PRINCIPIOS SOBRE LA

IDENTIFICACIÓN PARA EL DESARROLLO SOSTENIBLE: HACIA LA ERA DIGITAL

ENDORSING ORGANIZATIONS

African Development Bank

Asian Development Bank (ADB)

Bill & Melinda Gates Foundation (BMGF)

Center for Global Development (CGD)

Digital Impact Alliance (DIAL)

FHI 360

ID4Africa

International Organization for Migration (IOM)

International Union of Notaries

Mastercard

Omidyar Network

Open Identity Exchange UK/Europe

Organization of American States

OSCE Office for Democratic Institutions and Human Rights (ODIHR)

Plan International

Privacy and Consumer Advisory Group to the Government Digital Service and GOV.UK

Secure Identity Alliance (SIA)

The GSMA

UN World Food Programme

UNHCR, The UN Refugee Agency

United Nations Children's Fund (UNICEF)

United Nations Development Programme (UNDP)

United Nations Economic Commission for Africa (ECA)

World Bank Group

Facilitated by: World Bank Group and Center for Global Development

PRINCIPIOS SOBRE LA

IDENTIFICACIÓN PARA EL DESARROLLO SOSTENIBLE: HACIA LA ERA DIGITAL

PRINCIPIOS

INCLUSIÓN:
COBERTURA Y ACCESIBILIDAD UNIVERSAL

1. Garantizar una cobertura universal para los individuos desde el nacimiento hasta la muerte, sin discriminación.
2. Eliminación de obstáculos al acceso y uso y de las disparidades en la disponibilidad de información y tecnología.

DISEÑO:
ESTABILIDAD, SEGURIDAD, CAPACIDAD DE RESPUESTA Y SOSTENIBILIDAD

3. Establecimiento de una identidad única, segura y precisa desde el nacimiento hasta la muerte.
4. Creación de una plataforma que sea interoperable y que responda a las necesidades de los diversos usuarios.
5. Uso de estándares abiertos y garantía de neutralidad tecnológica y de proveedores.
6. Protección de la privacidad del usuario y control mediante el diseño de sistemas.
7. Planificación para la sostenibilidad financiera y operacional sin comprometer la accesibilidad.

GOBERNABILIDAD:
FOMENTO DE LA CONFIANZA MEDIANTE PROTECCIÓN DE LA PRIVACIDAD Y DERECHOS DE LOS USUARIOS

8. Salvaguarda de la privacidad de los datos, la seguridad y los derechos de las personas naturales a través de un marco jurídico y normativo amplio.
9. Establecimiento de mandatos institucionales claros y rendición de cuentas.
10. Aplicación de los marcos jurídicos y de confianza con vigilancia independiente y resolución de quejas.

PROPÓSITO

Creemos que toda persona tiene derecho a participar plenamente en la sociedad y la economía. Si una persona no tiene forma de comprobar su identidad, puede que se le deniegue el acceso a derechos y servicios tales como abrir una cuenta bancaria, asistir a la escuela, recibir beneficios sociales, obtener protección jurídica o incluso participar en la sociedad moderna. Nadie debería sufrir la humillación de ser excluido, de que se le deniegue la oportunidad de alcanzar su pleno potencial, de ejercer sus derechos o de participar en el progreso. Nadie debería quedarse atrás.

Las organizaciones que suscriben estos principios reconocen el potencial de contar con sistemas sólidos de identificación que propicien el desarrollo y el logro de los Objetivos de Desarrollo Sostenible (ODS)[1]. Creemos que la creación de sistemas de identificación incluyentes, seguros y confiables puede empoderar a los individuos y mejorar su acceso a derechos, servicios y la economía formal. Asimismo estos sistemas pueden fortalecer las capacidades de los Gobiernos, el sector privado, las organizaciones no gubernamentales (ONG) y todos aquellos participantes en ayuda al desarrollo para que así puedan gestionar programas y proveer servicios de manera transparente, eficiente y eficaz. Los beneficios para el desarrollo derivados de la mejora en los sistemas de identificación aumentarían considerablemente con la adopción de la tecnología digital y muchos países ya están avanzando en esta dirección. Sin embargo, al mismo tiempo que el desarrollo de sistemas de identificación —en particular los digitales— genera oportunidades para promover los objetivos de desarrollo, también puede generar diversos desafíos y riesgos.

---

1 La identidad es un conjunto de atributos que describen de forma inequívoca a una persona o entidad. El suministro de identificación —"prueba de identidad"— ha quedado plasmado en el objetivo 16.9 de los ODS que establece el suministro de "una identidad jurídica para todos, en particular mediante el registro de nacimientos". Además, la identificación es un elemento clave de muchos otros objetivos, incluidos el 1.3 (la implementación de sistemas de protección social), el 1.4 (garantizar que los pobres y vulnerables tengan control sobre la tierra, otros bienes y recursos financieros), el 5a (otorgar a las mujeres la igualdad de acceso, incluida la financiación), el 5b (mejorar el uso de tecnología, incluidas las TIC para promover el empoderamiento de las mujeres), el 10.7 (migración y movilidad seguras y responsables), el 10c (reducir el costo de transacción de remesas), el 12c (la eliminación gradual de subsidios perjudiciales), el 16a (fortalecer las capacidades para combatir el terrorismo y la delincuencia) y el 16.5 (reducir la corrupción) entre otros.

En esta declaración, por lo tanto, se identifica un conjunto de principios comunes y fundamentales para aprovechar al máximo los beneficios de los sistemas de identificación para el desarrollo sostenible y, al mismo tiempo, mitigar muchos de los riesgos. Estos principios son aplicables al concepto amplio de sistemas de "identificación legal" con los que es posible el registro e identificación de individuos para poder proporcionarles identificaciones reconocidas por las autoridades (por ejemplo, números de identificación, tarjetas, certificados digitales, etc.) que pueden utilizarse como prueba de identidad[2]. En virtud de esta definición incluyente, una identificación legal no necesita estar vinculada a la nacionalidad o ciudadanía[3].

Muchos países han avanzado considerablemente al proporcionar identificación legal; sin embargo, todavía queda mucho por hacer. El objetivo de estos principios es, por consiguiente, fomentar la cooperación en torno a la implementación de sistemas de identificación conforme a un conjunto de valores y normas compartidos. Estos principios se basan en normas internacionales existentes y reconocemos que tendrán que evolucionar con el tiempo para incorporar una gama más amplia de perspectivas de las partes interesadas, así como las nuevas tecnologías y la experiencia de la implementación.

Esperamos que estos principios sean respaldados por un espectro cada vez más amplio de partes interesadas, incluidos Gobiernos, organizaciones intergubernamentales, empresas privadas, ONG locales e internacionales y colaboradores en ayuda al desarrollo. Mediante el uso de estos principios armonizadores, las partes interesadas estarán en mejores condiciones de alinearse y canalizar su apoyo, facilitar el debate a nivel mundial, regional y de país, y trabajar juntos en el fomento de sistemas de identificación consistentes e incluyentes que permitan alcanzar los objetivos del desarrollo sostenible.

---

2 En la actualidad, la mayoría de las identificaciones legales es proporcionada por o en nombre de los Gobiernos. En el futuro, podrían ser posibles otros modelos, pero los Gobiernos deberían ser los responsables en última instancia de la identificación legal.

3 Algunos sistemas de identificación legal, como los programas nacionales de Perú, Pakistán y muchos otros países, están vinculados a la nacionalidad, mientras que otros no lo están. En el sistema Aadhaar de India, por ejemplo, se ha desvinculado el concepto de nacionalidad de la identificación a fin de establecer la singularidad de los 1.2 mil millones de residentes del país y de crear una plataforma para garantizar la autenticación por parte de terceros para la prestación de servicios. Véase Gelb & Clark (2013). Como se indica en los principios, la identificación legal básica debería, en todo caso, ser otorgada a todas las personas residentes en un territorio.

ANTECEDENTES

Unos 1.500 millones de personas del mundo en desarrollo carecen de un comprobante de identidad legal[4]. Esta "brecha" en materia de identificación es un serio obstáculo para la participación en la vida política, económica y social. Sin una forma segura y confiable de comprobar su identidad, una persona podría no estar en condiciones de ejercer toda la gama de los derechos humanos que las las leyes y convenciones internacionales le confieren. La falta de una identificación también hace que sea difícil abrir una cuenta bancaria, votar, obtener un empleo formal, asistir a la escuela, recibir atención sanitaria o una transferencia social, comprar una tarjeta SIM o solicitar una reparación de daños por vía judicial. Además, los estados con sistemas de identificación deficientes tienen dificultades con la administración pública, la planificación y la prestación de servicios, incluida la recaudación de impuestos, la focalización de programas sociales, la respuesta a situaciones de emergencia, desastres y epidemias, la gestión de sus fronteras y la seguridad[5].

El logro de un desarrollo inclusivo, por lo tanto, requiere un esfuerzo sostenido para cerrar esa brecha que representa la falta de una identificación. El objetivo 16.9 de los ODS aspira a "proporcionar acceso a una identidad jurídica para todos, en particular mediante el registro de nacimientos", para el año 2030. Con este fin, los Gobiernos de muchos países —junto con organismos internacionales, donantes y aliados del sector privado— han iniciado serios esfuerzos para fortalecer los sistemas de identificación legal, incluidos los registros civiles, los documentos de identificación nacional y las bases de datos poblacionales, así como los registros de votantes, de transferencias sociales, documentos de viaje y otros.

En muchos casos, estas reformas incluyen la transición de sistemas de identificación en papel a los digitales: un cambio que supone nuevas oportunidades y retos. Las tecnologías digitales, como la computación en nube, la biometría, las redes móviles, así como los dispositivos y tarjetas inteligentes, pueden aumentar la seguridad, la precisión y la conveniencia de identificar y autentificar a las personas. A medida que los proveedores de servicios públicos y privados hagan la transición a los sistemas digitales, será esencial que los individuos puedan comprobar su identidad para poder participar en el mundo digital.

---

4 Estimaciones del ID4D Dataset del Banco Mundial, a febrero de 2016. Estos datos se actualizarán anualmente.
5 Gelb, A. & Clark, J. 2013. 2016. *Identification for Development Strategic Framework*.

En consecuencia, los sistemas de identificación digital pueden significar importantes ahorros para los ciudadanos, los Gobiernos y las empresas al reducir los costos de transacción, aumentar la eficiencia, e impulsar la innovación en el suministro de servicios, especialmente para los grupos más pobres y desfavorecidos de la sociedad. Muchos países en desarrollo ya han usado estos sistemas para mejorar la gestión pública, fomentar la inclusión financiera, reducir las desigualdades de género empoderando a mujeres y niñas, y permitir que los pobres tengan un mayor acceso a los servicios sanitarios y a las redes de servicios sociales. También ofrecen un enorme potencial para solucionar los problemas de carencia de identificación que padecen decenas de millones de emigrantes y refugiados. Los nuevos avances tecnológicos —junto con la aplicación de estos principios— pueden ofrecer a los países la oportunidad de dejar atrás métodos tradicionales estableciendo ecosistemas de identidad digital. No obstante, estos principios se aplican tanto a sistemas digitales como aquellos en formato papel.

Estas oportunidades, sin embargo, suponen importantes retos y riesgos. Los esfuerzos para mejorar los sistemas de identificación legal —ya sea digitales o en papel— pueden enfrentar desafíos políticos, incluida la capacidad de mantener un compromiso a largo plazo con proyectos de identificación entre diversas partes interesadas y superar la resistencia de las partes que se benefician de sistemas de identificación deficientes. El garantizar que todas las personas sean incluidas en el sistema puede plantear un gran desafío, especialmente para los residentes de las zonas rurales y remotas, los desplazados por situaciones de fuerza mayor, los apátridas y otros grupos marginados. Además, a falta de leyes de protección de datos, prácticas y marcos normativos rigurosos, los sistemas de identificación pueden minar la confianza y los derechos individuales a la privacidad y el consentimiento con respecto al uso de la información personal. En algunos casos, pueden poner en grave riesgo a los grupos vulnerables. Estos riesgos se acentúan en el área de identificación digital y macro datos. En algunos contextos, la proliferación de nuevas tecnologías ha suscitado preocupaciones por la sostenibilidad, especialmente cuando existe dependencia de un proveedor o cuando las opciones tecnológicas no son totalmente adecuadas para el caso particular o la capacidad del país.

Es fundamental encarar estos retos a fin de garantizar que los sistemas de identificación legal sean eficaces y estén disponibles para todos los **usuarios finales**; es decir, todas aquellas personas que deben comprobar su identidad para tener acceso a derechos y servicios. Esto requiere un esfuerzo sostenido y coordinado por parte de las principales partes interesadas que participan en el suministro y uso de estos sistemas, entre ellos:

- **Individuos.** Estos son los usuarios finales de los sistemas de identificación pues requieren comprobar su identidad para tener acceso a derechos y servicios. Son los actores principales de los sistemas de identificación y tienen derecho a saber y controlar adecuadamente la forma en que se recopilan, utilizan, almacenan y comparten sus datos.

