MéTRIK

IA S.A.S.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN · V1.3

Política de Seguridad de la Información

Marco de controles técnicos, administrativos y físicos que METRIK IA S.A.S. aplica para proteger la confidencialidad, integridad y disponibilidad de la información que opera el Servicio MéTRIK Valida y demás productos.

VIGENTE DESDE	**5 de octubre de 2026**
EMISOR	**METRIK IA S.A.S. · NIT 902.079.601-9**
AUDIENCIA	**Equipo técnico cliente · auditoría · compliance**

POWERED BY MÉTRIK · METRIK.COM.CO

1. Objetivo y alcance

METRIK IA S.A.S. adopta esta Política de Seguridad de la Información para garantizar la confidencialidad, integridad y disponibilidad de los datos, sistemas e infraestructura tecnológica que opera el Servicio MéTRIK Valida y demás productos.

Aplica a:

- Personal interno y colaboradores externos
- Infraestructura propia y de terceros (Vercel, Supabase, proveedores conexos)
- Bases de datos, código fuente, documentación, credenciales y artefactos del Servicio
- Información de Clientes y Titulares cuyos datos son tratados

2. Principios rectores

- **Confidencialidad:** La información solo es accesible para quien debe acceder, en función de su rol y necesidad operativa.
- **Integridad:** La información es exacta, completa y no se altera sin trazabilidad.
- **Disponibilidad:** La información y los servicios están disponibles cuando son requeridos legítimamente.
- **Defensa en profundidad:** Múltiples capas de control reducen la probabilidad de que un único fallo comprometa el sistema.
- **Mínimo privilegio:** Todo acceso es el menor que permita cumplir la función. Se revisa periódicamente.
- **Auditabilidad:** Toda acción crítica deja registro inmutable y revisable.
- **Mejora continua:** La política y los controles se revisan periódicamente conforme cambian el riesgo, la normativa y las tecnologías.

3. Gobierno y responsabilidades

Representante Legal	Responde como administrador (Ley 222/1995 Art. 23) por la adopción y vigencia de esta Política.
Tech Lead / equipo	Diseña e implementa los controles técnicos. Mantiene la postura de seguridad de la infraestructura.
Encargado de protección de datos	Punto único de contacto para asuntos de habeas data y compliance Ley 1581/2012.
Personal y colaboradores	Aplican esta Política. Reportan incidentes. Cumplen acuerdos de confidencialidad.
Proveedores y terceros	Cumplen las cláusulas contractuales de seguridad y confidencialidad pactadas.

4. Clasificación de la información

Pública	Información destinada al público general (marketing, documentación, listas oficiales scrapeadas).
Interna	Información operativa de METRIK IA S.A.S. no destinada a publicación (configuraciones, métricas, dashboards).
Confidencial	Información de Clientes y Titulares (consultas, datos personales, bitácoras, credenciales del cliente).
Restringida	Secretos (claves de cifrado, llaves de servicio, credenciales raíz, código fuente sensible).

4.1. Disponibilidad para autoridades competentes

Toda información clasificada como Confidencial o Restringida, cuando esté vinculada a operaciones SARLAFT del Cliente, se mantiene disponible para ser puesta a disposición de la autoridad competente (UIAF, SFC, Supersociedades, Supertransporte u otra) mediante procedimiento legalmente válido y dentro de los plazos que la autoridad determine. La entrega sigue el conducto previsto en la Política de Tratamiento de Datos Personales y se documenta en bitácora interna.

5. Controles técnicos

- **Cifrado en tránsito:** TLS 1.2 o superior en todas las comunicaciones externas. HTTPS obligatorio en todos los endpoints.
- **Cifrado en reposo:** Bases de datos cifradas (AES-256). Backups cifrados con la misma política.
- **Autenticación API:** API keys con hash SHA-256 en BD. Clave en texto plano se entrega una sola vez y no es recuperable.
- **Rotación de credenciales:** Claves de servicio rotadas ante eventos de seguridad. Credenciales de cliente rotadas a solicitud.
- **Logs auditables:** Cada consulta, ingesta, modificación de configuración y acceso administrativo se registra con timestamp, identidad y resultado.
- **Segregación de ambientes:** Producción, staging y desarrollo separados. Sin datos reales en ambientes inferiores.
- **Hash de integridad:** Cada reporte PDF lleva hash SHA-256 verificable. Cada versión de lista oficial se almacena con hash.
- **Backups y monitoreo:** Backups automáticos diarios. Métricas operativas en tiempo real con alertas automáticas.

6. Gestión de accesos

- **Cuentas individuales:** Todo acceso a infraestructura es nominal. Sin cuentas compartidas.
- **MFA obligatorio:** Autenticación de doble factor obligatoria para todos los miembros del equipo en sistemas administrativos.
- **Revocación inmediata:** Al término del vínculo laboral o contractual, accesos revocados en 24 horas.
- **Revisión semestral:** Auditoría de privilegios al menos semestral, o ante cambios significativos de rol.
- **Mínimo privilegio:** Accesos otorgados estrictamente para la función requerida. Se eliminan al terminar la función.

7. Proveedores y terceros

METRIK IA S.A.S. solo contrata proveedores con certificaciones de seguridad razonables (SOC 2 Type II, ISO 27001 o equivalentes). Proveedores actuales relevantes:

Vercel Inc.	Hosting y entrega del Servicio. Certificación SOC 2 Type II.
Supabase Inc.	Base de datos PostgreSQL gestionada. SOC 2 Type II + HIPAA-ready.

Fuentes de listas. Valida descarga información pública de las autoridades emisoras de las listas que consulta (Consejo de Seguridad de la ONU, Consejo de Seguridad Nacional de Colombia, Función Pública vía SIGEP, U.S. Treasury, Consejo de la Unión Europea y U.S. Department of State, entre otras según el alcance vigente). Estas autoridades no son proveedores ni Encargados del Tratamiento: el flujo de información es únicamente de descarga desde su publicación oficial hacia Valida. Consultar a un tercero no transmite ningún dato suyo a esas autoridades: la consulta se resuelve contra la copia que Valida mantiene, sin contactarlas. Los únicos terceros que tratan datos personales por cuenta de METRIK IA S.A.S. son los Encargados relacionados en la tabla anterior.

Toda contratación de proveedor adicional con acceso a datos confidenciales o restringidos requiere evaluación previa de seguridad y suscripción de cláusulas contractuales de confidencialidad y protección de datos.

8. Gestión de incidentes de seguridad

8.1. Toda persona vinculada está obligada a reportar inmediatamente sospechas o evidencias de incidente.

8.2. El equipo técnico contiene, identifica causa raíz, evalúa alcance y aplica mitigación.

8.3. Si afecta datos personales: se aplica el procedimiento de notificación de brechas previsto en Política de Tratamiento de Datos.

8.4. Si afecta Servicio del Cliente: se aplica procedimiento de notificación del ANS.

8.5. Cada incidente queda documentado en bitácora con causa raíz y medidas para evitar reincidencia.

9. Continuidad del negocio

- **Backups automáticos diarios:** Recuperación de punto en el tiempo (PITR) habilitada en la base de datos.
- **Infraestructura distribuida:** Servicio sobre infraestructura serverless con redundancia geográfica del proveedor (multi-región).
- **Plan de recuperación:** Procedimiento documentado de restauración ante caída de proveedor crítico.
- **Multi-proveedor LLMs:** Cuando aplique uso de LLMs, MeTRIK mantiene plan B documentado para continuidad con proveedor alterno.

10. Cumplimiento y auditoría

- **Ley 1581/2012 + Decreto 1377/2013:** Protección de datos personales. Política específica en /recursos/privacidad.
- **Ley 1480/2011:** Operación B2B estricta con sujetos obligados — no consumidores.
- **Ley 1581 Art. 26:** Transferencias internacionales fundadas en cumplimiento de obligación legal del Cliente.
- **Marco SARLAFT colombiano:** Circular Básica Jurídica SFC, Circular Básica Jurídica Supersociedades (C.E. 100-000020/2026), Resolución 2328/2025 Supertransporte.
- **Revisión periódica:** Esta Política se revisa al menos anualmente, o ante cambios significativos que justifiquen actualización.

> Esta Política es un instrumento de gobierno interno. No constituye certificación de seguridad bajo norma internacional, sino el compromiso operativo de METRIK IA S.A.S. de aplicar prácticas razonables conforme al estado del arte. La obtención de certificaciones formales (ISO 27001, SOC 2) se incorpora al roadmap de METRIK IA S.A.S. según la escala del Servicio.

Versión 1.3 · vigente desde 5 de octubre de 2026. Actualiza la cita del marco SARLAFT de Supersociedades a la Circular Externa 100-000020 de 2026, que derogó la 100-000016 de 2020. La v1.2 (16 de septiembre de 2026) corrigió la razón social de la sociedad que adopta esta Política: METRIK IA S.A.S., NIT 902.079.601-9. La v1.1 regía desde el 10 de septiembre de 2026.