PROCEDIMIENTO	Código: **S03.04.11.02**
	Versión: 01
	Vigencia: 24/10/2025
Dueño del proceso: Oficina de Administración	

TRANSFERENCIA DE INFORMACIÓN ENTRE PARTES INTERESADAS

	Nombres y Apellidos	Cargo	Firma y Sello
Elaborado por:	Manuel Aguilar Cori	Oficial de Seguridad y Confianza Digital	Firmado digitalmente por: AGUILAR CORI Manuel Isidro FAU 20380799643 hard Fecha: 23/09/2025 14:47:30
	Víctor Chávez Gómez	Jefe de Tecnologías de la Información	Firmado digitalmente por: CHAVEZ GOMEZ Victor Hugo FAU 20380799643 soft Fecha: 23/09/2025 18:34:44
Revisado por:	Apolinar Madrid Escobar	Jefe (dt) de la Oficina de Planeamiento y Presupuesto	Firmado digitalmente por: MADRID ESCOBAR Apolinar Junior FAU 20380799643 hard Fecha: 23/09/2025 16:38:17
Aprobado por:	Alberto Blas Ortiz	Jefe de la Oficina de Administración	

Versión	Descripción de Cambios	Fecha
01	Versión inicial	24/09/2023

1. BASE LEGAL

1.1. ISO/IEC 27001:2022 “Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de Gestión de Seguridad de la Información – Requisitos” (en adelante ISO/IEC 27001).
1.2. NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de Gestión de Seguridad de la Información – Requisitos (en adelante NTP-ISO/IEC 27001).
1.3. ISO/IEC 27002 “Seguridad de la Información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información” (en adelante ISO/IEC 27002).
1.4. NTP-ISO/IEC 27002:2022 “Seguridad de la Información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información” (en adelante NTP-ISO/IEC 27002).
1.5. Versión Actualizada de la Directiva N° 02-2015-SERVIR/GPGSC Régimen Disciplinario y Procedimiento Sancionador de la Ley N° 30057, Ley del Servicio Civil
1.6. Reglamento Interno de los Servidores Civiles - RIS de la Agencia de Promoción de la Inversión Privada – PROINVERSIÓN.
1.7. Código de Ética de la Agencia de la Promoción de la Inversión Privada PROINVERSIÓN.

2. DEFINICIONES Y SIGLAS

2.1. Definiciones

2.1.1. **Activo de Información:** Información o soporte en que ella reside, que es gestionado de acuerdo con las necesidades de negocios y los requerimientos legales, de manera que puede ser entendida, compartida y usada. Es de valor para la empresa y tiene un ciclo de vida.

2.1.2. **Acuerdo de confidencialidad:** Documento firmado por varias partes con el objetivo de proteger información sensible o confidencial.

2.1.3. **Autenticación:** Es el proceso de verificar la identidad de alguien o algo, asegurando que una persona o entidad es quien dice ser antes de otorgarle acceso a un sistema o recurso.

2.1.4. **Canales autorizados de transferencia:** Medio o plataforma a través del cual se realiza una transferencia de información de forma segura y verificada. Estos canales pueden ser físicos o digitales.

2.1.5. **Ciberseguridad:** Protección de los activos de información mediante la prevención, detección, respuesta y recuperación ante incidentes que afecten su disponibilidad, confidencialidad o integridad en el ciberespacio; el que consiste a su vez en un sistema complejo que no tiene existencia física, en el que interactúan personas, dispositivos y sistemas informáticos.

2.1.6. **Cifrado de datos:** Proceso que convierte información legible en un formato ilegible (texto cifrado) para protegerla del acceso no autorizado.

2.1.7. **Confidencialidad:** Propiedad de que la información no esté disponible o sea revelada a personas no autorizadas, las entidades o procesos.

2.1.8. **Disponibilidad:** Propiedad de ser accesible y utilizable por petición de una entidad autorizada.

2.1.9. **Integridad:** Propiedad de exactitud y lo completo.

2.1.10. **Protección contra malware:** Conjunto de medidas y tecnologías diseñadas para prevenir, detectar y eliminar software malicioso (malware) de sistemas informáticos y redes.

2.1.11. **Registro de actividades:** Es un documento, ya sea físico o electrónico, que detalla las acciones y eventos realizados dentro de un sistema, proyecto o proceso.

2.1.12. **Seguridad de la Información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

2.1.13. **Sistema de Gestión de la Seguridad de la Información (SGSI):** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

2.2. Siglas:

- CGTD: Comité de Gobierno y Transformación Digital.
- SGSI: Sistema de Gestión de Seguridad de la Información.
- OSCD: Oficial de Seguridad y Confianza Digital.

3. RESPONSABILIDADES

3.1. De los Colaboradores de PROINVERSION

3.1.1. Seguir las políticas de transferencia de información (ej. no enviar datos confidenciales por correo no cifrado).
3.1.2. Utilizar solo los canales autorizados para compartir información.
3.1.3. Reportar incidentes (ej. envío accidental a destinatarios equivocados).