- **Gobiernos.** Las entidades públicas suelen ser las principales proveedoras de sistemas de identificación legal. Estos incluye, entre otros, al registro civil (nacimientos, defunciones y matrimonios), registros de población, identificaciones nacionales, pasaportes, así como los registros y tarjetas de identificación de votantes, etc. Las entidades públicas también utilizan los sistemas de identificación para gestionar programas tales como los de servicios sociales, recaudación de impuestos y licencias de conducir.

- **Sector privado.** Las empresas privadas son los principales desarrolladores, innovadores y proveedores de la infraestructura de los sistemas de identificación. Además, muchas empresas privadas dependen de los sistemas de identificación legal para identificar a sus clientes (por ejemplo, para abrir cuentas bancarias, registrar tarjetas SIM o crear sistemas de información crediticia). Los Gobiernos también han establecido acuerdos con empresas privadas para ofrecer formas de identificación —como identidad digital via móvil que incluye registro, certificación y acreditación y certificados digitales— que amplían el alcance y la uso de los sistemas de identificación legal a las poblaciones desatendidas.

- **Organismos internacionales y ONG.** Al proporcionar protección, asistencia jurídica y otros servicios, los organismos internacionales, la sociedad civil y las organizaciones comunitarias son aliados importantes en la generación de la demanda para los sistemas de identificación y para ayudar a la gente a conseguir la identificación que necesitan para participar en la vida económica, política y social.

- **Socios para el desarrollo.** Los organismos de desarrollo, los donantes y otros agentes humanitarios brindan apoyo a los sistemas de identificación legal en forma de financiación y asistencia técnica, y también pueden participar en el establecimiento de sistemas de identificación para la gestión de programas.

Si toda la gama de partes interesadas comparten una visión, congruente con estos principios comunes, será posible promover sistemas de identificación sólidos e incluyentes propicios para las oportunidades económicas y el logro de resultados en materia de desarrollo sostenible.

PRINCIPIOS

PILAR A. INCLUSIÓN: COBERTURA Y ACCESIBILIDAD UNIVERSAL

Debe hacerse un esfuerzo para que los sistemas de identificación alcancen una cobertura continua y universal desde el nacimiento hasta la muerte, sin discriminación y abiertos a todos los individuos.

1. Garantizar una cobertura universal para los individuos desde el nacimiento hasta la muerte, sin discriminación.

- *Universalidad.* Los países deben cumplir su obligación de proporcionar una identificación legal a todos los residentes —no sólo a los ciudadanos— desde el nacimiento hasta la muerte, como se establece en el derecho y convenciones internacionales y en sus propios marcos legislativos[6]. Esto incluye el compromiso del registro universal de nacimientos para los nacidos en el territorio nacional, que es una parte esencial de la gestión de la identidad.[7]

- *No discriminación.* Es preciso identificar y mitigar las barreras jurídicas, procesales y sociales para registrarse y utilizar los sistemas de identificación, con especial atención a los grupos y personas pobres que pueden estar en riesgo de exclusión por razones culturales, políticas o de otra índole (es decir, las mujeres, los niños, las poblaciones de áreas rurales, las minorías étnicas y lingüísticas, grupos religiosos, los migrantes, las personas desplazadas a la fuerza y los apátridas). Además, los sistemas y datos de identificación no deben utilizarse como instrumento de discriminación ni para atentar contra derechos individuales o colectivos.

---

6 De conformidad con el derecho internacional, los Estados tienen el derecho soberano de determinar quién reúne los requisitos para la ciudadanía. Si bien la prueba de la ciudadanía se limitará a los ciudadanos, los Estados deben proporcionar una identificación legal a todas las personas residentes en su territorio, incluido el registro de nacimientos. También deben proporcionar prueba de ciudadanía a *todas* las personas que tengan derecho a ella sin discriminación de ningún tipo.

7 Por ejemplo, el artículo 7 de la *Convención sobre los Derechos del Niño* establece que "[e]l niño será inscripto inmediatamente después de su nacimiento y tendrá derecho desde que nace a un nombre, a adquirir una nacionalidad y, en la medida de lo posible, a conocer a sus padres y a ser cuidado por ellos". Esta convención ha sido ratificada por todos los Estados miembros de la ONU, excepto por los Estados Unidos, que la ha firmado pero no ratificado. En la práctica, sin embargo, prácticamente todos los nacimientos en Estados Unidos son registrados.

