# MODELO DE MADUREZ DE SISTEMAS DE IDENTIFICACIÓN

## Guía de aplicación


**Autores**

Arturo Muente Kunigami
José Luis Hernández Carrión
Cecilia Fernández
Natalia Bottaioli
Javier Preciozzi


BID

Modelo elaborado con el apoyo del equipo de Everis NTT DATA y NATHAN liderado por Cecilia Fernández en 2018, y actualizado en 2024 por Natalia Bottaioli y Javier Preciozzi, con la colaboración de Fabricio Rodríguez Yánez.

**Códigos JEL:** H11, O21, O33

**Palabras clave:** sistemas de identificación, identidad, identidad digital, datos, gobierno




Banco Interamericano de Desarrollo
1300 New York Avenue, N.W.
Washington, D.C. 20577
**www.iadb.org**

El Sector de Instituciones para el Desarrollo fue responsable de la producción de la publicación.

**Colaboradores externos**

Coordinación de la producción editorial: Sarah Schineller (A&S Information Partners, LLC)

**Revisión editorial:** Clara Sarcone
**Diseño y diagramación:** .Puntoaparte Editores

# Resumen

El Modelo de Madurez de los Sistemas de Identificación es una herramienta impulsada por el Banco Interamericano de Desarrollo (BID) con el objetivo de comprender los aspectos clave para evaluar la madurez de los sistemas de identificación en los países de América Latina y el Caribe (ALC). Para ello, el modelo se basa en un análisis exhaustivo de los sistemas de identificación más avanzados a nivel global, a fin de identificar las dimensiones e indicadores más relevantes para caracterizar los elementos que determinan el grado de desarrollo de un sistema de identificación.

El modelo se estructura en torno a 6 dimensiones y 16 indicadores que abarcan tanto los aspectos relacionados con la definición de directrices, regulación y planificación del sistema, como aquellos vinculados a la ejecución de los procedimientos del ciclo de vida de la gestión de la identidad, es decir, registro, emisión, uso y actualización.

En definitiva, este modelo busca ser una guía práctica para la región, al proporcionar una ruta estratégica clara para la modernización de los sistemas de identificación, permitir una evaluación precisa del nivel de desarrollo en las áreas más importantes que los caracterizan y proponer los pasos a alcanzar para mejorar estos sistemas.

# Índice

# Listado de siglas

| | |
|---|---|
| **ALC** | América Latina y el Caribe |
| **BID** | Banco Interamericano de Desarrollo |
| **CRVS** | Registro civil y estadísticas vitales (siglas en inglés) |
| **CSP** | Proveedor de servicios de credenciales (siglas en inglés) |
| **DNI** | Documento nacional de identificación |
| **eIDAS** | Identificación electrónica, autenticación y servicios de confianza (siglas en inglés) |
| **eSENS** | Electronic Simple European Networked Services |
| **FIPS** | Federal Information Processing Standards |
| **GSMA** | Global System for Mobile Communications |
| **ICAO** | Organización de Aviación Civil Internacional (siglas en inglés) |
| **ID** | Identificación |
| **ID4D** | Identificación para el Desarrollo (siglas en inglés). Iniciativa del Banco Mundial |
| **IdP** | Proveedor de identidad |
| **IEC** | Comisión Electrotécnica Internacional (siglas en inglés) |
| **ISO** | Organización Internacional de Normalización (siglas en inglés) |
| **MRTD** | Machine Readable Travel Documents |
| **NIST** | Instituto Nacional de Estándares y Tecnología (siglas en inglés) |
| **PII** | Información de identificación personal (siglas en inglés) |
| **PKI** | Infraestructura de llave pública (siglas en inglés) |
| **PVC** | Policloruro de vinilo (siglas en inglés) |
| **RENIEC** | Registro Nacional de Identificación y Estado Civil |
| **RGPD** | Reglamento General de Protección de Datos |
| **STORK** | Identidades seguras enlazadas a través de fronteras (siglas en inglés) |
| **UE** | Unión Europea |
| **UIN** | Número único de identificación (siglas en inglés) |

# Resumen metodológico

El proyecto Simplificando Vidas a través de la Identidad Digital fue una iniciativa ejecutada por el Banco Interamericano de Desarrollo (BID, 2017) con el objetivo de servir de soporte a las agencias de registro de identidad y/o gobierno digital para desarrollar una estrategia integral y multisectorial que incluya la identidad digital.[1]

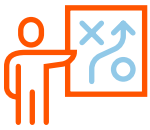
Esta iniciativa se fundamenta en la relación que existe entre la estimulación del desarrollo y la calidad de los sistemas de identificación de los países. El diseño o mejora de estos sistemas de identificación plantea una serie de desafíos complejos para los países que se encuentran iniciando esfuerzos para transformar estos sistemas.

Bajo el marco de este proyecto, este modelo busca comprender los ámbitos relevantes para determinar la madurez de los sistemas de identificación de los países, con el fin de encontrar cuáles son los principales ámbitos de mejora según su nivel de madurez. Esto se sostiene en la determinación de las variables que generen impacto económico a partir de la implantación de iniciativas asociadas a la mejora de los sistemas de identificación.

**Esta publicación desarrolla el enfoque metodológico utilizado para la definición del Modelo de Madurez, que se basa en:**

1. Análisis de experiencias de relevancia.

2. Determinación de los principios que rigen la visualización de un sistema de identidad robusto, aplicable e inclusivo.



3. Identificación de los componentes del modelo que permiten establecer las dimensiones e indicadores que serán materia de una evaluación integral del ecosistema.

4. Calibración/ponderación de las dimensiones respecto a los principios rectores y de las experiencias recogidas en los países de referencia.

1. Para conocer más del proyecto, visítese: **https://www.iadb.org/es/proyecto/RG-T3070**

1 2 3 4

1

# INTRODUCCIÓN

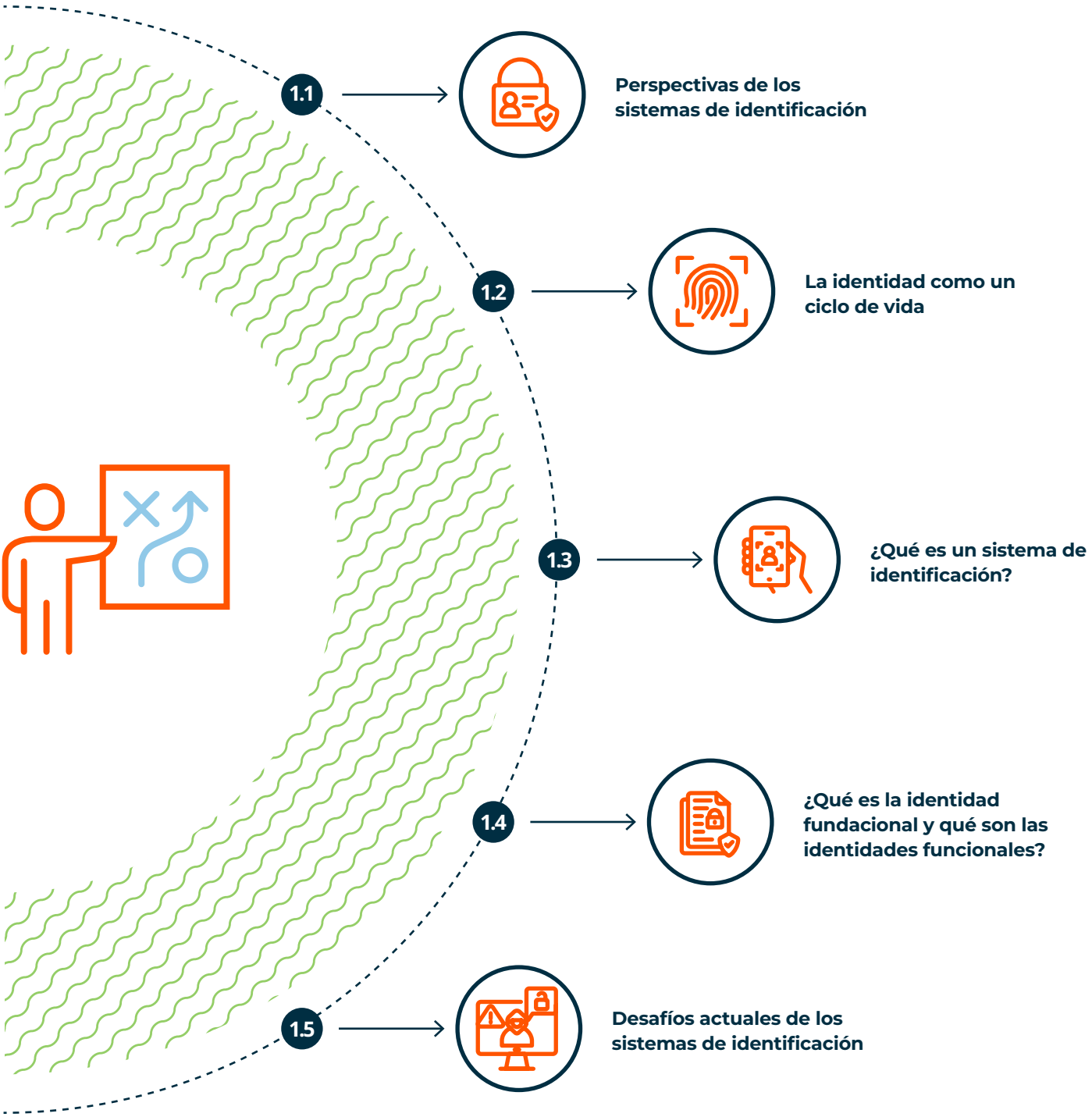
1 2 3 4

El concepto de **identidad** refiere al conjunto de información que caracteriza y reconoce a una persona en un determinado ecosistema; alrededor del concepto de identidad existe una serie de atributos que acompañan su definición. Uno de los desafíos más importantes de los sistemas de identificación es lograr que la totalidad de los ciudadanos se encuentren debidamente identificados por las administraciones de sus países.

A partir de la información disponible, se estima que hasta 2018 existían 1.100 millones de personas en el mundo que no contaban con un documento oficial para autentificar su identidad (Bujoreanu, Mittal y Noor, 2018).

Asociado a ello, el desafío de la cobertura ha sido la principal problemática hasta el momento. Sin embargo, el concepto de identidad ha evolucionado a una complejidad mayor en la que la autenticación de la identidad necesita de mecanismos robustos que permitan un espectro más amplio de uso por parte del ciudadano, así como una mejor experiencia del usuario final. Es así que se requiere de una visión holística que permita observar de manera global los ámbitos relevantes en la madurez de un sistema de identidad.

**El presente apartado busca determinar las premisas y conceptos de análisis sobre los cuales se cimienta esta publicación. Para ello, se desarrollarán los siguientes puntos:**



# 1.1. PERSPECTIVAS DE LOS SISTEMAS DE IDENTIFICACIÓN

Históricamente, identificar a una persona estuvo asociado a círculos específicos de la sociedad civil; por ejemplo, hace algunas décadas, las iglesias registraban datos biográficos y personales en el momento de brindar sacramentos a sus feligreses.

Dados los esfuerzos en el fortalecimiento institucional del Estado como garante principal de la gobernabilidad y formulador de políticas públicas, se establece la necesidad de cuantificar y cualificar a los ciudadanos de sus territorios, de manera exacta, confiable y actualizada. Del mismo modo, terceras partes involucradas entran en la ecuación y revelan la necesidad de establecer la veracidad de la identidad de una persona en el momento de realizar una transacción. Finalmente, el ciudadano también necesita acceder a bienes y servicios públicos y privados a través de la certificación de su entidad.

En ese sentido, a continuación, se describen tres ejes fundamentales sobre los cuales se ha dado el desarrollo de los sistemas de identificación:

- La identidad como **derecho fundamental**.
- La identidad como un **habilitador para el acceso a servicios**.
- La identidad en la **agenda pública actual**.

## La identidad como un derecho fundamental

La conceptualización de la identidad como un derecho fundamental obliga a los Estados a brindar un mecanismo de identificación a sus ciudadanos. Este derecho ha sido mencionado en diferentes acuerdos internacionales, los cuales buscan que los gobiernos realicen esfuerzos para cerrar las brechas de identificación que tienen en sus países. En este ámbito, se destacan dos acuerdos que se presentan a continuación.

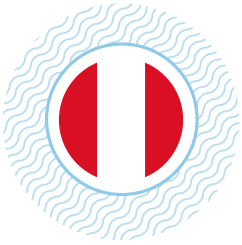
La **Declaración Universal de Derechos Humanos** (DUDH), promovida por la Asamblea Nacional de las Naciones Unidas, menciona como uno de los derechos fundamentales de la persona que **“todo ser humano tiene derecho, en todas partes, al reconocimiento de personalidad jurídica”** (Asamblea General de las Naciones Unidas, 2015).

Esta Carta Internacional ha servido como piedra angular de muchas iniciativas internacionales respecto a los derechos fundamentales de la persona, e incluso se ha adoptado en las políticas internas de los países firmantes.

**Objetivos de Desarrollo Sostenible** (ODS) 2015.[2] En 2015 diferentes países adoptaron la Agenda 2030 para el Desarrollo Sostenible y sus 17 ODS, en ámbitos como la reducción de la pobreza, educación de calidad, agua y saneamiento, entre otros.

En el ámbito de la identidad, la dimensión de Paz, Justicia e Instituciones determina la meta 16.9 en la que se menciona: "de aquí a 2030, proporcionar acceso a una identidad jurídica para todos, en particular mediante el registro de nacimientos".

Como se mencionó anteriormente, estos lineamientos fueron adoptados en la política interna de los países miembros, por lo que se contempla el otorgamiento a la identidad, como derecho fundamental del ciudadano y deber obligatorio del Estado, en las constituciones políticas. A continuación, se presentan dos ejemplos de su adopción.



***Perú:*** *"Artículo 2: A la vida, a su identidad, a su integridad moral, psíquica y física y a su libre desarrollo y bienestar. El concebido es sujeto de derecho en todo cuanto le favorece. [...]" (República Constitucional del Perú, 1993).*

***Estados Unidos Mexicanos:*** *"Artículo 4: [...] Toda persona tiene derecho a la identidad y a ser registrado de manera inmediata a su nacimiento. El Estado garantizará el cumplimiento de estos derechos. La autoridad competente expedirá gratuitamente la primera copia certificada del acta de registro de nacimiento. [...]" (Estados Unidos Mexicanos, 1917).*

## La identidad como un habilitador para el acceso a servicios

La identidad se constituye como un eje fundamental para garantizar el acceso a servicios, tanto del ámbito público como del ámbito privado. En el primer caso, el Estado, garante de la gobernabilidad y provisión de bienes y servicios públicos, necesita conocer y entender la cantidad y las características de su población para realizar estas funciones de manera eficiente. Respecto al ámbito privado cuyas actividades u operaciones se relacionan directamente con la identificación de una persona, se considera necesario que las verificaciones de los mecanismos de identificación tengan altos niveles de confiabilidad.

2. En 2015, 193 líderes mundiales establecieron y acordaron el cumplimiento de 17 ODS para los siguientes 15 años.

- En el **ámbito público** la identidad se vincula a la **gobernabilidad** y al **diseño e implementación de políticas y servicios públicos**. El Estado necesita conocer y entender a sus ciudadanos (cantidad, distribución geográfica, perfil, etc.) para estimar la capacidad y alcance del Estado y definir y priorizar políticas y servicios públicos de manera eficiente. Además, la identidad es un habilitador para los ciudadanos, ya que les permite acceder de manera formal a políticas y servicios públicos que otorga el Estado.

- En el **ámbito privado** las operaciones de negocio se relacionan directamente con la identidad de sus clientes, por lo que se requiere un nivel alto de confiabilidad y exactitud de esta información a fin de garantizar las políticas de calidad y fiabilidad de las operaciones. Es así que las entidades financieras, aseguradoras, de salud, de educación, entre otras, buscan acceder a servicios de autenticación o verificación de la identidad de sus clientes. De esta manera, una entidad certificadora externa puede brindarles esa exactitud y, además, disminuir el costo de generar una identidad particular funcional, para la que necesitarían costear plataformas tecnológicas, ampliar plazos de sus trámites, costos de oportunidad, etc.

En conclusión, la identidad funciona como un medio para garantizar un fin, que es el habilitar el acceso a servicios públicos y privados a través de la autenticación. Como parte del ciclo de la gestión de la identidad, la autenticación es el proceso que mide el nivel de adopción del mecanismo de identificación del sistema: cuantos más ámbitos haya en los que se pueda autenticar el mecanismo de identificación, más robusto será el sistema de identidad en general.

## La identidad en la agenda pública actual

Dada la importancia de la identidad de los ciudadanos, debido a su condición de habilitador para el acceso a servicios, existen múltiples esfuerzos en la agenda pública cuyo objetivo es consolidar no solo las tareas que robustecen la generación de la identidad, sino también las que la vinculan con iniciativas, tales como la digitalización de trámites, firma electrónica, entre otros. El principal ámbito en el que la identidad está cobrando mayor importancia es en el de gobierno electrónico, debido a la condición de acceso que tiene la identidad para realizar la solicitud de un bien o servicio público, digitalización del aparato burocrático, reducción de papel, entre otros.

La tendencia de los programas de gobierno electrónico es digitalizar las operaciones *front* y *back* a través de las tecnologías de información y las comunicaciones (TIC). Para lograrlo, es necesario aumentar los atributos digitales en la ejecución de los procesos. La identidad, al ser el habilitador que permite el acceso a estos servicios, no es la excepción.

# 1.2. LA IDENTIDAD COMO UN CICLO DE VIDA

La identidad de una persona se compone del conjunto de atributos que permiten identificar a un ciudadano y caracterizarlo con información personal e intransferible, como datos biográficos, códigos únicos de identificación, datos biométricos, entre otros.

Si bien usualmente una persona certifica su identidad a través de un elemento o mecanismo portable que la garantice, la identidad de la persona es un atributo intangible que se representa o expresa a través de un mecanismo de identificación, según las políticas y procedimientos del país en donde la persona nació o reside. La gestión de la identidad puede representarse a través de un ciclo de vida, que inicia en el primer momento de registro, culmina en las transacciones de uso y autenticación y se retroalimenta en la actualización de la información disponible.

Como el Modelo de Madurez requiere claridad, es muy importante formalizar la terminología empleada para designar las distintas fases y procesos. Si bien existen algunas referencias que pueden usarse como base, ninguna de ellas es completamente satisfactoria:

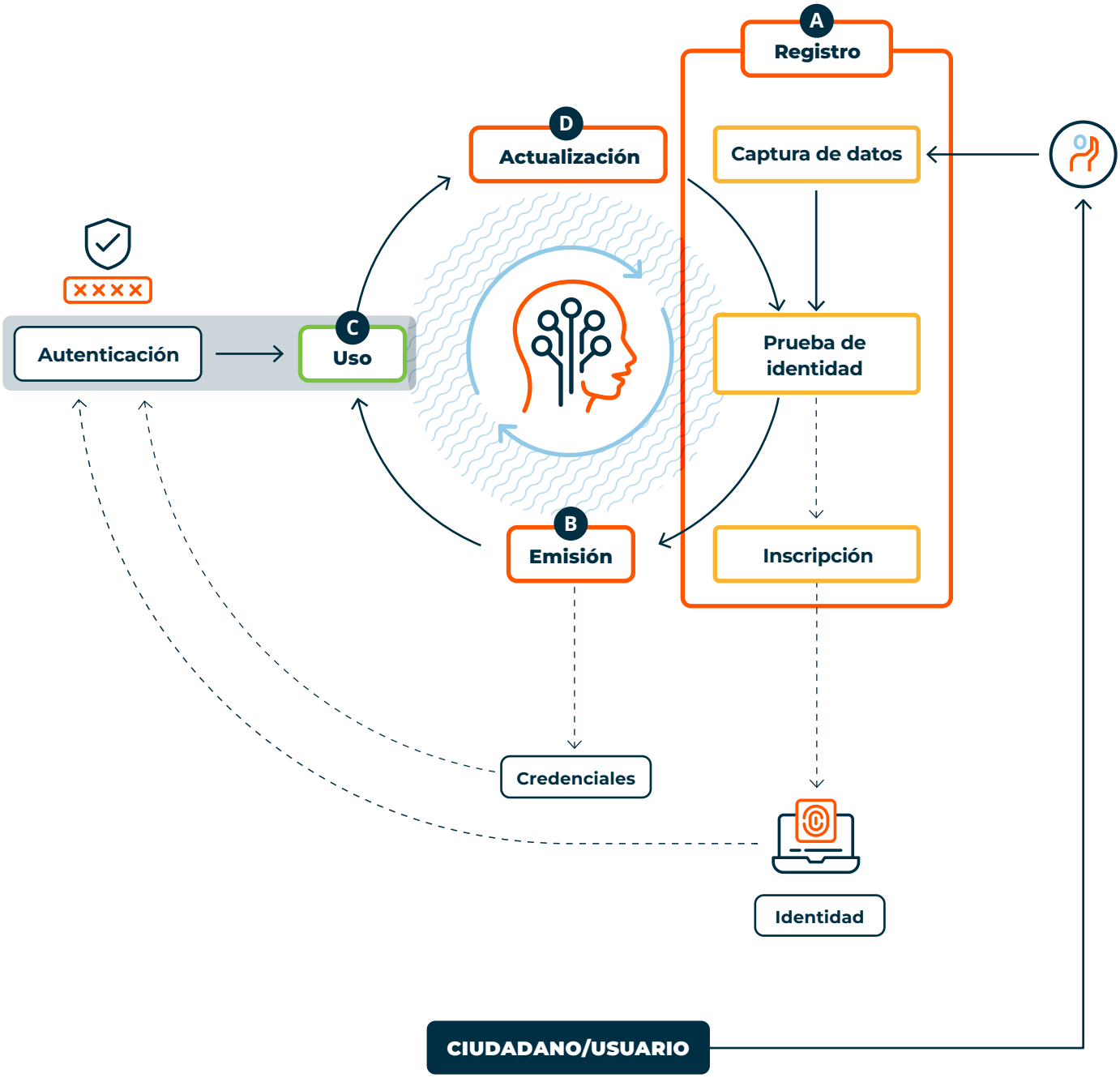
- **World Bank ID4D Practitioner's guide:** tiene un ciclo de vida claro, pero no existe una traducción al español. Esto hace que el término traducido dependa de quién lo interprete al español.

- **ISO/IEC 29115-1:** se trata de un documento en inglés, que además es más general de lo necesario para un sistema de identidad nacional ya que describe un *Entity authentication assurance framework* genérico.

En un intento por evitar ambigüedades, a continuación se presenta el ciclo de vida que se utilizará a lo largo de esta publicación (fuertemente inspirado en la identificación electrónica, autenticación y servicios de confianza [eIDAS, por sus siglas en inglés] y la ISO/IEC 29115-1) junto con una formalización de los principales términos utilizados.

El ciclo de vida de la gestión de la identidad puede describirse en cuatro fases principales (Gráfico 1.1).

**Gráfico 1.1.**
Ciclo de vida de la gestión de identidad



A

## Primera fase: registro

En esta fase se realiza la captura de toda la información requerida para acreditar y reconocer la identidad de una persona como única e intransferible. Usualmente, este tipo de información se compone de datos biográficos, como nombre, fecha de nacimiento y género, y de datos biométricos, como huella dactilar, fotografía del rostro o escaneo de iris. Esta fase consta generalmente de los siguientes procesos:

- **Captura de datos:** es el primer proceso en el ciclo de vida. En este momento se realiza la captura de los datos que permitirán acreditar y reconocer una identidad como única e intransferible.

- **Prueba de identidad:** son las acciones que permiten la validación de los datos recopilados durante el proceso de captura de datos. Este proceso incluye usualmente los siguientes subprocesos:

  - → **Validación:** es el proceso por el cual la información presentada durante la fase de captura de datos es validada, lo que permite determinar la completitud, veracidad y autenticidad de la misma.

  - → **Deduplicación:** es el proceso que garantiza la unicidad del registro en la base de datos, mediante la búsqueda de registros similares. Esta deduplicación puede ser biográfica (por ejemplo, verificar que no existan dos personas registradas con la misma acta de nacimiento), aunque generalmente incluye la deduplicación biométrica (por ejemplo, comprobar que no haya dos personas con las mismas huellas dactilares registradas).

  - → **Verificación:** dependiendo de las características del sistema, el proceso de prueba de identidad puede incluir un paso adicional de verificación, donde se compara la información obtenida durante la captura de datos contra datos previamente capturados (en otro sistema).

- **Inscripción:** es el proceso mediante el cual la identidad es finalmente creada en el sistema. En general, consta de la generación de un número único de identidad y de la creación de los registros correspondientes en la base de datos de identidad nacional.

B

## Segunda fase: emisión

Existen múltiples **mecanismos de identificación**, **físicos** y **digitales**. Las versiones físicas de los mecanismos de identificación son generalmente tarjetas (de policarbonato, policloruro de vinilo [PVC] o Teslin) en las que se registran los datos capturados, registrados y validados, cuyos mecanismos de autenticación pueden ser códigos de barra, código de identificación y datos biográficos. Actualmente, la tendencia digital es emitir una tarjeta con chip que contiene tanto la información del titular como el certificado de firma electrónica que mejora la seguridad de la información almacenada.

C

## Tercera fase: uso

Se trata de las transacciones de autenticación que se pueden realizar con el fin de acceder al consumo de bienes y servicios tanto del ámbito público como del privado. El nivel de adopción del mecanismo de identificación emitido dependerá de los mecanismos sistémicos de interoperabilidad que permitirán autenticar la identidad. En la medida en que existan menores niveles de interoperabilidad, el uso tenderá a ser reducido también.

D

## Cuarta fase: actualización

Todo registro de identidad requiere ser actualizado cada cierto tiempo (muchas veces definido por ley), lo cual en general está asociado a la emisión de una nueva credencial. Durante esta actualización es usual realizar una nueva captura de la información biométrica, que se utiliza tanto para garantizar la identidad de la persona como para actualizar los datos biométricos almacenados.

Es frecuente pensar que la relevancia de la identidad se debe centrar únicamente en la fase de registro y en la de emisión de credenciales. Por ese motivo, las administraciones públicas se han enfocado principalmente en mejorar los procesos de las fases de registro y emisión, motivados por el objetivo principal de que el 100% de sus poblaciones se encuentren identificadas. No obstante, como ya se mencionó, la identidad es un medio habilitador para el acceso a servicios; por lo tanto, el círculo solo se completa cuando se adopta el mecanismo de identificación emitido, es decir, cuando se utiliza para acceder a servicios de ámbitos públicos y/o privados.

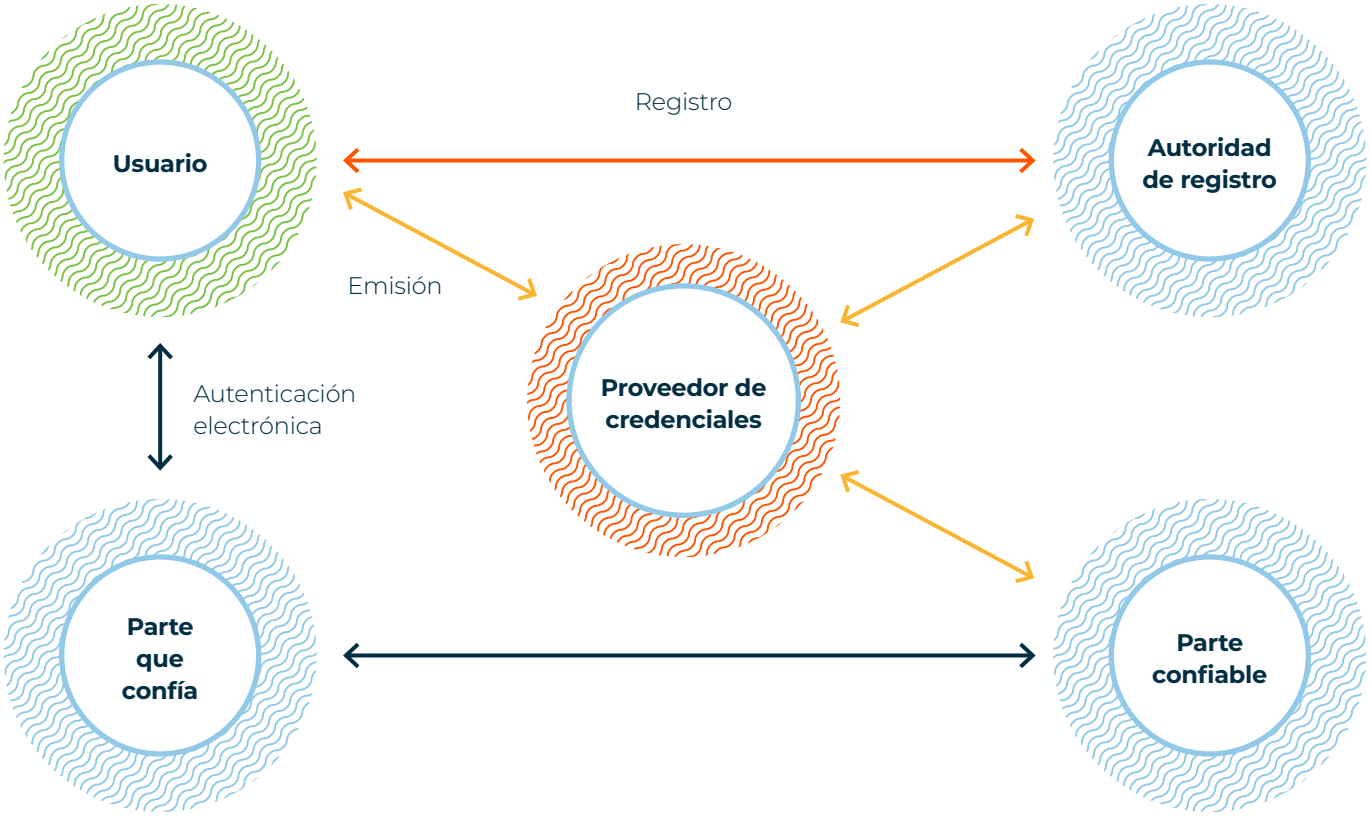
En ese sentido, la hipótesis central de esta publicación es que mientras un ciudadano utilice en más ámbitos su identidad, esta se robustece más, debido a que se recopila una mayor cantidad de datos funcionales que complementan la identidad de un ciudadano. El sistema de identidad más desarrollado será el que le permita al ciudadano autenticar su identidad en distintos ámbitos del sector público y privado, accediendo por más canales digitales y de forma más autogestionada.

En este punto se requiere conceptualizar el desafío de una manera más global y macro, introduciendo factores más amplios como el interinstitucional y el tecnológico, entre otros. Para ello, además del concepto de la identidad como un ciclo de vida, se plantean dos modelos de análisis complementarios con los que se asegura cubrir todos los aspectos importantes en cualquier sistema de identidad de cualquier país. Estos dos modelos son:

- La identidad concebida como un sistema.
- El vínculo de la identidad fundacional con las identidades funcionales.

Otro elemento relevante a considerar en el ciclo de vida de la identidad son los distintos actores o participantes que pueden formar parte del mismo. El estándar ISO/IEC 29115 define formalmente a dichos actores. El Gráfico 1.2 está basado en dicho estándar.

**Gráfico 1.2.**
Actores vinculados al ciclo de vida de la gestión de la identidad




- **Usuario (definido en el estándar como entidad):** algo que tiene una existencia separada y distinta y que puede ser identificado en un contexto.
- **Parte que confía (en el estándar es la *Relying Party*):** actor que depende de una aseveración o declaración de identidad.
- **Autoridad de registro:** actor de confianza que establece y/o verifica y garantiza la identidad de una entidad ante un proveedor de credenciales.
- **Proveedor de servicios de credenciales:** actor de confianza que emite y/o gestiona credenciales. El proveedor de servicios de credenciales (CSP, por sus siglas en inglés) puede abarcar autoridades de registro y verificadores. Un CSP puede ser una tercera parte independiente, o puede emitir credenciales para su propio uso.
- **Parte confiable:** autoridad en quien otros actores confían en lo que respecta a actividades relacionadas con la seguridad. Se trata de una tercera parte de confianza en la que una entidad y/o un verificador confía con fines de autenticación.

En sistemas de identificación centralizados es usual que la autoridad de registro sea también la proveedora de (servicios de) credenciales y la parte confiable en términos de identidad. Sin embargo, puede haber esquemas mixtos. A modo de ejemplo, Uruguay tiene varios actores dentro del mismo organismo (la Dirección Nacional de Identificación Civil): la autoridad de registro es también quien emite el documento de identidad (por lo tanto, es proveedor de credenciales) y además es parte confiable (porque provee servicios para validar la identidad). Sin embargo, en Uruguay existen otras credenciales adicionales relacionadas a la identidad digital (Mobile ID) que son administradas por proveedores privados de credenciales.

Debido a la importancia de la fase de registro, y en particular del proceso de prueba de identidad, en lo que sigue de esta publicación **el proceso de prueba de identidad se considera de forma particular, separado del proceso de registro.** En adelante, al aludir al ciclo de vida, se hará referencia a estas cinco fases: **registro, prueba de identidad, emisión, uso y actualización,** como cadena de actividades relevantes para la gestión de la identidad.

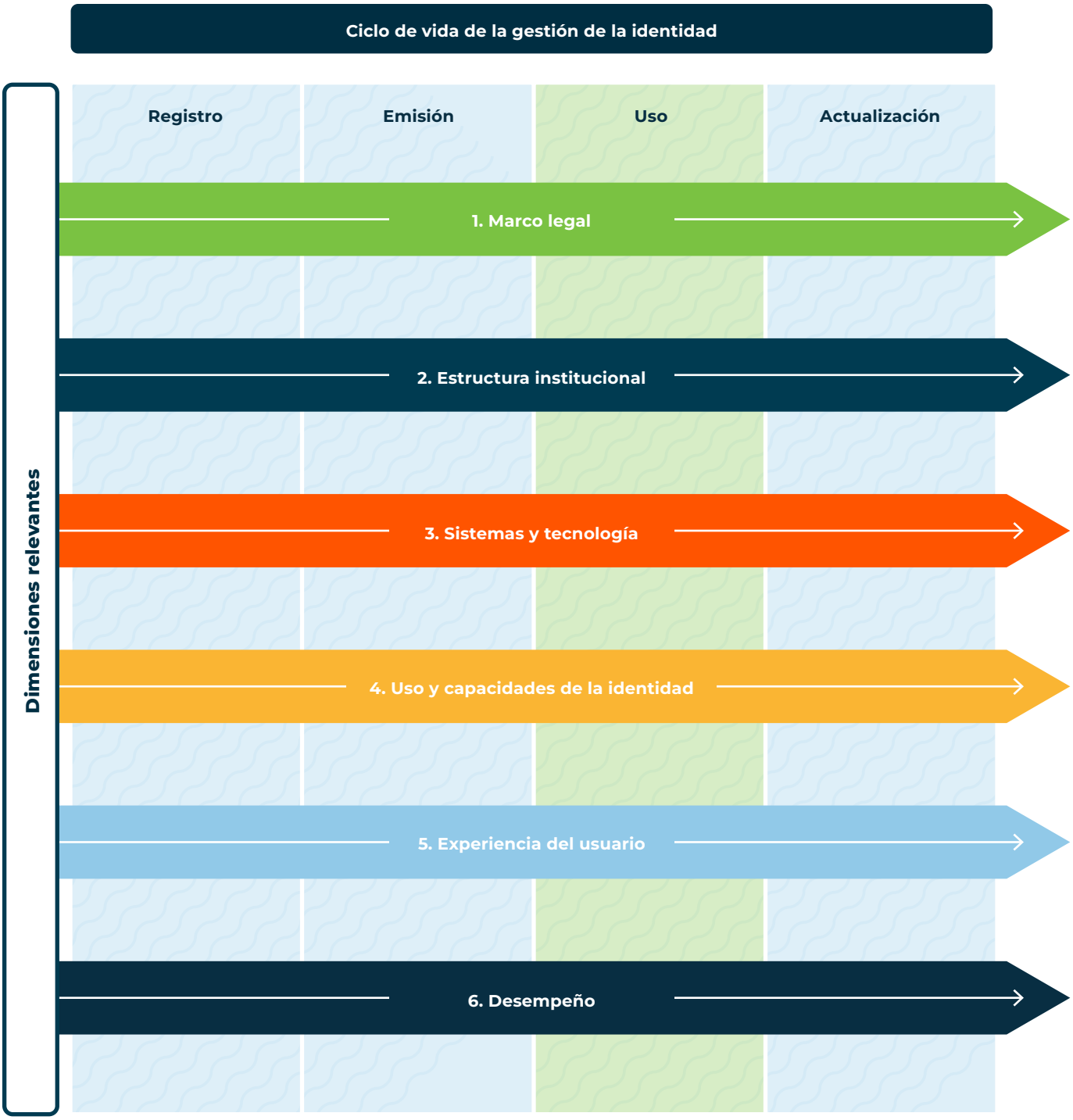
# 1.3. ¿QUÉ ES UN SISTEMA DE IDENTIDAD?

Como se mencionó, esta publicación busca analizar los ámbitos relevantes de un sistema de identidad, es decir, los mecanismos y/o ámbitos que permiten el diseño, planificación, operación y medición de los procesos que componen la gestión de la identidad. Por ejemplo, ¿cuáles son las normativas pertinentes que regulan los procesos de registro, prueba de identidad, emisión, uso y actualización? A nivel general, esta pregunta se asocia a los tipos de normativas y lineamientos técnicos que determinan la forma en que se ejecutarán estos procesos. Este aspecto sería el del marco normativo alrededor de la gestión de la identidad.

La perspectiva del ciudadano, como usuario principal de la gestión de la identidad, es pieza clave en la selección de ámbitos relacionados con la identidad. Por ello, es importante incluir tópicos relativos a la experiencia, uso y capacidades, ya que estos permitirán conocer el nivel de adopción de los mecanismos de identificación brindados.

Tal como se observa en el Gráfico 1.3, cada uno de los procesos de la gestión de la identidad se relaciona con uno de los ámbitos de un sistema de identidad. Allí se pueden visualizar los aspectos más relevantes de cualquier sistema de identidad de cualquier país.

**Gráfico 1.3.**
Dimensiones relevantes en el sistema de identidad



# 1.4. ¿QUÉ ES LA IDENTIDAD FUNDACIONAL Y QUÉ SON LAS IDENTIDADES FUNCIONALES?

Dentro de los sistemas de identificación de los países, la identidad fundacional convive con identidades funcionales, relacionando los datos de identificación de una persona con los distintos atributos funcionales que la persona va asumiendo a lo largo de su vida. A continuación, se muestran los conceptos y las diferencias entre ambas.

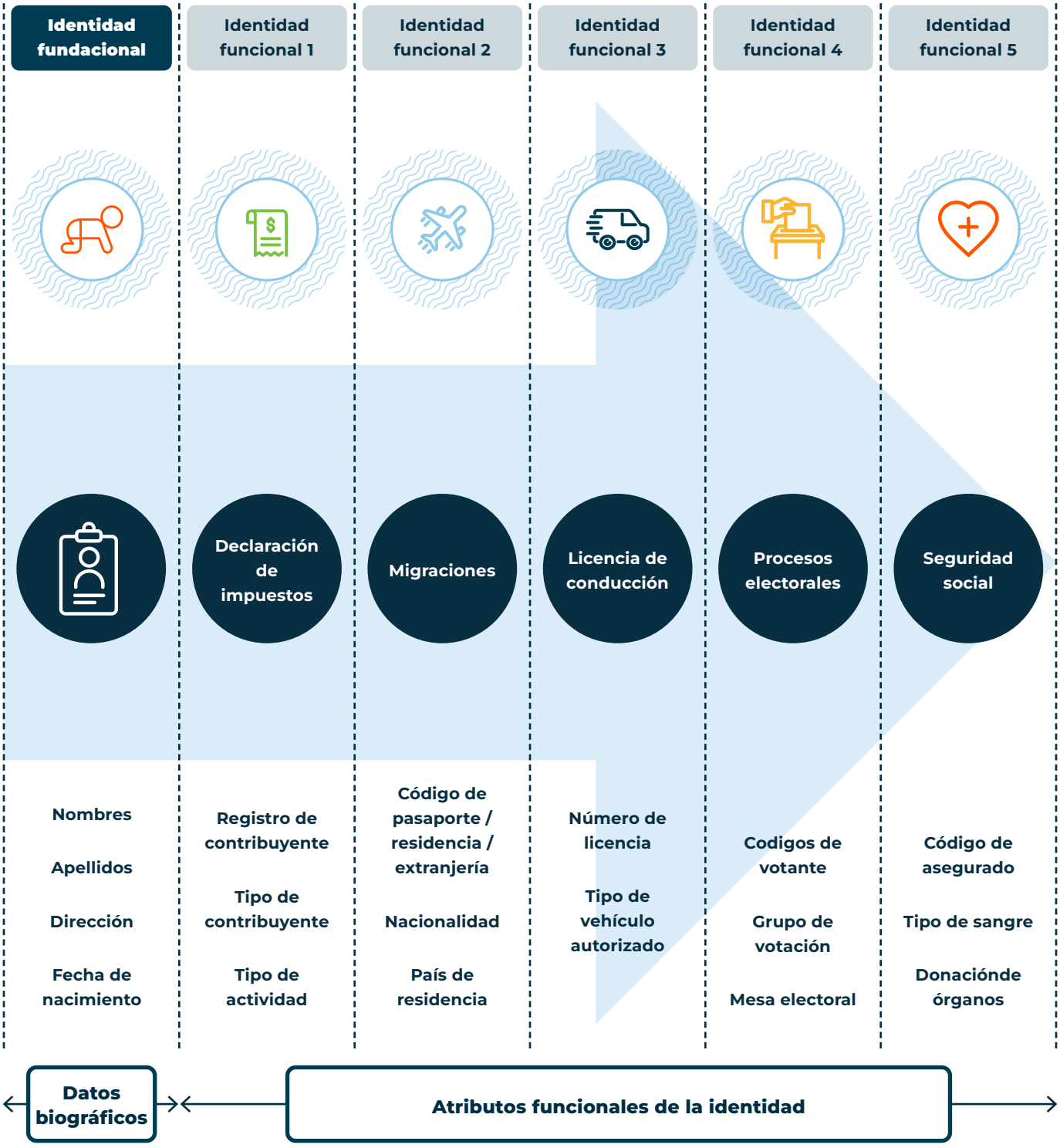
**Identidad fundacional:** es la identidad primigenia que los organismos certificadores otorgan a un ciudadano. Tiene como objetivo principal la identificación de un ciudadano, prevalece a nivel nacional y es reconocida tanto en el ámbito público como en el privado. Dependiendo de la madurez del sistema, la identidad fundacional estará fuertemente vinculada con la identidad registrada desde que un niño es certificado como nacido vivo. El ciclo común de la generación de la identidad es el siguiente: al nacer, se otorga un certificado de nacido vivo, se registran los datos biográficos del recién nacido en el registro civil, en un documento conocido como acta de nacimiento, y se obtiene una partida de nacimiento. A lo largo de su niñez, la persona puede recibir un documento de identidad que lo vincula a sus padres, y cuando la persona cumple la mayoría de edad (regulada por cada país) se acerca a una entidad de registro y solicita su documento de identidad de adulto. La identidad fundacional en muchos países está más relacionada con los procesos de registro, prueba de identidad y emisión. Por ejemplo, el documento nacional de identificación (DNI) de países como Argentina, Chile, Perú, etc. representa las identidades fundacionales de los ciudadanos de dichos países.

**Identidades funcionales:** son las identidades que los distintos sectores de los ámbitos público y privado crean para dar acceso a un bien o servicio. Las identidades funcionales pueden estar vinculadas a la identidad fundacional o no. Esto dependerá de la madurez institucional y tecnológica del sistema. Por ejemplo, una identidad funcional sería el código de tributación o seguridad social que permiten el pago de impuestos o la atención hospitalaria. La mayoría de los países que tienen una identidad fundacional incluyen el número único identificador en el código funcional creado. Las identidades funcionales están más relacionadas a los procesos de uso y autenticación.

Cuando la identidad fundacional no se encuentra vinculada con las identidades funcionales, el sistema de identidad está formado por islas, lo que genera que el ciudadano tenga múltiples credenciales de identificación. Por el contrario, cuando los niveles de interoperabilidad son altos, la identidad fundacional se vincula de forma directa con las identidades funcionales. Así, con la primera, el ciudadano accede a muchos servicios con el mismo mecanismo de identificación; por ejemplo, las tarjetas de seguridad social, licencia de conducir y las de declaración de impuestos son ámbitos en los que el ciudadano necesita utilizar su identidad, autenticándola para realizar una transacción.

En suma, se trata de la identidad nuclear de un ciudadano asociada a diversos atributos funcionales específicos. Los diferentes atributos o registros funcionales aumentan al vincularse a la fundacional, lo que hace necesario un mayor nivel de ramificación de los sistemas. Esta capacidad se verá reflejada en el nivel de madurez de los sistemas de identificación (Gráfico 1.4).

**Gráfico 1.4.**
Vinculación de la identidad fundacional con las identidades funcionales



# 1.5. DESAFÍOS DE LOS SISTEMAS DE IDENTIFICACIÓN DE EUROPA Y DE AMÉRICA LATINA Y EL CARIBE

## Europa

Actualmente, Europa se enfrenta a tres tipos de desafíos:

- La unicidad de los mecanismos de identificación.
- La interoperabilidad transfronteriza de los sistemas.
- La protección de datos personales.

El primero, de carácter global, refleja que la mayoría de los países cuenta con más de un mecanismo de identificación con múltiples propósitos de uso. Esto es principalmente debido a la característica física tradicional de las tarjetas de identificación y al aislamiento de los sistemas de identificación que impactan tanto al sector público como al privado. En este escenario, la digitalización permitiría contar con un mecanismo único que prevalezca sobre cualquier otra iniciativa específica de identidad, favoreciendo la autenticación para cualquier propósito de uso, sin necesidad de portar más de una identificación para cada uso.

El segundo se deriva de la propia condición de la Unión Europea (UE), que promueve la integración entre los países miembros. El escenario de libre tránsito entre países para ciudadanos y no ciudadanos de la UE presenta situaciones en las que las personas necesitarán hacer uso de sus identidades en cualquier ámbito de actuación, sin la restricción de tener que volver a sus países para realizar el trámite que deseen. En ese sentido, el reto es garantizar la interoperabilidad de los sistemas de gestión de la identidad, a través de marcos de actuación comunes entre los distintos niveles de la administración pública y privada.[3]

3. En 2010, se emite el eGovernment Action Plan i2010, que no solo incorpora la inclusión de lo digital en materia de identidad, sino también la actuación digital de las administraciones públicas a todo nivel.

A su vez, estos estándares de interoperabilidad requieren coincidir con políticas robustas de protección de datos que regulen el tipo de información que podrá mostrarse en sistemas fuera del alcance de uso, sin que ello afecte la usabilidad de la identidad. Esto lleva al siguiente desafío de la región: la calidad de las políticas y procedimientos de protección de datos que las entidades portadoras de identidad deben cumplir en aras de proteger todo dato personal que se atribuya a la identidad de cualquier individuo. Estas normativas deben tener una correspondencia con el cumplimiento, tanto formal como informal, e impactar durante todo el ciclo de vida del uso y posesión de la identidad (Fundación Telefónica, 2012).

## América Latina y el Caribe

Los países de América Latina y el Caribe (ALC) se encuentran realizando esfuerzos por digitalizar sus aparatos estatales, a la par de implementar medidas de ciberseguridad y de protección de la privacidad de datos personales y la transparencia de su uso (CAF, 2014). Estas iniciativas, enmarcadas en el llamado gobierno electrónico, buscan construir un ecosistema digital alrededor de la operación de la administración pública en general. En este marco, la identidad digital es un habilitador clave para lograr mayor accesibilidad a trámites y servicios públicos, además de favorecer la reducción de casos de suplantación y fraude, validez legal otorgada por la firma electrónica, votaciones electrónicas, pago de impuestos en línea, y acceso gratuito y en línea a servicios estatales y privados (CAF, 2017).

En conclusión, ambas regiones se encuentran desarrollando iniciativas alrededor de la identidad digital. Sin embargo, sus desafíos son distintos. En el caso de Europa, el reto consiste en lograr que la identidad sea una de las piezas en común que compartan los países europeos, de manera que se consolide la integración de la comunidad de países a la vez que se garantice la soberanía y autonomía de la información de los datos personales de los ciudadanos. Por otro lado, el desafío en ALC es utilizar la identidad como un habilitador o palanca para el desarrollo de otros servicios para el ciudadano.

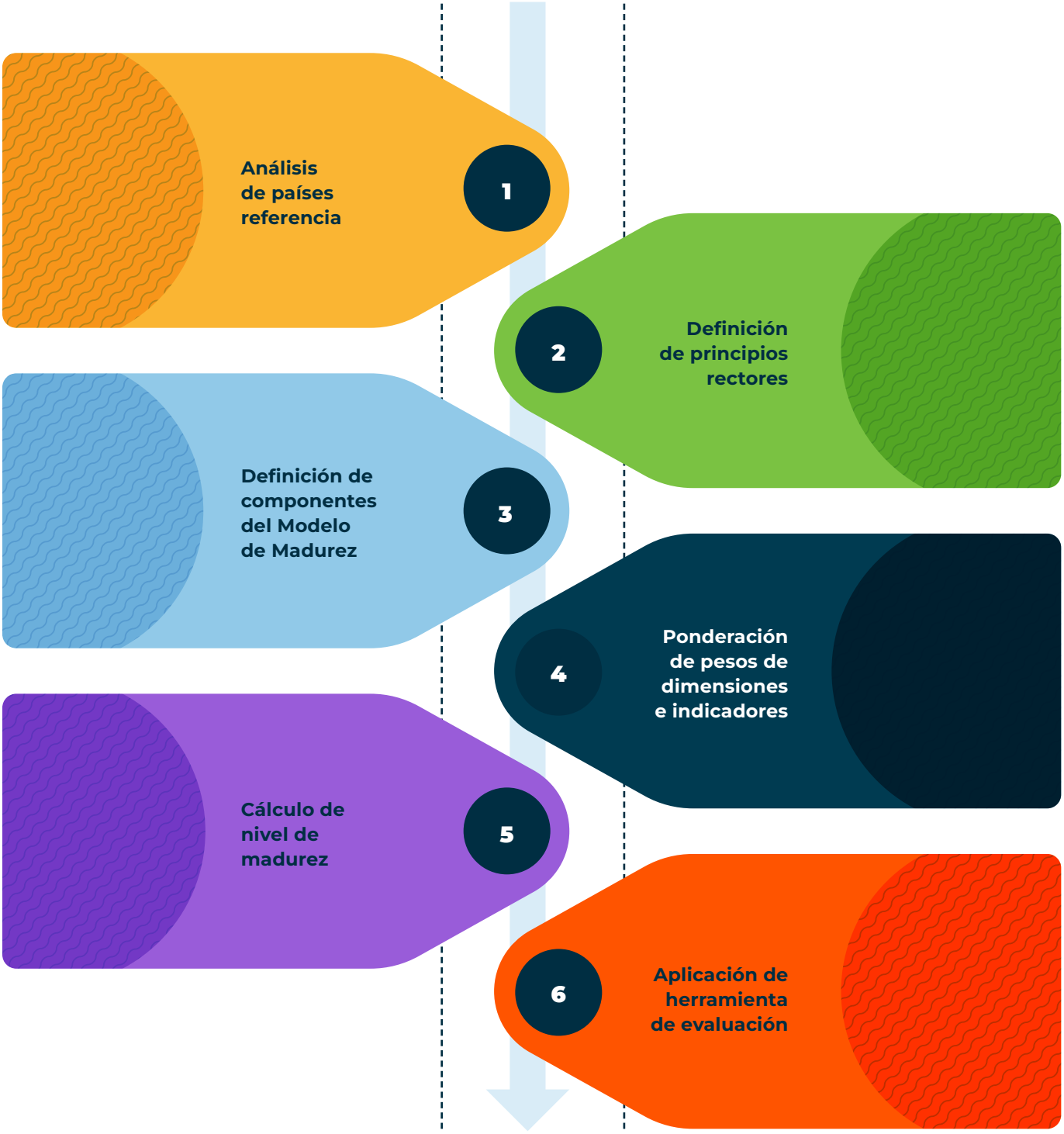
2

# MARCO METODOLÓGICO

1 2 3 4

Para la construcción del Modelo de Madurez de los Sistemas de Identificación, se siguieron los pasos metodológicos que se muestran en el Gráfico 2.1.

**Gráfico 2.1.**
Pasos metodológicos para la construcción del Modelo de Madurez



# 2.1. ANÁLISIS DE PAÍSES DE REFERENCIA[4]

El análisis de países de referencia consistió en investigar y caracterizar naciones con altos estándares de desarrollo en sus sistemas de identificación, incluyendo casos de la región de ALC, con el fin de **identificar las dimensiones e indicadores más relevantes para evaluar el grado de desarrollo de un sistema de identificación.** Este análisis, realizado en 2018, incluyó a Colombia y Perú como ejemplos de la región, y a Corea, España, Estonia y Japón como casos de experiencias extrarregionales con alto desarrollo.

4. Información recopilada en el año 2018.

# 2.2. PRINCIPIOS RECTORES

Los principios rectores[5] son los fundamentos del Modelo necesarios para guiar el objetivo o fin último de incrementar la madurez de los sistemas de identificación y favorecer el diseño de las dimensiones e indicadores del modelo. Su importancia o ponderación puede ser calibrada de acuerdo con la visión del modelo objetivo al que se apunte, cuyo plan de implementación no solo se avoque a contar con un marco regulatorio o al desarrollo de tecnologías, sino que también busque trabajar en la usabilidad de cara al ciudadano y la coordinación intersectorial, entre otros.

En ese sentido, en el Recuadro 2.1 se presentan los principios rectores del Modelo de Madurez.

**Recuadro 2.1.**
Principios rectores del Modelo de Madurez

### Accionabilidad

Determinar acciones específicas que lleven a un país a un estadio de mayor madurez y que, a su vez, puedan estar contempladas en un plan de implementación a corto, mediano y largo plazo.

### Enfoque del ciudadano

Contemplar la gestión de la identidad como un medio y no necesariamente como un fin. El objetivo final es la mejora de la experiencia del ciudadano que hace uso constante de su identidad en distintos ámbitos de su vida, cumpliendo con la política y estándares de protección de datos.

5. Su selección se basa principalmente en desafíos y prioridades de la región, los macroobjetivos del proyecto y criterios como complejidad de implementación, entre otros.

### Gobernanza

Contar con un marco regulatorio que regule el ecosistema general de la gestión de identidad, incluyendo políticas de privacidad de datos personales, así como los demás atributos de la gestión de la identidad.

### Inclusión

Asegurar la posibilidad para todo ciudadano de obtener una identidad, independiente del grupo etario al que pertenezca. La identidad tiene la capacidad de garantizar una mayor accesibilidad a servicios básicos y a programas sociales focalizados.

### Simplificación y reducción de costos

Afianzar la identidad como medio que contribuye directamente a la simplificación y modernización del Estado, a través de la reducción de la complejidad de los trámites de cara al ciudadano, a la vez que reduce los costos de atención de los trámites presenciales.

### Trazabilidad

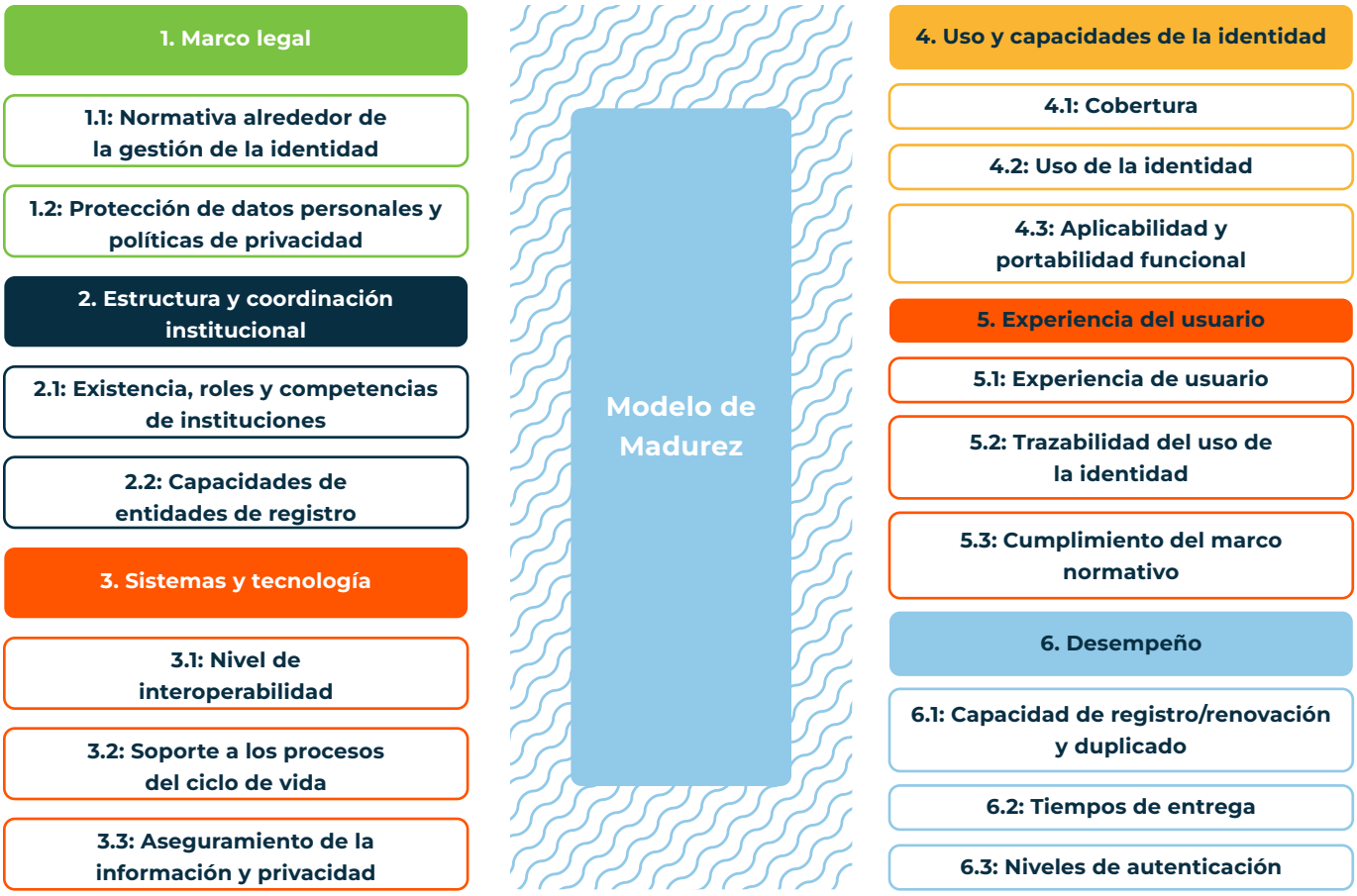
Garantizar la trazabilidad de la gestión de la identidad en los ámbitos públicos y privados, nacionales e internacionales, con el objetivo de lograr una portabilidad universal de la identidad de los ciudadanos, manteniendo los estándares de protección de datos.

# 2.3. COMPONENTES DEL MODELO DE MADUREZ

El Modelo se compone de **dimensiones e indicadores,** que buscan evaluar todos los aspectos a tener en cuenta en cualquier sistema de identidad, de manera integral, escalable y accionable. En otras palabras, se busca que cada punto de mejora vaya acompañado de una acción de evolución específica, que permita a los gestores públicos tomar decisiones para la mejora de la calidad y el desempeño.

Para su construcción, se utilizó como elemento vertebrador el ciclo de vida de la gestión de la identidad, así como los atributos que residen alrededor de este; es decir, actores involucrados, marco legal e institucional, tecnologías de información utilizadas, uso y servicios ofrecidos hacia el ciudadano y métricas de desempeño (Gráfico 2.2).

**Gráfico 2.2.**
Dimensiones e indicadores del Modelo de Madurez




Este Modelo contiene dimensiones e indicadores, aquí denominados INPUT u OUTPUT, que hacen referencia a los roles de cada dimensión dentro del ecosistema de la gestión de identidad:

- **Dimensiones INPUT:** estos atributos se refieren a los elementos relacionados con la definición de lineamientos, regulación y planificación del sistema, es decir, las piezas que sientan las bases, reglas de juego o lineamientos sobre los que los actores pertinentes ejecutarán la gestión de la identidad, e incluso disposiciones sobre elementos cruciales como el despliegue tecnológico. Estas bases se relacionarán directamente con los elementos de la dimensión OUTPUT, debido a que establecerán los procedimientos, formas, normativas y estándares sobre los cuales estos operarán. Es muy importante recalcar la importancia de estas dimensiones e indicadores, dado el alcance de la gestión de la identidad y su carácter de obligatoriedad por parte del Estado, que debe otorgar identidad a los ciudadanos. Por ejemplo, la regulación de los roles de los actores intervinientes en el sistema permitirá establecer los ámbitos de competencia de estas entidades, y que estas a su vez enmarquen su ámbito de actuación dentro de la operación.

- **Dimensiones OUTPUT:** estos elementos se refieren directamente a la operación del sistema de identidad como tal. Es decir, la ejecución de los procedimientos referidos al ciclo de vida de la gestión de la identidad: registro, emisión, uso y actualización. Si bien estas se ciñen a lo estipulado por las dimensiones INPUT, también tienen algunas características autónomas que dependen únicamente de cómo se realice la operación del sistema. Por ejemplo, la dimensión de uso y capacidades del sistema mide las capacidades que tienen los mecanismos de identidad otorgados al ciudadano para su uso. Sin embargo, una aproximación mucho más exigente es medir qué tan frecuentemente usa el ciudadano estas capacidades y, en todo caso, buscar la causa-raíz de por qué el ciudadano no tiene incentivos suficientes para su uso.

Cada dimensión se compone de un conjunto de indicadores que miden la existencia, uso, capacidad y eficiencia de los elementos y/o atributos referentes a los sistemas de identificación. Estos indicadores contienen cuatro niveles, que han sido establecidos desde una perspectiva de línea evolutiva respecto a cada conceptualización del indicador. De cara a lo que representan estos niveles como herramienta de evaluación, cada nivel se identifica con una letra y una puntuación.

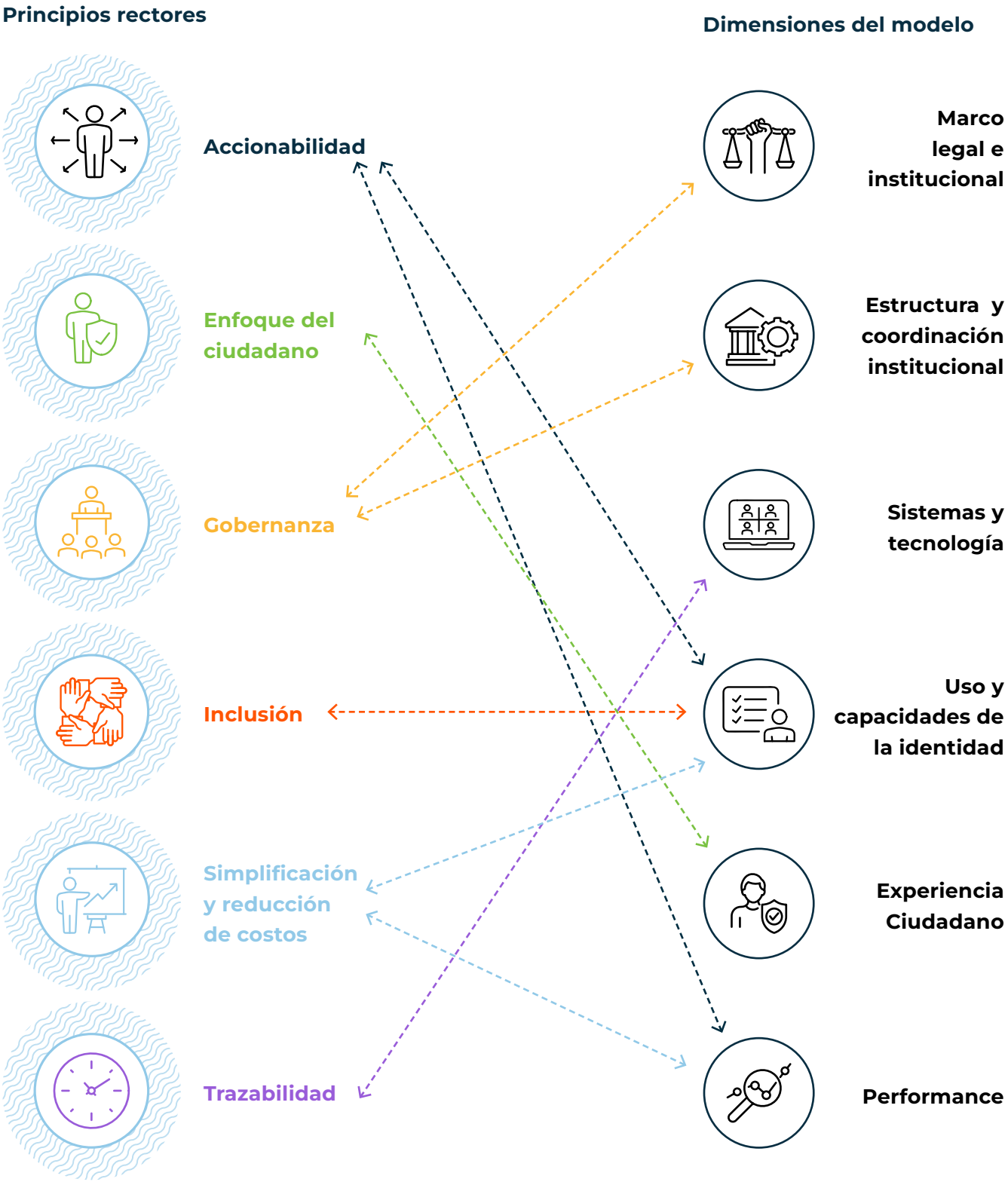
**Gráfico 2.3.**
Puntajes equivalentes de cada nivel por indicador

# 2.4. PONDERACIÓN DE PESOS DE DIMENSIONES E INDICADORES

Después de establecer los principios rectores, dimensiones e indicadores, es importante definir cuáles de los indicadores tienen mayor importancia para el Modelo de Madurez del sistema de identidad de un país. Este ejercicio se realiza sobre la base de las características de los elementos presentes en un ecosistema de identidad, específicamente del carácter estructural e institucional, de la complejidad de la implementación y de la cultura institucional, entre otros. A continuación, se listan una serie de criterios considerados para la ponderación de dimensiones e indicadores:

- **Principios rectores:** el establecimiento de principios rectores, además de establecer los pilares que debe tener un sistema de identidad idóneo, también sirve de guía al momento de realizar la calibración de pesos de las dimensiones. Por ejemplo, en el caso de la regulación y las instituciones, estas se encuentran fuertemente relacionadas con la gobernanza que debería caracterizar a un sistema de identidad. De igual manera, la trazabilidad asegura la necesidad de contar con mecanismos que garanticen la interoperabilidad de los ámbitos en los que la identidad es pertinente (Gráfico 2.4).

**Gráfico 2.4.**
Vinculación de principios rectores con dimensiones



- **Características de las dimensiones INPUT y OUTPUT:** en el caso de las dimensiones clasificadas como INPUT, se las considera críticas para el inicio y desarrollo adecuado de la gestión de identidad de un país. Estas dimensiones sientan las bases y reglas de juego sobre las que las distintas instituciones se relacionarán e involucrarán para ejecutar el registro, validación, emisión y uso de la identidad, así como los atributos que se encuentran alrededor de este ciclo de vida de la identidad. En cambio, las dimensiones OUTPUT son el resultado de la implementación y tangibilización de lo establecido en las dimensiones INPUT, dado que se refieren directamente a la ejecución y operación del ciclo de vida.

- **Complejidad de implementación:** existen dimensiones que son caracterizadas como complejas, debido a la dificultad y esfuerzo que supone implementarlas. Por ejemplo, las dimensiones legales y de arquitectura institucional resultan complejas, dado que, para existir, presuponen contar con un espacio en la agenda pública y en la planificación estratégica del gobierno y un presupuesto asociado para la implementación, entre otros. Del mismo modo, en el caso de la dimensión tecnológica, existen ocasiones en las que las soluciones a implementar requieren de importantes presupuestos y muchas veces coordinaciones intersectoriales para su logro.

**Gráfico 2.5a.**
Distribución de pesos por dimensión

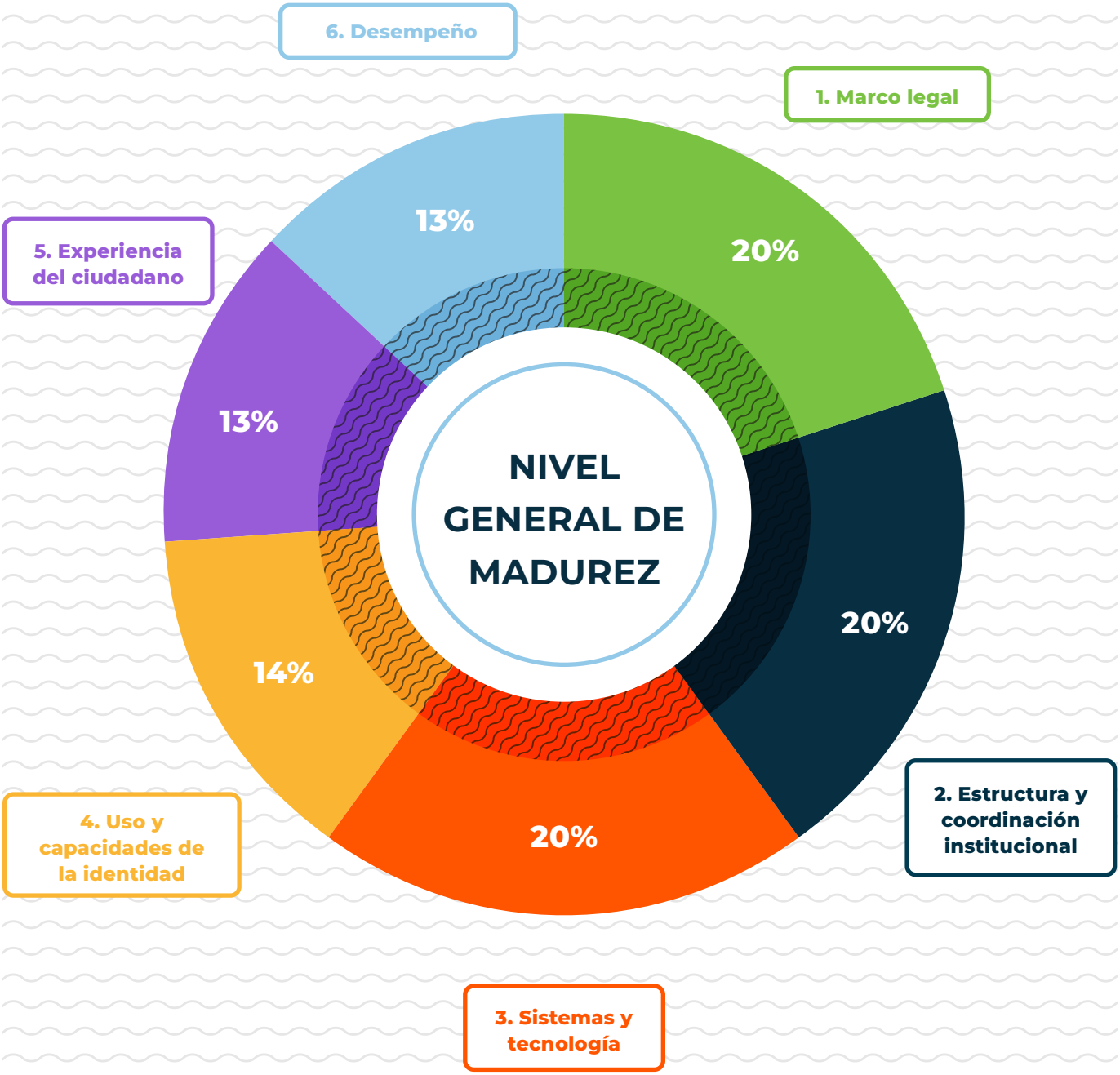
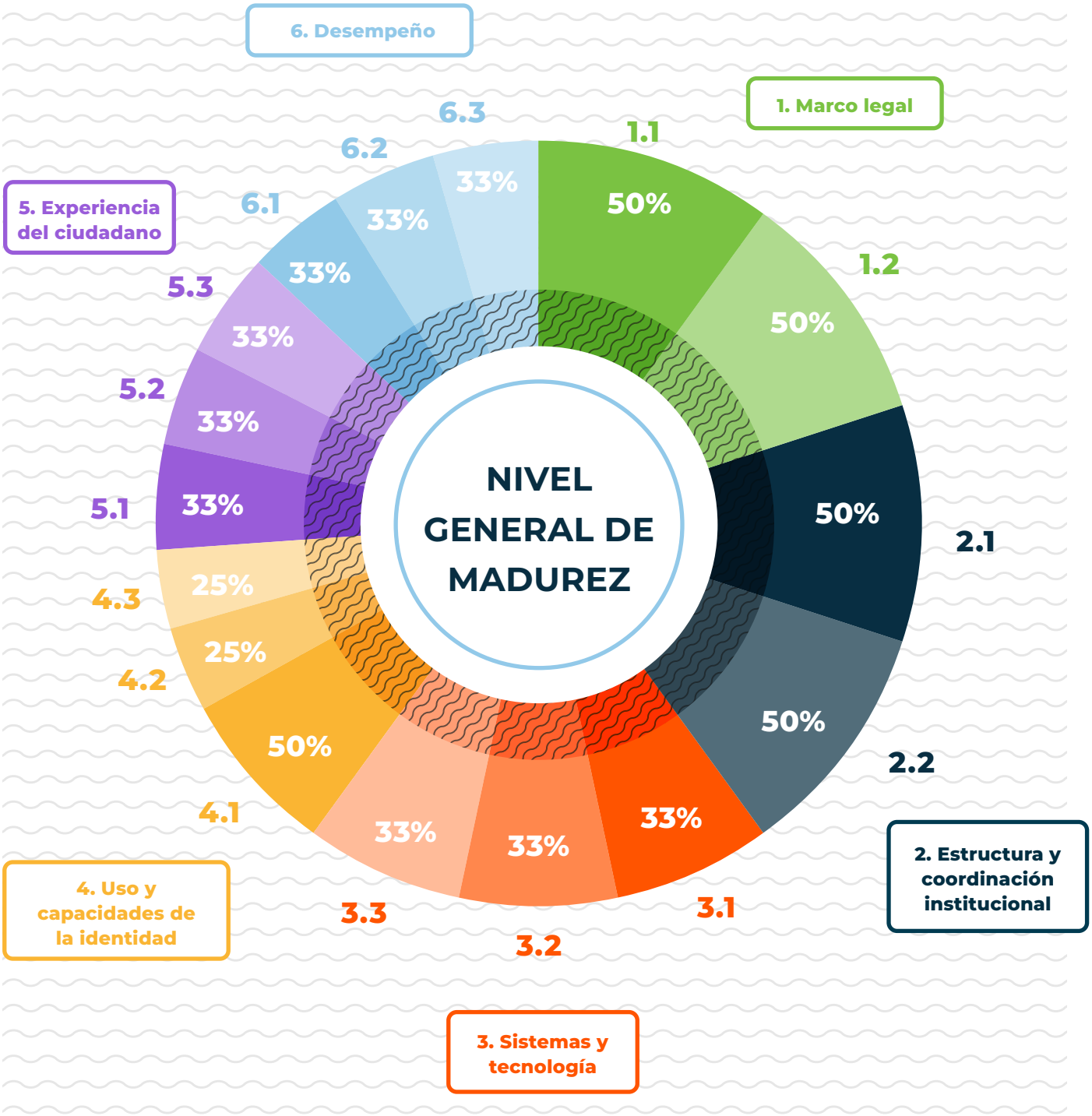


**Gráfico 2.5b.**
Distribución de pesos de indicadores por dimensión



# 2.5. CÁLCULO DEL NIVEL DE MADUREZ

Para realizar el cálculo del desempeño de las dimensiones e indicadores, de acuerdo a los pesos distribuidos en el apartado anterior, se utilizará la fórmula de cálculo que se presenta a continuación, en la que se toman en cuenta las siguientes variables:

**NIVEL DE MADUREZ** = PESO DE DIMENSIÓN (%) **X** PESO DE INDICADOR (%) **X** PUNTAJE OBTENIDO (CANTIDAD)

Con esta fórmula, se podrán obtener distintos escenarios según el avance de los sistemas de identificación de cada país. De acuerdo a lo establecido, los escenarios extremos (mínimo y máximo) que se puedan obtener serán los siguientes:

- **Puntaje mínimo obtenido:** todos los indicadores corresponden al nivel D, por lo que se obtiene un puntaje total de 0 puntos.
- **Puntaje máximo obtenido:** todos los indicadores corresponden al nivel A, con lo que se obtiene un puntaje total de 100 puntos.

En el Cuadro 2.1 se puede observar la versión preliminar de la herramienta de cálculo, en la que se incluyen los datos y en donde, finalmente, se obtienen los resultados generales que, a su vez, pueden dividirse por los subtotales obtenidos por cada dimensión. El objetivo es obtener una visión de cuáles son los puntos considerados avanzados y que deben ser consolidados, así como también de los puntos pendientes sobre los cuales es necesario trabajar.

**Cuadro 2.1.**
Versión preliminar de la herramienta de evaluación (ilustrativa)

| DIMENSIÓN | 1. Marco legal | | 2. Estructura y coordinación institucional | | 3. Sistemas y tecnología | | | 4. Uso y capacidades de la identidad | | | 5. Experiencia del ciudadano | | | 6. Desempeño | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Peso | 20% | | 20% | | 20% | | | 14% | | | 13% | | | 13% | | |
| INDICADOR | 1.1 Normativa alrededor de la gestión de la identidad | 1.2 Protección de datos personales y políticas de privacidad | 2.1 Existencia, roles y competencias de instituciones | 2.2 Capacidades de entidades de registro | 3.1 Nivel de interoperabilidad | 3.2 Sistemas de captura, emisión y verificación de identidad | 3.3 Mecanismos de aseguramiento de la información y privacidad | 4.1 Cobertura y accesibilidad | 4.2 Capacidades de uso de la identidad | 4.3 Aplicabilidad funcional | 5.1 Experiencia del usuario | 5.2 Trazabilidad de uso de la identidad | 5.3 Cumplimiento de marco legal | 6.1 Capacidad de registro / renovación y duplicado | 6.2 Tiempos de entrega | 6.3 Niveles de autenticación |
| Peso | 50% | 50% | 50% | 50% | 33% | 33% | 33% | 25% | 25% | 50% | 33% | 33% | 33% | 33% | 33% | 33% |
| Puntaje máximo por INDICADOR | 10,0 | 10,0 | 10,0 | 10,0 | 6,7 | 6,7 | 6,7 | 3,5 | 3,5 | 7,0 | 4,3 | 4,3 | 4,3 | 4,3 | 4,3 | 4,3 |
| Puntaje máximo por DIMENSIÓN | 20 | | 20 | | 20 | | | 14 | | | 13 | | | 13 | | |
| Referencia: España | A | A | A | A | A | B | A | A | A | B | B | B | B | A | B | A |
| | 100,0 | 100,0 | 100,0 | 100,0 | 100,0 | 66,0 | 100,0 | 100,0 | 100,0 | 66,0 | 66,0 | 66,0 | 66,0 | 100,0 | 66,0 | 100,0 |
| Subtotal obtenido por indicador | 10,0 | 10,0 | 10,0 | 10,0 | 6,7 | 4,4 | 6,7 | 3,5 | 3,5 | 4,6 | 2,9 | 2,9 | 2,9 | 4,3 | 2,9 | 4,3 |
| Total obtenido por dimensión | 20 | | 20 | | 18 | | | 12 | | | 9 | | | 12 | | |
| Total general obtenido | 89 | | | | | | | | | | | | | | | |
| Referencia: Estonia | A | A | A | A | A | A | A | A | A | A | A | B | B | A | B | A |
| | 100,0 | 100,0 | 100,0 | 100,0 | 100,0 | 100,0 | 100,0 | 100,0 | 100,0 | 100,0 | 100,0 | 66,0 | 66,0 | 100,0 | 66,0 | 100,0 |
| Subtotal obtenido por indicador | 10,0 | 10,0 | 10,0 | 10,0 | 6,7 | 6,7 | 6,7 | 3,5 | 3,5 | 7,0 | 4,3 | 2,9 | 2,9 | 4,3 | 2,9 | 4,3 |
| Total obtenido por dimensión | 20 | | 20 | | 20 | | | 14 | | | 10 | | | 12 | | |
| Total general obtenido | 96 | | | | | | | | | | | | | | | |
| Referencia: Corea del Sur | A | C | B | B | B | B | B | B | A | B | B | C | B | B | A | B |
| | 100,0 | 33,0 | 66,0 | 66,0 | 66,0 | 66,0 | 66,0 | 66,0 | 100,0 | 66,0 | 66,0 | 33,0 | 66,0 | 66,0 | 100,0 | 66,0 |
| Subtotal obtenido por indicador | 10,0 | 3,3 | 6,6 | 6,6 | 4,4 | 4,4 | 4,4 | 2,3 | 3,5 | 4,6 | 2,9 | 1,4 | 2,9 | 2,9 | 4,3 | 2,9 |
| Total obtenido por dimensión | 13 | | 13 | | 13 | | | 10 | | | 7 | | | 10 | | |
| Total general obtenido | 67 | | | | | | | | | | | | | | | |
| Perú | B | C | B | A | C | C | B | B | B | B | B | B | C | B | C | B |
| | 66,0 | 33,0 | 66,0 | 100,0 | 33,0 | 33,0 | 66,0 | 66,0 | 66,0 | 66,0 | 66,0 | 66,0 | 33,0 | 66,0 | 33,0 | 66,0 |
| Subtotal obtenido por indicador | 6,6 | 3,3 | 6,6 | 10,0 | 2,2 | 2,2 | 4,4 | 2,3 | 2,3 | 4,6 | 2,9 | 2,9 | 1,4 | 2,9 | 1,4 | 2,9 |
| Total obtenido por dimensión | 10 | | 17 | | 9 | | | 9 | | | 7 | | | 7 | | |
| Total general obtenido | 59 | | | | | | | | | | | | | | | |
| El Salvador | C | D | C | D | D | D | D | C | D | D | C | C | D | C | C | D |
| | 33,0 | 0,0 | 33,0 | 0,0 | 0,0 | 0,0 | 0,0 | 33,0 | 0,0 | 0,0 | 33,0 | 33,0 | 0,0 | 33,0 | 33,0 | 0,0 |
| Subtotal obtenido por indicador | 3,3 | 0,0 | 3,3 | 0,0 | 0,0 | 0,0 | 0,0 | 1,2 | 0,0 | 0,0 | 1,4 | 1,4 | 0,0 | 1,4 | 1,4 | 0,0 |
| Total obtenido por dimensión | 3 | | 3 | | 0 | | | 1 | | | 3 | | | 3 | | |
| Total general obtenido | 13 | | | | | | | | | | | | | | | |
| Argentina | B | B | B | A | B | B | A | A | A | B | B | B | B | A | C | B |
| | 66,0 | 66,0 | 66,0 | 100,0 | 66,0 | 66,0 | 100,0 | 100,0 | 100,0 | 66,0 | 66,0 | 66,0 | 66,0 | 100,0 | 33,0 | 66,0 |
| Subtotal obtenido por indicador | 6,6 | 6,6 | 6,6 | 10,0 | 4,4 | 4,4 | 6,7 | 3,5 | 3,5 | 4,6 | 2,9 | 2,9 | 2,9 | 4,3 | 1,4 | 2,9 |
| Total obtenido por dimensión | 13 | | 17 | | 15 | | | 12 | | | 9 | | | 9 | | |
| Total general obtenido | 74 | | | | | | | | | | | | | | | |

3

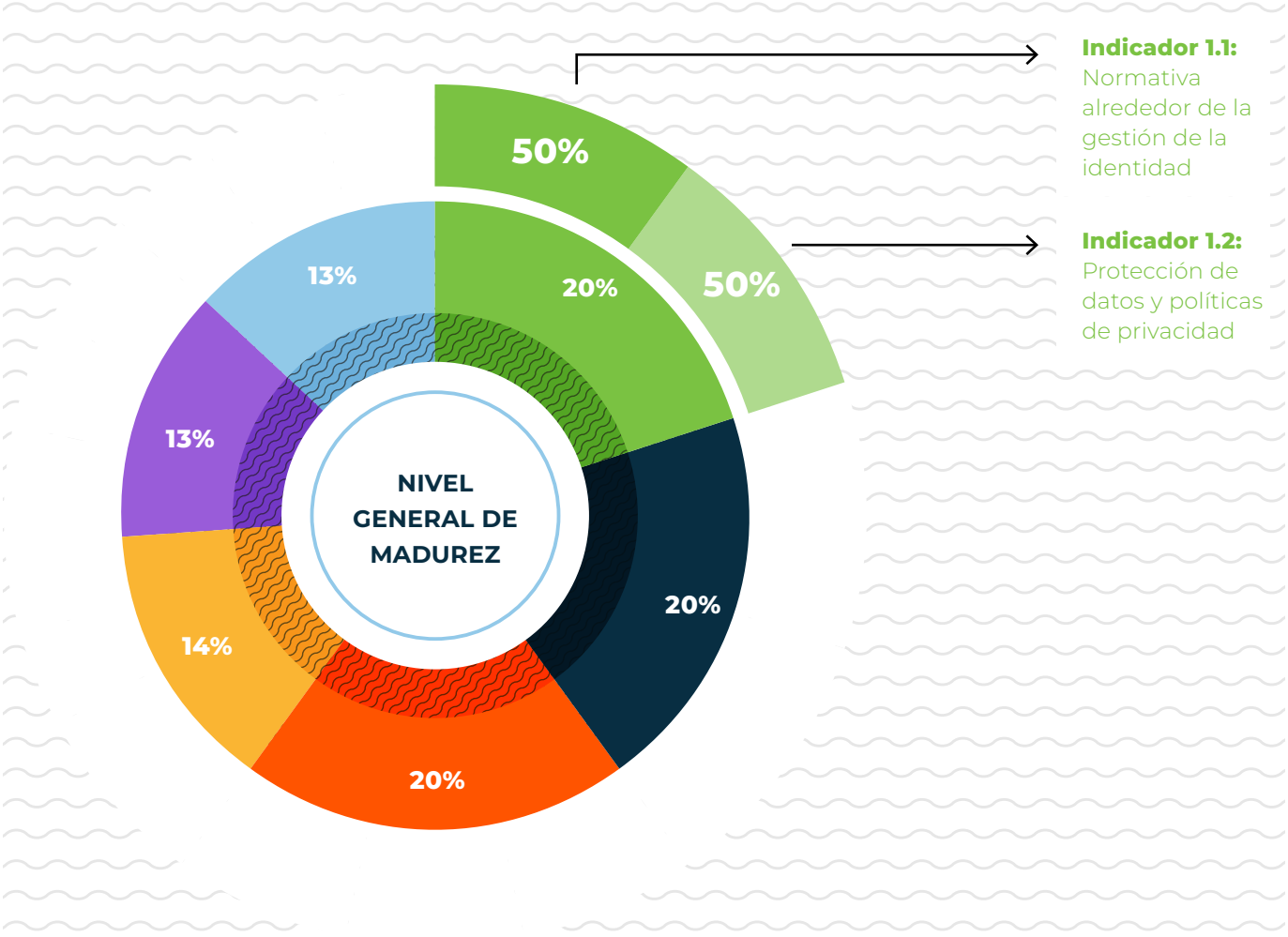
# DESARROLLO CONCEPTUAL DE DIMENSIONES E INDICADORES DEL MODELO DE MADUREZ

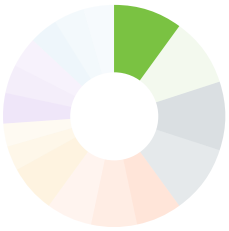
1 2 3 4

# 3.1. DIMENSIÓN 1: MARCO LEGAL

La dimensión 1, **Marco legal**, tiene un peso del 20% dentro del Modelo de Madurez, y está compuesta por dos indicadores: 1.1: **Normativa alrededor de la gestión de la identidad**, y 1.2: **Protección de datos y políticas de privacidad**. Ambos indicadores tienen el mismo peso dentro de la dimensión, es decir, el 50%.

**Gráfico 3.1.**
Peso de la dimensión Marco legal y de sus dos indicadores





# **Indicador 1.1:** Normativa alrededor de la gestión de la identidad

## A
## Definición del indicador

Existencia de instrumentos legales vigentes que regulen los procesos del ciclo de vida de la identidad.

## B
## Justificación de uso

La gestión de la identidad de los ciudadanos es necesaria para garantizar el cumplimiento de la identificación del propio individuo, para garantizar la gobernabilidad por parte del Estado, así como para la autenticación de la identidad frente a terceras partes. Respecto al individuo, para poder probar su condición de ciudadano, hijo, cónyuge, pariente, mayor de edad, tutela, etc. Respecto del Estado, para la prestación, diseño e implementación de muchos servicios administrativos. Respecto de los terceros, para dar certidumbre para el establecimiento de negociaciones entre sí.[6]

Dado este marco de relacionamiento, los sistemas nacionales de identidad requieren de un **marco normativo robusto** que parta de una definición de las competencias institucionales en la norma superior, como puede ser la Constitución Nacional, y que se despliegue en normas como leyes a cargo del Congreso, y reglamentarias a cargo del Ejecutivo a través de las distintas unidades orgánicas ejecutoras. Esta definición de competencias institucionales resulta fundamental, pues permitirá desplegar el documento de identificación y su uso en diversos procesos y trámites, no solo de la administración pública sino también en el ámbito privado.

## C
## Forma de medición

**Nivel** D C B A

No existen leyes sobre la creación de identidad.

### Factores clave de posicionamiento

- No existencia de leyes que dispongan la competencia de autoridades estatales y/o federales acerca de la creación de la identidad de ciudadanos. La existencia de normas técnicas no es suficiente para pasar al siguiente nivel.

6. Véanse Global Delivery Initiative (2017), Kim (2004), E-Governance Academy (2014) y Pedak (2013).

**Nivel** 


Existen leyes o normas técnicas que regulan el proceso del registro de una única identidad a nivel nacional/federal.

**Factores clave de posicionamiento**

- Existencia de leyes que definen la identificación de los ciudadanos.
- No existencia de leyes o normas técnicas que definan la labor del registro de la identidad.
- Existencia de múltiples autoridades en el Estado con competencias designadas para la creación de identificación, entre ellas, algunas de carácter nacional y otras provinciales o estatales, con diversos datos de identificación.
- No existencia de normas que permitan unificar bases de datos de identificación nacional y subnacional.
- No existencia de normas que promuevan la coordinación interinstitucional entre diversas autoridades en el proceso de identificación.

**Nivel** 


Existen leyes y normas técnicas que regulan el ciclo de vida de identidad implantando mecanismos digitales, tales como el DNI electrónico y la firma electrónica/digital.

**Factores clave de posicionamiento**

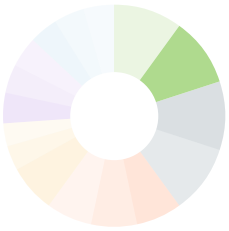
- Existencia de normas reglamentarias en lo relativo al procedimiento de autenticación de la identidad por parte de terceros, por ejemplo, la verificación biométrica electrónica de la identidad o la autenticación facial.
- Desarrollo de normas que permitan utilizar el mecanismo de identificación digital como método de autenticación y de firma electrónica.

**Nivel** 


Existen instrumentos legales que regulan los ámbitos de uso relacionados con la identidad digital. Ejemplos de aplicación: administración electrónica, comercio electrónico (*e-commerce*), e-salud, etc.

**Factores clave de posicionamiento**

- Desarrollo de normas que definen el DNI electrónico como habilitador para realizar procedimientos de autenticación de identidad en todo tipo de servicios públicos y privados.
- Normas que permitan la identidad desde el nacimiento hasta el fallecimiento, y recogida de la misma y actualización inmediata desde el propio momento y hecho en el que ocurre el evento (actualización de registros civiles desde hospitales y centros sanitarios, especialmente).
- Existencia de políticas de identidad digital definidas (por ejemplo: eIDAS).



# **Indicador 1.2:** Protección de datos personales y políticas de privacidad

## A

## Definición del indicador

Existencia de normativa relacionada a la utilización de medidas de seguridad específicas que garanticen el acceso a la información y privacidad de datos personales durante todo el ciclo de vida de gestión de la identidad por parte del ciudadano.

## B

## Justificación de uso

La mayoría de las legislaciones a nivel internacional contemplan como derecho fundamental el *habeas data* o protección de datos personales (normalmente en la norma superior, como la Constitución Política). Esta norma regula la necesidad de que los datos personales tengan una protección adecuada en todas las fases de tratamiento de la información.

El *habeas data* es una acción jurisdiccional, normalmente constitucional, que confirma el derecho de cualquier persona física o jurídica para solicitar y obtener la información existente sobre su persona, y de solicitar su eliminación o corrección si fuera falsa o estuviera desactualizada. Este derecho aplica a información almacenada en registros o bancos de datos de todo tipo, ya sea en instituciones públicas o privadas, y en registros informáticos o no. El *habeas data* puede cobijar también el concepto de derecho al olvido, esto es, el derecho a eliminar información que se considera obsoleta por el transcurso del tiempo y ha perdido su utilidad.

Este derecho se ha ido expandiendo y comenzó a ser reglamentado tanto por leyes de *habeas data* como por normas de protección de datos personales, que suelen tener un capítulo procesal donde se describe el objeto de la acción de *habeas data*, la legitimación pasiva y activa, y la prueba y la sentencia. También se ha encomendado a organismos de control la vigilancia sobre la aplicación de estas normas de *habeas data*. En diversos países, como Argentina, Alemania, Bélgica, Canadá, España, Estados Unidos, Francia y Uruguay, entre otros, existen organismos de control que tienen la misión de supervisar el tratamiento de datos personales por parte de empresas e instituciones públicas.

Además de la tangibilización de este derecho en el marco normativo de los países, existen diversos desafíos asociados a la protección de los datos que se administran durante la ejecución del ciclo de la identidad de ciudadano. Por un lado, aún se discuten los diferentes mecanismos (tecnología, protocolos, estándares, etc.) que las administraciones públicas deben implementar para asegurarse de proteger los datos del ciudadano. Esta problemática se hace todavía más relevante porque las administraciones públicas son las que mayor cantidad de información recopilan y generan referente a la identidad del ciudadano.

Uno de los habilitadores de esta protección es la tecnología implementada. Sin embargo, no todas las posibilidades que ofrece la tecnología son admisibles jurídicamente, sobre todo teniendo en cuenta los objetivos de uso por parte de la actividad administrativa. En ese sentido, actualmente se está promoviendo la privacidad por diseño, es decir, incluir mecanismos de aseguramiento de información en la construcción del sistema que permitan dar mayor seguridad a las funcionalidades de los sistemas creados.

En relación a la protección de los datos personales y los servicios administrados en línea, se han suscitado diversos debates sobre las implicaciones que pueda tener la utilización de sistemas de identificación digitales, especialmente a partir de la configuración de este documento como instrumento de identidad electrónica.

Si bien es cierto que se trata de un instrumento de gran utilidad para facilitar la gestión informativa referida a personas concretas, también lo es que la interconexión entre bases de datos diversas y heterogéneas en cuanto a su contenido y finalidad puede convertirse en un auténtico peligro en tanto permite crear perfiles de forma sencilla a quien pueda tener acceso a esas múltiples fuentes informativas.

Finalmente, otro desafío importante son las exigencias normativas de la protección de los datos personales de los titulares de los certificados, especialmente en lo que refiere a la consulta de la vigencia de esos certificados en ocasión de la ejecución de servicios de administración electrónica. Su importancia es tal que una deficiente articulación en la gestión de estos servicios puede convertirse en un obstáculo que dificulte gravemente, cuando no impida, la consolidación de este nuevo modelo de gestión administrativa basado en la tecnología.

C

## Forma de medición

**Nivel** D C B A

No existen leyes o normas técnicas en materia de seguridad y privacidad de los datos personales.

**Factores clave de posicionamiento**

- No existencia de una política pública sobre el tratamiento de datos personales.
- No existencia de medidas de seguridad de la información en las bases de datos personales, por lo que son altamente susceptibles de sufrir situaciones de adulteración, robo o pérdida de datos personales, acceso o uso no autorizado de los mismos.

**Nivel** D C B A

Existen leyes o normas técnicas en materia de protección de datos personales y de seguridad de la información, pero no hay normas particulares en materia de privacidad por diseño, que versa sobre los siguientes principios:

- Informar al ciudadano sobre qué datos se le piden y qué uso se les da.

- Minimización de la recolección, almacenamiento y uso de datos: los datos requeridos a los ciudadanos deben ser los mínimos para garantizar la creación de una identidad confiable y su uso debe limitarse a lo necesario para garantizar el servicio.
- Inclusión de prácticas preventivas y no solo correctivas frente al uso de datos personales.
- La privacidad como un estado predeterminado en los sistemas que utilizan las organizaciones.
- Protección del dato durante toda la intervención del ciudadano.
- Aplicación de estos principios durante todo el ciclo de vida del ciudadano y su identidad en todos los ámbitos.
- Enfoque centrado en el ciudadano.

**Factores clave de posicionamiento**

- Existencia de un reconocimiento de carácter fundamental del derecho a la protección de datos personales y un marco jurídico que establece los criterios mínimos para su desarrollo, incluyendo una adecuada clasificación de los datos, donde la identidad de una persona y el mecanismo de identificación se encuentran vinculados a la protección de datos.
- Inclusión de estándares internacionales en la implementación de mecanismos de protección.
- Establecimiento de guías de responsabilidad.
- Atribuciones legales sancionatorias de la autoridad de protección de datos.

**Nivel** 


Existen leyes o normas técnicas en materia de protección de datos personales que incluyen definiciones reglamentarias de estándares de privacidad para diversos trámites y servicios digitales estatales.

**Factores clave de posicionamiento**

- Existencia de legislación específica aplicable al sector público y privado.
- Existencia de una autoridad de control que garantice la adecuada aplicabilidad de la normativa, y que proteja y defienda a los ciudadanos en términos de su derecho a la protección de datos personales.
- Reconocimiento de los datos biográficos que componen a los mecanismos de identidad como datos personales.

**Nivel** 


Existen leyes o normas técnicas que exigen el cumplimiento de la privacidad por diseño en el uso de aplicaciones que requieren la autenticación de la identidad de los ciudadanos de manera digital.

### Factores clave de posicionamiento

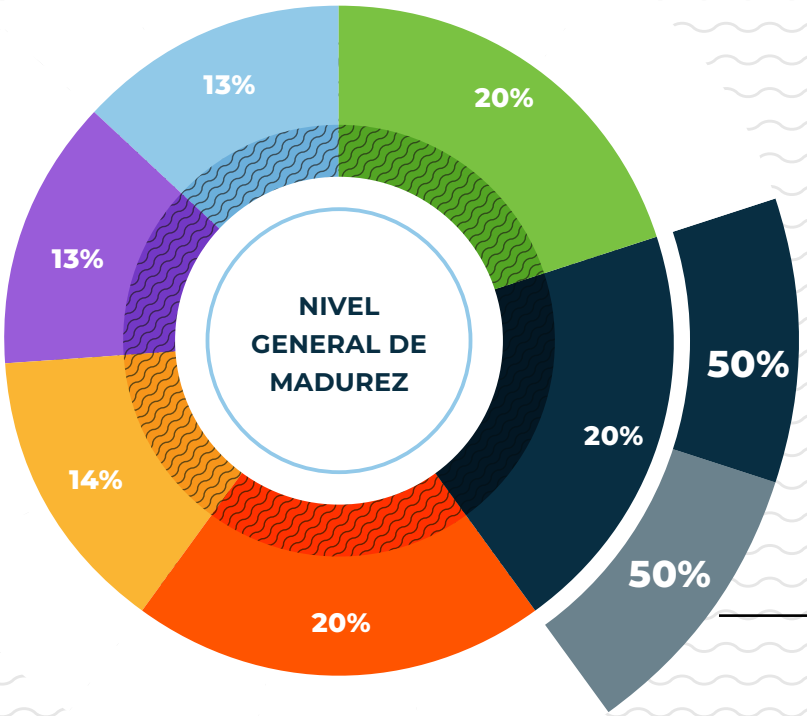
- Conformidad con el Reglamento General de Protección de Datos (RGPD).[7]
- Reconocimiento de derechos de **acceso**, **rectificación** y **cancelación**, y regulación detallada de lo relativo a la información y al consentimiento del titular de los datos.
- Reconocimiento de los datos de los documentos públicos de identidad como datos personales.
- Existencia de normas para la captura segura de los datos personales vinculados a documentos nacionales de identificación.
- Existencia de convenios de cooperación específicos que representen mecanismos de coordinación interinstitucional entre las autoridades de identificación y la de protección de datos personales.
- Existencia de un sistema de información por el que el ciudadano tenga la capacidad de acceder a la información de uso de su identidad digital por terceras partes de manera sencilla.

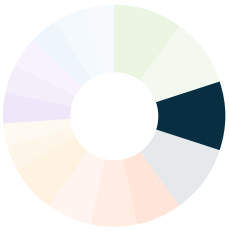
7. Más información sobre el RGPD disponible en: **https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm**.

# 3.2. DIMENSIÓN 2: ESTRUCTURA Y COORDINACIÓN INSTITUCIONAL

La dimensión 2, **Estructura y coordinación institucional**, tiene un peso del 20% dentro del Modelo de Madurez, y está compuesta por dos indicadores: 2.1: **Existencia de roles y competencias institucionales** y 2.2: **Capacidades de las entidades de registro**. Ambos indicadores tienen el mismo peso dentro de la dimensión, es decir, el 50%.

**Gráfico 3.2.**
Peso de la dimensión Estructura y coordinación institucional y de sus dos indicadores





# **Indicador 2.1:** Existencia, roles y competencias de instituciones

## A
## Definición del indicador

Existencia, roles y competencias de las instituciones que intervienen en el registro, validación, emisión, uso y actualización de la identidad del ciudadano.

## B
## Justificación de uso

Uno de los elementos más importantes que garantiza un eficiente funcionamiento del ecosistema de identidad es la estructura institucional, factor clave que determina la existencia, competencias, coordinación, comunicación y cooperación de las instituciones intervinientes en la ejecución del ciclo de vida de la identidad de manera armoniosa y congruente, y bajo lineamientos técnicos.

Estudios o experiencias de referencia que avalan la importancia del indicador en el nivel de madurez de los sistemas de identificación nacional son los siguientes:

- El Banco Asiático de Desarrollo en su reporte *Identity for Development in Asia and the Pacific* (ADB, 2016) establece como elemento crítico en los sistemas de identificación la existencia de una agencia que centralice y coordine a las diferentes instituciones implicadas en la gestión de la identidad y su uso, tales como las entidades de registro, de emisión, de validación y de certificación de calidad, entre otras.

- El Banco Mundial en el estudio *Technical Standards for Digital Identity* (Banco Mundial, 2017a) señala: "Este aspecto [de la estructura institucional] se ocupa de definir los objetivos de gobierno, modelar los procesos y fomentar la colaboración de las administraciones que desean intercambiar información y pueden tener diferentes estructuras y procesos internos" (traducción propia del inglés). De esta manera, el rol principal de la agencia reguladora del sistema será el de definir una visión y enfoque unificados que superen toda iniciativa particular o fragmentada de identidad.

- Asimismo, en el estudio *Identification for Development (ID4D) Integration Approach* (Banco Mundial, 2015) se afirma que los países más avanzados en la gestión de identidad desarrollaron un factor de éxito en común: definir e implementar un organismo o agencia independiente que supervise el ecosistema de manera integral, con el rol de propietario del sistema nacional de identidad. Con ello, se asegura que el sistema desarrolle de manera independiente los intereses individuales, otorgándole un mandato único y nacional a este organismo. De forma complementaria, esta estructura nacional tendrá que establecer los mecanismos de cooperación entre las agencias involucradas en el ciclo de vida de identidad digital, a fin de garantizar la contribución formal de estas instituciones.

- En cuanto al mayor estadio de madurez de este indicador, el Banco Asiático de Desarrollo en el documento *Identity for Development in Asia and the Pacific* (ADB, 2016) señala lo siguiente: "Un ejemplo de una actividad de la interoperabilidad de la identidad digital entre organizaciones/países sería mapear los procesos del ciclo de vida de la identidad de esa organización con los niveles del marco de garantía de autenticación ISO" (traducción propia del inglés). Es decir, el escenario de mayor madurez de este indicador se da cuando las estructuras de generación y uso de la identidad están basadas en estándares internacionales. Por ejemplo, este escenario ya existe en la realidad y las estructuras más representativas son las ejecutadas por la UE, como el proyecto Identidades seguras enlazadas a través de fronteras (STORK, por sus siglas en inglés), STORK2.0, Electronic Simple European Networked Services (eSENS) y eIDAS.

## C
## Forma de medición

**Nivel** D C B A

No existe una entidad que tenga la capacidad de gestionar una única identidad a los ciudadanos o existen registros funcionales de nicho y ninguno prevalece.

### Factores clave de posicionamiento

- No existencia de una organización única que regule la identidad a nivel nacional.
- Existencia de diferentes organizaciones o entidades a nivel nacional o subnacional, que emiten identidades a sus grupos de usuarios (tarjeta del votante, licencia de conducción, tarjeta del seguro social, etc.) pero ninguna de ellas prevalece o pueda ser utilizada por toda la población.

**Nivel** D C B A

Existe una estructura organizada para el registro, validación y emisión de mecanismos de identificación, y una prevalece en todo el Estado.

### Factores clave de posicionamiento

- Existencia de una única entidad gubernamental que regula la gestión de la identidad, ya sea emitida por una entidad pública que tiene definida dicha función dentro del Estado (forma centralizada) o por operadores públicos o privados (forma descentralizada).
- No existencia de una entidad con alguna de las siguientes competencias asignada:
  - → Entidad que regule los servicios digitales y el uso de la identidad.
  - → Agencia que tenga competencia sobre la regulación de estándares o procesos relacionados a identidad.

**Nivel** D C B A

Existe una estructura que, además de regular los procesos de registro, validación, emisión y actua-

lización de las identidades, contempla las competencias acerca del uso de las mismas en los diferentes sectores, e incluso canaliza la atención al ciudadano mediante los servicios electrónicos y permite su uso a nivel regional. Es decir, este nivel agrega respecto al anterior, el uso de los distintos mecanismos de identificación.

**Factores clave de posicionamiento**

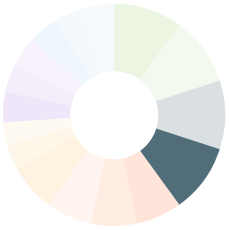
- Los siguientes roles se encuentran definidos y asignados en los actores intervinientes en el ecosistema de identidad:
  - → Entidad de registro, validación, emisión y actualización de la identidad.
  - → Agencia o entidad que regule los servicios digitales y uso de la identidad.
  - → Agencia para la regulación de estándares o procesos de homologación de los servicios vinculados con el mecanismo de identificación.
- Además de contar con los actores anteriormente definidos, el país se encontrará en este nivel cuando disponga de las siguientes estructuras:
  - → Entidades de registro funcionales vinculadas con la identidad fundacional: son las agencias encargadas de crear y mantener atributos de la identidad específicos para determinados usos o servicios, como procesos electorales, agencias tributarias, seguridad social. Esto permite al ciudadano usar su tarjeta de identificación para estas transacciones.

**Nivel** D C B A

Existe una estructura completa que contempla a todos los actores vinculados al ciclo de vida de la identidad y la adecuación de los procesos incluidos en dicho ciclo de vida a estándares internacionales, con la posibilidad de utilizar tanto el sistema del país, como de otros países que sigan estándares internacionales.

**Factores clave de posicionamiento**

Existencia de mecanismos voluntarios de integración a nivel regional, que permiten el reconocimiento y uso de la identidad. La entidad rectora tiene la capacidad de realizar este tipo de convenios.



# Indicador 2.2: Capacidades de entidades de registro

## A

## Definición del indicador

Capacidades competenciales de las entidades de registro. Estas entidades de registro no son o no tienen que ser necesariamente las entidades de registro civil. En este contexto, las entidades de registro son aquellas encargadas de gestionar el ciclo de vida de la identidad.

B

## Justificación de uso

Unas de las instituciones más importantes que intervienen en un sistema nacional de identidad son las entidades de registro, es decir, los órganos encargados de capturar y almacenar los datos biográficos y demás atributos asociados a la identidad del ciudadano. En algunos casos, estas entidades pueden también fungir como registros civiles, que administran los estados civiles de los ciudadanos, o pueden ser operadores públicos o privados.[8]

Para asegurar un eficiente desempeño de estos órganos, es importante definir las competencias y atribuciones técnicas con las que operarán. En ese sentido, las entidades de registro evolucionarán de acuerdo a la cobertura de actividades que puedan incorporar en sus funciones, es decir, un nivel maduro de funcionamiento de estas entidades de registro se dará cuando las entidades de registro de un país gestionen todo el ciclo de vida de identidad de los ciudadanos. En estadios menores, estas entidades solo serán capaces de realizar este ciclo de manera parcial, con apoyo de otras instituciones. Además de cubrir operativamente el ciclo completo de la emisión de mecanismos de identidad, estructuralmente estas entidades de registro también evolucionarán en la medida en que puedan operar de manera tercerizada, cumpliendo los mismos estándares de calidad del proceso.

Existen estudios y experiencias de países que hacen referencia a la validez e importancia de este indicador, y enfatizan en la vinculación de las entidades de registro con los registros civiles:

- El Banco Asiático de Desarrollo en su estudio *Identity for Development in Asia and the Pacific* (ADB, 2016) señala lo siguiente: "Los sistemas de identificación también se han estado moviendo hacia la integración. Originados a partir de los registros civiles que emitían certificados de nacimiento, diferentes ministerios han comenzado a emitir identificaciones funcionales para sus programas. [...] El sistema de registro civil y estadísticas vitales (CRVS, por sus siglas en inglés) actualmente está evolucionando hacia un sistema más integrado, aunque con el CRVS como una parte esencial del mismo. Un sistema de identificación integrado ayudará al gobierno a planificar mejor las políticas al proporcionar las estadísticas vitales de los individuos" (traducción propia del inglés).

- Asimismo, el Banco Mundial afirma en su estudio *Identification for Development (ID4D) Integration Approach* (Banco Mundial, 2015): "[...] En la mayoría de los casos, el registro civil o de estadísticas vitales y de población de un país (sistema RC) es el registro fundacional. Este registro contiene información básica de la población (como nacimientos y defunciones) e identificaciones únicas para vincular la identidad a todos los demás registros. Por lo tanto, es importante

8. Por ejemplo, en el caso del Reino Unido, las entidades financieras fungen de operadores certificadores que se encargan de certificar la identidad de un ciudadano.

que los sistemas de registro civil sean lo más completos y precisos posible, apuntando a una participación del 100% de la población y a la digitalización del sistema (es decir, que todos los registros correspondientes estén disponibles electrónicamente en el registro civil). Sin embargo, algunos países pueden desarrollar un registro fundacional incluso si su sistema CR no es robusto. Pueden hacerlo construyendo directamente un registro a partir de una inscripción nacional amplia y precisa. Por ejemplo, el programa Aadhaar de la India carece de un sistema de registro de nacimientos/defunciones desarrollado y alrededor del 80% de la población del país está registrada. Pero el país ha podido construir un registro fundacional desde cero, gracias a su masiva campaña de inscripción" (traducción propia del inglés).

- Del mismo modo, según *Technical Standards for Digital Identity* (Banco Mundial, 2017a), "Una vez que la persona ha reclamado una identidad durante la inscripción, esta identidad se valida verificando los atributos presentados contra los datos existentes. El proceso de validación asegura que la identidad existe (es decir, que la persona está viva) y es reclamada por una sola persona (es decir, que es única en la base de datos). También se pueden establecer vínculos entre la identidad reclamada y las identidades en otras bases de datos (por ejemplo, registros civiles, registros de población, etc.)" (traducción propia del inglés).

- En líneas similares, la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID, por sus siglas en inglés) indica al respecto en *Identity in a Digital Age* (USAID, 2017): "La inscripción generalmente incluye varios procesos: la verificación de identidad es el proceso de vincular los registros en una base de datos a una persona del mundo real. Esto requiere que el registro coincida con atributos individuales que sean lo suficientemente únicos y estables para garantizar que la coincidencia siga siendo válida con el tiempo. Cada sistema también tendrá un conjunto de requisitos sobre qué información se necesita para probar la identidad de una persona. Muchos sistemas dependen de 'documentos base', como certificados de nacimiento, y se basan en registros de nacimiento o bases de datos de población similares. Cuando estos no existen, una persona de confianza puede, a veces, sustituir a los documentos formales" (traducción propia del inglés).

## C
## Forma de medición

**Nivel** D C B A

Existen entidades de registro que cumplen con la función de **registrar** la identidad del ciudadano, las cuales no están conectadas con las entidades de registro civil.

### Factores clave de posicionamiento

Los puntos de registro para la obtención de la identidad no están conectados con los CRVS, por lo que no se pueden validar los datos biográficos directamente o el proceso de verificación es una consulta manual al CRVS.

**Nivel** 


Existen entidades de registro que cumplen con las funciones de **registrar** y **validar** la identidad del ciudadano contra los datos del registro civil pero tienen cobertura limitada.

**Factores clave de posicionamiento**

- Existencia de puntos de registro desplegados en las principales ciudades del país, que se encuentran integrados con sistemas de verificación biográficos, ya sea con conexión a CRVS u otros censos.
- La red de puntos de registro no está al alcance de toda la ciudadanía debido a que parte de la población no dispone de un punto cercano; por ejemplo, localidades de tamaño medio o pequeño no tienen un punto de registro.

**Nivel** 


Existen entidades de registro que cumplen con la función de **registrar**, **validar** y **emitir** mecanismos de identidad al ciudadano.

**Factores clave de posicionamiento**

- Existencia de puntos de enrolamiento desplegados en todo el territorio nacional con puntos cercanos a cualquier núcleo de población. El proceso de enrolamiento permite captar de forma masiva a los usuarios y en el proceso de verificación y emisión no se tienen rechazos o son despreciables.

**Nivel** 


Existe una red de entidades de registro que a nivel de competencias y funciones tienen la capacidad de realizar todas las actividades relacionadas con los procesos de **registro**, **validación**, **emisión** y **actualización**.

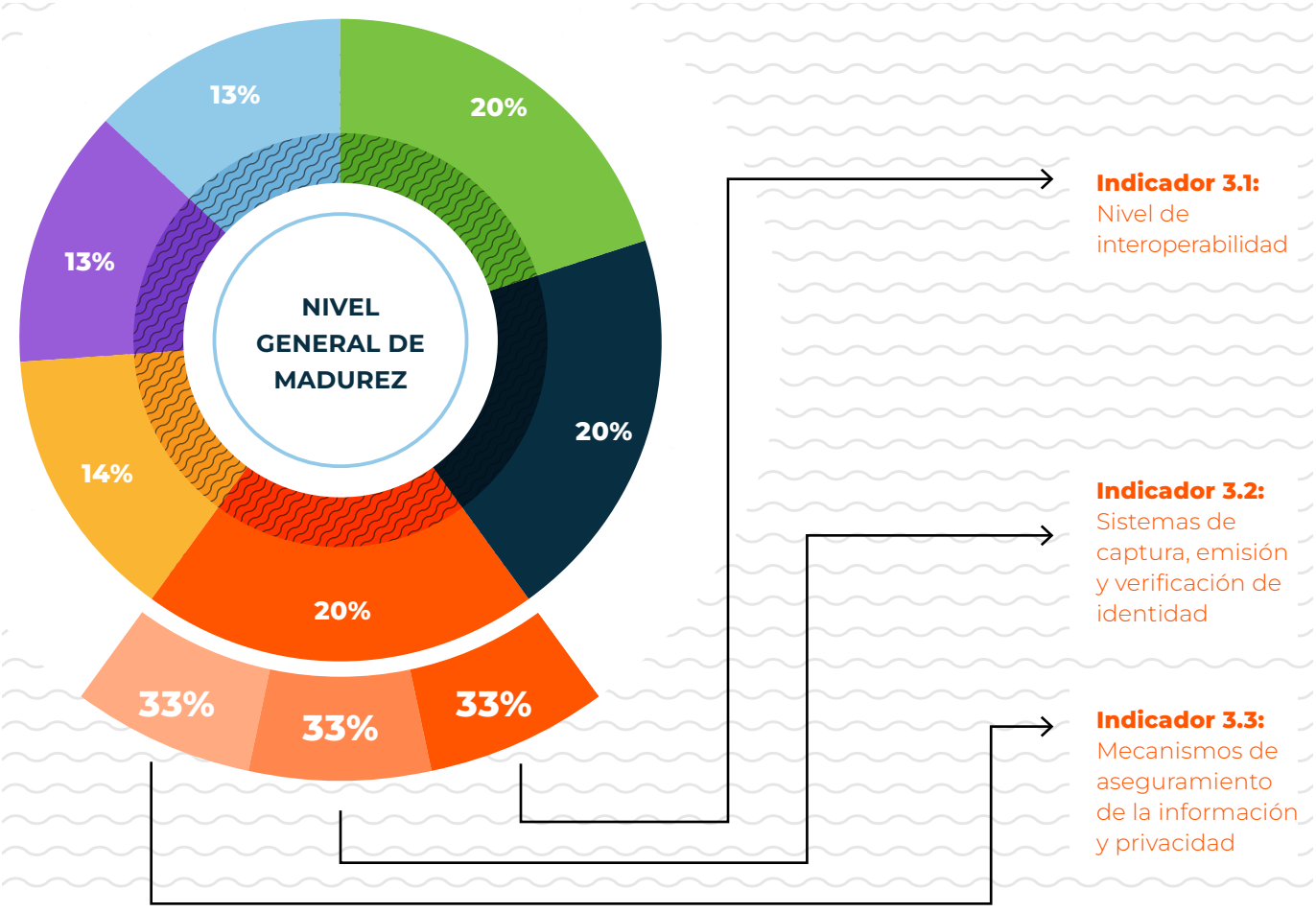
**Factores clave de posicionamiento**

- La operación de las entidades de registro es sólida, madura y consolidada.
- El sistema de enrolamiento desplegado tiene una tasa de no éxito de la emisión menor de un 0,01% (uno de cada 10.000) de las ocasiones, es decir, existe un muy bajo número de solicitudes de registro que no concluyen en la emisión de una identidad.
- La trazabilidad de los actos civiles del ciudadano se encuentra garantizada en la base de datos centralizada e interconectada con las instituciones encargadas del registro civil.

# 3.3. DIMENSIÓN 3: SISTEMAS Y TECNOLOGÍA

La dimensión 3, **Sistemas y tecnología**, tiene un peso del 20% dentro del Modelo de Madurez, y está compuesta por tres indicadores: 3.1: **Nivel de interoperabilidad**, 3.2: **Sistemas de captura, emisión y verificación de identidad**, y 3.3: **Mecanismos de aseguramiento de la información y privacidad**. Los tres indicadores tienen el mismo peso dentro de la dimensión, es decir, el 33%.

**Gráfico 3.3.**
Peso de la dimensión Sistemas y tecnología y de sus tres indicadores



# **Indicador 3.1:** Nivel de interoperabilidad

## A

## Definición del indicador

Existencia de características tecnológicas que interoperan el ecosistema de identidad, soportando todos los procesos del ciclo de vida de la identidad: registro, validación, emisión, uso y actualización de la identidad.

## B

## Justificación de uso

Uno de los retos más importantes en los sistemas de identificación es asegurar la interoperabilidad en todo el ciclo de vida, a través de organismos e instrumentos de coordinación que diseñan y definen el uso de estándares internacionales aplicables a sistemas de identificación de cualquier país. El uso de estos estándares internacionales permite garantizar la interoperabilidad de la tecnología utilizada, incluso hasta niveles que traspasan las fronteras nacionales.

Existen organismos internacionales y también países que han realizado esfuerzos en materia de diseño de estándares de aplicabilidad. A continuación, se presentan algunos ejemplos:

- El Comité Europeo de Normalización (CEN) y el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) de los Estados Unidos, al igual que organizaciones privadas como la Organización Internacional de Normalización (ISO, por sus siglas en inglés), OpenID Foundation, FIDO Alliance, Global System for Mobile Communications (GSMA) y Secure Identity Alliance, entre otras, tienen el objetivo de incrementar la interoperabilidad de los sistemas de identificación, construyendo o definiendo estándares aplicables.

- En ese sentido, existen países que cuentan con entidades que regulan y aseguran que los diferentes proveedores de servicios de identidad sigan estos estándares durante el ciclo de vida de la identidad (como T-Scheme en el Reino Unido). Adicionalmente, hay organizaciones e instrumentos supranacionales, como el Comité Europeo de Protección de Datos (CEPD) y eIDAS, que establecen los requerimientos mínimos que los países miembros deben cumplir para asegurar la interoperabilidad de sus sistemas, introduciendo en este concepto el nivel de madurez más alto para este indicador, es decir, la interoperabilidad transfronteriza del sistema de identidad de un país.

Por otro lado, el uso de estándares de encriptación de datos, intercambio de información, biometría y otros hace posible que sistemas externos puedan verificar la información del sistema de identidad y utilizarlo en transacciones. Ello dependerá de la tecnología utilizada para la emisión de la identidad y de los mecanismos de enrolamiento que se empleen, así como de si se utiliza biometría en el proceso o se emiten tarjetas inteligentes (*smart card*) o similares para la generación de la identidad.

A continuación, se listan los estándares que corresponden a un estadio maduro, tanto para los sistemas que utilizan biometría como para los que utilizan credenciales físicas.

En el caso de países que utilicen sistemas biométricos, existen estándares de mayor alcance internacional y cobertura.

**Estándares relacionados con el intercambio de información biométrica**

- **ISO/IEC 19794 (https://www.iso.org/standard/50862.html).** Formato de intercambio de datos biométricos. Es una familia de estándares (del 1 al 11) que definen los formatos y mecanismos de intercambio para distintos datos biométricos. A modo de ejemplo, el 19794-2 define cómo se almacenan e intercambian datos de minucias de huellas dactilares, mientras que el 19794-5 aplica a los datos de imágenes del rostro y el 19794-6 a datos de iris. Es un estándar muy importante para mantener la interoperabilidad entre sistemas.

- **ISO/IEC 19785:2020 (https://www.iso.org/standard/77892.html).** Este estándar define los mecanismos de comunicación entre sistemas biométricos.

**Estándares relacionados con la evaluación de sistemas biométricos**

- **ISO/IEC 19795.** En este documento se establecen principios generales para probar el rendimiento de los sistemas biométricos en términos de tasas de error y tasas de rendimiento, con, entre otros, los siguientes fines: medición del rendimiento, predicción del rendimiento, comparación del rendimiento y verificación de la conformidad con los requisitos de rendimiento especificados.

- **ISO/IEC 29109.** En este documento se especifican los elementos de la metodología de prueba de conformidad, las pruebas de consistencia y los procedimientos de prueba aplicables a las imágenes faciales bidimensionales definidas en el estándar de formato de intercambio de datos biométricos ISO/IEC 19794-5: 2005 para datos de imágenes faciales.

**Estándares relacionados con la seguridad y la privacidad**

- **ISO/IEC 24745.** Contiene orientaciones para la **protección de la información biométrica** en virtud de diversos requisitos de confidencialidad, integridad y renovabilidad/revocabilidad durante el almacenamiento y la transferencia. Asimismo, especifica requisitos y pautas para la gestión y el procesamiento seguro y compatible con la privacidad de la información biométrica.

- **ISO/IEC 29100.** Proporciona un marco de privacidad que especifica una terminología de privacidad común; define a los actores y sus roles en el procesamiento de información de identificación personal (PII, por sus siglas en inglés); describe las consideraciones de protección de la privacidad; e incluye un conjunto de referencias a los principios de privacidad usados para la tecnología de la información.

- **ISO/IEC 19989.** En este documento se presenta el marco general para la evaluación de la seguridad de los sistemas biométricos, incluidos los componentes funcionales de seguridad.

- **ISO/IEC 30107.** El propósito de este documento es proporcionar una base para la detección de ataques de presentación (PAD, por sus siglas en inglés). Esto mediante la definición de términos y el establecimiento de un marco a través del cual puedan especificarse y detectarse tales eventos, así como clasificarse, detallarse y comunicarse para la toma de decisiones posteriores y las actividades de evaluación de rendimiento.

**Estándares relacionados con la calidad**

- **ISO/IEC 29794 (https://www.iso.org/standard/79519.html).** Es una familia de estándares que especifica criterios de calidad para obtener **muestras biométricas**. A modo de ejemplo, el estándar **29794-5** especifica criterios para la **imagen del rostro** y el **29794-6** para el **iris**.

**Estándares relacionados con las credenciales físicas**

Para los países en los que sus sistemas de identificación estén basados en la emisión de una credencial física, los estándares internacionales que proveen una mayor madurez son los siguientes:

- **ISO/IEC 7810.** Es el estándar que define las características físicas de las tarjetas de identidad y aplica a todas las tarjetas (con y sin chip): "Es una de una serie de normas que describen las características de las tarjetas de identificación. La finalidad de la ISO/IEC 7810:2003 es proporcionar los criterios a los que deben ajustarse las tarjetas y especificar los requisitos para que dichas tarjetas sean utilizadas en intercambios internacionales. Tiene en cuenta tanto los aspectos humanos como los mecánicos y establece los requisitos mínimos" (traducción propia del inglés).

- **ISO/IEC 7816-X.** Esta familia especifica las características de las tarjetas de identidad con contacto.

- **ISO/IEC 14443.** Es un estándar internacional relacionado con las tarjetas y dispositivos de seguridad de identificación personal electrónicas, en especial las tarjetas de proximidad[9] (tarjetas sin contacto).

- **Organización de Aviación Civil Internacional (ICAO) 9303 (ISO/IEC 7501).** Es un estándar necesario si se adiciona el atributo de utilizar la credencial como documento de viaje, lo que permite que pueda ser leído y verificado de forma automática en el paso de las fronteras (Machine Readable Travel Documents [MRTD]).

9. Más información disponible en: **https://es.wikipedia.org/wiki/ISO_14443**.

### Estándares relacionados con las credenciales virtuales

- **Federal Information Processing Standards (FIPS) 186-5 (febrero 2023).** Es un estándar de los Estados Unidos pero que se utiliza a nivel mundial.[10] Esta norma especifica un conjunto de algoritmos que pueden utilizarse para generar una firma digital. Las firmas digitales se emplean para detectar modificaciones no autorizadas en los datos y autenticar la identidad del firmante. Además, el destinatario de los datos firmados puede utilizar una firma digital como evidencia para demostrar a un tercero que la firma fue generada efectivamente por el firmante declarado. Esto se conoce como no repudio, ya que el firmante no puede repudiar fácilmente la firma en un momento posterior.

- **FIPS PUB 180-4.** Es una norma que especifica algoritmos de *hash* (SHA-1, SHA-512/256, etc.) que pueden utilizarse para generar resúmenes de mensajes. Los resúmenes se utilizan para detectar si los mensajes han sido modificados desde que se generaron los resúmenes.

- **FIPS 140-2.** Es un estándar de seguridad de ordenadores del gobierno de los Estados Unidos para la acreditación de módulos criptográficos.[11]

- **RFC 3447 - PKCS #1.** Es el primero de una familia de estándares, llamados estándares de criptografía de clave pública (**PKCS**, por sus siglas en inglés), publicados por RSA Laboratories. El estándar proporciona las definiciones básicas y recomendaciones para implementar el algoritmo **RSA** para criptografía de clave pública. Define las propiedades matemáticas de las claves públicas y privadas, las operaciones primitivas para el cifrado y las firmas, esquemas criptográficos seguros y representaciones relacionadas de la sintaxis ASN.1.

- **ITU-T X.509 | ISO/IEC 9594-8.** Aborda algunos de los requisitos de seguridad en las áreas de autenticación y otros servicios de seguridad mediante la provisión de un conjunto de marcos sobre los cuales se pueden basar servicios completos. Específicamente, esta recomendación o norma internacional define marcos para:

  → Certificados de clave pública.

  → Certificados de atributos.

C

## Forma de medición

**Nivel** D C B A

Los sistemas que soportan el ciclo de vida de la identidad son operados de manera analógica, lo cual no posibilita o no incorpora ninguna tecnología que permita interoperabilidad.

10. Puede leerse más en: **https://csrc.nist.gov/pubs/fips/186-5/final.**
11. Visítese **https://es.wikipedia.org/wiki/FIPS_140-2** para más información.

**Factores clave de posicionamiento**

- El ciclo de vida de la identidad se realiza en su totalidad en formatos de papel.
- En la fase de registro no se realiza ninguna verificación biográfica con bases de datos centralizadas para validar la identidad del usuario ni tampoco se obtienen muestras biométricas del usuario para mejorar los procesos de deduplicación de información.
- En la fase de emisión no se entrega ningún mecanismo de identificación al usuario que cuente con algún tipo de tecnología que permita a terceros usuarios verificar la información de la identidad, como, por ejemplo, la entrega de una tarjeta física o virtual, con códigos de barras, la entrega de una *smart card* criptográfica o similar.

**Nivel** 


Los sistemas que soportan los procesos del ciclo de vida de la identidad contienen elementos tecnológicos que posibilitan la interoperabilidad con terceros sistemas; sin embargo, estos mecanismos están basados en protocolos propios no reconocidos. Alternativamente, alguna de las fases de registro, validación, emisión y actualización se realiza de forma analógica para algún caso de uso. En otras palabras, existen procesos que siguen siendo manuales.

**Factores clave de posicionamiento**

- En la fase de registro se realiza el registro de la identidad mediante la captura de huellas dactilares u otros mecanismos biométricos, pero los mecanismos no siguen los estándares internacionales y, por lo tanto, son solo explotables por el propio sistema.
- El proceso de validación se realiza mediante consultas a sistemas centralizados (como CRVS) o mediante la presentación y verificación de documentos de identidad. No existe, en este caso, verificación biométrica.
- En la fase de emisión se entrega al ciudadano algún mecanismo (*smart card*, tarjeta plástica con códigos de barras, aplicaciones con códigos de barras, etc.) que permite a terceros usuarios verificar la veracidad del documento y los datos que en él se presentan, tanto en procesos fuera de línea (*offline*) como en procesos en línea (*online*). Esta identidad está basada en un sistema propietario no reconocible por terceros a través del uso de estándares.
- La fase de emisión de la identidad le puede generar al usuario una identidad digital que no está basada en estándares ni en algoritmos criptográficos con atributos de seguridad para la interoperabilidad con otros sistemas o plataformas, sobre todo en internet.

**Nivel** 


Los sistemas que soportan los procesos del ciclo de vida se basan en estándares internacionales, lo cual permite la interoperabilidad con terceros sistemas; sin embargo, sus diseños no cuentan con capas de interoperabilidad o bus de comunicación con terceros sistemas basados en estándares.

**Factores clave de posicionamiento**

- En la fase de emisión, siguiendo las buenas prácticas y estándares internacionales, se entrega al ciudadano una identidad digital basada en Mobile ID y/o *smart card*, que cumple en cualquiera de las dos opciones con estándares en el tipo de dispositivo y chips, y con formatos de:
  - → Almacenamiento de información.
  - → Estructura de datos y formato.
  - → Protocolo de intercambio (definidos en el punto de justificación).
- Aunque el modelo implementa los estándares de la industria para la emisión de la identidad, y en particular de la identidad digital, en el diseño del sistema no existe un componente específico de interoperabilidad que permita conectar el sistema con terceros sistemas de identificación de otros países. Tampoco posibilita que el ecosistema de actores públicos y privados pueda hacer crecer el número de aplicaciones que utilicen el sistema, conectándose a la capa de interoperabilidad y a las interfaces de programación de aplicaciones (API, por sus siglas en inglés) definidas.

**Nivel** D C B A

Los sistemas que soportan los procesos del ciclo de vida cuentan con una capa de interoperabilidad basada en estándares internacionales o están conectados con capas de interoperabilidad de entidades supranacionales que permiten el uso y autenticación de la identidad y la verificación transfronteriza.

**Factores clave de posicionamiento**

- El sistema de identidad incorpora en el diseño una capa de interconectividad que permite explotar el sistema desde terceras aplicaciones y conectar con terceros sistemas de identificación. De esta manera, se obtiene un mecanismo de autenticación y verificación cruzada entre sistemas de identificación de diferentes países.
- El diseño del sistema de identidad incluye una capa de interconectividad debido a que está construido siguiendo estándares (OpenID connect, por ejemplo) o, en un mejor escenario, está basado en redes privadas que utilizan *frameworks* descentralizados o distribuidos como tecnología central y tecnología de infraestructura de llave pública (PKI, por sus siglas en inglés) para la emisión de las identidades de los ciudadanos. Estas capas de interoperabilidad las proporciona el propio modelo del país o, en su defecto, están conectadas a redes supranacionales, como sería el caso de eIDAS.

# **Indicador 3.2:** Sistemas que dan soporte a los procesos del ciclo de vida

## A

## Definición del indicador

Capacidad sistémica de los mecanismos utilizados para los procesos del ciclo de vida de la identidad para el ciudadano.

