GLOBAL STANDARDS PROPORTIONALITY (GSP) WORKING GROUP

MODELO DE POLÍTICAS PARA LA IDENTIFICACIÓN DIGITAL Y CONOCER A SU CLIENTE POR VÍA ELECTRÓNICA (E-KYC)

MODELO DE POLÍTICAS

ÍNDICE

Esta publicación es la versión traducida de la publicación original en Inglés: Policy Model for Digital Identity and Electronic Know Your Customer (e-KYC).

CONTEXTO Y ANTECEDENTES

Los países alrededor de todo el mundo han estado mejorando su infraestructura pública para una mejor prestación de servicios en la era digital. Uno de los avances clave en muchos países es la implementación de un sistema de identificación digital (ID digital). Un principal caso de uso con respecto a la identificación digital incluye los procesos electrónicos de conocimiento de su cliente (e-KYC), aprovechando el sistema de identificación digital. Las ventajas de estos usos van desde una mayor eficiencia, ahorros de costos e inclusión financiera acelerada en muchos países. Las experiencias de varios países miembros de AFI evidencian lo antedicho.

A medida que los países construyen la infraestructura y un sólido entorno regulatorio y de políticas para permitir el desarrollo de la identificación digital y e-KYC, es imperativo mantener el enfoque centrado en el usuario. El Grupo de Trabajo de Proporcionalidad de Estándares Globales (GSPWG) de AFI ha codificado las mejores prácticas de los países miembros de AFI, así como otras experiencias a nivel mundial dentro de este modelo de políticas. El modelo de políticas se construye en base al reconocimiento por parte de los miembros de AFI de la identificación digital como un pilar clave de un marco general de políticas de FinTech inclusivas, tal como se consagra en el Acuerdo de Sochi sobre FinTech para la Inclusión Financiera respaldado por los miembros en el año 2018.

OBJETIVO

El modelo de políticas proporciona orientación a los países que buscan desarrollar o mejorar sus sistemas de identificación digital y aprovecharlos para e-KYC. La finalidad es permitirles construir sistemas sólidos, interoperables, inclusivos y sostenibles, contribuyendo así al logro de los objetivos de inclusión financiera y la integridad financiera inclusiva.

ALCANCE Y APLICACIÓN

El modelo de políticas construye un marco que se basa en los enfoques utilizados por los países miembros de AFI para desarrollar un entorno normativo y de políticas que permita la identificación digital y e-KYC; para diseñar y construir la infraestructura y las características técnicas del sistema; y para aprovechar la identidad digital para los procesos de e-KYC. La inclusión financiera de las mujeres y otros grupos desfavorecidos, como los jóvenes, los ancianos, las personas con discapacidad y las personas desplazadas por la fuerza, son temas comunes a lo largo de todo el modelo. Se han formulado principios para abordar las necesidades específicas de estos grupos.

Estos principios ponen de relieve los aspectos prácticos y operativos clave que deben tenerse en cuenta a la hora de desarrollar un sistema de identificación digital y utilizarlo para e-KYC. Se basan en las mejores prácticas y experiencias de los países miembros de AFI, así como aquellas de los proveedores de servicios y las instituciones socias de conocimientos técnicos. Si bien el modelo de políticas se puede utilizar como una guía independiente, se debe tener en cuenta que la tecnología, las prácticas del sector y los casos de uso evolucionan rápidamente, y que los enfoques de políticas deben ser adaptables a tales avances. El modelo de políticas se revisará y actualizará periódicamente para tener en cuenta estos avances.

INSTRUCCIONES PARA LA LECTURA

Los temas centrales del modelo de políticas están interconectados. Por favor, lea todo el documento de manera holística.

VISIÓN GENERAL DE LOS CONCEPTOS Y DEFINICIONES CLAVE

ACCESO AL SISTEMA DE IDENTIFICACIÓN DIGITAL (ACLARACIÓN DE LA AUTENTICACIÓN, E-KYC)

A los efectos de este Modelo, el acceso se refiere a ser un usuario o administrador autorizado del sistema pudiendo autenticar la identidad de una persona basándose en uno o más factores o completar una transacción de e-KYC autenticando y viendo o recibiendo los datos del usuario necesarios para el cumplimiento de KYC.

SISTEMA ANTI-LAVADO DE ACTIVOS Y CONTRA EL FINANCIACIÓN DEL TERRORISMO (ALA/CFT)

Se refieren a las políticas, leyes y reglamentos para mantener la integridad del sistema financiero mediante la disuasión y la prevención del uso del sistema financiero para el lavado de dinero, la financiación del terrorismo y otras actividades ilícitas de este tipo.

AUTENTICACIÓN

Se refiere al proceso de comprobar si una persona que afirma tener una identidad es la persona propietaria legítima de esa identidad en base a uno o más factores (algo que tiene, sabe o es) previamente proporcionado junto con la información KYC.

CREDENCIALES

Una credencial es cualquier documento, objeto o estructura de datos que puede corroborar digitalmente la identidad de una persona individual a través de algún método de autenticación en un sistema de identificación.[1] Hay varios tipos de factores que pueden ser utilizados como credenciales de identidad, tales como las tarjetas inteligentes, los datos biométricos, las contraseñas, las contraseñas de un solo uso (OTP).

DEDUPLICACIÓN

La deduplicación se refiere a la eliminación de información duplicada o redundante. En el caso de un sistema de identidad digital, es el proceso de comprobación de entradas duplicadas, normalmente a través de un proceso de coincidencia biométrica, para cerciorarse que se realicen adiciones únicas.

IDENTIFICACIÓN DIGITAL (ID)

La identificación digital se refiere a cualquier documento de identidad digitalizado o emitido por los gobiernos, también podría incluir formas de identificación digital que se proporcionan en asociación con el sector privado u otras entidades autorizadas, como el Alto Comisionado de las Naciones Unidas para los Refugiados, pero que están vinculadas a la identidad "oficial" o "legal" de una persona y es reconocida por el gobierno para fines oficiales.[2]

SISTEMA DE IDENTIFICACIÓN DIGITAL

Es un sistema para el proceso de comprobación de la identidad y su inscripción, así como la autenticación de la misma. La comprobación de la identidad y la inscripción se pueden realizar con documentación digital o física, o una combinación de ambas. Sin embargo, la vinculación, las credenciales, la autenticación y la portabilidad o la federación de los datos deben ser digitales.[3]

CONOCER A SU CLIENTE POR VÍA ELECTRÓNICA (E-KYC)

E-KYC se refiere al proceso de verificar electrónicamente las credenciales de un cliente en línea con los procesos KYC del país con respecto a los enfoques basados en el riesgo. Por ejemplo, esto puede incluir la identificación biométrica y/o por vídeo, tal y como recomienda el Grupo de Acción Financiera Internacional (GAFI) en su guía de identidad digital (2020).

GRUPO DE ACCIÓN FINANCIERA INTERNACIONAL

El GAFI es un organismo intergubernamental y normativo encargado de establecer y promover normas internacionales para combatir el lavado de dinero, la financiación del terrorismo y la financiación de la proliferación de las armas de destrucción masiva.

IDENTIDAD FUNDACIONAL

Las identificaciones fundacionales son identificaciones multi-propósito, como un documento de identidad nacional y un registro civil, que proporcionan identificación para la población en general.

IDENTIFICACIÓN FUNCIONAL

Las identificaciones funcionales gestionan la identificación, autenticación y autorización para sectores o casos de uso específicos, como por ejemplo para efectos impositivos, de protección social y ejercer el derecho a voto.[4]

1 World Bank. 2019. ID4D Practitioner' Guide: Version 1.0 (October 2019). Washington, DC: World Bank. Disponible en: http://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

2 Ibid.

3 FATF (2020), Guidance on Digital ID, FATF, Paris. Disponible en: http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-on-Digital-Identity.pdf

4 World Bank. 2019. ID4D Practitioner's Guide: Version 1.0 (October 2019). Disponible en: http://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

PRUEBA/VERIFICACIÓN DE IDENTIDAD

Este es un proceso para establecer o determinar la identidad de una persona mediante la recolección y verificación de la información de identidad pertinente.

INTEGRIDAD FINANCIERA INCLUSIVA

Se refiere a una alineación exitosa de la inclusión financiera y los objetivos de la política de ALA/CFT o de integridad financiera. Esto se consigue esencialmente cuando un país ha implementado estándares mundiales de integridad financiera y también ha ampliado el acceso y el uso de servicios financieros formales de calidad. Una visión nacional clara, una coordinación eficaz de las partes interesadas públicas y privadas, y la integración de los procesos de ALA-CFT y procesos de inclusión financiera a nivel nacional son factores clave para lograr una integridad financiera inclusiva.

PRINCIPIO DE PROPORCIONALIDAD

A los efectos del modelo de política, el principio de proporcionalidad aboga a favor que los países recopilen datos adecuados que sean pertinentes para el funcionamiento óptimo del sistema de identificación digital. No se debe recopilar información en exceso.

DATOS CONFIDENCIALES

Estos datos comprenden la información biográfica, cuya recopilación es especialmente sensible porque la información podría utilizarse para elaborar perfiles o discriminar a una persona o poner su seguridad en grave peligro. Por lo tanto, los campos de información biográfica no deben ponerse fácilmente a disposición de terceros ni ser de dominio público. Incluyen, entre otros, datos sobre origen racial o étnico, opiniones políticas, creencias religiosas, orientación sexual, etc.[5]

USUARIO

Se refiere a la persona a la que se incorpora al sistema de identificación digital y que proporciona información sobre su identidad para los distintos casos de uso.

5 Ibid.

Este modelo de política se ha desarrollado en torno

TRES CONSIDERACIONES POLÍTICAS:

1

MARCO REGULATORIO Y DE POLÍTICAS PARA LA IMPLEMENTACIÓN DE LA IDENTIFICACIÓN DIGITAL Y E-KYC

Ver página 6

2

CONSIDERACIONES POLÍTICAS PARA EL DISEÑO DE LA PLATAFORMA Y LA CONSTRUCCIÓN DEL SISTEMA DE IDENTIFICACIÓN DIGITAL Y LA INFRAESTRUCTURA TECNOLÓGICA

Ver página 14

3

CONSIDERACIONES SOBRE POLÍTICAS PARA IMPLEMENTAR PROCESOS Y CASOS DE USO CLAVE QUE APROVECHAN DE MEJOR MANERA LA IDENTIFICACIÓN DIGITAL PARA E-KYC

Ver página 19

PARTE I. MARCO REGULATORIO Y DE POLÍTICAS PARA LA IMPLEMENTACIÓN DE LA IDENTIFICACIÓN DIGITAL Y E-KYC

Esta sección detalla el marco para construir un entorno regulatorio propicio para fomentar el uso más efectivo de la identificación digital y e-KYC. También se detallan las leyes generales sobre protección de datos y gobernanza, junto con las estrategias de inclusión financiera y las consideraciones de género.

I. LEYES Y REGULACIONES SOBRE LA IDENTIFICACIÓN DIGITAL Y E-KYC

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
LEYES, REGULACIONES Y POLÍTICAS PARA LA IDENTIFICACIÓN DIGITAL Y E-KYC	Promulgar leyes fundacionales específicas en el país que regulen los siguientes aspectos clave: **a.** ALA/CFT y KYC por niveles y basado en el riesgo **b.** Documentos de identificación e identidad digital[6] **c.** Protección de datos y privacidad **d.** Seguridad cibernética De manera adicional a, o integradas en, las leyes fundacionales: **e.** e-KYC No es necesario promulgar leyes específicas en el país que rijan la identificación digital y e-KYC. Basta con que se incluyan en el marco regulatorio.	Brindar claridad en la aplicación de la ley, normas o directivas sobre el uso y manejo de la identificación y sus diversas aplicaciones. Ayuda de las siguientes maneras: > Se incrementa el cumplimiento de las partes interesadas, y ellas toman decisiones fundamentadas > Se reducen los riesgos con respecto al fraude y la privacidad > Beneficios sociales y económicos tanto para el sector público como para el privado
CONTENIDO Y ALCANCE DE LAS LEYES, REGULACIONES Y POLÍTICAS	Antes de la implementación de un programa nacional de identificación digital o de e-KYC deben redactarse leyes, regulaciones y directrices para fomentar un entorno propicio dentro de los límites legales y regulatorios. Los aspectos clave que deberían formar parte del marco regulatorio de un país pueden incluir:[7] **a.** Objetivo y alcance de uso de la identificación digital, incluidos los casos de uso de la identidad digital, como por ejemplo e-KYC **b.** Puntos de datos a ser recolectados y credenciales a ser emitidas **c.** Antecedentes y justificativo **d.** Validez y proceso de renovación **e.** Detalles y restricciones en el procesamiento de datos	Las políticas que permiten el uso las identificaciones digitales y los marcos que detallan dicho uso ayudarán a las partes interesadas a dar pasos concretos hacia la creación de una amplia gama de aspectos en torno a la identidad digital, como la gobernanza, la política, el funcionamiento, la tecnología y la legislación, etc. Especificar claramente qué datos se deben recolectar asegurará la protección del consumidor y mitigará el arbitraje regulatorio.

6 Los sistemas de identificación digital son aquellos que utilizan tecnología digital durante todo el ciclo de vida de la identidad, incluyendo para la captura, validación, almacenamiento y transferencia de datos; gestión de credenciales; y verificación y autenticación de la identidad. Consultar, Banco Mundial. 2019. ID4D Practitioner's Guide: Version 1.0 (October 2019). Disponible en: http://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

7 Esta lista no es exhaustiva. Se pueden agregar más elementos según el contexto y los requisitos del país.

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
CONTENIDO Y ALCANCE DE LAS LEYES, REGULACIONES Y POLÍTICAS *continuada*	f. Detalles sobre el mecanismo/ arquitectura de consentimiento, con disposiciones para revocar el consentimiento g. Restricciones con respecto a compartir información, incluyendo restricciones al acceso, así como la emisión de permisos para terceros h. Integración de datos e interoperabilidad i. Detalles sobre el almacenamiento y la gestión de datos, incluidos planes de recuperación en caso de desastres y planes de continuidad de actividades j. Seguridad y confidencialidad de la información k. Estructuras institucionales y de gobernanza que rigen la identidad digital y e-KYC l. Roles, responsabilidades y rendición de cuentas por parte de las entidades a cargo y usuarios/ participantes m. Infracciones y sanciones n. Mecanismos para quejas y escalada de reclamaciones o. Procedimientos para la actualización de información p. Medidas especiales para las mujeres y otros grupos desfavorecidos como los jóvenes, los ancianos y las personas con discapacidad, y enmiendas específicas a las leyes existentes para integrar a las poblaciones desplazadas por la fuerza. q. Auditorías y revisiones r. Uso de la firma digital Las leyes deben ser adaptables y consistentes con otras leyes relacionadas en las respectivas jurisdicciones para hacerlas más efectivas.	Las directrices claras también fomentan la cooperación y la coordinación entre las diversas partes interesadas. Ayuda a comprender lo que permite la infraestructura de identificación digital (ID), cuáles son las limitaciones y oportunidades, qué hay que cambiar, a quién afecta y cómo.
REFERENCIAS ESTÁNDAR MUNDIALES PARA KYC	Consultar y velar a favor del cumplimiento de las normas del GAFI y las orientaciones conexas[8] en la formulación de las políticas de ALA/CFT, KYC y e-KYC[9]. Esto incluye la Guía del GAFI sobre identidad digital.[10] Asegurar el desempeño esperado, y/o resultados basados en determinados criterios al establecer los atributos, las pruebas y los procesos requeridos al demostrar la identidad oficial para la diligencia debida del cliente.	Construir un marco sólido de KYC con el máximo alcance para las partes interesadas. Seguir las recomendaciones y orientaciones de GAFI ayuda a mantener la sintonia con las normas y regulaciones que están en desarrollo. Sin embargo, es importante que las políticas de ALA/CFT, KYC y e-KYC se adapten cuidadosamente al contexto único del país y a los riesgos de LA/FT.
KYC POR NIVELES Y BASADO EN EL RIESGO	Llevar a cabo evaluaciones de riesgos regulares a nivel nacional, sectorial e institucional que deben servir como base para el desarrollo de KYC por niveles y basado en el riesgo. Esto ayudará a identificar los	Determinar el nivel de riesgo al que están expuestos los proveedores de servicios financieros cuando atienden

8 FATF. 2012-2021. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Disponible en: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

9 No existe un estándar internacional sobre e-KYC. Sin embargo, se aborda en cierta medida en: FATF. 2020. Guidance on Digital Identity. Disponible en: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-report.pdf

10 Ibid.

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
KYC POR NIVELES Y BASADO EN EL RIESGO *continuada*	desafíos en materia de exclusión financiera a los que se enfrenta cualquier categoría de la población, que pudiese necesitar la aplicación de requisitos KYC proporcionados o específicos para evitar restringir indebidamente el acceso de dicha categoría de la población a productos y servicios de bajo riesgo. Un enfoque basado en el riesgo debe velar a favor que los requisitos KYC que se apliquen sean proporcionales al nivel de riesgo evaluado, incluyendo la consideración de requisitos reducidos cuando los riesgos se consideren menores. La implementación efectiva del enfoque basado en el riesgo para la debida diligencia del cliente debe respaldar los objetivos de inclusión financiera. Las evaluaciones de riesgo se pueden realizar en varios niveles: > Cliente/País/Geografía > Productos/Servicios/Transacciones/Canales Determinar un calendario pertinente para llevar a cabo posteriores evaluaciones de riesgo.	a diferentes categorías de la población. Este es un paso importante para asegurar que los servicios y productos financieros se desarrollen para los más desfavorecidos y no impidan su acceso y uso, así como para mantener un conocimiento actualizado de los riesgos de LD/FT en el país. Un enfoque basado en el riesgo velará a favor de que las medidas adoptadas para prevenir o mitigar el lavado de dinero, la financiación del terrorismo y la financiación de la proliferación de armas de destrucción masiva sean proporcionales a los riesgos identificados. Se necesitan evaluaciones periódicas de riesgos a nivel nacional, sectorial o institucional para asegurarse de contar con prácticas actualizadas, así como prácticas dirigidas a la mitigación de nuevos riesgos.
E-KYC	Desarrollar una política clara y un plan de implementación para e-KYC, al aprovechar la identificación fundacional, como por ejemplo la identificación nacional o las identificaciones funcionales con una amplia penetración. Cerciorarse que el sistema e-KYC se adapte a las prácticas de KYC por niveles y basadas en el riesgo. *(Para más detalles, consultar la sección III)*	Para los proveedores de servicios financieros, la autenticación y verificación de la identidad a través de los procesos de e-KYC han demostrado resultar en un alto nivel de ahorro en los países, tanto en términos de tiempo como de costos. También fomentará la inclusión financiera de las mujeres al eliminar los desafíos específicos relativos al género (necesidad de desplazarse a los puntos de transacción, estar acompañada por un hombre, etc.).
IMPLEMENTACIÓN DEL SOPORTE	Publicar orientaciones para todas las partes interesadas sobre la interpretación de las diferentes leyes y regulaciones. Más específicamente, a las instituciones financieras, incluidas, entre otras, entidades bancarias, compañías de seguros, corredores, etc., así como a los intermediarios. La orientación debe asegurar la claridad, así como pasos claros para la implementación de conceptos relacionados con el cumplimiento y la regulación de las transacciones transfronterizas debido a que se realizan en jurisdicciones extranjeras. Los bancos centrales y las autoridades competentes deben estudiar la evolución del sistema de ALA/CFT a CFT a nivel local, regional y mundial, con el fin de	Para garantizar la claridad regulatoria entre las instituciones financieras y comprender los desafíos más urgentes que se presentan en el cumplimiento a las regulaciones ALA/CFT. Esto facilitará las acciones necesarias y las medidas de mitigación para afrontar tales desafíos.

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
SUPPORT IMPLEMENTATION *continued*	orientar a las instituciones responsables para que sigan cumpliendo las normas en todo momento, y documentar y compartir las interpretaciones de las Recomendaciones de GAFI, así como las orientaciones conexas. Esto permitirá una implementación efectiva y un mejor entendimiento entre las instituciones financieras. Proveer supuestos, si los hubiera, y un plan de implementación estandarizado para evitar cualquier desafío o discrepancia que pudiese surgir. Brindar apoyo y promover un diálogo abierto sobre la implementación y abordar cualquier desafío que pudiese surgir después de la implementación.	
RECOPILACIÓN DE INFORMACIÓN PERSONAL IDENTIFICABLE	Recopilar la cantidad mínima de valores de datos de los ciudadanos según sea necesario para satisfacer los requisitos de KYC e informar a los clientes explícitamente sobre el posible uso de los datos recopilados. La información de identificación personal recopilada debe considerar el alcance y utilidad del sistema y determinar por proporcionalidad, lo que es obligatorio. La información confidencial, si se la recopila, debe clasificarse por niveles aún más detalladamente con el fin de garantizar un mayor grado de privacidad y seguridad, al limitar que entidades de terceros tengan acceso completo a los datos.	Respetar la privacidad del usuario y adherirse a los principios de proporcionalidad al no recopilar más datos de los necesarios. Esto ayuda a: > Garantizar la mínima violación de la privacidad de los usuarios > Lograr ahorro de tiempo y costos incurridos en la recopilación y verificación de cada uno de los campos de datos recopilados > Reducir el riesgo de filtración de datos confidenciales y vigilancia
VERIFICACIÓN DE DATOS Y COMPROBACIÓN DE LA IDENTIDAD	Verificar los datos recopilados con datos o documentos independientes y confiables registrados por las entidades emisoras, tales como documentos nacionales de identidad. La verificación con otras bases de datos civiles y la autenticación biométrica en el mismo momento y lugar son métodos de prueba de identidad de uso común. Para la gestion de excepciones, hay que considerar estrategias de revisión comunitaria para usuarios sin documentos que pertenecen a categorías de bajo riesgo.[11]	Brindar protección contra el fraude y el robo de identidad de ser posible
RECOLECCIÓN DE DATOS BIOMÉTRICOS	Establecer políticas claras sobre la recopilación de información biométrica, su almacenamiento y uso. Determinar qué datos biométricos son más útiles para el sistema que se está desarrollando, teniendo en cuenta los principios de proporcionalidad y utilidad. Se deben recopilar datos biométricos mínimos para identificar a una persona de manera única: ¬se ha demostrado que las huellas dactilares, el rostro y el iris son los identificadores más usados. Se puede considerar el reconocimiento de voz para los países con un alto uso de teléfonos.Los métodos invasivos, como la recolección de ADN, deben pasar por un	La recolección de datos biométricos permite tanto la identificación como la autenticación. La autenticación que se basa en la coincidencia biométrica es más eficiente y precisa. También ayuda en la deduplicación de registros de identidad.

11 FATF. 2020. Guidance on Digital Identity, p. 38. Disponible en: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-report.pdf

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
RECOLECCIÓN DE DATOS BIOMÉTRICOS	proceso completo de diligencia debida y cumplir la legislación vigente sobre protección de datos y privacidad.	
ACTUALIZACIÓN DE DATOS BIOMÉTRICOS	Elaborar procedimientos para actualizar la información biométrica que está sujeta a cambios debido a la edad, la ocupación y las condiciones físicas o médicas. Elaborar directrices para llevar a cabo una actualización obligatoria en casos especiales, como en el caso de niños, ancianos y personas con discapacidad.	Asegurar que ocurran un mínimo de problemas y fallas durante la autenticación y verificación biométrica.
ACTUALIZACIÓN DE DATOS DEL USUARIO	Redactar directrices para realizar correcciones, enmiendas o eliminación de información inexacta con respecto a la identificación digital. Las directrices deben permitir flexibilidad para reconocer a los usuarios según el género con el que se identifican, en lugar del género que se les asignó al nacer y actualizar esta información.	Preservar la integridad, retener la precisión y asegurarse de almacenar y procesar los datos más recientes.

II. LEYES SOBRE PROTECCIÓN DE DATOS Y PRIVACIDAD

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
POLÍTICAS DE PRIVACIDAD Y PROTECCIÓN DE DATOS	Incluir elementos clave de protección de datos y privacidad en las notas de orientación, directrices y leyes existentes sobre la recolección, el procesamiento, la gestión y el almacenamiento de datos personales de las personas individuales, por ejemplo: a. Consentimiento obligatorio para el procesamiento de datos personales mediante la evaluación de la validez del consentimiento general en comparación con el consentimiento transaccional b. Detalles de escenarios en los que no se requeriría el consentimiento; por ejemplo, órdenes judiciales c. Disposiciones especiales para niños (recopilación de información demográfica limitada y aquella que se puede vincular con el tutor legal) y grupos desfavorecidos d. Principios de privacidad por diseño, incluyendo a los fiduciarios de los datos e. Clasificación de los datos confidenciales f. Eliminación de datos cuando el propósito de la recopilación de datos haya caducado g. Medidas y sanciones por el mal manejo de datos, incluyendo presentación de datos falsos por parte del personal	Es necesario contar con una política integral de protección de datos y privacidad para gobernar tanto el sector público como el privado, ya que es difícil para las partes interesadas cumplir con múltiples reglas y regulaciones sobre el uso y gestión de la identificación.
AUDITORÍAS Y EVALUACIONES SOBRE LA PRIVACIDAD	Establecer una autoridad de protección de datos independiente que sea responsable de asegurarse que el manejo de datos personales se realice de acuerdo con las disposiciones y lineamientos legales. Especificar el proceso para realizar revisiones/ evaluaciones de los riesgos en materia de privacidad del sistema en general. Las directrices deben indicar cuáles terceros están autorizados a llevar a cabo lo antedicho, así como los intervalos de tiempo para ello.	Revisar la política y los procedimientos sobre cómo se recolectan, gestionan y almacenan los datos. Asimismo se verificará el cumplimiento de las directrices sobre protección de datos y privacidad, ayudandoa identificar el riesgo y desarrollode estrategias de mitigación.

III. GOBERNANZA Y ESTRUCTURAS INSTITUCIONALES

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
ESTRUCTURAS DE GOBERNANZA Y DE EXIGENCIA DEL CUMPLIMIENTO	Establecer una entidad independiente encargada de la planificación, gestión y administración de la identidad digital. La entidad debe tener poderes para hacer cumplir y asignar responsabilidades que se fundamenten en las reglas y regulaciones establecidas en las leyes. Se deberá crear un consejo formado por representantes de las principales instituciones de regulación financiera, de la unidad de inteligencia financiera y de los ministerios pertinentes, como el de tecnologías de la información, comunicaciones, justicia y protección social, para supervisar las actividades de esta entidad independiente. Para cerciorarse de contar con la cooperación, colaboración y armonización de las partes interesadas en la implementación de la identidad digital, el organismo independiente también debe tener jurisdicción y supervisión de otras entidades de terceros que utilizan los datos de identificación, esto con el fin de velar por que no se produzcan usos indebidos. Desarrollar la capacidad de los actores en el ecosistema para destacar los principios de cooperación en la implementación del sistema de identificación, la adopción de una práctica e-KYC eficaz por parte de los proveedores de servicios financieros, así como una vigilancia y supervisión que sean apropiadas. Los socios implementadores también deben promover la alfabetización digital y la toma de conciencia por parte de sus clientes sobre la necesidad, los usos y los beneficios de la identificación antes de su lanzamiento.	Promover la eficiencia, la rendición de cuentas, la transparencia, así como evitar la exclusión y el mal uso.
FOMENTO DE LA INNOVACIÓN	Impulsar iniciativas en el país para impulsar innovaciones relacionadas con la identificación digital. Los sandboxes regulatorios, los centros de innovación o pruebas y los enfoques de aprendizaje han tenido éxito al ofrecer un entorno propicio para las innovaciones relativas a: a. Formas rentables de brindar servicios a través de canales habilitados por la tecnología b. Incorporación remota y e-KYC aprovechando la identificación digital para diferentes servicios y productos c. Opciones de alternativas de calificación crediticia para personas sin calificación crediticia formal, en particular mujeres emprendedoras d. Tecnología emergente Considerar los sandboxes regionales para crear un modelo de trabajo más sostenible a través del financiamiento conjunto y el intercambio de conocimientos técnicos. El sandbox se puede utilizar para innovaciones en todos los sectores y todos los casos de uso. Este entorno se puede utilizar específicamente para las innovaciones destinadas a acelerar la inclusión financiera en especial para los grupos desfavorecidos, a la par que se innovan nuevos productos y servicios para los clientes existentes.	Los enfoques para fomentar la innovación, los sandboxes regulatorios, los centros de innovación o los enfoques de prueba y aprendizaje, brindan el ambiente adecuado para la supervisión, visibilidad y vigilancia por parte de los reguladores, al mismo tiempo que permiten la innovación por parte del sector privado de soluciones eficientes y casos de uso interesantes.

IV. ESTRATEGIAS DE INCLUSIÓN FINANCIERA

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
ESTRATEGIAS NACIONALES DE INCLUSIÓN FINANCIERA	Integrar claramente la identificación digital y el desarrollo de e-KYC en las políticas, estrategias e iniciativas nacionales para acelerar la inclusión financiera, incluyendo: a. Estrategia Nacional de Inclusión Financiera (ENIF)[12] b. Estrategia Nacional de Educación o Alfabetización Financiera c. Una estructura de coordinación para impulsar los esfuerzos nacionales de inclusión financiera, que deberá estar dirigida por el banco central y/o el ministerio de finanzas, compuesta por las partes interesadas pertinentes, como los ministerios de finanzas, de tecnologías de la información, comunicaciones, protección social, educación, mujer y otros. La estructura puede tener grupos de trabajo para diferentes pilares de ENIF y que comprendan el sector privado, la sociedad civil, el desarrollo y los grupos humanitarios. d. Ajustes específicos para la incorporación al sistema de identidad digital para poblaciones desfavorecidas,[13] como la incorporación a domicilio, documentos alternativos y pruebas de la comunidad, por ejemplo, un respaldo de un intermediario calificado o una entidad como ACNUR e. Introducción de productos y servicios específicos dirigidos a grupos desfavorecidos, incluidos los ancianos y las personas con discapacidades, como productos y servicios de bajo riesgo, seguros de bajo costo respaldados por el gobierno, cuentas bancarias sencillas sin cargos de mantenimiento, crédito a bajo interés para grupos de bajos ingresos y mujeres, etc. f. Proyectos de alfabetización y concientización financiera	Garantizar que el diseño y la implementación de la identidad digital y e-KYC contribuyan al avance de la inclusión financiera de manera coherente, coordinada y enfocada, con dirección hacia un mayor acceso y uso de servicios financieros asequibles y de calidad específicamente para las poblaciones desatendidas y las deficientemente atendidas.
IMPLEMENTACIÓN DE ESTRATEGIAS NACIONALES DE INCLUSIÓN FINANCIERA	Aprovechar de mejor manera la estructura de coordinación nacional para la inclusión financiera con el fin de construir un esfuerzo colaborativo para la implementación de la ENIF, esfuerzo que esté dirigido por los organismos gubernamentales, establecido por ley o decreto, y que cuente con la participación de las partes interesadas del sector privado y de la sociedad civil. La estructura de coordinación garantizará una sólida coordinación de múltiples partes interesadas, la distribución de responsabilidades y una rendición de cuentas efectiva. La implementación de una ENIF debe estar alineada con las políticas y estrategias nacionales de educación financiera, alfabetización financiera y protección del consumidor. La implementación se puede acelerar mediante el uso de proyectos en "modo misión", que tengan objetivos y plazos claramente definidos con el fin de obtener resultados rápidos. Los países que cuentan con identidad digital pueden aprovechar mejor dicha identificación para una incorporación eficiente y para procesos de e-KYC.	Asegurar el logro de los objetivos nacionales de inclusión financiera, en particular a través de la aceptación de diferentes partes interesadas y ministerios clave, así como asegurar los recursos y el presupuesto comprometidos para implementar acciones de políticas y emprender las actividades.

12 Alliance para la Inclusión Financiera, 2020. Modelo de políticas para una Estrategia Nacional de Inclusión Financiera. Disponible en inglés: https://www.afi-global.org/publications/policy-model-for-national-financial-inclusion-strategy/ y en español: https://www.afi-global.org/wp-content/uploads/2020/09/AFI_NFIS_PM_SPANISH_AW2_digital.pdf

13 Los grupos desfavorecidos de la población incluyen a los económicamente desfavorecidos, los jóvenes, los ancianos, las personas con discapacidad, las personas desplazadas por la fuerza, las minorías raciales y étnicas, los niños de grupos de bajos ingresos y otros que el país podría haber definido explícitamente.

V. ESTRATEGIAS DE INCLUSIÓN DE GÉNERO

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
PROCESOS DE INCLUSIÓN DE GÉNERO	Elaborar una estrategia e iniciar un análisis exhaustivo de las políticas y el sistema de identidad digital para garantizar la inclusión de género a lo largo del ciclo de vida de la identidad digital. Algunas consideraciones clave son las soluciones fuera de línea y días de inscripción en lugares móviles o días de inscripción sólo para mujeres, así como la promoción de interfaces que tomen en cuenta los asuntos de género. La colaboración y cooperación de instituciones públicas y privadas especializadas en asuntos de la mujer respaldarían el desarrollo de una estrategia centrada en la inclusión de género.	Velar porque no haya exclusión en el sistema de identificación digital debido a las barreras adicionales a las que se enfrentan las mujeres.
RECOPILACIÓN DE DATOS DESGLOSADOS POR SEXO Y EDAD	Promover la recopilación, rastreo, análisis y seguimiento de datos desglosados por sexo y edad. Determinar la frecuencia y las fuentes (del lado de la oferta y del lado de la demanda) de recolección. Se debe considerar permitir el acceso a, y la difusión de, los datos por parte de otras entidades públicas que puedan beneficiarse de esta información.	Cerciorarse que los datos se recopilen con propósitos de tener mejores políticas y una mejor toma de decisiones estratégicas.

14 Microsave Consulting. 2021. Documento de trabajo: A Framework for Building Gender-Sensitive Identity Systems. Disponible en: https://www.microsave.net/wp-content/uploads/2021/03/Working-paper-A-framework-for-building-gender-sensitive-identity-systems.pdf

PARTE II. CONSIDERACIONES POLÍTICAS PARA EL DISEÑO DE LA PLATAFORMA Y LA CONSTRUCCIÓN DEL SISTEMA DE IDENTIFICACIÓN DIGITAL Y LA INFRAESTRUCTURA TECNOLÓGICA

Esta sección detalla los principios y consideraciones para diseñar y construir el sistema de identificación digital, la infraestructura tecnológica así como la arquitectura de soporte. Estos principios se inspiran, entre otros, en los de la gestión de datos y los servicios a los usuarios, que también son consideraciones clave para el sistema de identidad digital.

I. DISEÑO DEL SISTEMA DE IDENTIFICACIÓN

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
TIPOS Y CARACTERÍSTICAS DE LA IDENTIFICACIÓN DIGITAL	Definir claramente el tipo de[15] identificación digital (fundacional o funcional) que se está implementando en el país. La decisión debe basarse en un examen exhaustivo de las necesidades y los objetivos del programa de identidad y tras varias rondas de conversaciones con todas las partes interesadas pertinentes. Los parámetros clave a considerar son: a. Disponibilidad de un sistema de identificación fundacional y de una infraestructura sobre la que se puede construir la identificación digital b. Su escalabilidad y sus planes para aprovechar mejor la identificación c. Implicaciones de los costos (incluyendo el análisis de los recursos humanos y la infraestructura, la propiedad de los dispositivos digitales), así como los incentivos, como por ejemplo, los regímenes fiscales favorables y el reparto de los costos[16] d. Los planes de implementación y despliegue afectarán a la naturaleza de la identificación y a la decisión de utilizar una identificación funcional actual y convertirla en una identificación fundacional e. Registro obligatorio u opcional para algunos, y cualquier requisito previo como edad, ciudadanía	Hacer el mejor uso de los recursos disponibles, incluidos entre ellos el presupuesto, los recursos humanos, las bases de datos existentes y la tecnología. Ayudar a que el sector público y el sector privado demuestren el tipo de servicios (sanitarios, financieros, de seguridad social, etc.) a los que se puede acceder mediante el uso de la identificación.

15 Las identificaciones fundacionales son identificaciones polivalentes, como la identificación nacional y los registros civiles, que proporcionan identificación a la población en general. Las identificaciones funcionales administran la identificación, autenticación y autorización para sectores específicos o casos de uso, como votaciones, impuestos y protecciones sociales. Consultar, Banco Mundial. 2019. ID4D Practitioner's Guide: Version 1.0 (October 2019). Disponible en: https://id4d.worldbank.org/guide/types-id-systems).

16 World Bank. 2018. Understanding Cost Drivers of Identification Systems. Disponible en: https://documents1.worldbank.org/curated/en/702641544730830097/pdf/Understanding-Cost-Drivers-of-Identification-Systems.pdf

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
ADHERENCIA A LOS ESTÁNDARES INTERNACIONALES	sobre diseño y desarrollo de identidades, y seguir las recomendaciones sobre privacidad. Algunos principios clave se pueden encontrar en los siguientes documentos: a. Banco Mundial: Principios de identificación b. ID4D: Normas técnicas para la identificación digital c. Privacidad por diseño d. Orientación de GAFI sobre pautas de identidad digital e. G20 f. ISO g. Good ID h. Asociación Internacional de Profesionales de la Privacidad i. ISO 27001: 2013, sobre gestión de seguridad de la información Se pueden tomar decisiones estratégicas clave sobre la base de experiencias, conocimientos y desafíos de otros países, pero cerciorándose que el contexto y los requisitos del país sean fundamentales para el diseño.	Para cerciorarse que el desarrollo se basa en las mejores prácticas y los aprendizajes provenientes de otras jurisdicciones y para garantizar que se consideren cuidadosamente los elementos de diseño que sean más apropiados.
EMISIÓN DE CREDENCIALES	Evaluar en el contexto del país cuáles son las credenciales más apropiadas para el uso de la población en general. Se debe tener en cuenta factores como la funcionalidad, las preferencias del usuario y la seguridad. Los ejemplos incluyen, pero no se limitan a: a. Físicas (tarjetas) b. Digitales (tarjetas electrónicas (e-cards), número de identificación) c. Factores adicionales (PIN, contraseña, contraseña de un solo uso (OTP)) d. Código QR Las tarjetas físicas brindan una sensación de seguridad, las tarjetas inteligentes ofrecen varias funcionalidades, las credenciales digitales son más lucrativas, pero pueden representar una barrera adicional para los usuarios sin acceso a la tecnología y en áreas de baja conectividad. Asegurarse de que las credenciales elegidas sean inclusivas y no impidan el uso de la identificación digital para algunos sectores de la población. Las Identificaciones digitales que exigen la posesión de un teléfono inteligente o un dispositivo similar podrían perjudicar a algunos grupos de población, como por ejemplo a las mujeres de ciertos países, quienes pudiesen no tener acceso a un teléfono inteligente o no tener autonomía para utilizarlo. La emisión de más de una credencial ayudará a resolver estos desafíos.	Promover el uso equitativo de la identidad digital y los servicios asociados, velando al mismo tiempo a favor que no se cree ninguna barrera adicional de uso para ninguna categoría de usuarios.

II. PROCEDIMIENTOS DE INCORPORACIÓN Y REGISTRO

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
REQUISITOS PARA LA INCORPORACIÓN	Emitir directrices sobre los requisitos y el proceso de incorporación para las diferentes categorías de residentes (ciudadanos, extranjeros, solicitantes de asilo, distintos sexos). Establecer requisitos claros y fáciles para alcanzar los requisitos mínimos para la incorporación a la plataforma/sistema de identificación basándose en los objetivos del sistema. Se debe asegurar que los requisitos mínimos establecidos no impidan aún más que algunos sectores de la sociedad se incorporen al sistema. Considerar el contexto del país y el uso de la identidad digital para decidir si la incorporación debe basarse en la inserción (incorporación automática de todos los ciudadanos) o en la extracción (los ciudadanos deben presentar una solicitud explícita). En el caso de las identificaciones fundacionales que se aprovechan más para las prácticas de e-KYC, la incorporación debe abarcar a la mayoría de la población adulta. Los países con bases de datos digitales confiables que ya cubren una parte de la población pueden adoptar un enfoque totalmente digital basado en empujes para la incorporación. Sin embargo, el proceso de registro podría iniciarse para la población no identificada si hay brechas en la cobertura de las bases de datos digitales. Los países que prefieren construir una base de datos desde cero para evitar el uso de una base de datos con discrepancias pueden utilizar un enfoque basado en la extracción.	Garantizar una cobertura amplia e inclusiva de la identificación digital y una fácil incorporación para todos los ciudadanos y usuarios.
PUNTOS DE ACCESO PARA USUARIOS	Desarrollar directrices basadas en los requisitos del país sobre los puntos de acceso para que los usuarios interactúen con la plataforma de identidad digital y con propósitos de utilizar servicios de e-KYC. Estos puntos se pueden usar para la incorporación, verificación, autenticación y otros servicios según sea necesario y se debe contar con un sólido sistema de seguimiento para promover la integridad del proceso de registro. Las directrices deben velar a favor de una cobertura geográfica adecuada y de que se realicen ajustes para atender a los grupos desfavorecidos de la población. Los puntos de acceso pueden ser un centro administrado por el gobierno, una cadena separada de centros de registro o quioscos administrados por otras partes interesadas pero vigilados por el gobierno, o de manera remota. Aprovechar de mejor manera a los actores del sector privado para lograr un mejor alcance y eficiencia. Considerar la posibilidad de colaborar con puntos de acceso digitales para la banca, que ya podrían tener una red establecida.	Asegurar que se tengan puntos de fácil acceso con el fin de que los usuarios se registren e interactúen con el sistema de identificación digital, generando así confianza y buena voluntad entre dichos usuarios en cuanto a usar la identificación para varios otros usos.
COSTOS DIRECTOS PARA EL USUARIO	Publicar directrices y hacerlas cumplir para garantizar costos directos mínimos o nulos con el fin de que los ciudadanos o usuarios se incorporen al sistema de identificación digital o utilicen los mecanismos de e-KYC. Un costo mínimo para los usuarios fomentará su uso. Los costos, si los hubiera, se deben cobrar en caso de pérdida de credenciales (tarjetas) que deban volver a emitirse.	Uno de los principales objetivos para aprovechar mejor un sistema de identificación digital es reducir el costo y el tiempo dedicado a los usuarios. Los costos adicionales para usar este sistema reducirán su disposición a participar.

III. CAPACIDADES DEL SISTEMA

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
ESTÁNDARES TÉCNICOS	Definir estándares técnicos específicos a seguir en el desarrollo de la plataforma y la base de datos de identificación. Los estándares técnicos se pueden establecer utilizando referencias de otras prácticas de identificación digital y e-KYC así como la guía proveniente de los organismos que establecen los estándares.[17] Además de los estándares técnicos, el sistema debe garantizar los siguientes aspectos clave: a. Solidez y alta funcionalidad b. Capacidad de personalización y configurabilidad c. Privacidad integrada en el diseño.[18] d. Estándares para recopilar, almacenar y compartir los datos con terceros, cuando esté permitido e. Acceso en tiempo real a los datos para e-KYC y otros casos de uso f. Infraestructura adicional para apoyar las interfaces de programación de aplicaciones (API) para la identificación digital de e-KYC y los procedimientos de autenticación, y para simplificar el acceso a los datos para su uso productivo. Considerar las opciones de código abierto para el desarrollo de tecnología con el fin de evitar el bloqueo por parte de los proveedores y para un desarrollo a costo más bajo. Las decisiones sobre identificación centralizada o descentralizada deben tener en cuenta la infraestructura y las necesidades del país.	To help assess the country's available technology infrastructure and make further amendments in line with international standards. It will also ensure standards for digital ID and e-KYC meet the desired performance targets. API infrastructure will provide convenient mechanisms for stakeholders to verify and authenticate using the digital ID database.
CARACTERÍSTICAS TÉCNICAS DEL SISTEMA	Orientar sobre las características técnicas que deben programarse en el sistema para garantizar su eficacia. Algunas características clave que ayudarán a mejorar las capacidades del sistema son: a. Deduplicación dinámica y automatizada b. Controles de fraude y procesos antifraude integrados c. ases de datos separadas para datos biométricos y demográficos d. Vínculos en tiempo real con registros de nacimientos y defunciones con el propósito de que se actualicen automáticamente e. Admitir múltiples mecanismos de autenticación biométrica f. Autenticación e incorporación fuera de línea g. Procedimientos de gestión de excepciones h. Arquitectura para la gestión de consentimientos i. Vínculos con otros sistemas de identificación para promover diferentes casos de uso, como licencias de conducir, seguridad social, sistema de identificación fiscal, sistema nacional de salud, etc.	Garantizar que el sistema siga las mejores prácticas mundiales y se actualice y mantenga constantemente.
AUDITORÍAS Y EVALUACIONES TÉCNICAS	Emitir directrices y exigir que se realicen revisiones periódicas de la tecnología subyacente por razones de eficiencia, innovación y la rentabilidad.	Garantizar que se lleven a cabo actualizaciones oportunas, así como el cumplimiento de los estándares y mejores prácticas del sector que se encuentran en evolución.

17 World Bank. 2018. ID4D Practitioner's Note. Catalog of Technical Standards for Digital Identification Systems. Banco Internacional de Reconstrucción y Fomento / Banco Mundial. Disponible en: https://olc.worldbank.org/system/files/129743-WP-PUBLIC-ID4D-Catalog-of-Technical-Standards.pdf

18 Alliance for Financial Inclusion. 2021. Nota de orientación sobre la privacidad de los datos para servicios financieros digitales. Disponible en: https://www.afi-global.org/publications/guideline-note-on-data-privacy-for-digital-financial-services/

IV. GESTIÓN DE DATOS

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
GESTIÓN DE DATOS DE 360 GRADOS (DATOS EN REPOSO, EN USO Y EN MOVIMIENTO)	Publicar y hacer cumplir procedimientos estrictos de gestión de datos para todas las partes involucradas en la recolección, el procesamiento y el almacenamiento de datos de los usuarios. a. Tokenización, virtualización y autenticación de dos factores cuando se utilizan datos b. Barreras físicas y técnicas de acceso cuando los datos están almacenados y en reposo, incluidos los métodos autorizados de acceso, almacenamiento y archivo c. Cifrado y líneas seguras cuando se transmiten datos Los datos recopilados legalmente se pueden utilizar para generar datos agregados o resúmenes estadísticos sin referencia ni identificación de ninguna persona individual de manera específica.	Hacer cumplir todas las medidas de seguridad y privacidad de los datos, y cerciorarse que las prácticas de gestión de datos protejan los datos del usuario de ataques externos.

V. SERVICIOS PARA EL USUARIO

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
SERVICIOS PARA EL USUARIO	Los servicios para el usuario deben incluir: a. Capacidad para dar consentimiento y autorizaciones para el uso por parte de terceros b. Capacidad para revocar el consentimiento c. Capacidad para bloquear datos biométricos d. Capacidad y visibilidad para rastrear transacciones en las que se solicitaron y manejaron datos personales e. Opciones de portabilidad de la información f. Canal para mecanismo de disputa y solicitud de indemnización Se deben publicar y distribuir entre los usuarios las directrices sobre cómo los usuarios pueden acceder a dichos servicios. Se deben proporcionar múltiples canales, preferiblemente para facilitar el acceso, aplicaciones móviles; el acceso al USSD y al sitio web se pueden considerar por encima de las solicitudes manuales Las entidades que implementan también deben idear formas de comunicarse eficazmente con los usuarios para que tomen conciencia sobre disposiciones, consentimiento, derechos, servicios y casos de uso de los sistemas de identificación. Los usuarios también deben estar informados sobre los canales y dispositivos que se utilizan dentro del ecosistema.	Velar a favor de que los sistemas construidos estén centrados en el usuario y que el control de los datos esté en manos de dicho usuario.

PARTE III. CONSIDERACIONES SOBRE POLÍTICAS PARA IMPLEMENTAR PROCESOS Y CASOS DE USO CLAVE QUE APROVECHAN DE MEJOR MANERA LA IDENTIFICACIÓN DIGITAL PARA E-KYC

Esta sección destaca uno de los casos de uso clave para la identificación digital, el cual es e-KYC y los servicios de autenticación. Resume las prácticas eficaces aplicadas por los miembros de AFI y a nivel mundial, y detalla un marco y unos principios rectores para construir procesos sólidos para e-KYC, incluyendo el acceso, la interoperabilidad, la infraestructura de última milla y la gestión de excepciones.

I. MARCO DE AUTENTICACIÓN Y E-KYC

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
MARCO PARA LA IMPLEMENTACIÓN DE E-KYC	Orientar y construir un marco e-KYC, detallando los siguientes aspectos clave, en caso de que correspondan: a. Alcance del e-KYC simplificado y del e-KYC regular para diferentes partes interesadas en función del riesgo identificado b. Aplicabilidad de e-KYC (para personas con identificación digital y medidas de excepción para aquellas sin identificación digital) c. Recabar el consentimiento del usuario para el procesamiento, el almacenamiento y la gestión de datos d. Autorización de acceso a terceros para usos legítimos e. Uso de identificación por video[19]	Definir claramente el alcance y el uso de los servicios e-KYC y otras operaciones. Esto ayudará a elaborar una estrategia de implementación con objetivos y metas claros.
MECANISMO DE AUTENTICACIÓN	Consultar con las partes interesadas y los expertos técnicos pertinentes para desarrollar un mecanismo de autenticación que sea pertinente para el contexto del país y cumpla con los requisitos de ALA/CFT. El sistema de identificación digital puede aprovecharse de mejor manera para atender varios niveles de certeza, utilizando tanto la autenticación demográfica como la biométrica. Algunos de los factores clave que se utilizan en la autenticación de la identidad cuando se aprovecha un sistema de identificación digital son: a. Factores de posesión (número de identificación, código QR): algo que una persona demuestre que tiene, como una tarjeta o certificado físico o virtual b. Factores biométricos (huella dactilar, iris, rostro) c. Factores de conocimiento (PIN, contraseña de un solo uso (OTP), Identificación de inicio de sesión). algo que una persona ya sabe	Construir sistemas de autenticación flexibles, seguros y eficientes con medidas de recurso efectivas con el propósito de verificar y autenticar a la población vulnerable (personas cuyas huellas dactilares se desgastan con la edad o debido a cierto tipo de profesiones, personas con discapacidad que no pueden autenticarse mediante el iris, etcétera).

19 Transmisión de video de alta resolución que permite la identificación y la verificación remotas, así como las pruebas de "vida". Ver, FATF. 2020. Guidance on Digital Identity. Disponible en: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-report.pdf

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
MECANISMO DE AUTENTICACIÓN *continued*	Establecer si se trata de autenticación descentralizada, que utiliza dispositivos de última milla, como por ejemplo, lectores de tarjetas, o autenticación centralizada con coincidencia en tiempo real con la base de datos de identificación digital. Lo ideal es que el mecanismo de autenticación sea multimodal e independiente del dispositivo (es decir, capaz de utilizar diferentes factores y cédulas para fines de verificación). Los sistemas de autenticación de dos factores cumplen con requisitos de seguridad más altos y los sistemas multimodales ofrecerán un proceso integrado de manejo de excepciones.	
PARÁMETROS DE COINCIDENCIA PARA LA AUTENTICACIÓN	Desarrollar parámetros de coincidencia apropiados con base en referencias y límites técnicamente aceptados. Lo ideal es que los parámetros de coincidencia de datos numéricos, como la fecha de nacimiento, los números de teléfono, sean del 100 por ciento. Los factores biométricos pueden estar entre el 80 y el 100 por ciento para ajustar la calidad de los escáneres y los dispositivos de última milla.	Los parámetros de coincidencia definen la precisión del sistema; altos niveles de parámetros de coincidencia ayudarán a generar confianza en las capacidades del sistema. Sin embargo, con el fin de garantizar una métrica final equilibrada, esto se debe sopesar con la posibilidad de que aumenten los porcentajes de fallas.

II. ACCESO E INTEROPERABILIDAD PARA TERCERAS PARTES INTERESADAS

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
PROCEDIMIENTOS SIMPLIFICADOS DE ACCESO Y USO	Definir un conjunto estandarizado de reglas de participación para los terceros interesados que deseen acceder al sistema. Resaltar los requisitos y permisos mínimos necesarios para obtener acceso. Detallar los pasos y procedimientos para obtener el acceso y los requisitos del tercero, en cuanto a protección de datos y medidas de seguridad, sobre si se concede acceso a las partes interesadas de manera individual a través de un memorando de entendimiento o a través de entidades autorizadas.[20]	Promover que las partes interesadas cuenten con acceso uniforme y justo, con el fin de que se pueda aprovechar mejor el sistema. Garantizar documentación estandarizada como memorandos de entendimiento, acuerdos de confidencialidad (ADC) y otros acuerdos contractuales.
ACCESO A LOS DATOS POR NIVELES	Definir y publicar una lista estandarizada de diferentes niveles de servicios que utilizan la identificación digital, como por ejemplo autenticación y e-KYC (demográfico y biométrico), así como completar automáticamente los datos de los usuarios, entre otros. Este sistema por niveles debe basarse en principios y niveles de acceso en lugar de basarse en las necesidades de cada entidad.	Permitir que los actores del sector elijan de la lista establecida en función de sus requisitos, y por lo tanto ayudarlos a preparar sus sistemas internos.
CANALES DE ACCESO	Proporcionar directrices claras sobre los canales y mecanismos disponibles para que terceros accedan a datos de la plataforma de identificación digital. Los canales se pueden concretar de manera final en base a un análisis de riesgo de las diversas alternativas, así como sus puntos a favor y contra. El acceso se puede proporcionar a través de API, enlaces de servicios web o enlaces directos al sistema a través de autorizaciones.	Los canales disponibles deben garantizar un acceso fácil y simplificado para un uso económico e ininterrumpido de los datos y servicios.

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
ESTRUCTURAS DE COSTOS ECONÓMICOS	A través de consultas detalladas e intercambios de ideas sobre la estrategia de precios, se debe alcanzar una comprensión sobre la disposición a pagar que existe entre las partes interesadas. Los diferentes modelos adoptados podrían ser: a. Estructura de costos por niveles basada en transacciones con una tarifa que depende del nivel de acceso y servicio brindado b. Modelo basado en suscripción con cobros mensuales o anuales Los modelos de determinación de precios actualmente en uso son libres de costo para las entidades públicas, y las entidades privadas pagan montos mínimos.[21] Una autenticación simple que aprovecha mejor el sistema de identificación digital tiene costos insignificantes, mientras que una solicitud de e-KYC con intercambio de datos tiene un costo ligeramente superior.	Los costos más bajos de los servicios fomentarán la adopción entre las partes interesadas y proporcionarán algunos ingresos para los administradores del sistema con el fin de garantizar la sostenibilidad del sistema.
MONITOREO Y SUPERVISIÓN DE ACCESO Y USO	Brindar directrices a las entidades ejecutoras sobre los mecanismos de monitoreo que deben estar instituidos con el fin de vigilar a terceros con acceso. Estos mecanismos deben definirse en el Memorando de Entendimiento. Los mecanismos de seguimiento deben incluir informes periódicos, notificaciones sobre cualquier incumplimiento, y detalles de los cargos y multas impuestas. Estas medidas deben ser acordadas por las entidades ejecutoras, así como por terceros interesados.	Garantizar que las prácticas de protección de datos también sean respetadas por todos los actores del ecosistema y penalizar cualquier uso indebido o fraude.

III. INFRAESTRUCTURA Y DISPOSITIVOS DE ÚLTIMA MILLA

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
INFRAESTRUCTURA DE ÚLTIMA MILLA	Establecer y publicar directrices o estándares del sector con respecto a los dispositivos que se utilizan para la autenticación de última milla de los usuarios, como por ejemplo escáneres biométricos y lectores de tarjetas. Considerar la certificación de dispositivos utilizados en la última milla que pueda garantizar características técnicas estandarizadas, calidad y requisitos de seguridad. Los estándares y directrices deben asegurar que sólo se utilicen dispositivos autorizados/certificados para acceder a la plataforma de identidad digital. Se puede implementar el seguimiento del número de serie o el registro en una autoridad central para evitar el uso indebido y proporcionar una forma de supervisar los dispositivos utilizados por los funcionarios encargados de la última milla.	Para garantizar el cumplimiento de los protocolos de seguridad y la protección de datos y la privacidad de los datos durante la transferencia y el uso de datos.

21 World Bank. 2019. ID4D Practitioner's Note. Identity Authentication and Verification Fees: Overview of Current Practices. Washington, DC: World Bank. Disponible en: http://documents1.worldbank.org/curated/en/945201555946417898/pdf/Identity-Authentication-and-Verification-Fees-Overview-of-Current-Practices.pdf

IV. CASOS DE USO

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
INTEROPERABILIDAD E INFRAESTRUCTURA COMPARTIDA	Involucrar a los participantes de mercado y a otras partes interesadas para promover el debate y orientar sobre la interoperabilidad y los casos de uso que pueden aprovechar mejor la infraestructura construida.[22] Fomentar debates sobre la política y los requisitos regulatorios con el propósito de facilitar la interoperabilidad para: a. Prestación de servicios gubernamentales b. Prestación de protección social por parte de distintos departamentos/ministerios c. Instituciones financieras formales d. FinTechs e. Instituciones no financieras, como las telco (compañías telefónicas) f. Empresas de e-KYC/KYC de terceros que cuentan con autorización g. Votaciones h. Administración tributaria i. Actividades de litigio	Velar a favor del uso sostenido y la eficiencia del mercado mediante servicios interoperables y animar a las partes interesadas a comprometerse con la infraestructura compartida.

V: MANEJO DE EXCEPCIONES Y RESOLUCIÓN DE QUEJAS

CATEGORÍA REGULATORIA	PRINCIPIO RECTOR	JUSTIFICATIVO
PROCEDIMIENTOS DE MANEJO DE EXCEPCIONES	Documentar algunos de los desafíos clave que podrían surgir y los procedimientos y protocolos de manejo de excepciones para los mismos. Procedimientos que se deben emprender durante fallas de autenticación o de falta de coincidencia biométrica, particularmente para transacciones e-KYC. También deben establecerse procedimientos alternativos en áreas con baja conectividad o que enfrentan otros desafíos de infraestructura. Se pueden considerar opciones como el modo fuera de línea utilizando un código QR o lectores de tarjetas.	Velar a favor de procesos simplificados y descentralizados en torno a la autenticación biométrica eliminando las barreras tecnológicas y de capacidades de lectoescritura.
RESOLUCIÓN DE QUEJAS	Ofrecer una sólida infraestructura de resolución de quejas a través de múltiples canales que incorporen interfaces humanas y tecnológicas. Los canales deben ser de fácil acceso, tener bucles de retroalimentación adecuados y ofrecer tiempos de resolución rápidos. También se debe prever disposiciones con respecto a las reclamaciones y los litigios por parte de las instituciones financieras usuarias. Se pueden considerar distintos niveles de acuerdos para manejar las quejas de los clientes entre instituciones responsables clave para el sistema de identificación digital. Los detalles de los mecanismos de resolución de quejas deben ser difundidos públicamente, y los usuarios deben ser informados de esto durante la incorporación. Los canales eficaces que se deben poner a disposición de los usuarios como opciones son: un número de teléfono gratuito, una página web o una dirección de correo electrónico, o si el sistema pone a disposición de los usuarios una aplicación móvil, un canal basado en la aplicación (app).	Facilitar el acceso fácil de las personas a vías de recursos frente a cualquier aspecto relativo a la gestión de su identidad (inscripción, error de autenticación, falta de coincidencia biométrica, robo de identidad, uso indebido de datos, etc.).

22 Alliance for Financial Inclusion. 2019. Modelo de políticas para el dinero electrónico. Disponible en: https://www.afi-global.org/sites/default/files/publications/2019-09/AFI_DFS_Emoney_AW_digital_0.pdf, p.7— (En español)

ANEXO 1: PRÁCTICAS DE POLÍTICA DE IDENTIDAD DIGITAL Y E-KYC EN LOS PAÍSES MIEMBROS DE AFI

NOMBRE DEL PAÍS	POLÍTICA REPORTADA
BANGLADESH	AML/CFT: (Enlace) (En inglés) Orientaciones e-KYC: : (Enlace) (En inglés) Protección de datos: Ley de seguridad digital, 2018 (Enlace) (En inglés)
BANCO CENTRAL DE LOS ESTADOS DE ÁFRICA OCCIDENTAL (BCEAO)	Directiva N°02/2015 /CM/UEMOA sobre la lucha contra el blanqueo de capitales y la financiación del terrorismo en los estados miembros de la UEMOA (Enlace) (En francés) CEDEAO : Acta adicional A/SA.1/01/10 de 16 de febrero de 2010 relativa a la protección de datos personales (Enlace) (En francés) CEDEAO : Directiva C/DIR/1/08111 sobre la lucha contra la ciberdelincuencia en el área de la CEDEAO (Enlace) (En francés)
EL SALVADOR	El Salvador está en camino de construir la identificación digital, al establecer un anteproyecto de "LA LEY ESPECIAL PARA LA PREVENCIÓN, CONTROL Y PENALIZACIÓN DEL LAVADO DEL DINERO" (Enlace) (En español)
FILIPINAS	ALA/CFT: Ley de la República No. 9160, también conocida como la Ley contra el lavado de dinero de 2001 (Enlace) (En inglés) Digital ID: PhillID - Ley de la República No. 11055 (Enlace), o la Ley del Sistema de Identificación de Filipinas, firmada por el presidente Rodrigo Roa Duterte el 6 de agosto de 2018. (En inglés) Es una ley que establece un sistema único de identificación nacional que tiene como objetivo proporcionar una prueba válida de identidad para los ciudadanos filipinos y los extranjeros residentes en Filipinas. Protección de datos: Ley de privacidad de datos - Ley de la República No 10173 (Enlace) (En inglés) Ciberseguridad: Ley de prevención del delito cibernético de 2012 - Ley de la República No. 10175 (Enlace) (En inglés)
GHANA	Ley de la Autoridad Nacional de Identificación de 2006 (Ley 707), Ley de Registro Nacional de Identidad (Enmienda) de 2017 (Ley 750) (En inglés) Ley contra el lavado de activos, 2020 (Ley 1044) (En inglés) Directrices ALA/CFT para bancos e instituciones financieras no bancarias en Ghana, julio de 2018. (En inglés). Ley de Protección de Datos de 2012 (Ley 843) (En inglés) Ley de ciberseguridad, 2020 (Ley 1038) (En inglés) Ley de Servicios y Sistemas de Pago, 2019 (Ley 987) (En inglés) Ley de transacciones electrónicas de 2008 (Ley 772) (En inglés)
INDIA	ALA/CFT: Circular general sobre las normas de "Conozca a su cliente" (KYC) /normas contra el blanqueo de capitales (ALA)/lucha contra la financiación del terrorismo (CFT)/ obligación de los bancos en virtud de la Ley de prevención del blanqueo de capitales (PMLA), 2002 (Enlace) (En inglés) Identificación digital: Aadhaar y otras leyes (enmienda), 2019 (enlace) (Enlace) (En inglés) Protección de datos:

COUNTRY	REPORTED POLICY
MADAGASCAR	AML/CFT: (Enlace) Protección de datos: Loi n°2014-038 sur la protection des données à caractère personnel (Enlace), (en francés). Se estable un autoridad independiente para la protección de datos (la Comisión Nacional de la informática y las libertades). Es responsable de cerciorase que los manejos de datos personales se realicen siguiendo las disposiciones de la ley. Ciberseguridad: (Enlace)
MÉXICO	Identificación digital: Marco legal del Registro Nacional de Población e Identidad (Enlace) (En español) ALA/CFT: Artículo 15 de la Ley de Instituciones de Crédito (Enlace) (En español) Protección de datos y privacidad: Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Enlace) (En español) Ciberseguridad: Disposiciones generales sobre seguridad de la información para las entidades de crédito (Enlace) (En español)
NAMIBIA	ALA/CFT: Ley de Inteligencia Financiera, 2012 (Enlace) (En inglés)
NIGERIA	Regulaciones AFA/CFT (Regulación enmendada 2019) (Enlace) (En inglés) Reglamento de protección de datos de Nigeria 2019 (Enlace) (En inglés) Delitos Cibernéticos (Ley de Prohibición y Prevención) (Enlace) (En inglés) Ley de la Comisión Nacional de Gestión de la Identidad de 2007 (Enlace) (En inglés)
PERÚ	Identidad digital: Decreto Supremo N° 029-20221-PCM, Decreto Legislativo que aprueba el Reglamento de la Ley de Gobierno Digital (Enlace) (En español) Protección de datos: Ley N° 29733 y su Reglamento - regula el tratamiento adecuado de los datos, tanto por parte de entidades públicas como privadas (Enlace) (En español) Regulación para ciberseguridad (Enlace) (En español)
RUSIA	Protección de datos y privacidad: Ley Federal de Datos Personales, 2006 (Enlace) (En inglés) AML/CFT: (Enlace) Identificación digital: Resolución del Gobierno de la Federación de Rusia No. 710, 2019 (Enlace) (En inglés)
SENEGAL	Senegal: Ley n ° 2008-12 de 25 de enero de 2008 sobre Protección de datos personales (Enlace) (En francés) Senegal: Ley n ° 2008-11 de 25 de enero de 2008 sobre ciberdelito (Enlace) (En francés)
SINGAPUR	ALA/CFT: Directrices sobre la prevención del blanqueo de capitales y la lucha contra la financiación del terrorismo (Enlace) (En inglés) Identificación digital: (Enlace) (En inglés) Ley de protección de datos de 2012 (Enlace) (En inglés)
ZAMBIA	ALA/CFT: Ley del Centro de Inteligencia Financiera de 2016 (Enlace) (En inglés) Protección de datos: Ley de protección de datos de 2021 (Enlace) (En inglés) Ciberseguridad: El proyecto de ley de ciberseguridad y ciberdelitos (Enlace) (En inglés)

ANNEXURE 2: REFERENCES

1. World Bank. 2019. ID4D Practitioner's Guide: Version 1.0 (October 2019). Washington, DC: World Bank. Disponible en: http://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

2. World Bank. 2018. ID4D Practitioner's Note. Catalog of Technical Standards for Digital Identification Systems. Washington, DC: International Bank for Reconstruction and Development / The World Bank. Disponible en: https://olc.worldbank.org/system/files/129743-WP-PUBLIC-ID4D-Catalog-of-Technical-Standards.pdf

3. The Centre for Internet and Society. 2020. Governing ID: Principles for Evaluation. Disponible en: https://digitalid.design/docs/CIS_DigitalID_EvaluationFrameworkDraft02_2020.01.pdf

4. Alliance for Financial Inclusion. 2021. "Four policies to promote inclusive financial integrity in 2021". Disponible en: https://www.afi-global.org/newsroom/blogs/four-policies-to-promote-inclusive-financial-integrity-in-2021/

5. Alliance for Financial Inclusion. 2019. KYC Innovations, Financial Inclusion and Integrity. Disponible en: https://www.afi-global.org/wp-content/uploads/publications/2019-03/KYC-Innovations-Financial-Inclusion-Integrity-Selected-AFI-Member-Countries_0.pdf

6. Alliance for Financial Inclusion. 2020. Inclusive Financial Integrity: A Toolkit for Policymakers. Disponible en: https://www.afi-global.org/sites/default/files/publications/2020-07/AFI_CENFRI_toolkit_AW_digital.pdf

7. Alliance for Financial Inclusion. 2021. Guideline Note on Data Privacy for Digital Financial Services. Disponible en: https://www.afi-global.org/wp-content/uploads/2021/02/AFI_GN43_AW3_digital.pdf

8. FATF. 2020. Guidance on Digital Identity. FATF, París. Disponible en: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity-report.pdf

9. World Bank. 2018. G20 Digital Identity Onboarding. Disponible en: https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf

Alliance for Financial Inclusion
AFI, Sasana Kijang, 2, Jalan Dato' Onn, 50480 Kuala Lumpur, Malaysia
t +60 3 2776 9000 **e** info@afi-global.org www.afi-global.org
Alliance for Financial Inclusion AFI.History @NewsAFI @afinetwork