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

**RESOLUCION N°** 0115

**MAT.: APRUEBA POLITICA PARA EL RESPALDO DE INFORMACIÓN Y SOFTWARE.**

**SANTIAGO,** 03-12-2024

**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. 00426-2024 de fecha 22 de noviembre 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 respaldo de información y software, Política -SSI-A-8.13 Versión 3 de fecha 20 de octubre de 2024, adjuntando una copia firmada.

**3.-** Que resulta necesario establecer normas para el respaldo de información en FOSIS para así mantener y probar periódicamente los respaldos de seguridad de la información el software y los sistemas e implementar las instalaciones de tratamiento de información con suficiente redundancia para cumplir con los requisitos disponibles.

**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, corresponde dictar un acto administrativo aprobatorio.

**RESUELVO**

**APRUEBASE** la política para el respaldo de información y software, Política -SSI-A-8.13 Versión 3 fecha 20 de octubre de 2024 compuesta de siete páginas y cuyo texto es el siguiente:

| | | |
|---|---|---|
| FOSIS Ministerio de Desarrollo Social y Familia — Gobierno de Chile | **POLÍTICA PARA EL RESPALDO DE INFORMACIÓN Y SOFTWARE** | Fecha emisión: 13/09/2017<br>Versión: **3** |
| | **POLITICA-SSI-A-8.13** | Fecha versión: **20/10/2024** |

## 1. OBJETIVO

Establecer las normas para el respaldo de información en FOSIS, para **mantener y probar periódicamente los respaldos de seguridad de la información el software y los sistemas e implementar las instalaciones de tratamiento de información con suficiente redundancia para cumplir con los requisitos de disponibilidad.**

## 2. ALCANCE

Esta política se aplica a toda la información contenida en los servidores, estaciones de trabajo y equipos computacionales que contengan datos, configuraciones, aplicativos y servicios críticos para FOSIS.

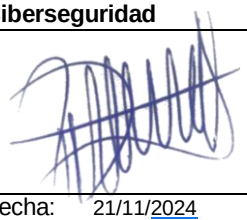
Es aplicable a todos los usuarios, ya sean funcionarios, servidores públicos a honorarios y terceras partes que prestan servicios para el FOSIS.

**Norma NCh ISO 27001:2023 Controles:**

- **5.37 Procedimientos de Operativos documentados**
- **8.13 Respaldo de Información**
- **8.14 Redundancia de Información**
- **8.15 Registro**

## 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.
- Dictamen 28.704, agosto de 1981. Sobre disposiciones y recomendaciones referentes a eliminación de documentos. Contraloría General de la República.
- Decreto N°10/2023 que establece norma técnica de documentos y expedientes electrónicos para la gestión de procedimientos administrativos.
- Decreto N°7/2023 Establece norma técnica de seguridad de la información y ciberseguridad conforma la ley N°21.180.
- Ley 21.663/2024 Ley Marco de Ciberseguridad

| Elaborado por:<br>Roxana Vercoutere Carter<br>Encargada Ciberseguridad | Revisado por:<br>Gabriel Rosales Villarroel<br>Jefe Departamento de Tecnologías de la Información y Telecomunicaciones | Aprobado por:<br>Cristian Salomó González<br>Encargado de Seguridad de la Información<br>Subdirector de Usuarios |
|---|---|---|
|  |  |  |
| Fecha: 21/11/2024 | Fecha: 22-11-2024 | Fecha: 22-11-2024 |
| Documento Impreso – Copia no controlada sin timbre original | | |

## 4. ROLES Y RESPONSABILIDADES

| ROL | RESPONSABILIDAD |
|---|---|
| **Jefe Tecnologías de la Información y Telecomunicaciones** | - **Define el estándar de respaldo para servidores y equipos de hardware.**<br>- **Autoriza solicitudes especiales de respaldo.**<br>- **Mantiene un inventario de activos de información para copia de seguridad.**<br>- **Coordina, ejecuta y supervisa las pruebas de restauración de copias de respaldo.** |
| **Encargado de Transformación Digital** | - Solicita respaldos y/o restauraciones según necesidad.<br>- Realiza pruebas y valida actividades de respaldo en desarrollo de software y sistemas. |
| Responsable de activos de información | - Determinar la utilidad de la información respaldada. |
| Funcionarios, servidores públicos a honorarios y terceras partes | - Dar cumplimiento a la presente política y la normativa del Sistema de Seguridad de la Información. |

## 5. POLÍTICA

El propósito de esta política es permitir recuperación de pérdida de datos o sistemas.

### 5.1 Consideraciones Generales

FOSIS considera que toda la información de sus sistemas informáticos críticos en producción debe ser protegidas de posibles daños, por lo que debe ser respaldada con cierta frecuencia, para asegurar el proceso de recuperación.

Bajo esta premisa, el **Departamento de Tecnologías de la Información y Telecomunicaciones** debe considerar soluciones de respaldo para equipos de escritorio, servidores y aplicaciones (códigos fuentes, bases de datos) que se consideren críticos para la institución, así como también garantizar la disponibilidad de la infraestructura adecuada de respaldo, para asegurar que éstos estén disponibles incluso después de un desastre o falla de un dispositivo.

Igualmente, el **Departamento de Tecnologías de la Información y Telecomunicaciones** debe considerar el respaldo para equipos de escritorio.

La información que no es relevante para el quehacer de la institución y que resida en los servidores y equipos de escritorio, no es respaldada[1]. La utilidad de la información es determinada por el responsable de los activos.

En las situaciones donde la confidencialidad es importante, se deben proteger los respaldos mediante cifrado.

Los medios de respaldo se deben probar de manera regular para garantizar que se puede confiar en ellos frente a su uso ante emergencias; esto se debe combinar con una prueba de los procedimientos de restauración y se debe comprobar contra la restauración según sea necesario, y contra el tiempo de restauración. Se deben realizar pruebas para probar la habilidad de restaurar los datos de respaldo en los medios de prueba, no sobrescribiendo los medios originales en caso de que falle el proceso de respaldo o restauración y provoque daños o pérdidas de los datos.

### 5.1.1 Lineamientos generales de respaldo

- **Se Deben proporcionar instalaciones de copia de seguridad adecuadas para garantizar que toda información esencial y "software" se pueda recuperar tras un incidente o fallo o pérdida de medios de almacenamiento[2].**
- **Se Deben desarrollar e implementar planes sobre cómo la organización hará copias de seguridad de información, "software" y sistemas, para abordar la política específica sobre copias de seguridad.**
- **Al momento de diseñar el plan de respaldo, se deben tener en cuenta los elementos siguientes:**
  - **a) elaborar registros precisos y completos de copias de seguridad y de procedimientos de restauración documentados;**
  - **b) reflejar los objetivos estratégicos institucionales, los requisitos de seguridad de la información implicada y criticidad de información para funcionamiento continuo en el alcance y la frecuencia de copias de seguridad;**
  - **c) almacenar copias de seguridad en una ubicación remota segura, a una distancia suficiente para o escapar de cualquier daño de un desastre en el sitio principal;**
  - **d) dar a la información de respaldo un nivel apropiado de protección física y ambiental consistente con los estándares aplicados en el sitio principal[3];**
  - **e) probar periódicamente los medios de copia de seguridad para garantizar que se puede confiar en ellos para un uso de emergencia cuando sea necesario. Probar la capacidad de restaurar datos de copias de seguridad en un sistema de prueba, no sobrescribiendo el medio de almacenamiento u original en caso de que el proceso de copia de seguridad o restauración falle y cause daños o pérdidas de datos irreparables;**
  - **f) proteger copias de seguridad mediante cifrado en función de riesgos identificados (por ejemplo, en situaciones en las que la confidencialidad es importante);**

**Los equipos operativos deben supervisar la ejecución de copias de seguridad y abordar los fallos de copias de seguridad programadas para garantizar la integridad y estar de acuerdo con esta política en relación con las copias de seguridad.**

### 5.2 Identificación de Información Crítica.

Los responsables de los activos de información y de los distintos procesos, en el nivel central y en las Direcciones Regionales, son los encargados de mantener una relación actualizada de aquella información que sus departamentos necesitan para mantener la continuidad de la operación, durante eventuales procedimientos de restauración.

---

[1] De acuerdo con la política de uso de dispositivos móviles, se debe priorizar el uso de la nube de office 365 disponible para todos/as los/as Trabajadores/as del FOSIS.