3.2. De los propietarios de Activos de información

3.2.1. Identificar y clasificar la información según su criticidad (critica, confidencial, interna, pública).
3.2.2. Autorizar qué información puede ser transferida y a quién.
3.2.3. Definir los requisitos de protección (cifrado, controles de acceso, etc.).
3.2.4. Aprobar o rechazar solicitudes de transferencia de información sensible.

3.3. Del Especialista de Tecnologías de Información y Redes

3.3.1. Implementar controles técnicos para transferencias seguras (ej. TLS/SSL, PGP, firmas digitales).
3.3.2. Configurar y gestionar canales seguros (correo cifrado, SFTP, servicios en la nube con cifrado).
3.3.3. Monitorear el tráfico de datos para detectar anomalías.
3.3.4. Asegurar la disponibilidad de los sistemas de transferencia.

3.4. Del Oficial de Seguridad y Confianza Digital (OSCD)

3.4.1. Verificar aleatoriamente si se han generado los registros de evidencia de transferencia de información.

4. GENERALIDADES

4.1. Definición de los requisitos de transferencia

- **Identificar tipo de información:** Clasificarla según su criticidad: pública, interna, confidencial, etc.
- **Establecer acuerdos formales**: (SLAs, NDAs) con terceros para transferencias externas
- **Determinar canales autorizados**: Correo electrónico cifrado, plataformas seguras (SFTP, VPN), medios físicos (USB cifrados), etc.

4.2. Seleccionar controles de seguridad

- **Cifrado:** Usar protocolos como TLS, PGP o AES para datos en tránsito/reposo
- **Autenticación:** Verificar identidades de remitente y destinatario.
- **Registro de actividades:** Logs de transferencias para auditoría
- **Protección contra Malware:** Escaneo de archivos antes/durante la transferencia

5. SECUENCIA DE ACTIVIDADES

N°	Descripción de la tarea	UO / Ente	Cargo
Inicio			
Identificar necesidad de trasferir información			
1	Identificación de la necesidad de transferencia • Determinar qué información se transferirá • Identificar quienes el emisor y el receptor de la información • Determinar cuál será el medio de transferencia (Correo electrónico, USB, Cloud, Impreso, etc.).	DEP DPP Área de TI. Oficina de Administración Área de Logística Área de Personal	Colaboradores de PROINVERSION
2	**Clasificación de la información** Verificar el nivel de confidencialidad • **Pública**→ Sin restricciones. • **Interna**→ Solo personal autorizado. • **Confidencial**→ Requiere cifrado/acuerdos de confidencialidad (NDA). • **Crítica**→ Máxima protección (ej.: datos personales, secretos empresariales propios o de inversionistas).	DEP DPP Área de TI. Oficina de Administración. Área de Logística Área de Personal	Colaboradores de PROINVERSION
3	Seleccionar medio de transferencia de información Decisión si la transferencia de información será física o digital ¿Medio de transferencia seleccionado es físico? Si: Ir a tarea 6 No: Ir a tarea 4	DEP DPP Área de TI. Oficina de Administración. Área de Logística Área de Personal	Colaboradores de PROINVERSION
Provisionar medios para transferir información			
4	Provisionar recursos para transferencia de información digital • Se usa cifrado (ej.: TLS, PGP) • La plataforma es segura (ej.: SFTP, correo corporativo)	Área de TI.	Especialista de Tecnología de Información y Redes
Seleccionar método para transferir información			
5	Seleccionar método para transferencia de información lógica	DEP DPP Área de TI. Oficina de Administración. Área de Logística Área de Logística	Colaboradores de PROINVERSIÓN
6	Seleccionar controles para transferencia de información física • Medios removibles cifrados (USB/HDD) • Documentos en sobres sellados	DEP DPP Área de TI. Oficina de Administración. Área de Logística Área de Personal	Colaboradores de PROINVERSIÓN
Ejecutar transferencia de información			
7	**Ejecución de la transferencia** **Transferencia digital:**	DEP DPP	Colaboradores de PROINVERSIÓN

	• Cifrado de archivos (Ej. AES-256) • Uso de contraseñas compartidas por otro canal • Notificación al receptor **Transferencia física:** • Entrega con acuse de recibo	Área de TI. Oficina de Administración. Área de Logística Área de Personal	
8	**Verificación y confirmación de entrega** **Transferencias físicas:** • El receptor confirma la recepción íntegra. **Transferencias digitales:** • Validación de integridad (ej.: checksum, firmas digitales). • Borrado seguro de archivos temporales o medios reutilizables (De aplicar)	DEP DPP Área de TI. Oficina de Administración. Área de Logística Área de Personal	Colaboradores de PROINVERSIÓN
Verificar transferencia de información			
9	Verificar registro de transferencia de información <u>Transferencias físicas:</u> • Se recibe cargos y se almacenan <u>Transferencias digitales</u> • Se resguarda log de eventos de transferencia El OSCD puede revisar aleatoriamente que se conserven registros de las transferencias de información y podrá actualizar el presente proceso para reforzar los canales de seguridad	Área de TI	OSCD
Fin			

6. ANEXOS (Opcional)

6.1. Flujograma de procedimiento de transferencia de información entre partes interesadas

ANEXO 1: Procedimiento de transferencia de información entre partes interesadas