1. Propósito

Definir y formalizar los **roles, responsabilidades y autoridades** en materia de seguridad de la información dentro de **la organización**, garantizando:

- Alineación con los objetivos estratégicos y con el **MAN 001 Manual del SGSI**
- Rendición de cuentas clara y verificable
- Segregación de funciones para reducir riesgos de fraude, error o abuso

2. Alcance

Esta política aplica a todo el personal, contratistas y terceros que intervienen en procesos, activos y servicios incluidos en el **DOC 001 Alcance del SGSI**, independientemente de su relación laboral o contractual.

3. Referencias Normativas y Documentales

- ISO/IEC 27001:2022 — Controles 5.2 (Roles y responsabilidades), 5.3 (Segregación de funciones) y 5.36 (Cumplimiento).
- **DOC 002 Organigrama** y **DOC 007 Partes Interesadas**.
- **PRO 003 Competencia y Capacitación** y **PRO 011 Evaluación y Selección del Personal**.
- **PSC 002 Gestión de Incidentes**, **PSC 004 Auditoría Interna** y **PSC 005 Revisión por la Dirección**.

4. Principios Rectores

1. **Necesidad de conocer & menor privilegio**: a cada persona se le asignan solo los privilegios requeridos para desempeñar su función.
2. **Responsabilidad individual**: toda acción sobre la información debe poder trazarse a un usuario nominal.
3. **Segregación de funciones (SoD)**: se evita que una misma persona ejecute actividades incompatibles (ej.: aprobación y ejecución de pagos).
4. **Sustitución y continuidad**: cada rol crítico tiene un suplente designado.
5. **Revisión periódica**: las responsabilidades se revisan ante cambios organizativos o al menos **una vez al año**.

5. Estructura de Roles SGSI

Rol	Responsabilidades clave	Autoridad	Reporta a	Documentos de apoyo
Dirección General	Aprobar políticas, asignar recursos y asumir la responsabilidad final del SGSI.	Alta	Junta/Accionistas	MAN 001, DOC 003
Comité de Seguridad	Definir estrategia, aprobar riesgos mayores, revisar desempeño KPI.	Ejecutiva	Dirección General	PSC 005

Responsable del SGSI	Mantener MAN-001, coordinar auditorías, gestionar mejoras y no conformidades.	Funcional	Comité de Seguridad	PSC 004, PSC 006
Responsable de TI	Implantar controles técnicos, administrar accesos y registrar logs.	Operativa	Responsable SGSI	POL 004, POL 005
Propietarios de Activos/Procesos	Clasificar información, aprobar accesos, validar controles y evidencias.	Operativa	Responsable SGSI	POL 010, FOR 027
Usuarios	Cumplir políticas, reportar incidentes, proteger credenciales.	—	Supervisores directos	POL 004, PRO 007
Auditor Interno	Verificar conformidad, emitir hallazgos y seguimiento de acciones.	Independiente	Comité de Seguridad	PSC 004
Proveedor Crítico TIC	Mantener niveles de servicio y controles acordados (SLA).	Contractual	Responsable de TI	POL 011

*Las funciones incompatibles (p. ej., "Desarrollar código" vs. "Aprobar paso a producción") se listan en el **Anexo A** de esta política y son revisadas en cada cambio organizativo.*

6. Asignación y Cambios de Rol

1. **Alta / Modificación**: se documenta mediante **FOR 003 Registro de Autorización de Usuarios** y se refleja en el **DOC 002 Organigrama**.
2. **Desvinculación**: el proceso **MAN 004 Desvinculación de Personal** asegura la revocación de accesos en ≤ 24 h.
3. **Cambios urgentes**: se gestionan bajo **PRO 006 Gestión de Cambios** y se registran en **FOR 017**.

7. Competencia y Formación

- Todo colaborador debe demostrar las competencias definidas en su **Ficha de Puesto** (custodiada por Talento Humano).
- Programas formativos se planifican anualmente (**DOC 013 Plan de Capacitación**) y se registran en **FOR 011**.
- La actualización de competencias SGSI es obligatoria tras cambios normativos o tecnológicos relevantes.

8. Indicadores de Desempeño (KPI)

KPI	Fórmula	Meta
% descripciones de puesto actualizadas	(Puestos actualizados / Total) × 100	≥ 98 %
Tiempo medio de revocación de acceso tras baja	Σ horas / nº bajas	≤ 24 h
% SoD violaciones detectadas en auditoría	(Casos / Total revisiones) × 100	0 %

9. Cumplimiento y Sanciones

El incumplimiento de esta política se considera falta grave:

- Medidas disciplinarias internas conforme al Reglamento Interno.
- Acciones civiles o penales según la legislación paraguaya.

10. Revisión y Mejora

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

- Cambios organizativos significativos.
- Resultados de auditorías internas/externas o incidentes relevantes.

Toda modificación se registra en **FOR 017 Registro de Cambios** y se comunica a través de **PRO 007 Comunicación Interna**.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO