



¿Su plataforma biométrica realmente **cumple la Circular Básica Jurídica?**

Lo que la SFC exige hoy... y lo que muchas plataformas todavía no hacen.

Mecanismos fuertes de autenticación, cifrado de plantillas biométricas, prueba de vida y verificación contra fuentes oficiales: **los requisitos técnicos de la Superintendencia Financiera para entidades vigiladas**, y cómo implementarlos sin rehacer su arquitectura.

Lo que la **CBJ** ya exige a sus canales digitales

La **Circular Básica Jurídica** de la Superintendencia Financiera (compilada en la C.E. 006 de 2025) instruye sobre seguridad de canales, autenticación y biometría en el **Capítulo I, Título II, Parte I**, y sobre conocimiento del cliente en el marco **SARLAFT (Capítulo IV, Título IV, Parte I)**.

Con la Ley 2573 de 2026 elevando el estándar probatorio, estos requisitos dejaron de ser una lista de chequeo de auditoría **para convertirse en la defensa jurídica de la entidad**.



Mecanismos fuertes de autenticación

La biometría califica como mecanismo fuerte: **en operaciones no presenciales debe combinarse con un segundo factor**; en presenciales puede usarse sola. También califican certificados de firma digital (Ley 527 de 1999) y OTP con segundo factor.



Verificación contra fuentes oficiales

Quien use biometría como factor de autenticación debe **verificar la identidad** contra bases de la Registraduría Nacional, operadores de servicios ciudadanos digitales o bases propias debidamente constituidas.



Protección de datos biométricos

Plantillas almacenadas con tokenización o cifrado fuerte; **prohibición de almacenar muestras de autenticación** (salvo excepciones autorizadas); información demográfica separada de las plantillas y relacionada por códigos no descifrables fácilmente.



Conocimiento del cliente (SARLAFT)

La verificación efectiva de identidad en la vinculación **debe usar fuentes confiables e independientes**; biometría, firma digital y autenticación fuerte son medios expresamente admitidos.



Prueba de vida obligatoria

Sin prueba de vida, una **autenticación puede ser objetada** durante una investigación de fraude.

Requisito de la CBJ, cómo lo cumple Unicus

Unicus fue construido sobre biometría facial 3D certificada (FaceTec) y una arquitectura cloud empresarial en AWS, con cada requisito de la CBJ resuelto de fábrica:



	Biometría como mecanismo fuerte de autenticación →	Motor biométrico único para enrolamiento y autenticación 1:1 en operaciones sensibles, integrable como factor fuerte en sus canales vía API/SDK (web, iOS, Android, React Native).
	Prueba de vida con propiedades fisiológicas →	Liveness 3D certificado: reconstrucción tridimensional del rostro y señales fisiológicas en vivo. Resiste fotos, videos, máscaras, deepfakes e inyección de cámara virtual.
	Cifrado y tokenización de plantillas →	Plantillas biométricas cifradas; cifrado en reposo (KMS) y en tránsito; datos demográficos almacenados por separado.
	No almacenamiento de muestras de autenticación →	Flujo de autenticación diseñado para operar sobre plantillas, con políticas de retención configurables según su marco de datos.
	Verificación documental y contra fuentes confiables →	Validación del documento de identidad y cotejo facial 1:1; arquitectura preparada para integrar verificación contra fuentes oficiales según la habilitación de su entidad.
	Trazabilidad para auditoría y supervisión →	Registro auditable por transacción: resultado, sello de tiempo y contexto, el insumo directo para auditoría interna, revisoría y requerimientos de la SFC.
	Seguridad de la plataforma →	Infraestructura AWS con arquitectura alineada a ISO 27001 y prácticas de remediación continua de hallazgos de seguridad.



Integración sin rehacer su arquitectura: Unicus se consume **vía API REST y SDKs nativos**. El equipo de ingeniería de Tekbees acompaña la integración de punta a punta — el mismo equipo que construyó la plataforma, no un partner de implementación.

Cumplir no tiene por qué costar como un proveedor global

Los proveedores globales de verificación de identidad suelen llegar con licencias de plataforma, mínimos anuales en dólares y consultoría de integración facturable. UNICUS entrega la misma clase de tecnología biométrica certificada con una estructura de costos pensada para el mercado colombiano:



Pago por verificación, no por promesas

Modelo de **tarifas escalonadas por volumen**: paga menos por transacción a medida que crece. Sin licencias de plataforma infladas.



Sin mínimos de entrada elevados

Planes de volumen graduado, volumen comprometido o usuario activo, según su operación. Empiece con un piloto y **escale con resultados**.



Costo total de propiedad menor

Integración vía API/SDK con **acompañamiento directo del equipo** de ingeniería — sin meses de consultoría facturable ni intermediarios.



Equipo local, contratación local

Soporte en español desde Bogotá, contratación en Colombia y acuerdos en moneda local posible: **sin la volatilidad ni los sobrecostos** de un contrato 100% en USD.

Descubra en **30 minutos** si su plataforma realmente **cumple la CBJ**

Sin costo • Sin compromiso

Durante la sesión revisamos



Autenticación fuerte

Evaluamos si su flujo cumple los mecanismos exigidos por la CBJ.



Prueba de vida

Verificamos si su solución resiste fotos, videos y deepfakes.



Trazabilidad

Revisamos la evidencia disponible para auditorías y supervisión.



Verificación de identidad

Analizamos el uso de fuentes confiables y controles de identidad.

¿Su plataforma puede responder **Sí** a estas preguntas?



¿Tiene prueba de vida certificada?



¿No almacena muestras biométricas?



¿Las plantillas están cifradas?



¿Puede demostrar cada autenticación ante una auditoría?



¿Verifica identidad contra fuentes confiables?



Si respondió “No” a una sola...

Vale la pena revisar su plataforma

Agende su Diagnóstico Express CBJ

30 minutos • Sin costo • Equipo Tekbees



<https://www.tekbees.com>



<https://www.linkedin.com/company/tekbees/>

Reciba un diagnóstico claro, recomendaciones y una demostración en vivo de la tecnología Unicus.