FATF

IDENTIDAD DIGITAL

MARZO DE 2020

El Grupo de Acción Financiera Internacional (GAFI) es un organismo inter-gubernamental independiente que desarrolla y promueve políticas para proteger el sistema financiero global contra el lavado de activos, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva. Las Recomendaciones del GAFI son reconocidas como la norma global de lucha contra el lavado de activos (ALA) y el financiamiento del terrorismo (CFT).

Para más información acerca del GAFI, por favor visite **www.fatf-gafi.org**

Este documento y/o todo mapa incluido aquí, se efectúa sin perjuicio del estado o de la soberanía sobre un territorio, de la delimitación de fronteras y límites internacionales y del nombre de un territorio, ciudad o área.

Referencia citada:

GAFI (2020), *Guía sobre Identidad Digital,* GAFI, París,
www.fatf-gafi.org/publications/documents/digital-identity-guidance.html

Índice de contenidos

SIGLAS

AAL 1/2/3	Nivel de Garantía de Autenticación (según el NIST)
AL	Nivel de garantía
ALA/CFT	Anti-lavado de activos y contra el financiamiento del terrorismo
API	Interfaz de programación de aplicaciones
ASP	Proveedor de servicios de autenticación
DDC	Debida diligencia del cliente
CEN	Comité Europeo de Normalización
CENELEC	Comité Europeo de Normalización Electrotécnica
CSP	Proveedor de servicios de credenciales
DCS	Servicio de verificación de documentos
DLT	Tecnología de libro mayor distribuido
APNFD	Actividades y Profesiones No Financieras Designadas
ETSI	Instituto Europeo de Normas de Telecomunicaciones
eIDAS	Reglamento (UE) nº 910/2014 sobre la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior
FAL 1/2/3	Nivel de garantía de la federación (según el NIST)
FIDO	Fast Identity Online (Identidad Rápida en Línea)
GDPR	Reglamento general de protección de datos
GPS	Sistema de posicionamiento global
GSMA	Sistema Global de Comunicaciones Móviles
ICT	Tecnología de la información y de las comunicaciones
IAL 1/2/3	Nivel de garantía de la identidad (según el NIST)
ID	Identidad
IDSP	Proveedor de servicios de identidad
IEC	Comisión Electrotécnica Internacional
NI R.	Nota Interpretativa de la Recomendación
IP	Protocolo de Internet
ISO	Organización Internacional para la Estandarización
ITU	Unión Internacional de Telecomunicaciones
IVSP	Proveedor de servicios de verificación de la identidad
LoA	Nivel de garantía
MAC	Control de acceso a los medios de comunicación
LA	Lavado de activos
MFA	Autenticación multifactorial
ONG	Organizaciones no gubernamentales
NIST	Instituto Nacional de Normas y Tecnología
OIDF	Fundación OpenID
PII	Información personal identificable
PIN	Número de identificación personal
R.	Recomendación
EBR	Enfoque basado en el riesgo

SAG	Grupo Asesor sobre Normas
SCA	Autenticación reforzada de clientes
FT	Financiamiento del terrorismo
PSAV	Proveedor de servicios de activos virtuales
W3C	Consorcio de la World Wide Web
ACNUR	Alto Comisionado de las Naciones Unidas para los Refugiados

RESUMEN EJECUTIVO

1. Los pagos digitales están creciendo a un ritmo estimado del 12,7% anual y se prevé que alcancen los 726.000 millones de transacciones anuales en 2020.1 Para 2022, se estima que el 60% del PBI mundial estará digitalizado.[2] Para el GAFI, el crecimiento de las operaciones financieras digitales requiere una mejor comprensión de cómo se identifican y verifican las personas en el mundo de los servicios financieros digitales. Las tecnologías de identidad digital (ID) están evolucionando rápidamente, dando lugar a una variedad de sistemas de identidad digital. Esta Guía está pensada para ayudar a los gobiernos, a los sujetos obligados[3] y a otras partes interesadas a determinar cómo se pueden utilizar los sistemas de identidad digital para llevar a cabo ciertos elementos de la debida diligencia del cliente (DDC) según la Recomendación 10 del GAFI.

2. La comprensión del funcionamiento de los sistemas de identidad digital es esencial para aplicar el enfoque basado en el riesgo recomendado en esta Guía. La Sección II de la Guía resume brevemente las características clave de los sistemas de identidad digital que se explican en detalle en el Anexo A.

3. La Sección III resume los principales requisitos del GAFI abordados en esta Guía, incluido el requisito de identificar y verificar la identidad de los clientes utilizando documentos, datos o información de fuentes «confiables e independientes» (Recomendación 10(a)). En el contexto de la identidad digital, el requisito de que los «documentos, datos o información de origen» digitales deben ser «confiables e independientes» significa que el sistema de identidad digital utilizado para llevar a cabo la DDC se basa en la tecnología, la gobernanza adecuada, los procesos y los procedimientos que proporcionan niveles adecuados de confianza en que el sistema produce resultados precisos.

> Los sistemas de identidad digital confiables e independientes, con medidas apropiadas de mitigación de riesgos, pueden ser de riesgo estándar, y pueden ser incluso de menor riesgo

La Guía aclara que la identificación del cliente y las transacciones no presenciales que se basan en sistemas de identidad digital confiables e independientes con medidas apropiadas de mitigación de riesgos, pueden presentar un nivel de riesgo estándar, e incluso menor.

4. El enfoque basado en el riesgo que se recomienda en esta Guía se basa en un conjunto de marcos de garantía y normas técnicas de código abierto, impulsados por el consenso, para los sistemas de identidad digital (denominados «marcos y normas de garantía de la identidad digital») que se han desarrollado en varias jurisdicciones. La Organización Internacional de Normalización (ISO), junto con la Comisión Electrotécnica Internacional

---

1 Capgemini & BNP Paribas (2018), *World Payments Report 2018*, consultado en línea en:https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf.

2 International Data Corporation (IDC), IDC FutureScape: Predicciones de la industria mundial de TI para 2019

3 A los objetivos de esta Guía, «sujetos obligados» se refiere a las instituciones financieras, a los proveedores de servicios de activos virtuales (PSAV) y a las actividades y profesiones no financieras designadas (APNFD), tal como se definen en los Estándares del GAFI y en la medida en que las APNFD están obligadas a llevar a cabo la DDC en las circunstancias especificadas en la R.22. En junio de 2019, el GAFI revisó la Recomendación 15 (Nuevas Tecnologías) y la NI.R.15 para, entre otras cosas, imponer las obligaciones de DDC de la Recomendación 10 a los PSAV.

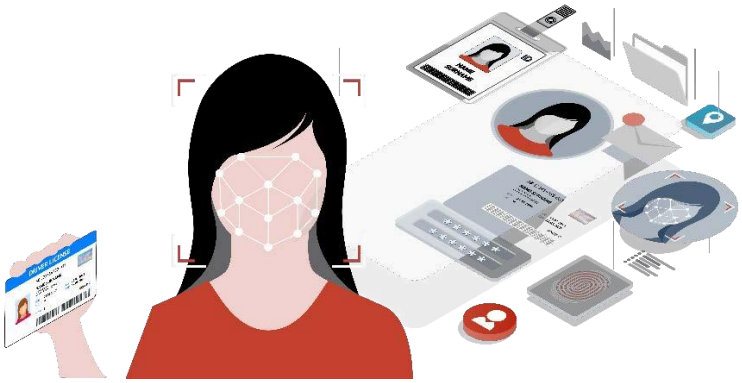
(IEC), está normalizando estos marcos de garantía de la identidad digital y actualizando una serie de normas técnicas ISO/IEC relacionadas con la identidad, la seguridad de la tecnología de la información y la privacidad para desarrollar una norma global completa para los sistemas de identidad digital. Un marco de garantía de identidad establece requisitos para diferentes «niveles de garantía». Los niveles de garantía miden el nivel de confianza en la confiabilidad e independencia de un sistema de identidad digital y sus componentes. Aunque los niveles de garantía desarrollados por las distintas jurisdicciones pueden variar en ciertos aspectos, para facilitar la referencia, esta Guía se refiere principalmente al marco y las normas de garantía de la identidad digital del Instituto Nacional de Normas y Tecnología (NIST) de EE.UU. (Guía de identidad digital del NIST)[4] y al reglamento e-IDAS de la UE.[5] Las jurisdicciones deben considerar el enfoque establecido en esta Guía en consonancia con sus marcos de garantía de la identidad digital nacionales y otras normas técnicas pertinentes.[6]

5. Los marcos y normas de garantía de la identidad digital y la normativa sobre ALA/CFT tienen orígenes y destinatarios diferentes. Esta Guía establece vínculos entre los marcos y normas de garantía de la identidad digital y los requisitos de DDC del GAFI. Como se ilustra en la tabla siguiente, los componentes clave de los sistemas de identidad digital son relevantes para los requisitos específicos de identificación y verificación de la Recomendación 10(a). En consecuencia, los marcos de garantía y las normas técnicas de identidad digital que definen estos componentes y establecen los requisitos para cada nivel de garantía, proporcionan una herramienta muy útil para evaluar la confiabilidad e independencia de los sistemas de identidad digital para fines ALA/CFT.

4 Las Normas de Identidad Digital NIST 800-63 constan de un conjunto de documentos: NIST SP 800- 63-3 Normas de Identidad Digital (Resumen); NIST SP 800-63A: Normas de Identidad Digital: Inscripción y comprobación de la identidad; NIST SP 800-63B Normas de identidad digital: Autenticación y gestión del ciclo de vida; y NIST SP 800-63C Normas de identidad digital: Federación y afirmaciones.

5 Reglamento (UE) nº 910/2014 sobre la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior

6 Una jurisdicción puede no tener un marco de garantía o normas técnicas de identidad digital específicas a los sistemas de identidad digital, pero puede tener otras normas técnicas que son muy relevantes (por ejemplo, de seguridad de la información de TI).



Requisitos de DDC (personas físicas)	Componentes clave de los sistemas de identidad digital
Identificación / verificación – R.10 (a)	Comprobación e inscripción de la identidad (con carácter vinculante) – ¿Quién es usted? Obtener atributos (nombre, fecha de nacimiento, número de identificación, etc.) y pruebas para esos atributos; validar y verificar las pruebas de identificación y asignarlas a una persona única con identidad comprobada. Vinculación-emisión de credenciales/autenticadores que vinculan a la persona en posesión/control de las credenciales con el individuo de identidad comprobada Autenticación – ¿Es usted el individuo identificado/verificado? Establecer que el solicitante tiene la posesión y el control de las credenciales vinculantes. La autenticación se aplica a 10(a) si el sujeto obligado lleva a cabo la identificación/verificación confirmando la posesión por parte del cliente potencial de credenciales de identidad digital preexistentes.

6. La Guía explica que (1) la autenticación es relevante para la R.10(a) cuando el sujeto obligado abre una cuenta para un cliente con credenciales de identidad digital preexistentes, es decir, no una solución de identidad digital interna, y (2) que, en un contexto de finanzas e identidad digitales, la autenticación efectiva de la identidad del cliente para autorizar el acceso a la cuenta puede apoyar los esfuerzos ALA/CFT.

7. La Sección V es el núcleo de la Guía y brinda una orientación a las autoridades gubernamentales, los sujetos obligados y otras partes relevantes sobre cómo aplicar un enfoque basado en el riesgo al uso de sistemas de identidad digital para la identificación y verificación del cliente, en consonancia con la Recomendación 10(a) y para apoyar la debida diligencia continua de la Recomendación 10(d). El enfoque recomendado es tecnológicamente neutro (es decir, no prefiere ningún tipo de sistema de identidad digital en particular). Este enfoque consta de dos elementos:

Aplicar un **enfoque basado en el riesgo** al uso de la identidad digital para la DDC: (1) comprender los niveles de garantía del sistema de identidad digital y (2) evaluar si, dados los niveles de garantía, el sistema de identidad es adecuadamente confiable e independiente a la luz de los riesgos de LA/FT

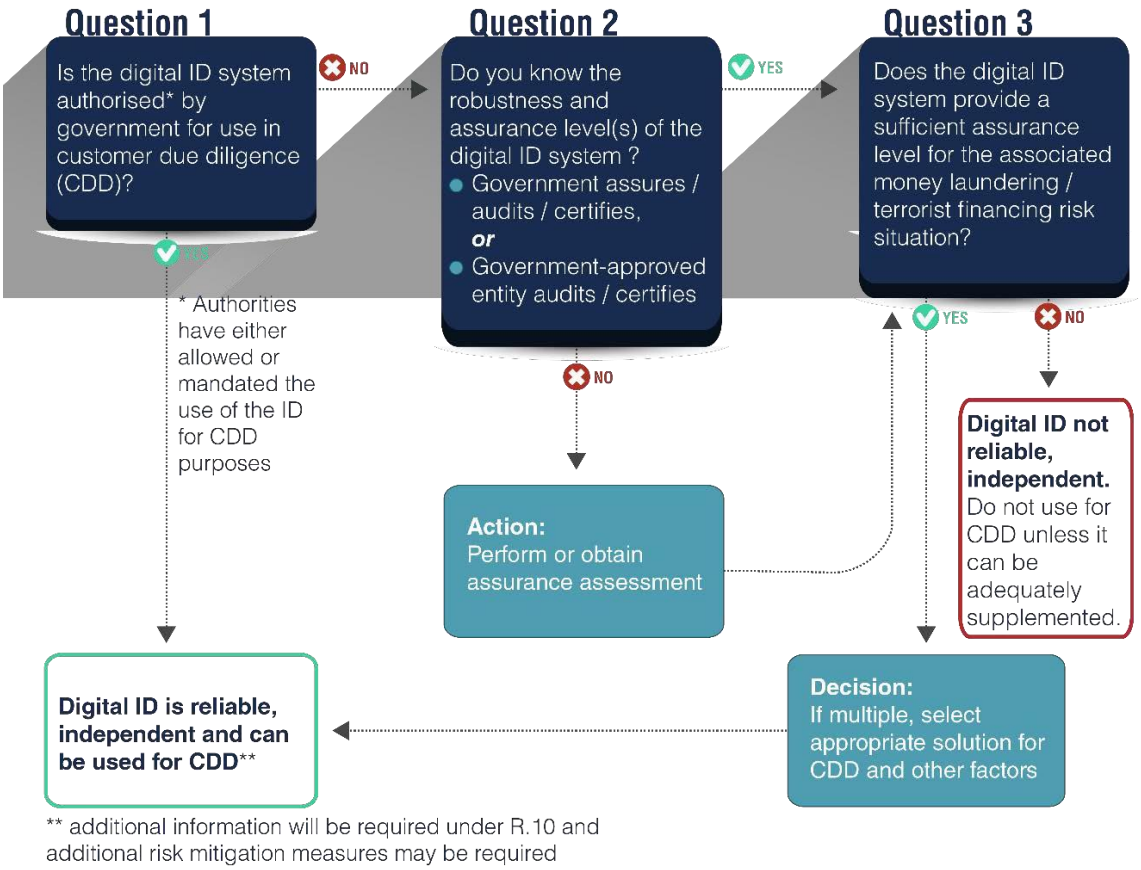
a. Comprender los niveles de garantía de los principales componentes del sistema de identidad digital (incluida su tecnología, arquitectura y gobernanza) para determinar si es una fuente de información confiable e independiente; y

b. Determinar de forma más amplia y basada en el riesgo si, teniendo en cuenta sus niveles de garantía, el sistema de identidad digital concreto proporciona un nivel adecuado de confiabilidad e independencia a la luz de los riesgos de LA, FT, fraude y otros riesgos de financiamiento ilícito.

8. La Sección V explica cómo aprovechar los marcos y normas de garantía de la identidad digital para evaluar la confiabilidad/independencia. También establece un proceso de decisión para que los sujetos obligados orienten sus decisiones sobre si el uso de la identidad digital para cumplir con algunos elementos de la DDC es apropiado según la Recomendación 10 del GAFI. Los gobiernos y los sujetos obligados tendrán que adaptar este proceso de decisión a las circunstancias particulares de la jurisdicción y de las entidades individuales. Dependiendo del sistema o sistemas de identidad digital y del marco regulatorio en una jurisdicción particular, los gobiernos y los sujetos obligados pueden tener diferentes funciones y responsabilidades en la evaluación de los niveles de garantía de un sistema de identidad y su idoneidad para la DDC, como se refleja en el diagrama de flujo de toma de decisiones para los sujetos obligados, a continuación.

9. Esta Guía no es vinculante. Aclara los Estándares del GAFI actuales, que son tecnológicamente neutrales.

Figura 1. Proceso de decisión para sujetos obligados



10. La sección IV de la Guía explora algunas de las ventajas de los sistemas de identidad digital, así como los riesgos que plantean. Muchos de los riesgos asociados a los sistemas de identidad digital también existen en los documentos de identidad. Sin embargo, la comprobación de la identidad y/o la autenticación de las personas a través de una red de comunicaciones abierta (Internet) crea riesgos específicos para los sistemas de identidad digital, especialmente en relación con los ciberataques y la posible apropiación de la identidad a gran escala. Por otra parte, los sistemas de identidad digital que mitigan estos riesgos de acuerdo con los marcos y normas de garantía de la identidad digital son una gran promesa para el fortalecimiento de los controles de DDC y ALA/CFT, el aumento de la inclusión financiera, la mejora de la experiencia del cliente y la reducción de los costos para los sujetos obligados.

11. La Guía destaca una serie de formas en las que el uso de sistemas de identidad digital para la DDC puede apoyar la inclusión financiera. En primer lugar, los sistemas de identidad digital pueden permitir a los gobiernos adoptar un enfoque más flexible, matizado y orientado al futuro a la hora de establecer los atributos requeridos, las pruebas de identidad y los procesos para demostrar la identidad oficial, incluso con el fin de llevar a cabo la identificación y verificación de los clientes en el momento de la admisión, de manera que se faciliten los objetivos de inclusión financiera. En segundo lugar, los propios marcos y normas de garantía de la identidad digital proporcionan cierta flexibilidad en el proceso que puede utilizarse para acreditar y autenticar la identidad de las personas, que puede adaptarse para cumplir los objetivos de inclusión financiera. Por último, los supervisores y los sujetos obligados, al adoptar un enfoque de la DDC basado en el riesgo, pueden apoyar la inclusión financiera, incluso mediante el uso de sistemas de identidad digital, en consonancia con el enfoque del suplemento del GAFI de 2017 sobre la DDC y la inclusión financiera.

Los sistemas de identidad digital pueden apoyar la inclusión financiera

Recomendaciones para las autoridades gubernamentales

12. Desarrollar pautas o regulaciones claras que permitan el uso apropiado, basado en el riesgo, de sistemas de identidad digital confiables e independientes por parte de los sujetos obligados a efectos ALA/CFT. Como punto de partida, entender los sistemas de identidad digital disponibles en la jurisdicción y cómo encajan en los requisitos u orientaciones existentes sobre la identificación y verificación de clientes y la debida diligencia continua (y los requisitos asociados de mantenimiento de registros y dependencia en terceros).

13. Evaluar si las regulaciones y orientaciones existentes sobre DDC de todas las autoridades pertinentes se adaptan a los sistemas de identidad digital, y revisarlas, según proceda, a la luz del contexto jurisdiccional y del ecosistema de identidad. Por ejemplo, las autoridades deberían considerar la posibilidad de aclarar que la admisión no presencial puede ser de riesgo estándar, o incluso de bajo riesgo a efectos de la DDC, cuando se utilicen sistemas de identidad digital con niveles de garantía adecuados para la identificación/verificación y autenticación de clientes a distancia.

14. Adoptar criterios basados en los principios, el rendimiento y/o los resultados al establecer los atributos, pruebas y procesos requeridos para demostrar la identidad oficial a efectos de la DDC. Dada la rápida evolución de la tecnología de identidad digital, esto ayudará a promover la innovación responsable y a preparar los requisitos reglamentarios para el futuro.

15. Adoptar políticas, reglamentos y procedimientos de supervisión y análisis que permitan a los sujetos obligados desarrollar un enfoque eficaz e integrado «basado en el riesgo» que aproveche los flujos de datos, la arquitectura tecnológica y los procesos en todas las actividades pertinentes de identidad digital, ALA/CFT, lucha contra el fraude y gestión del riesgo en general para reforzar todas las funciones relacionadas con el riesgo.

16. Desarrollar un enfoque integrado de múltiples partes interesadas para comprender las oportunidades y los riesgos relacionados con la identidad digital y desarrollar reglamentos y orientaciones pertinentes para mitigar los riesgos. Evaluar y aprovechar, en su caso, los marcos y las normas técnicas de garantía de la identidad digital existentes adoptadas por las autoridades responsables de la identidad, la ciberseguridad/protección de datos y la privacidad (incluidas las consideraciones de tecnología, seguridad, gobernanza y recursos) para evaluar los niveles de garantía de los sistemas de identidad digital para su uso en la DDC. En consonancia con la Recomendación 2 del GAFI, cooperar y coordinar con las autoridades pertinentes para facilitar un enfoque global y coordinado para comprender y abordar los riesgos en el ecosistema de identidad digital y garantizar la compatibilidad de los requisitos ALA/CFT sobre los sistemas de identidad digital con las normas de protección de datos y privacidad.

17. Las autoridades ALA/CFT podrían considerar la adopción de mecanismos para mejorar el diálogo y la cooperación con las partes interesadas del sector privado, incluidos los sujetos obligados y los proveedores de servicios de identidad digital, para ayudar a identificar las oportunidades, los riesgos y las medidas de mitigación clave relacionados con la identidad. Los mecanismos podrían incluir un enfoque regulatorio tipo «corral» para proporcionar un entorno supervisado y probar cómo los sistemas de identidad digital interactúan con las leyes y regulaciones ALA/CFT nacionales. Las autoridades también podrían considerar el desarrollo de mecanismos para promover la colaboración entre industrias para identificar y abordar las vulnerabilidades de los sistemas de identidad digital existentes.

18. Considerar la posibilidad de apoyar el desarrollo y la aplicación de sistemas de identidad digital confiables e independientes mediante su auditoría y la certificación en función de marcos y normas técnicas transparentes de garantía de la identidad digital, o mediante la aprobación de organismos expertos para llevar a cabo estas funciones. Cuando las autoridades no auditen o proporcionen la certificación de los IDSP por sí mismas, se les anima a apoyar las pruebas de garantía y la certificación por parte de los organismos expertos apropiados,[7] de modo que se disponga de una certificación fiable en la jurisdicción. Se anima a las autoridades a apoyar los esfuerzos de armonización de los marcos y normas de garantía de la identidad digital para desarrollar un entendimiento común de lo que constituye un sistema de identidad digital «confiable e independiente».

19. Aplicar los marcos y las normas técnicas de garantía de la identidad digital apropiadas al desarrollar e implementar la identidad digital proporcionada por el gobierno. Las autoridades deben ser transparentes sobre el funcionamiento del sistema de identidad digital de la jurisdicción y sus niveles de garantía.

7 Estos organismos expertos en certificación pueden prestar servicios para una jurisdicción o región concreta, u ofrecer sus servicios a nivel internacional.

20. Fomentar un enfoque flexible y basado en el riesgo para utilizar sistemas de identidad digital para la DDC que apoyen la inclusión financiera. Considerar la posibilidad de proporcionar orientación sobre cómo utilizar los sistemas de identidad digital con diferentes niveles de garantía para la comprobación/inscripción de la identidad y la autenticación para la DDC escalonada.

21. Supervisar los avances en el ámbito de la identidad digital con vistas a compartir conocimientos y mejores prácticas, y establecer marcos jurídicos tanto a nivel nacional como internacional que promuevan la innovación responsable y permitan una mayor flexibilidad, eficiencia y funcionalidad de los sistemas de identidad digital, tanto dentro como fuera de las fronteras.

Recomendaciones para los sujetos obligados

22. Comprender los componentes básicos de los sistemas de identidad digital, en particular la comprobación y autenticación de la identidad, y cómo se aplican a los elementos de DDC requeridos (véase la Sección II y el Anexo A).

23. Adoptar un enfoque informado basado en el riesgo para confiar en los sistemas de identidad digital para la DDC que incluya:

    a. La comprensión del nivel o los niveles de garantía del sistema de identidad digital, especialmente en lo que respecta a la comprobación y autenticación de la identidad, y

    b. La garantía de que los niveles de garantía son apropiados para los riesgos de LA/FT asociados con el cliente, el producto, la jurisdicción, el alcance geográfico, etc.

24. Considerar si los sistemas de identidad digital con niveles de garantía más bajos pueden ser suficientes para la debida diligencia simplificada en casos de bajo riesgo de LA/FT. Por ejemplo, cuando esté permitido, adoptar un enfoque de DDC escalonada que se beneficie de los sistemas de identidad digital con varios niveles de garantía para apoyar la inclusión financiera.

25. Si, como cuestión de política o práctica interna, las relaciones o transacciones comerciales no presenciales se clasifican siempre como de alto riesgo, considerar la posibilidad de revisar esas políticas para tener en cuenta que las medidas de identificación/verificación de clientes que se basan en sistemas de identidad digital confiables e independientes, con medidas apropiadas de mitigación de riesgos, pueden ser de riesgo estándar, e incluso menor.

26. Cuando proceda, utilizar los procesos de lucha contra el fraude y de ciberseguridad para respaldar la comprobación y/o autenticación de la identidad digital para los esfuerzos ALA/CFT (identificación/verificación del cliente en el momento de la admisión y debida diligencia continua y supervisión de las transacciones). Por ejemplo, los sujetos obligados podrían utilizar las salvaguardias integradas en los sistemas de identidad digital para prevenir el fraude (es decir, supervisar los eventos de autenticación para detectar

el uso indebido sistemático de las identidades digitales para acceder a las cuentas, incluso a través de credenciales/autenticadores de identidad digital perdidos, comprometidos, robados o vendidos) para alimentar los sistemas a fin de llevar a cabo la debida diligencia continua en la relación comercial y supervisar, detectar y notificar las operaciones sospechosas a las autoridades.

27. Los sujetos obligados deben asegurarse de que tienen acceso a la información de identidad subyacente y a las pruebas o a la información digital necesarias para la identificación y verificación de las personas, o de que disponen de un proceso que permita a las autoridades obtenerlas. Se anima a los sujetos obligados a colaborar con los reguladores y los responsables políticos, así como con los proveedores de servicios de identidad digital, para explorar cómo se puede lograr esto de manera eficiente y eficaz en un entorno de identidad digital.

Recomendaciones para los proveedores de servicios de identidad digital[8]

28. Comprender los requisitos ALA/CFT para la DDC (en particular la identificación/verificación del cliente y la debida diligencia continua) y otras regulaciones relacionadas, incluidos los requisitos para que los sujetos obligados mantengan registros de DDC.

29. Buscar pruebas de garantía y certificación por parte del gobierno o de un organismo experto aprobado, o cuando no estén disponibles, otro organismo experto de reputación internacional. Cuando esté disponible, participar en las zonas de pruebas regulatorias del sector público (u otros mecanismos pertinentes) para evaluar los niveles de garantía del sistema de identidad digital.

30. Proporcionar información transparente a los sujetos obligados ALA/CFT sobre los niveles de garantía del sistema de identidad digital para la comprobación de la identidad, la autenticación y, en su caso, la federación/interoperabilidad.

8 Aunque los Estándares del GAFI sólo son aplicables a los sujetos obligados (es decir, las instituciones financieras, los proveedores de servicios de activos virtuales y las actividades y profesiones no financieras designadas), esta Guía es un antecedente relevante para los proveedores de servicios de identidad digital que prestan servicio a los sujetos obligados (a efectos del GAFI). En última instancia, los sujetos obligados son los responsables del cumplimiento de los requisitos del GAFI.

SECCIÓN I: INTRODUCCIÓN

31. El Grupo de Acción Financiera Internacional (GAFI) se ha comprometido a garantizar que las normas mundiales contra el lavado de activos y el financiamiento del terrorismo (ALA/CFT) fomenten la innovación financiera responsable. En este sentido, el GAFI apoya firmemente el uso de las nuevas tecnologías en el sector financiero que se alinean con la aplicación de las normas ALA/CFT y los objetivos de inclusión financiera, y los refuerzan.[9]

32. El rápido ritmo de innovación en el espacio de la identidad digital (ID) ha alcanzado un punto de inflexión. Las normas, la tecnología y los procesos de identidad digital han evolucionado hasta el punto de que los sistemas de identidad digital están, o podrían estar pronto, disponibles a escala.

Algunas de estas tecnologías relevantes son: una serie de tecnologías biométricas; la casi ubicuidad de Internet y los teléfonos móviles (incluida la rápida evolución y adopción de «teléfonos inteligentes» con cámaras, micrófonos y otras tecnologías de «teléfonos inteligentes»); identificadores de dispositivos digitales e información relacionada (por ej. direcciones MAC e IP;10 números de teléfono móvil, tarjetas SIM, la geolocalización del sistema de posicionamiento global (GPS); escáneres de alta definición (para escanear tarjetas de identidad, permisos de conducir y otros documentos); transmisión de vídeo de alta resolución (que permite la identificación y la verificación a distancia y la prueba de «vida»); inteligencia artificial/aprendizaje automático (por ejemplo, para determinar la validez de un documento de identidad emitido por el gobierno); y tecnología de libro mayor distribuido (DLT).

El rápido ritmo de innovación ha alcanzado un punto de inflexión... Los sistemas de identidad digital están, o podrían estar pronto, disponibles a escala.

Beneficios potenciales

33. Los sistemas de identidad digital que cumplen con altos estándares tecnológicos, organizativos y de gobernanza son muy prometedores para mejorar la confiabilidad, seguridad, privacidad y conveniencia de la identificación de las personas físicas en una amplia variedad de escenarios, como los servicios financieros, la salud y la administración electrónica en la economía global de la era digital. Estas identidades digitales se denominan de mayor nivel de garantía.

34. En relación con los Estándares del GAFI, los sistemas de identidad digital debidamente confiables e independientes podrían:

- facilitar la identificación y verificación de los clientes en el momento de su admisión
- apoyar la debida diligencia continua y el escrutinio de las transacciones a lo largo de la relación comercial
- facilitar otras medidas de debida diligencia del cliente (DDC), y
- ayudar a la supervisión de las transacciones con el fin de detectar y notificar las operaciones sospechosas, así como la gestión general de riesgos y los esfuerzos de lucha contra el fraude.

9 Véase la posición del GAFI sobre *FinTech y RegTech* (3 de noviembre de 2017), disponible en www.fatf-gafi.org/publications/fatfgeneral/documents/fatf-position-fintech-regtech.html.

10 Las direcciones MAC identifican los dispositivos, las direcciones IP identifican las conexiones.

35. También tienen el potencial de reducir los costos y aumentar la eficiencia de los sujetos obligados, y permitir la reasignación de recursos a otras funciones ALA/CFT.

36. Los sistemas de identidad digital confiables e independientes[11] también pueden contribuir a la inclusión financiera al permitir que las personas desatendidas y subatendidas demuestren su identidad oficial en una amplia gama de circunstancias, incluso a distancia, con el fin de obtener servicios financieros regulados. La incorporación de un mayor número de personas al sector financiero regulado refuerza aún más las salvaguardias ALA/CFT.

Riesgos potenciales

37. Los sistemas de identidad digital también plantean riesgos de LA/FT que deben ser comprendidos y mitigados. Los sujetos obligados que no lo hagan, tampoco cumplirán los requisitos establecidos en la Recomendación 10(a) y los requisitos en los Estándares del GAFI que exigen que los sujetos obligados identifiquen, evalúen y mitiguen los riesgos de lavado de activos o financiamiento del terrorismo que puedan surgir en relación con el uso de tecnologías nuevas o en desarrollo, tanto para productos nuevos como preexistentes.[12]

38. La Sección IV aborda en detalle estos riesgos. Los sistemas de identidad digital a gran escala que no cumplen con los niveles de garantía adecuados plantean riesgos de ciberseguridad, incluyendo la posibilidad de que se produzcan ciberataques dirigidos a inutilizar amplias franjas del sector financiero, o a inutilizar los propios sistemas de identidad digital. También generan riesgos importantes a la privacidad, el fraude u otros delitos financieros relacionados, ya que los fallos de ciberseguridad pueden dar lugar a un robo de identidad masivo, comprometiendo la información personal identificable (PII) de los individuos.[13] Los riesgos relacionados con la gobernanza, la seguridad de los datos y la privacidad también tienen un impacto en las medidas ALA/CFT. Estos riesgos varían en relación con los componentes del sistema de identidad digital, pero pueden ser más devastadores que los incumplimientos asociados a los sistemas de identidad tradicionales debido a la escala potencial de los ataques. Los avances tecnológicos y los procesos de comprobación y autenticación de la identidad bien diseñados pueden ayudar a mitigar estos riesgos, tal y como se expone en la Sección IV y se analiza con más detalle en la Sección V.

39. Reconociendo los riesgos y beneficios potenciales de los sistemas de identidad digital, el GAFI ha desarrollado esta Guía para aclarar cómo se pueden utilizar los sistemas de identidad digital para cumplir con los requisitos específicos ALA/CFT bajo sus estándares.

Objetivo y destinatarios

40. Esta Guía tiene como objetivo ayudar a los organismos gubernamentales a desarrollar una comprensión más clara de cómo funcionan los sistemas de identidad digital y aclarar cómo se pueden utilizar en el marco de las normas globales ALA/CFT. Esto incluye a los legisladores, reguladores, supervisores y evaluadores de los sujetos obligados; autoridades de privacidad, protección de datos y ciberseguridad (según corresponda); así como otras autoridades gubernamentales con objetivos políticos relacionados (por ejemplo, aumentar la inclusión financiera).

---

11 Para favorecer la legibilidad, el término «digno de confianza» se utiliza como sinónimo de «confiable, independiente» en algunos casos.

12 R.15 (para las instituciones financieras y los PSAV) y R.22 (para APNFD).

13 La **PII** incluye cualquier información que por sí misma o en combinación con otra información pueda identificar a un individuo específico.

41. Esta Guía también pretende ayudar a las partes interesadas del sector privado, incluidos los sujetos obligados y los proveedores de servicios de identidad digital. También es relevante para las organizaciones internacionales, las organizaciones no gubernamentales (ONG) y otras que participan en la prestación y el uso de sistemas de identidad digital para los servicios financieros y la asistencia humanitaria.

Alcance

42. Esta Guía se centra en la aplicación de la Recomendación 10 (Debida Diligencia del Cliente) al uso de sistemas de identidad digital para la identificación/verificación en el momento de la admisión (apertura de cuentas) bajo la Recomendación 10(a). También examina el potencial de la identidad digital para apoyar la debida diligencia en curso (incluida la supervisión de las transacciones) en virtud de la Recomendación 10(d). Aborda la aplicación de la Recomendación 17 (Dependencia en terceros) a las situaciones en las que los sujetos obligados proporcionan sistemas de identidad digital para llevar a cabo la identificación/verificación de los clientes a otros sujetos obligados.

43. En virtud del principio de neutralidad tecnológica, los requisitos de la Recomendación 11 (Mantenimiento de registros) se aplican por igual al mantenimiento de registros en forma digital y física (documental). En la práctica, los sistemas de identidad digital pueden presentar problemas específicos en cuanto a la forma de conservar y acceder a la información de DDC requerida para que los sujetos obligados puedan cumplir los requisitos de la Recomendación 11. Los enfoques para el mantenimiento de registros en el contexto de la identidad digital variarán con el tipo y el diseño de los sistemas de identidad digital, los tipos y las responsabilidades de sus proveedores constituyentes, y los marcos regulatorios y contractuales pertinentes en la jurisdicción. Por ejemplo, cuando los gobiernos proporcionan sistemas de identidad digital, recogen o generan las pruebas de identidad subyacentes (documentos de origen, información y datos) para la comprobación o la inscripción de la identidad y, por lo tanto, se espera que tengan acceso a esta información con fines de regulación o de aplicación de la ley, satisfaciendo así los objetivos de la R.11. Cuando los sujetos obligados utilizan sistemas de identidad digital proporcionados por proveedores no gubernamentales, las pruebas de identidad subyacentes pueden ser retenidas en su totalidad, o en parte, por el proveedor de servicios de identidad digital (IDSP) u otras entidades. Además, un proveedor de servicios de identidad digital del sector privado puede obtener/confirmar algunos o todos los datos de identidad subyacentes directamente de la fuente digital (por ej., una base de datos gubernamental o registros de servicios públicos del sector privado). En ese caso, es posible que los registros digitales que especifican los tipos de pruebas de identidad utilizados para pruebas específicas, incluida la fuente de datos, la fecha/hora y los medios de acceso, se ajusten a la Recomendación 11. Las autoridades abordan estas cuestiones de forma adecuada en sus marcos normativos de ALA/CFT y de identidad digital, y los sujetos obligados lo hacen a través de las relaciones contractuales habituales con las agencias y los proveedores de servicios financieros. Por lo tanto, esta Guía no aborda el mantenimiento de registros ni estos requisitos.

44. Esta Guía se centra en la identificación de clientes que son individuos (personas físicas). La Guía no examina el uso de sistemas de identidad digital para ayudar a identificar y verificar la identidad de los representantes de las personas jurídicas como parte de la identificación/verificación de los clientes que son personas jurídicas, o para ayudar a llevar a cabo otros elementos del proceso de DDC, en particular, para identificar y verificar la identidad del beneficiario final bajo la Recomendación 10(b) o para entender y obtener información sobre el propósito y la naturaleza prevista de la relación comercial bajo la Recomendación 10(c), aunque los sistemas de identidad digital confiables e independientes son importantes para todas estas funciones de DDC.

45. Esta Guía comprende los sistemas de identidad digital proporcionados por el gobierno, o en nombre del gobierno,[14] y por el sector privado. Con respecto a los sistemas de identidad digital proporcionados por el gobierno, la Guía se centra en los sistemas de identidad digital de propósito general (es decir, la identidad válida para probar la identidad oficial para todos o la mayoría de los propósitos en la jurisdicción), aunque también analiza la identidad de propósito limitado (es decir, la identidad válida para un propósito específico), como el registro de la seguridad social u otras bases de datos, cuando el gobierno autoriza su uso para fines de DDC y los pone a disposición de los sujetos obligados y los proveedores de servicios de identidad digital. En la Sección II se ofrece más información sobre el tipo de sistemas de identidad digital cubiertos por esta Guía.

46. La Guía no establece marcos de garantía o normas técnicas para evaluar la independencia o fiabilidad de los sistemas de identidad digital en cuanto a su tecnología, procesos y arquitectura. En cambio, se basa en los marcos y las normas técnicas de garantía de la identidad digital (denominados marcos y normas de garantía de la identidad digital) desarrolladas, o en proceso de desarrollo, por otras organizaciones y en diferentes jurisdicciones. Véase la Sección II para una explicación de las normas técnicas, y la Sección V y el Anexo E para más información.

47. La Guía incluye cinco anexos y un glosario con lecturas adicionales relevantes:

- *Anexo A: Descripción de un sistema de identidad digital básico y sus participantes:* ofrece una descripción más detallada de los conceptos expuestos en la Sección V en relación con los componentes de un sistema de identidad digital.
- *Anexo B: Estudios de caso*: proporciona ejemplos de identidades digitales en uso en varias jurisdicciones, incluso para la DDC y el acceso a los servicios financieros.
- *Anexo C: Principios de Identificación para el Desarrollo Sostenible*: destaca la gobernanza/responsabilidad, la privacidad y otras cuestiones operativas que están siendo abordadas por diversas jurisdicciones y organizaciones. [15]
- *Anexo D: Marco de garantía de la identidad digital y organismos de establecimiento de normas técnicas*: enumera una serie de organismos de establecimiento de normas (sin incluir los organismos nacionales o regionales) que han desarrollado marcos o normas de garantía de la identidad digital pertinentes.
- *Anexo E: Descripción general de los marcos y las normas técnicas de garantía de la identidad digital de EE. UU. y la UE*: ofrece, a modo de ejemplo, los detalles de los marcos de garantía de la identidad digital nacionales y regionales de EE. UU. y la UE.
- *Glosario*: explicaciones de la terminología de la identidad digital utilizada en esta Guía.

14 Un sistema de identidad digital se proporciona «en nombre del gobierno» cuando el gobierno contrata o acuerda o autoriza a una organización internacional, como el ACNUR, o a otra entidad a proporcionar y operar el sistema de identidad digital. El actor no gubernamental sustituye al gobierno con respecto a estas funciones de identidad.

15 Estos Principios se elaboraron mediante un proceso de colaboración y han sido respaldados por 25 socios de desarrollo, organizaciones internacionales, ONG, asociaciones del sector privado y entidades gubernamentales.

SECCIÓN II: TERMINOLOGÍA Y CARACTERÍSTICAS PRINCIPALES DE LA IDENTIDAD DIGITAL

¿Qué es la «identidad» a los efectos de esta Guía?

Concepto de identidad oficial

48. La identidad es un concepto complejo con muchos significados. Para los fines del GAFI, en relación con la Recomendación 10(a), es decir, «identificar al cliente y verificar su identidad», «identidad» se refiere a la identidad oficial, que es distinta de los conceptos más amplios de identidad personal y social que pueden ser relevantes para fines no oficiales (por ejemplo, interacciones comerciales o sociales no reguladas, de igual a igual, en persona o en Internet). La Guía cubre el uso de sistemas de identidad digital para probar la «identidad oficial» para el acceso a los servicios financieros.

49. A efectos de esta Guía,[16] la **identidad oficial** es la especificación de una persona física única que:

a. se basa en características (atributos o identificadores) de la persona que establecen su singularidad en la población o en un contexto determinado, y

b. es reconocida por el Estado para fines regulatorios y otros fines oficiales.

Comprobación de la identidad oficial

50. La **comprobación de la identidad oficial** suele depender de algún tipo de registro, documentación o certificación (por ej., un certificado de nacimiento, un documento de identidad o una credencial de identidad digital) proporcionado o emitido por el gobierno que constituya una prueba de los atributos fundamentales (por ej., nombre, fecha y lugar de nacimiento) para establecer y verificar la identidad oficial.

51. Los criterios para demostrar la «identidad oficial» pueden variar según la jurisdicción. En el ejercicio de su soberanía, los gobiernos establecen los atributos, las pruebas y los procesos necesarios para demostrar la identidad oficial. Estos factores pueden cambiar con el tiempo. A medida que la tecnología y los conceptos culturales de identidad evolucionan, los gobiernos pueden autorizar diversos atributos. A la hora de establecer los criterios para demostrar la identidad oficial, los gobiernos pueden utilizar un enfoque fijo, prescriptivo y basado en normas o uno que sea de principios, de desempeño, y/o basado en resultados. Este último enfoque es más flexible. Dada la rápida evolución de la tecnología y los estándares de identidad digital, permite a las jurisdicciones preparar los requisitos para probar la identidad oficial y apoyar la innovación responsable en el futuro.

> El uso de un enfoque basado en resultados para establecer los atributos de identidad, permite a las jurisdicciones preparar los requisitos de comprobación de la identidad oficial para el futuro

52. En la UE, la confianza en los marcos de garantía comunes permite a los Estados miembros de la UE dar cabida a diferentes requisitos nacionales, como la aceptación de diferentes tipos de documentación y procedimientos de identidad oficial disponibles a nivel nacional, siempre que el resultado sea conforme a los requisitos del marco del eIDAS. Dependiendo del contexto en el que deba verificarse un aspecto de la prueba de identidad, las fuentes autorizadas pueden adoptar muchas formas, como registros, documentos y organismos pertinentes, entre otras cosas. Las fuentes autorizadas pueden ser diferentes en los distintos Estados miembros de la UE incluso en un contexto similar, pero el marco eIDAS permite la armonización y el reconocimiento cruzado. La Organización Internacional de Normalización (ISO)[17] trabaja actualmente en la elaboración de normas mundiales para la identificación de las personas físicas en los servicios financieros, incluso en el contexto digital.

53. En muchos países, la acreditación de la identidad oficial se realiza a través de sistemas de identidad de **propósito general** (a veces denominados sistemas fundacionales de identificación), como los sistemas nacionales de identidad y de registro civil. Estos sistemas suelen proporcionar credenciales documentales y/o digitales que son ampliamente reconocidas y aceptadas por los organismos gubernamentales y proveedores de servicios del

16 El uso de esta definición por parte del GAFI, a efectos de esta Guía, no pretende limitar las definiciones alternativas de otros SSB.

17 Grupo Asesor de Normas ISO (SAG) del Comité Técnico 68, Grupo de Trabajo 7

sector privado como prueba de identidad oficial para diversos fines. No todas las jurisdicciones tienen sistemas de identidad de uso general.

54. Las jurisdicciones también suelen tener una variedad de sistemas de identidad de «**propósito limitado**» (también denominados sistemas de identidad funcional) que se desarrollan para proporcionar identificación, autenticación y autorización para servicios o sectores específicos, como la administración tributaria; el acceso a prestaciones y servicios gubernamentales específicos; la votación; la autorización para conducir un vehículo de motor; y (en algunas jurisdicciones) el acceso a servicios financieros, etc. Entre los ejemplos de pruebas de identidad de uso limitado se incluyen, entre otros, los siguientes: números de identificación del contribuyente, permisos de conducir, pasaportes, tarjetas de registro de votantes, números de la seguridad social y documentos de identidad de los refugiados. En algunos casos, y sobre todo en los países que carecen de sistemas de identidad de uso general, estos sistemas funcionales y las credenciales pueden utilizarse también como prueba de identidad oficial.

55. Normalmente, la prueba de identidad oficial ha sido proporcionada por, o en nombre de, los gobiernos. En la era digital, hemos empezado a ver nuevos modelos, con credenciales digitales proporcionadas por el sector privado, o en asociación con él, que son reconocidas por el gobierno como prueba oficial de identidad en un entorno en línea (por ej., NemID en Dinamarca), junto con credenciales digitales más tradicionales emitidas por el gobierno (por ej., los documentos nacionales de identidad electrónicos).

56. En el caso de los refugiados, la prueba de identidad oficial también puede ser proporcionada por una organización internacionalmente reconocida con ese mandato.[18] Véase el Recuadro 8.

¿Qué es un sistema de identidad digital a los efectos de esta Guía?

57. Los sistemas de identidad digital utilizan medios electrónicos para confirmar y acreditar la identidad oficial de una persona en línea (digital) y/o en entornos presenciales en varios niveles de garantía.

58. Esta Guía se centra en los sistemas de identidad digital de extremo a extremo (es decir, los sistemas que abarcan el proceso de comprobación/inscripción y de autenticación de la identidad). Los sistemas de identidad digital pueden implicar diferentes modelos operativos y pueden depender de varias entidades y tipos de tecnología, procesos y arquitectura. Las referencias a los sistemas de identidad digital en esta Guía se refieren al sistema global y no a sus componentes.

59. No todos los elementos de un sistema de identidad digital son necesariamente digitales. Algunos elementos del componente de comprobación e inscripción de la identidad pueden ser digitales o físicos (documentales), o una combinación, pero la **vinculación, la credencialización, la autenticación y la portabilidad/federación (cuando corresponda) deben ser digitales**. Estos conceptos se describen con más detalle en la siguiente sección.

60. Los sistemas de identidad digital pueden utilizar la tecnología digital de diversas maneras, por ejemplo, pero no exclusivamente:

- Bases de datos electrónicas, incluidos los libros de contabilidad distribuidos, para obtener, confirmar, almacenar y/o gestionar las pruebas de identidad

18 Véase la Convención sobre el Estatuto de los Refugiados de 1951, artículos 25 y 27, y el Estatuto de la Oficina del Alto Comisionado de las Naciones Unidas para los Refugiados de 1950.

- Credenciales digitales para autenticar la identidad para acceder a aplicaciones móviles, en línea y fuera de línea
- Biometría para ayudar a identificar y/o autenticar a las personas, e
- Interfaces de programa de aplicación digital (API), plataformas y protocolos que facilitan la identificación/verificación y autenticación de la identidad en línea.

¿Cuáles son los componentes clave de un sistema de identidad digital?

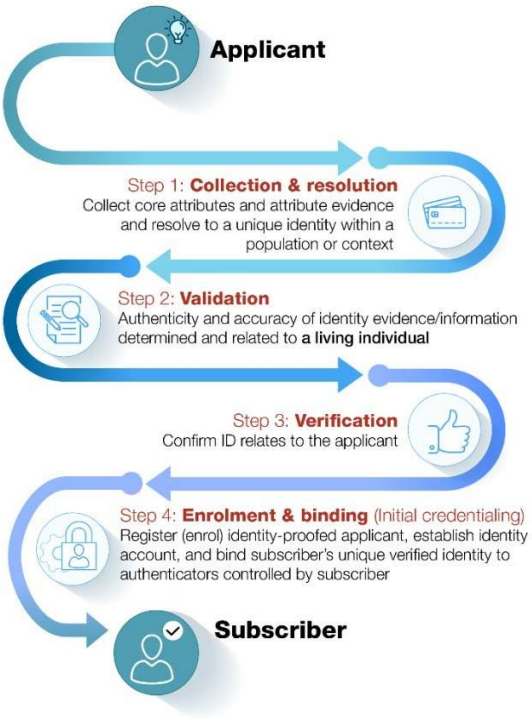
61. Tal y como se refleja en la Guía de identidad digital del NIST, los **sistemas de identidad digital** incluyen dos componentes básicos y un tercer componente opcional, tal y como se expone a continuación. Diferentes entidades pueden ser responsables de las operaciones de los subcomponentes, incluyendo una mezcla de entidades gubernamentales y entidades del sector privado. La terminología utilizada por las distintas jurisdicciones y organizaciones puede diferir ligeramente según el sistema que se describa. Se incluye una descripción más detallada de cada una de las etapas en el ***Anexo A: Descripción de un sistema de identidad digital básico y sus participantes***

Primer componente: Comprobación e inscripción de la identidad (con vinculación / credencialización inicial) *(esencial)*

62. Este componente responde a la pregunta: ***¿Quién es usted?*** E implica la recopilación, validación y verificación de las pruebas de identidad y la información sobre una persona; el establecimiento de una cuenta de identidad (inscripción) y la vinculación de la identidad única del individuo a los autenticadores que posee y controla esta persona.

63. Este componente es el más directa e inmediatamente relevante para (se solapa con) el requisito de identificación/verificación de la R.10 (a) (véase la Sección III).

Figura 2. Comprobación e inscripción de la identidad



Nota: Este diagrama es meramente ilustrativo, las etapas de comprobación e inscripción de la identidad podrían ocurrir en un orden diferente. El objetivo es identificar y verificar a la persona y vincular la identidad a un autentificador. Véase también el Anexo A para una explicación más detallada de los términos clave utilizados en este diagrama.

64. A efectos meramente ilustrativos, algunos ejemplos de acciones realizadas dentro del primer componente podrían ser:

- Recolección: Presentar y recoger atributos y pruebas de identidad, ya sea en persona y/o en línea (por ej., rellenar un formulario en línea, enviar una foto selfie, subir fotos de documentos como el pasaporte o el permiso de conducir, etc.).
- Validación: Inspección digital o física para garantizar que el documento es auténtico y que sus datos o información son precisos (por ej., comprobando las características físicas de seguridad, las fechas de caducidad y verificando los atributos a través de otros servicios).
- Desduplicación: Establecer que los atributos de identidad y las pruebas se refieren a una persona única en el sistema de identidad (por ej., mediante búsquedas de registros duplicados, reconocimiento biométrico y/o algoritmos de desduplicación).
- Verificación: Vincular a la persona con las pruebas de identidad proporcionadas (por ej., el uso de soluciones biométricas como el reconocimiento facial y la detección de la vida).
- Inscripción en la cuenta de identidad y vinculación: Crear la cuenta de identidad y emitir y vincular uno o varios autentificadores con la cuenta de identidad (por ej., contraseñas, generador de códigos de un solo uso (OTC) en un *smartphone*, tarjetas inteligentes PKI[19], certificados FIDO, etc.). Este proceso permite la autenticación (véase más adelante).

19 Infraestructura de clave pública

Segundo componente: Autenticación y gestión del ciclo de vida de la identidad (esencial)

65. La autenticación responde a la pregunta. ***¿Es usted la persona identificada y verificada?*** Establece, sobre la base de la posesión y el control de los autentificadores, que la persona que afirma una identidad (el cliente o solicitante admitido) es la misma persona que se comprobó e inscribió.

66. Hay tres tipos de factores que pueden utilizarse para autenticar a alguien (véase la Figura 3): (1) factores de propiedad (algo que se posee, por ej., claves criptográficas) (2) factores de conocimiento (algo que se sabe, por ej., una contraseña); (3) factores inherentes, (algo que se es, por ej., la biometría).[20]

67. La autenticación puede basarse en varios tipos de factores y protocolos o procesos de autenticación. Estos factores de autenticación tienen diferentes niveles de seguridad (véase la discusión de los riesgos de autenticación en la Sección V). Un solo factor de autenticación no suele considerarse suficientemente fiable. Un proceso de autenticación suele considerarse más sólido y fiable cuando emplea múltiples tipos de factores de autenticación.[21]

20 Cuando la Guía describe los componentes de la autenticación, éstos no son los mismos que la «autenticación reforzada del cliente (ARC)» según el marco legal de la UE. Lo que constituye o no constituye un factor ARC válido a los efectos de la Directiva (UE) 2015/2366 (PSDII) tiene que ser evaluado de acuerdo con la PSDII y las Normas Técnicas de Regulación sobre autenticación reforzada de clientes y comunicación segura en el marco de la PSDII (RTS sobre SCA & CSC), en lugar de las guías del GAFI.

21 A medida que los sistemas de identidad digital evolucionan, este entendimiento se vuelve más matizado. Cuando la autenticación es activa y continua, a veces la solidez de la autenticación se evalúa no en términos del número de factores y tipos de autenticación diferentes, sino en términos de solidez general resultante del uso de múltiples fuentes de datos digitales dinámicos del cliente, incluidos los canales de inicio de sesión previstos, la geolocalización, la frecuencia de uso, el tipo de uso, las direcciones IP y los patrones de comportamiento biomecánicos.

Figura 3. Factores de autenticación comunes

Fuente: ID4D del Banco Mundial

Cuadro 1. Función de la autenticación en la debida diligencia del cliente y otras medidas ALA/CFT

- Una vez que una persona ha comprobado su identidad y se ha inscrito en un sistema de identidad digital, puede utilizar las credenciales y los autentificadores vinculados a su identidad para «confirmar» esta identidad ante un tercero, «la parte que confía» (por ej., un sujeto obligado). Mientras que la solidez del proceso de comprobación e inscripción de la identidad proporciona a la parte que confía un nivel de confianza en la veracidad de la información de la identidad (por ej., que atributos como el nombre y la edad son correctos y se refieren a una persona real), el proceso de autenticación asegura a la parte que confía que la persona que presenta la credencial es realmente la persona a la que pertenece, y no un ladrón o impostor. La capacidad de los sistemas de identidad digital para autenticar a una persona es, por tanto, un componente importante de su funcionalidad, y puede ser utilizada por los sujetos obligados como parte del proceso de identificación/verificación de la DDC durante la apertura de cuentas.

- Obsérvese que la «autentificación» de los clientes existentes es también una medida de seguridad importante para la debida diligencia continua y para autorizar el acceso a las cuentas. En algunos casos, los sujetos obligados pueden utilizar las mismas credenciales de identidad digital y los mismos servicios de autenticación utilizados durante la apertura de la cuenta para autorizar el acceso a la misma, aunque no tiene por qué ser así. Por ejemplo, muchos sujetos obligados emiten sus propias credenciales/autenticadores (por ej., PIN y tokens, para acceder a cuentas en línea) y/o los vinculan a autenticadores en dispositivos integrados en teléfonos móviles o navegadores (por ej., utilizando los estándares FIDO).

68. La ***gestión del ciclo de vida de la identidad*** se refiere a las acciones que deben tomarse en respuesta a los eventos que pueden ocurrir durante el ciclo de vida de la identidad y que afectan al uso, la seguridad y la fiabilidad de los autenticadores, por ejemplo, la pérdida, el robo, la duplicación no autorizada, la caducidad y la revocación de **autenticadores** y/o **credenciales**.

Tercer componente: Mecanismos de portabilidad e interoperabilidad (opcional)

69. Los sistemas de identidad digital pueden incluir un componente que permite que la prueba de identidad sea portátil. La portabilidad de la identidad significa que las credenciales de identidad digital de un individuo pueden ser utilizadas para acreditar la identidad oficial para nuevas relaciones con clientes en entidades del sector privado o gubernamentales no relacionadas, sin que tengan que obtener y verificar los datos personales y llevar a cabo la identificación/verificación del cliente cada vez. La portabilidad puede apoyarse en diferentes arquitecturas y protocolos de identidad digital. En Europa, el Reglamento eIDAS proporciona un marco para el reconocimiento cruzado de los sistemas de identidad digital.

70. La federación es una forma de permitir la portabilidad de la identidad oficial. La federación se refiere al uso de una arquitectura federada y de protocolos de afirmación para transmitir información de identidad y autenticación *a través de un conjunto de sistemas en red*. Permite la interoperabilidad entre redes distintas. En el Reino Unido, GOV.UK Verify es un ejemplo de identidad digital federada (véase el Recuadro 16).

Marcos y normas técnicas de garantía de la identidad digital

71. Se han desarrollado o se están desarrollando marcos de garantía y normas técnicas para la fiabilidad de la tecnología, los procesos y la arquitectura de la identidad digital por parte de:

- diversas jurisdicciones o jurisdicciones supranacionales (por ej., la Unión Europea, Canadá y Australia)
- organizaciones internacionales de normalización u organizaciones específicas del sector, como la Organización Internacional de Normalización (ISO), la Comisión Electrotécnica Internacional (CEI), la Alianza Fast Identity Online (FIDO), la Fundación OpenID (OIDF), la Unión Internacional de Telecomunicaciones (UIT) y la GSMA.

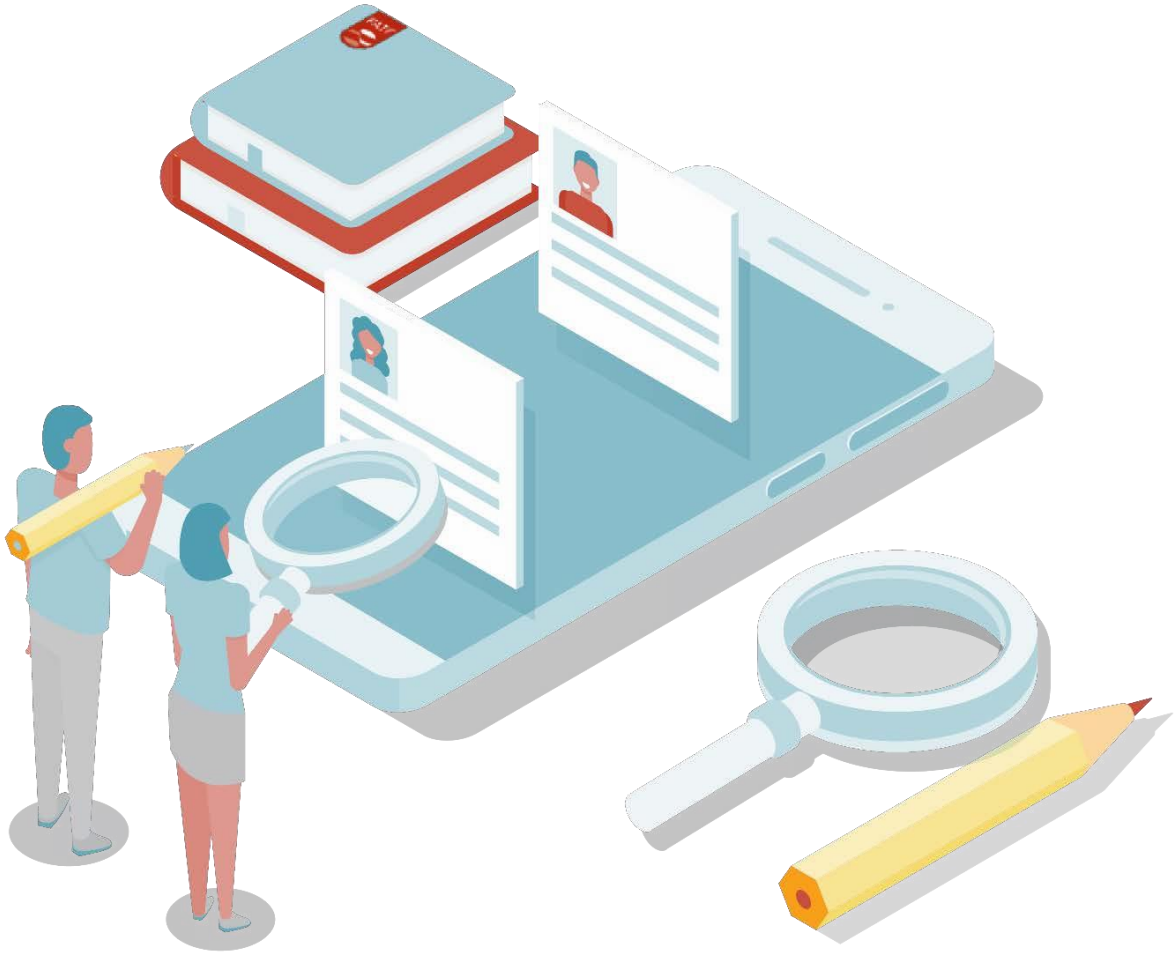
72. Véase el ***Anexo D: Marco de garantía de la identidad digital y organismos de establecimiento de normas técnicas*** para un resumen de alto nivel de estas organizaciones.

73. Los marcos de garantía de la identidad digital y las normas desarrolladas a nivel jurisdiccional utilizan actualmente diferentes números y/o nombres para los niveles de garantía, pero coinciden en gran medida en lo esencial. Las jurisdicciones están actualmente mapeando sus respectivas normas técnicas de identidad digital entre sí, para resolver cualquier discrepancia pendiente. En 2018, la ISO, junto con la CEI Internacional, publicó una norma internacional para la comprobación e inscripción de la identidad de personas físicas (ISO/CEI 29003:2018). La ISO está revisando actualmente su marco de garantía de autenticación de entidades (ISO/CEI 29115:2013) y abordando la aplicación de sus Pautas de Gestión de Riesgos (ISO 31000:2018) a los riesgos relacionados con la identidad. Además, la ISO está trabajando para actualizar, alinear y sincronizar todas las demás normas ISO para crear un marco de aseguramiento de la identidad digital internacional completo.

74. A la luz de la evolución de las normas, esta Guía hace muchas referencias a la Guía de identidad digital del NIST y al marco eIDAS. Las autoridades ALA/CFT deberían trabajar estrechamente con sus homólogos en materia de identidad digital, ciberseguridad y otros organismos pertinentes para identificar los marcos y normas de garantía de la identidad digital aplicables.

75. A medida que la tecnología, la arquitectura y los procesos de identidad digital evolucionan, los marcos de garantía y las normas técnicas para los propios sistemas de identidad digital tendrán que evolucionar, y es probable que se queden atrás con respecto a la evolución de los sistemas de identidad digital. Se insta a los gobiernos y al sector privado a que sigan de cerca la tecnología/procesos de identidad digital emergentes que ofrezcan una prueba de identidad o autenticación más sólida y a que traten los marcos y normas como una herramienta de evaluación útil, en lugar de utilizar los niveles de garantía más altos existentes para establecer un límite máximo.

SECCIÓN III: ESTÁNDARES DEL GAFI SOBRE DEBIDA DILIGENCIA DEL CLIENTE



76. Esta sección requiere una comprensión básica de cómo funcionan los sistemas de identidad digital. Se anima a los lectores a revisar la breve explicación de los pasos básicos en un sistema de identidad digital genérico en la Sección II y en el Anexo A, que proporciona la base para la discusión en esta Sección sobre cómo la Recomendación 10, y en particular, sus criterios de «confiables e independientes», entran en juego.

77. La Recomendación 10 requiere que las jurisdicciones impongan obligaciones de debida diligencia del cliente (DDC) a los sujetos obligados. La discusión que sigue aclara la aplicación de la Recomendación 10 (a) en el contexto de los sistemas de identidad digital. Los sujetos obligados deben determinar el alcance de las medidas de DDC utilizando un enfoque basado en el riesgo (EBR) de acuerdo con las Notas Interpretativas de la Recomendación 10 y de la Recomendación 1. También se considera brevemente cómo los sistemas de identidad digital confiables pueden apoyar otros requisitos ALA/CFT bajo la R.10(d).

Requisitos de identificación/verificación del cliente (admisión)

78. Los sujetos obligados, al establecer relaciones comerciales con un cliente (es decir, en el momento de la admisión), deben identificar al cliente y verificar su identidad, *utilizando documentos, datos o información confiables, de fuentes independientes»* (Recomendación 10, sub-sección (a)).

Pruebas y procesos documentales o digitales de la identidad

79. La Recomendación 10 es neutral desde el punto de vista tecnológico. La Recomendación 10 (a) permite a las instituciones financieras utilizar «documentos», así como «información o datos», al llevar a cabo la identificación y verificación de los clientes. La Recomendación 10 (a) no impone ninguna restricción en cuanto a la forma (documental/física o digital) que las pruebas de identidad, «documentos, información o datos», pueden adoptar.

80. Además, aunque la Recomendación 10 (a) exige a las instituciones financieras que vinculen la identidad verificada de un cliente con la persona de alguna manera «confiable», nada en los Estándares del GAFI establece requisitos sobre cómo una identidad verificada de un cliente debe estar vinculada a una persona única y real como parte de la identificación/verificación en el momento de la admisión. Por lo tanto, la Recomendación 10 no impone limitaciones en cuanto al uso de sistemas de identidad digital para ese fin. Los Estándares del GAFI dejan la cuestión en manos de cada jurisdicción, como parte de su marco legal nacional para acreditar la identidad oficial al realizar la DDC.

Prueba de identidad «confiable, independiente»

81. La clave para determinar cómo se pueden utilizar los sistemas de identidad digital para la identificación/verificación de clientes es entender qué significa en el contexto digital el requisito de la Recomendación 10 de «utilizar documentos, datos o información confiables, de fuentes independientes». Los marcos y normas de garantía de la identidad digital hacen referencia al término «garantía» para describir la solidez de los sistemas. Los niveles de garantía son, por tanto, útiles para determinar si un determinado sistema de identidad digital es «confiable e independiente» a efectos ALA/CFT.

82. El siguiente análisis explora el desarrollo del actual requisito de «confiabilidad e independencia» del GAFI, con el fin de profundizar en su significado y objetivos subyacentes.

83. En las 40 Recomendaciones del GAFI de julio de 1990, la Recomendación 12 exigía a los sujetos obligados que identificaran a sus clientes «sobre la base de un documento oficial u otro documento de identificación confiable».22 Esta redacción se mantuvo sin cambios a través de las revisiones de las Recomendaciones de junio de 1996 y junio de 2003,

22 Las 40 Recomendaciones del GAFI de julio de 1990 imponían requisitos de identificación de los clientes a las instituciones financieras para reforzar su papel en la lucha contra el LA de las ganancias ilícitas del narcotráfico. La Recomendación 12 (1990) establecía, en la parte pertinente (el énfasis es nuestro; la puntuación es el original): *[Las instituciones financieras* no deberían mantener cuentas anónimas o con nombres obviamente ficticios: *deberían estar obligadas* (por ley, por reglamento, por acuerdos entre las autoridades de supervisión y las instituciones financieras o por acuerdos de autorregulación entre las instituciones financieras) *a identificar, sobre la base de un documento oficial u otro documento de identificación confiable*, y registrar la identidad de *sus clientes*, ya sea

y se mantuvo hasta que se adoptó la versión actual de las Recomendaciones en febrero de 2012. En 2012, el GAFI añadió el requisito de «verificación de la identidad» y la exigencia de que las pruebas de identidad sean «independientes», además de «confiables». Al mismo tiempo, la revisión de 2012 adoptó un enfoque más flexible y amplio en cuanto a los tipos de pruebas de identidad (documentos, pero también datos o información digital) que podían utilizarse para la identificación/verificación de clientes. También abandonó la referencia explícita de las anteriores Recomendaciones a los «documentos de identificación oficiales».

84. En el contexto de la identidad digital, el requisito de que los «documentos, datos o información» digitales deben ser de fuentes «confiables e independientes» significa que el sistema de identidad digital utilizado para llevar a cabo la DDC se basa en la tecnología, la gobernanza adecuada, los procesos y los procedimientos que proporcionan niveles adecuados de confianza en que el sistema produce resultados precisos. Esto significa que cuentan con medidas de mitigación para evitar los tipos de riesgos expuestos en la Sección IV.

Enfoque basado en el riesgo a la DDC

85. La Recomendación 10 exige a los sujetos obligados que utilicen un enfoque basado en el riesgo (EBR) para determinar el alcance de las medidas de DDC que deben aplicarse, incluida la identificación/verificación del cliente. Según la Recomendación 10 y su Nota Interpretativa, los sujetos obligados deben identificar, evaluar y tomar medidas efectivas para mitigar sus riesgos de LA/FT (para clientes, países o áreas geográficas; y productos, servicios, transacciones o canales de entrega). Se requieren medidas reforzadas en situaciones de mayor riesgo y se pueden aplicar medidas simplificadas en situaciones de bajo riesgo. El GAFI ha publicado unas Guías sobre cómo las jurisdicciones/sujetos obligados podrían aplicar medidas de DDC utilizando el enfoque basado en el riesgo para apoyar los objetivos de inclusión financiera.[23]

Aplicar un enfoque basado en el riesgo a las medidas de DDC para apoyar los objetivos de inclusión financiera

86. Como se analiza en detalle en la Sección V, en virtud de las Recomendaciones 1 y 10 y sus NIR, los sujetos obligados deben aplicar medidas de DDC que sean acordes con el tipo y el nivel de los riesgos de LA/FT. La Nota Interpretativa a la Recomendación 1 enfatiza que al evaluar el riesgo, los sujetos obligados deben considerar todos los factores de riesgo relevantes antes de determinar cuál es el nivel de riesgo general y el nivel apropiado de mitigación que debe aplicarse. Junto con la Recomendación 10 y la NI R.10, la NI R.1 dispone específicamente que los sujetos obligados pueden diferenciar el alcance de las medidas, dependiendo del tipo y el nivel de riesgo de los distintos factores de riesgo (por ej., en una situación particular, podrían aplicar una DDC normal para las medidas de aceptación del cliente, pero una DDC intensificada para la supervisión continua, o viceversa).

---

ocasional o habitual, al establecer relaciones comerciales o realizar transacciones (en particular, la apertura de cuentas o libretas de ahorro, la realización de transacciones fiduciarias, el alquiler de cajas de seguridad [sic], la realización de grandes transacciones en efectivo).

23 GAFI (2013-2017), *Medidas anti-lavado de activos y contra el financiamiento del terrorismo e inclusión financiera - Con complemento sobre debida diligencia del cliente,* GAFI, París www.fatf- gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf

Relaciones comerciales y transacciones no presenciales

87. El GAFI utiliza los términos presencial y **no presencial** para clasificar las relaciones y las transacciones comerciales (incluida la admisión). A efectos del GAFI, se considera que las interacciones presenciales se producen en persona, es decir, que las partes de la interacción/transacción se encuentran en el mismo lugar físico y realizan sus actividades mediante la interacción física. Se considera que las **interacciones no presenciale**s se producen a distancia, es decir, que las partes no se encuentran en el mismo lugar físico y llevan a cabo sus actividades por medios digitales u otros medios no presenciales, como el correo o el teléfono.[24]

88. La Nota Interpretativa de la Recomendación 10 incluye las «relaciones o transacciones en las que no se entabla un contacto físico entre las partes» como *ejemplo* de una situación *potencialmente* de mayor riesgo a la hora de llevar a cabo la DDC. Por sus términos, esta declaración no exige que las autoridades competentes y los sujetos obligados clasifiquen siempre las relaciones comerciales o las transacciones financieras que no son presenciales como de mayor riesgo a efectos de LA y FT. Más bien, las relaciones comerciales y las transacciones que no son presenciales son *ejemplos* de circunstancias en las que el riesgo de LA o FT puede ser *potencialmente* mayor.

89. Dada la evolución de la tecnología de identidad digital, la arquitectura, los procesos y la aparición de normas técnicas de identidad digital de código abierto basadas en el consenso, es importante aclarar que la identificación del cliente y las transacciones no presenciales que se basan en sistemas de identidad digital confiables e independientes con medidas apropiadas de mitigación del riesgo, pueden presentar un nivel de riesgo estándar, e incluso menor cuando se implementan niveles de garantía más altos y/o se aplican medidas de control del riesgo de LA/FT adecuadas, como los límites de funcionalidad del producto y otras medidas discutidas en NI R.10 y la Guía del GAFI sobre inclusión financiera (véase también la sección sobre «Consideraciones especiales para la inclusión financiera, la comprobación e inscripción de identidad a distancia» más adelante en esta Guía).

Debida diligencia continua sobre la relación comercial

90. Además, en virtud de la Recomendación 10 (d), los sujetos obligados deben llevar a cabo «la debida diligencia continua de la relación comercial y examinar las transacciones llevadas a cabo a lo largo de esa relación para asegurar que las transacciones que se realicen sean consistentes con el conocimiento que tiene la institución sobre el cliente, su actividad comercial y el perfil de riesgo, incluyendo, cuando sea necesario, la fuente de los fondos».

91. Como se explica en la Sección II, más arriba, y con más detalle en el Anexo A, la **autenticación** mediante un sistema de identidad digital establece la confianza de que un individuo es la persona a la que se le comprobó la identidad y se le expidieron las credenciales pertinentes. Se anima a los sujetos obligados que utilizan sistemas de identidad digital para autenticar la identidad de sus clientes actuales como parte de la autorización de

24 La definición de interacciones presenciales y no presenciales puede variar según la normativa nacional. Por ejemplo, algunas jurisdicciones consideran que la identificación por vídeo es una interacción presencial.

cuentas a que aprovechen los datos generados por la autenticación y la información relacionada,[25] para apoyar la debida diligencia continua y la supervisión de las transacciones. Esta información se obtiene tradicionalmente con el fin de proteger al sujeto obligado contra el fraude. Sin embargo, con la aceleración de la transición a los sistemas financieros digitales y la consiguiente dependencia del uso de la autenticación de la identidad digital para autorizar el acceso a las cuentas, también puede ser relevante a efectos ALA/CFT.

92. Para los sujetos obligados, la autenticación continua de un cliente admitido proporciona una garantía razonable, basada en el riesgo (es decir, confianza), de que la persona que afirma su identidad hoy es la misma que abrió previamente la cuenta u otro servicio financiero, y es de hecho la misma persona que se sometió a una identificación y verificación «confiable e independiente» en el momento de la admisión. La autenticación digital continua de la identidad del cliente vincula a esa persona con su actividad financiera. Por lo tanto, puede facilitar el fortalecimiento de la capacidad para llevar a cabo una debida diligencia significativa y un seguimiento de las transacciones de conformidad con la R.10(d).

Requisitos para la dependencia en terceros

93. Esta sección explica cómo un sujeto obligado con fines ALA/CFT puede (1) confiar en la identificación/verificación del cliente realizada por otro sujeto obligado en el contexto de la identidad digital (en el ámbito de la Recomendación 17), y (2) actuar como agente o como entidad subcontratada para otro sujeto obligado (fuera del ámbito de la Recomendación 17).

94. En virtud de la Recomendación 17, los países pueden permitir a los sujetos obligados[26] que dependan de terceros para llevar a cabo la identificación/verificación del cliente en el momento de la incorporación,[27] siempre que se cumplan las siguientes condiciones:

- El tercero debe ser también un sujeto obligado sujeto a los requisitos de DDC en línea con las Recomendaciones 10, y regulado y supervisado o monitoreado para el cumplimiento.
- Los sujetos obligados deben:
  - Obtener inmediatamente la información necesaria sobre la identificación/verificación del cliente
  - Adoptar las medidas adecuadas para convencerse de que las copias de los datos de identificación y demás documentación relevante relativa a los requisitos de la Recomendación 10 (a) se pondrán a disposición del tercero que lo solicite sin demora;

25 La autenticación es una parte de la autorización de acceso a la cuenta. El sujeto obligado también puede recoger otros datos complementarios (como, por ejemplo, la geolocalización, las direcciones IP, etc.) para las decisiones de autorización.

26 La Recomendación 22 establece que los requisitos de dependencia de la R.17 se aplican a las APNFD.

27 La Recomendación 17 autoriza la dependencia en terceros para los elementos (a)-(c) de las medidas de DDC establecidas en la Recomendación 10, pero no autoriza la dependencia en terceros para llevar a cabo la debida diligencia continua en la relación comercial. Esta Guía discute la Recomendación 17 solo en lo que se refiere a la Recomendación 10 (a) identificación/verificación.

- Cerciorarse de que el tercero está regulado, supervisado o monitoreado en cuanto a los requisitos de DDC y de mantenimiento de registros de conformidad con las Recomendaciones 10 y 11; y
- Considerar la información sobre el riesgo país, al determinar en qué países puede estar radicado el tercero que cumple las condiciones anteriores.

95. Cuando se permite esta dependencia, la responsabilidad regulatoria final de las medidas de DDC sigue siendo del sujeto obligado que depende en el tercero.

Dependencia en terceros en el contexto de la identidad digital (cuando los sujetos obligados también actúan como proveedoras de servicios de identidad digital)

96. Si lo permite la jurisdicción, un sujeto obligado podría confiar en otro sujeto que cumpla los criterios descritos anteriormente para realizar la identificación/verificación del cliente en el momento de la admisión, utilizando un sistema de identidad digital, siempre que el sistema de identidad digital del tercero permita al sujeto obligado que confía:

- Obtener inmediatamente la información necesaria sobre la identidad del cliente (incluidos los niveles de seguridad (confianza), cuando proceda). Por ejemplo, el sistema de identidad digital podría permitir al posible cliente confirmar su identidad al sujeto obligado que confía y al tercero autenticar la identidad de la persona y proporcionar información, como el nombre de la persona, la fecha de nacimiento, un número de identidad único proporcionado por el estado u otros atributos necesarios para demostrar la identidad oficial para establecer una relación comercial en la jurisdicción.
- Tomar las medidas adecuadas para asegurarse de que el tercero pondrá a disposición copias u otras formas adecuadas de acceso a las pruebas de identidad (documentos, datos y otra información pertinente) relacionadas con los requisitos de la Recomendación 10 (a) cuando se le solicite sin demora. Por ejemplo, la entidad que confía podría tomar las medidas adecuadas para (1) asegurarse de que, como parte de la comprobación e inscripción de la identidad, el tercero estableció una cuenta de identidad digital para la persona identificada que contiene las pruebas de atributos adecuadas y otros datos e información de identidad, y (2) que los procesos de autenticación del tercero le permiten proporcionar esa información a la parte que confía si lo solicita sin demora.

Sujetos obligados como proveedores de servicios de identidad digital al margen de la Recomendación 17

97. Los sujetos obligados que hayan desarrollado sus propios sistemas de identidad digital podrían tratar de convertirse en proveedores de servicios de identidad digital actuando como agentes o entidades subcontratadas para otros sujetos obligados. Cuando se permita, esto implicaría la tercerización de la identificación/verificación del cliente en el momento de la admisión y la autenticación de los clientes. En esta situación, la dependencia en terceros según la Recomendación 17 no se aplica, ya que la Recomendación 17 no cubre la tercerización o las relaciones de agencia.

98. Al igual que otros proveedores de servicios de identidad digital que actúan como agentes o entidades de tercerización, los sujetos obligados que actúan como proveedores de servicios de identidad digital utilizarían su sistema de identidad digital para llevar a cabo la identificación/verificación del cliente (y la autenticación) *en nombre* del sujeto obligado que

delega. También, al igual que otros proveedores de servicios de identidad digital, podría buscar la certificación, de conformidad con los marcos de auditoría y certificación del gobierno de la jurisdicción, si están disponibles, o la auditoría y la certificación de una organización de certificación del sector privado de buena reputación.

99. En cualquier caso, como principal, la entidad designada seguiría siendo responsable de llevar a cabo una identificación/verificación *efectiva* del cliente, y una autenticación *efectiva*, utilizando el sistema de identidad digital proporcionado por el proveedor de servicios de identidad digital, y tendría que aplicar el EBR al uso de los sistemas de identidad digital para la identificación/verificación y autenticación del cliente, como se discute en la Sección V.

SECCIÓN IV: BENEFICIOS Y RIESGOS DE LOS SISTEMAS DE IDENTIDAD DIGITAL PARA EL CUMPLIMIENTO ALA/CFT Y CUESTIONES RELACIONADAS

100. Esta sección describe algunos de los beneficios potenciales de los sistemas de identidad digital para los sujetos obligados, sus clientes y el gobierno, así como los riesgos potenciales que deben ser identificados, comprendidos, supervisados y gestionados o mitigados adecuadamente. Estos beneficios y riesgos se relacionan tanto con la aplicación de las salvaguardias ALA/CFT como con la inclusión financiera.

101. Esta sección pretende concienciar a las partes interesadas de los posibles riesgos específicos de las tecnologías de identidad digital, de modo que puedan prevenirse o gestionarse eficazmente aplicando el EBR establecido en la Sección V. El análisis de los riesgos que se expone a continuación no pretende desalentar el uso de sistemas de identidad digital fiables e independientes, es decir, aquellos que cumplen con los niveles de garantía adecuados (a saber, acuerdos de gobernanza y normas técnicas) y que abordan adecuadamente los posibles riesgos. Tampoco se pretende sugerir que el uso de sistemas de identidad digital, especialmente para la identificación/verificación de clientes, sea necesariamente más vulnerable a los abusos que los métodos documentales tradicionales.

102. Esta sección también destaca una serie de retos más amplios que presentan los sistemas de identidad digital. La respuesta a estos retos no suele ser competencia directa de

las autoridades ALA/CFT, pero estos retos pueden tener un impacto indirecto en los esfuerzos ALA/CFT.

103. Mientras que esta sección proporciona una visión general de algunos de los riesgos y desafíos, los marcos y normas de garantía de identidad digital proporcionan un marco para evaluar las medidas de mitigación de riesgos de un sistema de identidad digital. Se anima a las jurisdicciones a que revisen estas normas, que abordan una amplia gama de riesgos (en relación con la tecnología, pero también con otros aspectos organizativos y de gobernanza pertinentes) que existen y cómo deben mitigarse.

Beneficios potenciales de los sistemas de identidad digital

Fortalecimiento de la DDC

104. Los sistemas de identidad digital tienen el potencial de mejorar la confiabilidad, la seguridad, la privacidad, la conveniencia y la eficiencia de la identificación de las personas en la prestación de servicios financieros, en beneficio de los clientes, los sujetos obligados y la integridad del sector financiero. Como se expone más adelante, los sistemas de identidad digital fiables e independientes pueden ofrecer ventajas significativas para mejorar la identificación/verificación de los clientes en el momento de la admisión y para autentificar la identidad de los clientes para autorizar el acceso a las cuentas. Además, la identificación precisa de los clientes podría permitir otras medidas de DDC, incluida la debida diligencia continua y eficaz sobre la relación comercial y la supervisión de las transacciones.

Minimizar las debilidades de las medidas de control humano

105. Los métodos documentales tradicionales para llevar a cabo la identificación/verificación de los clientes se basan en gran medida en medidas de control humano, por ejemplo, comparar la fotografía de un documento de identidad oficial con la persona que pretende abrir una cuenta, y juzgar que el documento de identidad es auténtico. El personal de primera línea puede carecer de las herramientas, la tecnología, la formación, las habilidades y la experiencia necesarias para identificar de forma fiable los documentos falsos, alterados o robados.

106. El uso de sistemas de identidad digital confiables e independientes puede reducir potencialmente la posibilidad de error humano en la identificación y verificación de la identidad de una persona.

- En primer lugar, incluso cuando el componente de comprobación de la identidad de un sistema de identidad digital se lleva a cabo en persona[28] y se basa en el juicio humano, ese proceso suele ser realizado por especialistas con acceso a herramientas técnicas avanzadas para detectar documentos de identidad fraudulentos y robados. Por ejemplo, la comprobación de la identidad a distancia, al menos en los niveles de garantía más altos, suele emplear tecnologías de identidad digital cada vez más sofisticadas y eficaces para determinar que los documentos de identidad son auténticos y no falsos, así como

28 Como se expone en la Sección II y en el Anexo A, en un sistema de identidad digital, la comprobación de la identidad es un componente que puede producirse en persona (es decir, no tiene que producirse a distancia para ser considerado un sistema de identidad digital).

datos e información adicionales que ayudan a acreditar la identidad del individuo de forma fehaciente.[29]

- En segundo lugar, el componente de autenticación de un sistema de identidad digital elimina en gran medida el papel del juicio humano subjetivo para determinar que los clientes son quienes dicen ser. Los sistemas de identidad digital con autenticación de múltiples factores y procesos seguros pueden ser siempre fiables a la hora de determinar que la persona que pretende abrir o acceder a una cuenta es, de hecho, el mismo individuo al que se emitieron originalmente las credenciales de identidad.

Mejorar la experiencia del cliente y generar un ahorro de costos

107. Los sistemas de identidad digital confiables e independientes también pueden proporcionar experiencias más eficientes y fáciles de usar para los clientes potenciales en la admisión y, posteriormente, para los clientes que buscan acceder a sus cuentas. La aceptación del cliente y la comodidad son factores importantes para completar las solicitudes y las transacciones, así como para retener a los clientes. La facilidad de uso para los clientes, combinada con el potencial aumento de la eficiencia para los sujetos obligados, puede ayudar a reducir los costos de admisión. Un informe sugiere que los sujetos obligados que utilizan sistemas de identidad digital podrían ver una reducción de costos de hasta el 90 por ciento en la admisión de clientes, ya que el tiempo necesario para la identificación/verificación y otros elementos de DDC se reduciría de días o semanas a minutos.[30] Este ahorro de costos podría permitir a los sujetos obligados asignar recursos de cumplimiento a otras funciones de cumplimiento ALA/CFT, y también facilitar la inclusión financiera de personas que de otro modo estarían excluidas o desatendidas al reducir los costos de admisión.

Monitoreo de transacciones

108. Como se ha señalado anteriormente, la autenticación digital robusta de la identidad del cliente para autorizar el acceso a la cuenta en curso puede facilitar la identificación y la notificación de transacciones sospechosas, porque ayuda al sujeto obligado a establecer que la persona que accede a una cuenta y realiza transacciones en la actualidad es la misma persona que accedió a la cuenta anteriormente, y es, de hecho, el cliente identificado/verificado que es titular de esa cuenta. Además, dependiendo del modelo operativo y de otros factores, como el consentimiento del usuario y las leyes de protección de datos/privacidad, la autenticación de la identidad digital para autorizar el acceso a la cuenta puede permitir a los sujetos obligados capturar información adicional, como la geolocalización, la dirección IP o la identidad del dispositivo digital utilizado para realizar las transacciones. Esta información puede ayudar a los sujetos obligados a desarrollar una comprensión más detallada del comportamiento del cliente como base para determinar cuándo sus operaciones financieras parecen ser inusuales o sospechosas, y puede ayudar a las fuerzas del orden a investigar delitos. Por ejemplo, los datos complementarios cuando

---

29 En la actualidad, los elementos de seguridad que sólo son legibles mediante luz ultravioleta (UV) o que son un elemento de la construcción física del documento, como las costuras de seguridad, los grabados o los agujeros perforados que atraviesan varias páginas, pueden ser más difíciles o imposibles de validar a distancia, pero la mayoría de los documentos de identidad cuentan con sólidos elementos de seguridad que pueden comprobarse eficazmente a distancia.

30. McKinsey Global Institute (2019), Identificación Digital, www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx.

son recogidos por los sujetos obligados a través de diferentes medios y canales (incluidos Internet y el teléfono móvil), de acuerdo con la normativa local, incluidas las normas de protección de datos y de privacidad, pueden ser muy útiles para determinar quién controla una cuenta; si controla varias cuentas; y la red de personas y entidades que participan en las transacciones financieras realizadas, utilizando esas cuentas.

Inclusión financiera

109. La rápida digitalización de los servicios financieros ha incrementado enormemente la importancia de los sistemas de identidad digital confiables e independientes para la inclusión financiera, especialmente en los países en desarrollo,[31] donde los sistemas de identidad digital y los servicios financieros digitales han surgido como motores centrales de la inclusión financiera.[32] El desarrollo de marcos y normas de garantía de identidad digital flexibles y basados en resultados puede permitir a las personas financieramente excluidas que no tienen acceso a los documentos de identidad oficiales tradicionales, como pasaportes y licencias de conducir, obtener identificaciones digitales con un nivel de garantía de identidad más bajo (que requiere pruebas de identidad y verificación menos estrictas) y utilizarlas para obtener servicios financieros en situaciones apropiadas de bajo riesgo. Los marcos y normas de garantía también permiten a las personas financieramente excluidas obtener identidades digitales utilizando pruebas de identidad alternativas (por ej., el uso de «árbitros de confianza» que respondan por el solicitante como forma de prueba de identidad). Además, los sistemas de identidad digital pueden llegar a las poblaciones excluidas en zonas remotas para respaldar la prueba de identidad/inscripción segura no presencial para la identificación/verificación del cliente. Estas cuestiones se analizan con mayor detalle en la sección «Consideraciones especiales para la inclusión financiera», más adelante en esta Guía.

110. En los países en desarrollo, los pagos de gobierno a personas (G2P), incluidas las transferencias de prestaciones sociales (por ej., transferencias condicionadas de efectivo, pagos de manutención infantil y subsidios estudiantiles), el pago de salarios y pensiones del gobierno y las devoluciones de impuestos son cada vez más digitales, al igual que las actividades comerciales y los pagos de los consumidores minoristas. En los contextos humanitarios, la ayuda para salvar vidas se presta cada vez más en forma de asistencia digital en efectivo. Todas estas actividades requieren el acceso a una cuenta de transacciones, que puede facilitarse mediante el uso de sistemas de identidad digital.

111. El uso de sistemas de identidad digital confiables e independientes podría reducir los costos de la DDC y permitir que muchas más personas desatendidas y subatendidas utilicen los servicios financieros regulados (véase el Recuadro 4 sobre el Aadhaar de la India y el Recuadro 5 sobre el Registro Nacional de Identificación y Estado Civil de Perú). Esto facilita la inclusión financiera y, con ello, mejora el alcance y la eficacia de los regímenes ALA/CFT.

31 En la Encuesta Global Findex de 2017, el 26% de las personas no bancarizadas en los países de bajos ingresos citaron la falta de documentación oficial de identidad como el principal obstáculo para obtener servicios financieros.

32 GAFI (2013-2017), *Medidas anti-lavado de activos y contra el financiamiento del terrorismo e inclusión financiera - Con complemento sobre debida diligencia del cliente*, GAFI, París www.fatf- gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html.

Riesgos y desafíos que presentan los sistemas de identidad digital

112. Esta Guía se centra en los sistemas de identidad digital para llevar a cabo determinados elementos de DDC, y no en el uso de los sistemas tradicionales de identidad documental. El análisis del riesgo que se hace a continuación no pretende sugerir que los riesgos de los sistemas de identidad digital superen sus beneficios, ni que sean más arriesgados en general que los sistemas de identidad documental tradicionales.

113. Al igual que cualquier sistema de identidad, la fiabilidad de los sistemas de identidad digital depende de la solidez de los documentos, los procesos, las tecnologías y las medidas de seguridad utilizadas para la comprobación de la identidad, la expedición de credenciales y la autenticación, así como la gestión continua de la identidad. Por ejemplo, tanto en los sistemas de identidad documentales como en los digitales, la fiabilidad puede verse socavada por la suplantación de identidad y los documentos de origen que pueden ser fácilmente falsificados o manipulados. Algunos tipos de fraude pueden ser menos probables en persona o en procesos que requieran la intervención humana, incluidos los «fraudes de ataque masivo» que son más probables a distancia. Aunque los sistemas de identidad digital ofrecen características de seguridad, como la autenticación segura, que mitigan algunos problemas de los sistemas basados en papel, también aumentan algunos riesgos, como la pérdida de datos, la corrupción de datos o el uso indebido de datos debido a un acceso no autorizado.

114. Los sistemas de identidad digital presentan una serie de retos y riesgos técnicos, ya que a menudo implican la comprobación de la identidad y la autenticación de las personas a través de una red de comunicaciones abierta (Internet). En consecuencia, los procesos y las tecnologías empleadas por los sistemas de identidad digital presentan múltiples oportunidades de ciberataques entre las partes (proveedor de servicios de identidad digital, cliente y parte que confía). Si no se tienen en cuenta los factores de riesgo pertinentes y no se aplican las salvaguardias adecuadas basadas en la tecnología, así como medidas eficaces de gobernanza y rendición de cuentas para hacerles frente, los delincuentes, los lavadores de dinero, los terroristas y otros agentes malintencionados podrían abusar de los sistemas de identidad digital para crear identidades falsas o explotar (piratear o suplantar) los autenticadores vinculados a una identidad legítima.

115. Los marcos y normas de garantía de la identidad digital proporcionan una herramienta clave para identificar y evaluar algunos de estos riesgos, y mitigarlos con tecnologías y procesos de identidad digital que ofrezcan una garantía adecuada para cada uno de los componentes de la identidad digital.[33] El siguiente análisis de riesgos se aplica a los sistemas de identidad digital que *no* son suficientemente fiables, en términos de los marcos de gestión de riesgos establecidos en los marcos y normas de garantía de la identidad digital. También se refiere a los retos más amplios de conectividad, ciberseguridad y privacidad en el espacio digital que pueden afectar a la integridad o disponibilidad de los sistemas de identidad digital para llevar a cabo la DDC.

116. El análisis que se realiza a continuación abarca tanto los riesgos de comprobación de la identidad/inscripción como los de autenticación. Los riesgos en la fase de comprobación de la identidad pueden dar lugar a identificaciones digitales «falsas» (es decir, obtenidas bajo premisas falsas a través de un acto intencionadamente malicioso) y pueden utilizarse para facilitar actividades ilícitas. Estos riesgos se mitigan con un nivel de garantía de identidad adecuado. Los riesgos de comprobación de la identidad se distinguen de los riesgos de autenticación, en los que una identidad digital legítimamente emitida se ha visto

33 Véase en el Apéndice E un análisis más detallado de los niveles de garantía de la identidad (IAL), los niveles de garantía de la autenticación (AAL) y los niveles de garantía de la federación (FAL), utilizados para evaluar y mitigar los riesgos en cada una de estas etapas básicas.

comprometida y sus credenciales o autenticadores están bajo el control de una persona no autorizada. Estos riesgos se mitigan con un nivel de garantía de autenticación adecuado.

Riesgos de comprobación e inscripción de la identidad

117. Hay dos fuentes generales de amenazas para el proceso de inscripción: (1) los ciberataques y las brechas de seguridad que conducen al compromiso de la información personal identificable (PII) y la presentación de pruebas falsas, ya sea robando la identidad de una persona real (suplantación) o creando una identificación sintética, y (2) el compromiso o la mala conducta del IDSP o el compromiso de la infraestructura de identidad digital más amplia. Esta sección se centra en la primera categoría, ya que el compromiso/la mala conducta del proveedor de identidad, la ciberseguridad y las amenazas a la infraestructura más amplia se abordan más directamente mediante requisitos más amplios de gobernanza/organización en los marcos y estándares de garantía de la identidad digital y los controles tradicionales de seguridad informática (por ej., protección contra intrusiones, mantenimiento de registros, auditorías independientes) que están fuera del alcance de esta Guía.

Riesgos de suplantación de identidad y documentos de identidad sintéticos (que implican ciberataques, protección de datos y/o violaciones de la seguridad)

118. En ciertos aspectos, los riesgos derivados de la presentación de pruebas falsas (robadas o falsificadas) en los sistemas de identidad digital, pueden actualizarse a una escala mucho mayor.[34] La **suplantación** implica que una persona se haga pasar por la identidad de otra persona genuina, esto puede ser a través del simple uso de un documento robado de alguien que se parezca, pero también puede combinarse con pruebas falsas o falsificadas (por ejemplo, la sustitución de la foto en el pasaporte genuino de una persona con la imagen del impostor). Las **identidades sintéticas** son desarrolladas por los delincuentes combinando información real (normalmente robada) y falsa para crear una nueva identidad (sintética), que puede ser utilizada para abrir cuentas fraudulentas y realizar compras fraudulentas. A diferencia de la suplantación, el delincuente se hace pasar por alguien que no existe en el mundo real, en lugar de suplantar una identidad existente. Por ejemplo, los grupos delictivos pueden dedicarse a la suplantación de identidad, generando un gran número de identidades digitales sintéticas que se basan en parte en los atributos de identidad de una persona real y en otros datos que han sido robados de transacciones en línea o mediante el pirateo de bases de datos de Internet, y en parte en información totalmente falsa. Las identidades sintéticas pueden utilizarse para obtener tarjetas de crédito o préstamos en línea y retirar fondos, abandonando la cuenta poco después. Según los expertos en identidad digital, el uso de identidades sintéticas supone el mayor riesgo en la fase de comprobación e inscripción de la identidad de los sistemas de identidad digital en Estados Unidos.[35]

119. A título ilustrativo, el cuadro siguiente expone estos riesgos y presenta algunas estrategias para mitigar las amenazas en los procesos de comprobación e inscripción de la identidad según las Normas del NIST.

---

34 Las búsquedas en Internet de «documentos de identidad falsos» revelan cientos de sitios web que prometen falsificaciones de permisos de conducir, pasaportes, certificados de nacimiento, documentos de inmigración y otros documentos oficiales que pueden ser indistinguibles de las versiones legítimas.

35 Reunión del equipo del proyecto del GAFI con expertos en identidad digital, septiembre de 2019.

Tabla 1. NIST - Estrategias de mitigación de riesgos de la prueba de identidad/inscripción

Tipo de riesgo	Descripción	Posibles estrategias de mitigación de riesgos
Pruebas de identidad falsificadas	Un solicitante alega una identidad incorrecta utilizando un permiso de conducir falsificado.	El IDSP (CSP) valida las características físicas de seguridad de las pruebas presentadas. El IDSP (CSP) valida los datos personales de las pruebas con el emisor u otra fuente autorizada.
Uso fraudulento de la identidad de otro	Un solicitante utiliza un pasaporte asociado a una persona diferente	El IDSP (CSP) verifica las pruebas de identidad y los datos biométricos del solicitante con la información obtenida del emisor o de otra fuente autorizada.

Fuente: NIST 800-63A

Riesgos de la gestión del ciclo de vida de la autenticación y la identidad

120. Las vulnerabilidades asociadas a los tipos y números de los diferentes factores de autenticación pueden dar lugar a riesgos no identificados y no intencionados que pueden permitir a los agentes malintencionados hacer valer la identidad legítima de un individuo (por ej., un cliente) ante una parte que confía para abrir una cuenta u obtener acceso no autorizado a productos, servicios y datos.

121. A título meramente ilustrativo, algunas de estas vulnerabilidades pueden ser:

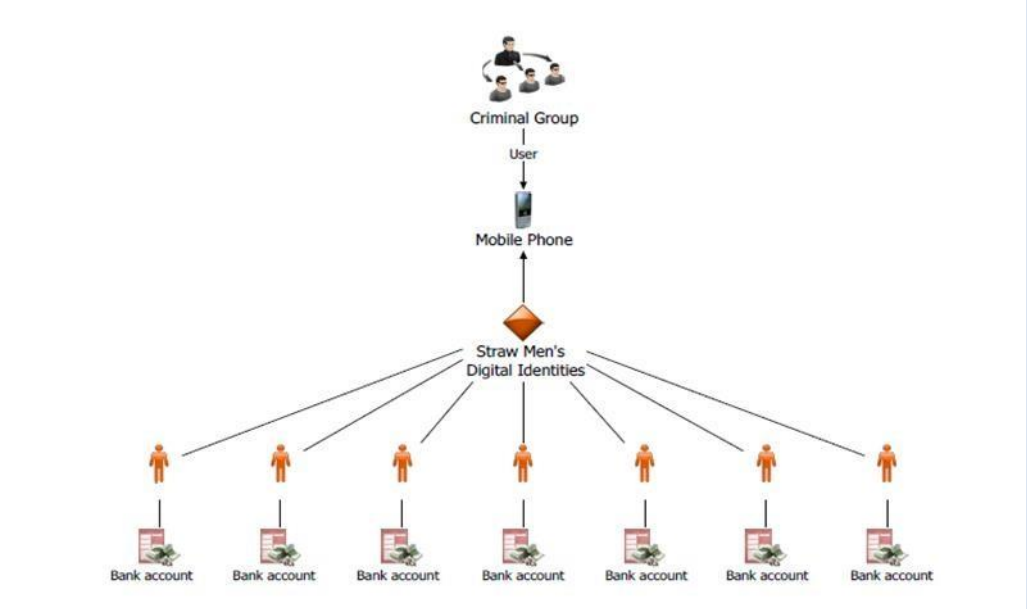
- Relleno de credenciales (también llamado *breach replay* o limpieza de listas): Tipo de ciberataque en el que se comprueban las credenciales de cuentas robadas (a menudo procedentes de una violación de datos) para ver si coinciden con las de otros sistemas. Este tipo puede tener éxito si la víctima ha utilizado la misma contraseña (que fue robada en la violación de datos) para otra cuenta.
- *Phishing*: Es un intento fraudulento de obtener credenciales de víctimas desconocidas mediante ataques de ingeniería social como correos electrónicos engañosos, llamadas telefónicas, mensajes de texto o sitios web. Por ejemplo, un delincuente intenta engañar a su víctima para que proporcione nombres, contraseñas, números de identificación del gobierno o credenciales a una fuente aparentemente fiable.
- Intervención de credenciales o *man-in-the-middle*: Intenta conseguir el mismo objetivo que el *phishing* y puede ser una herramienta para cometerlo, pero lo hace interceptando las comunicaciones entre la víctima y el proveedor de servicios.
- Captura y repetición del código PIN: consiste en capturar un código PIN introducido en el teclado de una PC con un registrador de teclas y, sin que el usuario se dé cuenta, utilizar el PIN capturado cuando la tarjeta inteligente está presente en el lector para acceder a los servicios).

122. La mayoría de las vulnerabilidades de autenticación se explotan sin que el propietario de la identidad lo sepa, pero el abuso también puede implicar la participación consciente de los abonados o de los IDSP. Por ejemplo, los autentificadores secretos compartidos, como las contraseñas, pueden ser robados y explotados por agentes malintencionados, pero también pueden ser compartidos deliberadamente por el propietario de las credenciales de identidad con fines ilícitos.

123. Por ejemplo, las organizaciones delictivas pueden comprar credenciales de identidad digitales de individuos que les permitan acceder a las cuentas de los individuos en sujetos obligados, convirtiéndolos de hecho en mulas digitales para la organización. Las personas pueden tener ya una cuenta o aceptar abrir una en relación con la venta de las credenciales de identidad (véase el estudio de caso más abajo).

Cuadro 2. Uso indebido de la identidad digital por parte de los testaferros

Suecia destacó los riesgos de LA/FT derivados de la utilización sistemática por parte de un delincuente de la identidad digital de un testaferro para lavar el producto del delito. Se trata de un riesgo que también podría existir en las transacciones presenciales, pero que se ofrece para ilustrar cómo podrían producirse estos ataques en el mundo digital. Los servicios de los proveedores de servicios de pago que ofrecen transacciones en tiempo real son especialmente útiles para los delincuentes, ya que, junto con las identidades digitales mal utilizadas, permiten transferir rápidamente dinero entre varias cuentas.



Cuando los grupos delictivos desean lavar dinero mediante el uso indebido de identidades digitales, primero tienen que abrir cuentas bancarias, lo que se hace mediante testaferros. El papel de un testaferro es abrir una cuenta bancaria, obtener una identidad digital y un código de seguridad, y proporcionar sus credenciales al grupo delictivo, a cambio de dinero. Se pueden utilizar varias identidades digitales en un solo teléfono móvil o tableta (véase el diagrama anterior). Luego, las cuentas bancarias son controladas por el grupo delictivo. Es importante señalar que la inmensa mayoría de las identidades digitales que son utilizadas indebidamente por los grupos delictivos, se emiten sobre esta base de pruebas de identidad legítimas (es decir, pruebas de identificación).

Fuente: Suecia

124. A continuación se describen algunos de los principales riesgos conocidos asociados a tipos específicos de autentificadores/procesos que son particularmente relevantes para los esfuerzos ALA/CFT.

125. **Vulnerabilidades de la autenticación multifactorial (MFA):** Las contraseñas o códigos de acceso, que se supone que son autenticadores de conocimiento «secreto compartido», son vulnerables a los ataques de inicio de sesión de fuerza bruta, a los ataques de *phishing* y a las violaciones masivas de datos en línea, y son muy fáciles de derrotar. Las contraseñas

robadas, débiles o por defecto están detrás del 81% de las violaciones de datos.[36] Las soluciones de autenticación multifactor (MFA), como los códigos de un solo uso enviados por SMS al teléfono del abonado, añaden otra capa de seguridad a las contraseñas/códigos de acceso, pero también pueden ser vulnerables al *phishing* y a otros ataques. Los autenticadores resistentes al *phishing* en los que al menos uno de los factores se basa en el cifrado de clave pública[37] (por ejemplo, los autenticadores basados en certificados PKI o en los estándares FIDO) pueden ayudar a combatir estas vulnerabilidades.

126. **Autenticadores biométricos:** Los autentificadores biofísicos, como las huellas dactilares y los escáneres de iris, son más difíciles de superar que los autentificadores tradicionales y son cada vez más omnipresentes. La mayoría de los teléfonos inteligentes tienen escáneres de huellas dactilares incorporados; algunos teléfonos inteligentes tienen escáneres de iris incorporados; y las capacidades de reconocimiento facial están incorporadas en muchos sistemas de ordenadores personales y teléfonos inteligentes avanzados.

127. Las características biométricas podrían ser robadas en bloque de las bases de datos centrales.[38] También podrían obtenerse mediante la toma de imágenes de alta resolución (fotos); levantadas de objetos que el individuo toca (por ejemplo, huellas dactilares latentes); o capturadas con imágenes de alta resolución (por ejemplo, patrones de iris), y posteriormente falsificadas. Sin embargo, en la actualidad, estos tipos de ataques son difíciles y/o requieren muchos recursos, por lo que no son escalables. Por ejemplo, los autentificadores biométricos que requieren una coincidencia en el dispositivo no pueden ser utilizados de forma fraudulenta a escala porque requieren acceso físico al dispositivo del cliente.

128. La biometría tiene otros puntos débiles que plantean problemas de fiabilidad cuando se utiliza con fines de autenticación, y han llevado a algunas normas técnicas a restringir su uso para la autenticación (frente a la prueba de identidad). [39] Las huellas dactilares pueden no leerse, o leerse incorrectamente. Los factores de reconocimiento facial pueden dejar de ser fiables por las expresiones faciales de diferentes estados de ánimo, los cambios en el vello facial, el maquillaje; y las condiciones de iluminación variables. Debido a conjuntos de datos incompletos, el reconocimiento facial ha sido menos fiable en el caso de personas con una pigmentación de piel más oscura y ciertos rasgos étnicos, aunque esto está mejorando. A diferencia de los autentificadores basados en el conocimiento o la posesión, los autentificadores biométricos robados son difíciles de revocar o sustituir.[40]

129. **Riesgos del ciclo de vida de la identidad:** Una gestión deficiente del ciclo de vida de la identidad y del acceso puede, consciente o inconscientemente, comprometer la integridad de los autenticadores y permitir que personas no autorizadas accedan a las cuentas de los clientes y hagan un uso indebido de ellas, lo que socava el propósito de la identificación/verificación de los clientes y los requisitos de debida diligencia y supervisión de las transacciones en curso para proteger el sistema financiero de los abusos.

---

36 Informe de investigación de fugas de datos (DBIR) de Verizon 2018, disponible en https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf.

37 En el **cifrado de clave pública**, se genera un par de claves para una entidad, una persona, un sistema o un dispositivo, y esa entidad mantiene la clave privada de forma segura, mientras que distribuye libremente la clave pública a otras entidades. Cualquiera que tenga la clave pública puede entonces utilizarla para cifrar un mensaje y enviarlo al titular de la clave privada, sabiendo que sólo él podrá abrirlo.

38. En un ataque a la Oficina de Gestión de Personal de Estados Unidos (OPM) en 2015, se robaron 5,6 millones de conjuntos de imágenes de huellas dactilares.

39 Véase NIST 800-63-3, NIST 800-63 (b) y Anexo E.

40 Aunque existen métodos para revocar las credenciales biométricas, en la actualidad su disponibilidad es limitada, y las normas técnicas para probarlas aún están en desarrollo.

130. **Riesgos desconocidos:** Los sistemas de identidad digital se desarrollan y evolucionan. En muchos casos, los cambios en el diseño técnico introducen mejoras operativas, pero traen consigo vulnerabilidades que no son evidentes hasta que son explotadas por agentes malintencionados de forma que revelan cómo se ha visto comprometido el sistema de identidad digital.

Obstáculos potenciales para acceder a la información de identidad para la debida diligencia y la supervisión de las transacciones

131. La autenticación en el entorno de la identidad digital puede contribuir a la debida diligencia continua y a la supervisión de las transacciones. Cuando el sujeto obligado adopta el sistema de identidad digital de terceros y no recopila por sí mismo información como los patrones de las transacciones, las ubicaciones, el acceso a los dispositivos, etc., puede no tener acceso a la información que es importante para analizar el comportamiento de los clientes y los patrones de las transacciones con el fin de determinar si las transacciones que se realizan son coherentes con el conocimiento que tiene la entidad del cliente, su negocio y su perfil de riesgo, incluyendo, cuando sea necesario, el origen de los fondos. Cuando esta información se recopila con fines de lucha contra el fraude, también podría ser útil a efectos ALA/CFT. Los sujetos obligados podrían considerar la posibilidad de obtener acceso a sus datos de autenticación de acceso a la cuenta (o el análisis por parte de terceros) para permitir la detección del uso indebido sistemático de las identidades digitales, incluidas las identidades digitales comprometidas, robadas o vendidas. Esta información podría utilizarse para identificar y determinar si hay que denunciar actividades sospechosas. Una ventaja importante del modelo de identidad federada es que la detección del fraude de identidad puede compartirse en una red de proveedores de identidad y partes que confían.

Cuestiones más amplias que presentan los sistemas de identidad digital y que pueden repercutir en los esfuerzos ALA/CFT

Problemas de conectividad

132. La falta de una infraestructura fiable puede socavar los sistemas de identidad digital en una jurisdicción o en determinadas zonas geográficas durante períodos de tiempo significativos. Sin embargo, los sistemas de identidad digital pueden diseñarse para permitir las transacciones tanto en línea como fuera de línea, lo que les permite funcionar con o sin acceso a Internet o a una red móvil. Los sujetos obligados deben tener en cuenta la capacidad de resiliencia a la hora de decidir si utilizan un sistema de identidad digital para la DDC.

Marcos nacionales para la identidad oficial

133. En la medida en que los sistemas de identidad digital se basan en documentos de identidad oficiales para probar la identidad, las deficiencias en la fiabilidad de las pruebas de identidad documentales pueden tener un efecto dominó en los riesgos que plantean los sistemas de identidad digital. La «confiabilidad e independencia» de los enfoques puramente documentales puede verse socavada por el robo de identidad y la falsificación generalizada de documentos de identidad oficiales, incluso cuando éstos carecen de características de seguridad avanzadas para evitar la manipulación o la falsificación o se emiten sin una prueba de identidad adecuada. El robo de identidad a partir de bases de datos en línea genera riesgos similares tanto para los sistemas de identidad digital como para los enfoques documentales.

134. Un documento de identidad digital que se haya desarrollado para un propósito limitado o específico no relacionado con la DDC del sector financiero puede no ser capaz de hacer frente a la demanda de aplicaciones en otras situaciones o enfrentarse a limitaciones y puede crear altos costos para los sujetos obligados o resultar inviable su uso para fines de DDC (véase, por ejemplo, el recuadro 7 del apéndice II) .

Retos de la protección de datos y la privacidad

135. La identidad digital implica la recopilación y el tratamiento de datos personales (PII), incluidos los biométricos. Es importante que los marcos y normas de garantía para la identidad digital incorporen requisitos de protección de datos y privacidad (DPP), que pueden basarse en normas independientes establecidas por una jurisdicción y/o una organización internacional de normalización. Además, se están desarrollando soluciones innovadoras basadas en la tecnología (por ej. la identidad digital descentralizada) para dar al individuo un mayor control sobre cómo se comparte la PII con otros y con qué propósito para abordar aún más las cuestiones de privacidad y protección de datos.

136. El gobierno es el principal responsable de establecer el régimen de DPP en la jurisdicción. Estos requisitos, que protegen la confidencialidad, la exactitud y la integridad de los datos, suelen aplicarse a los proveedores de servicios de identidad digital y les exigen, por ejemplo, que lleven a cabo una evaluación del impacto de la protección de datos (DPIA) para identificar los posibles problemas y las medidas de control de riesgos adecuadas. Las salvaguardias de DPP son importantes para reducir el riesgo de robo de identidad y los riesgos de ciberseguridad que podrían socavar la fiabilidad del sistema de identidad digital. Por lo tanto, de acuerdo con la Recomendación 2 del GAFI, las autoridades ALA/CFT y de DPP deben tratar de cooperar y coordinar para garantizar la compatibilidad de los requisitos y las normas.

Consideraciones sobre la exclusión financiera

137. Cuando los sistemas de identidad digital no cubren a todas, o a la mayoría, de las personas de una jurisdicción, o excluyen a ciertas poblaciones, pueden impulsar (o al menos no mitigar) la exclusión financiera, que es un riesgo de ALA/CFT. El uso obligatorio de una identidad digital específica que no está disponible universalmente para la DDC presenta retos similares a los del uso prescriptivo de una identidad documental que no es accesible para toda la población. La falta de acceso a la tecnología digital o los bajos niveles de conocimientos tecnológicos pueden agravar los riesgos de exclusión. Por ejemplo, la falta de acceso a teléfonos móviles, teléfonos inteligentes u otros dispositivos de acceso digital, o la falta de cobertura y/o conectividad poco fiable, pueden excluir a las poblaciones pobres y rurales o a las mujeres, así como a quienes viven en zonas frágiles y afectadas por conflictos, como los refugiados y los desplazados. Los sistemas de identidad digital también pueden contribuir a la exclusión financiera si utilizan la autenticación biométrica sin proporcionar mecanismos alternativos de autenticación, ya que ciertas modalidades biométricas tienen mayores índices de fracaso para algunos grupos vulnerables. Los trabajadores manuales suelen tener las huellas dactilares desgastadas, que a menudo no pueden ser leídas por los lectores biométricos; los ancianos pueden experimentar frecuentes fallos de coincidencia, debido a la alteración de las características faciales, la pérdida de cabello u otros signos de envejecimiento, enfermedad u otros factores; y ciertos grupos étnicos e individuos con determinadas características físicas relacionadas con la pigmentación más oscura, la forma de los ojos o el vello facial experimentan fallos de reconocimiento facial desproporcionados.

SECCIÓN V: EVALUACIÓN SOBRE SI LOS SISTEMAS DE IDENTIDAD DIGITAL SON LO SUFICIENTEMENTE CONFIABLES E INDEPENDIENTES BAJO UN ABORDAJE A LA DDC BASADO EN EL RIESGO

138. Como se ha señalado en la Sección III, en el contexto de la identidad digital, el requisito de que la identificación/verificación del cliente debe realizarse utilizando «documentos, datos o información de fuentes» confiables e independientes significa que los sistemas de identidad digital deben basarse en la tecnología, los procesos, la gobernanza y otras salvaguardias que proporcionen un nivel *adecuado* de fiabilidad. Esto significa que existe un nivel adecuado de confianza (garantía) de que el sistema de identidad digital funciona como se supone que debe hacerlo y produce resultados precisos. También debe estar adecuadamente protegido contra la manipulación o falsificación interna o externa, para fabricar y acreditar identidades falsas o autenticar a usuarios no autorizados, incluso mediante un ciberataque o una conducta indebida del personal interno.

139. Para determinar si el uso de un sistema de identidad digital es coherente con los requisitos de la Recomendación 10 (a) y (d), los gobiernos, las instituciones financieras y otras partes interesadas deberían realizar las siguientes evaluaciones:

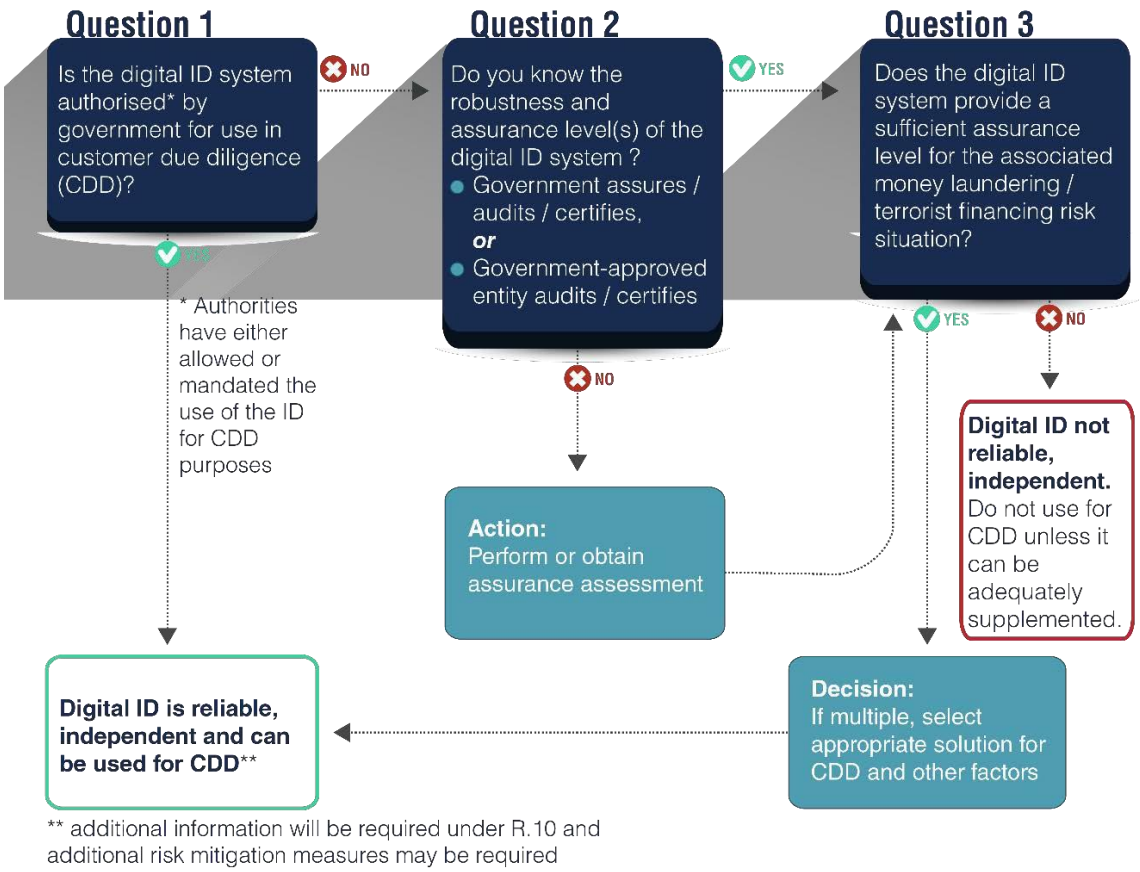
   a. Comprender los niveles de garantía que ofrece el sistema de identidad digital sobre la base de su tecnología, arquitectura y gobernanza para determinar su confiabilidad e independencia; y

b. Teniendo en cuenta los niveles de garantía de la identidad digital, determinar, en función del riesgo, si el sistema de identidad digital es adecuadamente confiable e independiente a la luz de los posibles riesgos de LA, FT, fraude y otros riesgos de financiamiento ilícito.

140. Dependiendo del sistema de identidad digital y del marco regulatorio en una jurisdicción particular, los gobiernos y los sujetos obligados pueden tener diferentes funciones y responsabilidades en la evaluación de los niveles de garantía de un sistema de identidad y su idoneidad para la DDC, como se refleja en el diagrama de flujo de toma de decisiones para los sujetos obligados, a continuación.

141. El proceso de decisión del diagrama de flujo establece un camino para los sujetos obligados a la hora de decidir si utilizan un sistema de identidad digital para la identificación y verificación de clientes y para la debida diligencia continua. Las dos evaluaciones expuestas anteriormente se reflejan en las preguntas dos y tres, respectivamente.

Figura 4. Proceso de decisión para sujetos obligados



Primera pregunta ¿El sistema de identidad digital está autorizado por el gobierno para su uso en la DDC?

142. De acuerdo con la primera pregunta, cuando el gobierno «respalda» un sistema de identidad digital *y* lo considera apropiado para su uso en la DDC, los sujetos obligados pueden utilizar el sistema de identidad digital sin realizar las evaluaciones de la segunda y tercera pregunta. En efecto, el gobierno ha llevado a cabo los dos pasos de la evaluación recomendada, al menos para los riesgos estándar de DDC, para los sujetos obligados y las partes restantes del proceso de decisión no se aplican. Sin embargo, dependiendo de las leyes ALA/CFT y del ecosistema de identidad digital en la jurisdicción, se puede exigir a los sujetos obligados que tomen medidas adicionales (véanse los párrafos 147 y 148 más abajo).

143. Los gobiernos pueden considerar explícitamente que un sistema de identidad digital es apropiado para su uso en la DDC emitiendo reglamentos o proporcionando directrices a los sujetos obligados, *permitiendo o exigiendo* a los sujetos obligados que utilicen el sistema o sistemas de identidad digital para determinados aspectos de la DDC. La autorización explícita puede ocurrir, por ejemplo, cuando el gobierno desarrolló y opera los sistemas de identidad digital y, por lo tanto, tiene confianza en ellos, o cuando el gobierno tiene un mecanismo para obtener información auditada y certificada sobre los niveles de garantía del sistema de identidad digital de otro proveedor.

144. Los gobiernos también pueden «respaldar» implícitamente un sistema de identidad digital y considerarlo apropiado para que los sujetos obligados lo utilicen en la DDC. Este podría ser el caso, por ejemplo, cuando el gobierno proporciona un sistema de identidad digital de uso general que se utiliza para probar la identidad oficial, siempre que se requiera en la jurisdicción. Los gobiernos deben ser transparentes sobre el funcionamiento de su sistema de identidad digital y sus niveles de garantía pertinentes. Lo mismo ocurre con sus sistemas de identidad de propósito limitado, autorizados para su uso en el sector financiero.

145. Dependiendo de las leyes y normativas nacionales en materia ALA/CFT, los sujetos obligados deberán complementar el uso de los sistemas de identidad digital autorizados en determinadas circunstancias, incluyendo, por ejemplo, las situaciones de mayor riesgo y la recopilación de información sobre otros aspectos de la DDC no contemplados a los objetivos de esta Guía (es decir, la comprensión del objetivo y la naturaleza prevista de la relación comercial). Algunas jurisdicciones pueden tener regulaciones que sólo autorizan el uso de sistemas de identidad digital para situaciones de menor riesgo.

146. Aparte de los requisitos normativos de su jurisdicción, se anima a los sujetos obligados a considerar si deben adoptar medidas adicionales de mitigación del riesgo de la identidad digital (si están disponibles), como puntos de datos de atributos de identidad adicionales o autenticadores adicionales, y/o medidas de mitigación del riesgo de LA/FT, teniendo en cuenta las propias políticas de gestión del riesgo ALA/CFT, antifraude y generales de la institución financiera.

Segunda pregunta: ¿Conoce el nivel de garantía pertinente del sistema de identidad digital?

147. Cuando el gobierno no haya autorizado explícita o implícitamente el uso de sistemas de identidad digital específicos para la DDC, el sujeto obligado debe determinar primero, para cualquier sistema de identidad digital que esté considerando adoptar, los niveles de garantía del sistema. [41]

148. Si el gobierno asegura, audita o certifica los sistemas de identidad digital (ya sea directamente o designando organizaciones para que actúen en su nombre),[42] los sujetos obligados pueden basarse en estas evaluaciones para responder a la segunda pregunta del proceso de decisión. Del mismo modo, el gobierno también puede aprobar un organismo experto, nacional o extranjero, para probar/auditar y certificar los niveles de garantía de los sistemas de identidad digital en los que pueden confiar los sujetos obligados. Véase en el Anexo D un resumen de algunos de estos organismos expertos. Los sistemas de identidad digital pueden estar certificados como que cumplen un nivel de garantía mínimo, o pueden tener diferentes niveles de garantía cada vez más sólidos (ya sea de forma unitaria o para cada uno de sus componentes), pero la información autorizada debe estar disponible públicamente.

149. Si el gobierno no ha autorizado un sistema de identidad digital para su uso en la DDC, ni ha proporcionado un mecanismo para obtener información autorizada sobre el nivel de garantía de un sistema de identidad digital, los sujetos obligados deben determinar la confiabilidad e independencia del sistema por sí mismos, ya sea:

a. realizando ellos mismos la evaluación de garantía, o

b. utilizando información de auditoría o certificación sobre los niveles de garantía por parte de un organismo experto (aunque no esté oficialmente aprobado por el gobierno).

150. Cuando el sujeto obligado realiza la evaluación de garantía por sí mismo, debe llevar a cabo la debida diligencia sobre el proveedor del sistema de identidad digital, incluidos los sistemas de gobernanza existentes, y actuar con mayor precaución.

151. Un sujeto obligado sólo debe utilizar la información de otro organismo experto si tiene una base razonable para concluir que la entidad aplica con precisión los marcos y normas de garantía de la identidad digital adecuados y divulgados públicamente. Por ejemplo, la entidad puede estar aprobada para fines similares por otro gobierno o puede ser ampliamente reconocida como fiable por los expertos apropiados en la jurisdicción, región o internacionalmente.

---

41 Como se ha expuesto anteriormente en esta Guía, el término «**nivel de garantía**» se refiere al nivel de confianza en la confiabilidad de cada uno de los componentes del proceso de identidad digital.

42 Estas actividades no pueden ser llevadas a cabo por los reguladores ALA/CFT de la jurisdicción, porque la capacidad de determinar si una entidad aplica marcos de garantía y normas técnicas apropiadas y públicamente divulgadas, es probable que resida en otra parte del gobierno. La elección de las autoridades competentes para desempeñar esta función es una cuestión que debe determinar cada jurisdicción. A modo de ejemplo, en Estados Unidos, la Administración de Servicios Generales (GSA) ha aprobado una serie de proveedores de marcos de confianza para certificar los sistemas de identidad para uso gubernamental.

Tercera pregunta: El sistema de identidad digital, ¿es adecuado para situaciones de riesgo de LA/FT?

152. Una vez que el sujeto obligado esté convencido de que conoce los niveles de garantía del sistema de identidad digital (a través de los procesos descritos en la segunda pregunta), debe analizar si el sistema de identidad digital es adecuado, en el contexto de los riesgos de financiamiento ilícito pertinentes, según el enfoque basado en el riesgo del GAFI para la DDC. En otras palabras, dados los niveles de seguridad, ¿es el sistema de identidad digital adecuado para su uso en la identificación/verificación del cliente y en la debida diligencia continua a la luz de los riesgos potenciales de LA/FT asociados al cliente, los productos y servicios, el área geográfica de las operaciones, etc.? Los sujetos obligados deben analizar si, dados sus niveles de garantía, el sistema de identidad digital es adecuado, en el contexto de los riesgos de financiamiento ilícito pertinentes. Dependiendo de los requisitos ALA/CFT de la jurisdicción y de los sistemas de identidad digital disponibles, los sujetos obligados pueden tener la opción de seleccionar entre varios sistemas de identidad digital que tengan diferentes niveles de garantía para la comprobación y autenticación de la identidad. En esta situación, los sujetos obligados deben adecuar la solidez de la prueba de identidad y/o la autenticación del sistema al tipo de actividades ilícitas potenciales y al nivel de riesgos de LA/FT.

153. En algunos países, el gobierno ha estipulado un nivel de garantía exigido (unitario) para situaciones de riesgo de LA/FT estándar o alto. Los sujetos obligados pueden seguir eligiendo dentro de una gama de sistemas de identidad digital con el nivel de garantía requerido, o seleccionar distintos niveles de prueba de identidad y/o credenciales y autenticadores particulares ofrecidos por el mismo sistema. Cuando este sea el caso, deberán considerar las especificidades de sus riesgos de LA/FT en relación con la comprobación y autenticación de la identidad a la hora de decidir la(s) opción(es). Los sujetos obligados también pueden tener la opción de elegir la identidad digital adecuada para los escenarios de menor riesgo (véase también el debate sobre la inclusión financiera más adelante en esta sección).

Aprovechamiento de los marcos y las normas técnicas de garantía de la identidad digital para aplicar el EBR

154. Como se ha comentado anteriormente, los gobiernos (como IDSP y/o como reguladores, supervisores y responsables políticos) y los sujetos obligados (como partes que confían) deben considerar adecuadamente los factores de riesgo de la identidad digital y los niveles de garantía, en relación con los factores de riesgo de LA/FT pertinentes y las medidas de mitigación ALA/CFT. Como se explica con más detalle a continuación, los **marcos y normas de garantía de la identidad digital** proporcionan una herramienta útil para llevar a cabo esta evaluación.

155. Por lo tanto, se anima a los gobiernos y a los sujetos obligados a considerar la información proporcionada por los marcos y normas de garantía al evaluar si un sistema de identidad digital satisface los criterios «fiables e independientes» de la Recomendación 10 (a). También se les anima a considerar la fiabilidad de cada uno de los principales componentes de identidad digital del sistema por separado. Esto se debe a que, en función de los posibles factores de riesgo de LA/FT y de las medidas de mitigación, es posible que no se requiera el mismo grado de confiabilidad para cada uno de los componentes del sistema de identidad digital (prueba de identidad/inscripción, autenticación o, si corresponde, federación).

156. Comprender el nivel de garantía de cada componente del sistema de identidad digital puede ayudar a los sujetos obligados a adoptar un enfoque de la DDC más adaptado al riesgo cuando confíen en la identidad digital. El **enfoque proceso por proceso para evaluar la garantía** es particularmente relevante en el contexto de la inclusión financiera. Las normas técnicas de GOV.UK Verify y la versión final de las Normas de Identidad Digital NIST 800-63-3 de EE. UU. han adoptado «niveles de garantía» separados para cada uno de los procesos básicos del sistema de identidad.[43] En el caso de los marcos y normas de garantía que adoptan un único nivel de garantía para todo el sistema de identidad digital (como el Reglamento eIDAS), el enfoque proce so por proceso puede aplicarse examinando cómo cada componente del proceso cumple los requisitos de cada nivel de garantía.

157. La tecnología y la arquitectura de la identidad digital, así como los marcos y normas de garantía de la identidad digital, son dinámicos y están en evolución.[44] Las propias normas son flexibles y se basan en los resultados para facilitar la innovación. Permiten que diferentes tecnologías y arquitecturas satisfagan los requisitos de los distintos niveles de garantía en la actualidad, y se enmarcan en formas que pretenden ayudar a que se preparen lo más posible para el futuro. Las jurisdicciones deben evitar la adopción de un enfoque fijo y prescriptivo que bloquee los requisitos del nivel de garantía actual como un techo, en lugar de un suelo, para la fiabilidad.

Utilización de normas y marcos de garantía de la identidad digital

158. Los marcos y normas de garantía de la identidad digital suelen establecer varios niveles de garantía, progresivamente más confiables, con requisitos técnicos cada vez más rigurosos, para cada uno de los tres pasos principales de un sistema de identidad digital.

159. Al igual que la Nota Interpretativa de la Recomendación 10 proporciona ejemplos de factores de mayor y menor riesgo de LA/FT, las normas técnicas proporcionan factores de confiabilidad de la identidad, en forma de niveles de garantía para los procesos constitutivos básicos de un sistema de identidad digital. Cada nivel de garantía refleja un nivel específico de certeza o confianza en el proceso en cuestión. Un proceso con un nivel de garantía más alto es más confiable; un proceso con un nivel de garantía más bajo presenta un mayor riesgo de fracaso y es menos confiable. Las autoridades y los sujetos obligados pueden utilizar los niveles de garantía para evaluar la confiabilidad de un determinado sistema de identidad digital. Esta Guía no exige ni recomienda ningún nivel de seguridad en particular.

160. Algunas normas técnicas apoyan una evaluación de la fiabilidad proceso por proceso, y contemplan que diferentes procesos de identidad digital pueden, aunque no necesariamente, estar todos al mismo nivel de garantía (AL). Más fundamentalmente, el EBR requiere que se determine qué niveles de garantía para qué procesos son apropiados, dados los riesgos de LA, FT, fraude y otros riesgos de financiamiento ilícito. Incluso con marcos que asignan un único nivel de garantía, las entidades pueden examinar cómo cada componente del proceso cumple los requisitos individuales de cada nivel de garantía.

---

43 Por ejemplo, según las Normas del NIST, hay niveles de garantía (1-3) para cada una de las etapas del proceso de identidad digital: Nivel de garantía de la identidad (IAL); nivel de garantía de la gestión del ciclo de vida de la autenticación y las credenciales (ALA); y nivel de garantía de la federación (FAL).

44 Hay que reconocer que las normas de identidad digital no siempre han estado a la altura de de la evolución de la tecnología. Por ejemplo, en el momento de finalizar esta Guía, los marcos y normas de garantía de la identidad digital aún no abordaban la autenticación continua. Tampoco abordaban la noción de identidad progresiva en lo que respecta a la comprobación continua y dinámica de la identidad.

161. Para ilustrar tanto el tipo de factores que las autoridades competentes, las instituciones financieras y otras partes interesadas podrían aprovechar para evaluar si la identidad digital es confiable e independiente, como la flexibilidad que permiten los marcos y normas de garantía de la identidad digital, el ***Anexo E: Visión general de los marcos y las normas técnicas de garantía de la identidad digital de EE. UU. y la UE*** establece, a modo de ejemplo, los niveles de garantía de EE. UU. y la UE. Describe a grandes rasgos algunos de los requisitos técnicos para la comprobación de la identidad (la primera fase de un sistema de identidad digital). También señala brevemente algunas de las consideraciones clave asociadas a los niveles de garantía de la autenticación.

Consideraciones especiales para la inclusión financiera

La relación de la gestión del riesgo de la identidad digital con el EBR ALA/CFT y las medidas de mitigación del riesgo de LA/FT

162. Idealmente, la adopción de sistemas de identidad digital permitirá a las personas demostrar su identidad oficial con mayores niveles de garantía, especialmente en los países que aún no proporcionan una identidad oficial sólida a la mayoría de la población. Sin embargo, como la identidad digital suele basarse en pruebas de identidad documentales, en los países en los que la cobertura de un sistema de identidad oficial es escasa, es posible que parte de la población siga sin poder obtener una identidad digital con niveles de garantía más elevados debido a las dificultades para acreditar la identidad.

163. Como se ha destacado anteriormente en este documento, las jurisdicciones que se enfrentan a retos de inclusión financiera deben adoptar un enfoque flexible a la hora de establecer los atributos de identidad requeridos, las pruebas y los procesos para demostrar la identidad oficial. Esto garantizará que las personas financieramente excluidas puedan ser captadas bajo los requisitos de prueba de identidad (por ejemplo, haciendo que una dirección residencial permanente sea un atributo opcional y permitiendo que personas de confianza den fe de la identidad de una persona). Como parte de iniciativas internacionales, gubernamentales o de ONG más amplias para abordar estas cuestiones, incluso aumentando el acceso a las pruebas de identidad, las autoridades ALA/CFT y los sujetos obligados deben considerar cómo se aplica un enfoque basado en el riesgo a la DDC en relación con los sistemas de identidad digital, particularmente en jurisdicciones o dentro de poblaciones particulares donde la exclusión financiera se ha identificado como un riesgo de LA/FT.

164. En 2017, el GAFI publicó un suplemento de la Guía sobre medidas ALA/CFT e inclusión financiera de 2013, centrado específicamente en la DDC y la inclusión financiera.[45] El documento destaca las medidas de mitigación de riesgos que los sujetos obligados deben aplicar, en consonancia con la naturaleza y el nivel de los riesgos identificados. También presenta diferentes enfoques de DDC que pueden eliminar los obstáculos a la inclusión financiera relacionados con la verificación de la identidad del cliente, como una amplia comprensión de la fuente de información confiable e independiente, o medidas simplificadas de debida diligencia. La Guía señala que, en varios países, la expansión de los servicios financieros digitales se ha apoyado en un enfoque escalonado de la DDC. En virtud de este

45 GAFI (2013-2017), Medidas anti-lavado de activos y contra el financiamiento del terrorismo e inclusión financiera - Con complemento sobre debida diligencia del cliente, GAFI, París www.fatf- gafi.org/publications/financialinclusion/documents/financial-inclusion-cdd-2017.html

enfoque, por ejemplo, a una persona anteriormente excluida o desatendida se le proporciona una cuenta con mitigadores de riesgo ALA/CFT incorporados, como limitaciones en el valor total de la cuenta y/o el valor y el número de transacciones dentro de un marco de tiempo especificado, y la verificación de la identidad del cliente se retrasa hasta que se alcancen umbrales específicos.

165. La aplicación de las lecciones de la Guía de Inclusión Financiera de 2017 al uso de sistemas de identidad digital significa que, cuando los riesgos de LA/FT de la admisión de un cliente potencial determinado son menores, puede ser apropiado un sistema de identidad digital con un nivel de garantía menor para la comprobación de la identidad. Es posible que se requieran medidas adicionales para garantizar la mitigación del riesgo de LA/FT, incluyendo, por ejemplo, la imposición de restricciones al uso de la cuenta, como se ha descrito anteriormente. Del mismo modo, cuando los riesgos de financiamiento ilícito asociados con el acceso no autorizado a la cuenta son más altos (por ejemplo, debido a la prevalencia de nombres de usuario y contraseñas robadas en una jurisdicción), pero el cliente es de bajo riesgo, se puede utilizar un sistema de identidad digital con un nivel de garantía más bajo para la prueba de identidad (para la identificación/verificación del cliente en la admisión), pero una mayor garantía para su componente de autenticación para evitar que la cuenta sea utilizada por una persona no autorizada. La autenticación de la identidad del cliente para autorizar el acceso a la cuenta para realizar transacciones, incluso en el caso de las cuentas de bajo valor, es importante para combatir las transferencias fraudulentas y asegurarse de que no se eluden los requisitos de valor, velocidad y volumen de la DDC.

166. La posibilidad de adoptar un enfoque flexible para el uso de sistemas de identidad digital en el marco de las normas del GAFI tiene importantes implicaciones para la inclusión financiera. Puede facilitar la aplicación de la DDC escalonada y la verificación de identidad retardada, ya que, en virtud de los marcos y normas de garantía de la identidad digital, los sistemas de identidad digital con un nivel de garantía más bajo para la comprobación/inscripción de la identidad requieren pruebas de identidad d menos estrictas o la verificación de la identidad de la persona (véase el Anexo E). Esto significa que una persona anteriormente excluida o desatendida (que carece de ciertos documentos para demostrar su identidad oficial para la admisión) puede inscribirse en un sistema de identidad digital. El individuo puede entonces utilizar los autenticadores de la identidad digital para la identificación del cliente y abrir una cuenta sin verificación, sujeto a controles y umbrales específicos.

167. Además, los sistemas de identidad digital pueden permitir a las personas anteriormente desatendidas o excluidas desarrollar con el tiempo una huella digital más sólida y un perfil de riesgo que les permita acceder a una gama más amplia de servicios financieros. Dependiendo del enfoque de la jurisdicción sobre los requisitos para demostrar la identidad oficial, los sistemas de identidad digital pueden transformar potencialmente el concepto de identidad oficial en sí mismo, de algo que es fijo a algo que puede fortalecerse con el tiempo, es decir, la identidad progresiva. Con la identidad progresiva, a medida que un individuo (por ej., el cliente) se involucra en actividades financieras digitales y otras actividades en línea y construye una presencia digital, los atributos de identidad adicionales y los factores de autenticación están disponibles y pueden fortalecer la identidad digital del individuo, aumentando así el nivel de confianza en la identidad de un cliente.

168. La identidad progresiva apoya la inclusión financiera, incluso cuando los sistemas de identidad digital no son interoperables y la identidad digital no es portátil, porque permite a un sujeto obligado concreto conocer mejor al cliente individual y crear confianza en la relación comercial para proporcionar una gama más amplia de servicios financieros.

Sin embargo, su valor se incrementa en gran medida, incluso con fines de inclusión financiera, cuando la identidad progresiva es portátil, ya que permite que la identidad más sólida creada por los patrones de comportamiento del individuo, los datos de las transacciones y la información de autenticación asociada recopilada por un sujeto obligado viaje con el individuo y se utilice para la identificación/verificación del cliente en un sujeto obligado no relacionado. En ausencia de la portabilidad, los clientes tendrían que restablecer su identidad progresiva en cada sujeto obligado durante un periodo de tiempo, durante el cual sólo podrían acceder a productos y servicios de bajo valor/bajo riesgo.

Cuadro 3. Ilustración de cómo el uso de la identidad digital en la DDC escalonada y progresiva puede apoyar la inclusión financiera

Un individuo financieramente excluido solicita una cuenta bancaria básica, utilizando una identidad digital obtenida sin presentar pruebas de identidad. La identidad digital tiene un nivel de garantía más bajo para la prueba de identidad, pero un nivel de garantía de autenticación que proporciona la confianza de que el solicitante controla el autentificador vinculado a la persona identificada.

El sujeto obligado incorpora al cliente y le proporciona una cuenta bancaria de bajo riesgo, con un umbral muy bajo de valor, volumen de transacciones y velocidad y sin transacciones transfronterizas (estas medidas de mitigación del riesgo se basan en el análisis de riesgos). El cliente utiliza esta cuenta para obtener un teléfono móvil en virtud de un contrato y recibe pagos de salarios digitales directamente en la cuenta bancaria, entre otras actividades.

El sujeto obligado utiliza los datos relacionados con el depósito directo de los salarios, las transferencias sociales o las prestaciones, para verificar el empleo, la ocupación y el origen de los fondos, así como los pagos regulares de la cuenta para el teléfono móvil y los servicios públicos para establecer un patrón de comportamiento financiero responsable. El sujeto obligado también recoge otra información sobre transacciones y autenticación asociada para verificar la dirección del cliente. Con el tiempo, el sujeto obligado utiliza las actividades financieras constantes del cliente y los patrones de comportamiento (por ej., horarios de las transacciones, importes típicos, propósitos/contrapartes y geolocalización) para reforzar la autenticación para el acceso a la cuenta y las medidas antifraude.

El marco jurídico de la jurisdicción en materia ALA/CFT se basa en los principios, el rendimiento y los resultados. Sus normas de identificación/verificación de clientes exigen que los sujetos obligados tengan una base razonable para creer que saben quiénes son sus clientes, pero no prescriben de forma rígida cómo deben lograr este objetivo. El sujeto obligado trata los datos generados por las actividades del cliente a lo largo del tiempo como pruebas de identidad y los utiliza para generar confianza en que sabe quién es su cliente y su perfil de riesgo. Cuando esa confianza satisface al sujeto obligado de que ha cumplido con sus obligaciones de identificación/verificación del cliente y ha satisfecho su propio apetito de riesgo y sus prácticas y procedimientos de gestión del riesgo para otros servicios financieros, el sujeto obligado ofrece una cuenta bancaria estándar con umbrales más altos y mayor funcionalidad y, más tarde, concede un pequeño préstamo, que el cliente utiliza para iniciar un negocio.

Este enfoque para la identidad digital refleja el mismo proceso que se establece en la Guía sobre DDC e inclusión financiera de 2017 del GAFI, donde las personas sin documentos de identidad adecuados pueden someterse a una DDC escalonada y ampliar progresivamente su nivel de acceso a los servicios financieros, comenzando por una forma de cuenta restringida y de bajo riesgo.

Fuente: Tesoro de Estados Unidos

Las normas y marcos de identidad digital pueden favorecer la inclusión financiera

Árbitros de confianza

169. Un ejemplo, en el que algunos marcos y normas de garantía de la identidad digital dan cabida a quienes carecen de pruebas de identidad tradicionales, es permitir el uso de árbitros de confianza, como alcaldes, autoridades del gobierno local, jueces/magistrados, empleadores; personas con buena reputación en la comunidad (por ej., empresarios, abogados, notarios); o alguna otra forma de persona capacitada y aprobada o certificada, para responder por el solicitante como forma de prueba de identidad,[46] de acuerdo con las leyes, reglamentos o políticas de la agencia aplicables de la jurisdicción.

170. Por ejemplo, según el NIST, el uso de árbitros de confianza requiere que el IDSP:

- Establezca políticas y procedimientos por escrito, que aborden cómo se determina un árbitro de confianza (criterios de selección) y el ciclo de vida del estatus del árbitro de confianza como árbitro válido, para incluir cualquier restricción, revocación y requisitos de suspensión;
- Acredite la identidad del árbitro de confianza al mismo nivel que el solicitante, y determinar las pruebas de identidad mínimas necesarias para establecer la relación entre el árbitro de confianza y el solicitante.

Pruebas de identidad a distancia y admisión no presencial

171. Como se ha señalado anteriormente, los sistemas de identidad digital pueden permitir la identificación/verificación de clientes a distancia y apoyar las transacciones financieras a distancia con niveles de riesgo estándar o incluso bajos. Las normas técnicas permiten la comprobación e inscripción de la identidad a distancia, incluso con niveles de garantía más elevados. Véase el Anexo E.

46 NIST 800-63A 4.4.2. IAL2 Requisitos de comprobación de árbitros de confianza.

ANEXO A: DESCRIPCIÓN DE UN SISTEMA DE IDENTIDAD DIGITAL BÁSICO Y SUS PARTICIPANTES

Este Anexo ofrece una explicación más detallada de los componentes básicos de un sistema de identidad digital genérico, ampliando el breve resumen expuesto en la Sección II. La descripción se presenta con un alto nivel de generalidad. Proporciona algunos ejemplos de tecnología o proceso que pueden aplicarse sólo con fines ilustrativos para el lector; no fomenta ni aprueba el uso de ninguna tecnología, arquitectura o proceso de identidad en particular, como la biometría o la tecnología de telefonía móvil. Por lo tanto, se aplica a una amplia gama de sistemas de identidad digital. Este Anexo se centra en los dos primeros componentes de un sistema de identidad digital, porque son los más directamente relevantes para la aplicación de los requisitos de la Recomendación 10 para la identificación/verificación del cliente en el momento de la incorporación y para la autenticación de la identidad del cliente para el acceso a la cuenta. Este Anexo se ofrece para proporcionar un contexto y no pretende estipular los requisitos técnicos u organizativos para una identidad digital elegible en el marco ALA/CFT.

Resumen del proceso de identidad digital

Como se refleja en las normas de identidad digital del NIST, el proceso de identidad digital incluye dos componentes básicos y un tercer componente opcional:

> **Primer componente: Comprobación e inscripción de la identidad (con vinculación/credencialización inicial)** (esencial)
>
> **Segundo componente: Autenticación y gestión del ciclo de vida de la identidad** (esencial); y
>
> **Tercer componente: Mecanismos de portabilidad e interoperabilidad** (opcional).

La comprobación e inscripción de la identidad pueden ser digitales o documentales, y presenciales (en persona) o no presenciales (a distancia).[47] En un sistema de identidad digital, la vinculación/credencialización, la autenticación y la portabilidad/federación son siempre, y necesariamente, digitales.

La terminología utilizada por las distintas jurisdicciones y organizaciones puede diferir ligeramente según el sistema que se describa. A continuación se incluye una descripción más detallada de cada una de las etapas.

Componente 1: Comprobación e inscripción de la identidad

La comprobación e inscripción de la identidad (con la vinculación/credencialización inicial) constituyen la primera etapa de un sistema de identidad digital.

La **comprobación de la identidad** responde a la pregunta «¿Quién es usted?» y se refiere al proceso por el cual un proveedor de servicios de identidad (IDSP) recoge, valida y verifica la información sobre una persona y la resuelve a un individuo único dentro de una población o contexto determinado.

47 Véase una explicación más detallada de estos términos en la Guía.

A continuación se describe el flujo del proceso de comprobación de la identidad en tres acciones: (1) recopilación/resolución, (2) validación, y (3) verificación.

- ***(1) La recopilación y resolución*** implica la obtención de atributos, la recopilación de pruebas de atributos y la resolución de las pruebas de identidad y los atributos a una única identidad dentro de una población o contexto determinado. El proceso de resolver las pruebas de identidad y los atributos a una única identidad dentro de una población o contexto(s) determinado(s) se denomina **desduplicación**. Algunas soluciones de identidad digital proporcionadas por el gobierno incluyen un proceso de desduplicación como parte de la comprobación de la identidad, que puede implicar la comprobación de atributos biográficos específicos del solicitante (por ej., nombre, edad y sexo); datos biométricos (por ej., huellas dactilares, escaneos del iris o imágenes de reconocimiento facial); y atributos asignados por el gobierno (por ej., números de licencia de conducir y/o pasaporte o número de identificación del contribuyente) contra la base de datos del sistema de identidad de las personas inscritas y sus atributos y pruebas de identidad asociados para evitar la duplicación de la inscripción.
  - Las **pruebas de atributos** pueden ser físicas (documentales) o puramente digitales, o una representación digital de pruebas de atributos físicos (por ej., una representación digital de un permiso de conducir de papel o plástico). Tradicionalmente, las pruebas de identidad han adoptado una forma física, como (en el caso de las personas físicas) un documento emitido por el gobierno (preferiblemente, para mayor fiabilidad, con una fotografía y un holograma o garantías similares), por ej., un certificado de nacimiento, un documento nacional de identidad, un permiso de conducir o un pasaporte. Además, tradicionalmente, las pruebas documentales de identidad han sido presentadas físicamente por el solicitante al IDSP. Con el desarrollo de la tecnología digital, las pruebas de identidad pueden ahora generarse digitalmente (o convertirse de forma física a digital) y almacenarse en bases de datos electrónicas, lo que permite que las pruebas de identidad se *obtengan a distancia* y/o que los atributos de identidad y otra información *se verifiquen y validen a distancia en una base de datos digital.*
  - Los atributos también pueden ser inherentes, es decir, basados en las características biométricas personales (biológicas o de comportamiento) de un individuo.[48] La biometría ha evolucionado rápidamente, pasando de ser estática a dinámica, dando lugar a distintos tipos de tecnología de identidad biométrica, con distintos riesgos de fiabilidad y privacidad. Por orden de madurez tecnológica y escala de adopción comercial, así como por la gravedad de las posibles amenazas a la privacidad, los sistemas de identidad digital pueden incluir el uso de:
    - Atributos biométricos físicos, como huellas dactilares, patrones de iris, huellas vocales y reconocimiento facial, todos ellos estáticos.
    - Atributos biométricos biomecánicos, como la mecánica de las pulsaciones de las teclas, que son el producto de interacciones únicas de los músculos, el sistema esquelético y el sistema nervioso de un individuo, todos ellos dinámicos.

48 Es importante distinguir el uso de la biometría como atributos de identidad de la biometría para la identificación o desduplicación (es decir, como se utiliza para establecer la identidad y la singularidad de un individuo) frente a su uso como autentificadores. Las normas técnicas de identidad digital (por ej., las normas del NIST) sólo admiten un uso limitado de la biometría con fines de autenticación e imponen requisitos y directrices rigurosos para este uso con el fin de abordar una serie de preocupaciones.

  - Los atributos biométricos de comportamiento, basados en la nueva disciplina de ciencias sociales computacionales de la física social, consisten en los diversos patrones de movimiento y uso de un individuo en *flujos de datos temporales geoespaciales*, e incluyen, por ejemplo, los patrones de correo electrónico o mensajes de texto de un individuo, el uso del teléfono móvil, los patrones de geolocalización y el registro de acceso a archivos (incluidos los canales de inicio de sesión previstos, la geolocalización, el momento; la frecuencia y el tipo de uso (revisión del saldo de la cuenta y la actividad frente a la transacción).49

- Los atributos de identidad oficial requeridos (básicos) varían según la jurisdicción, pero podrían incluir: nombre oficial completo; fecha de nacimiento; lugar de nacimiento; domicilio y un número de identidad único emitido por el gobierno. Sin embargo, los gobiernos tienen una flexibilidad considerable a la hora de determinar los atributos y las pruebas necesarias para demostrar la identidad oficial en la jurisdicción. El enfoque de un gobierno para determinar los atributos de identidad requeridos puede cambiar con el tiempo, con la evolución de la tecnología y la correspondiente confianza en la fiabilidad de los diversos tipos de atributos de identidad.50 Además, los gobiernos pueden considerar el contexto del país y los objetivos de inclusión financiera al establecer los atributos de identidad requeridos. Por ejemplo, especialmente en los países en vías de desarrollo con una importante población itinerante o sin hogar y con personas que no tienen una dirección formal, el gobierno puede decidir no exigir la dirección como identificador principal para demostrar la identidad oficial.

- ***(2) La validación*** consiste en determinar que las pruebas son auténticas (no son falsas, ni falsificadas, ni malversadas) y que la información que contienen es exacta, cotejando la información/prueba de identidad con una fuente aceptable (autorizada/confiable) para establecer que la información coincide con datos/registros de fuentes fiables e independientes. Por ejemplo, el IDSP podría (1) comprobar las pruebas físicas de identidad (documento de identidad), como el permiso de conducir y/o el pasaporte, o las imágenes digitales de las pruebas físicas de identidad del solicitante, y (a) determinar que no hay alteraciones; los números de identificación siguen formatos estándar; y los elementos de seguridad físicos y digitales son válidos e intactos; y (b) consultar a las fuentes gubernamentales emisoras del permiso y/o el pasaporte y validar (confirmar) que la información coincide.

- ***(3) La verificación*** consiste en confirmar que la identidad validada corresponde a la persona (solicitante) cuya identidad se está comprobando. Por ejemplo, el IDSP podría pedir al solicitante que tome y envíe un vídeo o una foto de teléfono móvil con otras comprobaciones de vida; comparar la foto enviada por el solicitante con las fotos de la prueba de identidad del pasaporte o la foto archivada en la base de datos de pasaportes o licencias del gobierno; y determinar que coinciden con un determinado nivel de certeza. Para vincular esta prueba de identidad con el solicitan-

49 Véase D. Shrier, T. Hardjono y A. Pentland, «Biometría del comportamiento» (*Behavioral Biometrics*), capítulo 12, Nuevas soluciones de ciberseguridad (*New Solutions for Cybersecurity*) (ed. de H. Shrobe; D. Shrier; y A. Pentland (MIT Connection Science and Engineering, MIT Press 2017).

50 Por ejemplo, la evolución de la tecnología de la interfaz persona-ordenador (HCI) (por ejemplo, combinando el movimiento de los ojos y el uso del ratón) o las interfaces hápticas pueden llevar a algunos gobiernos a sustituir eventualmente la dependencia de los identificadores tradicionales por la dependencia de los atributos biomecánicos. Véase en la Sección V un análisis de la evolución del papel de los atributos biométricos del comportamiento en la identificación/verificación y autenticación digitales.

te real, el IDSP podría enviar un código de inscripción al número de teléfono validado del solicitante que está vinculado a la identidad; pedir al solicitante que proporcione el código de inscripción al IDSP; y confirmar que el código de inscripción enviado coincide con el código que el IDSP envió, verificando que el solicitante es una persona real, en posesión y control del número de teléfono validado. En este punto, se ha comprobado la identidad del solicitante.

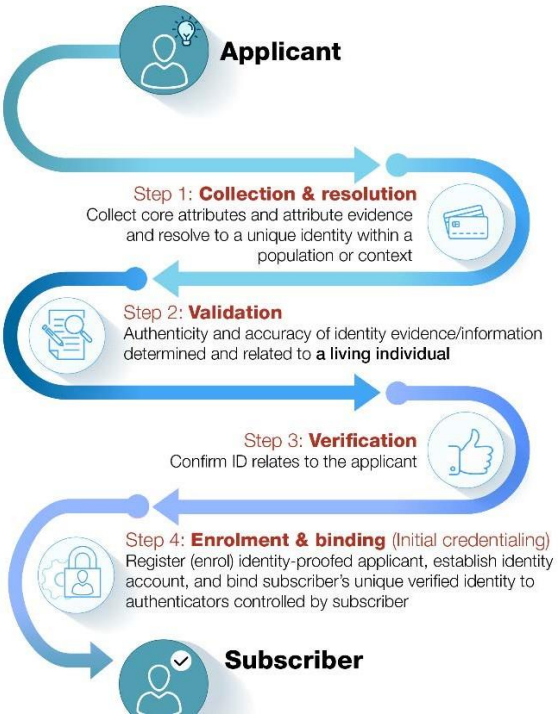
La **inscripción** es el proceso por el cual un IDSP registra (inscribe) a un solicitante con prueba de identidad como «abonado» y establece su cuenta de identidad. Este proceso vincula de forma autorizada la identidad única verificada del abonado(es decir, los atributos del abonado) a uno o varios autenticadores que posee y controla el abonado, utilizando un protocolo de **vinculación** adecuado. El proceso de vinculación de la identidad del abonado con el autenticador o autenticadores también se denomina «credencialización».

Un **autenticador** es algo que el solicitante posee y controla, normalmente un módulo criptográfico, un generador de códigos de una sola vez o una contraseña, que se utiliza para autenticar (confirmar) al solicitante. Más concretamente, un **autenticador** es algo que el demandante posee y controla y que se utiliza para autenticar (confirmar) que el demandante es la persona a la que se le ha expedido una credencial y, por tanto, (en función de la solidez del componente de autenticación del sistema de identidad digital) es (con distintos grados de probabilidad, especificados por el nivel de garantía de autenticación) el abonado real y el titular de la cuenta. Una **credencial** es un objeto físico o una estructura digital que vincula de forma autorizada la identidad probada de un abonado, a través de un identificador o identificadores, con al menos un autentificador que posee y controla el abonado. Cuando un IDSP digital (que actúa como proveedor de servicios de credenciales (CSP)) emite el o los autenticadores y los vincula de forma autorizada a la identidad del abonado, el objeto físico o la estructura digital resultante es una credencial.

Normalmente, el IDSP emite el o los autenticadores al abonado y los registra de forma que los vincula a la identidad probada del abonado en el momento de la inscripción. Sin embargo, el IDSP también puede vincular la cuenta del abonado a autenticadores proporcionados por el abonado que sean aceptables para el IDSP (que actúa como CSP). Además, aunque la vinculación es una parte esencial de la inscripción de confianza, el IDSP también puede vincular las credenciales de un abonado a autenticadores adicionales o alternativos en un momento posterior, como parte de la gestión del ciclo de vida de la identidad, que se analiza más adelante.

La comprobación de la identidad puede ser realizada por un único proveedor de servicios o por varios (véase el resumen de los participantes en el sistema de identidad digital, más adelante). En el primer caso, es posible que una sola entidad, proceso, técnica o tecnología lleve a cabo cada uno de los procesos de comprobación de la identidad. Del mismo modo, la vinculación de la identidad probada durante el registro puede ser llevada a cabo por un único proveedor de servicios o por un proveedor de servicios independiente que no realice también la prueba de identidad.

Figura 5. Comprobación e inscripción de la identidad



Componente 2: Autenticación

La autenticación responde a la pregunta: ***«¿Es usted el individuo identificado/verificado?»*** Establece que el individuo que busca acceder a una cuenta (u otros servicios o recursos), el solicitante, es la misma persona a la que se le ha comprobado la identidad, se ha inscrito y se le han otorgado credenciales, y que tiene la posesión y el control de las credenciales vinculantes y otros autenticadores, si es el caso (por ej., es el cliente admitido). La autenticación puede basarse en varios tipos de factores y procesos, como se describe a continuación. La fiabilidad de la autenticación depende del tipo de factores de autenticación utilizados y de la seguridad de los procesos de autenticación.[51]

Factores de autenticación

Tradicionalmente, existen tres categorías básicas de factores de autenticación:

- Factores de conocimiento: Algo que se conoce como: un secreto compartido (por ejemplo, nombre de usuario, contraseña o frase de contraseña), un número de identificación personal (PIN) o una respuesta a una pregunta de seguridad preseleccionada.
- Factores de propiedad: Algo que se tiene, como: claves criptográficas almacenadas en hardware (por ejemplo, en un teléfono móvil, una tableta, un ordenador o un dispositivo USB) o en software que el abonado controla; una contraseña de un solo uso (OTP) generada en un dispositivo de hardware; o un generador de OTP de soft-

51 Cuando la Guía describe los componentes de la autenticación, éstos no son los mismos que la «autenticación reforzada de clientes (ARC)» según el marco legal de la UE. Lo que constituye o no constituye un factor ARC válido a los efectos de la PSDII debe ser evaluado de conformidad con la PSDII y las RTS sobre SCA+ CSC, en lugar de la guía del GAFI.

ware instalado en un dispositivo digital, como un teléfono móvil.

- Factores de inherencia: Algo que se es (biometría biofísica, como el reconocimiento facial y la biometría de huellas dactilares o de patrones de retina; biometría biomecánica, basada en la forma única en que un individuo interactúa con los dispositivos digitales, como la forma en que el individuo sostiene el teléfono móvil, desliza la pantalla, la cadencia del teclado o utiliza ciertos atajos de teclado o gestuales; y biometría conductual avanzada).

Como se explica más adelante, un sistema de identidad digital determinado no utilizará necesariamente cada uno de estos tipos de factores. Por ejemplo, aunque muchos de los sistemas de identidad digital actuales utilizan la biometría, no debe suponerse que todos los sistemas de identidad digital lo hagan.

Los factores de autenticación basados en el conocimiento (algo que se sabe) pueden no ser realmente secretos. La autenticación basada en el conocimiento, en la que se pide al solicitante que responda a preguntas que presumiblemente sólo conoce él, no constituye un secreto aceptable para la autenticación digital según las normas del NIST. Del mismo modo, un factor de inherencia biométrico no constituye un secreto, por lo que las normas del NIST permiten el uso de la biometría biofísica para la autenticación sólo cuando está fuertemente vinculada a un autenticador físico.

Es importante destacar que los nuevos tipos de autenticadores de propiedad e inherencia basados en la tecnología (incluidos los autenticadores de dispositivos digitales avanzados, la biometría biomecánica y los **patrones biométricos de comportamiento**), muchos de los cuales han sido o están siendo desarrollados y desplegados principalmente con fines de lucha contra el fraude, tienen un potencial significativo para fortalecer los procesos de autenticación de identidad digital con fines de cumplimiento ALA/CFT. [52]

Tradicionalmente (y como se refleja en las normas de identidad digital del NIST), la autenticación de la identidad digital se lleva a cabo en un momento determinado: cuando el solicitante afirma la identidad del cliente/abonado y solicita autorización para iniciar una interacción digital (sesión en línea) o en persona para acceder a la cuenta del cliente o a otros servicios o recursos financieros. Sin embargo, hoy en día, muchos sujetos obligados, especialmente las grandes instituciones financieras de los países desarrollados, aumentan la autenticación tradicional al inicio de una interacción en línea con soluciones de «autenticación continua» que aprovechan la **biometría biomecánica, los patrones biométricos de comportamiento** y/o el **análisis dinámico del riesgo de las transacciones**. En lugar de basarse en una combinación de algo que el solicitante tiene/sabe/es para establecer al principio de la interacción que el solicitante es el cliente admitido y tiene el control de los autenticadores/credenciales emitidos para ese cliente, la autenticación continua se centra en garantizar que ciertos puntos de datos recogidos a lo largo de una interacción en línea, como la geolocalización, las direcciones MAC e IP, la cadencia de tecleo y el ángulo del dispositivo móvil, coinciden con «lo que debería esperarse» durante toda la sesión.

Las formas de medir el impacto (eficacia) de la tecnología de autenticación continua para mitigar los riesgos de autenticación no han alcanzado la madurez, y las normas técnicas de identidad digital, como la del NIST, no las abordan actualmente. El Reglamento Delegado (UE) 2018/389

52 Como se señala en la propia Guía, los sistemas de identidad digital también presentan riesgos significativos (incluidos los riesgos de privacidad) y oportunidades de abuso (por ej., sesgo o abuso de los derechos humanos), que están fuera del alcance de esta Guía, pero deben abordarse de manera efectiva.

de la Comisión Europea (RTS sobre autenticación reforzada de clientes y comunicación segura) en el marco de la segunda Directiva de Servicios de Pago (PSD2) requiere que todos los proveedores de servicios de pago (PSP) cuenten con mecanismos de supervisión de transacciones que les permitan detectar operaciones de pago no autorizadas o fraudulentas con el fin de implementar los requisitos de ARC en PSD2 (Art. 2 Normas Técnicas de Regulación (RTS)). Además, los PSP que deseen beneficiarse de la exención del «análisis del riesgo de las operaciones» en relación con la ARC en virtud del art. 18 de las RTS deben disponer de mecanismos de supervisión de riesgos en tiempo real de conformidad con el artículo 2 de las RTS y demostrar que sus índices de fraude están por debajo de determinados umbrales definidos en las RTS.[53]

Lo que sigue se aplica a los métodos de autenticación de identidad estáticos y en un solo momento, a los que se refieren las normas del NIST para la identidad digital.

Procesos de autenticación

Los procesos de autenticación se suelen clasificar según el número y el tipo de factores de autenticación que requiere el proceso, entendiendo que cuantos más factores emplee un proceso de autenticación, más sólido y fiable será el sistema de autenticación. A medida que la tecnología y los procesos de autenticación han ido evolucionando, esta noción está siendo revisada y complementada por un enfoque más moderno, basado en los resultados, en el que se asume la autenticación multifactorial, pero la solidez del componente de autenticación no depende de cuántos factores y tipos de factores utiliza, sino más bien de si sus procesos de autenticación son resistentes a la comprensión por parte de ataques comúnmente ejecutados y en evolución, como el *phishing* y los vectores de ataque *man-in-the-middle*. (Este enfoque más holístico y basado en los resultados debería adaptarse mejor a la aparición de la autenticación continua).

Los tipos de protocolos/procesos de autenticación por niveles crecientes de seguridad incluyen:

- La **autenticación de factor único (1FA)** utiliza un solo autenticador para autenticar la identidad de una persona.
- La **autenticación de múltiples factores (MFA)** utiliza dos o más autenticadores independientes de al menos dos categorías de factores de autenticación diferentes (conocimiento/posesión/inherencia) para autenticar la identidad del solicitante. Por ejemplo, cuando un solicitante trata de iniciar sesión en una cuenta bancaria en línea, utilizando un autenticador basado en el conocimiento (por ej., nombre de usuario y contraseña), el solicitante también tendría que introducir un factor de autenticación adicional de una categoría de factor de autenticación diferente para poder acceder con éxito a la cuenta. Para ello, el solicitante podría utilizar un factor de autenticación de propiedad, como una clave privada generada en el autenticador certificado por FIDO integrado en su teléfono móvil. La MFA puede implementarse utilizando múltiples autenticadores que, en combinación, presenten factores de autenticación de diferentes categorías directamente al verificador, o un único autenticador que proporcione más de un tipo de factor, como ocurre cuando un autenticador

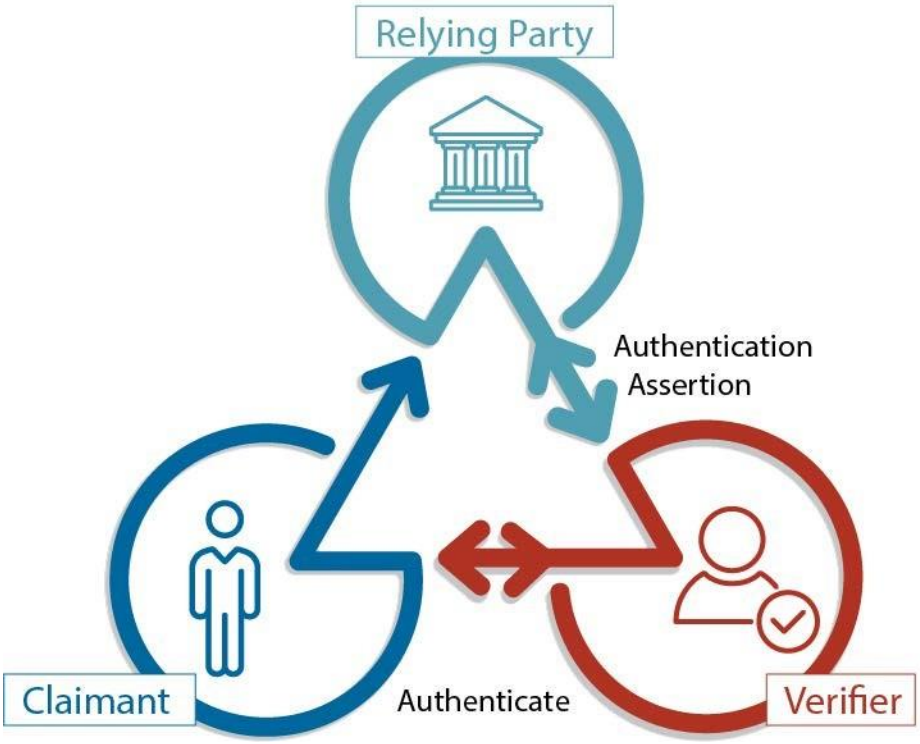
53 El texto de las RTS está disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:3A32018R0389.

utiliza uno o más factores para proteger otro tipo de factor, que a su vez se presenta directamente al verificador. [54]

La figura siguiente ilustra el proceso de autenticación, utilizando el ejemplo de una transacción financiera típica. En este diagrama, un cliente existente quiere iniciar una transacción financiera y primero debe demostrar, mediante uno o varios autenticadores, que es quien dice ser, es decir, que es el propietario de la cuenta. El cliente (solicitante) demuestra su posesión y control de los autenticadores comunicándose con el IDSP (verificador) a través de un protocolo de autenticación seguro. El verificador confirma la validez (verifica) de los autenticadores con el CSP y proporciona una afirmación de autenticación a la institución financiera, que es la RP en el escenario ilustrado. Nota: el CSP, el verificador y la RP pueden ser la misma entidad (autenticación simple y bipartita, compuesta únicamente por el solicitante y la RP).

Figura 6. Autenticación digital

Nota: el CSP, el verificador y la RP pueden ser la misma entidad (autenticación simple y bipartita, compuesta únicamente por el solicitante y la RP).



54 Según las normas del NIST, la autenticación reforzada requiere una autenticación de dos factores o una MFA que utilice dos o más factores de autenticación mutuamente independientes de diferentes tipos, al menos uno de los cuales no sea reutilizable ni replicable y no pueda ser robado subrepticiamente a través de Internet. De acuerdo con la DSP2 de la UE, y como se reitera en las RTS, la «autenticación reforzada de clientes» se define como una «autenticación basada en el uso de dos o más elementos categorizados como conocimiento (algo que sólo el usuario sabe), posesión (algo que sólo el usuario posee) e inherencia (algo que el usuario es) que son independientes, en el sentido de que la vulneración de uno de ellos no compromete la fiabilidad de los demás, y está diseñado de tal manera que protege la confidencialidad de los datos de autenticación». Véase el Anexo E para un análisis más detallado de las normas técnicas.

Tradicionalmente (y como se refleja en las normas del NIST), la autenticación de la identidad digital se lleva a cabo en un momento determinado: cuando el solicitante afirma la identidad y solicita autorización para iniciar una interacción digital (sesión en línea) o en persona para acceder a una cuenta o a otros servicios financieros. Sin embargo, hoy en día, muchos sujetos obligados, especialmente las grandes instituciones financieras de los países desarrollados, aumentan la autenticación tradicional al inicio de una interacción en línea con soluciones de «autenticación continua» que aprovechan la biometría biomecánica, los patrones biométricos de comportamiento y/o el «análisis del riesgo de las transacciones».

Gestión del ciclo de vida de la identidad

La **gestión del ciclo de vida** de la identidad se refiere a las acciones que los IDSP deben tomar en respuesta a los eventos que pueden ocurrir durante el ciclo de vida del autenticador de un abonado y que afectan al uso, la seguridad y la fiabilidad del autenticador. Estos eventos podrían incluir: la emisión y vinculación de autenticadores a credenciales, ya sea en el momento de la inscripción o después de la misma, la pérdida, el robo, la duplicación no autorizada, la caducidad y la revocación de autenticadores y/o credenciales.

Los atributos asociados a una identidad pueden cambiar de un año a otro. Los sistemas de análisis pueden descubrir señales de riesgo que sugieran que una identidad está siendo utilizada de manera consistente con el fraude o el compromiso de la cuenta (como se ha señalado anteriormente, en el análisis de la «autenticación continua»). Algunos sistemas de gestión de identidad comercial están desarrollando capacidades que analizan si una identidad evoluciona y cómo lo hace a lo largo de su ciclo de vida.

A continuación se utiliza el término basado en la función, CSP, para describir las acciones que deben llevarse a cabo en respuesta a un tipo específico de evento del ciclo de vida del autenticador, aunque un único IDSP pueda llevar a cabo la gestión del ciclo de vida del autenticador, así como la comprobación e inscripción de la identidad, y/o la autenticación.

- **Emisión y registro de credenciales:** El CSP emite la credencial y registra y mantiene la credencial y los datos de inscripción asociados en la cuenta de identidad del abonado durante todo el ciclo de vida de la credencial. Normalmente, el abonado posee la credencial, pero el CSP/verificador también puede poseerla. En todos los casos, el abonado posee necesariamente los autenticadores, que, como ya se ha dicho, se utilizan para reclamar una identidad cuando se interactúa con una parte que confía.
- **Vinculación (también conocida como credencialización o emisión de credenciales):** A lo largo del ciclo de vida de la identidad digital, el CSP también debe mantener un registro de todos los autenticadores que están, o han estado, asociados a la cuenta de identidad de cada uno de sus abonados, así como la información necesaria para controlar los intentos de autenticación. Cuando un CSP vincula (es decir, emite credenciales que vinculan) un nuevo autenticador a la cuenta del abonado después de la inscripción, debe exigir al abonado que se autentique primero en el nivel de garantía (o superior) en el que se utilizará el nuevo autenticador.
- **Autenticadores comprometidos: pérdida, robo, daños, duplicación no autorizada:** Si un abonado pierde (o experimenta el compromiso de) todos los autenticadores de un factor requerido para la MFA, y se ha probado la identidad en IAL2 o IAL3, el abonado debe repetir el proceso de prueba de identidad, confirmando la vinculación del solicitante de la autenticación con la evidencia previamente probada antes de que el CSP vincule un sustituto del autenticador perdido a la identidad/cuenta del abonado. Si el abonado tiene MFA y pierde un autenticador, el CSP debe exigir al solicitante que se autentique, utilizando los factores de autenticación restantes.
- **Caducidad y renovación:** Los CSP pueden emitir autenticadores que caducan y ya

no son utilizables para la autenticación. El CSP debe vincular un autenticador actualizado antes de que caduque un autenticador existente, utilizando un proceso que se ajuste al proceso y protocolo de vinculación del autenticador inicial, y luego revocar el autenticador que caduca.

- **Revocación (también conocida como terminación):** Los CSP deben revocar rápidamente la vinculación de los autenticadores cuando una identidad deja de existir (por ej., porque el abonado ha fallecido o se descubre que es fraudulento); cuando lo solicite el abonado; o cuando el CSP determine que el abonado ya no cumple sus requisitos de elegibilidad.

Tercer componente: Mecanismos de portabilidad e interoperabilidad (opcional)

Los sistemas de identidad digital pueden, aunque no es necesario, incluir un componente que permita la portabilidad de la prueba de identidad oficial. La portabilidad de la identidad significa que las credenciales de identidad digital de un individuo pueden ser utilizadas para acreditar la identidad oficial para nuevas relaciones con clientes en entidades del sector privado o gubernamentales no relacionadas, sin que tengan que obtener y verificar información personal identificable (PII) y llevar a cabo la identificación/verificación del cliente cada vez. La portabilidad requiere el desarrollo de productos, sistemas y procesos de identificación digital interoperables. La portabilidad/interoperabilidad puede apoyarse en diferentes arquitecturas y protocolos de identidad digital.

La federación es una forma de permitir la portabilidad de la identidad oficial. La federación se refiere al uso de una arquitectura digital federada y de protocolos de afirmación para transmitir información de identidad y autenticación a través de un conjunto de sistemas en red. La arquitectura de identidad federada proporciona interoperabilidad a través de redes separadas, es decir, proporciona la infraestructura que une sistemas separados en una red interoperable. Las API que no utilizan la arquitectura federada y los protocolos de afirmación son otra forma de lograr la portabilidad.

En varias jurisdicciones también se están desarrollando y adoptando la arquitectura y los protocolos de identidad digital federados para permitir la interoperabilidad y la portabilidad de la identidad en muchos sistemas de identidad de propósito limitado a nivel nacional.

La federación de confianza y otros enfoques para permitir la portabilidad de los sistemas de identidad digital del sector privado podrían proporcionar muchos beneficios significativos. Por ejemplo, la portabilidad/interoperabilidad podría ahorrar a las partes que confían (por ej., instituciones financieras y entidades gubernamentales) tiempo y recursos en la identificación, verificación y gestión de las identidades de los clientes, incluso para la apertura de cuentas y la autorización de acceso a las mismas. Las soluciones de portabilidad basadas en la federación o en la API también podrían ahorrar a los clientes la molestia de tener que demostrar su identidad ante cada institución financiera o servicio gubernamental no relacionado, y reducir el riesgo de robo de identidad derivado de la exposición repetida de la PII.

Por ejemplo, el marco de interoperabilidad del Reglamento eIDAS garantiza la cooperación transfronteriza y la interoperabilidad de los sistemas nacionales de identidad digital. La infraestructura de interoperabilidad establecida por el marco eIDAS creó interfaces técnicas basadas en nodos eIDAS que desempeñan un papel central en la interconexión entre las partes que confían y los diferentes sistemas nacionales de identidad digital conectados a los nodos.

Participantes en un sistema de identidad digital

Como se ha señalado anteriormente, los sistemas de identidad digital pueden implicar diferentes modelos operativos, con diferentes funciones para el gobierno y el sector privado en el desarrollo y el funcionamiento del sistema y/o el suministro de componentes o subcomponentes o procesos específicos.

La siguiente tabla describe los participantes básicos y sus funciones en un sistema de identidad digital genérico. Aunque la tabla describe cada tipo de participante por su función específica, debe entenderse que en los sistemas de identidad digital de propósito general o limitado proporcionados por el gobierno, éste realiza directamente (o hace que otra(s) entidad(es) realice(n) en su nombre) todas las funciones fundamentales de proveedor/operador. Del mismo modo, en los sistemas de identidad digital del sector privado, una sola entidad o varias pueden desempeñar todas o algunas de las funciones de proveedor/operador.

Tabla 2. Participantes en sistemas de identidad digital

PROVEEDORES DE SERVICIOS DE IDENTIDAD	
Proveedor de servicios de identidad (IDSP)	Término genérico que se refiere a todos los diversos tipos de entidades que participan en el suministro y funcionamiento de los procesos y componentes de un sistema de identidad digital. Los IDSP proporcionan sistemas de identidad digital a los usuarios y las partes que confían. Como se ha señalado anteriormente, una sola entidad puede desempeñar las funciones de uno o varios IDSP.
Proveedor de servicios de verificación de la identidad (IVSP)	Entidad que lleva a cabo la comprobación de la identidad (validación de las pruebas y verificación que vincula las pruebas validadas con el solicitante).
Proveedor de identidad (IDP)	Entidad que gestiona las credenciales de autenticación primaria de un abonado y emite afirmaciones derivadas de esas credenciales a las RP. Un IDP suele ser también el proveedor de servicios de credenciales (CSP), pero puede depender de un tercero para la comprobación de la identidad y el otorgamiento de credenciales.
Proveedor de servicios de credenciales (CSP)	Entidad que emite y/o registra autenticadores y las correspondientes credenciales electrónicas (que vinculan los autenticadores a la identidad verificada) a los abonados. El CSP es responsable de mantener la credencial de identidad del abonado y todos los datos de inscripción asociados durante el ciclo de vida de la credencial y de proporcionar información sobre el estado de la credencial a los verificadores. Un CSP suele actuar también como Autoridad de Registro (RA) y Verificador, pero puede delegar determinados procesos de inscripción, comprobación de la identidad y emisión de credenciales/autenticadores en una entidad independiente, conocida como RA o Gestor de Identidades (IM), es decir, los CSP pueden estar formados por múltiples entidades empresariales de funcionamiento y propiedad independientes. Un CSP puede ser un proveedor externo independiente o puede emitir credenciales para su propio uso (por ejemplo, una gran institución financiera o una entidad gubernamental). Un CSP también puede proporcionar otros servicios, además de los servicios de identidad digital, como la realización de funciones adicionales de cumplimiento de DDC/KYC en nombre de una parte que confía (RP).
Autoridad de Registro (RA) (o Gestor de Identidad)	Entidad responsable de la inscripción. La RA registra (inscribe) al solicitante y sus [credenciales y] autenticadores del solicitante tras la comprobación de la identidad.

PROVEEDORES DE SERVICIOS DE IDENTIDAD	
Verificador	Entidad que verifica la identidad del solicitante a una parte que confía (RP) confirmando la posesión y el control del solicitante de uno o más autenticadores, utilizando un protocolo de autenticación. El verificador confirma que los autenticadores son válidos interactuando con el proveedor de servicios de credenciales (CSP) y proporciona una aserción sobre el protocolo de autenticación a la RP. La aserción comunica a la RP los resultados del proceso de autenticación y, opcionalmente, información sobre el abonado. Para confirmar la posesión y el control de autenticadores válidos por parte del solicitante, es posible que el verificador tenga que confirmar también que las credenciales que vinculan al autenticador o autenticadores con la cuenta del abonado son válidas. El verificador es responsable de proporcionar un mecanismo mediante el cual la RP pueda confirmar la integridad de la afirmación que comunica a la RP. El papel funcional del verificador suele implementarse en combinación con el CSP, la RP o ambos.
USUARIO	
Usuario	Es el individuo único, de la vida real, cuya identidad ha sido probada, inscrita, acreditada y autenticada por un sistema de identidad digital y que lo utiliza para probar su identidad (legal). Los usuarios suelen recibir diferentes nombres en las distintas fases de un sistema de identidad digital, dependiendo de su función basada en las actividades con respecto a cada uno de los tres componentes de un sistema de identidad digital, como se indica a continuación.
Solicitante	Persona a la que se le va a acreditar la identidad y a la que se va a inscribir. El solicitante se refiere a la persona que se somete a los procesos de comprobación de la identidad y de inscripción/vinculación (credencialización) y se aplica al usuario desde el momento en que éste solicita una identidad digital y proporciona pruebas de identidad de apoyo hasta que la identidad del usuario ha sido verificada y se ha establecido una cuenta de identidad y se ha vinculado al autenticador o autenticadores, momento en el que el solicitante se convierte en ABONADO
Abonado (también denominado Sujeto)	Persona cuya identidad ha sido verificada y vinculada a autenticadores (credencializada) por un proveedor de servicios de credenciales (CSP) y que puede utilizar los autenticadores para demostrar su identidad. Los abonados reciben un autenticador o autenticadores y la correspondiente credencial de un CSP y pueden utilizar el autenticador o autenticadores para demostrar su identidad.
Demandante	Es el abonado que afirma la propiedad de una identidad a una PARTE QUE CONFÍA (RP) y busca que se verifique, utilizando protocolos de autenticación. Un solicitante es una persona que busca probar su identidad y obtener los derechos asociados a esa identidad (por ejemplo, para abrir o acceder a una cuenta financiera).
Parte que confía (RP)	Persona (física o jurídica) que confía en las credenciales o autenticadores de un abonado, o en la afirmación de la identidad de un solicitante, para identificar al abonado, utilizando un protocolo de autenticación. Una RP confía en una aserción de identidad basándose en la fuente, el momento de la creación, el tiempo de validez de la aserción desde el momento de la creación y el correspondiente marco de confianza que rige las políticas y procesos de los CSP y RP. La RP es responsable de autenticar la fuente de una aserción (es decir, el verificador) y de confirmar la integridad de la aserción. Una RP se basa en los resultados de un protocolo de autenticación para establecer la confianza en la identidad o los atributos de un abonado para establecer una relación comercial (apertura de cuenta) o autorizar el acceso a la cuenta y/o realizar una transacción. Las RP pueden utilizar la identidad autenticada de un abonado, el IAL, el AAL y el FAL, los metadatos, que proporcionan información sobre la fiabilidad de cada uno de los componentes y procesos de la identidad digital, y otros factores para tomar una decisión final de identidad/verificación o autorización. Las RP típicas son las instituciones financieras y los departamentos y agencias gubernamentales.
Proveedor del marco de confianza / Autoridad de confianza	Entidad de confianza que certifica y/o audita el cumplimiento del IDSP con las normas técnicas (procesos y controles) para los niveles de garantía de identidad, autenticación y federación (IAL, AAL y FAL). Los proveedores de marcos de confianza también pueden ser responsables de establecer normas técnicas para estos niveles de garantía. Los proveedores de marcos de confianza pueden ser entidades gubernamentales (por ej., EU/eIDAS) o una organización industrial de confianza, como *Open Identity Exchange* (OIX); FIDO (*Fast Identity Online*) Alliance (especificaciones y certificaciones para autenticadores basados en hardware, móviles y biométricos que reducen la dependencia de las contraseñas y protegen contra la suplantación de identidad, los ataques de *man-in-the-middle* y los ataques de repetición con contraseñas robadas); Kantara; o GSMA (para dispositivos de comunicaciones móviles).

ANEXO B: CASOS DE ESTUDIO

Cuadro 4. Número de identificación único de la India (UID)

Características del sistema de identidad digital: El programa de identidad del número de identidad único (UID) de la India, o Aadhaar, utiliza múltiples datos biométricos y biográficos, así como la documentación oficial de identidad cuando está disponible, para proporcionar una identidad digital a todos los residentes en la India, independientemente de su edad o nacionalidad.

La Autoridad de Identificación Única de la India (UIDAI) ha lanzado una aplicación móvil, m-Aadhaar, que genera un número de «identidad virtual», vinculado al número Aadhaar pero diferente de él, para aumentar la privacidad y la seguridad. Tanto el número Aadhaar como el ID virtual pueden autenticarse en línea, con la base de datos Aadhaar, o fuera de línea, mediante un código QR.

Medidas de inclusión financiera: El proceso de inscripción en Aadhaar de la UIDAI tiene unos requisitos de prueba de identidad flexibles para lograr una cobertura completa en una jurisdicción en la que muchas personas carecen de documentos de identidad básicos, y se basa en la biometría para establecer la unicidad. La inscripción debe hacerse en persona, pero se lleva a cabo en registradores autorizados ubicados en todo el país (principalmente gobiernos estatales, ministerios centrales, bancos y organizaciones del sector público), utilizando programas informáticos y equipos de captura biométrica y otros prescritos por la UIDAI mediante un memorando de entendimiento. Los registradores deben tomar medidas especiales para inscribir a las mujeres, los niños, las personas mayores, los discapacitados, los trabajadores no cualificados y no organizados, las tribus nómadas y todos los demás grupos marginados/vulnerables de individuos que no tienen una vivienda permanente.

La UIDAI acepta numerosos tipos de documentos de identidad para verificar los atributos básicos en el momento de la inscripción: 32 tipos de documentos de identidad con nombre y foto; 14 documentos de prueba de parentesco; 10 documentos de fecha de nacimiento; 45 documentos de prueba de domicilio. (Véase https://uidai.gov.in/images/commdoc/valid_documents_list.pdf).

Si una persona no dispone de ninguno de los documentos de identidad «notificados», puede inscribirse en Aadhaar si un documento familiar de derecho incluye su nombre y el jefe de familia que figura en el documento de derecho se inscribe en Aaadhar, utilizando los documentos de prueba de identidad y de domicilio requeridos y presenta al miembro de la familia mientras se inscribe. Cuando no se disponga de un PdP u otros documentos requeridos, el residente puede utilizar a los introductores o certificadores, que son personas notificadas por el Registrador o la oficina regional de la UIDAI, que están disponibles en el centro de inscripción

Utilización para la DDC: Es importante destacar que, en virtud de la Ley de Enmienda de Aadhaar, adoptada en julio de 2019 para cumplir con la decisión del Tribunal Supremo del 26 de septiembre de 2018 que anuló ciertas disposiciones de la Ley original de Aadhaar por motivos de privacidad, el uso de Aadhaar sigue siendo obligatorio para fines fiscales y para recibir beneficios, subsidios y servicios gubernamentales financiados por el Fondo Consolidado de la India, pero ya no es obligatorio para abrir una cuenta bancaria (u obtener un número de teléfono móvil). En cambio, el uso de Aadhaar para la DDC es estrictamente voluntario y debe basarse en el consentimiento informado del cliente. Los sujetos obligados pueden verificar la identidad de sus clientes mediante:
(i) autenticación o verificación fuera de línea de Aadhaar, (ii) pasaporte, o (iii) cualquier otro documento notificado por el gobierno central.

Fuente: Banco Mundial

Cuadro 5. Perú

El sistema nacional de identidad digital de Perú, el Registro Nacional de Identificación y Estado Civil (RENIEC), presta servicios de identidad digital a una amplia gama de entidades públicas y privadas de numerosos sectores, lo que les permite agilizar la verificación y autenticación de la identidad y mejorar la prestación de servicios. En el sector financiero, el RENIEC sirve como sistema central para llevar a cabo la identificación/verificación de los clientes en cumplimiento de los requisitos de DDC para la plataforma de dinero electrónico y dinero móvil de Perú, Billetera Móvil (BiM), que se lanzó en febrero de 2016 y proporciona servicios tales como la entrada y salida de efectivo en los agentes, la capacidad de comprobar los saldos, realizar pagos P2P y recargar el crédito a millones de clientes.

Fuente: Banco Mundial (2018), *Digital ID On-boarding*

Cuadro 6. Números de verificación bancaria de Nigeria (BVN)

Cada nigeriano con una cuenta bancaria está registrado en el sistema de Número de Verificación Bancaria (BVN), que consiste en una base de datos de identificación biométrica y la infraestructura de e-KYC gestionada por el Sistema de Liquidación Interbancaria de Nigeria (NIBSS). Más de 36 millones de adultos están incluidos en la base de datos del BVN y pueden utilizarlo para abrir una nueva cuenta en otro banco, abrir un monedero electrónico o solicitar un préstamo. Esto ha reducido los costos de admisión y contribuye a una mayor competencia en el mercado de servicios financieros. La identificación y verificación del cliente con el BVN es instantánea y también permite la verificación a distancia (no presencial) a través de dispositivos móviles. El NIBSS ha proporcionado interfaces de programación de aplicaciones (API) que permiten la integración del BVN a los bancos y a los proveedores de servicios financieros digitales no bancarios, incluidas las FinTechs de todo el país.

Fuente: Banco Mundial

Cuadro 7. México - Altos costos en el uso de un sistema de identificación para fines de DDC

En México, el sistema fundacional de identificación de las personas es la Clave Única de Registro Nacional de Población (CURP), si bien se dirige a toda la población y tiene el potencial de utilizar la biometría, no es única y no cumple con los niveles de garantía necesarios para los requisitos normativos de DDC en México.

Por el contrario, la credencial de elector que emite el Instituto Nacional Electoral cada diez años incluye dos formas de biometría desde 2016 (reconocimiento facial y huellas dactilares) lo que presenta menores riesgos de duplicidades que la CURP. El carácter de «propósito general» del INE para los adultos en México fue creado bajo una disposición legal temporal incluida en la Ley General de Población para ser utilizado como la principal fuente de identidad de los mexicanos hasta que la CURP pudiera proporcionar niveles de garantía similares a los del INE.

El INE desarrolló un servicio para permitir que terceros verifiquen las credenciales en la base de datos, pero el costo de este servicio, aunque necesario, está impactando a las pequeñas y medianas instituciones financieras, así como a las empresas Fintech que desean operar en el país.

En 2018, se emitió la Ley Fintech y, conscientes en ese momento de los crecientes casos de robo de identidad en el país, las autoridades emitieron medidas para mitigar tales preocupaciones mientras cumplían con las recomendaciones del GAFI sobre DDC. Las medidas emitidas incluyeron el uso del INE como fuente primaria de credencial de verificación para los sujetos obligados y reglas detalladas con respecto al uso de la biometría, lo que impulsó a los sujetos obligados a buscar soluciones adecuadas del mercado de identidad digital para cumplir con los requisitos regulatorios de DDC.

Sin embargo, el INE fue desarrollado para servir como credencial de elector y no como un servicio de verificación de identificación de propósito general, por lo que las autoridades han iniciado, de manera coordinada, una reforma integral en materia de identidad digital con el objetivo de contar con una identidad digital oficial que también pueda ser utilizada para fines relacionados con la DDC.

Fuente: Banco Mundial

Cuadro 8. ACNUR - Identidad digital para los refugiados

A finales de 2018, la Agencia de las Naciones Unidas para los Refugiados (ACNUR) estimó que había 25,9 millones de refugiados y 3,5 millones de solicitantes de asilo en todo el mundo. Los países de las regiones desarrolladas acogían al 16% de los refugiados, mientras que un tercio de la población mundial de refugiados (6,7 millones de personas) se encontraba en los países menos desarrollados del mundo.

Los países de acogida son los principales responsables de expedir pruebas de identidad oficial a los refugiados, aunque este proceso puede ser administrado por una autoridad reconocida y con mandato internacional.

Los problemas de identidad a los que se enfrentan los refugiados son, en muchos sentidos, únicos. Muchos refugiados no poseen credenciales de identidad cuando llegan a un Estado de acogida porque sus credenciales se quedaron atrás, se perdieron o se destruyeron durante la huida. Es posible que a algunos refugiados no se les haya expedido nunca un documento de identidad oficial u otra credencial, a menudo porque proceden de zonas frágiles o afectadas por conflictos o porque han sido discriminados, impidiendo su registro. Al mismo tiempo, existe un principio general que impide el contacto con las autoridades del país de origen para verificar la identidad de un refugiado sin el consentimiento de éste y si existe algún riesgo de daño. Por lo tanto, las normas internacionales indican que la comprobación de la identidad de los refugiados requiere una mayor confianza en las pruebas recogidas durante las solicitudes y entrevistas en persona, así como el conocimiento del país de origen del solicitante, la cultura y otra información locales. La garantía de la identidad aumenta a través del contacto regular y la validación a lo largo del tiempo para controlar la coherencia, gestionar el riesgo y construir la identidad del refugiado en el nuevo contexto.

El sistema de identidad digital del ACNUR es utilizado por muchos gobiernos de acogida y por el ACNUR para el registro y la gestión de la identidad de los solicitantes de asilo y los refugiados. En marzo de 2020 más de 9 millones de refugiados en 72 países habían sido inscritos biométricamente en el sistema.

Características del sistema de identidad digital:

- El ACNUR está reforzando su sistema de identidad digital para los solicitantes de asilo y los refugiados. El proceso del ACNUR de comprobación e inscripción de la identidad de estas personas se describe en la Guía del ACNUR sobre Registro y Gestión de la Identidad,[55] capítulo 5.3 «Determinación de la identidad de una persona: revisión de documentos y recopilación de datos» y 5.6 «Inscripción biométrica y fotografías».
- Los medios de autenticación de la identidad proporcionados por el sistema de identidad digital del ACNUR varían, dependiendo del contexto del país y de los casos de uso. Las credenciales de identidad emitidas por el sistema se utilizan principalmente en entornos presenciales. Las credenciales de identidad de los solicitantes de asilo y de los refugiados varían en función de los requisitos del gobierno de acogida, pero contienen una imagen facial e información biográfica, que incluye un conjunto mínimo de datos y atributos adicionales que identifican a una persona de forma exclusiva. Las credenciales de identidad también tienen un código de barras impreso o un código QR y un número de referencia único para el titular.
- El sistema de identidad digital del ACNUR puede admitir la autenticación mediante biometría, que se utilizó inicialmente para la distribución de asistencia humanitaria, incluidas las transferencias de efectivo (que se denominan intervenciones basadas en efectivo). Por ejemplo, en varios países de Oriente Medio, entre ellos Jordania, las intervenciones basadas en efectivo se realizan a través de cajeros automáticos con equipos de escaneo del iris para autenticar la identidad del usuario.
- En Malasia e Indonesia, las autoridades utilizan una aplicación de Android para comprobar la validez del documento de identidad expedido a un refugiado por el ACNUR y facilitar la verificación de la identidad del titular mediante la comparación con una fotografía que aparece en la aplicación.
- En Uganda, la Oficina del Primer Ministro (que es responsable del registro y la identidad de los refugiados y utiliza el sistema de identidad digital del ACNUR), en cooperación con la Comisión de Comunicaciones de Uganda y el ACNUR, está estableciendo un sistema que permitirá la autentificación biométrica en el punto de venta por parte de los vendedores de tarjetas SIM. En el momento de redactar este informe, el proceso estaba en fase de pruebas. En Somalia se ha implantado la autenticación biométrica para la incorporación a los servicios financieros de los refugiados que regresan (véase más abajo para más detalles).

Participantes en un sistema de identidad digital: Las funciones de los participantes en el sistema de identidad digital del ACNUR varían en función del contexto del país.

- Cuando el ACNUR se encarga del registro de refugiados y de la gestión de la identidad en nombre del gobierno de acogida o en el contexto del retorno y el reasentamiento, el ACNUR es el único controlador de datos.
- En otros contextos, se adopta una solución híbrida, la más común cuando el Estado de acogida utiliza el sistema del ACNUR para el registro y la gestión de la identidad de los refugiados. En estas circunstancias, el ACNUR proporciona el sistema y el Gobierno de acogida y el ACNUR son los controladores de datos conjuntos, regulados a través de acuerdos de intercambio de datos.

55. ACNUR, «Guía sobre Registro y Gestión de la Identidad» https://www.unhcr.org/registration-guidance/es/chapter1/introduction-to-the-guidance-on-registration/

- En el caso del sistema biométrico utilizado en Egipto, Irak, Jordania, Líbano y Siria, el ACNUR trabaja con un proveedor del sector privado en el contexto de un protocolo de protección de datos.

Uso para la DDC y la normativa pertinente: El sistema de identidad digital del ACNUR y las credenciales emitidas por él pueden utilizarse para la identificación/verificación de los clientes en el momento de la admisión en varios países, entre ellos: Burundi, Malawi, Jordania, Níger y Zambia.[56]

El Banco Central de Somalia ha acordado adoptar un enfoque de DDC para los refugiados que regresan y que han sido inscritos biométricamente en el sistema del ACNUR en Kenia y otros países vecinos. Se permitirá que el Formulario de Retorno Voluntario emitido por el ACNUR al repatriado antes de la salida en el país de asilo, junto con la autenticación biométrica de la identidad utilizando el sistema del ACNUR se utilice para la identificación/verificación del cliente al abrir una cuenta bancaria. Esta solución se probó en diciembre de 2018 con cuentas abiertas para dos personas y se espera que se implemente a mayor escala con un proveedor de servicios financieros en 2020.

Nivel de garantía del sistema: El nivel de garantía del sistema del ACNUR no ha sido auditado con respecto a los marcos de confianza de identidad digital y las normas técnicas que se analizan en esta Guía, sin embargo, en el momento de redactar este documento, el ACNUR ha encargado evaluaciones externas a consultores expertos y está evaluando las conclusiones.

Inclusión financiera: La inclusión financiera de los refugiados es un componente importante de la protección, la autosuficiencia y la resiliencia de los refugiados. El ACNUR distribuyó 2.400 millones de dólares en intervenciones humanitarias basadas en efectivo entre 2016 y 2019. Para promover la inclusión financiera, el ACNUR se propone realizar intervenciones basadas en efectivo a través de las cuentas bancarias o de dinero móvil de los beneficiarios (respetando la normativa local), y dar prioridad a los sistemas de «bucle abierto» que aprovechan los mercados y ecosistemas locales, en lugar de invertir en sistemas de «bucle cerrado», que solo contribuyen de forma limitada a la inclusión financiera. Aprovechando la tecnología digital y las plataformas móviles específicamente, el ACNUR pretende promover la inclusión financiera, que ha demostrado un impacto positivo y tangible en la vida de los refugiados.

Fuente: ACNUR

Cuadro 9. China - El sector privado proporcionó una identidad digital

Características y participantes del sistema de identidad digital: Ant Financial ha creado un sistema de identidad digital, basado en la información de DDC que ha sido verificada por el Ministerio de Seguridad Pública de China (MPS), así como en otros datos recogidos, incluido el reconocimiento facial. El nombre y el número de identificación del cliente se verifican mediante la base de datos autorizada que posee el MPS para garantizar la exactitud de la información de identidad. El reconocimiento facial (coincidencia con los avatares de los documentos válidos), la validación cruzada multicanal y la comprobación de la lista negra se combinan con

56 ACNUR, «Desplazados y desconectados» (2019) https://www.unhcr.org/innovation/wp-content/uploads/2020/04/Desplazados-Desconectados-Web-April_2020.pdf

escenarios comerciales para completar la diligencia debida del cliente. Cada verificación se basa en la autorización explícita del usuario y confirma el uso del servicio de verificación.

Uso para servicios financieros: Ant Financial y las instituciones financieras cooperan para proporcionar servicios financieros como seguros, fondos y microfinanzas a los clientes, y también utilizan plenamente la identidad digital para proporcionar a las instituciones financieras servicios como la identificación de clientes y la evaluación del riesgo de estos. La identidad digital de Ant Financial ha sido ampliamente aceptada en varios escenarios de servicios financieros, proporcionando más de 3.000 millones de servicios de verificación facial a cientos de millones de usuarios de Alipay. También se utiliza en la consulta de pensiones, el cobro de pensiones, la declaración de impuestos y otros servicios públicos. Además, Ant Financial proporciona identidades digitales a los turistas de corta duración en China que no tienen una cuenta bancaria china pero quieren hacer pagos a través del móvil. Ant Financial toma medidas especiales de verificación de la identidad con la Oficina de Inmigración para confirmar que la información del pasaporte es auténtica.

Nivel de garantía del sistema: En China no existen marcos ni normas técnicas transparentes de garantía de identidad digital, pero se ha sugerido que, si se evalúa según las normas del NIST, el sistema de identidad digital de Ant Financial podría tener un nivel de garantía de identidad 2 (IAL2), un nivel de garantía de autenticación 1(AAL1) y un nivel de garantía de federación 2 (FAL2).

Medidas de inclusión financiera:

(1) Para los residentes en zonas rurales o remotas subdesarrolladas sin acceso a cuentas bancarias o donde la tecnología de las cámaras no es lo suficientemente avanzada como para soportar las tecnologías de reconocimiento facial, Ant Financial puede verificar la información del cliente a través de la Plataforma de Verificación de la Información de la Identidad Ciudadana. La cuenta tiene limitaciones (los pagos no pueden superar los 1.000 yuanes) y no se permiten los pagos transfronterizos.

(2) En el caso de los estudiantes universitarios que no tienen acceso a cuentas bancarias, Ant Financial puede verificar la identidad de los estudiantes a través de la Red de Información de Estudiantes de Educación Superior de China, incluida la situación educativa del estudiante.

Fuente: China

Cuadro 10. Singapur - Identidad digital nacional (NDI)

En el marco de la Identidad Digital Nacional (NDI), el Gobierno de Singapur está desarrollando una batería de servicios de identidad digital para que los residentes y las empresas de Singapur puedan realizar transacciones digitales con el Gobierno y el sector privado de forma cómoda y segura. La NDI se basa en técnicas de seguridad criptográfica de infraestructura de clave pública (PKI), y los servicios se han desplegado gradualmente desde 2017 y se espera que estén completamente operativos en 2020.

Características del sistema de identidad digital: Hay 4 capas distintas en la batería de la NDI.

- Datos de confianza: MyInfo constituye el servicio de datos de identidad de confianza de la NDI y se puso en marcha a principios de 2017. MyInfo incluye datos verificados por el gobierno recuperados de varias agencias gubernamentales y contiene más de 100 datos personales. Proporciona a los ciudadanos y residentes el acceso y el control sobre el intercambio de sus datos. Los ciudadanos pueden autocompletar su información personal verificada por el Gobierno en los servicios electrónicos

del sector público y privado a través de un canal confiable e independiente con el consentimiento del individuo.

- Identidad de confianza: El Gobierno pondrá en marcha una Autoridad Nacional de Certificación (NCA) para otorgar a cada residente una identidad digital basada en la criptografía, generada de forma segura y alojada en un teléfono móvil. Una identidad digital en la que podrán confiar universalmente tanto el gobierno como las empresas del sector privado. Admitirá un modelo de garantía de identidad de varios niveles, que permitirá a los usuarios realizar transacciones más delicadas a medida que aumente su nivel de garantía de identidad.
- Acceso de confianza: La NDI admitirá un ecosistema abierto y federado de proveedores de servicios de autenticación (ASP). El Gobierno operará uno de los ASP, pero otros ASP pueden ser operados por el sector privado, todos ellos con referencia a la misma identidad digital emitida por el Gobierno. A finales de 2018, se lanzó SingPass Mobile para permitir la autenticación segura sin necesidad de tokens de hardware o SMS-OTP, lo que proporciona una mayor inclusión digital y facilidad de acceso tanto para el sector público como para el privado.
- Servicios de confianza: Son servicios digitales construidos sobre las capas de la NDI. Un ejemplo es la firma digital. Las instituciones financieras pueden confiar en la NDI para proporcionar servicios más fiables y de alta seguridad, así como para agilizar los viajes de los clientes, independientemente de los límites de los sistemas u organizaciones.

Participantes en el sistema de identidad digital: Las capas de datos e identidad de confianza son proporcionadas por el Gobierno. La capa de acceso de confianza apoyará un ecosistema abierto y federado de proveedores de servicios de autenticación y firma digital (ASP y DSAP). El Gobierno gestionará uno de los ASP.

Utilización para la DDC: En la actualidad, más de 60 instituciones financieras de Singapur utilizan MyInfo para más de 220 servicios digitales con el fin de incorporar y realizar la DDC de los clientes.

Normativa específica de identidad digital en materia ALA/CFT: La Autoridad Monetaria de Singapur ha publicado una Guía sobre el «Uso de MyInfo y las medidas de DDC para las relaciones comerciales no presenciales» (AMLD 01/2018).57 Cuando se utiliza MyInfo, las instituciones financieras no tendrán que obtener documentos físicos para verificar la identidad de un cliente y tampoco se espera que obtengan por separado una fotografía del cliente. La MAS ha aclarado que considera que MyInfo es una fuente confiable e independiente para verificar el nombre del cliente, su número de identificación único, su fecha de nacimiento, su nacionalidad y su dirección residencial. Las instituciones financieras están obligadas a mantener un registro adecuado de los datos, incluidos los obtenidos de MyInfo, de acuerdo con los requisitos reglamentarios de Singapur.

Nivel de garantía del sistema: La NDI ha utilizado el NIST estadounidense y el e-IDAS de la UE como ejemplos de referencia. La NDI evaluará su nivel de garantía en comparación con el de otros países a medida que Singapur se embarque en oportunidades de cooperación bilateral. Para la garantía de autenticación, se basa en el Nivel de Garantía de Evaluación (EAL) de Common Criteria (CC), con el uso de AVA: Evaluación de Vulnerabilidad (AVA_VAN, de 1 a 5).

57. www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Anti_Money-Laundering_Countering-the-Financing-of-Terrorism/Circular-on-MyInfo-and-CDD-on-NFTF-business-relations.pdf

Inclusión financiera: La NDI se proporciona gratuitamente a todos los ciudadanos y residentes de Singapur, y forma parte del programa de inclusión de los organismos gubernamentales pertinentes.

Fuente: Singapur

Cuadro 11. Sudáfrica

Para responder a la creciente necesidad de mitigar el fraude y el robo de identidad, así como para cumplir los requisitos de DDC, en 2002 se creó el Centro de Información sobre Riesgos Bancarios de Sudáfrica (SABRIC). Inicialmente compuesto por los cuatro bancos más grandes, el SABRIC ahora también incluye otros bancos, tres proveedores de efectivo en tránsito y un proveedor de servicios de cajeros automáticos. En 2007, el SABRIC y el Departamento de Interior (DHA) empezaron a colaborar en la lucha contra los delitos relacionados con la identidad. Al principio, los bancos verificaban la identidad de los clientes sobre la base de una inspección visual de la libreta de identificación verde con código de barras y la comparación visual de la foto que figuraba en ella con la apariencia del (posible) cliente. Sin embargo, el método «manual» de verificación de la identidad tenía puntos débiles. Para subsanarlos, los miembros del SABRIC y el DHA colaboraron para permitir la verificación de la identidad de los clientes cotejando sus huellas dactilares directamente con la base de datos biométricos HANIS del DHA, que devuelve una respuesta de «verificado» o «no verificado». Se estableció una conexión segura para acceder a la base de datos del DHA en las oficinas bancarias participantes a través de la Agencia Estatal de Tecnología de la Información (SITA) de Sudáfrica. Los bancos pagan al DHA por la verificación. El proceso de verificación genera una pista de auditoría y el sistema proporciona información de gestión fiable. A finales de 2018, siete bancos y 4.000 sucursales participaban en el proyecto. Actualmente, el número de verificaciones es de unos 3 millones al mes. Las consultas de la base de datos DHA suelen durar entre 4 y 16 segundos. Entre el 2% y el 3,8% de las verificaciones electrónicas no han tenido éxito, porque la persona cuya identidad se verificó carecía de un registro biométrico en HANIS.

Fuente: Banco Mundial

Cuadro 12. Interoperabilidad y reconocimiento mutuo del eIDAS

En el marco del eIDAS, los Estados miembros pueden utilizar la identidad digital para acceder a los servicios en línea. También pueden decidir involucrar al sector privado en el suministro de soluciones de identidad digital (medios). En virtud del principio de reconocimiento mutuo, los Estados miembros están obligados a aceptar los medios de identidad digital notificados de otros Estados miembros si permiten el uso de la identidad digital para el acceso en línea a sus servicios públicos, y el nivel de garantía de los medios notificados es igual o superior al necesario para acceder al servicio. El Reglamento eIDAS define tres niveles de garantía diferentes (bajo, sustancial y alto) en función del grado de confianza en la identidad declarada o afirmada de una persona.

Fuente: Comisión Europea

Cuadro 13. Bélgica – eCards & ItsMe ®

El sistema de identidad digital belga incluye componentes tanto del sector público como del privado. Como se explica con más detalle a continuación, el gobierno proporciona credenciales de identidad digital de uso general, la tarjeta electrónica de ciudadano belga y la tarjeta electrónica de extranjero (denominadas conjuntamente tarjetas electrónicas belgas). También proporciona la plataforma de autenticación de identidad digital para los servicios del gobierno electrónico. Casi todos los ciudadanos y residentes belgas disponen de una eCard, que permite acceder a una amplia gama de más de 800 aplicaciones del gobierno electrónico, entre ellas Tax-on-Web, aplicaciones de la seguridad social y de la salud electrónica, Police-on-web, aplicaciones de los gobiernos regionales y portales en línea para los municipios. Además, un servicio de autenticación de identidad digital del sector privado, Itsme®, proporciona autenticación por teléfono móvil de las identidades vinculadas a una tarjeta electrónica y a un teléfono móvil y una tarjeta SIM específicos para los bancos y operadores de redes móviles (ORM) participantes. Los clientes actuales pueden utilizar Itsme® para autenticar su identidad con el fin de acceder a sus cuentas y realizar transacciones.

Características del sistema de identidad digital y participantes clave:

Tarjetas electrónicas

- El registro de las tarjetas electrónicas belgas se realiza en persona. Los municipios / consulados y embajadas son responsables de la comprobación de la identidad, el registro, la emisión y la entrega de la tarjeta electrónica.
- El Gobierno belga proporciona el Servicio Federal de Autenticación (FAS) para autenticar las identidades para acceder a los servicios gubernamentales en línea. La plataforma FAS admite tanto el acceso por navegador de Internet como por teléfono móvil, y se basa en el estándar TLS del IETF, que proporciona seguridad de extremo a extremo en las comunicaciones criptográficas a través de las redes. La autenticación del FAS implica los siguientes pasos:

  - El ciudadano o el extranjero trata de iniciar sesión en un servicio de gobierno electrónico introduciendo el código PIN de su tarjeta electrónica en línea.
  - El navegador de Internet envía un certificado de autenticación al FAS, que tal vez realice las verificaciones de certificado necesarias para garantizar la integridad, validez y autenticidad del certificado de autenticación de cliente TLS presentado.
  - El FAS autentifica el certificado, permitiendo al individuo completar el inicio de sesión y acceder a la aplicación gubernamental solicitada.

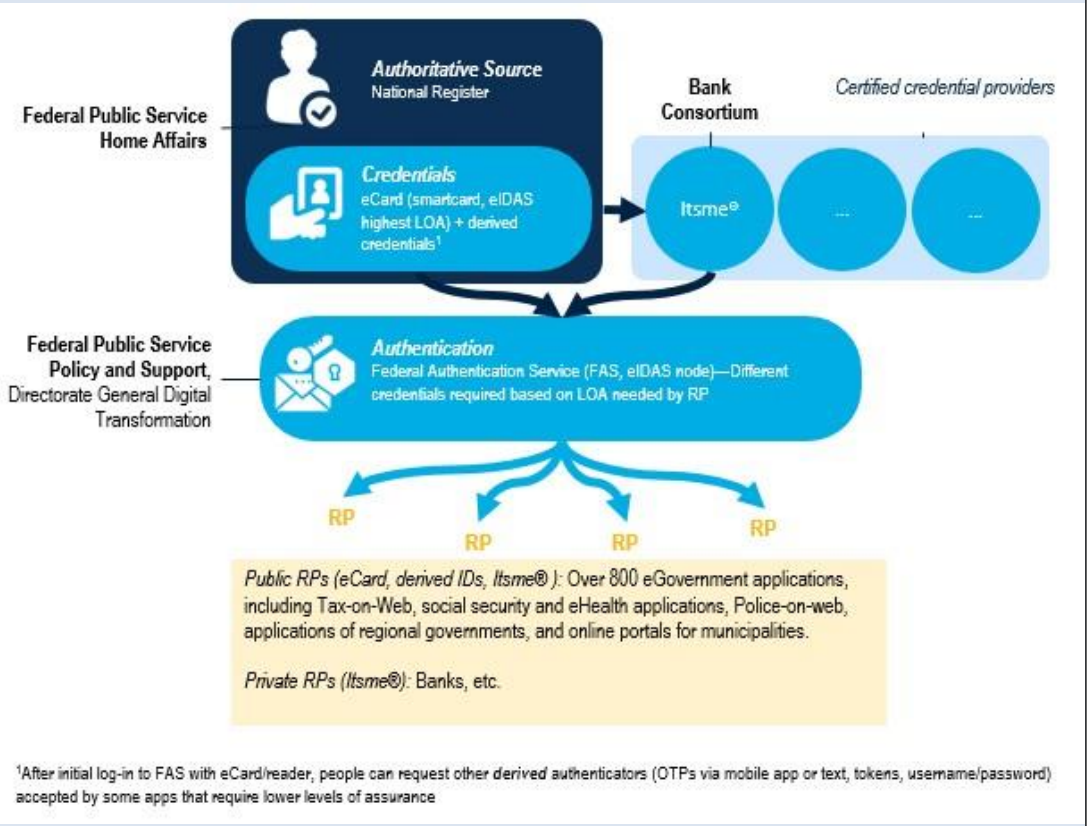
Itsme®

- Itsme® es una iniciativa de Belgian Mobile iD, un consorcio de cuatro de los principales bancos belgas (Belfius, BNP Paribas Fortis, ING, KBC) y operadores de redes móviles (Orange, Proximus, Telenet). La activación de Itsme® en un dispositivo móvil está vinculada al documento de identidad electrónico belga, para garantizar la prueba de identidad. El flujo de autenticación entre el usuario de Itsme® y el FAS, mediante la aplicación Itsme®, se basa en el estándar OpenID Connect (Doc Ref. 1.2.4).

Uso para servicios financieros: La plataforma del FAS belga sólo está disponible para acceder a los servicios públicos, por el momento no es posible prestar servicios financieros. La solución itsme® se utiliza para autenticar las transacciones.

Nivel de garantía del sistema:

- Las tarjetas electrónicas belgas ofrecen un alto nivel de garantía según las especificaciones de eIDAS, tal y como ha confirmado la red de cooperación eIDAS tras una profunda revisión por parte de los Estados miembros.
- Itsme® ha sido sometido a una exhaustiva auditoría de seguridad y gobernanza y ha sido reconocido por el gobierno belga como un medio válido de autenticación con un Nivel de Garantía «alto».



Fuente: Bélgica

Cuadro 14. Suecia - Marco de identificación electrónica y BankID

El Gobierno sueco, que mantiene una base de datos central de las identidades de todos los ciudadanos y residentes suecos, facilita la identidad digital a través de una asociación público-privada. El gobierno proporciona la arquitectura de la identidad digital federada (el marco eID - Sweden Connect Technical Framework) y las entidades privadas, incluidos los bancos, actúan como proveedores de servicios de identidad digital, emitiendo credenciales de identidad digital y proporcionando servicios de autenticación.

Características del sistema de identidad digital y participantes clave: La federación incluye tanto a los proveedores de servicios de identidad digital como a las partes usuarias que proporcionan bienes o servicios comerciales o servicios gubernamentales en línea. Actualmente hay cuatro proveedores de servicios de identidad digital: (1) AB Svenska Pass, (2) BankID, (3) Freja eID, y (4) Telia E- identification—aunque Telia dejó de inscribir a personas para la identificación electrónica en otoño de 2017, las credenciales de identificación electrónica que había emitido son válidas hasta que expiran.

Lanzado por primera vez en 2003 y gestionado por un consorcio de 10 bancos suecos, BankID proporciona a los clientes una identidad digital gratuita, que puede utilizarse para autenticar la identidad para realizar transacciones en el sector privado y público. Las empresas que desean integrar BankID en sus servicios contratan con un banco de la red BankID y pagan una cuota por los servicios de BankID, lo que genera un flujo de ingresos para los bancos participantes. Las credenciales de identidad están disponibles en forma «física», codificada en un chip inteligente, o «electrónica», disponible como software en el ordenador personal, la tableta, el teléfono móvil u otro dispositivo digital del usuario.

Uso para servicios financieros: La identificación bancaria puede utilizarse para la admisión de clientes. Para obtener una identificación bancaria en primer lugar, la persona debe someterse a una DDC documental por parte del banco que emite la identidad digital. Una vez obtenida, la identificación bancaria puede utilizarse para abrir cuentas en otras instituciones financieras. En 2016, BankID facilitó 2.000 millones de transacciones al año y fue utilizado por más del 80% de los ciudadanos suecos.

Normativa específica de identidad digital en materia ALA/CFT: El uso de la identidad digital para la identificación/verificación del cliente está explícitamente previsto en la Ley de ALA/CFT (capítulo 3, artículo 7):

«Un sujeto obligado debe identificar al cliente y verificar su identidad mediante documentos de identidad o extractos de registros o mediante otra información y documentos procedentes de una fuente independiente y confiable.

En la aplicación del primer subapartado, podrán utilizarse instrumentos de identificación electrónica y servicios de confianza de conformidad con el Reglamento eIDAS. También podrán utilizarse otros procesos seguros de identificación remota o electrónica que estén regulados, reconocidos, aprobados o aceptados por las autoridades pertinentes».

Nivel de garantía del sistema: El Consejo Sueco de Identificación Electrónica realiza comprobaciones de los emisores de identificación electrónica de acuerdo con Svensk e-legitimation. En el marco de garantía de la identificación electrónica sueca se definen cuatro niveles de garantía (1 a 4).[58]

Fuente: Suecia
Referencias: *https://elegitimation.se/inenglish/howeidentificationworks.4.769a0b711614b669f2953f.html*

58 https://docs.swedenconnect.se/technical-framework/mirror/digg/Tillitsramverk-for-Svensk-e-legitimation-2018-158.pdf (en sueco)

Cuadro 15. Italia - Sistema público de identidad digital

Características y participantes del sistema de identidad digital: Desarrollado en el marco del Reglamento eIDAS de la UE y puesto en marcha en 2016, el Sistema Público Italiano de Identidad Digital (SPID), es un sistema de identidad digital abierto y público que permite a las entidades públicas y privadas (proveedores de identidad) acreditadas por la Agencia para la Italia Digital (AgID) ofrecer servicios de registro de identidad digital a las personas físicas (ciudadanos y/o individuos con permiso de residencia) de 18 años o más, y autenticar las credenciales de identidad digital SPID, permitiendo al individuo identificado acceder a los servicios públicos y privados. En marzo de 2018, SPID contaba con unos 2,5 millones de identidades digitales. El registro de SPID puede realizarse en persona, en línea o utilizando un dispositivo móvil con cámara web, dependiendo de los procedimientos de registro ofrecidos por un determinado proveedor de identidad. Para obtener las credenciales de identificación SPID, una persona puede proporcionar a un Proveedor de Identidad un documento de identidad válido (tarjeta de identidad o pasaporte), tarjeta de salud, dirección de correo electrónico y número de teléfono móvil, o utilizar su firma digital, tarjeta de identidad electrónica (CIE) o tarjeta de servicio nacional (CNS).

Uso para servicios financieros: La aceptación del SPID es obligatoria para el sector público y opcional para los sectores privados (comercial y financiero). Según una encuesta de ABI Lab (Asociación Bancaria Italiana) a los bancos italianos, a finales del 2019, el 38% de los bancos de la muestra tenía previsto utilizar el sistema SPID para la admisión de clientes de la banca móvil y el 18% tenía previsto utilizarlo para la admisión de la banca por internet.

Normativa específica de identidad digital en materia ALA/CFT: La legislación italiana permite a los sujetos obligados utilizar identidades digitales conformes con el eIDAS, como el SPID, para la identificación de los clientes y la verificación de los clientes que son personas físicas. .

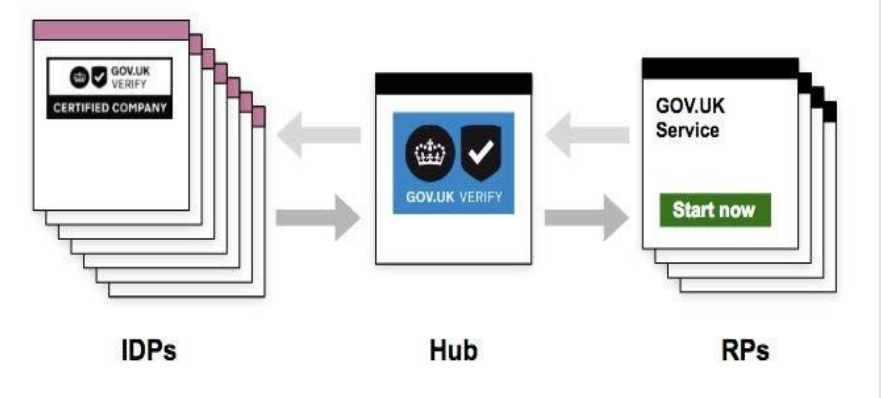
Nivel de garantía del sistema: El SPID ofrece tres niveles de garantía para la autentificación de la identidad, de acuerdo con la norma ISO-IEC 29115. El nivel 1 permite el acceso a los servicios en línea, utilizando un nombre de usuario y una contraseña elegidos por el usuario. El nivel 2, para los servicios que requieren un mayor grado de seguridad, permite el acceso mediante un nombre de usuario y una contraseña elegidos por el usuario, más la generación de un código de acceso temporal (contraseña de un solo uso), utilizable a través de un dispositivo digital (por ejemplo, un teléfono inteligente). El nivel 3 proporciona medidas de seguridad adicionales, incluyendo el uso de dispositivos físicos (por ejemplo, tarjetas inteligentes) proporcionados por el gestor de identidad. El nivel de seguridad requerido para la autenticación de la identidad SPID depende del nivel de seguridad requerido por los proveedores de servicios en línea.

Fuente: Banco Mundial, Banca d'Italia y Federación Bancaria Europea

Cuadro 16. Reino Unido – GOV.UK Verify

En 2012, el Gobierno del Reino Unido publicó una Estrategia Digital Gubernamental, que introdujo el concepto de «Digital por defecto», es decir, proporcionar servicios en línea y permitir un amplio acceso a quienes desean acceder a estos servicios, sin excluir a quienes no pueden o no desean acceder a estos servicios en un canal en línea. Como parte de esta política «digital por defecto», se reconoció la necesidad de una solución de identidad digital sólida que permitiera a los usuarios demostrar su identidad en línea, y al Gobierno confiar en que esos usuarios son quienes dicen ser.

GOV.UK Verify es un sistema de identidad digital federado que permite a los ciudadanos y residentes del Reino Unido demostrar su identidad en línea. Utiliza proveedores de identidad del sector privado (IDP) para probar y autenticar la identidad del individuo según un conjunto de requisitos y especificaciones. Los IDP han cumplido con las normas del gobierno y de la industria para proporcionar servicios de garantía de identidad como parte de GOV.UK Verify.

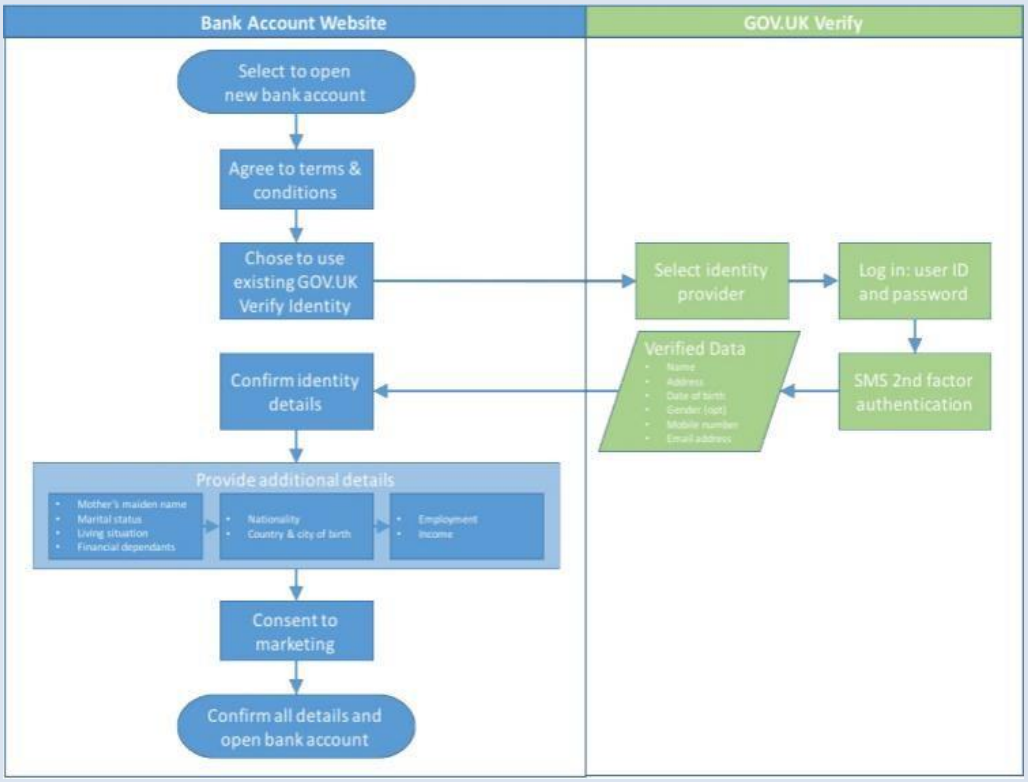


El GOV.UK Verify Hub es la infraestructura centralizada que gestiona las interacciones entre los usuarios, los servicios gubernamentales, los IDP y los servicios de correspondencia con el fin de autenticar a un usuario en un servicio gubernamental. También garantiza que se solicite el nivel requerido de garantía de identidad a un IDP.

Un producto llamado Document Checking Service (DCS) es un punto final de la API que permite a los IDP realizar comprobaciones de los documentos emitidos por el gobierno del Reino Unido en las bases de datos gubernamentales, en apoyo de la prueba de identidad para GOV.UK Verify.

Todas las cuentas de GOV.UK Verify requieren como mínimo 2FA.

El siguiente diagrama desarrollado por Open Identity Exchange muestra un prototipo de recorrido utilizando GOV.UK Verify para abrir una cuenta bancaria.



Fuente: OIX (2017), https://openidentityexchange.org/wp-content/uploads/2017/01/The-value-of-digital-identity-to-the-financial-service-sector-Full.pdf p.13
Fuente: Reino Unido

Cuadro 17. Estonia

Características del sistema de identidad digital: En Estonia hay una serie de sistemas de identidad digital:

- Tarjetas de identidad: el principal documento de identificación en Estonia, es obligatorio para todos los ciudadanos y residentes y es la opción de identidad digital más utilizada. La tarjeta de identidad tiene una fotografía y un chip que almacena de forma segura los datos de identidad personal y los certificados de firma digital, utilizando una infraestructura de clave pública (PKI).
- El Mobile-ID es un servicio de identidad digital del sector privado que puede utilizarse a través del teléfono móvil de una persona. El proveedor de telecomunicaciones emite el Mobile-ID en conexión con la tarjeta SIM y la tarjeta de identificación de una persona. El servicio debe activarse en el sitio web de la Junta de Policía y Guardia de Fronteras (PPA).
- Smart-ID es un servicio de identidad digital del sector privado que utiliza la API de Smart-ID en el teléfono móvil de una persona y el servicio de servidor de gestión de claves de Smart-ID. Smart-ID puede ser emitido a personas con un código de identificación personal estonio. Funciona de forma similar a la tarjeta de identificación y al Mobile-ID en la identificación y verificación de un cliente.

Participantes en un sistema de identidad digital:

- La Autoridad del Sistema de Información de Estonia (RIA) coordina las soluciones de autenticación de la identidad digital. La Junta de Policía y Guardia de Fronteras expide credenciales de identidad (tarjeta de identidad, tarjeta de residencia, Digi-ID y Digi-ID de residente electrónico) de acuerdo con la Ley de Documentos de Identidad. El Ministerio de Asuntos Exteriores es responsable del programa de residencia electrónica.
- Dos empresas privadas aportan soluciones técnicas: Tieto Estonia AS ofrece asistencia al usuario para el software básico del documento de identidad y SK ID Solutions AS emite y valida los certificados de identidad electrónicos.

Utilización para la DDC: Las soluciones de identidad digital de Estonia se utilizan para la identificación/verificación del cliente en el momento de la admisión, así como para la autenticación reforzada del cliente en cumplimiento de la Directiva (UE) 2015/2366 (la segunda Directiva sobre servicios de pago) y sus normas técnicas reglamentarias para autorizar las operaciones de pago.

Normativa específica de identidad digital en materia ALA/CFT: En Estonia, un cliente puede ser admitido cara a cara, a través de medios informáticos (admisión por video) y utilizando dos fuentes diferentes de verificación de la identidad. La legislación no especifica cuáles deben ser los dos medios de verificación, pero la Autoridad de Supervisión Financiera de Estonia ha publicado las orientaciones pertinentes[59] diciendo que las soluciones de identidad digital (es decir, la información obtenida mediante la autenticación con la identidad digital) pueden ser una de esas fuentes (punto 4.3.1.22), pero debe haber una fuente de información adicional (punto 4.3.1.23) para verificar la identidad del cliente.

Nivel de garantía del sistema: Todos los sistemas de identificación electrónica estonios notificados tienen un alto nivel de garantía en el marco del sistema eIDAS

Fuente: Estonia

59. www.fi.ee/sites/default/files/2019-01/FI%20rahapesu%20t%C3%B5kestamise%20juhend%202018%20%28EN%29_pdf.

ANEXO C: PRINCIPIOS SOBRE LA IDENTIFICACIÓN PARA EL DESARROLLO SUSTENTABLE

Esta Guía destaca varias formas concretas en las que los países pueden desarrollar ecosistemas de identidad digital que les permitan aprovechar los beneficios de estos sistemas y, al mismo tiempo, mitigar los riesgos descritos en la Sección IV. Para empezar, los países deberían seguir los diez *Principios de Identificación para el Desarrollo Sostenible*, que ya han sido respaldados por más de 25 organizaciones internacionales, agencias de desarrollo y otros socios.[60] Aunque estos *Principios* se desarrollaron para apoyar la creación de sistemas de identidad «buenos» reconocidos por el gobierno, se aplican de forma más amplia y pueden ser adoptados por sistemas y servicios de identidad tanto públicos como privados.

Tabla 3. Principios sobre la identificación para el desarrollo sustentable

	PRINCIPIOS
INCLUSIÓN: COBERTURA Y ACCESIBILIDAD UNIVERSAL	1. Garantizar la cobertura universal de las personas desde el nacimiento hasta la muerte, sin discriminación. 2. Eliminar las barreras de acceso y uso y las disparidades en la disponibilidad de información y tecnología.
DISEÑO: ROBUSTO, SEGURO, SENSIBLE Y SOSTENIBLE	3. Establecer una identidad robusta, única, segura y precisa. 4. Crear una plataforma interoperable y que responda a las necesidades de los distintos usuarios. 5. Utilizar estándares abiertos y garantizar la neutralidad tecnológica y de los proveedores. 6. Proteger la privacidad y el control del usuario mediante el diseño del sistema. 7. Planificar la sostenibilidad financiera y operativa sin comprometer la accesibilidad
GOBERNABILIDAD: CREAR CONFIANZA PROTEGIENDO LA PRIVACIDAD Y LOS DERECHOS DE LOS USUARIOS	8. Salvaguardar la privacidad de los datos, la seguridad y los derechos de los usuarios a través de un marco jurídico y normativo completo. 9. Establecer mandatos institucionales claros y responsabilidad. 10. Hacer cumplir los marcos legales y de confianza a través de la supervisión independiente y la resolución de quejas.

Meta 1. Garantizar la inclusión

Los dos primeros principios pretenden garantizar que nadie se quede atrás en los sistemas de identificación, en apoyo del SDG 16.9. El *Principio 1* exige a los países que cumplan sus obligaciones de proporcionar una identificación legal a todos los residentes (no sólo a los ciudadanos) desde el nacimiento hasta la muerte y sin discriminación, tal y como se establece en el derecho y las convenciones internacionales y en sus propios marcos legislativos. Esto incluye el compromiso de un registro de nacimiento universal para los nacidos en su territorio o jurisdicción, pero también se extiende a los sistemas de identidad digital, especialmente cuando éstos son un requisito previo para acceder a servicios básicos del sector público y privado, como la banca, las tarjetas SIM y las transferencias de efectivo.

En reconocimiento del hecho de que ciertos grupos se enfrentarán a dificultades desproporcionadas en el acceso a los servicios de identidad, y a los servicios digitales en particular, el *Principio 2* requiere que los profesionales identifiquen y mitiguen las barreras legales, de procedimiento y sociales para inscribirse y utilizar los sistemas de identidad digital, con especial atención a las personas y grupos pobres que pueden estar en riesgo de exclusión

60 Banco Mundial 2017. *Principios sobre la identificación para el desarrollo sustentable Hacia la era digital.* Washington, DC. Grupo del Banco Mundial id4d.worldbank.org/principles. Se puede encontrar una lista de organizaciones que los respaldan en el sitio web.

por razones culturales, políticas o de otro tipo (como las mujeres y las minorías de género, los niños, las poblaciones rurales, las minorías étnicas, los grupos lingüísticos y religiosos, las personas con discapacidad, los migrantes, los desplazados forzosos y los apátridas). Además, los sistemas de identidad digital y los datos de identidad no deben utilizarse como instrumento de discriminación ni vulnerar los derechos individuales o colectivos.

Meta 2. Diseñar sistemas de identificación robustos, seguros, sensibles y sostenibles

Además de proporcionar una cobertura universal, los sistemas de identidad digital deben ser robustos frente al fraude y los errores, útiles para una variedad de partes interesadas y sostenibles, al tiempo que protegen la privacidad del usuario y adoptan estándares abiertos para facilitar la innovación y evitar el bloqueo de proveedores y tecnologías.

En concreto, el *Principio 3* establece que una información de identidad precisa y actualizada es esencial para garantizar la fiabilidad de las identidades y los atributos utilizados en las transacciones. Además, las identidades deben ser únicas en el contexto, evitando duplicaciones o el uso de identificadores que puedan ser atribuidos a múltiples personas. Además, los sistemas de identidad digital deben contar con salvaguardas contra la manipulación (alteración u otros cambios no autorizados en los datos o credenciales), la usurpación de la identidad, el mal uso de los datos y otros errores que se produzcan a lo largo del ciclo de vida de la identidad.

El *Principio 4* destaca la necesidad de que los servicios de identificación y autenticación sean flexibles, escalables y respondan a las necesidades y preocupaciones de las personas (usuarios) y de las partes que confían en ellos (por ejemplo, organismos públicos y empresas privadas). Para garantizar que los sistemas y servicios relacionados con la identidad satisfagan las necesidades específicas de los usuarios, los profesionales deben involucrar al público y a las partes interesadas importantes a lo largo de la planificación y la implementación. El valor de los sistemas de identidad digital para las partes que confían depende en gran medida de su portabilidad e interoperabilidad con múltiples entidades, sujetas a las salvaguardias de privacidad y seguridad adecuadas, tanto dentro de un país como a través de las fronteras.

Para la identidad digital reconocida por el gobierno en particular, el Principio 5 enfatiza aún más la necesidad de la neutralidad del proveedor para aumentar la flexibilidad y evitar el diseño del sistema que no es adecuado para el propósito o adecuado para cumplir con los objetivos de política y desarrollo. Esto requiere unas directrices de contratación sólidas para facilitar la competencia y la innovación y evitar el posible «bloqueo» de la tecnología y del proveedor, que puede aumentar los costos y reducir la flexibilidad para adaptarse a los cambios con el tiempo. Además, los principios de diseño abierto permiten la competencia y la innovación basadas en el mercado. Son esenciales para una mayor eficiencia y una mejor funcionalidad de los sistemas de identidad digital, así como para una interoperabilidad duradera. Del mismo modo, las API abiertas también apoyan el intercambio eficiente de datos y la portabilidad, garantizando que un componente del sistema de identidad digital, por ejemplo, un tipo particular de credencial, pueda ser reemplazado con una interrupción mínima.

Además de una arquitectura sensible y flexible, el *Principio 6* subraya que los sistemas de identidad digital deben proteger la privacidad de las personas y el control de sus datos mediante el diseño del sistema. Esto es crucial para mitigar muchos de los riesgos para la privacidad y la protección de datos identificados en la Sección IV de esta Guía. Diseñar teniendo en cuenta la privacidad de las personas significa que no debería ser necesaria ninguna acción por parte del individuo para proteger sus datos personales. La información debe estar protegida de un uso indebido y no autorizado por defecto, tanto mediante normas técnicas como mediante prácticas empresariales preventivas.

Estas medidas deben complementarse con un marco jurídico sólido (como se subraya más adelante en el *Principio 8*).

Por ejemplo, los datos recogidos y utilizados para la identificación y la autenticación deben ser adecuados para el propósito, proporcionales al caso de uso y gestionados de acuerdo con las normas mundiales de protección de datos, como las Prácticas Justas de Información (FIP) de la OCDE y con referencia a las mejores prácticas internacionales emergentes, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea o la Ley de Privacidad del Consumidor de California. Los protocolos de autenticación sólo deben proporcionar una confirmación de «sí o no» de una identidad declarada o, si lo exige una ley relacionada con la lucha contra el lavado de activos o la delincuencia organizada, sólo revelar los datos mínimos necesarios para la transacción. El método de autenticación debe reflejar una evaluación del nivel de riesgo de las transacciones y puede basarse en normas y marcos internacionales reconocidos para los niveles de garantía. Además, los sistemas de numeración de credenciales e identificadores no deben revelar innecesariamente información personal sensible (por ejemplo, los números de referencia deben ser aleatorios).

El *Principio 7* reconoce la importancia de diseñar sistemas del sector público que sean sostenibles desde el punto de vista financiero y operativo, manteniendo al mismo tiempo la accesibilidad para las personas y las partes que confían en ellos. Esto puede implicar diferentes modelos de negocio, incluyendo tarifas razonables y apropiadas para los servicios de verificación de la identidad, ofreciendo servicios mejorados o acelerados a los usuarios, asociaciones público-privadas (APP) cuidadosamente diseñadas y gestionadas, recuperando los costos a través de la eficiencia y el aumento de la productividad y la reducción de las fugas, y otras fuentes de financiación que no comprometan el objetivo de proporcionar una prueba de identidad que sea accesible para todos y satisfaga las necesidades de las personas y las partes que confían.

Meta 3. Crear confianza protegiendo la privacidad y los derechos de los usuarios

El último grupo de principios aborda cómo deben gobernarse los sistemas de identidad digital para proteger la privacidad y los derechos de los usuarios, la seguridad del sistema y una clara responsabilidad y supervisión.

El *Principio 8* establece los requisitos de un marco jurídico completo. Los sistemas de identidad digital deben estar respaldados por políticas, leyes y reglamentos que promuevan la confianza en el sistema, garanticen la privacidad y la seguridad de los datos, mitiguen los abusos, como la vigilancia no autorizada en violación del debido proceso, y garanticen la responsabilidad del proveedor. Esto suele incluir una ley de habilitación y reglamentos para el propio sistema de identidad digital, así como leyes y reglamentos sobre la protección de datos, el gobierno digital o electrónico, las transacciones y el comercio electrónicos, la lucha contra el lavado de activos, el registro civil, los sistemas de identificación de propósito limitado y la libertad de información, entre otros.

La ley y los reglamentos de habilitación de un sistema de identidad digital deben describir claramente la finalidad del sistema, sus componentes, las funciones y responsabilidades de las diferentes partes interesadas, cómo y qué datos se van a recopilar, la responsabilidad y los recursos de los titulares de la identidad digital (sujetos) y las partes que confían en ella, las circunstancias en las que se pueden compartir los datos, la corrección de los atributos de datos inexactos y cómo se mantendrá la inclusión y la no discriminación. Las leyes y reglamentos sobre protección de datos y privacidad deben incluir también la supervisión de un organismo de control independiente (por ejemplo, una comisión nacional de privacidad) con los poderes adecuados para proteger a los sujetos contra el acceso y el uso inapropiados de sus datos por parte de terceros para la vigilancia comercial o la elaboración de perfiles sin consentimiento informado o una finalidad legítima. Los marcos requieren un equilibrio adecuado entre los modelos reguladores y autorreguladores que no repriman la competencia, la innovación o la inversión.

Además, el Principio 9 destaca la necesidad de mandatos institucionales claros y de responsabilidad en la gobernanza de los sistemas de identidad digital. Los marcos de confianza de todo el ecosistema deben establecer y regular los acuerdos de gobernanza para los sistemas de

identificación. Esto debe incluir la especificación de los términos y condiciones que rigen las relaciones institucionales entre las partes participantes, de modo que los derechos y responsabilidades de cada uno estén claros para todos. Debe haber una clara rendición de cuentas y transparencia en torno a las funciones y responsabilidades de los proveedores de sistemas de identificación.

Por último, el *Principio 10* subraya que el sistema de identificación debe incluir disposiciones claras para la supervisión de estos requisitos legales y reglamentarios. El uso de los sistemas de identificación debe ser supervisado de forma independiente (en cuanto a eficacia, transparencia, exclusión, uso indebido, etc.) para garantizar que todas las partes interesadas utilicen adecuadamente los sistemas de identificación para cumplir con los fines previstos, supervisar y responder a las posibles violaciones de los datos, y recibir las quejas o preocupaciones individuales sobre el tratamiento de los datos personales. Además, los litigios relacionados con la identificación y el uso de los datos personales que no sean resueltos satisfactoriamente por los proveedores, por ejemplo, la negativa a registrar a una persona o a corregir los datos, o la determinación desfavorable del estatus legal de una persona, deberían estar sujetos a una revisión rápida y de bajo costo por parte de autoridades administrativas y judiciales independientes con autoridad para proporcionar una reparación adecuada.

ANEXO D: MARCO DE GARANTÍA DE IDENTIDAD DIGITAL Y ORGANISMOS DE NORMALIZACIÓN TÉCNICA

Esta lista no incluye los organismos nacionales o regionales, como el eIDAS y el NIST, que también han desarrollado marcos y normas a nivel nacional/regional (véase el Apéndice E).

La **Organización Internacional de Normalización (ISO)** es una organización internacional independiente con sede en Ginebra, que cuenta con 163 entidades nacionales de normalización (una por país) y que elabora normas internacionales voluntarias, basadas en el consenso y relevantes para el mercado, que proporcionan especificaciones para productos, servicios y sistemas, con el fin de garantizar la calidad, la seguridad y la eficiencia y apoyar la innovación. Algunas de las normas pertinentes son: prueba de identidad y registro de personas físicas (ISO/IEC 29003:2018); marco de garantía de autenticación de entidades (ISO/IEC 29115:2013 en revisión) y la aplicación de las directrices de gestión de riesgos (ISO 31000:2018) a los riesgos relacionados con la identidad. A través de su recién convocado Grupo de Trabajo 7 TC68[61], ISO está trabajando actualmente en normas globales para la identificación de personas físicas, incluso en el contexto digital.

La **Unión Internacional de Telecomunicaciones (UIT)** es el organismo de las Naciones Unidas especializado en tecnologías de la información y la comunicación (TIC), fundado para facilitar la conectividad internacional en las redes de comunicaciones. La UIT atribuye el espectro radioeléctrico mundial y las órbitas de los satélites y elabora normas técnicas destinadas a garantizar la interconexión sin fisuras de las redes y tecnologías de las TIC en todo el mundo.

El **Consorcio de la World Wide Web (W3C)** es una organización internacional que desarrolla y promueve una amplia gama de normas y protocolos técnicos abiertos, voluntarios y basados en el consenso, para que Internet apoye la interoperabilidad, la escalabilidad, la estabilidad y la resistencia. En el ámbito de la identidad digital, el W3C ha desarrollado el estándar de navegador/plataforma de autenticación web para la MAF, que utiliza la biometría, los dispositivos móviles y las claves de seguridad FIDO, y está desarrollando estándares para las declaraciones de identidad verificadas en los sistemas de identidad descentralizados.

La **Alianza Fast Identity Online (FIDO)** es una asociación de la industria que promueve soluciones de autenticación sólidas, eficaces y fáciles de usar, mediante el desarrollo de especificaciones técnicas que definen un conjunto de mecanismos abiertos, escalables e interoperables para autenticar a los usuarios; el funcionamiento de programas de certificación de la industria para ayudar a garantizar la adopción exitosa de las especificaciones en todo el mundo; y la presentación de especificaciones técnicas maduras a organizaciones de desarrollo de normas reconocidas (por ejemplo, ISO, ITU X.1277 y X.1278) para su estandarización formal. FIDO también participa en la verificación a través de su Grupo de Trabajo de Verificación y Vinculación de la Identidad (IDWG).

La **OpenID Foundation (OIDF)** es una organización comercial sin fines de lucro, independiente de la tecnología, que se dedica a promover la adopción de servicios de identidad digital basados en estándares abiertos.

61 ISO/TC68 es el Comité Técnico de ISO encargado de desarrollar y mantener las normas internacionales que cubren las áreas de banca, valores y otros servicios financieros.

GSMA es la asociación mundial de la industria de los operadores de redes de comunicaciones móviles, y participa en el desarrollo de una serie de normas técnicas aplicables a las plataformas de comunicaciones móviles, incluidas las normas de identificación y autenticación de usuarios.

El **Instituto Europeo de Normas de Telecomunicaciones (ETSI)** es uno de los tres principales organismos europeos de normalización, junto con el CEN y el CENELEC. El ETSI ofrece a sus miembros un entorno abierto e inclusivo para apoyar el desarrollo, la ratificación y la comprobación de normas aplicables a nivel mundial para sistemas y servicios de TIC en todos los sectores de la industria y la sociedad. El ETSI ha estado trabajando en la comprobación de la identidad, principalmente dirigida a los servicios de confianza definidos por el eIDAS, con aplicación potencial en otras áreas como la emisión de la identificación electrónica y los procesos de DDC. El ETSI ha desarrollado un conjunto de normas para aplicar los requisitos del RTS en el marco de la PSD2 para el uso de los certificados cualificados definidos en el eIDAS para identificar a terceros (TPP) en las operaciones de pago.

ANEXO E: DESCRIPCIÓN GENERAL DE LOS MARCOS DE GARANTÍA DIGITAL DE EE. UU. Y LA UE Y ESTÁNDARES TÉCNICOS

NIST – Estados Unidos

- El nivel de garantía de la identidad (IAL) se refiere a la fiabilidad del proceso de comprobación de la identidad, según los requisitos técnicos de la identidad digital que requiere. Los niveles de garantía para la comprobación de la identidad, en orden de fiabilidad creciente, son IAL1; IAL2; y IAL3;
- El Nivel de Garantía de Autenticación (AAL) se refiere a la fiabilidad del proceso de autenticación. Los niveles de garantía para la autenticación (y la gestión del ciclo de vida de las credenciales), por orden de fiabilidad creciente, son AAL1; AAL2; y AAL3; y
- El nivel de garantía de la federación (FAL) (si procede) se refiere a la fiabilidad de la red federada, es decir, a la fiabilidad (solidez) de una afirmación utilizada para comunicar los resultados de la autenticación y la información de atributos de identificación en un entorno federado. Los niveles de garantía para la federación, en orden de fiabilidad creciente, son FAL1; FAL2; y FAL3;

Comprobación de identidad

Cuadro 18. Aprovechamiento de las normas técnicas de identidad digital del NIST para evaluar la fiabilidad de la comprobación de la identidad

IAL1: No es necesario vincular al solicitante con una identidad concreta de la vida real, es decir, no hay garantía de que el solicitante sea quien dice ser, porque no se requiere ninguna prueba de identidad. Esto significa que:

- No se requieren atributos de identidad;
- El solicitante puede, pero no es necesario, autoafirmar los atributos de identidad.
- Si se proporcionan o recogen atributos, se autoafirman o se tratan como autoafirmados y no se validan o verifican.

IAL2: Existe un alto grado de confianza en que las pruebas de identidad son auténticas, en que la información de atributos que contienen es exacta y en que se refieren al solicitante.

- Las pruebas de atributos de identidad se recogen en función de la calidad de las pruebas (débil, regular, reforzada y superior) y del número de documentos o información digital en que se basan.
- Las pruebas de identidad se validan como auténticas.
- Las pruebas de identidad y los atributos de identidad que contienen respaldan la existencia en el mundo real de la identidad reivindicada, y

- Las pruebas de identidad se verifican, confirmando que la identidad validada se refiere a la persona (solicitante), incluida la confirmación de la dirección.
- Se permite la comprobación de la identidad a distancia o en persona. NB: En las normas de identidad digital del NIST, la comprobación de la identidad «en persona» incluye las **interacciones remotas supervisadas con el solicitante**, así como las interacciones en las que el solicitante y el proveedor de servicios de identidad están físicamente presentes en el mismo lugar (véase la discusión más adelante).
- La biometría es opcional
- En los casos en los que una persona no pueda cumplir los requisitos convencionales de comprobación de identidad, como los requisitos de prueba de identidad, se puede utilizar un árbitro de confianza para ayudar a comprobar la identidad del solicitante.
- Las pruebas de los atributos de identidad deben cumplir con los requisitos de calidad de las pruebas especificados, lo que permite varias combinaciones de números requeridos de piezas de prueba con una fuerza determinada, determinada por las características especificadas.

IAL3: Hay una confianza muy alta en que las pruebas de identidad son auténticas y precisas; que los atributos de identidad pertenecen a una persona del mundo real, y que el solicitante es esa persona y está adecuadamente asociado con esta identidad del mundo real.

- La comprobación de la identidad debe ser presencial; NB: La comprobación de la identidad «en persona» incluye las interacciones remotas supervisadas con el solicitante, así como las interacciones en las que el solicitante y el proveedor de servicios de identidad están físicamente presentes en el mismo lugar. (Véase el análisis de la admisión no presencial en la Sección III)
- Los requisitos de calidad de las pruebas de identidad son más rigurosos
  - Requiere más pruebas de identidad adicionales con mayor solidez
  - La biometría es obligatoria. Se requieren atributos de identidad y procesos biométricos para detectar inscripciones fraudulentas o duplicadas y como mecanismo para vincular la identidad verificada a una credencial
- Los atributos de identidad deben ser verificados por un representante autorizado y capacitado del proveedor de servicios de credenciales (CSP).

Fuente: Normas del NIST de los Estados Unidos

Tabla 4. Resumen de los requisitos de comprobación de la identidad para IAL 1, IAL2 e IAL 3

Requisito	IAL1	IAL2	IAL3
Presencia	Sin requisitos	En persona y remoto sin supervisión.	En persona y remoto con supervisión.
Resolución	Sin requisitos	• Los mínimos atributos necesarios para conseguir la resolución de la identidad. • Se puede utilizar la KBV para aumentar la confianza.	Igual que IAL2
Pruebas	No se recaban pruebas de de identidad.	• Una prueba SUPERIOR o REFORZADA dependiendo de solidez de la prueba original y la validación ocurre al emitir la fuente, O • Dos pruebas REFORZADA, O • Una prueba REFORZADA Más dos (2) pruebas JUSTA	• Dos pruebas SUPERIOR O • Una prueba SUPERIOR y una prueba REFORZADA según la fuerza de la prueba original y la validación ocurre cuando se emite el origen, O • Dos pruebas REFORZADAS más una pieza de prueba JUSTA.
Validación	Sin validación	Cada prueba debe ser validada con un proceso que sea capaz de alcanzar la misma fuerza que la prueba presentada.	Igual que IAL2
Verificación	Sin verificación	Verificado por un proceso que sea capaz de alcanzar una fuerza de REFORZADA.	Verificado por un proceso que sea capaz de alcanzar una fuerza de SUPERIOR.
Confirmación del domicilio	Sin requisitos para la confirmación del domicilio	Obligatorio. Código de inscripción enviado a cualquier dirección registrada. La notificación se envía mediante medios distintos que el código de inscripción.	Obligatorio. Notificación de comprobación al domicilio postal.
Biométrico Recolección	No	Opcional	Obligatorio
Controles de seguridad	N/D	• Línea de base moderada (o norma federal o industrial equivalente)	• Línea de base alta (o norma federal o industrial equivalente)

Cuadro 19. Comprobación e inscripción de la identidad en persona

Como se ha señalado anteriormente, las normas técnicas permiten la acreditación de la identidad en persona en el IAL2 y la exigen en el IAL3. Es importante, incluso con respecto a los objetivos de inclusión financiera, que la comprobación e inscripción de identidad en persona puedan llevarse a cabo mediante:

- Una interacción física con el solicitante, supervisada por un operador; o
- Una *interacción a distancia* con el solicitante, *supervisada por un operador*, basada en los requisitos especificados para la comprobación de la identidad en persona a distancia, que alcanza niveles de confianza y seguridad comparables a los de la comprobación de la identidad en persona (interacción física).

Para cualquiera de los dos tipos de comprobación de identidad en persona, las normas técnicas exigen que (1) el operador debe inspeccionar la fuente biométrica (por ejemplo, los dedos, la cara) para detectar la presencia de materiales no naturales como parte del proceso de comprobación; (2) el CSP debe recoger los datos biométricos de forma que se garantice que los datos biométricos se recogen del solicitante y no de otro sujeto y que se aplican todos los requisitos de rendimiento biométrico establecidos en las normas.

Requisitos de comparabilidad para la comprobación e inscripción de identidad en persona a distancia, bajo supervisión

Para establecer la comparabilidad entre la comprobación de la identidad y el registro en persona a distancia supervisados, y la comprobación de la identidad y el registro cuando el solicitante se encuentra en la misma ubicación física que el CSP, deben cumplirse los siguientes requisitos (además de los requisitos de validación y verificación de la IAL3, mencionados anteriormente):

El CSP debe:

- Supervisar toda la sesión de comprobación de identidad (por ejemplo, mediante una transmisión continua de vídeo de alta resolución del solicitante).
- Disponer de un operador en directo que participe a distancia con el solicitante durante toda la sesión de comprobación de identidad. Los operadores deben haber recibido un programa de formación para detectar posibles fraudes y realizar correctamente una sesión de comprobación virtual durante el proceso.
- Hacer que toda la verificación digital de las pruebas (por ejemplo, mediante tecnologías de chip o inalámbricas) se realice mediante escáneres y sensores integrados.
- Garantizar que todas las comunicaciones se produzcan a través de un canal protegido y autentificado mutuamente.
- Emplear características físicas de detección y resistencia a la manipulación apropiadas para el entorno en el que se produce la sesión de comprobación de identidad (por ejemplo, un quiosco situado en una zona restringida o supervisado por una persona de confianza requiere menos detección física de manipulación que uno situado en una zona semipública, como la explanada de un centro comercial).

El solicitante debe permanecer continuamente en la sesión de comprobación de identidad supervisada (no puede salir de ella) y todas las acciones realizadas por el solicitante durante la sesión de comprobación de identidad deben ser claramente visibles para el operador remoto.

Cuadro 20. Autenticación y gestión del ciclo de vida

Los NIVELES DE ASEGURAMIENTO DE LA AUTENTICACIÓN (AAL) establecen los requisitos técnicos para (1) los protocolos y procesos de autenticación (incluida la emisión y vinculación de credenciales y autenticadores) y (2) la gestión del ciclo de vida de los autenticadores (incluida la revocación en caso de pérdida o robo, y la caducidad/reprobación y revinculación). Una autenticación más fuerte (un AAL más alto) requiere que los agentes maliciosos tengan mejores capacidades y gasten más recursos para subvertir con éxito el proceso de autenticación. La autenticación con AAL más altos puede reducir eficazmente el riesgo de suplantación, repetición y otros ataques que pueden llevar a reclamaciones fraudulentas de la identidad digital de un sujeto. Los AAL incluyen requisitos técnicos para los tipos de autenticadores; criptografía aprobada y canales de autenticación seguros (incluidos los requisitos de detección de compromiso, suplantación y resistencia a la repetición); reautenticación de sesiones de abonado (ampliadas); conservación de registros; ciberseguridad; y privacidad. Los AAL también establecen requisitos para la vinculación de los autenticadores a una identidad probada y para las acciones que deben tomarse en respuesta a los eventos que pueden ocurrir a lo largo del ciclo de vida del autenticador de un abonado que van a la confiabilidad del autenticador después de la vinculación, incluyendo la pérdida, el robo, la duplicación no autorizada, la expiración y la revocación. Muchos de estos requisitos son muy técnicos e incorporan por referencia otras normas de seguridad de la información muy técnicas.

El siguiente resumen describe a un alto nivel de generalidad sólo algunos de los requisitos para la autenticación en varios AAL. Véase el NIST 800-63(b) para una discusión detallada.

- AAL1: Proporciona *cierta garantía* de que el solicitante (la persona que afirma (reclama) su identidad para la autorización de la cuenta) controla un autenticador o autenticadores vinculados a la cuenta del abonado. AAL1 permite una amplia gama de tecnologías de autenticación y tipos de autenticadores, así como controles de seguridad de la información en una *línea de base baja*. MFA es opcional). La biometría por sí sola puede utilizarse como autenticador de factor único en AAL1.

- AAL2: Proporciona una *alta confianza* en que el solicitante controla el autenticador o autenticadores vinculados a la cuenta del cliente/abonado. Requiere MFA (ya sea un autenticador de múltiples factores o dos autenticadores de un solo factor), utilizando protocolo(s) de autenticación seguro(s) que incorpore(n) técnicas criptográficas aprobadas especificadas, y controles de seguridad de la información en una línea de base *moderada*. El AAL2 impone requisitos más estrictos a los tipos de autenticadores que el AAL1.[62] La biometría puede utilizarse como un *factor* de autenticación

62 AAL2 permite el uso de cualquiera de los siguientes autenticadores multifactor: dispositivo OTP multifactor; software criptográfico multifactor; o dispositivo criptográfico multifactor. Cuando se utiliza una combinación de dos autenticadores de factor único, un autenticador debe ser un autenticador secreto memorizado y el otro debe estar basado en la posesión (es decir, «algo que se tiene») y utilizar cualquiera de los siguientes: secreto de búsqueda; dispositivo fuera de banda; dispositivo OTP de factor único; software criptográfico de factor único; o dispositivo criptográfico de factor único.

(algo que se es), con el dispositivo autenticado como segundo factor (algo que se tiene), pero no puede servir como único tipo de autenticador.

- AAL3: Proporciona una *confianza muy alta* en que el solicitante controla el autenticador o autenticadores vinculados a la cuenta del abonado. AAL3 requiere una MFA que utilice tanto un autenticador basado en hardware como un autenticador que ofrezca resistencia a la suplantación de identidad por parte de un verificador (VIR), basado en la prueba de la posesión de una clave a través de un protocolo criptográfico aprobado.[63] Los solicitantes deben demostrar la posesión y el control de dos factores de autenticación distintos a través de uno o varios protocolos de autenticación seguros, utilizando técnicas criptográficas aprobadas. Los autenticadores deben ser resistentes a la suplantación del verificador, a la repetición y a los ataques secundarios pertinentes. (verificador) deberá determinar por sí mismo que el sensor biométrico y el posterior procesamiento cumplen los requisitos de rendimiento especificados. El CSP debe emplear controles de seguridad adecuadamente adaptados a una línea de base *elevada*.

eIDAS – Unión Europea

El marco del eIDAS prevé tres niveles de garantía para los medios de identificación electrónica suministrados en el marco de un sistema de identificación electrónica notificado: bajo, sustancial y alto. El Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015, establece las especificaciones mínimas de seguridad para cada uno de estos niveles. Se ha tenido en cuenta la norma internacional ISO/IEC 29115 para las especificaciones y procedimientos establecidos en el presente acto de ejecución por ser la principal norma internacional disponible en el ámbito de los niveles de seguridad para los medios de identificación electrónica. El contenido del Reglamento eIDAS difiere de dicha norma internacional, en particular en lo que respecta a los requisitos de prueba y verificación de la identidad, así como a la forma en que se tienen en cuenta las diferencias entre los dispositivos de identidad de los Estados miembros y las herramientas existentes en la UE para el mismo fin. Si, en un país de la UE/EEE, un organismo del sector público requiere, para acceder a uno de sus servicios en línea, una identificación electrónica con un nivel de garantía sustancial o alto, también tiene que aceptar, para acceder a este servicio en línea, todos los medios de identificación electrónica con un nivel de garantía igual o superior y relativos a un sistema de identificación notificado a la Comisión y publicado en el DO (Diario Oficial de la Unión Europea). Además, los organismos del sector público pueden decidir, de forma voluntaria, reconocer los sistemas de identificación electrónica con un nivel de garantía bajo.

63 El solicitante utiliza una clave privada almacenada en el autenticador para demostrar la posesión y el control de este. Un IDSP (verificador), que conoce la clave pública del solicitante a través de alguna credencial (normalmente, un certificado de clave pública), utiliza un protocolo de autenticación criptográfica aprobado para verificar que el solicitante tiene la posesión y el control del autenticador de clave privada asociado, y afirma la identidad verificada de la persona a la RP.

A efectos del eIDAS, los componentes de un sistema de identidad digital son los siguientes:

- La **inscripción** asegura la identificación que representa de forma única a una persona física o jurídica, o a una persona física que representa a una persona jurídica. La inscripción implica diferentes pasos:
  - Solicitud y registro: (1) Asegurarse de que el solicitante conoce los términos y condiciones relacionados con el uso de los medios de identificación electrónica. (2) Asegurarse de que el solicitante conoce las precauciones de seguridad recomendadas en relación con los medios de identificación electrónica. (3) Recoger los datos de identidad pertinentes necesarios para la comprobación y verificación de la identidad.
  - La comprobación y verificación de la identidad, que consiste en la verificación de la autenticidad y validez del documento de identidad, y se refiere a una persona real, y la verificación de que la identidad de esa persona es la identidad reclamada.
- Gestión de los medios de **identificación electrónica**, trata del número y la naturaleza de los factores de autenticación, de si el medio de identificación electrónica está diseñado para que se pueda suponer que sólo se utiliza si está bajo el control o la posesión de la persona a la que pertenece, la revocación y la renovación de este.
- La **autenticación** establece los requisitos por nivel de garantía con respecto al mecanismo de autenticación, a través del cual la persona física o jurídica utiliza los medios de identificación electrónica para confirmar su identidad a una parte que confía.
- **Gestión y organización**, todos los participantes que presten un servicio relacionado con la identificación electrónica en un contexto transfronterizo deberán contar con prácticas documentadas de gestión de la seguridad de la información, políticas, enfoques de la gestión de riesgos y otros controles reconocidos, a fin de garantizar a los órganos de gobernanza apropiados para los sistemas de identificación electrónica en los respectivos Estados miembros que se aplican prácticas eficaces.

Para cada una de estas cuatro etapas, se definen tres niveles de garantía, bajo, sustancial y alto, de acuerdo con los siguientes criterios:

- **Bajo**: proporciona un grado limitado de confianza en la identidad declarada o afirmada de una persona, y se caracteriza por hacer referencia a las especificaciones técnicas, las normas y los procedimientos relacionados con ella, incluidos los controles técnicos, cuyo objetivo es disminuir el riesgo de uso indebido o alteración de la identidad;
- **Sustancial**: proporciona un grado sustancial de confianza en la identidad declarada o afirmada de una persona, y se caracteriza por hacer referencia a las especificaciones técnicas, las normas y los procedimientos relacionados con ella, incluidos los controles técnicos, cuyo objetivo es disminuir sustancialmente el riesgo de uso indebido o alteración de la identidad;
- **Alto**: proporciona un grado más alto de confianza en la identidad declarada o afirmada de una persona que el medio de identificación electrónica con el nivel de garantía sustancial, y se caracteriza por hacer referencia a las especificaciones técnicas, las normas y los procedimientos relacionados con ella, incluidos los controles técnicos, cuyo objetivo es prevenir el uso indebido o alteración de la identidad.

Se presume que cuando los medios de identificación electrónica emitidos en el marco de un sistema de identificación electrónica notificado cumplen un requisito enumerado en un nivel de garantía superior, entonces cumplen el requisito equivalente de un nivel de garantía inferior.

Tabla 5. Requisitos para la autenticación según los niveles de garantía del eIDAS

NIVEL DE GARANTÍA	ELEMENTOS NECESARIOS
BAJO	• La divulgación de los datos de identificación de la persona va precedida de una verificación fiable de los medios de identificación electrónica y de su validez. • Cuando los datos de identificación de la persona se almacenan como parte del mecanismo de autenticación, esa información está asegurada para protegerla contra la pérdida y el compromiso, incluido el análisis fuera de línea. • El mecanismo de autenticación implementa controles de seguridad para la verificación de los medios de identificación electrónica, de modo que es muy poco probable que actividades como la adivinación, la escucha, la reproducción o la manipulación de la comunicación por parte de un atacante con potencial de ataque básico mejorado puedan subvertir los mecanismos de autenticación.
Nivel SUSTANCIAL	Nivel bajo, más: • La divulgación de los datos de identificación de la persona va precedida de una verificación fiable de los medios de identificación electrónica y de su validez mediante una autenticación dinámica. • El mecanismo de autenticación implementa controles de seguridad para la verificación de los medios de identificación electrónica, de modo que es muy poco probable que actividades como la adivinación, la escucha, la reproducción o la manipulación de la comunicación por parte de un atacante **con potencial de ataque moderado** puedan subvertir los mecanismos de autenticación.
Nivel ALTO	Nivel sustancial, más: • El mecanismo de autenticación implementa controles de seguridad para la verificación de los medios de identificación electrónica, de modo que es muy poco probable que actividades como la adivinación, la escucha, la reproducción o la manipulación de la comunicación por parte de un atacante **con potencial de ataque alto** puedan subvertir los mecanismos de autenticación.

GLOSARIO

Aplicación: programa informático diseñado para ayudar a un usuario a realizar tareas específicas.

Interfaz de programación de aplicaciones (API): conjunto de definiciones y protocolos para construir e integrar software de aplicación. Las API permiten que los productos o servicios digitales se comuniquen fácilmente con otros productos y servicios.

Niveles de seguridad o niveles de garantía: se refiere al nivel de confianza en la fiabilidad de cada una de las tres etapas del proceso de identidad digital. Véase la visión general de las normas técnicas en la Sección II del informe y «Aprovechamiento de las normas técnicas de identidad digital para aplicar el EBR» en la Sección V del informe.

Las **pruebas de atributos** pueden ser físicas (documentales) o puramente digitales, o una representación digital de pruebas de atributos físicas (por ejemplo, una representación digital de un permiso de conducir de papel o plástico).

La **autenticación** establece que el solicitante que afirma su identidad es la misma persona cuya identidad se obtuvo, verificó y acreditó durante la admisión.

Un **autenticador** es algo que el demandante posee y controla y que se utiliza para autenticar (confirmar) que el demandante es la persona a la que se le ha expedido una credencial y, por tanto, (en función de la solidez del componente de autenticación del sistema de identidad digital) es (con distintos grados de probabilidad, especificados por el nivel de garantía de autenticación) el abonado real y el titular de la cuenta.

Biometría

- Atributos biométricos físicos, como huellas dactilares, patrones de iris, huellas vocales y reconocimiento facial, todos ellos estáticos.
- Atributos biométricos biomecánicos, como la mecánica de las pulsaciones de las teclas, que son el producto de interacciones únicas de los músculos, el sistema esquelético y el sistema nervioso de un individuo, todos ellos dinámicos.
- Patrones biométricos de comportamiento: atributos basados en la nueva disciplina de ciencias sociales computacionales de la física social, consisten en los diversos patrones de movimiento y uso de un individuo en flujos de datos temporales geoespaciales, e incluyen, por ejemplo, los patrones de correo electrónico o mensajes de texto de un individuo, el uso del teléfono móvil, los patrones de geolocalización y el registro de acceso a archivos.

La **recopilación y resolución** forman parte de la comprobación de la identidad e implican la obtención de atributos (identificadores), la recopilación de pruebas de atributos y la resolución de las pruebas de identidad y de los atributos a una única identidad dentro de una población o un contexto determinados.

La **autenticación continua** es una forma dinámica de autenticación. Puede aprovechar la biometría biomecánica, los patrones biométricos de comportamiento y/o el Análisis de Riesgo de Transacción dinámico para centrarse en garantizar que determinados puntos de datos recogidos a lo largo de una interacción en línea con una persona (como la geolocalización, las direcciones MAC e IP, la cadencia de tecleo y el ángulo del dispositivo móvil) coincidan con «lo que debería esperarse» durante toda la sesión.

Un **solicitante** es una persona que busca probar su identidad y obtener los derechos asociados a esa identidad (por ejemplo, para abrir o acceder a una cuenta financiera). Un Solicitante también puede ser descrito como el abonado que afirma la propiedad de una identidad a una parte que confía (RP) y busca que se verifique, utilizando protocolos de autenticación.

Una **credencial** es un objeto físico o una estructura digital que vincula de forma autorizada la identidad probada de un abonado, a través de un identificador o identificadores, con al menos un autentificador que posee y controla el abonado.

Proveedor de servicios de credenciales (CSP): Entidad que emite y/o registra autenticadores y las correspondientes credenciales electrónicas (que vinculan los autenticadores a la identidad verificada) a los abonados. El CSP es responsable de mantener la credencial de identidad del abonado y todos los datos de inscripción asociados durante el ciclo de vida de la credencial y de proporcionar información sobre el estado de la credencial a los verificadores.

Relleno de credenciales (también llamado breach replay o limpieza de listas): Tipo de ciberataque en el que se comprueban las credenciales de cuentas robadas (a menudo procedentes de una violación de datos) para ver si coinciden con las de otros sistemas. Este tipo puede tener éxito si la víctima ha utilizado la misma contraseña (que fue robada en la violación de datos) para otra cuenta.

Desduplicación: El proceso de resolver las pruebas de identidad y los atributos a una única identidad dentro de una población o contexto(s) determinado(s).

Los **sistemas de identidad digital,** a efectos de esta Guía, son sistemas que cubren el proceso de comprobación/inscripción de la identidad y la autenticación. La comprobación e inscripción de la identidad pueden ser digitales o físicos (documentales), o una combinación, pero la vinculación, la credencialización, la autenticación y la portabilidad/federación deben ser digitales.

Los **marcos y normas técnicas de garantía de la identidad digital** son un conjunto de marcos de garantía y normas técnicas de código abierto y basadas en el consenso para los sistemas de identidad digital que han sido desarrollados en varias jurisdicciones y también por organizaciones internacionales y organismos del sector. Véase el ***Anexo D: Marco de garantía de identidad digital y organismos de normalización técnica.*** Véanse, por ejemplo, las normas del NIST y el Reglamento eIDAS en el *Anexo E*: *Descripción general de los marcos de garantía digital de EE. UU. y la UE y estándares técnicos*

Reglamento eIDAS: (UE) nº 910/2014 sobre la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

La **inscripción** es el proceso por el cual un IDSP registra (inscribe) a un solicitante con prueba de identidad como «abonado» y establece su cuenta de identidad. Este proceso **vincula** de forma autorizada la identidad única verificada del abonado (es decir, los atributos/identificadores del abonado) a uno o varios autenticadores que posee y controla el abonado, utilizando un protocolo de vinculación adecuado. El proceso de vinculación de la identidad del abonado con el autenticador o autenticadores también se denomina «**credencialización**».

La **federación** se refiere al uso de una arquitectura digital federada y de protocolos de afirmación para transmitir información de identidad y autenticación a través de un conjunto de sistemas en red.

Los sistemas de identidad de propósito general (o sistemas de identidad fundacionales) suelen proporcionar credenciales documentales y/o digitales que son ampliamente reconocidas y aceptadas por los organismos gubernamentales y los proveedores de servicios del sector privado como prueba de identidad oficial para diversos fines (por ejemplo, los sistemas nacionales de identificación y el registro civil).

Prueba de identidad: véase prueba de atributos.

La **gestión del ciclo de vida de la identidad** se refiere a las acciones que deben tomarse en respuesta a los eventos que pueden ocurrir durante el ciclo de vida de la identidad y que afectan al uso, la seguridad y la fiabilidad de los autenticadores, por ejemplo, la pérdida, el robo, la duplicación no autorizada, la caducidad y la revocación de autenticadores y/o credenciales.

La **comprobación de la identidad** responde a la pregunta «¿Quién es usted?» y se refiere al proceso por el cual un proveedor de servicios de identidad (IDSP) recoge, valida y verifica la información sobre una persona y la resuelve a un individuo único dentro de una población o contexto determinado. Implica tres acciones: (1) recopilación/resolución, (2) validación, y (3) verificación.

Proveedor de servicios de identidad (IDSP): Término genérico que se refiere a todos los diversos tipos de entidades que participan en el suministro y funcionamiento de los procesos y componentes de un sistema o solución de identidad digital. Los IDSP proporcionan soluciones de identidad digital a los usuarios y a las partes que confían. Una sola entidad puede desempeñar las funciones de uno o varios IDSP, véase el ***Anexo A***: ***Descripción de un sistema de identidad digital básico y sus participantes*** para conocer un resumen de todas las entidades relevantes incluyendo: proveedor de identidad, proveedor de servicios de credenciales (CSP), autoridad de registro (RA) (o gestor de Identidad), verificador, usuario/individuo, solicitante, abonado, parte que confía y Proveedor de marco de confianza / Autoridad de confianza.

La **suplantación** de identidad implica que una persona se haga pasar como si tuviera la identidad de otra persona genuina, esto puede ser a través del simple uso de un documento robado de alguien que se parezca, pero también puede combinarse con pruebas falsificadas o fraguadas (por ejemplo, la sustitución de la foto en un pasaporte con la imagen del impostor).

Sistemas de identidad de propósito limitado (o sistemas de identidad funcional) proporcionan identificación, autenticación y autorización para servicios o sectores específicos, como la administración tributaria; el acceso a prestaciones y servicios gubernamentales específicos; la votación; la autorización para conducir un vehículo de motor; y (en algunas jurisdicciones) el acceso a servicios financieros, etc. Entre los ejemplos de sistemas de identificación funcionales se incluyen, entre otros, los siguientes: números de identificación del contribuyente, permisos de conducir, pasaportes, tarjetas de registro de votantes, números de la seguridad social y documentos de identidad de los refugiados.

Ataque Man-in-the-middle: Intenta conseguir el mismo objetivo que el phishing y puede ser una herramienta para cometerlo, pero lo hace interceptando las comunicaciones entre la víctima y el proveedor de servicios.

Autenticación multifactor (MFA) combina el uso de dos o más factores de autenticación para mejorar la seguridad.

Norma/Pautas del NIST: Normas del Instituto Nacional de Estándares y Tecnología de EE. UU. 800- 63 sobre la identidad digital.

La **identidad oficial**, a efectos de esta Guía, es la especificación de una persona física única que (1) se basa en características (identificadores o atributos) de la persona que establecen la singularidad de la persona en la población o en un contexto o contextos particulares, y (2) es reconocida por el Estado para fines reglamentarios y otros fines oficiales.

La **Información personal identificable** (**PII)** incluye cualquier información que por sí misma o en combinación con otra información pueda identificar a un individuo específico.

El **phishing** (también denominado interceptación de credenciales o man-in-the-middle) es un intento fraudulento de obtener credenciales de víctimas desconocidas utilizando correos electrónicos y sitios web engañosos. Por ejemplo, un delincuente intenta engañar a su víctima para que proporcione nombres, contraseñas, números de identificación del gobierno o credenciales a una fuente aparentemente fiable.

Captura y repetición del código PIN consiste en capturar un código PIN introducido en el teclado de una PC con un registrador de teclas y, sin que el usuario se dé cuenta, utilizar el PIN capturado cuando la tarjeta inteligente está presente en el lector para acceder a los servicios).

Portabilidad/interoperabilidad: La portabilidad de la identidad significa que las credenciales de identidad digital de un individuo pueden ser utilizadas para acreditar la identidad oficial para nuevas relaciones con clientes en entidades del sector privado o gubernamentales no relacionadas, sin que tengan que obtener y verificar información personal identificable (PII) y llevar a cabo la identificación/verificación del cliente cada vez. La portabilidad requiere el desarrollo de productos, sistemas y procesos de identificación digital interoperables. La portabilidad/interoperabilidad puede apoyarse en diferentes arquitecturas y protocolos de identidad digital.

Identidad progresiva: Identidad oficial que puede cambiar con el tiempo a medida que la persona identificada desarrolla una huella digital cada vez más sólida que proporciona un número creciente de atributos y/o autenticadores que pueden ser verificados con un número y una gama cada vez mayor de fuentes.

La **comprobación de la identidad oficial** suele depender de algún tipo de registro, documentación o certificación (por ejemplo, un certificado de nacimiento, un documento de identidad o una credencial de identidad digital) que constituya una prueba de los atributos o identificadores fundamentales (por ejemplo, nombre, fecha y lugar de nacimiento) para establecer y verificar la identidad oficial. Los criterios para demostrar la «identidad oficial» pueden variar según la jurisdicción.

Cifrado de clave pública (utilizado en los certificados de infraestructura de clave pública (PKI)): Cuando se genera un par de claves para una entidad, ya sea una persona, un sistema o un dispositivo, y esa entidad mantiene la clave privada de forma segura, mientras que distribuye libremente la clave pública a otras entidades. Cualquiera que tenga la clave pública puede entonces utilizarla para cifrar un mensaje y enviarlo al titular de la clave privada, sabiendo que sólo él podrá abrirlo.

A los objetivos de esta Guía, **sujetos obligados** se refiere a las instituciones financieras, a los proveedores de servicios de activos virtuales (PSAV) y a las actividades y profesiones no financieras designadas (APNFD), tal como se definen en los Estándares del GAFI y en la medida en que las APNFD están obligadas a llevar a cabo la DDC en las circunstancias especificadas en la R.22. En junio de 2019, el GAFI revisó la Recomendación 15 (Nuevas Tecnologías) y la NI.R.15 para, entre otras cosas, imponer las obligaciones de DDC de la Recomendación 10 a los PSAV.

Parte que confía (RP): Persona (física o jurídica) que confía en las credenciales o autenticadores de un abonado, o en la afirmación de la identidad de un solicitante, para identificar al abonado, utilizando un protocolo de autenticación. Las RP típicas son las instituciones financieras y los departamentos y agencias gubernamentales.

Abonado: Persona cuya identidad ha sido verificada y vinculada a autenticadores (credencializada) por un proveedor de servicios de credenciales (CSP) y que puede utilizar los autenticadores para demostrar su identidad. Los abonados reciben un autenticador o autenticadores y la correspondiente credencial de un CSP y pueden utilizar el autenticador o autenticadores para demostrar su identidad.

Las **identidades sintéticas** son desarrolladas por los delincuentes combinando información real (normalmente robada) y falsa para crear una nueva identidad (sintética), que puede ser utilizada para abrir cuentas fraudulentas y realizar compras fraudulentas. A diferencia de la

suplantación, el delincuente se hace pasar por alguien que no existe en el mundo real, en lugar de suplantar una identidad existente.

DDC escalonada (a veces denominada cuentas escalonadas o DDC progresiva): acceso a una serie de funcionalidades de cuenta diferentes en función del grado de identificación/verificación realizado por el sujeto obligado. El acceso al conjunto de servicios básicos de primer nivel se proporciona tras una identificación mínima. El acceso a los niveles de cuenta posteriores y a los servicios adicionales (por ejemplo, límites de transacción o saldos de cuenta más elevados, acceso y canales de entrega diversificados) sólo se permite si/cuando el cliente proporciona la información de identificación/verificación adicional requerida. Mientras tanto, las cuentas disponen de servicios limitados (por ejemplo, límites de extracción diario/mensual, límites de depósito basados en el nivel de DDC realizada y el perfil de riesgo del cliente). Véase GAFI (2013-2017), Medidas anti-lavado de activos y contra el financiamiento del terrorismo e inclusión financiera - Con complemento sobre debida diligencia del cliente.

Los **árbitros de confianza** (también denominados «presentadores») pueden ser personas u organizaciones designadas (por ejemplo, notarios, tutores legales, profesionales de la medicina, curadores, personas con poder de representación, o alguna otra forma de persona capacitada y aprobada o certificada) que pueden responder por el solicitante como forma de prueba de identidad, de acuerdo con las leyes, reglamentos o políticas de la agencia aplicables de la jurisdicción. Se trata de un término utilizado en las normas del NIST estadounidense: véase NIST 800-63A 4.4.2. IAL2 Requisitos de comprobación de árbitros de confianza.

La validación forma parte de la comprobación de la identidad y consiste en determinar que las pruebas son auténticas (no son falsas, ni falsificadas, ni malversadas) y que la información que contienen es exacta, cotejando la información/prueba de identidad con una fuente aceptable (autorizada/confiable) para establecer que la información coincide con datos/registros de fuentes fiables e independientes.

La verificación forma parte de la comprobación de la identidad y consiste en confirmar que la identidad validada corresponde a la persona (solicitante) cuya identidad se está comprobando.

Verificador: Entidad que verifica la identidad del solicitante a una parte que confía (RP) confirmando la posesión y el control del solicitante de uno o más autenticadores, utilizando un protocolo de autenticación.