Unión Africana

An Integrated, Prosperous and Peaceful Africa

MARCO DE INTEROPERABILIDAD DE LA UNIÓN AFRICANA PARA LA IDENTIFICACIÓN DIGITAL

FEBRERO 2022

SUMARIO

RESUMEN

Cientos de millones de personas carecen de identificación legal en África y muchas más aún poseen identificaciones incompatibles con la era digital. Como resultado, a esta población le es complicado acceder a servicios y oportunidades generados digitalmente. Por lo tanto, para abordar tales retos, sería de gran ayuda la creación de identificaciones digitales, interoperables, confiables e inclusivas que permitan a la ciudadanía verificar su identidad jurídica con o sin conexión. Dichos sistemas tienen un potencial significativo para acelerar la digitalización de las economías y sociedades africanas, contribuyendo al estímulo empresarial, así como al éxito de la aplicación del Acuerdo de Libre Comercio Continental Africano (AfCFTA). Por estas razones, la mayoría de los países africanos están modernizando actualmente sus sistemas de identificación, aunque todos se encuentran en fases diferentes.

El Marco de Interoperabilidad de la Unión Africana para la identificación digital (el Marco) establece un proyecto que **permitirá a todos los ciudadanos del continente africano acceder de forma fácil y segura a aquellos servicios públicos y privados que necesiten, cuando lo necesiten e independientemente de su ubicación.** Con este fin, el Marco define los requisitos comunes, las normas mínimas, los mecanismos de gobernanza y demás armonizaciones entre marcos jurídicos que:

1. Permitan a los ciudadanos africanos comprobar su identidad jurídica con y sin conexión para acceder a servicios del sector público y privado en los estados miembros de la UA. Todo ello, contribuyendo a lograr un progreso acelerado hacia la unidad e integración continental con miras al crecimiento sostenido, el comercio, los intercambios de bienes y servicios y la libre circulación de personas y capitales mediante el establecimiento de una África unida y la integración económica acelerada a través de la AfCFTA, tal como se establece en la segunda aspiración de la Agenda 2063. Además, estos marcos jurídicos darán a los ciudadanos africanos el control de sus datos personales, incluyendo la capacidad para difundir solamente aquellos atributos necesarios para una determinada transacción. La información personal que sería publicada debería ser mínima, proporcionada y contener únicamente aquella información relevante para una determinada transacción, que tenga en cuenta la situación particular de África y esté en línea con las mejores prácticas internacionales[1];

2. Refuercen la confianza y la interoperabilidad entre sistemas de identificación fundamental de los estados miembros de la UA.

El Marco proporciona una norma a nivel continental con el fin de presentar digitalmente las pruebas de identidad emitidas por una fuente fiable proveniente de un estado miembro de la UA, y de garantizar la interoperabilidad en todo el continente. Toda persona que posea una identificación emitida por un sistema nacional podrá obtener una credencial de identidad digital legal interoperable (IDC-ID), que adoptará la forma de una declaración verificable[2]. Se establecerán normas para el Marco de Interoperabilidad que definirán los elementos clave

1 Véase el Reglamento General de Protección de Datos (RGPD) de la EU del 2016: https://gdpr.eu.

2 Las declaraciones son una colección de atributos sobre el interesado, por ejemplo, el apellido o la fecha de nacimiento. Una declaración verificable es una versión segura de dicha información que puede verificarse de forma criptográfica para comprobar su autenticidad.

facilitados por la IDC-ID, que constituirán la prueba de confianza en las credenciales digitales, ya que estas se crean bajo la gobernanza de un marco de confianza que define las condiciones según las cuales dicha credencial será emitida por fuentes fiables de un estado miembro de la UA.

Los estados miembros de la UA son libres de elegir cómo emitir esta credencial digital. Se puede almacenar en formato puramente digital en una aplicación para teléfonos inteligentes, un servidor en la nube, una tarjeta inteligente, o bien se puede crear un enlace a la representación digital usando códigos de barras de una o dos dimensiones sobre un documento en formato papel (impreso en papel o tarjeta de plástico). Del mismo modo, pueden decidir reutilizar esta norma para presentar datos de identidad a nivel nacional, continental o de las REC (Comunidades Económicas Regionales), o incluso, emitirlos por separado como complemento a los sistemas de identificación digital preexistentes.

El Marco se basará en el desarrollo de sistemas de identificación digital fundamental interoperables, inclusivos y confiables. Estos conforman el eje central de las fuentes de datos autorizadas sobre la identidad jurídica de las personas y, por lo tanto, permiten que la IDC-ID alcance mayores niveles de seguridad. Por este motivo, se alienta a los estados miembros de la UA a reforzar sus sistemas de identificación digital fundamental, considerando el uso de mecanismos como los *Principios sobre identificación para el desarrollo sostenible*. Este Marco tiene en cuenta también los esfuerzos llevados a cabo a nivel continental para crear un entorno propicio con el fin de proteger los datos personales, mantener la ciberseguridad y garantizar los derechos de las personas mediante la aprobación del Convenio de la Unión Africana sobre ciberseguridad y protección de datos personales (Convenio de Malabo)[3], así como el trabajo permanente de desarrollo de un marco continental en materia de política de protección de datos.

La emisión de la IDC-ID se podrá completar con una infraestructura que permita usos de caso más avanzados, como la autenticación a distancia. Este marco destaca varias opciones técnicas disponibles para los países miembros de la UA con el objetivo de aplicar esta capa, por ejemplo, una federación de proveedores de identidad que ofrezcan mecanismos de autenticación a los titulares de la IDC-ID, el desarrollo de soluciones de cartera o cualquier otro modelo que permita la interoperabilidad. Asimismo, los estados miembros de la Unión Africana podrán alcanzar nuevos acuerdos sobre cómo poner en marcha esta capa de infraestructura de autenticación y asociarse con las REC y otras iniciativas continentales que ya se encuentran investigando la introducción de soluciones interoperables de identidad digital fundamental para acceder a servicios a distancia.

La aplicación del Marco se basa en el supuesto de que será aprobado y avalado por los estados miembros de la UA. El posible bloqueo por parte de los proveedores, unos mecanismos de escasa seguridad, el deterioro de la privacidad personal, la incertidumbre sobre el beneficio de un sistema de identificación digital fundamental, la falta de capacidad técnica y financiera, la escasez de centros de datos en toda África para almacenar datos confidenciales y la presencia de sistemas de identificación no interoperables y de marcos legales y normativos obsoletos constituyen los principales problemas identificados que habrá que mitigar.

3 Unión Africana, Convenio de la Unión Africana sobre ciberseguridad y protección de datos personales, consultar (todos los enlaces incluidos en el presente documento dirigen a páginas web en inglés): https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

El documento contiene las secciones siguientes:

1. Los **antecedentes** del trabajo de la Unión Africana que ha llevado a la creación de este documento, un panorama del estado de los sistemas de identificación en África y una serie de iniciativas que promueven la interoperabilidad de la identificación digital en el continente.
2. Una **introducción** a la visión, objetivos, alcance y posibles casos de uso para el Marco de Interoperabilidad de la UA para la identificación digital.
3. Una descripción general de los **elementos clave que constituyen el Marco,** concretamente, de los principios rectores para su diseño y aplicación, el modelo elegido, los elementos clave del marco que tendrán que definirse posteriormente (por ejemplo, las reglas de participación y los requisitos técnicos), así como las tres posibles opciones estructurales para establecer una capa de autenticación interoperable.
4. Una hoja de ruta de alto nivel, donde se detalla el enfoque gradual propuesto para la definición y la aplicación del Marco, así como las acciones concretas que han de tomar los estados miembros de la Unión Africana
5. Supuestos de alto nivel, retos, riesgos que han de abordarse y mecanismos de mitigación recomendados.

El Marco no exige crear un sistema continental de identificación digital unificado, sino establecer una interoperabilidad entre los sistemas de identificación digital fundamental existentes en los países miembros de la UA que tenga en cuenta la soberanía digital de los Estados miembros de la UA, las diferencias en el despliegue de la infraestructura digital, la disponibilidad de políticas y normativas asociadas, los diferentes tipos de sistemas de identificación y la vulnerabilidad de las poblaciones durante y después de la implantación de los sistemas de identificación digital interoperables.

SIGLAS Y ABREVIATURAS

AfCFTA	African Continental Free Trade Area
AML/CFT	Anti-Money Laundering/Combating Financing of Terrorism
API	Application Programming Interface
AU	African Union
AUC	African Union Commission
CIRTs	Computer Incident Response Teams
CRVS	Civil Registration and Vital Statistics
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
EAC	East African Community
ECOWAS	Economic Community of West African States
GIZ	Gesellschaft für Internationale Zusammenarbeit
GSMA	GSM Association
HSMs	Hardware Security Modules
ICT	Information and Communication Technology
IDC-ID	Interoperable Digital Credential for Identity
ITU	International Telecommunications Union
KYC	Know-Your-Customer
LOA	Level of Assurance
PATF	Pan African Trust Framework
REC	Regional Economic Community
RP	Relying Party
SATA	Smart Africa Trust Alliance
The Framework	AU Interoperability Framework for Digital ID
UNECA	United Nations Economic Commission for Africa
WURI	West Africa Unique Identification for Regional Integration and Inclusion

See Annex I for working definitions.

1. ANTECEDENTES

1.1. CONTEXTO

Poder acreditar su propia identidad resulta esencial para toda aquella persona que desee acceder a servicios públicos y ejercer sus derechos. Tradicionalmente, en comunidades más pequeñas e informales, la identidad se podía acreditar a partir de la familiaridad, la apariencia y por los otros miembros de la comunidad. A medida que las sociedades y las economías crecían, se fueron introduciendo credenciales físicas integradas, tales como las tarjetas de identidad y los pasaportes para crear confianza. Sin embargo, cuando los países pasan a ser sociedades y economías digitales, dichas credenciales físicas no resultan muy útiles para acreditar la identidad en internet, ni tampoco para llevar a cabo otras transacciones digitales, como pagar de forma digital o compartir datos personales. Por lo tanto, las identidades digitales son un requisito previo para la confianza en línea, representadas por las identificaciones digitales que usan tecnologías y enfoques modernos con el fin de permitir que las personas acrediten y verifiquen su identidad en línea de forma segura.

Las identificaciones y, sobre todo, las identificaciones digitales, pueden proporcionar un amplio panel de beneficios a los países, como por ejemplo, una buena gobernanza, inclusión financiera, igualdad de género y la potenciación del papel de la mujer, así como una mejora de los resultados sanitarios, educativos y de protección social. Ofrecen a las personas una herramienta para reivindicar sus derechos y poder optar a servicios y operaciones. Igualmente, facilitan una plataforma a gobiernos y negocios para simplificar, expandir y renovar sus operaciones y prestaciones de servicios mediante el uso de la digitalización y de la automatización, especialmente cuando estas se prevén como una "pila digital" con plataformas de intercambio de datos confiables y de pago digital. La COVID-19 ha puesto de relieve la importancia de las pilas digitales, pues los países que las tenían total o parcialmente implantadas antes de que comenzara la pandemia fueron los que pudieron prestar con mayor rapidez y eficacia la asistencia social y los que tuvieron mayor capacidad de recuperación cuando los servicios presenciales tuvieron que trasladarse a la red. Si tenemos en cuenta que en internet no existen fronteras, las identidades digitales emitidas en un país y reconocidas en otros pueden constituir un potente motor de integración social y económica a nivel bilateral, regional o mundial.

Las identificaciones digitales alcanzan su mayor seguridad e impacto cuando se basan en la identidad jurídica de la persona. La identidad jurídica suele gestionarla un sistema de identificación fundamental del país, que incluye el registro civil, la identidad nacional y otros sistemas semejantes. Sin embargo, cientos de millones de personas en África carecen aún de una identificación fundamental, tales como un documento nacional de identidad o una partida de nacimiento[4]. En este contexto, en julio de 2016, la Asamblea de la Unión Africana declaró que 2017-2026 sería la década de reorientación del registro civil y las estadísticas vitales en África, como agenda de desarrollo continental, regional y nacional e instó a los gobiernos a aplicar las medidas adecuadas.

Agenda 2063: El África que queremos, que constituye el marco estratégico para el desarrollo socioeconómico y la transformación del continente para los próximos 50 años, ha exigido

4 Banco Mundial, Global ID4D Dataset (Conjunto de datos mundial del grupo Identificación para el desarrollo –ID4D–), consultar: https:// .worldbank.org/global-dataset

una identidad jurídica para todos. La Estrategia de Transformación Digital para África (DTS), ratificada en la 36ª Sesión ordinaria del Consejo Ejecutivo de la Unión Africana en febrero de 2020 en Adís Abeba, Etiopía, (EX.CL/Dec. 1074(XXXVI), también subrayó la importancia de la identificación digital como pilar fundamental para la creación de un Mercado Único Digital (una misión que comparte con la Smart Africa Alliance) en línea con el AfCFTA.

La Estrategia de Transformación Digital para África reconoce también que el desarrollo de la economía y la sociedad digitales cuenta con importantes facilitadores, especialmente con un entorno propicio en lo que se refiere a ciberseguridad y protección de datos. El Convenio de la Unión Africana sobre ciberseguridad y protección de datos personales de Malabo de 2014[5] establece un marco jurídico, político y regulador que incentiva la creación de un entorno digital seguro para las transacciones digitales, el comercio electrónico y la transferencia de datos. Lamentablemente, este marco legal no ha sido firmado ni ratificado por el número de estados miembros de la UA necesario para su entrada en vigor, lo que limita efectivamente su eficacia[6]. Dicho marco legal no solo contribuirá a la promoción de la confianza en el Marco y a la inclusión, sino que mitigará también los riesgos asociados a la vigilancia no autorizada y a la discriminación, especialmente en el caso de colectivos vulnerables o marginalizados, y garantizará la responsabilidad de las autoridades encargadas de aplicarlo.

1.2 SITUACIÓN DE LOS SISTEMAS DE IDENTIFICACIÓN EN ÁFRICA

Los sistemas de identificación inclusivos y confiables permiten obtener numerosos resultados, tales como la eliminación de la pobreza, la buena gobernanza, la migración segura y regulada, la protección social, la igualdad de género, además de constituir un importante impulsor de la transformación digital. Dadas las necesidades fundamentales para la identificación y autenticación seguras y precisas en línea, la identificación, la identificación digital y otros servicios de confianza –como las firmas electrónicas– representan la próxima frontera para los países del continente. Cuando lo permite la infraestructura que posibilita la conexión de personas y organizaciones, las plataformas gubernamentales y comerciales pueden potenciar la identificación digital y los servicios fiduciarios con el objetivo de facilitar diferentes operaciones digitales que incluyen los pagos digitales. A nivel nacional, la identificación digital podría actuar como un identificador único para los sistemas centrados en el ciudadano, haciendo viable la integración de sistemas. Tanto la identificación digital como las plataformas de pago proporcionan los medios para avanzar hacia una sociedad sin pago en efectivo, lo que generará un aumento de la productividad, limitará la corrupción y el fraude, y mejorará el confort del usuario.

En todo el continente existe una amplia gama tipos de sistemas de identificación y de niveles de desarrollo de la conexión con la prestación del servicio. Otros se hallan en niveles de desarrollo intermedios con deficiencias de cobertura en poblaciones vulnerables y unas competencias digitales incipientes, mientras que, en otros lugares, los sistemas de identificación digital fundamental son inexistentes o muy recientes. En general, el número de países que establecen sistemas de identificación nacional ha crecido exponencialmente en las últimas dos décadas, movidos por el deseo de mejorar la eficiencia y orientar los pagos y

5 Unión Africana, Convenio de la Unión Africana sobre ciberseguridad y protección de datos personales, consultar: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

6 Hasta julio de 2021, de los 55 estados miembros, solo 14 han firmado el Convenio de Malabo, de entre los cuales 8 lo han ratificado. Para que entre en vigor, es necesario que lo ratifiquen al menos 15 estados miembros.

transferencias gubernamentales, reforzar la integridad del sector financiero (incluido el registro mediante "conozca a su cliente" o KYC y SIM) y la de las elecciones, reforzar la seguridad pública y fomentar una migración segura y regulada. Se constata un esfuerzo continuado para reformar y modernizar los enfoques de diseño y aplicación del sistema de acuerdo a las pruebas fehacientes en materia de buenas prácticas y las enseñanzas extraídas de los programas de identificación satisfactorios[7]. Un buen ejemplo lo encontramos en Ruanda, donde se ha llevado a cabo una campaña para digitalizar su economía y potenciar el papel de la clase media a través de acciones como el paso a una economía sin pago en efectivo, que el gobierno se propone conseguir mediante el uso omnipresente del teléfono móvil y un acceso a internet de alta velocidad. Ruanda ingresó en la Better Than Cash Alliance (Alianza Mejor sin efectivo), una asociación mundial cuyo compromiso es la transición del pago en efectivo al pago digital. Ruanda está experimentando ya un aumento de la eficiencia y de los ingresos al eliminar costes de recaudación y otros gastos. Se ha convertido asimismo en un líder regional en la materia, y está compartiendo sus buenas prácticas con otros países interesados en seguir su mismo camino (Marco de inversión digital para los ODS, Unión Internacional de Telecomunicaciones –UIT–/Alianza para el impacto digital –DIAL–, 2019).

Las funciones digitales de los sistemas de identificación han aumentado considerablemente, a pesar de que la identificación digital en el ámbito de las operaciones en línea se encuentre aún en ciernes. En la última década, un gran número de países ha realizado esfuerzos para modernizar sus sistemas de identificación con el objetivo de crear una plataforma digital y credenciales de emisión que vertebran una amplia variedad de usos y servicios. Estas reformas requieren a menudo una transición del formato papel a sistemas digitales que usan captación y gestión de datos electrónicos, y que introducen la verificación de la identidad digital y mecanismos de autenticación. Por ahora, la mayoría de ellos se dan en el ámbito de las transacciones en persona. La mayoría (85%) de los países africanos posee sistemas de identificación nacionales sustentados por una base de datos electrónica, a pesar de que muchos de ellos todavía cuenten con un registro civil y procedimientos en formato papel, y de que numerosos sistemas ofrezcan una utilidad limitada en cuanto a la prestación del servicio. Más del 70 por ciento de los países africanos recopilan datos biométricos en el momento del registro para garantizar la unicidad de las identidades. Aunque algunos países –como Kenia, Lesoto, Nigeria, Ruanda y Sudáfrica– ofrezcan servicios de verificación de identidad digital (para el gobierno, ministerios, bancos, etc.) para verificar la información de identidad o credenciales frente a una base de datos central, a la hora de autenticar la mayoría de las operaciones se sigue usando la verificación manual de las tarjetas de identidad físicas. Las soluciones de identidad digital que permiten una autenticación segura para servicios y operaciones en línea se encuentran aún en ciernes en todo el continente, donde solo un puñado de países posee tales servicios (por ejemplo, en Sudáfrica, en los bancos o en Cabo Verde y en Seychelles, en servicios de administración electrónica).

A pesar de numerosas mejoras y la creación de nuevos sistemas en los últimos años, los países africanos y sus habitantes se enfrentan a varios retos a la hora de identificarse. Algunos de los elementos clave que han de reforzarse son la accesibilidad a los sistemas de identificación, su compatibilidad efectiva con la prestación del servicio y la aplicación de garantías que promuevan la confianza y la confidencialidad.

7 Una encuesta de funcionarios africanos en 2018 reveló que el 60 por ciento de los países africanos estaba planeando crear un sistema de identificación o modernizar el ya existente para finales de 2020.

Garantizar el acceso universal a sistemas de identificación constituye un reto permanente. Se estima que mil millones de personas en todo el mundo carecen de documentos de identidad, y aproximadamente la mitad de ellas reside en África[8]. Del mismo modo, el continente africano alberga 8 de los 10 países del mundo con las mayores desigualdades de género en materia de identificación. La cobertura de identificación entre adultos del África Subsahariana es cerca de 10 puntos porcentuales menor en las mujeres que en los hombres[9]. Los retos de la identificación comienzan al nacer: 100 millones de niños de menos de cinco años no poseen aún registro de nacimiento[10]. Entre las múltiples causas de tal ausencia de cobertura se encuentran unos elevados costes de inscripción directos y (sobre todo) indirectos, unos requisitos documentales y administrativos de inscripción complejos, y una demanda poco importante, donde los sistemas de identificación ofrecen una escasa utilidad para facilitar el acceso a los servicios[11].

El uso de nuevas tecnologías también ha aumentado la complejidad y presenta nuevos riesgos. Por ejemplo, no todas las soluciones se adaptan bien a las necesidades y a los contextos locales, ya que el acceso a internet, a la electricidad o la alfabetización digital de los funcionarios o de la población general puede ser limitado. La dependencia de los proveedores resulta ser una preocupación común, que a menudo está ligada a unos costes operativos elevados e insostenibles, una escasa interoperabilidad de los sistemas de identificación y a un control y supervisión de los datos de identidad deficientes por parte de los gobiernos y de los usuarios. Además, con el aumento de la utilización de tecnologías digitales para la identificación y autenticación, así como el cambio hacia credenciales digitales, las personas que poseen una escasa alfabetización digital y un acceso limitado a dispositivos conectados corren el riesgo de quedarse atrás.

A medida que los sistemas y el procesamiento de datos se han ido digitalizando, ha aumentado también la necesidad de crear garantías efectivas para proteger los datos y la privacidad de los usuarios. Unas garantías inadecuadas de protección de datos, privacidad y derechos del usuario –legales, institucionales o tecnológicos– pueden exponer los sistemas de identificación a brechas de seguridad y dejar los datos de las personas sin protección. A un gran número de países les queda aún un largo camino que recorrer para crear sistemas de identificación seguros y confiables: según la UNCTAD, solo 28 países (50 %) de África han aprobado una legislación en materia de protección de datos y privacidad y 39 (70 %) posee legislación sobre ciberdelincuencia[12]. Incluso, en los casos en el que dicho marco existe, aplicar las disposiciones legales por medio de controles efectivos institucionales, operativos y técnicos puede representar una dificultad. Hasta hoy, solo pocos países almacenan y gestionan sus datos según las buenas prácticas internacionales para protegerse contra el robo o la pérdida involuntaria de datos[13].

8 ID4D Global Dataset (Conjunto de datos mundial del grupo Identificación para el desarrollo –ID4D–) 2018: https://id4d.worldbank.org/global-dataset

9 https://documents1.worldbank.org/curated/en/727021583506631652/pdf/Global-ID-Coverage-Barriers-and-Use-by-the-Numbers-An-In-Depth-Look-at-the-2017-ID4D-Findex-Survey.pdf

10 https://www.unicef.org/media/62981/file/Birth-registration-for-every-child-by-2030.pdf

11 https://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf

12 https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

13 https://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf

Los sistemas de identificación digital se enfrentan a los mismos retos que el desarrollo de los sistemas digitales propios. Dichos retos comprenden, entre otros, los asuntos relacionados con la financiación, ya que los ciclos de financiación se encuentran desconectados de los ciclos de desarrollo tecnológico, sobre todo las donaciones, que se basan en proyectos y poseen plazos limitados. Además, la planificación compartimentada y la toma de decisiones de los grupos interesados tienen como consecuencia una limitación de las oportunidades de coordinación por parte de los grupos de actores, lo que limita la reutilización de las soluciones digitales y socava su posible aplicabilidad en diversos programas y sectores. La escasez de alfabetización digital, es decir, la ausencia de capacidad de liderazgo en materia de TIC y en la selección, diseño, aplicación, ampliación y mantenimiento de soluciones TIC, representa a menudo un problema para los gobiernos y los profesionales del desarrollo. Otra de las principales preocupaciones que existen últimamente es la falta de financiación para ampliar las soluciones TIC, ya que por regla general suele haber fondos suficientes para financiar las primeras etapas del desarrollo de la tecnología, pero la financiación se vuelve escasa cuando se amplía a nivel nacional. (Marco de inversión digital para los ODS, Unión Internacional de Telecomunicaciones –UIT–/Alianza para el impacto digital –DIAL–, 2019).

1.3 OTRAS INICIATIVAS QUE PROMUEVEN EL RECONOCIMIENTO MUTUO Y LA INTEROPERABILIDAD DE LAS IDENTIFICACIONES DIGITALES EN ÁFRICA

Además del marco, existen otras iniciativas complementarias que promueven el reconocimiento mutuo y la interoperabilidad de las identificaciones digitales en África, entre las que se encuentran:

1.3.1. ESTRATEGIA DE TRANSFORMACIÓN DIGITAL PARA ÁFRICA (2020-2030)

La identificación digital constituye uno de los cinco temas transversales de la Estrategia, que también formula diez recomendaciones políticas y acciones, propuestas a lo largo de dos temas sobre las garantías de la inclusión, la seguridad y la privacidad y la propiedad de los datos, y el apoyo de la interoperabilidad y la neutralidad. Mientras que dichas recomendaciones se refieren principalmente al desarrollo de los sistemas de identificación digital nacional, otra de las recomendaciones, por su parte, exige la creación de una "identidad digital continental interoperable y abierta que permita la verificación y la autenticación de las personas", y otra pide a la CUA, a la CEPA y a otros socios que "trabajen juntos para establecer normas continentales y regionales que incluyan protocolos de autenticación, campos de datos mínimos, protocolos de duplicación, formatos biométricos y otros formatos, reglamentos modelo así como otras normas".

1.3.2. INICIATIVA DE LA CEPA SOBRE IDENTIFICACIÓN DIGITAL

La Comisión Económica para África de las Naciones Unidas (CEPA) ha creado una iniciativa sobre Identidad digital, Comercio y Economía Digital (DITE) que actúa como un Centro de Excelencia, cuyo objetivo es armonizar las normas conexas, aprobar reglamentos para garantizar la seguridad, aumentar las inversiones y desarrollar las capacidades y habilidades de

los actores clav[14]. El Centro Digital de Excelencia de la CEPA trabaja con el objetivo de crear un marco continental africano armonizado en materia de identificación digital que defina y elabore políticas y normas para la identificación digital y otorgue capacidad de desarrollo a los estados miembros, a las Comunidades Económicas Regionales y a la Unión Africana. La CEPA ha redactado un libro blanco sobre el marco para la interoperabilidad digital mediante la creación de un Marco Panafricano de Confianza (PATF).

1.3.3. SMART AFRICA TRUST ALLIANCE (SATA)

Smart Africa es una iniciativa de los jefes de estado africanos para acelerar el desarrollo socioeconómico de África mediante la potenciación de las TIC. En 2020, Benín defendió un proyecto emblemático de Smart Africa para desarrollar el Digital ID Blueprint (Plan General sobre Identidad Digital), llevado a cabo por un grupo de trabajo formado por Ruanda, Túnez, la Unión Africana (UA), la Unión Internacional de Telecomunicaciones (UIT), el Banco Mundial, la Omidyar Network, la Comisión Económica para África de las Naciones Unidas (CEPA), la Asociación GSM, el Foro Económico Mundial, la Sociedad Alemana para la Cooperación Internacional (GIZ) y varias empresas privadas. Fue ratificada por el Smart Africa Board, formado por sus 32 estados miembros, la UA y la UIT. El Plan General[15] plantea la SATA como una plataforma que facilite el reconocimiento confiable de las identificaciones digitales entre una amplia gama de actores mediante mecanismos de certificación federados. Los proyectos piloto de la SATA está previsto que los lleven a cabo Benín, Ruanda, Túnez y otros estados miembros de Smart Africa. La SATA constituirá una solución ágil y adaptable que permita la interoperabilidad entre varios esquemas de identidad públicos y privados del continente. Para más información consultar: sata.smartafrica.org.

1.3.4. PROGRAMA DE IDENTIFICACIÓN ÚNICA PARA LA INTEGRACIÓN Y LA INCLUSIÓN EN ÁFRICA OCCIDENTAL (WURI)

El WURI[16] es un programa regional que potencia la financiación del Banco Mundial para mejorar el acceso a los servicios en colaboración con los estados miembros de la CEDEAO mediante la creación de sistemas de identificación digital fundamental que sean accesibles a todos los ciudadanos del territorio del país –sin tener en cuenta su nacionalidad o su situación legal– y diseñados con interoperabilidad transfronteriza con el objetivo de permitir el acceso a servicios sociales, sanitarios, financieros y de otro tipo en varios países. Costa de Marfil, Guinea y la Comisión de la CEDEAO integraron la fase 1 del programa en 2018, y Benín, Burkina Faso, Níger y Togo entraron en la fase 2 durante 2020. Los principios fundamentales del WURI son un registro accesible para todo el mundo e inclusivo, minimización de datos y credenciales básicas que se ofrecen gratuitamente a la población.

1.3.5. PROTOCOLO DE MERCADO COMÚN DE LA CAO

Mediante el Artículo 8 del Protocolo, los seis países miembros de la CAO se comprometieron a avanzar progresivamente hacia: "... un sistema común de normas para emitir documentos

14 CEPA, DITE para África, consultar: https://www.uneca.org/dite-africahttps://www.uneca.org/dite-africa

15 Smart Africa, Plan General | Smart Africa Alliance – Digital Identity, octubre de 2020, consultar: https://smartafrica.org/knowledge/digital-id/

16 Banco Mundial. Programa de identificación única para la integración y la inclusión en África Occidental (WURI). https://projects.worldbank.org/en/projects-operations/project-detail/P161329; https://projects.worldbank.org/en/projects-operations/project-detail/P169594

de identificación a sus ciudadanos".[17] Esto último se encuentra estrechamente relacionado con los otros objetivos del Protocolo, como la libre circulación de bienes (Artículo 6), personas (Artículo 7), trabajo/trabajadores (Artículo 10), servicios (Artículo 16) y capitales (Artículo 24), así como los derechos de establecimiento y residencia (Artículos 13 y 14 respectivamente). No obstante, los sistemas de identificación nacional se encuentran en varias fases de desarrollo. A pesar de ello, y teniendo en cuenta el concepto de geometría variable y como iniciativa de los Proyectos de integración del Corredor del Norte (NCIP), Kenia, Ruanda y Uganda comenzaron a reconocer mutuamente sus tarjetas nacionales de identidad como documentos de viaje válidos. Dentro del marco del NCIP se ha debatido la posibilidad de ampliar este principio a otros casos de uso, como los servicios electrónicos, pero no se ha concretizado todavía. En 2018, el Banco Mundial y la secretaría de la CAO llevaron a cabo un estudio sobre las posibilidades de reconocimiento mutuo de las identificaciones nacionales dentro de la CAO, que fijó cuatro objetivos.

1.4. SOBERANÍA DIGITAL Y DE DATOS

Al albergar 55 naciones soberanas, África ha de tener en cuenta 55 jurisdicciones. La soberanía digital se refiere a un conjunto de diferentes conceptos técnicos y reguladores que van de la ubicación física de los servidores y la construcción de cables submarinos a las leyes y prácticas relativas a la protección de datos y a la tributación de los mercados de datos, que permite a los estados tomar sus propias decisiones en cuanto a las opciones tecnológicas y a su regulación.

Con el objetivo de garantizar tanto la soberanía digital como la soberanía de los datos[18], se insta a los estados miembros de la UA a:

crear sistemas seguros de almacenamiento de datos personales (incluidos los datos confidenciales) mediante el diseño y la creación de centros de datos que deben prever el control de los datos por parte del estado y contener un mínimo de espacio de almacenamiento y de tratamiento dedicado exclusivamente a los datos personales y confidenciales. También será necesario establecer garantías necesarias (especialmente técnicas) para asegurarse de que los datos que se usan en intercambios de información transfronterizos no contienen en absoluto datos personales o confidenciales, cuyo almacenamiento o procesamiento pueda generar riesgos graves tanto para los derechos de los ciudadanos como para la soberanía digital de los estados miembros de la UA. Los estados miembros de la UA también deben establecer un mecanismo para proteger los datos de los ciudadanos dentro y fuera de las fronteras, y dar a la ciudadanía el control sobre sus datos personales. Además, se espera que los estados miembros tomen la iniciativa de potenciar las habilidades digitales y las competencias de resiliencia cibernética de los ciudadanos/residentes y de los actores del sistema;

17 https://www.eac.int/images/doc_image_png_NnlwzXikEvuHdytNzkKNVDMScreen%20Shot%202017-06-20%20at%20153445.png

18 La "soberanía de los datos ", tal como se utiliza en este Marco, tiene el siguiente significado: los datos personales (incluidos los datos confidenciales) relacionados con los sistemas de identificación digital en un estado miembro de la UA que deben recopilarse, almacenarse y procesarse (i) en instalaciones que sean propiedad o estén controladas por el estado miembro de la UA y (ii) cumplan la legislación aplicable.

fomentar la capacidad y las infraestructuras para el desarrollo de las competencias y los talentos en África a fin de hacer frente a los nuevos desafíos y reforzar la soberanía digital;

establecer una colaboración basada en el respeto mutuo y en una situación en la que todos salgan ganando, sin comprometer la soberanía y la propiedad nacional, y evitar injerencias extranjeras que puedan afectar negativamente a la seguridad nacional, los intereses económicos y el desarrollo digital de los Estados miembros de la UA.

El Marco se guiará por las normas soberanas representadas por la autoridad o autoridades de registro y emisoras de la identidad de cada estado miembro de la UA. Los estados miembros de la UA ratificarán la estructura de gobernanza, que incluye la creación de una institución coordinadora continental de control. Además, los estados miembros de la UA definirán y ratificarán mecanismos de responsabilidad, como la gestión de las obligaciones en caso de irregularidades. El fomento de la confianza a nivel continental entre estados soberanos que poseen esquemas de identificación digital divergentes constituye una tarea compleja, aunque realizable, que requiere una colaboración de todos los actores. Para alcanzar la interoperabilidad en el intercambio de información de identidad en los respectivos países africanos, se deben reconocer los puntos comunes entre las reglas y normas existentes, a partir de un conjunto mínimo de criterios que permitirán tanto la soberanía local como la confianza necesaria en el enfoque de cada uno.

Para ello, los estados miembros de la UA necesitan reforzar y mejorar sus marcos jurídicos y sus capacidades de ejecución, sobre todo las competencias de las autoridades de protección de datos en la vigilancia de los intercambios de datos transfronterizos, así como la aplicación de las disposiciones legales y regulaciones pertinentes en caso de infracción o uso indebido.

El Marco propuesto examinará la situación de las tecnologías puntas y respetará las leyes y la reglamentación de los distintos países. No se debe obligar a los gobiernos a usar unas tecnologías en concreto. El uso de reglas y normas abiertas debería garantizar un amplio abanico de posibilidades para los estados, al mismo tiempo que se fomenta la propiedad e interoperabilidad del país.

2. INTRODUCCIÓN

En 2020, los estados miembros de la Unión Africana aprobaron la Estrategia de Transformación Digital para África 2020-2030 (DTS) con la intención de crear:

Unas sociedades y economías integradas e inclusivas en África, que mejoren la calidad de vida de los ciudadanos africanos, refuercen el sector económico existente, permitan su diversificación y desarrollo y garanticen la propiedad continental para que África desempeñe un papel de productor y no solo de consumidor en la economía mundial.

El cumplimiento de esta meta –así como la de la AfCFTA– depende del desarrollo de sistemas de identificación digital fundamental inclusivos y confiables que permitan a todos los ciudadanos de África comprobar y verificar su identidad de forma segura y fiable a la hora de realizar operaciones en persona o en línea, así como permitir a los proveedores de servicios del sector público y privado reconocer las credenciales de identidad sin importar el lugar de África donde se emitieron. De igual modo, los sistemas de identificación digital fundamental deben diseñarse con el fin de potenciar el papel de las personas, sobre todo de las poblaciones desfavorecidas y marginalizadas. Este hecho permitirá que todos los ciudadanos africanos participen en la economía y la sociedad digitales, que se desbloquee el acceso a servicios en el interior de los países y más allá de sus fronteras, que se incentive el comercio como parte de la AfCFTA, se refuerce la confianza en la sociedad y economía digitales y se limite el fraude y los costes de la actividad empresarial.

Otro hecho importante es que los sistemas de identificación digital fundamental también pueden contribuir al desarrollo de "pilas digitales"[19] que propongan pago digital y plataformas confiables de intercambio de datos para crear oportunidades de innovación y una amplia gama de operaciones sin dinero en efectivo, desmaterializadas y a distancia en todo el continente. Sin embargo, este hecho entraña también riesgos relacionados con la exclusión, protección de datos, ciberseguridad y los bloqueos tecnológicos y de proveedores que han de ser resueltos de forma integral. Por ello, la identificación digital forma parte de los cinco temas transversales de la DTS, que estipula el mandato y el establecimiento del presente Marco.

2.1. VISIÓN, OBJETIVOS Y CASOS ORIENTATIVOS DE USO

La visión del Marco de Interoperabilidad de la Unión Africana para la identificación digital consiste en que todo ciudadano de África pueda acceder fácilmente y de forma segura a los servicios que necesite, cuando lo necesite, a partir de proveedores del sector público o privado con el fin de fomentar la participación inclusiva y significativa en una economía y una sociedad digitales más amplias y permitir que los servicios funcionen con mayor grado de confianza y seguridad.

19 En el ámbito de las tecnologías digitales, una "pila" es una colección de componentes de software independientes o infraestructura que funcionan de forma conjunta para contribuir a la ejecución de un caso de uso.

Con este fin, el Marco establece requisitos comunes, estándares mínimos, normas, mecanismos de gobernanza y mayor armonización entre marcos legales y los objetivos para:

1. permitir que todos los ciudadanos africanos **verifiquen su identidad con o sin conexión** y accedan a servicios del sector público y privado en todos los países miembros de la Unión Africana participantes. Todo ello, contribuyendo a lograr un progreso acelerado hacia la unidad e integración continental con miras al crecimiento sostenido, el comercio, los intercambios de bienes y servicios y la libre circulación de personas y capitales mediante el establecimiento de un África unida y la integración económica acelerada a través de la AfCFTA, tal como se establece en la segunda aspiración de la Agenda 2063;
2. potenciar el papel de los ciudadanos africanos en **el control de sus datos personales,** como la posibilidad de revelar solo aquellos elementos necesarios en una operación dada;
3. reforzar la **confianza y la interoperabilidad** entre los sistemas de identificación digital fundamental de los estados miembros de la UA.

El Marco no exige la creación de un sistema de identificación digital único a nivel continental, sino que crea una base para la interoperabilidad entre los sistemas de identificación digital existentes en los estados miembros, que tiene en cuenta la soberanía digital de los estados miembros de la UA, las diferencias en el despliegue de la infraestructura digital, la disponibilidad de políticas y reglamentos asociados, los diferentes niveles de sistemas de identificación y la vulnerabilidad de las poblaciones durante y después de la implementación de los sistemas de identificación digital.

Resulta primordial que este Marco se lleve a cabo respetando las buenas prácticas y las normativas internacionales[20], cuyo fin es proteger los datos personales, garantizar la ciberseguridad y preservar los derechos de las personas. Con la ratificación del Convenio de Malabo sobre ciberseguridad y protección de datos personales y el trabajo permanente para desarrollar un marco continental en materia de política de datos[21], la Unión Africana ha dado un paso importante en la creación de un entorno digital creíble para las operaciones en línea a través de la aprobación de un conjunto de reglas comunes que rigen el intercambio transfronterizo de datos personales en todo el continente y armonizan los marcos nacionales en materia de protección de datos y ciberseguridad.

Un Marco a nivel continental puede facilitar el **acceso a servicios en todos los países participantes, autorizando a las personas y a los negocios** a verificar credenciales y otros datos sin divulgar información personal. Esto incluye la posibilidad de autenticar su identidad cuando se acceda a servicios en línea (por ejemplo, servicios gubernamentales) en otro país con una identificación digital y sin necesidad de registrarse en las soluciones de identidad fundamentales locales reconocidas por los proveedores de servicios extranjeros. La interoperabilidad de la identificación digital facilita también el intercambio y el consentimiento para credenciales verificables y datos confiables a la hora de solicitar servicios cuando la ley requiera tal verificación (por ejemplo, un justificante de seguro o la situación vacunal), lo que permite ganar tiempo y reducir los trámites burocráticos.

20 Estas incluyen UIT-T X.1058 | ISO/CEI 29151, los principios y recomendaciones de la ONU para sistemas de estadísticas vitales, los Diez Principios sobre la identificación para el desarrollo sostenible, normativas internacionales sobre protección de datos y el Reglamento General de Protección de Datos de la EU, entre otros.

21 Unión Africana, Convenio sobre ciberseguridad y protección de datos personales, consultar: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

Además, puede **reforzar la integridad y la accesibilidad a pagos y servicios financieros transfronterizos en África y crear oportunidades para la innovación.** Unos sistemas de identificación vulnerables y no confiables y la ausencia de armonización de reglas generan riesgos relacionados con la prevención del blanqueo de capitales y la financiación del terrorismo o AML/CFT[22], que constituyen una barrera para los intercambios transfronterizos, aumentan los costes de los servicios (por ejemplo, las remesas) y obstaculizan la innovación. La identificación digital puede facilitar la identificación y la verificación del consumidor, respaldar los procedimientos "conozca a su cliente" (KYC), así como asistir en la supervisión de operaciones para identificar y denunciar operaciones sospechosas. La interoperabilidad no solo beneficiará a los migrantes que envían dinero a sus países de origen, al simplificarse la verificación KYC y la autenticación, sino que también ayudará a reducir costes y permitirá a África acercarse a la meta de los ODS (10.c) del tres por ciento en 2030.

Asimismo, un **Marco a nivel continental puede reforzar los intercambios comerciales y el comercio electrónico al aumentar la confianza en las operaciones comerciales en línea y facilitar los negocios y el comercio en toda África**. En 2020, el comercio entre países africanos representó aproximadamente solo el 16.6% del PIB africano.[23] En 2019 se creó el AfCFTA para favorecer nuevas oportunidades comerciales y de comercio electrónico para 2030. Un reconocimiento transfronterizo de las identificaciones digitales puede ayudar a reforzar los controles de identidad de compradores y vendedores, sobre todo en los artículos sujetos a restricciones de venta por internet. También puede autorizar las firmas electrónicas para operaciones realizadas únicamente por internet y sin papel, lo que ahorra tiempo a empresas y clientes, y reduce el riesgo de robo de identidad. Se simplifican de igual modo las operaciones comerciales transfronterizas al permitir a las empresas gestionar su interacción con el gobierno de forma digital, por ejemplo, a la hora de declarar los impuestos, participar en procedimientos de adquisición, solicitar el número de IVA y solicitar autorizaciones.

2.2 ALCANCE

Para lograr estos objetivos, el Marco definirá:

- el **tipo de información/datos** que se pueden compartir a través de un conjunto de datos mínimo para información de identidad fundamental;[24]
- la **manera de comprobar quién es el emisor de los datos** y si es confiable mediante la:
  - creación de un procedimiento para comunicar fuentes confiables autorizadas[25] para datos de identidad en cada estado miembro de la UA;
  - determinación del modo en que se verifica la autenticidad de la declaración digital;
- las normas y procedimientos que describen **la manera en que los usuarios comparten** sus datos y los otros los verifican en entornos con o sin conexión.

22 Siglas en inglés que se refieren a los riesgos relacionados con la prevención del blanqueo de capitales y la financiación del terrorismo. El GAFI recomienda a los gobiernos que desarrollen un enfoque integrado por los distintos actores para identificar las oportunidades y riesgos relacionados con la identificación digital y desarrollar reglamentos y orientaciones para mitigarlos.

23 UNCTAD, Informe sobre Desarrollo económico en África 2019: Made in Africa: Reglas de origen para reforzar el comercio dentro de África, consultar: https://unctad.org/press-material/facts-figures-0

24 Aunque el alcance de este documento se centre en los datos de identidad, el marco de confianza propuesto, los estados miembros de la UA pueden ampliarlo a otros pruebas y logros, tales como títulos académicos, cualificaciones profesionales, etc.

25 Los estados miembros asumirán la responsabilidad legal y la obligación de rendir cuentas en relación con las fuentes autorizadas de confianza (emisores de datos)

Este documento esboza las bases de un marco de confianza e interoperabilidad para los sistemas de identificación digital en todo el continente africano. Definirá los requisitos mínimos necesarios para asegurar la interoperabilidad entre sistemas de identificación digital existentes y futuros. La interoperabilidad se refiere a la capacidad de las distintas partes del Marco –como los sistemas de identificación digital y los sistemas de las partes confiables– para comunicarse e interactuar eficazmente a nivel técnico y semántico. La interoperabilidad puede facilitar el reconocimiento mutuo, lo cual es un constructo jurídico, pero no supone un requisito previo ni garantiza dicho reconocimiento. El Marco no define un sistema de identificación digital unificado para África y no aborda los convenios comerciales y de responsabilidades entre los estados miembros participantes.

Numerosos países de África poseen sistemas de identificación digital muy avanzados y algunos de ellos han creado formas de autenticación digital. **El Marco proporciona requisitos comunes para comunicar datos de identidad fundamental y procedimientos que serían interoperables y aceptados por otros estados miembros africanos, al mismo tiempo que los estados miembros siguen teniendo el control total del diseño de sus sistemas nacionales.**

El Marco servirá de complemento y estructura para las actividades asociadas con el Protocolo del Tratado por el que se crea la Comunidad Económica Africana en materia de libre circulación de personas, derecho de residencia y derecho de establecimiento, la Conferencia de Ministros Africanos Responsables del Registro Civil y el Programa Africano para acelerar la mejora del registro civil y las estadísticas vitales (APAI-CRVS). La aplicación del Marco debería coordinarse en estrecha colaboración con esta y otras iniciativas pertinentes, como por ejemplo, el estudio de la migración como otro caso de uso para la identificación digital en el momento oportuno y la ratificación de la mejora de la cobertura y la calidad de los sistemas de CRVS como contribución importante para los sistemas de identificación digital fundamental.

2.3. MARCO DE CONFIANZA, CONFIDENCIALIDAD, INTEROPERABILIDAD Y NORMAS

Los sistemas de identidad deberían favorecer la confianza entre las distintas entidades participantes, asegurándose de que se aplican los derechos legales tanto de los usuarios particulares como de las empresas de explotación y que se promueve el uso ético de los sistemas de identidad. **Para garantizar dicha confianza, es preciso definir un conjunto de reglas que todas las partes tienen que corroborar y aplicar,** es decir, un marco de confianza.

Mientras que la tecnología actúa como una herramienta clave, los marcos de confianza se centran también en los procesos y procedimientos. Un marco de confianza sólido debería definir con claridad los:

El Marco se basa en la **interoperabilidad**. Para facilitar la interoperabilidad, una entidad debe poder confiar en otra basándose no solo en la integridad de los procesos técnicos (por ejemplo, la verificación criptográfica), sino también considerando el origen de los datos compartidos (por ejemplo, los procesos para su recopilación y para atribuir un determinado registro a un particular).

La interoperabilidad no requiere que los sistemas de identificación digital fundamental sean uniformes, sino que sigan simplemente normas comunes y abiertas. Con el Marco, cada país participante puede crear sistemas de identificación fundamental adaptados a las necesidades, costumbres y legislación locales, siempre que se sigan unas normas determinadas que permitan la interoperabilidad. Las normas abiertas establecen protocolos de intercambio coherentes y universalmente reconocidos, regímenes de pruebas, medidas de calidad y buenas prácticas con respecto a la captación, almacenamiento, transmisión y uso de datos de identidad, así como el formato y características de las credenciales de identidad y de los protocolos de autenticación.

Al examinar la interoperabilidad de las credenciales de identificación y la autenticación en todo el continente, será esencial tener en cuenta las normas abiertas para las declaraciones de identidad, su modo de expedición y la forma en que las entidades que participan en el marco de confianza comunican entre sí dicha confianza. Estas declaraciones, que constituirán la **base para crear la identificación digital**, provendrán a menudo de fuentes autorizadas, tales como los servicios gubernamentales. Se debe definir asimismo un mecanismo de autenticación para que los propietarios de la identidad digital puedan compartir adecuadamente dichas declaraciones con los proveedores de servicios, garantizándose así que la difusión de datos se efectúa de forma binaria, que ningún metadato se encuentra oculto y que la privacidad y los derechos de los particulares se encuentran protegidos en todo momento.

Este Marco definirá el **modo en que se debe crear confianza en esas declaraciones verificables y cómo funcionan los elementos de gobernanza y las normas para los datos.** La aplicación técnica de la solución la puede llevar a cabo el mercado, que podrá impulsar el marco de confianza para desarrollar soluciones fundamentales de identidad digital innovadoras. La confidencialidad, la auditoría y la protección de datos son el eje central del Marco. Este establece un procedimiento transparente para que todas las partes confiantes lo apliquen en lo relativo al modo en que se solicitan, recopilan, transmiten y almacenan los datos y sigue normas ampliamente aceptadas sobre procedimientos de intercambio de información/datos. Otro aspecto que será elaborado ulteriormente para reforzar la confidencialidad a nivel nacional/continental es la relevancia de la toquenización para limitar la recolección, clonado y robo de datos, añadiendo al documento de identificación la funcionalidad de emitir identificaciones virtuales, con el objetivo de proteger las verdaderas identidades.

3. EL MARCO

El Marco de Interoperabilidad de la UA para la identificación digital propone definir un enfoque armonizado a nivel continental para que los particulares puedan compartir con los proveedores de servicios declaraciones de identidad digitales[26] emitidas por autoridades confiables con el objetivo de probar su identidad en un entorno con o sin conexión. Consistirá en aprobar una **norma común para presentar pruebas de identidad existentes, emitidas por los estados miembros de la UA en formato digital**[27]. La autenticidad de tales credenciales[28] se podría verificar para garantizar un máximo nivel de confianza y seguridad.

No existen restricciones en los sistemas de identidad fundamental nacional en cuanto a cómo funcionan o qué tipos de credenciales usan estas para autenticar a los particulares. Cada país es soberano en este asunto. La intención del Marco es crear condiciones de interoperabilidad en el continente tomando como base los sistemas ya existentes, donde dichas condiciones se encuentran presentes y ampliar su uso en lugar de restringirlo.

Las credenciales de identidad digital interoperables (IDC-ID), que se expiden de acuerdo al Marco de la UA, se materializarán en una declaración verificable que será complementaria a los sistemas de identificación fundamental nacional y a los proyectos de cooperación regional, pero que no sustituirá a los sistemas de identificación digital domésticos de los estados miembros de la UA. **Los estados miembros de la UA son libres de elegir de qué modo emiten dicha credencial digital.** Se puede almacenar en un formato puramente digital o en una aplicación para teléfonos inteligentes, en un servidor en la nube, en una tarjeta inteligente, o bien se puede crear un enlace a la representación digital, usando códigos de barras de una o dos dimensiones en un documento en formato papel (impreso en papel o en forma de tarjeta de plástico).

El Marco se basará en el desarrollo de sistemas de identificación digital fundamental interoperables, inclusivos y confiables, ya que estos proporcionan el eje central de las fuentes de datos autorizadas sobre la identidad jurídica de las personas y, por lo tanto, permiten que la IDC-ID alcance mayores niveles de seguridad. Por este motivo, se alienta a los estados miembros de la UA a reforzar sus sistemas de identificación digital fundamental, así como los *Principios sobre identificación para el desarrollo sostenible.* Se pueden analizar soluciones alternativas para que las personas que se encuentren actualmente fuera de un sistema de identificación puedan obtener una IDC-ID.

Las normas para una identidad digital interoperable se podrían usar a nivel doméstico o servir en casos de uso transfronterizos. Por ejemplo, la norma se podría aprobar para:

- contener datos de identificación digital fundamental a nivel nacional en credenciales de identidad digital nuevas o actualizadas;
- contener datos de identificación digital fundamental a nivel del continente o de las REC;
- emitirse por separado como complemento de sistemas de identificación digital fundamental preexistentes.

26 Las declaraciones son una colección de atributos sobre el interesado, por ejemplo, el apellido o la fecha de nacimiento.
27 El presente marco se centra en la definición de declaraciones verificables para comprobar datos de identidad, pero podría ampliarse a fin de abarcar el intercambio de declaraciones verificables en materia de logros académicos, cualificaciones profesionales, etc.
28 Una credencial se compone de una declaración de identidad, de metadatos sobre el emisor y de una prueba de autenticidad, a menudo, una firma digital.

El componente de interoperabilidad, confianza e inclusión definido en este Marco constituye un punto de arranque para la elaboración de un marco continental y una infraestructura más amplios para la identificación y la autenticación en el continente.

3.1. PRINCIPIOS RECTORES

Los siguientes principios orientarán la aplicación de la interoperabilidad transfronteriza del Marco:

1. Transparencia en la gobernanza y en el funcionamiento.
2. De fácil acceso, rentable financieramente, operacionalmente sostenible y ampliamente utilizable.
3. Promover el respeto y la defensa de los derechos humanos y la libertad[29].
4. Garantizar la integridad técnica, incluida una identidad única, segura, modulable y precisa.
5. Garantizar la soberanía de los estados miembros, reforzando la soberanía de datos, especialmente de datos de identidad digital, que pertenecen y permanecen bajo el control de África.
6. Ser interoperable entre estados miembros de la UA.
7. Usar normas abiertas[30] y evitar bloqueos de proveedores y de tecnología.
8. Proteger la privacidad de los datos digitales y permitir a las personas que controlen sus propios datos personales, incluida la proporcionalidad de datos mediante un diseño adecuado del sistema.
9. Preservar la confidencialidad, la seguridad y los derechos mediante un amplio marco jurídico y regulador.
10. Crear mandatos institucionales claros y responsabilidad.

Teniendo en cuenta que el Marco depende de fuentes autorizadas, tales como sistemas de identificación legales, la calidad y cobertura de dichos sistemas tendrá por lo tanto un impacto en su aplicación. La exclusión de esos sistemas y otros retos, como la escasa seguridad, por ejemplo, conducirán a lo mismo en términos de capacidad de emisión y de uso adecuado de las credenciales.

Por consiguiente, los estados miembros de la UA deberían cumplir con sus obligaciones para garantizar que todas las personas presentes en su territorio tengan acceso a una identificación legal, de acuerdo con la Convención sobre los Derechos del Niño y otros instrumentos legales internacionales y regionales. Además, se les recomienda encarecidamente que aprueben las

29 Como lo establece la Carta de la Unión Africana de los Derechos Humanos y de los Pueblos (ratificada el 27 junio de 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 [1982], en vigor el 21 de octubre de 1986)

30 Las normas abiertas son normas que se ponen a disposición de la población general y que se elaboran (o aprueban) y preservan mediante un proceso colaborativo y consensual. Las "normas abiertas" facilitan la interoperabilidad y el intercambio de datos entre diferentes productos o servicios, y están destinadas a aplicarse de forma generalizada (adaptado del UIT-T).

normas[31] y principios[32] adecuados existentes y que se aseguren de que las fuentes autorizadas y, sobre todo, sus sistemas de identificación, sean inclusivos, que protejan los datos y los derechos de las personas y que estén diseñados para favorecer la economía continental y la integración social.

3.2. MODELO

El Marco propondrá una aplicación en tres fases:

1

Aprobación del Marco de la UA y creación del marco legislativo propicio.

2

Aplicación del Marco y aprobación de las especificaciones técnicas para la IDC-ID.

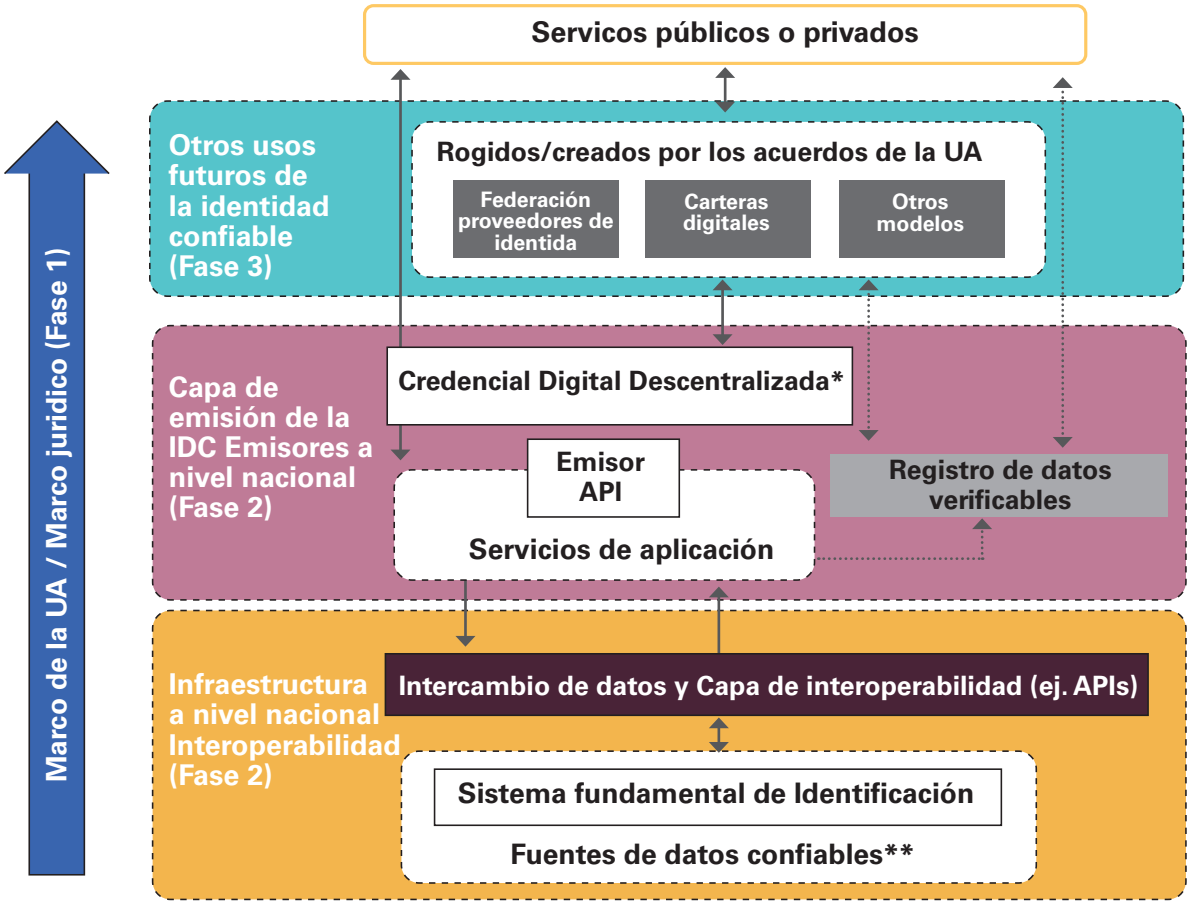
3

Ampliación de la aplicación del Marco y la provisión de una infraestructura que permita casos de uso más avanzados, como la autenticación a distancia.

31 Que incluyen, entre otras, el Convenio de Budapest sobre ciberdelincuencia, los Principios y recomendaciones sobre sistemas de estadísticas vitales de la CEI, ISO y el UIT-T, normas internacionales sobre protección de datos (como el Reglamento General de Protección de Datos de la EU y el Convenio 108 del Consejo de Europa), normas mundiales y regionales y marcos de confianza para la identificación.

32 Tales como los Diez Principios sobre la identificación para el desarrollo sostenible, que han sido ratificados por 30 organizaciones internacionales y regionales, incluidas instituciones africanas como la CEPA, el Banco Africano de Desarrollo (BAFD) y Smart Africa, y aprobadas también por varios países africanos. Consultar: https://id4d.worldbank.org/principles, y los Principios sobre desarrollo digital, que han sido ratificados por más de 200 organizaciones: https://digitalprinciples.org/.

GRÁFICO 1 – ENFOQUE DE APLICACIÓN POR FASES DEL MARCO



** Los estados miembros de la UA debatirán ulteriormente los detalles de la aplicación de la fase 2.*

*** Los estados miembros decidirán qué fuentes de datos confiables comportarán sus sistemas de identificación fundamental*

La IDC-ID garantizará que la **autoridad emisora no conozca a qué servicios accede el particular con sus identificaciones digitales,** aunque se podrá comprobar la autenticidad de las credenciales de identidad. Esto proporciona garantías en términos de confidencialidad y protección de datos y, para el particular, un mayor control del modo en que se usan sus datos.

La capa de infraestructura permitirá unos casos de uso más avanzados y consistirá en conectar las credenciales de identidad emitidas con el formato de la IDC-ID con los particulares. Los estados miembros de la UA disponen de varias opciones técnicas para desarrollar esta infraestructura: una federación de proveedores de identidad que ofrezca mecanismos de autenticación a los titulares de la IDC-ID, el desarrollo de soluciones de cartera de identidad digital u otros modelos que permitan la interoperabilidad. Cada una de estas aplicaciones puede ofrecer un enfoque de minimización de datos y servicios de divulgación selectiva para casos de uso específicos, como por ejemplo, compartir solamente los datos pertinentes desde una tarjeta de identidad y un informe crediticio para solicitar un préstamo, solicitar prestaciones sociales o sanitarias, recibir una pensión, solicitar becas o anonimizar el conjunto de datos mínimo la IDC-ID (nombre y fecha de nacimiento) para que se transforme en un justificante de mayoría de edad (más de 18 o 21 años o una respuesta de sí/no).

3.2.1. COMPONENTES ESTRUCTURALES

Las fuentes de datos confiables deben acogerse a normas establecidas por el Marco de la UA para la calidad e integridad de los datos. En muchos casos, los sistemas de identificación digital fundamental (cuyas fuentes de datos confiables serán aprobadas por los estados miembros) desempeñarán esta función, puesto que pueden proporcionar una prueba de identidad jurídica.

El gráfico 1 describe la ampliación del acceso a los sistemas nacionales existentes y a las fuentes de datos confiables mediante una capa de intercambio de datos e interoperabilidad basada en normas y protocolos que permiten la emisión de IDC confiables. Los proveedores de servicios han de verificar y recuperar datos de identidad jurídica al crear credenciales fundamentales de identidad digital.

La capa de emisión de la IDC describe la emisión normalizada de la credencial IDC basándose en la fuente de datos confiable del sistema de identificación de nivel fundamental/nacional. Cada emisor de credencial (como mínimo, uno por cada estado miembro participante) dispondrá de un número de funciones clave (aunque no haya que limitarse a ellas):

- Una API emisora que permitan a las carteras u otros sistemas solicitar y recuperar credenciales.
- Un registro de datos verificables que permita la verificación de los identificadores y la comprobación de la revocación de la credencial.
- Gestión de claves criptográficas.
- Visibilidad y transparencia del uso de la credencial para el titular de una credencial IDC.
- Proporcionar los metadatos de la credencial junto a cada credencial emitida con el objetivo de informar sobre la calidad, origen y nivel de confianza asociada a la credencial emitida.

3.2.2. REQUISITOS A NIVEL NACIONAL E INTEROPERABILIDAD

No existe ningún requisito de reestructuración de los sistemas de identidad domésticos existentes para que alcancen la interoperabilidad a nivel continental. En cambio, se aprobarán normas para la interoperabilidad de los datos, interoperaciones técnicas a través de las API y protocolos y presentación técnica de las credenciales. La emisión de las credenciales, así como su creación, se encuentra lógicamente separada de los sistemas nacionales existentes, pero quedarían bajo el control de los servicios nacionales responsables.

Aunque la confianza técnica no requiera una infraestructura de clave pública continental u otra infraestructura supranacional, gracias a la criptografía avanzada, esta provendrá de la preferencia o capacidad del estado miembro de la UA para utilizar una infraestructura de clave pública nacional (en el caso en el que se use) u otra alternativa legalmente reconocida. Todos los estados miembros de la UA seguirán ejerciendo su soberanía nacional en cuanto al diseño de los sistemas de identidad nacional y el modo en el que dichos sistemas interactúan con el Marco de la UA.

3.2.3. NORMAS PARA LA PARTICIPACIÓN DE LAS FUENTES DE DATOS CONFIABLES

Las normas se establecerán siguiendo el Marco de la UA, con el objetivo de garantizar la calidad, seguridad, fiabilidad y un nivel mínimo de garantía de cada fuente de datos confiable. Los sistemas de los estados miembros deberían demostrar que han alcanzado los requisitos mínimos antes de participar en el Marco de la UA y comenzar a emitir credenciales de IDC conformes. Los estados miembros de la UA determinarán de común acuerdo el carácter de estas normas.

3.3. PROCESOS CONFIABLES – EL MARCO DE CONFIANZA

El marco de confianza describe claramente las reglas de participación de las diferentes entidades (por ejemplo, emisores, titulares y verificadores de la identidad), el funcionamiento del Marco y los requisitos técnicos para la interoperabilidad de las credenciales confiables.

Esto permitirá que todas las entidades acepten las credenciales compartidas por los titulares de identidad gracias a la confianza que establece la autoridad emisora (en el caso de la credencial) y los procesos que cada parte ha acordado seguir dentro del marco de confianza.

Se espera que los estados miembros elaboren un borrador de las siguientes secciones clave como partes integrantes del marco de confianza.

3.3.1. FUNCIONES Y RESPONSABILIDADES

Para conservar la confianza, se deberá definir de forma clara cada entidad (por ejemplo, un emisor de credenciales) y sus responsabilidades, como la gestión segura y protegida de datos y servicios, así como la notificación de incidentes.

Se espera que figuren en el marco de confianza las siguientes entidades fundamentales:

- Las **autoridades confiables:** fuentes de datos autorizadas para comprobar jurídicamente la identidad, según lo ratifiquen los estados miembros de la UA.
- Los **emisores**: entidades encargadas de expedir al titular la prueba de identidad jurídica, según el formato digital normalizado del Marco. Las autoridades confiables pueden emitir las credenciales o mandatar a otra entidad que posea mayores competencias en la materia (por ejemplo, un servicio de TIC o empresas privadas).
- El/La **titular** de la IDC-ID: persona que posee una o más credenciales digitales. El/La titular puede ser, aunque no siempre, objeto de los atributos compartidos a través de la IDC.
- El **verificador**: parte confiante (por ejemplo, un proveedor de servicios público o privado) que desea verificar la declaración de identidad de un sujeto determinado.
- **Los proveedores de identidad, los proveedores de credenciales y los proveedores de carteras digitales:** proporcionan un autenticador con el objetivo de vincular la identidad del titular a las credenciales y así permitir casos de uso que necesitan autenticación a distancia más avanzados, contribuyendo ampliamente a este sistema.

Un **órgano independiente de supervisión,** creado por los estados miembros, será necesario para garantizar que las entidades participantes respeten las reglas establecidas por el marco de confianza y establezcan las herramientas y tecnologías mínimas necesarias para su cumplimiento. Este órgano de supervisión también debería encargarse de concienciar sobre las competencias en materia de ciberresiliencia en todo el continente para garantizar la sostenibilidad del marco.

3.3.2. REGLAS DE PARTICIPACIÓN

Las reglas de participación deben incluir unos requisitos jurídicos, operacionales u organizacionales mínimos, necesarios y confiables para toda entidad autorizada que ofrezca un servicio de acuerdo al marco de confianza. Por ejemplo, a un emisor se le puede exigir que posea un acuerdo oficial (de una fuente autorizada o de un servicio gubernamental) para ejercer su actividad.

A los servicios que acepten la IDC-ID se les puede pedir que confirmen su conformidad con los requisitos de confidencialidad, privacidad y compensación (para titulares de identidad) de referencia.

Del mismo modo, se podrá exigir un memorando de entendimiento para garantizar que todas las entidades operativas aceptan los términos del marco de confianza.

3.3.3. GOBERNANZA

Se exigirán mecanismos de gobernanza, que han de ser ratificados por los estados miembros de la UA, con el objetivo de establecer y garantizar las reglas del marco de confianza, aprobar los cambios efectuados en los requisitos de interoperabilidad y delegar la responsabilidad de redacción/elaboración de las modificaciones efectuadas en el Marco a subgrupos de gobernanza, si resultase necesario.

Es preciso que los estados miembros de la UA creen un órgano de supervisión independiente que garantice que las entidades participantes respetan en todo momento las reglas establecidas por el marco de confianza. Este órgano también podría ser responsable de garantizar que todas las partes cumplen formalmente con las normas y que, en caso contrario, se les audite o que rindan cuentas según como se considere necesario, por ejemplo, en caso de violación de datos.

La protección de los particulares debería ser primordial. El órgano de supervisión debe estar facultado para recibir denuncias de titulares de la IDC-ID víctimas de malas prácticas, violación de datos, robo de identidad y otros incidentes relacionados con la identidad digital, así como para tomar medidas al respecto. También debe ser el eje central para los mecanismos de compensación, aunque se trate solo de una función de coordinación, y debería actuar como defensor de los particulares y de sus derechos.

3.3.4. REQUISITOS DE INTEROPERABILIDAD

3.3.4.1. NIVELES DE SEGURIDAD

Puesto que se trata de un medio para comunicar el nivel de confianza de la credencial que presenta un titular a un verificador, el Marco debería definir las condiciones necesarias para

alcanzar cada nivel gracias a la verificación de la identidad por parte de una fuente autorizada, al proceso de emisión y a los medios de conservar y presentar una credencial.

3.3.4.2. CONJUNTO DE DATOS MÍNIMO

La cantidad mínima de datos sobre la identidad de un titular tal y como aparecen en una credencial de identidad debería ser adecuada para la identificación de la persona en la mayoría de las operaciones corrientes, siempre que respete el principio de minimización de datos. Los atributos los puede facilitar una entidad confiable diferente.

El órgano rector será libre de definir la manera en que las declaraciones adicionales (conjunto de datos) pueden añadirse de forma opcional al marco de confianza. Toda emisión de las respectivas credenciales debe cumplir con las mismas condiciones y reglas que los emisores de credenciales de identidad fundamental.

3.3.5. REQUISITOS TÉCNICOS

3.3.5.1. SEGURIDAD

Cada entidad que ofrece un servicio dentro de la infraestructura de identidad debería definir los requisitos de seguridad de referencia.

3.3.5.2. PRUEBA CRIPTOGRÁFICA

Las credenciales se podrán verificar mediante la inclusión de una firma digital creada por la autoridad emisora. La comprobación de la validez de la firma sirve de prueba criptográfica de que la declaración que realiza el titular al presentar la credencial puede ser de confianza. Se necesitará una clave pública para poder comprobar la firma digital. La clave pública se puede proporcionar mediante un método descentralizado o centralizado, que tendrá que fijarse dentro del marco de confianza y de sus requisitos técnicos.

3.3.5.3. FORMATO DE LA CREDENCIAL

Las especificaciones técnicas para la creación y la transmisión de credenciales se deben definir sobre la base de normas existentes, tales como las credenciales verificables del W3C cuando corresponda.

- La **credencial de identidad digital interoperable (IDC-ID)** es un conjunto de declaraciones de identidad (por ejemplo, atributos) y la relación efectuada por un emisor que puede verificarse de forma criptográfica. Concretamente se compone de:
    - metadatos de la credencial sobre el tipo de credencial emitida, fecha de emisión y nombre del emisor;
    - información sobre el titular de la declaración y la declaración de identidad real (por ejemplo, la fecha de nacimiento);
    - prueba de autenticidad, que a menudo es una firma digital.

El titular de la IDC-ID tiene la capacidad de generar presentaciones verificables de una o más IDC-ID de tal modo que la autenticad de la declaración se puede seguir verificando (por ejemplo, la divulgación selectiva).

3.4. POSIBLES OPCIONES DE AUTENTICACIÓN

Se pueden adoptar varios enfoques estructurales con el objetivo de permitir que el titular de la IDC-ID se identifique con un nivel de garantía dado. Todas las opciones que se citan a continuación pueden coexistir y aplicarse en diferentes niveles de cooperación (por ejemplo, entre determinados agentes sectoriales o las REC).

Se podrán explorar otras opciones en función de la disponibilidad de tecnologías diferentes que posean prácticas de aplicación probadas.

3.4.1. OPCIÓN 1 – CARTERAS DIGITALES PERSONALES

Esta opción consiste en proporcionar a las personas y a las empresas una cartera digital personal que contenga una prueba verificable de atributos de identidad jurídica, que se puede usar para demostrar su identidad o para compartir hechos específicos con el proveedor de servicios. Esta opción de estructura corresponde a los casos de uso de credenciales verificables del W3C.[33]

GRÁFICO 2 – DESCRIPCIÓN DE LA OPCIÓN 1 - CARTERAS DIGITALES PERSONALES

PROCESO DE AUTENTICACIÓN

1. La persona elige un proveedor de cartera de identidad para almacenar su IDC y es necesario un proceso de integración.
2. La persona recibe una IDC verificable (por ejemplo, una identificación o justificante de dirección) de la fuente autorizada emisora y la almacena en una cartera digital.
3. Al mismo tiempo, la autoridad guarda una impresión digital de la declaración en una infraestructura de clave pública descentralizada teniendo en cuenta la privacidad de los ciudadanos.
4. Las personas pueden usar su cartera para presentar a un proveedor de servicios (por ejemplo, a una aseguradora) una declaración, como por ejemplo, un justificante de domicilio (mediante un código QR, Bluetooth o NFC)

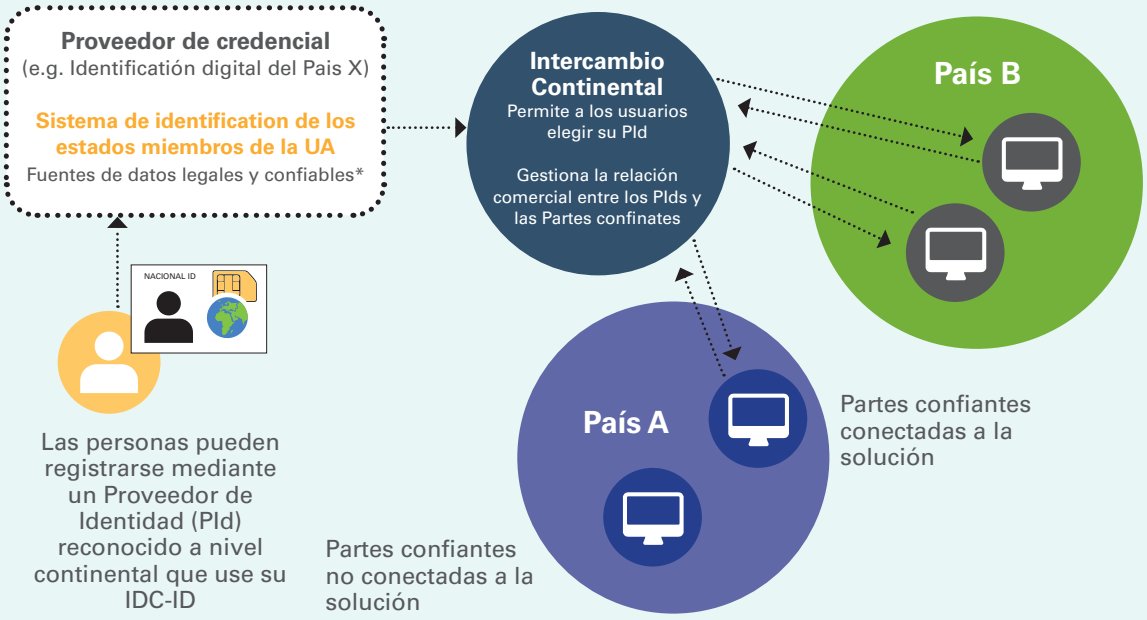
33 W3C, Verifiable Credentials Use cases [Casos de uso de credenciales verificables], consultar: https://www.w3.org/TR/vc-use-cases/

5. El proveedor de servicios puede comprobar en la infraestructura de clave pública descentralizada que la declaración es auténtica y que la ha emitido una autoridad reconocida.

3.4.2. OPCIÓN 2 – FEDERACIÓN DE IDENTIFICACIÓN DIGITAL CONTINENTAL

Con este modelo, todos los residentes en África podrán conectarse con un proveedor de credencial de su elección a nivel continental.

GRÁFICO 3 – DESCRIPCIÓN DE LA OPCIÓN 2 – FEDERACIÓN DE IDENTIFICACIÓN DIGITAL CONTINENTAL



* Los estados miembros decidirán qué fuentes de datos de confianza contienen sus sistemas de identificación fundamental.

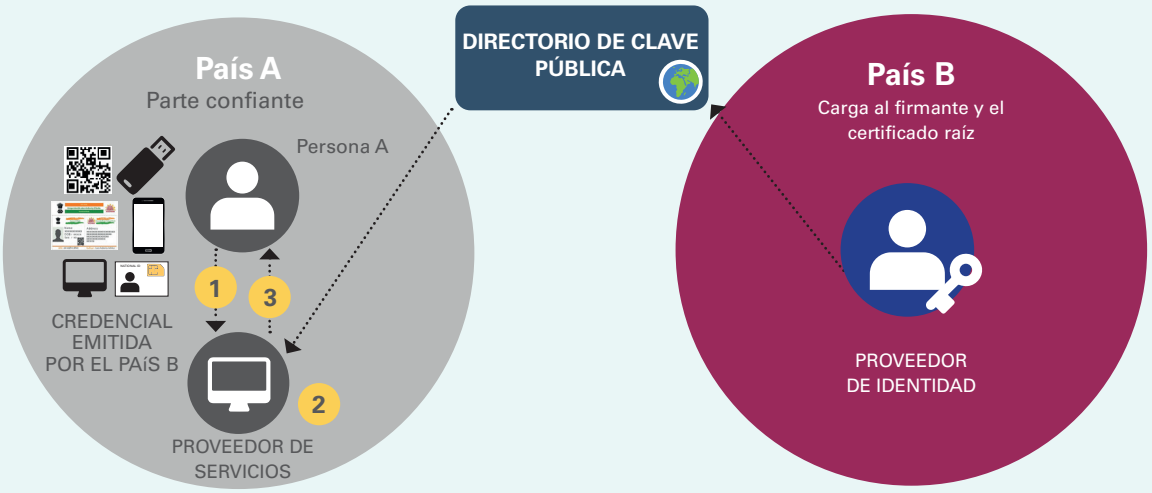
PROCESO DE AUTENTICACIÓN

1. **Se crea una federación de proveedores de credenciales de identificación continental:** operadores de telecomunicaciones, bancos, gobiernos, etc., que pueden ofrecer servicios de autenticación.
2. Se establece un intercambio continental, que ofrece un único punto de contacto a todos los proveedores de credenciales participantes y otras partes confiantes que deseen autenticar personas.
3. Las personas pueden usar su IDC emitido por una fuente autorizada (por ejemplo, un sistema de identificación legal) para conectarse con un proveedor de credencial de su elección. El proveedor de credencial puede comprobar la autenticidad de la IDC.
4. Si la verificación funciona, el proveedor de credencial expide un medio de autenticación a la persona.
5. La persona puede usar su medio de autenticación para acceder a los servicios en línea y en persona que se encuentran conectados al intercambio continental.

3.4.3. OPCIÓN 3 – CREDENCIALES FIRMADAS DIGITALMENTE

Este modelo permite la autenticación mediante la verificación de los datos de identidad firmados digitalmente en una credencial que usa una clave pública. Se trata también de otro medio para compartir la foto del titular.

GRÁFICO 4 – DESCRIPCIÓN DE LA OPCIÓN 3 – CREDENCIALES FIRMADAS



PROCESO DE AUTENTICACIÓN

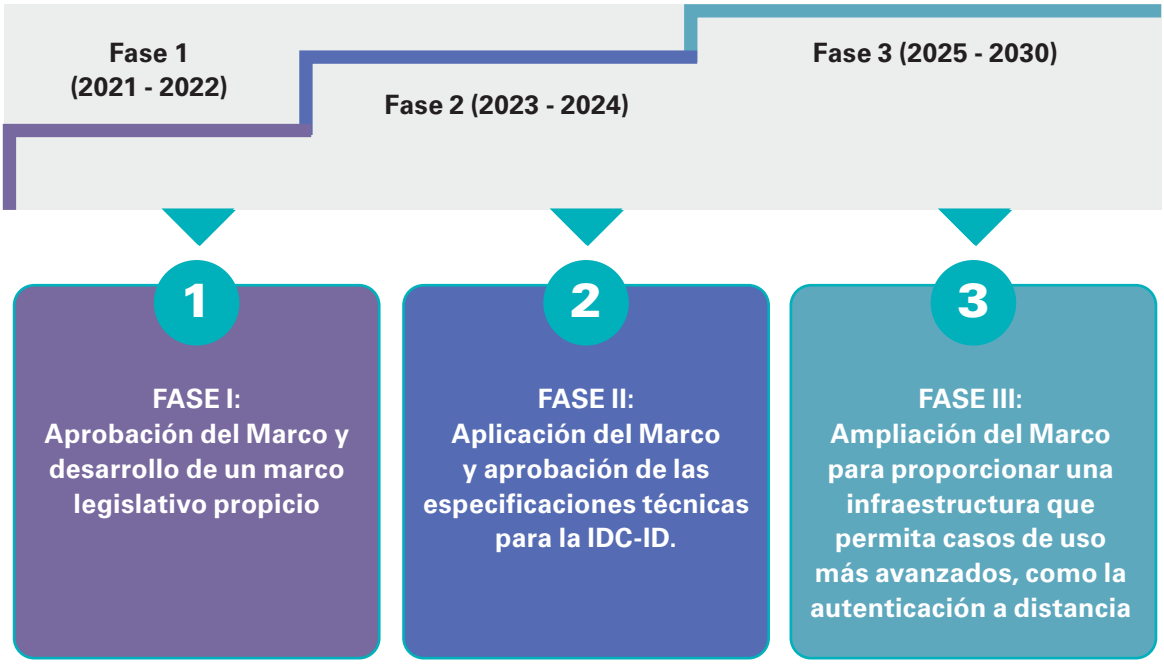
1. Los países acuerdan una norma (por ejemplo, el código QR) y las fuentes autorizadas firman las credenciales de forma criptográfica (mediante una clave privada).
2. Las fuentes autorizadas comparten su clave pública en un Directorio de clave pública, cuya gobernanza ratificarán los estados miembros de la UA y que será gestionado a nivel continental.
3. Los países crean un servicio aparte que permite compartir una copia de la fotografía del titular de la IDC-ID, accesible mediante una API segura con el objetivo de autenticar al titular. Para que funcione sin conexión, también cabe la posibilidad de que un grupo de países (por ejemplo, las REC) aprueben la emisión de una credencial física que contenga la foto del titular.[34]
4. Las fuentes autorizadas de los países emiten a las personas formas normalizadas de IDC.
5. Se crea un software de verificación (aplicación o sitio web) para permitir que los proveedores de servicios verifiquen la autenticidad y la integridad de la firma de la IDC.
6. Los particulares pueden usar su IDC para que otros organismos públicos o privados de su país o del extranjero verifiquen digitalmente su identidad jurídica y puedan así acceder a servicios.
7. Se espera de cada estado miembro que conserve las claves privadas, los certificados raíz y los algoritmos de hash que se usan en el cifrado y en la verificación de integridad en almacenamientos seguros, como por ejemplo, módulos de seguridad de hardware (HSM).

34 La emisión de las credenciales físicas genera un coste adicional. Los estados miembros tendrían que debatir ulteriormente sobre la financiación de esta solución con el objetivo de evitar crear barreras de acceso.

4. HOJA DE RUTA DE ALTO NIVEL PARA LA APLICACIÓN

Para acelerar el cumplimiento de los ambiciosos objetivos de este Marco, los estados miembros de la UA deberían reforzar su colaboración para afinar los detalles del marco técnico y de referencia, y las normas y procedimientos comunes.

Se propone dividir la aplicación del Marco en tres fases, como se muestra a continuación:



Para cada fase, está previsto que se creen oportunidades para consultar a los estados miembros de la UA, a la sociedad civil y a los actores de los ecosistemas de identidad con el objetivo de garantizar que el Marco y su aplicación siguen ajustándose a las necesidades de los particulares y a las realidades locales. Se publicará documentación fundamental y se dará un plazo razonable para realizar consultas y contribuciones

4.1. FASE 1: APROBACIÓN DEL MARCO Y CREACIÓN DE UN ENTORNO PROPICIO

Submission of the draft Framework to the 4th ordinary session of the STC on communication and ICT for adoption and the endorsement by policy organs.

Following the endorsement of the present document, the details of the Trust Framework will be further specified and the following activities will be conducted notably:

- Sensibilización.
- Estudio de viabilidad sobre el panorama actual del sistema de identificación digital en África.

- Establecimiento de un marco de consulta para los actores del ecosistema digital destinado a proteger los intereses de cada uno de ellos.
- Creación de instrumentos jurídicos y normativos armonizados.
- Definición de las reglas de participación.
- Creación de mecanismos de gobernanza y de un foro para compartir buenas prácticas a lo largo del proceso de implantación.
- Creación de disposiciones jurídicas que se integrarán en los ámbitos jurídicos nacionales de los estados miembros para aplicar el Marco. Asimismo, se incluirán garantías apropiadas en materia de protección de datos y ciberseguridad.
- Ratificación de la Convención de Malabo sobre ciberseguridad y protección de datos personales.
- Aprobación del marco continental sobre política de datos.
- Constitución de grupos de expertos por parte de los estados miembros de la UA para definir la interoperabilidad y los requisitos técnicos.
- Creación de estructuras institucionales independientes y nacionales (Áreas protegidas –AP– de datos, Controlador de Autoridad Certificadora y equipos de respuesta a incidentes de seguridad informática o CIRT) y fortalecimiento de la cooperación entre las instituciones nacionales.
- Desarrollo de iniciativas para la formación de capacidades.
- Apoyo al despliegue de la infraestructura digital, incluyendo los centros de datos a nivel nacional, regional o continental necesarios para sustentar y mantener la operatividad de los sistemas de identificación digital.
- Movilización de recursos.

Con el fin de garantizar el éxito del Marco, se definirán una serie de casos de uso que representen numerosas oportunidades para el continente. Un grupo de estados miembros de la UA trabajará ulteriormente para ensayar un proyecto piloto de casos de uso específicos, junto a otros actores si fuese necesario.

Se debe llevar a cabo una evaluación de los principales costes y beneficios del Marco propuesto y de las opciones de autenticación posteriores para proporcionar una mayor visibilidad de las necesidades de financiación, y así asesorar a los estados miembros de la UA en la toma de decisiones. Actualmente, se prevé que el cumplimiento de una norma armonizada que presente información sobre la identidad generará unos costes limitados para los estados miembros de la UA, ya que se podrá integrar como un requisito técnico en los proyectos de digitalización existentes de sus sistemas de identificación digital fundamental. Sin embargo, la creación de la infraestructura para la autenticación se prevé que genere otros costes y que, en función de los actores implicados, sea necesario la implantación de modelos empresariales. En esta fase, se tendrá que llevar a cabo una detallada evaluación del impacto previsto para garantizar que las opciones de autenticación propuestas siguen siendo incluyentes.

Al mismo tiempo, los estados miembros de la UA se comprometen a:

- desarrollar e implementar marcos legales y normativos propicios que generen confianza en los sistemas de identificación digital fundamental;
- establecer una normativa y regulaciones armonizadas en materia de protección de datos que potencien el papel de los particulares, al mismo tiempo que se preserva la soberanía de los datos;
- desplegar la infraestructura digital, incluida la infraestructura de datos (centros de datos nacionales), que es la base para el funcionamiento del sistema de identificación digital;
- ratificar (si no se ha hecho ya) el Convenio de la Unión Africana sobre ciberseguridad y protección de datos personales y agilizar su entrada en vigor, así como trabajar para acelerar la creación de organismos de protección de datos en varios países para establecer un control;
- elaborar la estrategia nacional de ciberseguridad y establecer equipos de respuesta a incidentes informáticos (CIRT) para mitigar los riesgos y amenazas relacionados con los ciberataques, el robo de datos y el mal uso de la información confidencial;
- aprobar el marco continental en materia de política de datos de la UA, el cual insta a que los sistemas de identificación digital se construyan y apliquen de forma cohesionada en consonancia con un marco general de gobernanza de datos que asegure las garantías oportunas a la hora de combinar y reutilizar los datos administrativos públicos que generan los sistemas de identificación digital. Esto debería potenciar el papel de los particulares y proteger la privacidad en la red como un derecho fundamental (que abarca el derecho del usuario a elegir y controlar el consentimiento informado/significativo, la soberanía/propiedad de datos, etc.);
- emprender o reforzar la labor de potenciación de los sistemas de identificación digital fundamental para garantizar que sean inclusivos y confiables de acuerdo a normas e iniciativas pertinentes, tales como el Programa Africano para acelerar la mejora del registro civil y las estadísticas vitales (APAI-CRVS) y los *Principios sobre identificación para el desarrollo sostenible.*

Estas fases concluirán con la aprobación de la versión completa del Marco por parte de los estados miembros de la UA.

4.2. FASE 2: APLICACIÓN DEL MARCO Y APROBACIÓN DE LAS ESPECIFICACIONES TÉCNICAS PARA LA CREDENCIAL DE IDENTIDAD DIGITAL INTEROPERABLE (IDC-ID)

La segunda fase consistirá en crear el marco de confianza y los mecanismos de gobernanza y cooperación, así como proporcionar la especificación técnica para la introducción de la IDC-ID, que comprenderá:

- el desarrollo de estándares y normas mínimas para la interoperabilidad;
- la atribución de perfiles para el conjunto de datos mínimo (formatos de datos) y metadatos asociados;
- el formato de presentación (por ejemplo, códigos de barras en 2D, credenciales verificables del W3C);

- el nivel de garantía (como punto de referencia para la interoperabilidad);
- los elementos criptográficos para la firma de datos y el cifrado;
- la verificación de protocolos para casos de uso con y sin conexión.

Un grupo de estados miembros de la UA podrá desarrollar una **ejecución de prueba** (aplicación o sitio web) para la verificación de base de las IDC-ID, con el objetivo de comprobar la interoperabilidad de la credencial y aportar así pruebas verificables de identidad jurídica. La ejecución pondrá en práctica la privacidad y la seguridad mediante el diseño.

Se podrá estudiar un acuerdo sobre la **definición de soluciones alternativas** para obtener una IDC-ID para personas que se encuentren actualmente fuera de los sistemas de identificación digital fundamental.

Se elaborará una **cartografía de otras iniciativas en curso de la Unión Africana** que puedan contribuir al Marco (por ejemplo, el Marco africano de cualificaciones)

La Fase 2 llegará a su fin con la formulación de un **plan de acción claro para la definición de la infraestructura de autenticación** como parte de la Fase 3

4.3. FASE 3: DESARROLLO DE LA INFRAESTRUCTURA PARA PONER EN SERVICIO LA AUTENTICACIÓN A DISTANCIA

La Fase 3 comenzará con la ejecución del marco de confianza definido en la Fase 2.

En esta fase, la capa que representa la emisión de la IDC-ID se ampliará y extenderá para adoptar una infraestructura que permita casos de uso más avanzados, como la autenticación a distancia. Esta capa de autenticación permitirá a los particulares demostrar su identidad digitalmente mediante el control de uno o más factores de autenticación que se encuentren vinculados a su identidad jurídica previamente verificada (por ejemplo, un código biométrico o PIN). Los estados miembros de la UA disponen de varias opciones técnicas para poner en práctica esta capa, por ejemplo, una federación de proveedores de identidad que ofrezca mecanismos de autenticación a los titulares de la IDC-ID, el desarrollo de soluciones de cartera de identidad digital o cualquier otro modelo que permita la interoperabilidad. Cada una de estas aplicaciones puede ofrecer un enfoque de minimización de datos y servicios de divulgación selectiva para casos de uso específicos, entre los que se encuentran: compartir solamente los datos pertinentes desde una tarjeta de identidad, un informe crediticio para pedir un préstamo, solicitar prestaciones sociales o sanitarias, recibir una pensión, en los que la autenticación es un requisito legal, o anonimizar el conjunto de datos mínimo la IDC-ID (nombre y fecha de nacimiento) para que se transforme en un justificante de mayoría de edad (más de 18 o 21 años, o una respuesta de sí/no).

Igualmente, los estados miembros de la Unión Africana podrán buscar acuerdos sobre la manera en que ha de crearse la infraestructura necesaria para esta capa de autenticación y asociarse con las REC y otras iniciativas continentales que ya están estudiando la introducción de soluciones interoperables de identificación digital para acceder a servicios a distancia. De hecho, los estados miembros y las organizaciones podrán impulsar una presentación común de información de identidad de forma confiable y segura, y agregarle otros servicios.

Los estados miembros de la UA continuarán colaborando para reforzar el marco de confianza y los mecanismos de gobernanza y cooperación tras alcanzar un acuerdo sobre las siguientes infraestructuras adicionales:

- **Coordinación con otras iniciativas** con el fin de establecer la interoperabilidad a nivel continental (por ejemplo la SATA o las REC).

- **Un acuerdo sobre la opción estructural más idónea** (por ejemplo, una federación o carteras digitales) para desarrollar el tipo de autenticación a distancia que se basaría en las credenciales digitales interoperables (IDC-ID).

La Fase 3 concluirá con un plan de acción claro sobre la aplicación de la capa de autenticación, de acuerdo con la opción estructural que los estados miembros de la UA y las organizaciones tendrán que corroborar.

5. SUPUESTOS, RETOS Y RIESGOS DE ALTO NIVEL

5.1. SUPUESTOS

Los estados miembros aprobarán el Marco y colaborarán entre sí para, comprometidos a aplicarlo, emprender las reformas jurídicas y normativas necesarias.

5.2. RETOS GENERALES Y MEDIDAS DE MITIGACIÓN DE ALTO NIVEL

El siguiente cuadro resume los retos generales y las medidas de mitigación propuestas:

#	Retos	Medidas de mitigación propuestas
1	Exclusión, escasa seguridad y deterioro de la protección de datos personales	Aplicar los principios definidos en el Marco (3.1) y reforzar el marco jurídico en materia de seguridad y protección de datos, así como la infraestructura en los países miembros de la UA.
2	Reticencia de los estados miembros de la UA a aprobar y ejecutar el Marco	Concienciar sobre el beneficio del Marco de Interoperabilidad, tanto a nivel doméstico como continental y reforzar el sistema fundamental de identificación.
3	Falta de capacidad técnica y financiera de los estados miembros de la UA	Aumentar la capacidad y promover los intercambios de conocimiento entre iguales, así como considerar el principio de coste-eficacia de las soluciones tecnológicas que han de acordarse en las Fases 2 y 3.
4	Centros de datos inadecuados a nivel nacional/regional/continental.	Construir centros de datos nacionales/ regionales/continentales e incitar a África a usarlos.

5.3. RIESGOS Y MEDIDAS DE MITIGACIÓN PROPUESTAS

El siguiente cuadro resume los riesgos y las medidas de mitigación propuestas:

#	Riesgos	Medidas de mitigación propuestas
1	Ausencia de una definición adecuada de las normas comunes. Falta de acuerdo entre los países miembros de la UA. Fracaso en la aprobación y seguimiento de normas comunes.	Definición de las normas y comunicación de las mismas a los estados miembros de la UA durante su aplicación. Seguimiento periódico por parte de un órgano panafricano confiable y autorizado, que todos los estados miembros apoyen y ratifiquen, para garantizar el cumplimiento de las normas. Debates y grupos de trabajo especializados con los diferentes actores para garantizar una definición clara de las normas aplicables a la estrategia de ejecución elegida. Análisis comparativo de la estrategia de ejecución basada en normas de los estados miembros de la UA frente a normas similares existentes que se basan en programas de identificación fundamental nacional de todos los estados miembros de la UA.
2	Los bajos niveles de confianza entre las autoridades nacionales con capacidades de ejecución heterogéneas conducen a una lenta adopción del marco Marco a gran escala continental. Además, la falta de voluntad de los estados miembros para aceptar un organismo de supervisión supranacional, ralentiza la aplicación del marco de confianza.	El Marco debería aspirar a la armonización y el reconocimiento mutuo como objetivo a largo plazo, además de mantenerse abierto a que se desarrollen soluciones flexibles y eficaces que puedan crear mecanismos de auditoría compartidos entre los países dispuestos a instaurar confianza entre ellos, sin perder la soberanía –mediante el reconocimiento unilateral de los certificados de confianza emitidos.
3	La solución, los beneficios y las opciones no se adaptan debidamente al entorno local o bien la información no se difunde de forma adecuada y las personas no usan la solución, lo que lleva a una utilización escasa de esta y, en definitiva, a unos costes elevados y a un beneficio mínimo.	Desarrollar estructuras potentes basadas en un diseño centrado en el usuario para identificar qué soluciones son fáciles de usar y accesibles a todos. Poner en marcha, en todos los estados miembros, mecanismos de difusión sólidos que asocien a todos los actores locales que comparten los mismos intereses.

