1. Propósito

Establecer criterios uniformes para **identificar, clasificar, etiquetar y proteger** toda la información que gestiona **la organización**, garantizando que cada activo reciba los controles adecuados según su nivel de sensibilidad y los requisitos legales, contractuales y de negocio.

2. Alcance

Aplica a:

- Información en **cualquier formato** (digital, físico, verbal) tratada dentro del **DOC 001 Alcance del SGSI**.
- Empleados, contratistas y terceros que manipulen datos de la organización.
- Sistemas, aplicaciones, redes y soportes físicos incluidos en el inventario (**FOR 027**).

3. Referencias Normativas y Documentales

- ISO/IEC 27001:2022 — Controles 5.32-5.35, 8.3, 8.11-8.14, 8.24.
- **DOC 008 Estrategia de Seguridad de la Información**.
- **PRO 008 Planificación y Ejecución de Controles**.
- **POL 005 Control de Acceso** y **POL 006 Dispositivos Móviles**.
- **FOR 014 Evaluación del Contexto** y **FOR 015 Partes Interesadas**.

4. Esquema de Clasificación

Nivel	Definición	Ejemplos	Control mínimo requerido*	Etiqueta obligatoria
Pública	Información cuyo acceso está abierto y su divulgación no afecta a la organización.	Comunicados de prensa, material publicitario.	Ninguno adicional	“PÚBLICA”
Interna	Uso interno; la divulgación no autorizada puede causar impacto menor.	Políticas, manuales internos no sensibles.	Autenticación básica, acceso mediante credenciales.	“INTERNA”
Confidencial	Su divulgación puede afectar la ventaja competitiva o producir sanciones.	Datos de clientes, contratos, estados financieros.	Cifrado en tránsito y reposo, control de acceso granular, MFA.	“CONFIDENCIAL”
Restringida	Su exposición ocasionaría perjuicio grave o incumplimiento legal.	Credenciales, PII sensible, estrategias corporativas.	Cifrado fuerte, registro de acceso, almacenamiento en repositorios seguros,	“RESTRINGIDA”

			aprobación de propietario.	

* Controles adicionales se detallan en la **Declaración de Aplicabilidad (SOA 001)**.

5. Directrices de Manejo por Nivel

Actividad	Pública	Interna	Confidencial	Restringida
Almacenamiento	Sistemas comunes	Carpeta corporativa	Repositorio cifrado	Repositorio cifrado + bóveda
Transporte digital	Sin restricción	HTTPS/TLS	VPN + TLS	VPN + TLS + cifrado de archivo
Transporte físico	Sin restricción	Sobre cerrado	Sobre sellado	Custodia autorizada
Impresión	Libre	Impresora corporativa	Impresora segura	Impresora segura + recogida inmediata
Retención	Según necesidad	5 años (*o política interna*)	7 años (*mínimo*)	10 años / requisito legal
Destrucción	Reciclaje	Picado	Triturado o borrado seguro	Triturado certificado / borrado criptográfico

6. Proceso de Clasificación y Etiquetado

1. **Identificación**: el *Propietario del Activo* registra la información en **FOR 027 Inventario de Activos**.
2. **Evaluación**: se aplica la **Matriz de Riesgo (DOC 018)** para determinar el impacto potencial.
3. **Asignación de nivel**: el propietario clasifica y lo documenta en el inventario.
4. **Etiquetado**:
    - Digital → prefijo en nombre de archivo y metadatos (ej.: “CONFIDENCIAL-Contrato-ABC.pdf”).
    - Físico → sello o etiqueta visible según tabla.
5. **Revisión**: revisiones anuales o tras cambios significativos en el contexto del activo.

7. Roles y Responsabilidades

Rol	Responsabilidades
Propietario del Activo	Clasificar, revisar y aprobar accesos.
Usuarios	Manejar la información según nivel y reportar violaciones.
Responsable del SGSI	Supervisar la correcta aplicación de la política y auditar cumplimiento.
Responsable de TI	Implementar controles técnicos (cifrado, backups, DLP).
Comité de Seguridad	Resolver disputas de clasificación y aprobar cambios al esquema.
Auditor Interno	Verificar registros y evidencias de cumplimiento.

8. Concienciación y Capacitación

- Módulo "Clasificación y Manejo Seguro de la Información" es obligatorio al ingreso y se repite cada 12 meses (registro **FOR 011**).
- Campañas trimestrales de recordatorio con casos prácticos.

9. Indicadores de Desempeño (KPI)

KPI	Meta
% activos correctamente clasificados y etiquetados	≥ 98 %
Nº incidentes por manejo inadecuado de datos	Tendencia descendente
Tiempo medio de actualización después de cambio de clasificación	≤ 5 días

10. Cumplimiento y Sanciones

El incumplimiento podrá conllevar sanción disciplinaria y/o acciones legales conforme a la legislación paraguaya. Se gestionará bajo el **PSC 006 Gestión de No Conformidades y Acciones Correctivas**.

11. Revisión y Mejora

La política se revisa **anualmente** o ante:

- Cambios regulatorios (p. ej., protección de datos personales).
- Resultados de auditorías internas/externas.
- Incidentes significativos.

Las modificaciones se documentan en **FOR 017 Registro de Cambios** y se comunican mediante **PRO 007 Comunicación Interna**.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO