Transferencia Electrónica de Archivos (TEA)
Normas Técnicas

Fecha de actualización: abril de 2026

Este documento establece los requisitos técnicos y de seguridad para la Transferencia Electrónica de Archivos (TEA) entre la Superintendencia de Pensiones y las instituciones reguladas y no reguladas.

1. Características de los enlaces de comunicaciones

La comunicación con la Superintendencia de Pensiones deberá realizarse mediante enlaces de red que cumplan las siguientes características:

a) La conexión puede implementarse mediante:
   - Enlaces dedicados entre cada institución y la Superintendencia, o
   - Enlaces a Internet provistos por cada institución.

b) Los enlaces dedicados basados en protocolo TCP/IP deberán disponer de un ancho de banda mínimo de 100 Mbps simétricos, garantizado para las transmisiones requeridas.

c) Dos o más instituciones podrán compartir un mismo enlace hacia la Superintendencia, ya sea dedicado o a través de Internet.

d) Cada institución será responsable de la correcta operación, disponibilidad, desempeño y continuidad operacional de sus enlaces de comunicación.

e) Todo el tráfico entre los puntos de conexión deberá estar cifrado en la capa de transporte, asegurando confidencialidad e integridad mediante VPN u otros mecanismos equivalentes.

f) La conexión deberá establecerse preferentemente mediante VPN Site-to-Site. En casos justificados, podrá utilizarse un cliente VPN provisto por la Superintendencia.

g) Cuando se utilice cliente VPN:
   - Las cuentas deberán ser nominativas.
   - Se deberá implementar autenticación multifactor (MFA).

h) Todos los costos asociados a la implementación, operación y mantención de los enlaces serán de cargo de cada institución.

2. Servidores para Repositorio Transitorio

La transferencia de archivos con la Superintendencia debe realizarse utilizando uno o más servidores SFTP que operen como un servicio de **repositorio transitorio**.

La Superintendencia dispondrá para este servicio una plataforma centralizada denominada Plataforma de Transmisiones de la Superintendencia, operativa en modalidad **24x7**, encontrándose disponible en todo momento para la recepción y transmisión de información, salvo en aquellos casos de mantención programada que serán informados con la debida antelación a las instituciones.

Cada institución en acuerdo con la Superintendencia debe definir un único **repositorio transitorio** como principal para operación habitual. Adicionalmente, podrá definirse un repositorio alternativo para contingencia, sujeto a coordinación previa.

Las instituciones podrán:

- Utilizar la plataforma provista por la Superintendencia, o
- Implementar un repositorio propio, individual o compartido.

En caso de repositorios externos a la Superintendencia:

- Se deberá garantizar acceso físico y lógico equivalente al requerido para la operación y supervisión del servicio.

Los repositorios deberán cumplir con los siguientes requisitos:

- Uso obligatorio de protocolo SFTP.
- Capacidad de almacenamiento dimensionada según los volúmenes de transferencia.
- Operación continua, con ventanas de mantención controladas.
- Niveles adecuados de disponibilidad, confiabilidad y desempeño.
- Sincronización horaria mediante al menos dos servidores NTP públicos confiables.

La responsabilidad sobre la infraestructura (hardware, sistema operativo y software) será de cada institución, independientemente de si el servicio es propio o contratado.

3. Soporte Técnico y Canales de Atención

El equipo técnico de la Superintendencia de Pensiones atenderá consultas y requerimientos los días hábiles en los siguientes horarios:

- Lunes a jueves: 09:00 a 18:00 horas
- Viernes: 09:00 a 17:00 horas

Todas las consultas técnicas relacionadas con conectividad, cuentas de acceso, credenciales, VPN y aspectos operativos de la plataforma TEA deberán ser canalizadas exclusivamente a través del correo electrónico **admintra@spensiones.gob.cl**.

4. Seguridad

Las comunicaciones entre las instituciones y el **repositorio transitorio** deberán establecerse mediante canales cifrados utilizando VPN Site-to-Site o cliente VPN provisto por la Superintendencia.

Las responsabilidades de seguridad se distribuyen de la siguiente forma:

- Cada institución: seguridad de sus enlaces, sistemas y plataformas.
- Superintendencia: seguridad de los repositorios bajo su administración.

Las instituciones deberán:

- Cumplir permanentemente las normas de transferencia de archivos.
- Gestionar riesgos de ciberseguridad asociados, incluyendo aquellos derivados de terceros.
- Implementar controles de seguridad proporcionales a la criticidad del servicio.

En el caso de instituciones clasificadas como **Operadores de Importancia Vital (OIV)** o prestadoras de servicios esenciales, deberán aplicar controles reforzados considerando el impacto sistémico.

5. Bitácora (log) de conexión, recepción y envío

Los repositorios transitorios deberán mantener registros (logs) detallados de:

- Conexiones al servicio SFTP
- Transferencias (envíos y recepciones)

Cada registro deberá incluir al menos:

- Usuario
- Dirección IP
- Fecha y hora
- Resultado de la transacción
- Motivo de error (si aplica)

Los logs deberán garantizar trazabilidad, integridad y disponibilidad para auditoría.

6. Autorización de Operación

La habilitación de enlaces y repositorios estará sujeta a pruebas de interoperabilidad con la Superintendencia.

Dichas pruebas no constituyen certificación de:

- Seguridad
- Disponibilidad
- Capacidad

Estas responsabilidades recaen exclusivamente en cada institución.

Las instituciones deberán informar oportunamente cambios relevantes en su arquitectura o configuración que puedan afectar:

- Interoperabilidad
- Disponibilidad
- Seguridad

La Superintendencia podrá requerir pruebas adicionales posterior a dichos cambios.

7. Responsabilidad y Continuidad Operacional

Cada institución es responsable de asegurar la continuidad operacional de:

- Infraestructura tecnológica
- Enlaces de comunicación
- Repositorios transitorios
- Procesos asociados a la transmisión de información

Las fallas internas no eximen del cumplimiento de las obligaciones regulatorias.

Las pruebas que involucren componentes de la Superintendencia deberán coordinarse previamente.

8. Monitoreo y Gestión Proactiva de Incidentes

Las instituciones deberán implementar mecanismos de monitoreo continuo que permita supervisar, al menos, la disponibilidad de los enlaces de comunicación, servicios de transferencia de archivos (SFTP), capacidad de almacenamiento, integridad de los archivos transmitidos y funcionamiento de las conexiones VPN.

Ante la detección de fallas o degradaciones del servicio, las instituciones deberán ejecutar acciones correctivas de forma proactiva, incluyendo aquellos originados en servicios provistos por terceros bajo responsabilidad de la institución, y activar sus procedimientos de contingencia cuando corresponda y coordinar oportunamente con la Superintendencia, sin perjuicio de sus responsabilidades regulatorias.

9. Contingencia

En caso de fallas en los sistemas de transmisión principales, la Superintendencia dispondrá de un repositorio transitorio en un sitio de contingencia habilitado para la recepción y transmisión segura de información, al cual se podrá acceder mediante un cliente VPN y una cuenta SFTP que serán proporcionados para este propósito. Las pruebas de este mecanismo deben ser coordinadas con el Administrador de Transmisiones.

Asimismo, las instituciones podrán implementar un sitio de contingencia propio para garantizar la continuidad operativa. No obstante, dicha implementación deberá ser previamente solicitada a la Superintendencia y contar con su aprobación formal. Dicho sitio deberá cumplir con los mismos estándares de seguridad, confidencialidad, integridad y disponibilidad establecidos para el ambiente productivo, incluyendo el uso de conexiones cifradas, controles de acceso, autenticación robusta y resguardo de la trazabilidad de los datos transmitidos.

La información transmitida, ya sea al sitio de contingencia de la Superintendencia o desde el sitio de contingencia de la institución externa, deberá mantener los lineamientos definidos en la sección **"Definición de informes y archivos a transferir",** disponible en la sección “Transferencia Electrónica de Archivos” del sitio WEB de la Superintendencia.

En situaciones excepcionales, debidamente justificadas y autorizadas por la Superintendencia, podrán evaluarse mecanismos alternativos de intercambio de archivos, siempre que garanticen la seguridad y trazabilidad de los datos.