## B

## Justificación de uso

La capacidad tecnológica de los sistemas de identificación se medirá de acuerdo a cada fase del ciclo de vida de identidad —registro, validación (prueba de identidad), emisión, uso y actualización—, y sobre la base de prácticas internacionales registradas en iniciativas como Identificación para el Desarrollo (ID4D, por sus siglas en inglés) del Banco Mundial, *Digital Identity Guidelines: Enrollment and Identity Proofing Requirements* del NIST (2017) y eiADS de la UE, entre otros.

- **Registro:** el usuario solicitante entrega la documentación e información necesaria para acreditar que él es el acreedor de dicha identidad (datos biográficos, documentos en papel que acrediten su identidad, mecanismos electrónicos de validación de identidad, respuestas a cuestionarios, etc.). Por su parte, el funcionario encargado de la tarea de registro captura el resto de la información necesaria para crear la identidad del usuario solicitante, como datos biográficos adicionales y datos biométricos (huella biométrica, firma autógrafa, iris, biometría facial, etc.).

  La información que se capture en este momento permitirá medir el Modelo de Madurez e integridad de un sistema de identidad, así como el grado de utilidad e interoperabilidad con otros sistemas, tanto a nivel nacional como internacional (Banco Mundial y GSMA, 2016). Los sistemas de menor madurez serán los basados en sistemas en papel y que no capturen información biométrica del usuario.

- **Prueba de identidad:** la unicidad de un registro es una de las características básicas de un sistema de identidad, para lo cual se utilizan procesos para purgar información duplicada y verificar la autenticidad de la información suministrada. Este proceso ha evolucionado significativamente: en el pasado el sistema consistía en la validación basada en papel en la que se cruzaban datos demográficos entre diferentes fuentes de información, lo que hacía que el proceso fuera lento y con muchas posibilidades de falsificación, o incluso resultara imposible identificar a una persona. Actualmente, en países de mayor madurez, este mecanismo utiliza sistemas de verificación biométrica, lo que evita duplicidades, falsificaciones y búsqueda automatizadas.

- **Emisión:** uno de los aspectos más importantes para medir el grado de madurez de un sistema es la tecnología utilizada para la emisión de dicha identidad. Los sistemas menos maduros se basan en modelos en papel, pasando por sistemas basados en *smart card*, hasta llegar a los más maduros, que integran las tecnologías que permiten portabilidad móvil del mecanismo de identificación (por ejemplo, Mobile ID) o el almacenamiento en la nube (Cloud ID), incluso con capacidades de descentralización de los procesos de emisión y validación.

- **Uso:** un sistema maduro será aquel que permita al usuario utilizar su sistema de identidad de forma electrónica. En este sentido, el grado de madurez de un sistema de identidad será determinado por la seguridad y usabilidad que dicho mecanismo ofrece al ciudadano. En este ámbito, la capacidad tecnológica está directamente asociada con el uso de estándares o normas que definen los niveles de garantía o integridad de los sistemas de identificación. Estándares como la ISO/IEC 29115:2013 o la reglamentación de la UE eIDAS pueden ser usados como referencia.

- **Actualización:** cuando los datos que forman parte del registro de la identidad cambian, es necesario actualizarlos. Esto en general no se realiza al momento de la modificación, sino que se aprovecha la instancia de renovación de credenciales para hacerlo. Un sistema maduro debería realizar esta operación de actualización luego de una verificación exhaustiva de que la persona es la titular de los datos que están siendo modificados. Es usual, por ejemplo, que en este proceso se realice una verificación biométrica del titular.

De acuerdo a estos niveles establecidos, se podrá identificar el grado de seguridad de los sistemas de identificación y, por lo tanto, la capacidad de uso para un mayor número de operaciones a ser realizadas por los ciudadanos. La premisa será: a menor riesgo, mayor capacidad de aplicación a usos de cualquier sector y a cualquier tipo de transacción.

C

## Forma de medición

**Nivel** D C B A

Las fases de registro, validación, emisión o actualización se realizan de forma analógica.

### Factores clave de posicionamiento

- En el proceso de registro la información suministrada por el usuario se basa en formularios en papel, y luego es validada de forma manual con información demográfica o biográfica de otras entidades.

- El proceso de registro no incorpora ningún mecanismo biométrico.

- El documento de identificación emitido está basado en un documento en papel que no incorpora ninguna tecnología, como *smart card* o códigos de barras, que permitan automatizar los procesos de verificación de la identidad, ya sea en procesos presenciales como electrónicos.

- No se dispone de un único identificador o número único representativo de la identidad del usuario y sus diferentes tecnologías.

**Nivel** 


Los mecanismos de **registro** y **validación** se realizan tanto de forma **analógica** como de forma **electrónica**.

### Factores clave de posicionamiento

- Los procesos de registro están basados en un sistema electrónico que almacena la información registrada en una base de datos de información demográfica que posibilita su consulta por terceras partes.

- En la fase de registro se le genera al ciudadano un número único para que pueda utilizarse como único identificador (independientemente de que existan heterogéneos sistemas de identificación en diferentes sectores o usos).

- La validación de la información suministrada se realiza mediante un proceso manual, debido a que se debe verificar la información almacenada en diferentes fuentes y el proceso no es electrónico.

- Se emite un documento físico que incorpora mecanismos técnicos que permiten verificar de forma automatizada la veracidad del mismo, tanto en procesos presenciales como electrónicos (códigos de barras u otros mecanismos similares). Este documento físico está basado en una tarjeta de PVC, Teslin u otras, en las que se inserta el número único de identificación (UIN, por sus siglas en inglés) y otros datos básicos ya sea mediante bandas magnéticas o códigos de barras. El documento debe incorporar algún mecanismo de seguridad físico, como hologramas, guilloché, tintas UV, etc., para evitar, en la medida de lo posible, falsificaciones.

- No se dispone de una completa identidad digital que permita al usuario realizar transacciones electrónicas.

**Nivel** 


Los mecanismos de registro, validación y emisión se realizan de forma electrónica, y puede optarse por las siguientes tecnologías: *smart card*, Cloud ID o Mobile ID.

### Factores clave de posicionamiento

- En el proceso de emisión se le genera al ciudadano una identidad física y una identidad digital, por alguno de los siguientes mecanismos:

  → *Smart card* (comunicación de campo cercano [NFC, por sus siglas en inglés] con contacto o sin contacto).

  → Cloud ID.

  → Mobile ID.

- El proceso de prueba de identidad incorpora mecanismos tecnológicos que producen un riesgo de falsa identidad mínimo o nulo, lo cual implica que no existan altas tasas de no verificación de identidad o de falsas identidades generadas. Por ejemplo, deduplicación biométrica y/o biográfica.

- Toda la evidencia entregada por el usuario para conformar su identidad (partida de nacimiento, pasaporte, etc.) es validada en forma electrónica contra la entidad emisora de dicho documento para comprobar su veracidad.

- La tecnología de generación de la identidad está basada en mecanismos que aseguren la integridad y no repudio de la identidad, como por ejemplo, una PKI.

**Nivel** 


Los mecanismos de registro, validación y emisión se realizan de forma electrónica. En la emisión el ciudadano puede, además de obtener una credencial física, optar por algún otro mecanismo de identificación, por ejemplo, Cloud ID o Mobile ID. Además, los procedimientos de emisión y validación se realizan mediante la aplicación de tecnologías descentralizadas.

**Factores clave de posicionamiento**

- Existe un mecanismo entre el registro civil y el registro de identidad por el cual el identificador único asociado a la identidad (y emitido por el registro de identidad) queda unívocamente asociado a la partida de nacimiento del registro civil. Ejemplos de esto son los procesos de certificado de nacido vivo de Perú y Uruguay.

- La identidad digital generada incorpora la tecnología de Mobile ID o Cloud ID, lo que permite al usuario realizar transacciones en sistemas electrónicos mediante dispositivos móviles o cualquier otro medio electrónico, sin depender de lectores o *drivers* específicos, complejos de utilizar.

- El sistema cuenta con capacidades de descentralización de los procesos de emisión y validación, lo cual permite evolucionar hacia los conceptos de identidad autogestionada.

- La identidad generada integra funcionalidades adicionales a la identidad, lo que permite la utilización de la identidad para otros usos. Por ejemplo, si se implementa el estándar ICAO 9303 se podría utilizar la credencial como documento de viaje, al permitir que pueda ser leído y verificado de forma automática en el paso de las fronteras (MRTD).

- En los casos en que el registro de identidad interopera con los registros de, por ejemplo, nacidos vivos o registro civil, este número puede generarse incluso antes del momento del registro, y quedar “reservado” hasta el momento en que se realice el registro.

# **Indicador 3.3:** Mecanismos de aseguramiento de la información y privacidad

## A
## Definición del indicador

Existencia de mecanismos tecnológicos que aseguren no solo la protección de datos personales, sino que permitan garantizar el nivel de confianza de la identidad durante todo el ciclo de vida de la misma.

## B
## Justificación de uso

Desde el punto de vista de la seguridad es crítico contar con mecanismos de **captura**, **almacenamiento** e **intercambio de información sensible**, que se basen en principios y políticas de privacidad frente a terceras partes.

Antes de aplicar estos mecanismos, es necesario establecer los metadatos obligatorios que debe incorporar el sistema y, en su caso, los metadatos extendidos opcionales que podrían ser utilizados por otros sistemas que requieran la identidad, como servicios de e-salud, licencia de conducir y votaciones, entre otros. Esta selección se debe realizar bajo el enfoque de finalidad del servicio que se quiera prestar, de manera que no se custodien datos que no tengan relación directa con este.

Por ejemplo, en el Reglamento eIDAS (2015/1501) (Comisión Europea, 2015) la UE establece los metadatos obligatorios que un sistema de identidad debe solicitar, custodiar y compartir para personas naturales (nombres, apellidos, fecha de nacimiento y UIN) y atributos adicionales (como lugar de nacimiento de los padres, lugar de nacimiento, género y dirección actual).

Uno de los mecanismos para garantizar la privacidad del dato es la aplicación de estándares. A continuación, se mencionan algunos ejemplos:

- La norma **ISO/IEC 29115** proporciona a los sistemas de identificación un *framework* que permite asegurar los niveles de garantía de la identificación electrónica en relación a la confianza que merecen los procesos, las actividades de gestión y tecnologías utilizados para establecer y gestionar de forma efectiva la identidad de una entidad para su uso en las transacciones de autenticación de sus ciudadanos.

- La norma **ISO/IEC 29100:2011** provee un marco de trabajo de alto nivel para la protección de la PII que les permite a las organizaciones la definición de sus requerimientos de protección de la privacidad mediante la especificación de una terminología común, la definición de actores y sus roles en el procesamiento de datos, los requerimientos de privacidad y la referencia de una serie de principios orientados a la gestión de los aspectos organizativos, técnicos y procedimentales de esta estrategia.

C

## Forma de medición

Para el análisis de esta dimensión, se ha optado por hacer una fuerte correlación entre los niveles de garantía del estándar ISO/IEC 29115 con los niveles del Modelo de Madurez.

**Nivel** 


No se dispone de políticas documentadas ni de tecnologías para la protección de la información.

### Factores clave de posicionamiento

- Para la emisión del mecanismo de identificación y su uso se utilizan metodologías, procesos y tecnologías del nivel 1 de la ISO/IEC 29115.

**Nivel** 


Se disponen de mecanismos tecnológicos para la protección de la información pero no se basan en estándares.

### Factores clave de posicionamiento

- Para la emisión del mecanismo de identificación y su uso se utilizan metodologías, procesos y tecnologías del nivel 2 de la ISO/IEC 29115.
- La información confidencial almacenada en las bases de datos no incluye texto plano.
- La información almacenada no debe contener contraseñas que permitan acceder a la credencial del usuario.

**Nivel** 


Los mecanismos tecnológicos para la protección de la información están basados en estándares, como ISO/IEC 29115, o recomendaciones, como eIDAS.

### Factores clave de posicionamiento

- Para la emisión del mecanismo de identificación y su uso se utilizan metodologías, procesos y tecnologías del nivel 3 de la norma ISO/IEC 29115.
- Las políticas para la protección de la información están basadas en estándares, como el ISO/IEC 27001.

**Nivel** 


Los mecanismos tecnológicos para la protección de la información están implementados bajo los principios de privacidad por diseño y nivel 4 ISO/IEC 29115, el cual garantiza el máximo nivel de seguridad para transacciones que así lo requieran.

### Factores clave de posicionamiento

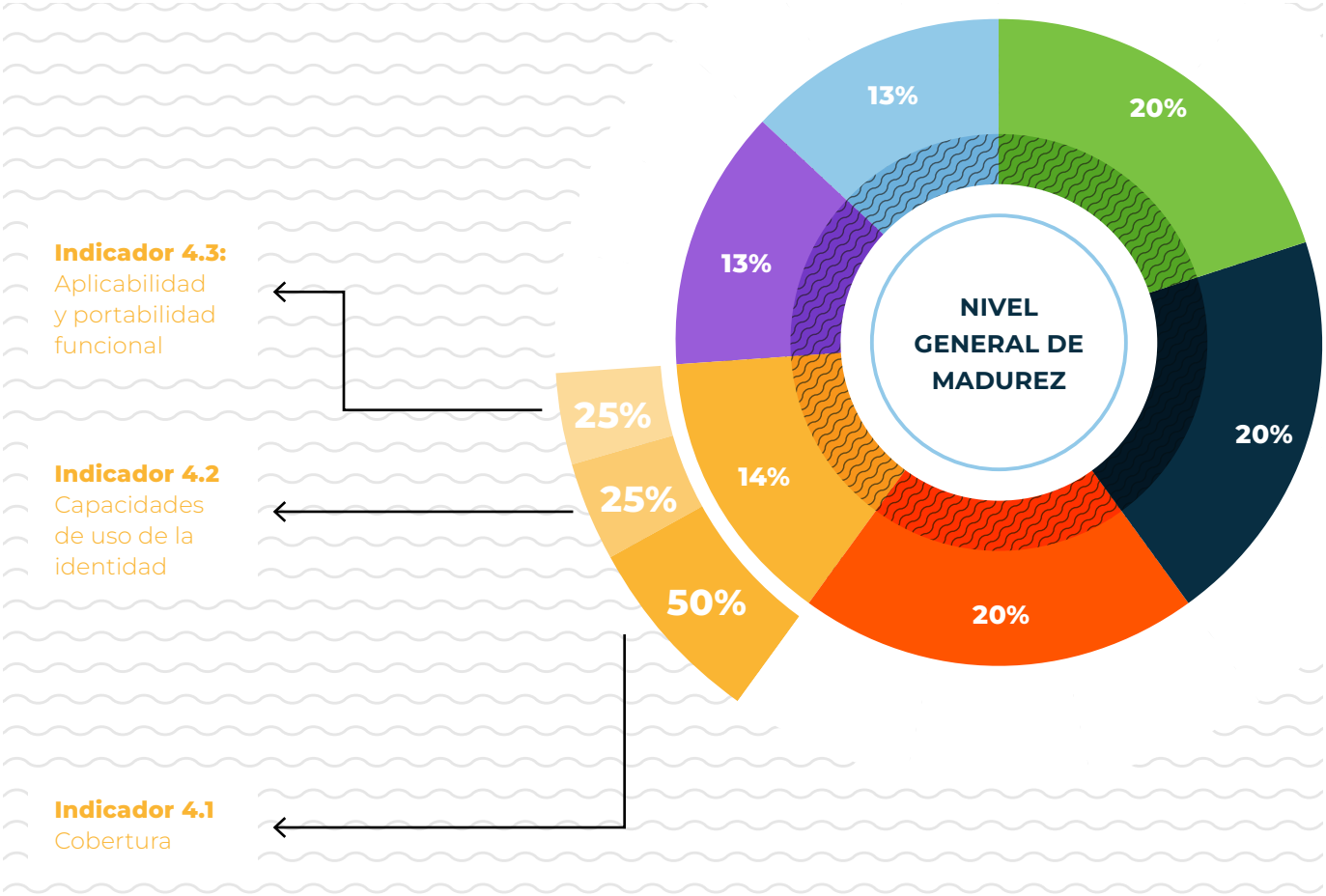
- Para la emisión del mecanismo de identificación y su uso se utilizan metodologías, procesos y tecnologías del nivel 4 de la ISO/IEC 29115.

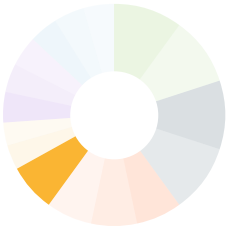
- El sistema cumple con los siguientes principios de diseño:
  - → Los datos capturados son los **mínimos** indispensables para el uso del sistema (proporcionalidad y riesgo mínimo).
  - → Los datos de la identidad almacenados están segregados o separados (por ejemplo, los identificadores están separados de los metadatos de identidad como nombre, apellido)
  - → No se deja rastro de las transacciones que terceros pudieran utilizar para recuperar información del usuario.
  - → Derecho al olvido: supresión, bloqueo o desindexación de información que se considera cierta pero obsoleta o no relevante por el transcurso del tiempo.
  - → Derecho al acceso a información pública: una persona puede buscar, solicitar y recibir información pública.
- Se pueden realizar transacciones pseudoanónimas o anónimas.

# 3.4. DIMENSIÓN 4: USO Y CAPACIDADES DE LA IDENTIDAD

La dimensión 4, **Uso y capacidades de la identidad**, tiene un peso del 14% dentro del Modelo de Madurez, y está compuesta por tres indicadores: 4.1: **Cobertura**, 4.2: **Capacidades de uso de la identidad** y 4.3: **Aplicabilidad y portabilidad funcional**. Dentro de la dimensión, el primer indicador tiene un peso del 50% mientras que los dos restantes tienen un peso del 25% cada uno.

**Gráfico 3.4.**
Peso de la dimensión Uso y capacidades de la identidad y de sus tres indicadores





# **Indicador 4.1:** Cobertura

## A
## Definición del indicador

Nivel de adopción del registro efectivo de las personas que interactúan en el ecosistema.

## B
## Justificación de uso

El desafío de obtener el mayor porcentaje de cobertura es más complejo que solo buscar emitir más registros de entidad. Está más relacionado a las consecuencias de aumentar este porcentaje y cuáles pueden ser los mecanismos o incentivos para tener mayor población identificada, ante dificultades de distinta índole, dependiendo de cada realidad nacional.

A continuación, se presentan estudios o experiencias de referencia que avalan la importancia del indicador en el nivel de madurez de los sistemas de identificación nacional:

- El Banco Asiático de Desarrollo en su reporte *Identity for Development in Asia and the Pacific* (ADB, 2016) menciona que un sistema de identidad va a incrementar su utilidad de acuerdo al porcentaje de masa poblacional que logre registrar. Sin ello, no puede mantener una inscripción ni tampoco incentivar a entidades terceras a utilizar esta información. En suma, señala que la relación entre la accesibilidad y la cobertura es directamente proporcional debido a que el aumento de población con identidad dependerá de los costos en los que se incurre para obtener un mecanismo de identificación. En un estadio intermedio de desarrollo de este indicador, sostiene que aun cuando la adquisición de una identificación (ID) es de bajo costo hacia los ciudadanos, la política gubernamental que regula el sistema es bastante costosa, por lo tanto, más dependiente de aprobación de presupuesto adicionales.

El caso de estudio del programa indio Aadhaar, realizado por la Universidad de Toronto (2016), detalla que para mayo de 2017 el 89,6% de la población del país había sido parte del proceso de enrolamiento, lo cual lo convertía en uno de los países de referencia para el indicador de cobertura. Es importante considerar que este logro se realizó en el marco de desafíos estructurales, como los culturales, la geografía compleja de su territorio y que el 70% de la población vive en áreas rurales. Asimismo, los mecanismos que se utilizaron para el despliegue de la estructura encargada del registro se basaron en la premisa de agilidad y simplicidad, de manera de buscar un proceso rápido de cara al ciudadano. Incluso en los casos de ciudadanos no alfabetos, pertenecientes a castas, se realizaron entrevistas de corta duración con los sacerdotes o jefes de castas para reconocer y otorgar una identidad a las personas pertenecientes a su comunidad. Dos de los factores de éxito del programa están directamente relacionados con los costos y mecanismos definidos para alcanzar una mayor cobertura, estos son:

- → Diseñar e implementar un proceso de enrolamiento fácil, rápido, sin ningún costo y con un número reducido de requisitos.

- → Incluir a la población con difícil acceso.

El primero de ellos se complementó con el aumento de la capilaridad de las agencias de enrolamiento a nivel nacional, de manera que el ciudadano pudiera elegir cuándo y dónde iniciar el proceso. El segundo involucró buscar iniciativas para las personas que no tenían medios probatorios de su identidad, de manera de introducir el sistema de identidad de forma paulatina en estas comunidades con dificultades de acceso, para lo cual se aceptaron en una primera instancia para el enrolamiento documentos que prueben la identidad (pasaportes, licencia de conducir y carnet de servicio militar, entre otros) o la dirección (certificado de salud, documento de trámite bancario, certificación de dirección, etc.).

- Estonia es el país de mayor referencia en este indicador debido a que su gestión de la identidad se ha enfocado en mucho más que en brindar una única identidad digital a la totalidad de sus ciudadanos, ya que también ha incluido en su ecosistema a no ciudadanos, es decir a los residentes de otras nacionalidades que tienen vínculos familiares o laborales en el país. Asimismo, otro componente positivo de su gestión es el otorgamiento de una identidad digital a través de un dispositivo móvil, como un teléfono inteligente (*smartphone*). La cobertura de población con identidad es del 98% y, actualmente, el 12% de la población estonia gestiona su identidad mediante un dispositivo móvil, es decir, autentifica su identidad para el uso de transacciones a través de un dispositivo.

C

## Forma de medición

**Nivel** 


Menos del 50% de la demografía del país cuenta con un mecanismo de identificación integrado.

### Factores clave de posicionamiento

- Las causas-raíz de este desempeño se deben a consideraciones estructurales de la sociedad del país, tales como pobreza, nivel de alfabetización, demografía, niveles de ruralidad y organización sociopolítica.

- Limitaciones en la focalización de población que no cuenta con un mecanismo de identificación.

- Diferencias sustanciales de cobertura entre grupos etarios. Por ejemplo, los porcentajes de no cobertura no son compatibles con los censos practicados en los países.

- Existencia de múltiples mecanismos de identificación del ciudadano, creados para un uso específico, por ejemplo, bautismo, votación, licencias, entre otros. Estos mecanismos no se encuentran integrados de forma tal que puedan garantizar la unicidad de la identidad.

