Documento de conclusiones sobre el desarrollo y los resultados de las pruebas del proyecto "DIDIT".

DIRECCIÓN GENERAL DE POLÍTICA ESTRATÉGICA Y ASUNTOS INTERNACIONALES
Febrero 2026

1. ANTECEDENTES

La Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero (en adelante, "**Ley del sandbox**") regula un entorno controlado de pruebas que permite llevar a la práctica proyectos tecnológicos de innovación en el sistema financiero. Con fecha 13 de octubre de 2023, MARKETS PROLIVE 360, S.L. (en adelante, "**el Promotor**") presentó una solicitud para acceder al espacio controlado de pruebas (en adelante, "el **Sandbox**") con un proyecto piloto denominado **"DIDIT**".

El objetivo de este Proyecto en el Sandbox era verificar el cumplimiento regulatorio de una solución de identidad digital, con el fin de implementarla en la industria financiera para fomentar economías de escala y reducir la complejidad operativa. La solución se materializa a través de la creación de una identidad digital para cada usuario que está asociada a una wallet digital que podría permitir custodiar y transferir criptoactivos.

Con fecha 16 de enero de 2024 la Secretaría General del Tesoro y Financiación Internacional publicó, en su sede electrónica, la lista de proyectos de la cuarta cohorte que recibieron una evaluación previa favorable para acceder al entorno de pruebas. Entre los proyectos que se asignaron a la Comisión Nacional del Mercado de Valores (**CNMV**) como Autoridad Supervisora encargada de su monitorización, se encontraba el referido Proyecto.

Con fecha 29 de mayo de 2024 la CNMV y el Promotor suscribieron el Protocolo de Pruebas (en adelante, el "**Protocolo**") de acuerdo con el artículo 8 de la Ley del Sandbox. En el mismo, se establecían los términos y condiciones de la participación de los Promotores en el espacio controlado de pruebas y, entre otras cuestiones, se detallaban las distintas pruebas que se llevarían a cabo por parte del Promotor en las distintas fases del Proyecto, así como los objetivos que se pretendían alcanzar con cada una de las pruebas.

Las pruebas previstas en el Protocolo se iniciaron el 1 de noviembre de 2024 y finalizaron el 9 de julio de 2025.

Con fecha 31 de julio de 2025, el Promotor remitió a la CNMV la Memoria de Resultados requerida por el apartado 1 del artículo 17 de la Ley del Sandbox, con la evaluación de los resultados de las pruebas y del conjunto del Proyecto.

El apartado 3 del artículo 17 de la Ley del Sandbox establece que la Autoridad Supervisora que haya sido responsable del seguimiento de las pruebas elaborará un documento de conclusiones sobre su desarrollo y resultados. Dichas conclusiones se tendrán en cuenta a efectos de lo previsto en los artículos 25 (el Informe anual sobre transformación digital del sistema financiero elaborado por la Secretaría General del Tesoro y Financiación Internacional) y 26 (inclusión en la Memoria anual de las autoridades supervisoras de un informe sobre la aplicación de la innovación de base tecnológica a sus funciones supervisoras). En cumplimiento de lo establecido en el citado apartado 3 del artículo

17 de la Ley del Sandbox, se elabora el presente documento, en el que se recogen las conclusiones sobre el desarrollo de las pruebas y sus resultados.

2. PARTICIPANTES, DESCRIPCIÓN Y OBJETIVO DE LAS PRUEBAS

2.1. Descripción

El Proyecto se basa en la implementación de una solución de identidad digital basada en la lectura criptográfica del chip NFC de documentos oficiales y en técnicas de biometría facial con prueba de vida activa. Su finalidad es reforzar los procesos de alta digital de clientes en cumplimiento de la normativa de prevención de blanqueo de capitales y financiación del terrorismo.

2.2. Participantes

En las pruebas han participado 50 usuarios para darse de alta en la solución de DIDIT. Asimismo, el propio equipo de DIDIT realizó pruebas específicas en el sector financiero para conseguir los objetivos perseguidos.

2.3. Objetivo

El objetivo del Proyecto se ha centrado en verificar el funcionamiento y las oportunidades de la utilización de la identificación digital a través de la lectura de los NFC, probando una solución que da respuesta a una necesidad del mercado: identificar de manera ágil y segura a los clientes cumpliendo con la normativa aplicable de PBC/FT y lucha contra el fraude.

El proyecto tenía como propósito crear una solución de custodia de wallets que quedaba vinculada a una identidad verificada por DIDIT a través de un proceso robusto que utilizaba la lectura del NFC del Documento Nacional de Identidad. Se validaría si la solución de identidad digital cumplía con la normativa de PBC/FT actual y, si era susceptible de una adopción amplia para la identificación y verificación de la identidad por parte de los sujetos obligados u otras entidades que deben verificar la identidad o luchar contra el fraude adoptaran la solución.

De acuerdo con este objetivo se establecieron las siguientes fases:

- Fase 1: Registro y onboarding digital para la verificación de la identidad.
- Fase 2: Creación de la identidad digital verificada.
- Fase 3: Uso de la identidad digital por parte del usuario en una entidad financiera (opcional)[1].
- Fase 4: Actualización de la identidad digital por parte del usuario[2].
- Fase 5: Realizar transacciones de criptoactivos MiCA desde la wallet verificada (opcional)[3].

No obstante, tras los avances del proyecto, se mantuvieron reuniones con SEPBLAC y se acordó con el promotor centrar las pruebas en la propuesta de valor de verificación de la identidad y poner a prueba su solución con mecanismos de suplantación de identidad modernos como forma de prevención de fraude. Se decide por tanto no afrontar las pruebas opcionales inicialmente definidas.

A partir de esta redefinición del enfoque inicial, los esfuerzos se han centrado en **analizar si la**

[1] Esta fase finalmente no se ha realizado.

[2] Esta fase finalmente no se ha realizado.

[3] Esta fase se ha realizado únicamente con importes muy bajos de criptoactivos (5 USDC) que los promotores regalaron a los participantes dados de alta.

solución de identidad digital propuesta se ajustaba a las exigencias normativas vigentes y determinar su viabilidad para ser utilizada en procesos de identificación y verificación de identidad que requieran un alto nivel de garantías.

Los Promotores llevaron a cabo labores de investigación sobre los mecanismos de fraude más utilizados en el ámbito financiero, para poner a prueba si su herramienta era capaz de detectar estas situaciones fraudulentas y, por tanto, aportaban un valor claro al ecosistema financiero actual.

Por todo ello, las pruebas realizadas, y que se describen a continuación se han centrado exclusivamente en las fases 1 y 2.

3. DESARROLLO Y RESULTADO DE LAS PRUEBAS

3.1 Desarrollo de las pruebas previstas en el protocolo

De las **fases establecidas en el protocolo de pruebas**, finalmente las mismas se centraron, en un primer momento, en las Fases 1 y 2.

El objetivo de estas fases era testear la propia herramienta de identificación de clientes a través del uso de NFC dentro del aplicativo de DIDIT. Para ello, se llevaron a cabo pruebas con documentos de identidad de otras personas, con documentos de identidad falsos o pruebas de cruces contras listas y se fueron recabando las distintas evidencias de cada uno de los casos. Si bien, como estas pruebas eran sencillas, posteriormente se decidió realizar pruebas más avanzadas.

Los resultados de estas primeras pruebas han sido los siguientes:

FASE 1. Registro y onboarding digital para la verificación de la identidad

Esta primera fase se centró en probar el acceso a la app por los distintos participantes y el proceso de identificación digital con el documento de identidad. Para ello se realiza la verificación utilizando diversas tecnologías (OCR[4], NFC, y biometría) y la revisión de listas.

Se ha probado la solución de DIDIT que incluye una capa de seguridad adicional mediante la lectura del chip recogido en el DNI, lo que permite:

- Seguridad muy elevada de que el documento original se utiliza en el momento del proceso, y, por tanto, que no se utiliza un documento falso ni modificado.
- Mediante la prueba de vida que se realiza durante el propio proceso, garantías muy elevadas de la verificación de la identidad, dado que se prueba que la persona titular del documento se encuentra en el momento de la verificación. Mediante la lectura del NFC se accede a una foto que se coteja con la persona que está siendo verificada.
- Realizar el cruce contra listas de la persona identificada.

Se realizaron pruebas con un DNI caducado verificando que el proceso da error y no permite continuar.

Asimismo, se han llevado a cabo pruebas intentando falsear la identidad del usuario mediante:

- El uso de un DNI de otro usuario (suplantación de identidad). La herramienta identifica que no hay correlación entre la fotografía del DNI y la prueba de vida realizada donde se observa que, si bien la prueba de vida es correcta, no se trata de la misma persona por lo que existe una suplantación de identidad rechazándose la identificación.

[4] Reconocimiento óptico de caracteres.

- Pruebas con un DNI falso impreso (falsedad documental). Al ser un documento fotocopiado y no uno real no se puede proceder a la lectura del NFC y el proceso no permite llevar a cabo la identificación, siendo esta rechazada. En este caso se acaba el proceso y no permite continuar.

- El cambio de la foto de un DNI supuestamente robado (fraude por sustitución de fotografías). En este caso se inserta una fotografía falsa encima del DNI auténtico. Al haber realizado la lectura del NFC correspondiente del DNI, la herramienta procede a realizar la relación de la fotografía original del documento, extraída del NFC, por lo que puede verificarse debidamente que la prueba de vida realizada posteriormente no concuerda con la persona del DNI.

Asimismo, se han realizado pruebas de registro de un sujeto criminal perseguido por el FBI y una PEP (Persona Expuesta Políticamente), y en ambos casos se ha detectado.

El resultado de las pruebas anteriores ha sido satisfactorio.

FASE 2. Identidad digital verificada

- Creación identidad digital verificada asociada a una *wallet* digital

Se crea la identidad digital para un grupo de 50 usuarios. Cada identidad digital se asocia a una *wallet* digital. Las wallets se crean con una serie de restricciones de acuerdo con los siguientes parámetros:

- Limitación del valor máximo de cada transacción individual a 500 euros.

- Limitación de 10 transacciones diarias.

Se confirma que la *wallet* digital, que va asociada a cada una de las identidades digitales creadas a los usuarios, se crea sin que exista ninguna interacción por parte de los usuarios, sino de forma automática cuando se supera satisfactoriamente el proceso de identificación previo.

3.2 Pruebas avanzadas y análisis de procesos de identificación de clientes realizado por DIDIT

FASE 3. Análisis de procesos de identificación de clientes.

Los Promotores propusieron analizar distintos procesos de identificación de clientes para poder adaptar las pruebas a situaciones reales. Para ello:

- Identificaron las prácticas más habituales de suplantación de identidades y fraude.

- Adquirieron una impresora de tarjetas para falsificar documentos de identidad que les permitía hacer falsificaciones con distintos niveles de calidad y sofisticación.

- Adquirieron máscaras hiperrealistas para tratar de realizar suplantaciones de identidad con caras falsas.

- Realizaron pruebas de alta en diferentes entidades para verificar si su solución era capaz de detectar las distintas actividades fraudulentas.

Estas pruebas se realizaron durante los meses de abril y mayo de 2025.

El objetivo de esta fase era demostrar que cualquier proceso de identificación digital, aunque cumpla con los estándares normativos de PBC/FT, podría ser más eficaz con la validación del chip

NFC para evitar situaciones de suplantación de identidad.

Las conclusiones obtenidas en estas pruebas han sido las siguientes:

- Con un DNI impreso con una foto falsa (Deep-fake[5]) un atacante puede superar muchos de los procesos de identificación digital, incluso el procedimiento de video-identificación que incluye prueba de vida, mostrar el anverso y el reverso del DNI mientras se graba al potencial cliente o la verificación manual si es necesario.
- Los procesos que introducen prueba criptográfica (lectura NFC del chip del documento de identidad) y prueba de vida activa han sido capaces de detectar y bloquear el fraude en los ensayos de laboratorio realizados.
- Disponer de acceso a una API estatal que devuelva datos e imagen originales del DNI reduciría drásticamente el fraude. Sin embargo, hoy su cobertura es nacional y fragmentada mientras que la lectura NFC ya protege más de 150 países gracias al estándar ICAO 9303[6].

Los vectores de ataque que se han verificado en las pruebas han sido los siguientes:

a) Ataque sobre el documento

Ataque	Compleljidad	Mitigación
DNI impreso con foto del atacante	Media	Lectura NFC+DG2[7] ↔ selfie
DNI impreso con foto Deep-fake	Media	Lectura NFC+DG2 ↔ selfie El Deep-fake debe además sincronizarse con PAD[8] activo.
Documento robado o chip clonado	Alta	Cadena PKI[9] (CSCA[10] → DSC[11]) + PIN CAN + selfie matching.

- DNI impreso con foto del atacante: En este caso se realiza una impresión de un DNI con foto de alta calidad del atacante. La prueba del selfie pasa los controles, pero no en el caso de realizarse la lectura del NFC.
- DNI impreso con foto Deep-fake: En este caso la foto se genera mediante inteligencia artificial. Para que el ataque sea exitoso hay que sincronizarlo con la prueba de vida activa. Los mecanismos de Detección de Ataques de Presentación (PAD), que son sistemas diseñados para determinar si una muestra biométrica es auténtica o si es un intento de suplantación de identidad, detectan intentos de engaño utilizando soportes falsos como impresiones, vídeos o imágenes generadas por IA lo que dificulta el ataque.
- Documento robado o chip clonado: En este caso ya se cuenta con el documento original (DNI robado) o bien con el chip clonado que permitiría acceder al control del

[5] Un deepfake es una técnica de inteligencia artificial que permite crear o manipular imágenes, videos o audios para que parezcan reales, incluso cuando son completamente falsos. En esencia, se trata de "ultrafalsos" generados con aprendizaje profundo, donde se reemplazan o superponen rostros o voces de personas en contenido existente, o se crean desde cero

[6] Establece los estándares internacionales para los documentos de viaje, incluyendo los pasaportes, tarjetas de identidad y visas. Las normas ICAO están vigentes para los DNI electrónicos (eID) los Kids-ID y los pasaportes. Esta norma propone unas exigencias a nivel mundial para que sus fotos de identificación sean infalsificables y no puedan ser sustituidas.

[7] Fotografía de alta calidad.

[8] PAD: es como se denomina la solución de detección de ataques de presentación biométrica que requiere el estándar ISO. Este estándar establece las técnicas o mecanismos para la detección automatizada de ataques de presentación. Estas técnicas se denominan mecanismos de detección de ataques de presentación (PAD).

[9] PKI: Infraestructura de clave pública.

[10] CSCA: Autoridad de Certificación de País Emisor.

[11] DSC: Firma digital

NFC (accedería a los datos del DNI que tiene la Autoridad de Certificación del País Emisor - en el caso de España se accedería a la información de la Policía Nacional y a la firma digital). Sin embargo, tendría que pasar el control del selfie ya que el atacante no coincidiría con la foto en poder de la Autoridad Certificadora.

b) Ataque sobre biometría facial

Ataque	Compleljidad	Mitigación
Replay selfie	Baja	PAD activo (gestos, latencia).
Mascara 3D	Media	PAD multiespectral, profundidad.
Deep fake en vivo	Alta	PAD ISO 30107-3 L2+[12], análisis forense de frames.

- Replay selfie: En estos casos la complejidad del ataque es baja ya que se trata de fotos estáticas y la mitigación es sencilla con una prueba de vida.
- Deep-fake en vivo. Se genera la imagen con inteligencia artificia. La complejidad del ataque es alta y la mitigación se basa en la aplicación de la norma ISO 30107-3, concretamente en los ataques de nivel 2 que se centran en pruebas de ataques más sofisticados como máscaras 3D y otras réplicas complejas.

Métodos de verificación y exposición a IA generativa

Método	Fatores verificados	Exposición a IA generativa	Dificultas de bypass	Riesgo residual
Estándar Foto documento + selfie (PAD pasiva)	OCR + face-matching	Muy alta	Baja-media	Alto
Vídeo + PAD activo Documento en vídeo + gestos	Vídeo automático + PAD activo	Alta	Media	Medio-alto
Vídeo-identificación Vídeo sincrónico + revisor humano	Mostrar anverso/reverso y girar documento + Revisión manual certificada	Alta Un DNI impreso con foto cambiada (o deep-fake) supera la revisión ocular si el impostor hace la prueba de vida	Baja-media	Medio-alto
NFC + Selfie con PAD activo Lectura chip + gestos (propuesta estándar)	Validación PKI (DG1/DG2) - Selfie ↔ foto DG2 - PAD activo L2	Muy baja Requiere documento físico y deep-fake que coincida con foto firmada	Muy alta	Bajo

- Estándar: Se realiza con fotos estáticas. Es posible vulnerar estos controles con falsificaciones de documentos impresos y sin grandes sofisticaciones ya que, al no haber firma digital es fácil engañar al sistema.
- Control vídeo + PAD activo: Mejora el método anterior, pero sigue sin evidencia criptográfica. Los Deep-fakes ya ejecutan gestos aleatorios. Además, el atacante puede pasar la prueba de vida si usa su imagen en el documento.
- Vídeo-identificación: Cumple con los requisitos formales (grabación, custodia, revisor). La

[12] ISO 30107-3 que se centra en la detección de ataques de presentación (PAD) para garantizar la seguridad de los sistemas biométricos. Establece métodos para probar la eficacia de los mecanismos PAD y clasifica los tipos de ataques conocidos en dos niveles. El nivel 1 (L1) prueba ataques básicos como fotos impresas y vídeos. El nivel 2 (L2) prueba ataques más sofisticados como máscaras 3D de alta calidad.

limitación viene porque el revisor no valida la firma del chip. Basta con un documento de DNI impreso con foto alterada y una prueba de vida convincente para engañar al sistema.

- Solución DIDIT: verificación de NFC y PAD activo: La combinación de la lectura del chip NFC del DNI/pasaporte junto con una Prueba de vida activa (PAD) representa un estándar más seguro y fiable por las siguientes razones:

  - Validación criptográfica auténtica y no replicable del documento de identidad.

    La lectura NFC permite acceder al chip integrado en documentos oficiales (DNI, pasaporte electrónico, tarjetas de residencia, etc) y verificar la firma digital (DSC) del documento frente a la Autoridad de Certificación de País Emisor (CSCA).

    Esta verificación es criptográficamente segura y no puede ser reproducida ni falsificada por técnicas tradicionales de impresión o manipulación visual.

    Es el único mecanismo técnico que permite verificar con certeza que el documento ha sido emitido por una autoridad oficial válida y no ha sido alterado.

  - Uso de un estándar internacional reconocido (ICAO 9303)

    Este protocolo está definido por la Organización de Aviación Civil Internacional (ICAO) y adoptado globalmente como el estándar para documentos de identidad electrónicos.

    Actualmente está implementado en los pasaportes y en e-IDs de más de 150 países, lo que garantiza interoperabilidad legal y técnica.

    Esto lo convierte en una solución alineada con los principios de neutralidad tecnológica, reconocimiento mutuo de documentos y proporcionalidad, esenciales en el marco del Reglamento eIDAS, la 6ª Directiva AML y otras normativas europeas.

  - Método eficaz contra la suplantación sofisticada

    La verificación NFC + PAD es capaz de bloquear intentos avanzados de suplantación de identidad como el uso de documentos físicos falsificados (aunque sean de alta calidad), las imágenes manipuladas digitalmente o los Deepfakes o vídeos pregrabados.

    La comprobación biométrica activa (PAD) asegura que hay una persona viva frente a la cámara y la lectura NFC garantiza que la imagen facial biométrica proviene de un documento auténtico emitido por una autoridad válida.

  - Solución alineada con los estándares exigidos por las autoridades supervisoras

    Cada vez más supervisores financieros, registradores, notarios y auditores requieren que los procesos de identificación a distancia puedan acreditar la autenticidad del documento, la identidad real de la persona y la integridad del proceso de verificación.

    La lectura del chip NFC es un medio considerado equivalente funcional a una revisión presencial del documento físico, al proporcionar evidencia verificable de origen y no manipulación.

3.3 Resultados de las pruebas

- Ataque sin utilización de NFC- vulnerabilidad genérica del sector

Las pruebas se han realizado con foto o vídeo más PAD activo (equivalente al de la mayoría de los proveedores). Los resultados fueron los siguientes:

1. El documento impreso supera las validaciones documentales y de lógica MRZ[13].
2. El vídeo-selfie (vídeo real del atacante) coincide con la imagen alterada del documento. El face-matching se hace contra la foto que el atacante ha impreso y no contra la imagen oficial con lo que pasa el sistema.
3. PAD activo detecta parpadeo y giro de cabeza. Las pruebas de vida basadas en gestos no distinguen si la foto del documento es auténtica.
4. Resultado de la prueba: El proceso se pasa y el alta del cliente es aprobado.

- Ataque con utilización de NFC- fraude abortado al instante

  En este caso las pruebas se realizaron accediendo al NFC del documento. El resultado fue que el flujo NFC fue el único que bloqueó la suplantación, sin intervención humana, confirmando que la vulnerabilidad es inherente a cualquier KYC sin verificación criptográfica.

- Otras pruebas realizadas

  Se creó una identidad sintética con máscara hiperrealista y se realizaron las mismas pruebas. En este caso, se rechaza la prueba de vida.

  La conclusión es que con máscaras hiperrealista cuesta mucho engañar al sistema.

En conclusión, la solución de DiDIT que combina NFC + PAD representa una herramienta técnica avanzada para prevenir suplantaciones de identidad en procesos regulados. No solo eleva el nivel de seguridad antifraude, sino que permite a las entidades cumplir con mayor solidez los requerimientos legales de diligencia debida, trazabilidad y prevención de blanqueo de capitales y de la financiación del terrorismo, como también el fraude.

4. CONCLUSIONES

4.1. Conclusiones del Promotor

En el entorno actual de transformación digital, los procesos de alta de clientes en entidades financieras a distancia mediante vídeo-identificación se han consolidado como una práctica habitual entre los sujetos obligados en materia de prevención del blanqueo de capitales y financiación del terrorismo (PBC/FT). Esta expansión ha estado motivada por criterios de eficiencia, escalabilidad y experiencia de usuario.

En los últimos años, la mejora de las herramientas tecnológicas aplicadas a la identificación remota ha llevado a una percepción generalizada de que la no presencialidad no implica necesariamente un mayor riesgo. No obstante, esta conclusión no siempre se ajusta a la realidad ya que, sin controles reforzados, los procesos digitales pueden presentar vulnerabilidades superiores a los presenciales.

Los resultados de las pruebas realizadas ponen de manifiesto que los procedimientos de identificación no presencial autorizados presentan ciertas vulnerabilidades derivadas del uso de nuevas herramientas surgidas por la propia evolución tecnológica desde el momento de aprobación de los procedimientos hasta la actualidad.

[13] El código MRZ o Machine-Readable-Zone (Zona legible por la máquina) es un conjunto de cadenas alfanuméricas que suelen aparecer en el reverso del documento de identidad o pasaporte.

Uno de los principales factores es la priorización de la usabilidad y la experiencia de usuario sobre la seguridad o la dificultad y coste operativo de un cambio tecnológico sin una adecuada valoración del riesgo real que conllevan los canales remotos y su evolución. Este desequilibrio se agrava ante el crecimiento de amenazas como la suplantación de identidad, deepfakes o el uso de documentos manipulados, especialmente en procesos de verificación sin validación criptográfica.

La normativa española considera de alto riesgo los procesos de alta no presenciales, motivo por el cual exige medidas reforzadas como la firma electrónica cualificada, el primer ingreso desde cuentas verificadas, o procedimientos expresamente autorizados por SEPBLAC.

Por todo ello, el promotor **concluye**, a la luz de las pruebas realizadas:

1. **Sería recomendable establecer, en los procesos digitales verificación, NFC y Prueba de Vida Activa (PAD) especialmente en altas de clientes o productos de riesgo medio o alto.**

   Para entornos de contratación con alto nivel de riesgo (entidades de dinero electrónico, entidades de concesión de crédito, o entidades del ámbito de los criptoactivos, etc.), sería recomendable utilizar la lectura del chip NFC del documento oficial (DNIe, pasaporte electrónico, tarjeta de residencia, etc.) junto con una prueba de vida activa y dinámica, que permita verificar la correspondencia biométrica con garantías de integridad y autenticidad. Este modelo impide la suplantación mediante imágenes manipuladas, deepfakes o documentos falsos impresos. En todo caso, las recomendaciones o exigencias deben ser lo suficientemente flexibles para permitir a las entidades encontrar y cambiar a las medidas de control que sean necesarias para combatir los riesgos derivados de la digitalización que están en permanente evolución.

2. **Integración de mecanismos de verificación estatal mediante API, con fallback al chip NFC**

   En los casos en los que existan APIs nacionales oficiales de validación documental (como ocurre en algunos organismos del Estado), se debería permitir el uso de éstas como vía principal. En su defecto, el sistema debería recurrir de forma automática a la verificación mediante chip NFC, garantizando en todo caso la prueba criptográfica de validez del documento.

3. **Incorporación de atributos adicionales (data points) que refuercen la identidad digital**

   Para reducir el fraude residual, sería recomendable incorporar elementos verificables adicionales a la identidad digital del usuario, como el número de teléfono verificado por código SMS, la cuenta bancaria verificada vía conexión PSD2 (como prueba de titularidad) o la vinculación con perfiles digitales de redes sociales o historial digital persistente.

4. **Actualización de la guía del SEPBLAC**

   En la opinión del promotor sería razonable que el SEPBLAC reiterara la necesidad de cumplir en cualquier proceso de alta digital la normativa en vigor, incluyendo las Directrices EBA sobre identidad digital. De esta forma, se conseguiría clarificar la posibilidad que tienen los sujetos obligados de elaborar sus propios procedimientos de identificación no presencial con diferentes herramientas, pudiéndose apartar de la literalidad de los previsto en la Ley 10/2010 y su Reglamento de desarrollo.

   Atendiendo al contexto actual, sería aconsejable que las medidas de prevención contra el blanqueo de capitales y la financiación del terrorismo y lucha contra el fraude incluyeran mecanismos de verificación criptográfica de los documentos (p.e. mediante chip NFC o API oficial). Sería muy positivo promover modelos de identidad digital robustos que combinen

técnicas como las que se han puesto a prueba en el Sandbox y que se citan a continuación, u otras que sean técnicamente equivalentes:

- Verificación criptográfica mediante NFC.
- Biometría viva validada en tiempo real.
- Datos adicionales de contexto (teléfono, cuenta bancaria, etc.). Este modelo compuesto —basado en múltiples factores independientes— permite alcanzar niveles de seguridad equivalentes o superiores a la identificación presencial tradicional, con trazabilidad total y resistencia efectiva al fraude.

El modelo de vídeo-identificación ha cumplido una función esencial en la expansión de la identificación remota en España. No obstante, a la luz de las nuevas amenazas, las capacidades tecnológicas actuales y las exigencias regulatorias europeas, es necesario dar certeza regulatoria para exigir a las entidades sujetos obligados dar un paso más allá. La integración de verificación criptográfica (chip NFC o API oficial) junto con biometría activa y atributos digitales adicionales serviría para abordar prácticamente todos los vectores de ataque conocidos, permitiendo reducir el fraude a niveles residuales y garantizando el cumplimiento normativo de forma más sólida y estandarizada.

Valor añadido que ha demostrado el proyecto

El promotor considera que las pruebas realizadas con **su solución** han demostrado que **esta tecnología, basada en la lectura criptográfica del chip NFC** de documentos oficiales **y en técnicas avanzadas de biometría facial y prueba de vida activa**, **constituye una alternativa más segura**, **robusta y alineada con los estándares europeos y ayudaría a reforzar procesos actuales**. En particular, considera que esta solución:

- **Garantiza la autenticidad del documento** mediante verificación criptográfica.
- **Reduce de forma significativa el riesgo de suplantación de identidad**, incluso ante amenazas avanzadas como deepfakes o ataques con overlays[14].
- **Mejora la experiencia de usuario**, eliminando pasos innecesarios sin comprometer la seguridad.
- **Cumple con los requisitos de protección de datos, trazabilidad y control** exigidos por reguladores nacionales e internacionales.

Adicionalmente, **la solución cumple con las Directrices EBA mencionadas (EBA/GL/2022/15) sobre onboarding digital de clientes**, tanto en los aspectos técnicos como en los requisitos organizativos y de seguridad. En este sentido, el cumplimiento de estas directrices debería ser suficiente para que los sujetos obligados puedan utilizar la solución con total validez y seguridad regulatoria.

Además, el sistema incorpora funcionalidades adicionales de prevención, como:

- Análisis de IP desde el que se realiza el onboarding.
- Bloqueo facial ante intentos de fraude repetidos.

[14] La técnica del overlay consiste en interponer una pantalla por encima de la aplicación a la que quiere acceder el usuario, que queda en segundo plano. De esta manera, registra las pulsaciones o los datos que introducimos en ella en lugar de hacerlo en la página o la app a la que el usuario cree que está accediendo.

- Control de duplicidades de identidad.
- Registro y validación del cruce contra listas de sanciones y PEPs en tiempo real.
- Gestión de alertas y controles manuales en caso de alertas o porcentajes de error o alertas.
- Mantiene el registro de todas las operaciones e interacciones del sujeto obligado con cada alta de cliente, dando una trazabilidad completa.

Consideraciones finales y propuesta de actuación

El modelo de vídeo-identificación SEPBLAC tiene un papel clave desde su aprobación en España. No obstante, sería conveniente avanzar en la línea de permitir a las entidades cumplir con las Directrices de la EBA y en consecuencia, clarificar que pueden diseñar sus propios procedimientos de identificación no presencial, De esta forma, el proceso de DIDIT puede ser perfectamente válido como cualquier otro, siempre y cuando se cumplan las Directrices de la EBA.

4.2. Conclusiones de la autoridad supervisora

Las pruebas han permitido conocer los posibles riesgos a los que se enfrentan las entidades financieras en los procesos de onboarding. Trabajar de la mano del Promotor ha permitido, asimismo, identificar soluciones y alternativas seguras para evitar fraudes y ataques.

Durante todo el proceso se ha mantenido contacto no solo con el Promotor sino también con SEPBLAC que ha participado en las pruebas, creando un espacio de colaboración y aprendizaje mutuo, aportando evidencias y soluciones a los casos de riesgo. Asimismo, se ha mantenido informado al Tesoro sobre las diferentes decisiones y planteamientos de las pruebas al objeto de que las mismas pudieran ser de valor en el caso de una propuesta normativa, por parte del regulador o del propio SEPBLAC, que ayude en la mejora de la seguridad y confianza en el sector financiero. Desde el SEPBLAC se han valorado positivamente las medidas de refuerzo incorporadas en los procesos de identificación no presencial por parte del promotor.

Por último, se concluye que es necesario que las medidas incorporadas en estos procesos de identificación sean acordes con los riesgos que en cada momento se suscitan como consecuencia de la evolución de la tecnología, especialmente en sectores de alto riesgo como el financiero.