1. OBJETIVO

Establecer las normas para el respaldo de información en FOSIS, para proteger los datos y software contenidos en los dispositivos de hardware que la soportan, almacenan y distribuyen.

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 27001:2013 Controles:

- 12.03.01 Respaldo de información
- 12.01.01 Procedimientos de operación documentados.

3. DOCUMENTOS RELACIONADOS

- Política general de seguridad de la información del FOSIS, Resolución exenta 0879/12-07-2019
- NCh- ISO 27001:2013 Tecnología de la Información – Técnicas de seguridad – Sistema de gestión de la seguridad de la información – Respaldo de información.
- PR-SSI-A-11-2-7 Procedimiento de seguridad de la eliminación o re uso del equipo.
- Circular 28.704, agosto de 1981. Circular sobre disposiciones y recomendaciones referentes a eliminación de documentos. Contraloría General de la República.

Elaborado por: **Roxana Vercoutere Carter** y **Armando Guajardo San Martín,** Profesionales Depto. Procesos y mejora continua	**Revisado por:** **Gabriel Rosales Villarroel**, jefe Departamento de soporte y operaciones TIC	**Aprobado por:** **Pedro Guerra Araya**, Encargado de Seguridad Subdirector de Desarrollo e Innovación (s)
Fecha:	Fecha:	Fecha:
Documento Impreso – Copia no controlada sin timbre original		

4. ROLES Y RESPONSABILIDADES

ROL	RESPONSABLE
Jefe Departamento soporte y operaciones TIC	Definir el estándar de respaldo de los servidores y equipos de hardware, que detalle los respaldos de software básico, de las aplicaciones, configuraciones de servicios y de los datos en ambiente de producción, autorizar las solicitudes de respaldo especiales. Mantener un inventario de los activos de información sobre los que se realiza copia de seguridad, en el nivel central. Coordinar, ejecutar y velar por la realización de las pruebas y restauración de las copias de respaldo efectuadas utilizando herramientas pertinentes para tales efectos
Jefe Departamento de transformación digital	Solicitar respaldos y/o restauración según la necesidad que se requiere y los recursos disponibles, realizar pruebas y validar que la actividad se realice **en el desarrollo y actualización de software y sistemas.**
Responsable de activos de información	Determinar la utilidad de la información respaldada.
Funcionarios, Planta, contrata, honorarios	Dar cumplimiento a la presente política y la normativa del Sistema de seguridad de la información.

5. POLÍTICA

5.1 Consideraciones Generales

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

Bajo esta premisa, el Departamento de soporte y operaciones TIC 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 cómo también garantizar la disponibilidad de infraestructura adecuada, para asegurar que éstos estén disponibles incluso después de un desastre o falla de un dispositivo.

Igualmente, el Departamento de soporte y operaciones TIC 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. 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.

5.2 Identificación de Información Crítica.

Los responsables 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 procesos necesitan para mantener la continuidad de la operación, durante eventuales procedimientos de restauración.

5.3 Frecuencia y tipo de respaldo

El Departamento de soporte y operaciones TIC, 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 estén asignados a usuarios, no podrá 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 operacional.

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 desastres o falla de un dispositivo.

Para asegurar la continuidad de las 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 se deben almacenar en un lugar protegido, con acceso controlado.

Toda información 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 soporte y operaciones TIC debe mantener un inventario actualizado de la información almacenada externamente.

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

El Departamento de Soporte y Operaciones TIC ha definido como periodo de retención de la información esencial para el negocio el plazo de seis años, considerando la obsolescencia tecnológica de los medios de recuperación. Lo anterior, de acuerdo con el ordenamiento jurídico vigente[1] 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 soporte y operaciones TIC 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 utilizar la herramienta determinada por el Departamento de soporte y operaciones TIC.

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 deberán 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.

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, a lo menos se deberá hacer difusión mediante los siguientes canales:

- Publicación en la intranet de FOSIS.
- Correo informativo.

[1] Circular 28.704, agosto de 1981. Circular sobre disposiciones y recomendaciones referentes a eliminación de documentos. Contraloría General de la República

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 deberá 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	13/09/2017	Crea Política
2	06/09/2019	Actualiza logo Actualiza roles