1. Propósito

Establecer los controles y procedimientos para la transferencia segura de información dentro y fuera de **la organización**, asegurando que los datos sensibles sean protegidos durante su transmisión y que se cumpla con los requisitos legales, contractuales y de seguridad.

2. Alcance

Aplica a:

- La transferencia de **información clasificada** dentro del ámbito de **la organización** (internos y externos).
- Transferencia de datos en formato físico y digital (correos electrónicos, archivos, aplicaciones, almacenamiento en la nube, medios físicos).
- Todos los empleados, proveedores y terceros que gestionan, almacenan o transmiten datos de **la organización**.

3. Referencias normativas y documentales

- ISO/IEC 27001:2022 — Controles 8.2, 8.3, 8.12, 5.34, 5.36.
- **MAN 002 Manual de Procedimientos** – Sección Transferencia de Información.
- **POL 005 Control de Acceso** y **POL 006 Dispositivos Móviles**.
- **PRO 014 Registro y Supervisión de Accesos**.
- **DOC 019 Plano de Áreas Críticas** (para control de medios físicos).
- **SOA 001 Declaración de Aplicabilidad** — Controles 5.33-5.34.

4. Definiciones

Término	Descripción
Transferencia de Información	Proceso de mover datos de un lugar a otro, ya sea de manera física o digital.
Medios seguros	Métodos de transmisión de datos que garantizan confidencialidad e integridad, como cifrado y canales seguros.
Información sensible	Información clasificada como **Confidencial** o **Restringida** según **POL 010**.

5. Principios de Transferencia de Información

1. **Confidencialidad**: Asegurar que la información solo sea accesible por las partes autorizadas.
2. **Integridad**: Garantizar que la información no sea alterada de manera no autorizada durante el proceso de transferencia.
3. **Autenticidad**: Asegurar que las partes involucradas en la transferencia son quienes dicen ser.
4. **Auditoría**: Toda transferencia debe ser registrada para permitir la trazabilidad y monitorización.
5. **Cumplimiento normativo**: Cumplir con los requisitos legales, regulatorios y contractuales para la protección de la información.

6. Requisitos para la Transferencia de Información

1. **Transferencias internas**
    - **Correo electrónico**: Uso obligatorio de cifrado (TLS 1.2+) para correos electrónicos con información sensible.
    - **Aplicaciones y sistemas internos**: Transferencia de datos solo a través de sistemas internos autorizados y con mecanismos de autenticación y autorización predefinidos.
    - **Archivos compartidos**: Los datos deben almacenarse en repositorios cifrados y se debe mantener el control de acceso según los roles de los usuarios.
2. **Transferencias externas**
    - **Correo electrónico**: Cifrado de correo (PGP, S/MIME) o uso de plataformas de transferencia segura (ej., servicios de almacenamiento en la nube con cifrado).
    - **Medios físicos**: Las transferencias de datos en discos duros, memorias USB u otros dispositivos físicos deben ir cifradas, aseguradas con contraseñas y enviadas a través de servicios de mensajería seguros.
    - **Transferencias a terceros**: Se deben realizar a través de acuerdos contractuales que incluyan cláusulas de confidencialidad y protección de la información (**POL 011 Seguridad del Proveedor**).
3. **Transferencia de datos personales (PII)**
    - La transferencia de datos personales deberá cumplir con la normativa vigente (Ley de Protección de Datos Personales), garantizando que se utilizan medios cifrados y seguros.

7. Procedimientos para la Transferencia de Información

1. **Solicitud y autorización**
    - La transferencia de información sensible debe ser solicitada mediante **FOR 003 Registro de Autorización de Usuarios** y aprobada por el propietario del activo o área responsable.
2. **Transferencia física**
    - Los datos deben ser almacenados en medios cifrados y enviarse solo a través de servicios de mensajería de confianza con confirmación de recepción.
3. **Transferencia electrónica**
    - Utilizar medios electrónicos seguros y cifrados (VPN, TLS 1.2, aplicaciones de cifrado de extremo a extremo).
4. **Registro de la transferencia**
    - Todas las transferencias deben ser registradas y almacenadas en **FOR 019 Registro de Comunicaciones** para su posterior auditoría.
5. **Monitoreo de la transferencia**
    - Los registros de transferencia deben ser monitoreados para detectar transferencias no autorizadas o fallidas (ver **PSC 002 Gestión de Incidentes**).

8. Roles y responsabilidades

Rol	Responsabilidades
Responsable del SGSI	Asegurar que las transferencias se realicen conforme a esta política y auditar el cumplimiento.
Propietarios de Activos	Asegurar que la información se clasifique correctamente y que solo se transfiera conforme al nivel de acceso.
Responsable de TI	Implementar y gestionar los controles técnicos para la transferencia segura de datos.
Usuarios	Cumplir con los requisitos para transferir información y reportar cualquier incidente relacionado.
Auditor Interno	Verificar el cumplimiento de la política en las auditorías de seguridad.

9. Indicadores de desempeño (KPI)

KPI	Meta
% transferencias realizadas con cifrado	100 %
Nº incidentes de transferencia no autorizada	Tendencia descendente
Tiempo de respuesta ante incidente de transferencia fallida	≤ 4 h

10. Cumplimiento y sanciones

El incumplimiento de esta política será considerado una falta grave y podrá resultar en:

- Medidas disciplinarias internas, que pueden incluir amonestaciones, suspensiones o despidos.
- Acciones legales si se demuestra negligencia en la protección de la información.
- Sanciones contractuales y/o terminación del contrato con proveedores que no cumplan con los estándares de seguridad acordados.

11. Revisión y mejora

Esta política será revisada **anualmente tras** incidentes significativos, cambios regulatorios, o en la infraestructura tecnológica. Las modificaciones se documentan en **FOR 017 Registro de Cambios** y se comunican a través de **PRO 007 Comunicación Interna**.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO