

Maestría en
Protección de Datos

**Trabajo de investigación previo a la obtención del título de
Magíster en Protección de Datos**

AUTORES:

Bastidas Aslalema Dayana Carolina
Fernández Villareal Edison Armando
Gross González Rosangel Milena
Robalino Moscoso Daniel Esteban
Torres Sarango Nadia Estefanía
Trelles Astudillo Carmita Alexandra

TUTORES:

Profesor PBL1: Humberto Ortiz Rodríguez
Profesor PBL2: Camila Valdez González
Profesor PBL3: Jacqueline Guerrero Carrera

**“Privacidad desde el diseño y por defecto: aplicación al uso de biometría en el escenario de
una entidad financiera”**

Quito, junio 2026

RESUMEN

La incorporación de mecanismos biométricos en el sistema financiero ha surgido como una respuesta al incremento de riesgos asociados al fraude y a la suplantación de identidad en entornos digitales. Dentro de este escenario, esta investigación examina la viabilidad jurídica del tratamiento de datos biométricos específicamente reconocimiento facial y huellas dactilares en una entidad financiera privada ecuatoriana, Banco Andino del Ecuador S.A., que implementa estos servicios mediante una empresa integradora denominada BioTrust. El análisis se desarrolla considerando el régimen establecido por la Ley Orgánica de Protección de Datos Personales y su normativa complementaria.

El estudio se organiza en cinco capítulos. Inicialmente se presentan los fundamentos metodológicos y conceptuales vinculados con privacidad, protección de datos personales y biometría, abordados desde perspectivas internacional, regional y nacional. Posteriormente, se analiza el marco normativo aplicable, junto con el inventario de datos y los mecanismos institucionales necesarios para asegurar un tratamiento legítimo y controlado. En una tercera etapa se identifican las condiciones mínimas requeridas para un tratamiento ético y estratégico de datos biométricos que incorporan herramientas de inteligencia artificial, incluyendo una matriz de riesgos y lineamientos de actuación frente a incidentes. El cuarto capítulo desarrolla una evaluación sobre la tensión entre derechos fundamentales, incorpora una Evaluación de Impacto en la Protección de Datos y sustenta el análisis de viabilidad jurídica. Finalmente, se presentan las conclusiones y recomendaciones derivadas de la investigación.

Como resultado, se concluye que el tratamiento propuesto puede considerarse jurídicamente admisible, aunque sujeto al cumplimiento previo de determinadas garantías reforzadas derivadas de la naturaleza sensible del dato biométrico y de su carácter esencialmente irreversible. El análisis de proporcionalidad permitió establecer que el modelo únicamente resulta compatible con el marco jurídico cuando se implementan medidas concretas orientadas a reducir riesgos y fortalecer el control institucional. Entre ellas destacan la administración directa de las plantillas biométricas por parte del banco, mecanismos de cifrado con capacidad de revocación, verificación empírica del

desempeño del componente de inteligencia artificial, fortalecimiento contractual con el proveedor tecnológico, disponibilidad de alternativas no biométricas equivalentes, definición verificable de plazos de conservación y obtención diferenciada del consentimiento según cada finalidad de tratamiento. La ausencia de estas condiciones comprometería la licitud del tratamiento y podría generar afectaciones permanentes para los titulares de los datos.

Palabras clave: Biometría, protección de datos personales, privacidad desde el diseño, evaluación de impacto, inteligencia artificial.

ABSTRACT

The incorporation of biometric mechanisms in the financial system has emerged as a response to the growing risks associated with fraud and identity theft in digital environments. Within this context, this research examines the legal viability of processing biometric data — specifically facial recognition and fingerprints — in a private Ecuadorian financial institution, Banco Andino del Ecuador S.A., which implements these services through a technology integrator called BioTrust. The analysis is conducted within the framework established by the Organic Law on Personal Data Protection and its complementary regulations.

The study is organized into five chapters. The first presents the methodological and conceptual foundations related to privacy, personal data protection and biometrics, addressed from international, regional and national perspectives. The second analyzes the applicable regulatory framework, along with the data inventory and institutional mechanisms required to ensure legitimate and controlled processing. The third identifies the minimum conditions for the ethical and strategic processing of biometric data involving artificial intelligence tools, including a risk matrix and guidelines for incident response. The fourth chapter develops an assessment of the tension between fundamental rights, incorporates a Data Protection Impact Assessment, and substantiates the legal viability analysis. Finally, the conclusions and recommendations derived from the research are presented.

As a result, it is concluded that the proposed processing may be considered legally admissible, though subject to the prior fulfillment of specific enhanced safeguards arising from the sensitive nature of biometric data and its essentially irreversible character. The proportionality analysis established that the model is only compatible with the legal framework when concrete measures are implemented to reduce risks and strengthen institutional control. These include direct administration of biometric templates by the bank, encryption mechanisms with revocation capability, empirical verification of the artificial intelligence component's performance, contractual strengthening with the technology provider, availability of equivalent non-biometric alternatives, verifiable definition of retention periods, and differentiated collection of consent for each processing

purpose. The absence of these conditions would compromise the lawfulness of the processing and could generate permanent harm for data subjects.

Keywords: Biometrics, personal data protection, privacy by design, impact assessment, artificial intelligence.