2. Eliminación de obstáculos al acceso y uso y de las disparidades en la disponibilidad de información y tecnología.

- *Costos directos e indirectos.* Los costos no deberían ser una barrera para tener acceso a los servicios de identificación. El registro civil y los primeros certificados de nacimiento y defunción deberían ser gratuitos para la persona que los solicite, al igual que la emisión de la primera credencial de identidad obligatoria. Si se cobra por determinados servicios adicionales (por ejemplo, la reposición de credenciales perdidas), las tarifas deben ser razonables y proporcionales a los costos incurridos, además de ser transparentes para el público. Los costos indirectos para obtener una identificación —incluidos los cargos por documentos de apoyo, gastos de viaje y otros procedimientos administrativos complejos — deben ser mínimizados al máximo.

- *Disparidades informáticas y tecnológicas.* Las partes interesadas deben trabajar para garantizar que los usuarios conozcan los sistemas de identificación, a fin de fomentar una cultura de comprensión y confianza, y reducir las lagunas de información que podrían impedir que las personas accedan a los servicios o beneficios relacionados con la identidad. Dado el aumento de sistemas digitales, a nadie se le deben negar los servicios de identificación ni servicios conexos sólo porque carecen de conectividad a las TIC o conocimientos técnicos. Las partes interesadas deben trabajar juntas para garantizar que la infraestructura tanto en línea como fuera de ella pueda ampliarse y llegar hasta las zonas rurales más apartadas.[8]

8 Una de las consecuencias es que la identificación debe ser posible tanto en línea como fuera de línea.

PILAR B. DISEÑO: ESTABILIDAD, SEGURIDAD, CAPACIDAD DE RESPUESTA Y SOSTENIBILIDAD

Los sistemas de identificación deben ser sólidos, adecuados al entorno e interoperables. Si bien deben responder a la demanda de los usuarios y las necesidades a largo plazo, deben recopilar y utilizar únicamente la información necesaria para el propósito explícito del sistema. Los estándares abiertos y la neutralidad de los proveedores ayudan a asegurar la eficiencia y sostenibilidad financiera y operativa.

3. Establecimiento de una identidad única, segura y precisa desde el nacimiento hasta la muerte.

- *Robustez.* La información precisa y actualizada es esencial para la fiabilidad de cualquier base de datos y credenciales de identificación utilizados para la autenticación. Los sistemas de identificación deben proporcionar una identidad estadísticamente única[9] y verificable para toda la vida de una persona, desde el nacimiento hasta la muerte, con salvaguardias contra la manipulación (alteración u otros cambios no autorizados de datos o credenciales), robo de identidad y otros errores que ocurran durante el ciclo de vida de la identidad.

4. Creación de una plataforma que sea interoperable y que responda a las necesidades de los diversos usuarios.

- *Capacidad de respuesta.* Los proveedores de identificación deben esforzarse para asegurar que la identificación y servicios de autenticación sean flexibles, fáciles de extender, y su vez satisfagan las necesidades e inquietudes de los usuarios finales (particulares). También deben satisfacer las necesidades de organismos públicos y empresas privadas que utilizan o podrían utilizar esta identidad como base para otros servicios u operaciones.

---

9 Estadísticamente "única" significa que la probabilidad de que cualquier individuo pueda tener múltiples identidades en el mismo sistema (es decir, varias identidades) es muy baja, aunque ningún sistema es completamente infalible. Debe distinguirse de la posibilidad de que una persona pueda tener múltiples mecanismos para autenticar su identidad, como puede darse el caso en un sistema federado.

10 La interoperabilidad entre fronteras puede facilitar la migración y el comercio, pero deben existir controles para proteger la seguridad de los grupos vulnerables, como es el caso de los refugiados, cuyos datos personales a menudo deben ser protegidos del país de origen.

- *Interoperabilidad.* La interoperabilidad aumenta la eficiencia y permite que múltiples partes interesadas aprovechen las ventajas del sistema de identificación, tanto dentro de un país como entre países. En el plano nacional, esto incluye la habilidad de diferentes bases de datos o registros (por ejemplo, documentos nacionales de identidad y sistemas de registro civil) para comunicarse entre sí o intercambiar información en forma oportuna y a bajo costo, dotadas de las salvaguardias de privacidad y seguridad pertinentes.[10]

5. Uso de estándares abiertos y garantía de neutralidad tecnológica y de proveedores.

- *Estándares abiertos.* Los principios de diseño abierto propician la competencia de mercado y la innovación.[11] Son esenciales para una mayor eficiencia y una mejor funcionalidad de los sistemas, tanto dentro del país como a nivel internacional.

- *Neutralidad tecnológica y de proveedores.* Deben existir sólidas directrices en materia de adquisiciones de TIC a fin de facilitar la competencia y la innovación, y evitar la posible dependencia de un sólo proveedor y tecnología, lo cual podría traducirse en aumento de costos y menor flexibilidad para ajustarse a los cambios. Debe fomentarse la neutralidad y diversidad tecnológicas a fin de aumentar la flexibilidad y evitar diseños inadecuados para el propósito que se pretende o que no sea propicio para alcanzar los objetivos de política y desarrollo.

---

11 Por ejemplo, ISO/IEC han elaborado normas que abarcan muchos aspectos de los sistemas de identificación. Para más información, véase Banco Mundial, 2016. "Technical Standards for Digital Identity Systems: Formulating a Strategic Approach."

12 Las Directrices de Privacidad son un conjunto de principios reconocidos internacionalmente para la protección de la información personal, incluido el alcance de la recopilación, la especificación del propósito, la calidad de los datos, la seguridad, la responsabilidad y la transparencia.

13 Estas evaluaciones del impacto de riesgos deben ser llevadas cabo por la entidad responsable que crea, recopila, comparte o usa los datos para propósitos de autenticación e identificación vinculados a un uso específico. Algunos ejemplos de las normas vigentes para los niveles de fiabilidad para verificación de identidad incluyen la norma ISO/IEC 29115 y aquellas emitidas por eIDAS, el Cabinet Office del Reino Unido, NIST y otros.

14 La "información personal confidencial" puede variar según el contexto, pero generalmente incluye información que podría utilizarse para crear identidades fraudulentas y caracterizar o identificar a personas específicas. La divulgación de información de identificación puede implicar riesgos particularmente graves para ciertas personas, por ejemplo, los solicitantes de asilo y los refugiados.

6. Protección de la privacidad del usuario y control mediante el diseño de sistemas

- *Privacidad desde el diseño.* Los sistemas de identificación deben ser diseñados teniendo en cuenta la privacidad de los usuarios finales. La persona no debería tener que emprender ninguna acción para proteger sus datos personales. La información debe estar protegida contra cualquier uso indebido de manera predeterminada, tanto por normas técnicas como por prácticas comerciales preventivas.

- *Proporcionalidad y divulgación mínima.* Los datos recopilados y utilizados para identificación y autenticación deben ser aptos para el propósito y proporcionales a la situación, y gestionados de conformidad con las estándares internacionales para la protección de datos, como las Directrices de Privacidad[12]. Los protocolos de autenticación solo deben revelar la información mínima necesaria para garantizar los niveles adecuados de fiabilidad. Estos niveles deben reflejar una evaluación del nivel de riesgo en las transacciones y pueden basarse en normas internacionales reconocidas[13]. Los sistemas de identificación —incluidos los sistemas de numeración y credenciales— no deben revelar información personal confidencial.[14]

7. Planificación para la sostenibilidad financiera y operacional sin comprometer la accesibilidad.

- *Sostenibilidad.* Los sistemas de identificación deben ser diseñados de manera que aseguren su estabilidad a a largo plazo, tanto operativa como fiscal, sin comprometer la accesibilidad de los usuarios finales. Esta estabilidad se podría alcanzar mediante la aplicación de un modelos financiero adecuado que considere el cobro de honorarios razonables por determinados servicios relacionados con la verificación de identidad, incluyendo servicios adicionales o expeditos a los usuarios, alianzas público-privadas o fuentes adicionales de financiación. Asimismo el modelo financiero escogido debería tener en cuenta, criterios de eficiencia y reducción de filtraciones que conllevaran a una reducción de costos. Deben diseñarse modelos comerciales de sistemas de identificación a fin de incentivar altos niveles de fiabilidad para las todas partes de la cadena de valor.