2 Ver política de continuidad operacional en intranet

[3] Ver procedimiento perímetro de seguridad física en intranet

**5.3 Frecuencia y tipo de respaldo**

El **Departamento de Tecnologías de la Información y Telecomunicaciones**, debe definir los tipos de respaldos a utilizar como estándar para cada Departamento y Dirección Regional. Cada estándar debe considerar la frecuencia de respaldo, los medios de almacenamiento, tipo de contenidos, tiempo de almacenamiento y borrado de esta información.

La periodicidad con que se realizan los respaldos de los computadores personales o estaciones de trabajo de la institución que están asignados a usuarios, no puede ser menor a un respaldo anual.

Por otro lado, la periodicidad con que se realizan los respaldos de los sistemas informáticos y los equipos considerados críticos no puede ser menor a un respaldo mensual.

**5.4 Protección a los medios de respaldo.**

Las configuraciones de respaldo para los sistemas individuales deben ser probadas con regularidad, a lo menos cada dos años, para asegurar que ellas satisfacen los requisitos estipulados en los planes de continuidad institucionales.

Ante un cambio tecnológico que se produzca en los medios de respaldo, que pueda generar obsolescencia tecnológica, deben generarse las acciones necesarias de resguardo de la información en ellos.

**5.5 Protección de la información en medios de respaldo.**

Para prevenir pérdidas accidentales, se deben respaldar todos los archivos, base de datos e información existente en los sistemas relevantes para la institución, disponibilizar la infraestructura adecuada de respaldo para cada caso, y asegurar su disponibilidad en caso de desastre o falla de un dispositivo.

Para asegurar la continuidad operaciones, los respaldos deben ser almacenados en una ubicación remota.

Dicho respaldo debe tener registros exactos y completos de las copias y procedimientos documentados de restablecimiento.

El respaldo de datos y software críticos se deben almacenar en un lugar protegido, con acceso controlado.

Toda información crítica grabada en respaldos que son almacenados fuera de la institución debe ser traspasada con los elementos de seguridad adecuados, ya sea utilizando métodos de encriptación o utilizar métodos adecuados para prevenir intentos de acceso físico no autorizado.

El **Departamento de Tecnologías de la Información y Telecomunicaciones** debe mantener un inventario actualizado de la información almacenada externamente.

**5.6 Periodo de existencia de las copias de respaldo y su eventual destrucción**

Se debe determinar el periodo de retención de la información esencial para el negocio, considerando cualquier tipo de requisito para archivar copias que se deben retener de manera permanente. Lo anterior, de acuerdo con el ordenamiento jurídico vigente y el uso eficiente del espacio físico disponible para el almacenamiento.

Se debe establecer el período de existencia para las copias de seguridad y los procedimientos a seguir para su destrucción definitiva una vez concluido tal periodo.

**5.7 Respaldo de estaciones de trabajo.**
El **Departamento de Tecnologías de la Información y Telecomunicaciones** debe considerar, dentro de sus recursos asignados, soluciones de respaldo para equipos de escritorio. Siendo los usuarios de la institución los responsables de alojar la información que necesita ser respaldada en los lugares establecidos para ello.

Para la realización de estas copias de respaldo, debe utilizarse la herramienta **por el Departamento de Tecnologías de la Información y Telecomunicaciones**.

**5.8 Pruebas de realización y restauración de las copias de respaldo**
La realización de las pruebas de restauración de las copias de respaldo confirmará el funcionamiento correcto del proceso de recuperación de copias de datos, y garantizará la integridad de los datos que contienen, por lo que se deben realizar pruebas respecto a la restauración de las copias de respaldo, de forma rotativa y con una periodicidad con una regularidad, a lo menos cada seis meses.

**5.9 Automatización y monitoreo**
**El Departamento de Tecnologías de la Información y Telecomunicaciones ha implementado herramientas automatizadas de respaldo y monitorización para asegurar que los respaldos se realicen de acuerdo con la frecuencia establecida y detectar fallos en tiempo real, lo que permite una respuesta rápida y eficiente.**

**5.10 Auditoría y Registro Detallado:**
**Se debe determinar el propósito para el que se crean los registros, qué datos se recopilan, registran y cualquier requisito específico de los registros para protegerlos y manejarlos. Esto se debe documentar.**

**5.10.1 Los registros de respaldos deben incluir:**

- **Identificación del respaldo: Fecha, hora, usuario o sistema responsable de la creación del respaldo, y dispositivo o ubicación donde se almacena.**
- **Verificación de integridad: Resultados de pruebas de verificación para confirmar la integridad de los datos respaldados.**
- **Frecuencia del respaldo: Indicadores de cumplimiento con la periodicidad definida en la política de respaldos.**
- **Estado del respaldo: Éxito o fallo de la operación, incluyendo detalles del error en caso de fallo.**
- **Conformidad con políticas: Verificación de que el respaldo cumple con los requisitos legales y organizacionales.**
- **Actividades relacionadas con la restauración: Detalles de pruebas de restauración realizadas para validar la utilidad del respaldo.**

**5.10.2 Aspectos Específicos para la Auditoría**
**Se deben registrar:**

- **Intentos de respaldo exitosos y fallidos: Incluyendo información sobre el usuario o sistema que inició la actividad.**
- **Verificaciones de respaldos: Resultados de las pruebas automatizadas o manuales que aseguren que los datos respaldados son recuperables y están completos.**
- **Cambios en la configuración del sistema de respaldos: Como modificaciones en rutas**

**de almacenamiento, sistemas de cifrado, o ajustes de política.**

- **Uso de privilegios en actividades de respaldo: Usuarios o sistemas que ejecutaron acciones relacionadas con la configuración o manipulación de respaldos.**
- **Acciones sobre archivos respaldados: Cualquier eliminación, sobreescritura o alteración de archivos en las ubicaciones de respaldo.**
- **Alarmas del sistema: Alertas relacionadas con fallos en los respaldos, intentos de acceso no autorizado o amenazas a la integridad del sistema de respaldo.**
- **Activación y desactivación de medidas de seguridad: Como cifrado de datos respaldados y sistemas de detección de anomalías en el proceso de respaldo.**
- **Pruebas de restauración: Registro detallado de las transacciones ejecutadas para validar la restauración de los datos respaldados.**

**Es importante que todos los sistemas tengan fuentes de tiempo sincronizadas, ya que esto permite la correlación de registros entre sistemas para el análisis, la alerta y la investigación de un incidente.**

### 5.10.3 Protección de los registros[4]

**Los/as usuarios/as, incluidos los que tienen derechos de acceso privilegiados, no deben tener permiso para borrar o desactivar registros de sus propias actividades.**

**Pueden manipular potencialmente registros de instalaciones de procesamiento de información bajo su control directo. Por lo tanto, es necesario proteger y revisar los registros para mantener la responsabilidad de usuarios privilegiados.**

**Los controles deben tener como objetivo proteger contra los cambios no autorizados en información de registro y problemas de funcionamiento con la instalación de registro, incluyendo:**

- **alteraciones de los tipos de mensajes que se registran;**
- **archivos de registro editados o borrados;**
- **falta de registro de eventos o sobreescritura de eventos registrados anteriormente si se excede el medio de almacenamiento que contiene un archivo de registro.**

**Los registros de sistema suelen contener un gran volumen de información, mucha de la cual es ajena a la supervisión de seguridad de información. Para ayudar a identificar los eventos significativos para la supervisión de seguridad de la información, se puede considerar uso de programas de utilidad[5] o adecuados o herramientas de auditoría para realizar la interrogación de archivos.**

**El registro de eventos sienta las bases para sistemas de supervisión automatizados que son capaces de generar informes consolidados y alertas sobre seguridad de sistema.**

---

[4] Ver procedimiento para el registro y monitoreo

[5] Ver procedimiento para la gestión de vulnerabilidades técnicas

## 6. DIFUSIÓN

La comunicación de la presente política se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, mediante los siguientes canales:

- Publicación en la Intranet del 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 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 **dos 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 | 13/09/2017 | Crea Política |
| 2 | 06/09/2019 | Actualiza logo<br>Actualiza documentación relacionada<br>Incorpora responsabilidad del responsable del activo de información |
| **3** | **20/11/2024** | **Actualiza según norma ISO 27001:2022** |

**Distribución:**

- **Todo el país**

**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: 2024-12-03 (17:16)

Válido indefinidamente

Código Verificación:

DOCUMENTO FIRMADO ELECTRÓNICAMENTE
FOSIS

Nicolas Navarrete Hernandez
Director Ejecutivo
FOSIS

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