

Biometría y datos sensibles

Tratamiento reforzado bajo el régimen colombiano de protección de datos

Fundamento principal: Ley 1581 de 2012, especialmente las reglas aplicables a datos sensibles y los límites de su tratamiento. **Complementos:** Decreto 1074 de 2015 y criterios orientadores de la SIC.

Los datos biométricos —como reconocimiento facial, huella dactilar u otros patrones que permiten identificar o autenticar a una persona— pueden constituir datos sensibles cuando revelan características individuales cuyo tratamiento exige especial cuidado. Por ello requieren base jurídica válida, finalidad reforzada, medidas de seguridad elevadas y una justificación estricta de necesidad y proporcionalidad.

Fundamento jurídico colombiano

- La Ley 1581 define los datos sensibles como aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación.
- El tratamiento de datos sensibles está sometido a reglas más estrictas y no puede asumirse como una práctica automática o indiferenciada.
- La biometría, por su poder de autenticación e identificación, exige una evaluación jurídica y técnica reforzada.

Condiciones mínimas de tratamiento

- Debe existir una finalidad clara, legítima y proporcional a la operación real del sistema.
- El titular debe recibir información comprensible sobre el tratamiento, sus alcances, riesgos y canales de atención.
- Se requieren controles físicos, lógicos y administrativos reforzados, además de trazabilidad sobre accesos, soporte y administración de la información.

Aplicación en control de acceso y seguridad

- En soluciones de reconocimiento facial o biometría para ingreso, la decisión de implementar el mecanismo debe estar respaldada por análisis legal, operativo y de riesgo.
- No basta con que la tecnología funcione: también debe existir soporte documental, delimitación de roles y políticas claras de conservación, consulta y seguridad.
- Cuando sea posible, conviene evaluar si existen mecanismos alternos o complementarios acordes con la finalidad y el contexto del proyecto.

Conclusión práctica

- La biometría no debe tratarse como un dato ordinario. Su gestión exige un estándar reforzado de legalidad, información, seguridad y responsabilidad.
- Toda implementación debe quedar articulada con la política de privacidad, la arquitectura técnica y la realidad operativa del cliente.

Síntesis operativa

Norma base	Ley 1581 de 2012 y Decreto 1074 de 2015, en articulación con la orientación administrativa de la SIC.
Uso en la landing	Sirve de soporte para la tarjeta de biometría y para explicar por qué este tipo de información requiere tratamiento reforzado.
Nota técnica	El tratamiento biométrico debe analizarse caso por caso y no reemplaza la asesoría jurídica especializada cuando el proyecto lo demande.

Aviso importante: Este documento es un material de apoyo jurídico-operativo para la landing de privacidad de LAM Seguridad & Integración S.A.S. No constituye concepto jurídico vinculante ni reemplaza la revisión integral de la norma aplicable o la asesoría especializada en casos particulares.