PILAR C. GOBERNABILIDAD: FOMENTO DE LA CONFIANZA MEDIANTE PROTECCIÓN DE LA PRIVACIDAD Y DERECHOS DE LOS USUARIOS

Los sistemas de identificación deben, desde el punto de vista jurídico y operacional, basarse en la confianza y la rendición de cuentas entre entidades públicas, organismos internacionales, el sector privado y particulares. Los individuos deben sentirse seguros de la privacidad y la protección de sus datos, la capacidad de controlar y vigilar su uso, los procesos de supervisión independiente y la reparación de daños.

8. Salvaguarda de la privacidad de los datos, la seguridad y los derechos de las personas naturales a través de un marco jurídico y normativo amplio.

- *Marcos jurídicos y normativos.* Los sistemas de identificación deben estar respaldados por marcos jurídicos y normativos y por sólidas políticas que promuevan la confianza en el sistema, garanticen la privacidad y la seguridad de los datos, mitiguen los abusos, como la vigilancia no autorizada en violación de las leyes, y garanticen que el proveedor asuma su responsabilidad. Los marcos jurídicos deben delinear claramente las responsabilidades y los recursos a disposición de los usuarios finales, y deben ser supervisados por organismos regulatorios independientes con las facultades apropiadas. También deben proteger a los particulares contra el acceso indebido y el uso de sus datos por parte de terceros para la elaboración de perfiles o monitoreo de hábitos de compras no autorizados por la legislación vigente. El marco normativo deberá equilibrar el marco regulatorio con los modelos de autoconducta para que no supongan un obstáculo a la libre competencia, la innovación o la inversión.

- *Derechos de las personas naturales.* Los servicios de identificación deben proporcionar a los usuarios particulares una genuina opción y control sobre el uso de sus datos, incluida la capacidad para divulgar selectivamente sólo aquellos atributos que sean necesarios para una determinada operación. Los usuarios deben contar con medios sencillos para corregir, de forma gratuita, los datos inexactos y obtener una copia de la información personal que se tiene sobre ellos. No debería haber segundas intenciones ni propósitos velados en el uso de la información personal sin el consentimiento informado del usuario a menos que así lo exija la ley. Las partes interesadas deben obrar con transparencia en la gestión de la identidad,

desarrollar los recursos adecuados para que los usuarios estén mejor enterados de cómo se usan sus datos y darles herramientas para gestionar su privacidad. Los proveedores de identificación deben facilitar un proceso administrativo y no judicial para corregir errores a fin de acelerar su resolución y reducir los costos. Los convenios para el intercambio de datos también deben ser transparentes, estar plenamente documentados y ser firmados solo si son en beneficio de los intereses de la persona afectada.

9. Establecimiento de mandatos institucionales claros y rendición de cuentas.

- *Mandatos institucionales.* Para asegurar confianza en el medio, se debe establecer y regular los marcos de gobernabilidad para los sistemas de identificación. En este contexto, deberían abarcarse las especificaciones de los términos y condiciones que rigen las relaciones institucionales entre los participantes, de modo que los derechos y las responsabilidades de cada uno sean claros para todos.

- *Rendición de cuentas.* Es importante que exista transparencia asi como un sistema de redición de cuentas respecto a las responsabilidades asi como al papel que desempeñan los provedores de sistemas de identificación.

10. Aplicación de los marcos jurídicos y de confianza con vigilancia independiente y resolución de quejas.

- *Supervisión.* El uso de sistemas de identificación debe ser vigilado de manera independiente (en cuanto a su eficiencia, transparencia, exclusión, abuso, etc.) a fin de asegurar que todos los interesados los utilicen adecuadamente para cumplir sus propósitos, supervisar y responder a posibles filtraciones de datos, y atiendan denuncias individuales o inquietudes por el manejo de los datos personales.
- *Arbitraje.* Las controversias acerca de la identificación y el uso de datos personales que no sean resueltas satisfactoriamente por los proveedores (por ejemplo, el negar el registro de una persona o corregir datos, o una determinación desfavorable para la condición jurídica de una persona) deben ser objeto de una revisión rápida y asequible por vía administrativa a cargo de una autoridad independiente o bien por via judicial con capacidad suficientre para otorgar el resarcimiento del daño a la persona afectada.

Photo Credits | Cover Top: UN Women/Fatma Elzahraa Yassin; Page 7: UNICEF/BANA2012-02020/Jannatul Mawa; Page 15: UN Media/Jashim Salam; Page 11: Sébastien Rieussec/Safran

ENDORSING ORGANIZATIONS

We welcome additional organizations to join us in endorsing these Principles and hope to maintain this as a living document to be updated based on lessons of experience.

February 2017