñen sin poner en riesgo la información ni los activos de información en general.

5.2. 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, por lo que no se debe descuidar la seguridad y la protección de la información y los datos de la Institución.

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

5.3. 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 contraseñas vigente, y no compartirlas con nadie, ni siquiera con los miembros de su familia (Política de controles criptográficos y gestión 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.

FOSIS debe 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, debe 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 Institución entrega todos los mecanismos de almacenamiento virtual para prevenir la pérdida o manipulación de información en medios locales[2].

La capacidad de los usuarios de acceso remoto es limitada por el **área de operaciones y seguridad informática**, 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.

---

[1] Ley 21.220 de 2020.

[2] https://fosis.sharepoint.com/

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[3].

5.4. 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[4], 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 Institución al momento de acceder.

5.5. TRABAJO A DISTANCIA Y TELETRABAJO

Por la complejidad y transversalidad del concepto se implementan las medidas que apoyan la seguridad para proteger la información a la que se accede, procesa o almacena en los sitios de trabajo a distancia y de teletrabajo.

5.5.1. Definiciones estructurales:

Las definiciones fundamentales que se tendrán en consideración en todas las políticas en las que se integre el concepto de “trabajo a distancia” o “teletrabajo” serán las establecidas en la Ley N°21.220:

Trabajo a distancia:
Es trabajo a distancia aquel en el que el trabajador presta sus servicios, total o parcialmente, desde su domicilio u otro lugar o lugares distintos de los establecimientos, instalaciones o faenas.

Teletrabajo:
Se denomina teletrabajo si los servicios son prestados mediante la utilización de medios tecnológicos, informáticos o de telecomunicaciones o si tales servicios deben reportarse mediante estos medios.

5.5.2. condiciones del uso del trabajo a distancia y del teletrabajo

Cada unidad organizacional establece:

- que funcionarios están en condiciones de realizar trabajo a distancia o teletrabajo.
- que roles son los que se consideran dentro de los posibles de incorporar.
- Que información o sistemas son lo que necesitan (previa validación con Unidad TIC)

La Unidad TIC establece:

- que servicios están disponibles para teletrabajadores
- los tipos de servicios de red y aplicaciones
- los esquemas de identificación, autenticación y autorización, es decir, cómo deben identificarse los teletrabajadores, autenticarse y recibir la autorización antes de acceder a los recursos del FOSIS.
- Especificaciones de equipos y software: ¿hay algún dispositivo específico o producto de software que deba implementarse en el equipo del teletrabajador? (por ejemplo, firewall, pendrive encriptado o software de encriptación).
- Integridad y confidencialidad: cómo debe protegerse la conexión desde el equipo remoto (es decir, VPN) y cómo deben protegerse los datos en dicho equipo.
- Pautas de mantenimiento: ¿cómo debe ser la configuración equipo del teletrabajador?
- Directrices del usuario: que aclaren el papel del usuario en la protección de los recursos, por ejemplo, uso apropiado de los recursos; el usuario no debe modificar las configuraciones de seguridad; utilizar de software antivirus; almacenamiento de datos corporativos en unidades locales; uso de encriptación herramientas.

[3] Se debe registrar el incidente en el registro de incidentes de seguridad de la información
[4] Bring Your Own Device, dispositivo propio.

El comité de Seguridad de la Información debe velar por que se cumplan las siguientes exigencias normativas:

- la seguridad física existente del sitio de teletrabajo, considerando la seguridad física del edificio y del entorno local;
- el entorno de teletrabajo físico propuesto;
- los requisitos de seguridad para las comunicaciones, considerando la necesidad de contar con acceso remoto a los sistemas internos de la Institución, la sensibilidad de la información a la que se accede y que se traspasa por el enlace de comunicaciones y la sensibilidad del sistema interno;
- la provisión de acceso a un escritorio virtual que evite el procesamiento y el almacenamiento de información en equipos de propiedad privada;
- la amenaza del acceso no autorizado a la información o a los recursos de parte de otras personas que utilizan el recinto, es decir, la familia y los amigos;
- el uso de redes domésticas y los requisitos o restricciones en la configuración de los servicios de redes inalámbricas;
- las políticas y procedimientos para evitar disputas en cuanto a los derechos de propiedad intelectual desarrollados en equipos de propiedad privada;
- acceso a equipos de propiedad privada (para verificar la seguridad de la máquina durante una investigación), lo que se puede evitar por legislación;
- acuerdos de licenciamiento de software que pueden hacer que la Institución se haga responsable del software en estaciones de trabajo de propiedad privada de empleados o de usuarios externos;
- requisitos de protección de malware firewall (cortafuegos).
- Las pautas y disposiciones que se deben incluir son:
    a) la provisión de equipos idóneos y muebles de almacenamiento para las actividades de teletrabajo, donde no se permite el uso de equipos de propiedad privada que no estén bajo el control del FOSIS;
    b) una definición del trabajo permitido, las horas de trabajo, la clasificación de información que se puede tener y los sistemas y servicios internos que se autoriza al teletrabajador a acceder;
    c) la provisión de equipos de comunicación idóneos, incluidos los métodos para proteger el acceso remoto;
    d) seguridad física;
    e) normas y orientación sobre el acceso a familiares y visitas a los equipos y a la información;
    f) la provisión de soporte y mantenimiento de hardware y software;
    g) la provisión de seguros;
    h) los procedimientos para el respaldo y la continuidad en el negocio;
    i) auditoría y monitoreo de seguridad;
    j) revocación de autoridad y derechos de acceso y la devolución de los equipos cuando concluyen las actividades de teletrabajo.
    k) Siempre se debe evaluar incorporar las recomendaciones y buenas prácticas sugeridas por el CSIRT de Gobierno.

5.5.3. consideraciones del uso del trabajo a distancia y del teletrabajo

- Las principales consideraciones que deben contemplar los jefes de cada una de las unidades son:
- Restricciones de información
- ¿hay tipos de información confidencial/interna/sensible que no deben estar a disposición de los teletrabajadores?
- Analizar los privilegios que necesita el teletrabajador para aplicarlos bajo el principio de los mínimos privilegios (en cuando acceso a la plataforma de sistemas) para funcionar.
- El equipo del teletrabajador debe estar protegido, actualizado y monitoreado.

- Educación del usuario: los usuarios deben conocer y entender los posibles riesgos de la información asociados con el teletrabajo, cómo se abordan esos riesgos y el papel del usuario en minimizar los riesgos.
- La seguridad en modalidad de trabajo a distancia o teletrabajo no debe ser inferior a la seguridad mínima exigida en modo presencial.

5.5.4. medidas que apoyan la seguridad para proteger la información a la que se accede, procesa o almacena en los sitios de trabajo a distancia o de teletrabajo

- Modo de operación
- La activación del trabajo remoto debe estar previamente autorizada por el jefe de la unidad correspondiente y los usuarios definidos deben tener sus anexos de contrato firmados y validados por sus jefaturas correspondientes y con su equipamiento de trabajo debidamente asignado.

5.5.5. Consejos preventivos para teletrabajo

- Habilitar una zona dentro de tu hogar con suficiente espacio para contener los equipos y materiales de trabajo.
- Aislar los ruidos externos y los propios de la casa
- Controlar la iluminación, temperatura y ventilación de lugar definido.
- Es conveniente disponer de luz natural, esta disminuye el riesgo de fatiga visual.
- Evite consumir alimentos y líquidos cerca del su equipo, podría dañarlo.
- Evite cableado eléctrico suelto, fíjelo cosa de evitar accidentes.
- Utilice pausas de trabajo para consumir alimentos.
- Si tiene cansancio o pérdida de concentración realice un descaso.

5.5.6. Medidas de seguridad

- A modo de “mejores prácticas” se deben promover e implementar las siguientes medidas de seguridad, asociadas al uso de computadores utilizados bajo modalidad de teletrabajo:
- Usar protector de pantalla con clave cuando el computador no esté en uso.
- No usar Pendrive/Flash Drive en los computadores.
- Bloquear puertos USB del equipo para periféricos de almacenamiento externos. Es importante mencionar que en caso de excepciones previamente autorizadas podrán ser habilitados para tal efecto en forma temporal.
- Fomentar la costumbre de: “Darle a los bienes el mismo cuidado que le daría Ud. Como si fuera el propio”.
- El usuario debe asegurarse de que su equipo cuenta con el software antivirus, el cuál debe ser actualizado por lo menos una vez por semana.
- Queda estrictamente prohibido que el personal conecte a la red equipos o dispositivos que no sean de FOSIS, salvo que algún apolítica específica lo autorice y regule, acogiendo conceptos como BYOD.
- Quedará prohibido la conexión a redes que no sean del FOSIS mientras se encuentre en dependencias de la ésta.
- Queda prohibido la descarga de aplicaciones o software no autorizado por parte de los usuarios en particular para aquellos definidos con acceso remoto.
- El usuario es responsable de copiar, en forma periódica, los archivos de trabajo que residan en su PC; para ello, deberá copiarlos en el servidor que está disponible en la red para estos efectos
- Tics controlará el direccionamiento IP y dirección física de los dispositivos mediante la dirección MAC

5.5.7. Instalación de software base

A todo equipo, antes de ser asignado para trabajo remoto, se le debe instalar el siguiente software base:

- Sistema operativo debidamente licenciado y aprobado por el FOSIS.
- Drivers internos y de periféricos utilizados en el FOSIS.
- Actualizaciones, probadas en el FOSIS.

- Software de ofimática debidamente licenciado.
- Antivirus corporativo.
- Cliente Firewall activo.
- Compresor de archivos utilizado por el FOSIS.
- Aplicaciones requeridas y utilizadas por el FOSIS.
- Visualizador de PDF de ser requerido.
- Java (JRE = Java Runtime Environment), de ser requerido.
- Browser actualizado, como navegador de Internet.
- Acceso VPN .

Una vez que el computador tenga todo el software base instalado, pasa a llamarse Dispositivo para trabajo remoto y puede ser asignado a un usuario.

5.5.8. Registro e inventario de equipos y software instalado

- El inventario está a cargo de la unidad de Inventario de equipos y debe identificar claramente[5]:
    - el modelo
    - la serie del equipo
    - su dueño
    - el nivel de criticidad (alto, medio o bajo)
    - el tipo de acceso que el usuario tendrá (local, remoto)
    - N° de IP
    - características del equipo (Ram, DD, CPU)
    - otros antecedentes que sean importantes a considerar.

Tics posee un registro de equipos conectados a los servicios de Active Directory que le permite identificar claramente el equipo conectado.

5.5.9. Cuidados especiales para trabajo remoto

- Protector de pantalla con clave activado y con tiempo de activación inferior a 5 minutos.
- Evitar navegar por sitios desconocidos.
- No descargue música, videos, películas o programas desde Internet.
- No instale ninguna aplicación en los equipos móviles que no sea autorizada y supervisada por área de TI
- Evite ingresar a sitios desde publicidad en páginas web.
- Si el remitente de un mail no es seguro o es extraño, ¡Nunca abra los archivos adjuntos!
- Mantenga su antivirus actualizado.
- Revisiones periódicas (diarias) de su equipo para asegurar que esté actualizado (antivirus y sistema operativo).

5.5.10. Consideraciones especiales en trabajo remoto:

Contacte vía teams a la Unidad TIC cuando:

- su equipo no se pueda conectarse a internet.
- su equipo no se pueda conectarse a alguna aplicación.
- su equipo no se encienda.
- su conexión VPN no funcione.

5.5.11. Aspectos mínimos para verificar la operatividad de la política

- Normativa de protección del puesto de trabajo remoto.
- Informar al personal sobre la normativa de protección del puesto de trabajo fuera de la oficina llevando a cabo auditorías periódicas para asegurar su cumplimiento.
- Relación de usuarios que disponen de la opción de trabajar en remoto.
- Llevar un control de las personas que, por su perfil dentro del FOSIS o las características de su trabajo, tienen la opción de teletrabajar.
- Procedimientos para la solicitud y autorización del teletrabajo.

[5] Ver Procedimiento para la gestión de activos

    - Redactar un documento donde se contemplen todas las cuestiones relativas al teletrabajo (duración de este, dispositivos facilitados, etc.), que es firmado por cada teletrabajador.
- Periodo de implantación y pruebas.
    - Valorar diferentes escenarios y configuraciones antes de habilitar el teletrabajo, contemplando todos los riesgos de seguridad.
- Realizar pruebas de carga en escenarios simulados.
    - Si existe un volumen considerable de empleados que van a teletrabajar al mismo tiempo, valorar la carga que esto ocasiona en los sistemas internos del FOSIS.
- Aplicaciones y recursos a los que tiene acceso cada usuario.
    - Dar acceso a cada empleado solo a las aplicaciones y recursos necesarios para llevar a cabo su trabajo, dependiendo de su perfil dentro del FOSIS. Detallar las aplicaciones permitidas, así como sus condiciones de uso. Valorar la inclusión del nuevo software solicitado por los empleados.
- Acceso seguro.
    - Gestionar las credenciales de acceso de los empleados forzando el uso de contraseñas robustas y su cambio periódico, además de incluir el doble factor de autenticación siempre que sea posible.
- Configuración de los dispositivos de teletrabajo.
    - Configurar los dispositivos utilizados por el empleado para teletrabajar (sistema operativo, antivirus, control de actualizaciones, etc.), tanto si son corporativos como si son aportados por el trabajador (BYOD).
- Cifrado de los soportes de información.
    - Implantar tecnologías de cifrado que protegen la información de posibles accesos malintencionados.
- Definición de la política de almacenamiento en los equipos de trabajo y en la red corporativa.
    - Elaborar las políticas que detallan a los empleados dónde deben guardar la información con la que trabajan en remoto.
- Planificación de las copias de seguridad de todos los soportes.
    - Comprobar regularmente que se realizan periódicamente y que pueden restaurarse.
- Uso de conexiones seguras a través de una red privada virtual o VPN.
    - Implementar una red VPN extremo a extremo que permite que la información que se intercambia entre los equipos del FOSIS viaje cifrada a través de Internet.
- Aplicaciones de escritorio remoto siempre a través de una VPN.
    - Para ofrecer un extra de seguridad y privacidad a las comunicaciones, solo se permite el uso de las aplicaciones de escritorio remoto bajo una VPN.
- Virtualización de entornos de trabajo.
    - Valorar la implementación de la virtualización como método para proporcionar a cada empleado su propio espacio de trabajo, eliminando los riesgos asociados al uso de un dispositivo físico.
- Priorizar el uso de dispositivos corporativos.
    - Elegir los dispositivos corporativos para teletrabajar, ya que cuentan con las políticas de seguridad que la empresa considera necesarias y tienen instalado el software preciso para realizar el trabajo de forma segura.
- Conexión a Internet.
    - Cuando no es posible utilizar la red doméstica para teletrabajar o cualquier otra red considerada segura como alternativa, utilizar la red de datos móvil 4G o 5G siempre evitando la conexión a redes wifi-públicas.
- Uso de dispositivos personales bajo una política BYOD.
    - Utilizar las configuraciones y conexiones permitidas y seguras al teletrabajar desde tus dispositivos personales.
- Concienciar a los empleados antes de empezar a teletrabajar.
    - Educar a los empleados en ciberseguridad antes de que comiencen a teletrabajar para que conozcan las políticas y las medidas que se llevaran a cabo en la empresa.
- Cumplimiento Ley de Datos Personales.

- Educar a los empleados que manejan datos personales para la protección de estos durante el teletrabajo y realizar los cambios en los tratamientos para contemplar estas situaciones.

- Aplicaciones de teleconferencia y colaborativas.
  - Configurar estas aplicaciones para un uso seguro que permita que se respeten la privacidad y la propiedad intelectual de los participantes

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.

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 dos 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
2	**24/10/2024**	**Actualiza según normativa vigente**

ANOTESE, COMUNIQUESE Y PUBLIQUESE.

NICOLAS NAVARRETE HERNANDEZ

DIRECTOR EJECUTIVO

FONDO DE SOLIDARIDAD E INVERSIÓN SOCIAL.

Distribución.

1.- Subdirección de usuarios.

2.- Subdirección de administración y finanzas.

3.- Oficina de Partes.

Fecha de Emisión: 2024-11-28 (19:02)

Válido indefinidamente

Código Verificación:

Nicolas Navarrete Hernandez
Director Ejecutivo
FOSIS

Documento firmado con FIRMAGOB
Verifique la validez de este documento escaneando el código QR.