VerificaID

Onboarding digital e identidad

Análisis ético de vulnerabilidad

Noviembre 2025

PROHIBIDA LA REPRODUCCÍON TOTAL O PARCIAL DEL DOCUMENTO SIN AUTORIZACIÓN EXPRESA DE VERIFICAID O LOS RESPONSABLES DEL ESTUDIO
Difusión controlada

La Falla de la Puerta Abierta

Cero Fricción = Cero Certeza

Nuestro análisis identificó una brecha estructural en la lógica de onboarding.

El sistema actual prioriza la velocidad sobre la verificación.

Caso plataforma fintech anónima

ENTRADA: DNI + Fecha de Nacimiento

↓

RESULTADO: Acceso Completo e Inmediato

Cualquiera con datos públicos puede crear una cuenta válida.

Resumen ejecutivo

Bajo el método y supuestos aplicados, e incluso asumiendo que la empresa evaluada cuente con ciertos elementos propios de un sistema de cumplimiento como lineamientos internos, roles asignados o procesos operativos, **la fragilidad del modelo de identidad observada tendría la capacidad de limitar o neutralizar la efectividad de cualquier control posterior**.

Hoy, la plataforma autocompleta los datos y otorga acceso inmediato.

Este diseño expone a la organización a riesgos inmediatos y materiales:

- Suplantación de identidad
- Creación de perfiles falsos
- Operaciones realizadas por terceros
- Incidentes de fraude operativo
- Reclamos y reversos por transacciones no reconocidas
- Observaciones regulatorias (Indecopi / ANPD)
- Afectación directa a la confianza del usuario

La brecha identificada es estructural, ya que en un negocio completamente digital que mueve fondos de terceros, la validación de datos es el pilar central de cualquier modelo de control.

Sobre el análisis

El estudio se centró exclusivamente en:

- **El proceso de onboarding digital:** captura de datos, flujo de registro, habilitación de la cuenta y lógica de validación.
- **Los mecanismos de identidad inicial esperados:** documentos requeridos, autenticación, biometría, prueba de vida, verificación contra fuentes confiables.
- **La coherencia entre UX y seguridad:** evaluación de cómo la experiencia del usuario impacta en la mitigación del riesgo de suplantación.
- **Riesgos derivados del diseño observado:** impacto en fraude, reputación, operaciones y cumplimiento.

Importante:

No se evaluaron estructuras internas, niveles de madurez del sistema de cumplimiento ni documentación operativa, dado que dicha información es propiedad de la organización propietaria de la plataforma y confidencial.

Las conclusiones se basan únicamente en la evidencia observable en el flujo de registro y en el criterio aplicado para identificar oportunidades de mejora a nivel sectorial.

Red flags críticas

Validación de identidad insuficiente (brecha estructural)

El usuario puede registrarse con datos públicos (DNI + fecha de nacimiento) y acceder sin controles que confirmen que es el titular.

Ausencias detectadas:

Sin validación documental (DNI físico/digital)
Sin captura de selfie o prueba de vida
Sin comparación biométrica

Impacto

Máxima exposición a suplantación y perfiles falsos

Falta de trazabilidad y fiabilidad del proceso de verificación

El sistema no genera evidencia suficiente para demostrar que la persona es el titular de los datos en el momento del registro.

Impacto

Limitación severa de mecanismos posteriores de control KYC o antifraude

Red flags críticas

Riesgo normativo transversal

Aunque no sea Sujeto Obligado supervisado, la entidad enfrenta riesgos por:

Indecopi: fallas de seguridad, suplantación, afectación al consumidor.

ANPD: medidas insuficientes de protección de datos personales.

Entidades financieras: cuestionamientos sobre identidad del cliente.

Impacto

Posibles acciones administrativas y requerimientos de mejora por parte de Indecopi y ANPD, así como restricciones operativas de bancos corresponsales, además de un desgaste reputacional derivado de incidentes de suplantación o fallas percibidas de seguridad.

Red flags críticas

Exposición operativa elevada

La brecha de identidad incrementa:
Reclamos
Reversos
Reprocesos manuales
Falsos positivos
Carga sobre equipos internos

Impacto

Ineficiencia técnica, tiempos de atención y costos operativos.

Autenticación posterior no robusta

Dependencia de mecanismos del dispositivo (Face ID/Touch ID) y no de la plataforma.

Impacto

Operaciones no reconocidas

Riesgos estratégicos identificados

- Suplantación de identidad (alta probabilidad)
- Operaciones realizadas por terceros (sin trazabilidad real)
- Afectación a la confianza del usuario y reputación de marca
- Desgaste en áreas críticas (soporte, operaciones, riesgo)
- Debilitamiento del modelo KYC y del ciclo de vida del cliente
- Vulnerabilidad frente a incidentes mediáticos o regulatorios

Conclusión ejecutiva

La brecha representa un riesgo central que afecta la integridad del modelo operativo y la gestión del riesgo.

Independientemente del grado de madurez que la empresa pueda tener internamente, **el modelo de onboarding observado no cumple con los estándares mínimos esperados para el año 2025**.

Corregir esta brecha va más allá de un ajuste técnico, **es una decisión estratégica clave** para proteger la operación, la reputación y la confianza del usuario, además de elevar el estándar de las operaciones digitales peruanas.

En el contexto fintech peruano, marcado por suplantación de identidad creciente y validaciones débiles, **mantener procesos digitales con el diseño identificado expone a las empresas a riesgos operativos, económicos y regulatorios.**

Ficha técnica del estudio

Características de la plataforma evaluada

Entidad digital especializada en servicios de cambio de divisas (Fintech FX).
Clasificación Tier 1 VerificaID, con expectativas altas de madurez en controles de onboarding, KYC y prevención de LA/FT.

Proceso analizado

El estudio se concentró en el onboarding digital y la creación de cuentas, evaluando el flujo completo de registro, los puntos de control de identidad y la habilitación de acceso al entorno transaccional.

Importante: Quedaron fuera del alcance los componentes no relacionados con la creación de cuentas de usuario.

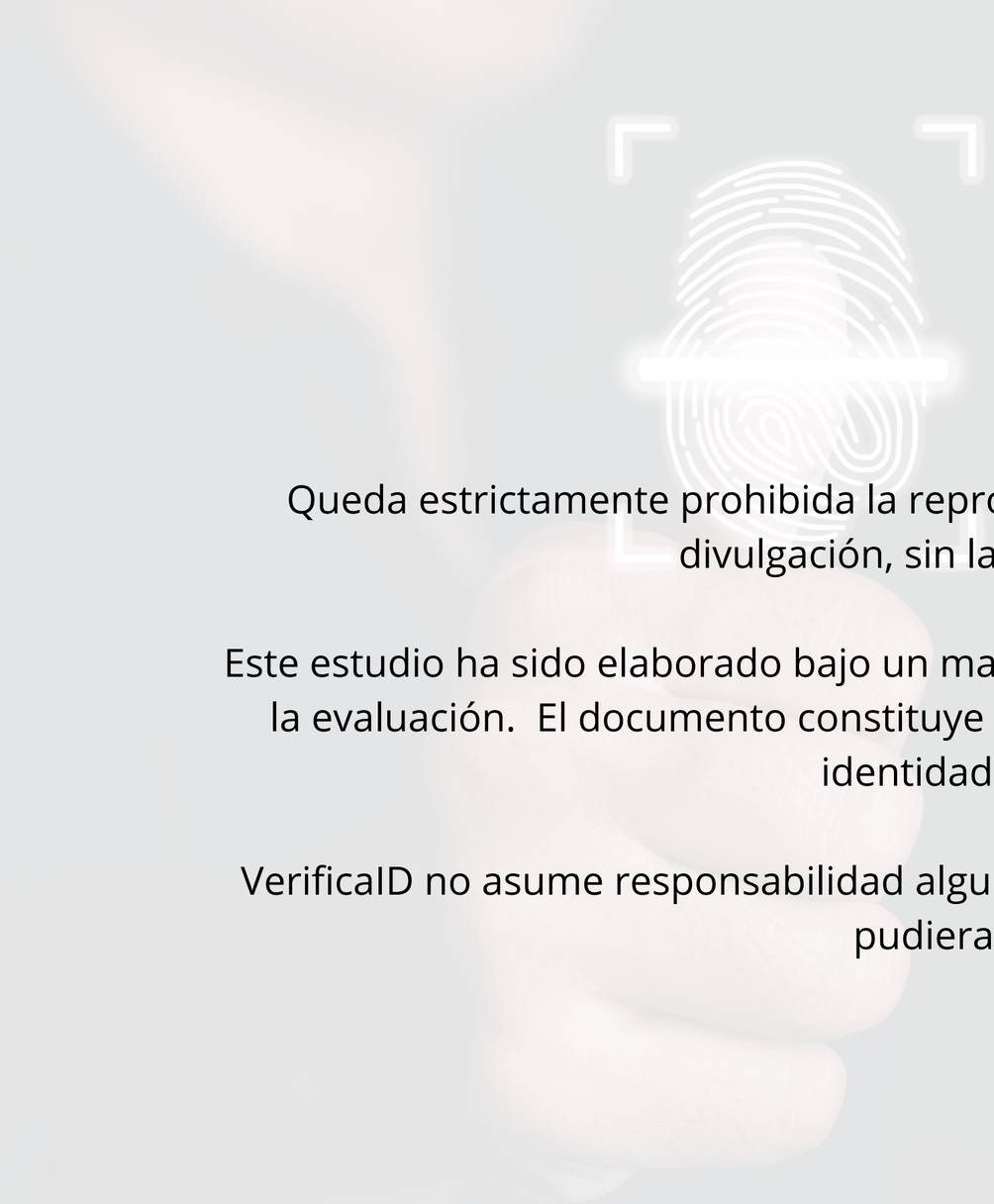
Equipo responsable

NATALIA SOLIS

Definición de la visión global del estudio, presentación de hallazgos y alineamiento con la agenda de VerificaID.

YEMIKO HAMADA - COMPLIANCE PARTNER Y ESPECIALISTA EN RIESGO REGULATORIO (SBS/UIF)

Análisis y traducción de los hallazgos en implicancias regulatorias concretas, identificación de posibles observaciones de supervisión y estimación del nivel real de exposición a sanciones, medidas correctivas y riesgos LAFT asociados.



Queda estrictamente prohibida la reproducción total o parcial de este documento, así como su distribución o divulgación, sin la autorización expresa y por escrito de VerificaID.

Este estudio ha sido elaborado bajo un marco metodológico ético, utilizando información disponible al momento de la evaluación. El documento constituye un diagnóstico estratégico orientado a exponer brechas potenciales de identidad digital, riesgo operativo y cumplimiento.

VerificaID no asume responsabilidad alguna, directa o indirecta, derivada de decisiones, acciones o inacciones que pudieran tomarse con base en este contenido.