#	Riesgos	Medidas de mitigación propuestas
4	Los estados miembros decidirán la tecnología más adecuada durante la fase de aplicación. Sin embargo, si optan por la infraestructura de clave pública, a falta de una institución certificadora continental y de una gobernanza adecuada, los requisitos criptográficos para la firma digital pueden suponer un obstáculo para crear un sistema de interoperabilidad.	La creación de un marco jurídico que permita la fundación de una institución coordinadora continental, incentivada por una estructura equitativa de gobernanza que controle la soberanía de cada estado miembro en materia de aplicación y gestión de las firmas digitales, su emisión, revocación, así como su oportuna renovación y actualización. La creación de una estructura organizativa exhaustiva y dinámica para permitir la gobernanza de la firma digital / infraestructura de clave pública a lo largo de la aplicación y de la fase operativa.
5	Debido a datos erróneos e incompletos, la estrategia de diseño y de aplicación de algunos de los componentes, como las firmas digitales, puede verse afectada. El retraso en el intercambio de datos e información pertinentes del ciudadano o residente también podría afectar al calendario del proyecto.	Reuniones con los servicios gubernamentales para recopilar datos con el objetivo de cubrir las lagunas de información, aprovechando la experiencia de los expertos mediante el aprendizaje entre iguales con el fin de incentivar la colaboración y la propiedad regional y continental. Hacer un seguimiento del calendario del proyecto y los objetivos para evitar retrasos. También resulta fundamental establecer un calendario de ejecución completo y detallado que haya sido aprobado previamente por los estados miembros de la UA y los principales actores.
6	Ausencia de directivas de gestión del cambio claramente definidas para garantizar que el Marco cumple con las prácticas vigentes, las necesidades y el desarrollo tecnológico.	Poner en marcha un procedimiento de gestión del cambio sólido y bien definido como parte del marco de gobernanza.

#	Riesgos	Medidas de mitigación propuestas
7	Los estados miembros decidirán la tecnología más adecuada durante la fase de aplicación. Sin embargo, si optan por la infraestructura de clave pública, es probable que las entidades de certificación de África no alcancen un consenso con respecto a la gestión de la infraestructura de clave pública cuando se implante en todo el continente. En segundo lugar, puede que no se llegue a un consenso sobre la creación del intercambio de firmas digitales.	Los estados miembros de la UA crearán una nueva institución de certificación para la gestión de la infraestructura de clave pública continental o ratificarán un mecanismo para reunir a las entidades existentes en una plataforma común.
8	No contar con un marco jurídico mínimo necesario a nivel nacional y regional.	Los estados miembros de la UA deben acelerar la aplicación de los marcos jurídicos y reglamentarios armonizados pertinentes.

6. ANEXO

6.1 DEFINICIONES PRÁCTICAS

Armonización: se trata de garantizar la uniformidad de los sistemas mediante el uso de las normas mínimas para facilitar la interoperabilidad y los marcos legales y de confianza (por ejemplo, para los niveles de seguridad), con el objetivo de establecer reglas y de reforzar la seguridad en los sistemas respectivos.

Atributo: se refiere a una determinada cualidad o característica inherente o atribuida a alguien o a algo (adaptado del Instituto Nacional de Estándares y Tecnología - NIST 800-63:2017). En los sistemas de identificación, los atributos de identidad más comunes son el nombre, la edad, el sexo, el lugar de nacimiento, la dirección, las huellas dactilares, la fotografía, la firma, el número de identidad, etc.

Autenticación: se trata del proceso por el que se garantiza que una persona es quien declara ser. La autenticación digital se refiere, de forma general, a una persona que presenta electrónicamente uno o más "factores" para "afirmar" su identidad, esto es, para demostrar que se trata de la misma persona a la que, en su momento, se le emitió la credencial. Dichos factores corresponden a algo que la persona conoce (por ejemplo, una contraseña o un PIN), tiene (por ejemplo, un documento de identidad, una ficha o una tarjeta SIM) o la define (por ejemplo, sus huellas dactilares) (adaptado del Instituto Nacional de Estándares y Tecnología - NIST 800-63:2017).

Autoridad de protección de datos: se trata de autoridades públicas independientes, dotadas de facultades de investigación y de enmienda, que controlan y supervisan la aplicación de la ley de protección de datos. Facilitan asesoramiento especializado en temas relacionados con la protección de datos y gestionan de las denuncias relativas al incumplimiento de la ley.

Autorización: es el proceso por el que se determina qué acciones se pueden llevar a cabo o los servicios a los que se puede acceder basándose ensegún la identidad declarada y autenticada. (Nyst et al. 2016)

Consentimiento del titular de los datos: cualquier indicación de la voluntad del titular de los datos dada libremente, de forma específica, informada y sin ambigüedad por la que este/a, mediante una afirmación o una acción afirmativa, consiente el tratamiento de su información personal.

Controlador de datos: se refiere a una persona física o jurídica, pública o privada, o cualquier otra organización o asociación que decide, individualmente o junto a otros, recopilar y procesar datos personales y determinar sus fines.

Credencial: documento, objeto o estructura de datos que avala la identidad de una persona mediante cualquier método de confianza y autenticación. Los tipos de credencial de identidad más comunes –aunque no los únicos– son las tarjetas de identidad, los certificados, los números, los pasaportes o las tarjetas SIM. En el caso del presente Marco, la credencial es una declaración verificable llamada IDC-ID.

Datos personales: toda información relacionada con una persona física identificada o identificable, a partir de la que dicha persona puede ser identificada directa o indirectamente, y especialmente recurriendo a un número de identificación u otros rasgos específicos de su identidad física, fisiológica, mental, económica, cultural o social.

Declaración: cualificación, logro, calidad o elemento de información sobre la experiencia del interesado, tales como el nombre, identificación gubernamental, domicilio o título universitario. (Adaptado del W3C)

Dignidad digital (en el ámbito de la identificación digital): significa que la identidad humana que se halla tras la identificación digital tiene derecho a la privacidad y que sus datos están protegidos.

Evaluación del impacto sobre la protección de datos: consiste en un proceso pensado para identificar los riesgos que genera el procesamiento de datos personales, con el fin de minimizar dichos riesgos tan pronto como sea posible. Se trata de herramientas esenciales para anular los riesgos y para mostrar que se cumple con las leyes y normativas en materia de protección de datos.

Firma digital: es una operación de clave asimétrica, donde la clave privada se usa para firmar datos digitalmente y la pública, para verificar la firma. Las firmas digitales permiten la protección de la autenticidad, la protección de la integridad y el no repudio, pero no la protección de la confidencialidad (adaptado del Instituto Nacional de Estándares y Tecnología - NIST 800-63:2017).

Fuente autorizada: se trata de una fuente autorizada de información de identidad, que consiste en un depósito o sistema que alberga atributos de un particular y que se considera como la fuente principal y más fiable para dicha información. En el caso en el que dos o más sistemas estén desajustados o posean datos contradictorios, los datos existentes en la fuente de datos autorizada se considerarán como los más precisos. (Identidad Federal, Credenciales y Gestión de Acceso –FICAM–, sin fecha).

ID: son las siglas para la credencial de identidad o el documento de identidad en algunas zonas.

Identidad digital: se refiere a un conjunto de atributos y/o credenciales captados y almacenados electrónicamente, que identifican únicamente a una persona (adaptado de Harbitz & Kentala, 2013, y del Informe informe panorama Panorama tecnológico de la ID4D).

Identidad: son las coordenadas sociales que distinguen a una persona de otra. La identidad puede cambiar en función de los actores o del entorno en el que se encuentren las personas y, por lo tanto, no es ni fija ni absoluta.

Identificación: es el proceso por el que se crea, determina o reconoce la identidad de una persona (adaptado de ISO/CEI 24760-1:2011 y UIT-T X.1252 –Sector de Normalización de las Telecomunicaciones de la UIT–).

Interoperabilidad: capacidad que poseen diferentes unidades funcionales –por ejemplo, sistemas, bases de datos, dispositivos o aplicaciones– para comunicar, ejecutar programas o transferir datos, de tal manera que no sea necesario conocer el modo de funcionamiento de tales unidades funcionales.

Marco de confianza: se refiere a los requisitos empresariales, técnicos, operacionales y jurídicos que el sistema de identidad necesita para permitir la interoperabilidad entre las distintas partes participantes.

Nivel de garantía: es la capacidad para determinar, con cierto nivel de certeza o seguridad, que una declaración de una determinada identidad realizada por alguna persona o entidad se puede certificar como la "verdadera" identidad del solicitante (Adaptado adaptado del Informe de cooperación pública-privada de la ID4D). El nivel de garantía general depende del grado de confianza en que la identidad declarada del solicitante sea su identidad real (el nivel de garantía de identidad), de la solidez del proceso de autenticación (nivel de garantía de autenticación) y –si se usa una identidad federada– del protocolo de declaración empleado por la federación para comunicar la autenticación y atribuir información (nivel de garantía de la federación) (adaptado del Instituto Nacional de Estándares y Tecnología - NIST 800-63:2017).

Normas abiertas: son normas que se ponen a disposición de la población general y que se elaboran (o aprueban) y preservan mediante un proceso colaborativo y consensual. "Las normas abiertas" facilitan la interoperabilidad y el intercambio de datos entre diferentes productos o servicios y están destinadas a aplicarse de forma generalizada (adaptado del UIT-T).

Parte confiante: es una entidad que se basa en las credenciales y mecanismos de autenticación facilitados por un sistema de identificación, normalmente, para tramitar una operación o garantizar el acceso a la información o a un sistema (adaptado del Instituto Nacional de Estándares y Tecnología - NIST 800-63:2017).

Presentación verificable: es una presentación segura (los datos provienen de una o más credenciales verificables), codificada de tal modo que la autoría de los datos se puede garantizar tras un proceso de verificación criptográfica. Por ejemplo, los enfoques de divulgación selectiva que sintetizan los datos y no transmiten las credenciales originales verificables (Adaptado adaptado del W3C).

Privacidad y seguridad mediante el diseño: incorporar de manera dinámica los mecanismos de privacidad y seguridad al diseño y realización de productos y servicios, tanto a sistemas informáticos como a los que no lo son, a la infraestructura en red y a las prácticas empresariales. Para ellos, es necesario que la gobernanza de la privacidad y seguridad se tenga en cuenta a lo largo de todo el proceso de ingeniería y del ciclo de vida del producto.

Procesamiento de datos personales: toda operación o conjunto de operaciones que se llevan a cabo sobre los datos personales, a través, o no, de medios automáticos, tales como la recopilación, registro, organización, almacenamiento, recuperación, copia, consulta, uso, divulgación mediante transmisión, difusión o cualquier otra forma de habilitación de acceso, armonización o fusión y bloqueo, cifrado, supresión o destrucción de datos personales.

Protección de datos: regula la forma en que se usan o procesan los datos y por quién, y garantiza el derecho de los ciudadanos sobre sus propios datos. Resulta especialmente importante para garantizar la dignidad digital, puesto que puede mostrar el desequilibrio de poder inherente entre los "titulares de los datos" y las instituciones o personas que recopilan dichos datos.

Proveedor de identidad: entidad autorizada –por ejemplo, un servicio gubernamental o una compañía privada– que emite y gestiona identidades jurídicas, credenciales y procesos de autenticación a lo largo de todo el ciclo de vida de la identidad (Adaptado adaptado del Informe de cooperación pública-privada de la ID4D).

Prueba de conocimiento cero: es un método criptográfico por el que una entidad puede probar a otra que conoce un determinado valor sin tener que divulgar el valor en sí. (W3C) Por ejemplo, revelar la edad en lugar de la fecha de nacimiento.

Prueba de identidad: es una credencial, como por ejemplo, una partida de nacimiento, un documento de identidad o una credencial de identidad digital que se reconoce como prueba de la identidad jurídica por parte la legislación nacional y que cumple con las normas y principios internacionales que se están imponiendo (Grupo de expertos sobre la identidad jurídica de la ONU. Definición práctica de la identidad jurídica).

Sistema de identificación digital: es un sistema de identificación que usa tecnología digital a lo largo de todo el ciclo de vida de la identidad, incluida. Incluye la captación de datos, su validación, almacenamiento y transferencia, así como de la verificación y autenticación de la identidad (Adaptado adaptado de Informe de cooperación pública-privada del Grupo Identificación para el desarrollo –ID4D–).

Sistema de identificación: son las bases de datos, procedimientos, tecnología, infraestructura, credenciales y marcos legales asociados a la captación, gestión y uso de datos de identidad personal para un fin general o específico (adaptado de los Principios sobre identificación).

Sistema fundamental de identificación: sistema de identificación que se creó, en un principio, para gestionar la información de identidad para de la población general y para proporcionar credenciales que sirvieran de prueba de identidad, con el objetivo de acceder a servicios públicos y privados, como la educación, la sanidad, la protección social, los servicios financieros, etc. (adaptado de Gelb & Clark 2013a y de varias publicaciones de la ID4D). En el caso del presente Marco, los estados miembros de la UA decidirán qué fuentes de datos confiables adoptarán sus sistemas de identificación digital fundamental.

Sistemas de identificación funcional: es un sistema de identificación creado para gestionar la identificación, la autenticación y la autorización para un servicio u operación concreta, como las elecciones, la administración tributaria, los programas sociales, las transferencias, los servicios financieros, entre otros. Las credenciales de identidad funcional –como las identificaciones del votante, los registros de seguros, los números de identificación tributaria, las cartillas de racionamiento, los permisos de conducir, etc.– se pueden aceptar generalmente como prueba de identidad para otros usos, especialmente cuando no existe ningún sistema de identificación fundamental (adaptado de Gelb & Clark, 2013a[a], y de varias publicaciones de la ID4D).

Titulares de los datos: son las personas físicas que son objeto del procesamiento de datos personales.

Verificación: consiste en verificar unos atributos de identidad específicos o determinar la autenticidad de las credenciales con el objetivo de dar la autorización a un determinado servicio.

Bureau of the Chairperson
African Union Headquaters
P.O. Box 3243, Roosevelt Street
W21K19, Addis Ababa, Ethiopia
Tel: +251 (0) 11 551 77 00
Fax: +251 (0) 11 551 78 44
www.au.int