- Utilización de mecanismos de identificación que nacen por propósitos más relacionados a la sociedad civil, como las estructuras religiosas. Estos mecanismos no se encuentran integrados de forma tal que puedan garantizar la unicidad de la identidad.

**Nivel** 


Más del 50% de la demografía del país cuenta con algún mecanismo de identificación.

**Factores clave de posicionamiento**

- Las causas-raíz de este desempeño se relacionan con la usabilidad de la identidad, es decir, ya no con la accesibilidad al registro, sino con las motivaciones que tiene el ciudadano para iniciar un proceso de registro.

- Los puntos de atención para el registro suelen tener dificultades técnicas para garantizar mayor cantidad de enrolamientos por día. Por ejemplo, pueden tener bajos estándares de calidad para la atención de los servicios, requisitos complejos para obtener la identidad o no disposición de sistemas para la emisión.

- Coexistencia constante de una única identidad con fragmentos de identidad recogidos con otro propósito, tales como procesos electorales o instituciones religiosas. Estos mecanismos no se encuentran integrados de forma tal que puedan garantizar la unicidad de la identidad.

**Nivel** 


Todos los ciudadanos del país cuentan con un mecanismo de identificación.

**Factores clave de posicionamiento**

- Hay disponibles procesos de autenticación basados en biometría.

- Se ponen a disposición mecanismos de identificación digital que se vinculan con tarjetas de identificación físicas.

- Existen aplicativos que permiten el registro de identidad en línea, como *smartphones*.

- Los procesos de registro y emisión de identidad están implementados bajo estándares de calidad.

- Existe una única identidad que hace referencia a una única base de datos que se actualiza durante el ciclo de vida del ciudadano. Esta única identidad se utiliza para uso en trámites en el ámbito público y privado.

**Nivel** 


Todos los ciudadanos y no ciudadanos (residentes) ubicados en el país cuentan con una identidad.

**Factores clave de posicionamiento**

- Mecanismos de incorporación de los no ciudadanos que también necesitan una identidad dentro del ecosistema, tales como carnet de residencia. Esta incorporación debe ser integral: la identidad para no ciudadanos debería permitir a dichas personas interactuar en el ecosistema de identidad de forma análoga a los ciudadanos.

# Indicador 4.2:
## Capacidades de uso de la identidad

A

### Definición del indicador

Posibilidad de realizar transacciones de autenticación presencial y *online*, o de llevar a cabo transacciones de firma para autorización de trámites y documentos de forma *online*. Esto se determinará por el tipo de conexión entre las entidades participantes del ecosistema y los organismos certificadores de la entidad.

B

### Justificación de uso

Uno de los retos adicionales a la gestión de la identidad digital es la usabilidad que en definitiva tiene para los usuarios finales. De ello dependerán las capacidades que se le otorguen a la identidad y, por ende, el tipo de uso que requerirá el ciudadano, así como los ambientes en los que necesitará hacerlo.

A continuación, se presentan estudios o experiencias de referencia que avalan la importancia del indicador en el nivel de madurez de los sistemas de identificación nacional:

- El Banco Asiático de Desarrollo en su reporte *Identity for Development in Asia and the Pacific* (ADB, 2016) señala que un estadio maduro de un sistema de identidad apunta a cumplir los procesos de identidad, autentificación y servicios transaccionales. De esta manera, los sistemas de identificación robustos y escalables son capaces de gestionar servicios múltiples sin comprometer el rendimiento del sistema, haciendo posible la identificación y autenticación a través del mismo número o tarjeta de identificación.

- La experiencia a nivel mundial de mayor referencia para un estadio mayor de madurez del sistema es Estonia,[12] debido a que los ciudadanos usan sus identidades digitales para distintas transacciones a nivel público y privado, tales como: trámites de migración, seguro social, firma electrónica, apertura de cuentas bancarias, voto electrónico, pago de impuestos, y hasta prescripciones médicas.

- Además, Estonia pone a disposición de sus ciudadanos la posibilidad de utilizar su ID a través de un *smartphone*, lo que evita la necesidad de una lectora física que verifique la autenticidad de la tarjeta. Incluso asociada a esta experiencia, existe una aplicación para quienes no disponen de una tarjeta SIM en sus dispositivos móviles, que se orienta sobre todo a los extranjeros. Estas buenas prácticas de usabilidad en las distintas transacciones también son aplicables para los residentes de otras nacionalidades en Estonia, quienes a través de la e-residencia pueden crear una empresa en menos de un día, declarar impuestos y realizar la apertura de una cuenta bancaria, entre otros.

12. Véase **https://e-estonia.com/solutions/estonian-e-identity/id-card/**

C

## Forma de medición

**Nivel** 


No existen mecanismos de validación en línea de las credenciales emitidas por lo que no se pueden verificar transacciones de autenticación o de firma digital. Tampoco existen mecanismos de validación de la credencial (servicio web o similar) que permita validar la autenticidad del contenido de la credencial física.

### Factores clave de posicionamiento

Existencia de códigos de barra para la autenticación a través de sistemas de verificación pero sin un servicio que permita validar la autenticidad de la credencial física.

**Nivel** 


La conexión entre las entidades participantes del ecosistema y los organismos certificadores de identidad se realiza de forma electrónica, lo que permite llevar a cabo transacciones de autenticación de forma presencial.

### Factores clave de posicionamiento

- El ciudadano utiliza mecanismos de autenticación electrónica en todo tipo de trámites electrónicos ofrecidos por el Estado o por particulares que requieran de autenticación.
- Se implementan mecanismos tales como usuario y contraseña, certificados digitales, *tokens*, preguntas reto y vinculación de contraseñas con *smartphones*.
- Se utilizan mecanismos estándar centralizados para la implementación de la firma digital (PKI), y/o mecanismos federados de autenticación, tales como OpenID o el lenguaje de marcado de confirmaciones de seguridad (SAML, por sus siglas en inglés).

**Nivel** 


La conexión entre las entidades participantes del ecosistema y los organismos certificadores de identidad se realiza de forma electrónica, lo que posibilita llevar a cabo transacciones de autenticación de forma presencial. Además, se permiten las transacciones de firma electrónica.

### Factores clave de posicionamiento

- El ciudadano titular de la tarjeta electrónica podrá utilizar su mecanismo de autenticación electrónica y firma digital en todo tipo de trámites electrónicos ofrecidos por el Estado.
- El ciudadano utiliza mecanismos de autenticación electrónica en todo tipo de trámites electrónicos ofrecidos por el Estado o por particulares (sector privado) que requieran de autenticación.

**Nivel** 


La conexión entre las entidades participantes del ecosistema y los organismos certificadores de identidad se realiza de forma electrónica, lo que posibilita realizar transacciones de autenticación de forma presencial y *online*. Además, se permiten las transacciones de firma electrónica.

### Factores clave de posicionamiento

- Utilización de mecanismos descentralizados para seguridad.

# **Indicador 4.3:** Aplicabilidad y portabilidad funcional

A

## Definición del indicador

Capacidad del ciudadano de utilizar un único mecanismo de identificación para cualquier transacción independiente de la geografía, propósito y ámbito de uso. Este mecanismo de identificación podría ser utilizado en los canales presenciales y remotos, tanto en el ámbito público como privado.

En este contexto, el término mecanismo de identificación refiere a la identidad generada y administrada dentro del ciclo de vida y no hace referencia a las distintas credenciales: un ciudadano puede validar su identidad utilizando distintas credenciales emitidas en el marco del mismo ciclo de vida.

B

## Justificación de uso

Tradicionalmente, los ciudadanos manifiestan su identidad repetidamente en distintas instituciones tanto públicas como privadas (en algunos países, este suceso se mantiene), por lo que incurren en repeticiones innecesarias de verificación y autenticación. Además de ello, en muchos ecosistemas, la identidad ha surgido en contextos más sociales, como el de la religión, los procesos electorales o la gestión de comunidades culturales más pequeñas.

Por esos motivos, uno de los retos más importantes del uso de la identidad son los ámbitos de aplicabilidad. Este indicador medirá si el mecanismo de identificación se puede utilizar para cualquier tipo de transacción pública y/o privada que lo requiera, independiente de la geografía o voluntad de uso.

Existen estudios o experiencias de referencia que avalan la importancia de este indicador en el nivel de madurez de los sistemas de identificación nacional, los cuales son los siguientes:

- En los estudios recogidos sobre el caso de India, se menciona que al inicio del despliegue del programa Aadhaar, uno de los principales retos eran los numerosos documentos de identidad presentes dentro del ecosistema de identidad. Existían identidades que habían nacido con propósitos distintos al de generar una identidad al ciudadano, muchos de ellos se referían a la casta a la que pertenecían, tarjetas de racionamiento, identificación de votantes, e incluso tarjetas de identificación emitidas por autoridades subnacionales. Cada uno de ellos tenía limitaciones en cuanto a la información, por lo que no podía servir como una identidad única, no tenían el soporte adecuado para evitar documentos fraudulentos y la usabilidad se reducía al propósito para el que fue creado.

- En el estudio elaborado por el Banco Asiático de Desarrollo (ADB, 2016) se menciona como uno de los componentes de medición

la utilidad de la identificación. En ese sentido, una de las referencias de este indicador es que un sistema de identidad maduro será capaz de proporcionar identificación, autenticación y funciones como (débito, retiro de efectivo, seguro médico, etc.) bajo el mismo número de identificación.

- Asimismo, en el documento de investigación elaborado por la Fundación Telefónica (2013) acerca de los retos de los nuevos usuarios en el mundo digital, se señala la necesidad de que el ciudadano no repita sus datos personales (distinto nivel de información demográfica) a diferentes grupos. Esta portabilidad no solo involucra la comodidad de los usuarios, sino también la eficiencia de los procedimientos que ofrecen tanto las empresas privadas como las instituciones públicas.

C

## Forma de medición

**Nivel** D C B A

El ciudadano dispone de diversos mecanismos funcionales de identidad, cuyos propósitos dependen de la geografía, objetivo y ámbito de uso.

**Factores clave de posicionamiento**

- Otorgamiento de mecanismos de identidad generados para propósitos específicos; por ejemplo, identidades otorgadas por estructuras religiosas, por autoridades subnacionales, con propósitos electorales, etc.

**Nivel** D C B A

El ciudadano dispone de diversos mecanismos funcionales de identidad, cuyos propósitos dependen de la geografía, objetivo y ámbito de uso. En algunos casos, dichos mecanismos de identidad pueden ser utilizados para más de un propósito.

**Factores clave de posicionamiento**

- Otorgamiento de mecanismos de identidad generados se retroalimentan entre sí, e identifican la información demográfica recogida que puede ser utilizada para otros ámbitos o transacciones.

**Nivel** D C B A

El ciudadano dispone de un único mecanismo de identificación que permite su uso a nivel presencial para cualquier propósito de identificación, tanto en el ámbito público como en el privado.

**Factores clave de posicionamiento**

- Otorgamiento de una única identidad al ciudadano, que cubra todo el ciclo de vida de la identidad (registro, validación, emisión, uso y actualización), desde el nacimiento hasta el mantenimiento (neonato, actos registrales y muerte), siendo este mecanismo el único para identificar los datos personales.

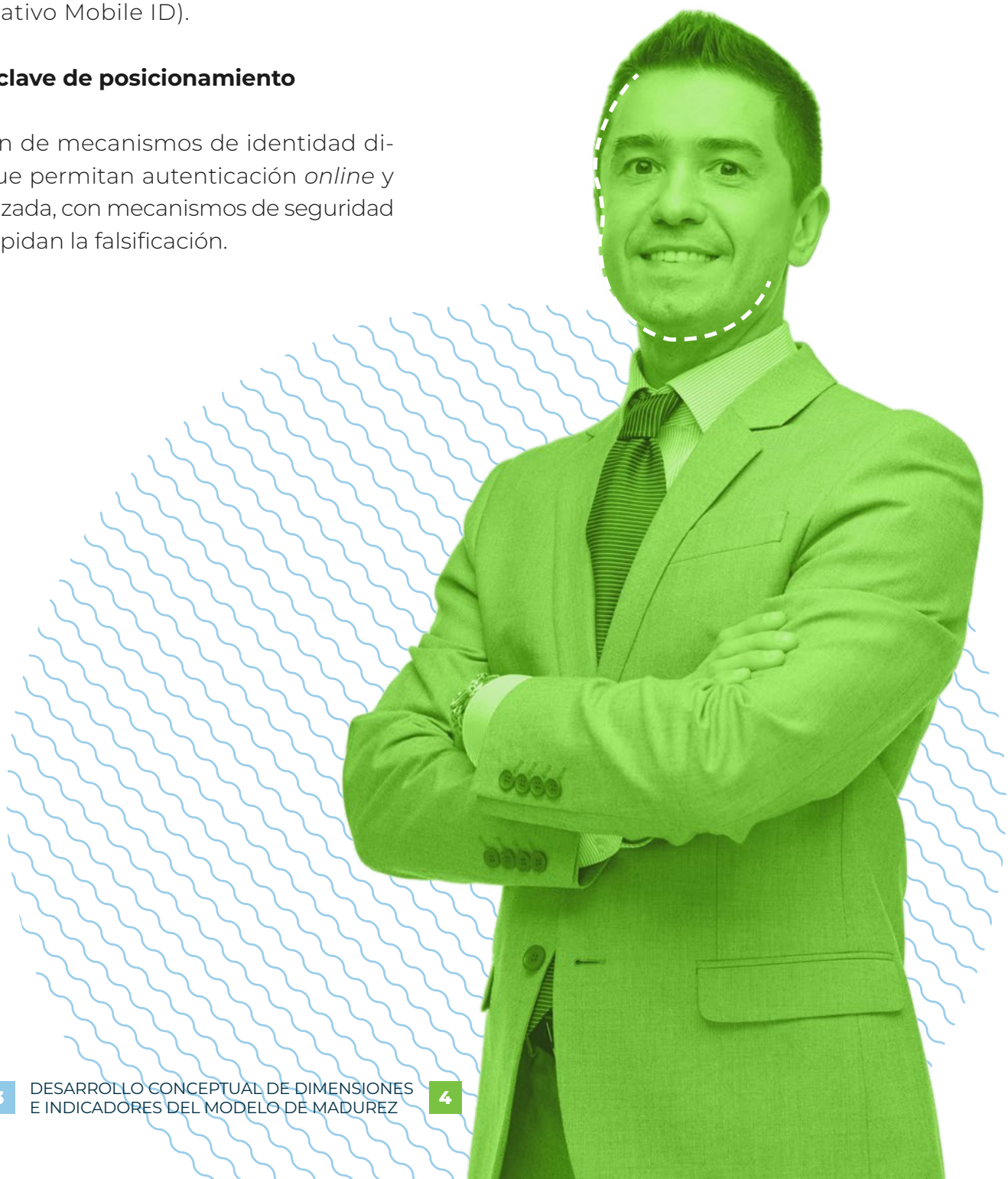
**Nivel** D C B A

El ciudadano dispone de un único mecanismo de identificación digital que permite

su uso, a nivel presencial y en remoto, para cualquier propósito de identificación, tanto en el ámbito público como en el privado. Vale aclarar que un "único mecanismo de identificación digital" no es exactamente lo mismo que una única credencial. Un sistema maduro puede tener varias credenciales pero todas ellas vinculadas a la misma identidad (por ejemplo, una tarjeta de identidad y un aplicativo Mobile ID).

**Factores clave de posicionamiento**

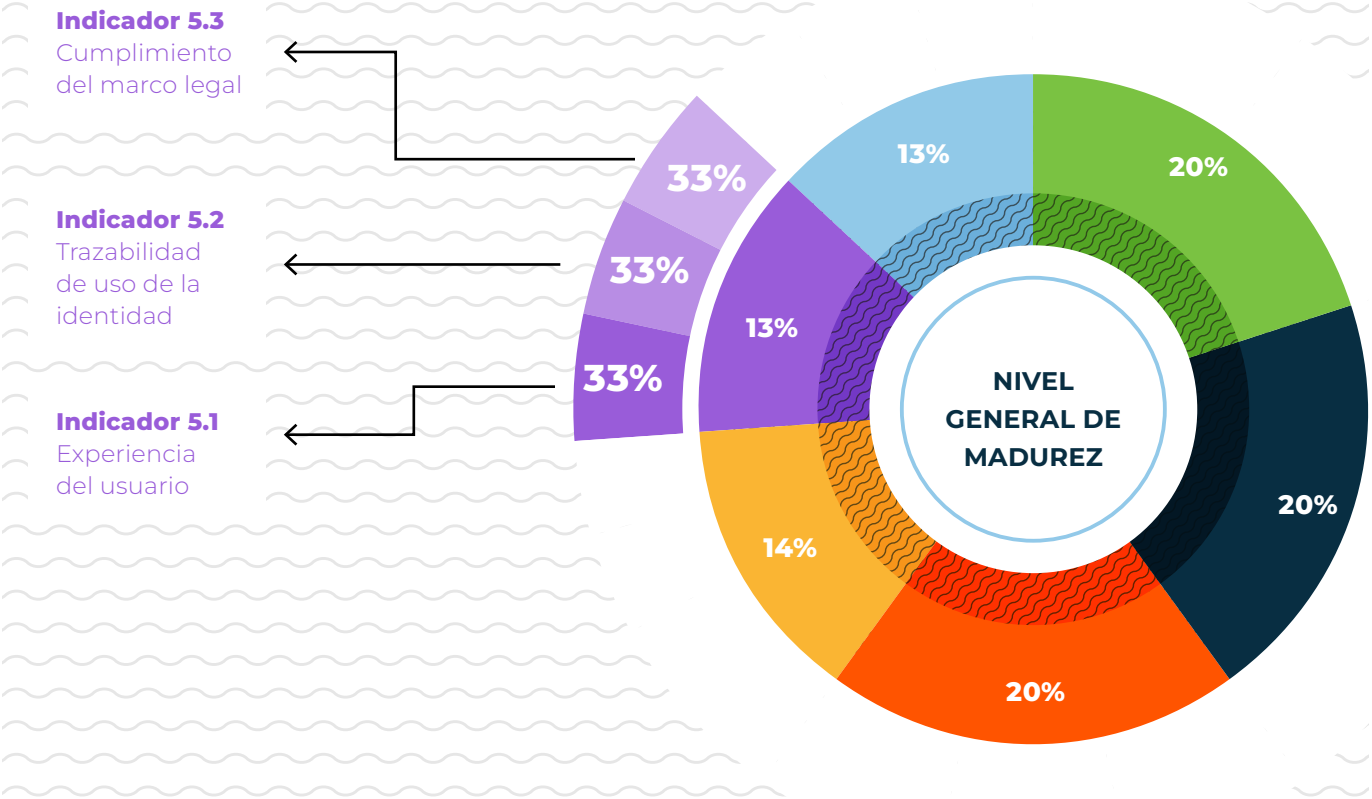
- Emisión de mecanismos de identidad digital que permitan autenticación *online* y centralizada, con mecanismos de seguridad que impidan la falsificación.
- Emisión de mecanismos de identidad que tengan el atributo de inicio de sesión único (SSO, por sus siglas en inglés), bajo estándares de autorización con el objetivo de contar con una única identidad digital a ser utilizada en distintos ámbitos y para diferentes transacciones.

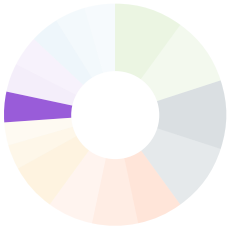


# 3.5. DIMENSIÓN 5: EXPERIENCIA DEL USUARIO

La dimensión 5, **Experiencia del usuario**, tiene un peso del 13% dentro del Modelo de Madurez, y está compuesta por tres indicadores: 5.1: **Experiencia del usuario**, 5.2: **Trazabilidad del uso de la identidad** y 5.3: **Cumplimiento del marco legal**. Los tres indicadores tienen el mismo peso dentro de la dimensión, es decir, el 33%.

**Gráfico 3.5.**
Peso de la dimensión Experiencia del usuario y de sus tres indicadores





# **Indicador 5.1:** Experiencia de usuario

## A

## Definición del indicador

Expresión de la satisfacción del usuario durante todos los procesos del ciclo de vida de la identidad.

## B

## Justificación de uso

Como servicio brindado al usuario, y por ser la identidad uno de los derechos fundamentales de la persona, la experiencia del usuario está muy relacionada con la experiencia que finalmente el ciudadano percibe a lo largo del ciclo de vida de la identidad. Esta experiencia es entendida de manera integral: no solo se enfoca, por ejemplo, en los procesos o tecnología disponible, sino también en la cercanía de los puntos de registro, el catálogo de transacciones que puede realizar, las capacidades de los asesores de servicios y los tiempos de entrega, entre otros. En ese sentido, la experiencia del usuario se convierte en uno de los retos más integrales y que se relaciona de manera directa con los demás elementos del ecosistema de identidad de cualquier país. Por ejemplo, la experiencia de usuario que se busque establecer para el ciudadano, no solo tendrá que resolver las dificultades que el ciudadano mencione, sino que también deberá proveer la regulación del sistema y servir como mecanismo para garantizar el acceso a un derecho fundamental como la identidad por parte del Estado.

En los estadios de madurez de un sistema respecto a la experiencia de usuario, se consideran como puntos críticos el enfoque con el que se implementen mejoras a la operación del ecosistema, es decir, con base en qué estrategia se desarrollan las mejoras al ciclo de vida en el que el ciudadano solicita, obtiene y usa su identidad. En un primer momento, cuando se empiezan a establecer mejoras, estas se desarrollan identificando dificultades básicas que resuelven problemas puntuales y, en su mayoría, no tienen mayor impacto en la percepción del ciudadano. Un paso siguiente es diagnosticar las principales problemáticas de la operación de manera integral; con estos aportes (*input*), las iniciativas que se desarrollen tendrán un alto impacto, ya que se eliminarán retrabajos, duplicidades y vacíos, se automatizarán tareas, pero aún de manera interna. El estadio más maduro de este indicador implica incorporar la voz del ciudadano a través de encuestas, cuestionarios, entrevistas a profundidad que develen las expectativas y principales dificultades que tiene el ciudadano para solicitar, obtener y usar los mecanismos de identificación en distintos escenarios y ámbitos. Con este *input*, es posible lograr un alto impacto en la experiencia del usuario.

A continuación, se mencionan estudios o experiencias de referencia que avalan la importancia del indicador en el Modelo de Madurez de los Sistemas de Identificación nacional:

- El BID publicó *Simplificando vidas: Calidad y satisfacción con los servicios públicos* (Pareja et al., 2015), que tiene el objetivo de analizar cuantitativa y cualitativamente los índices de satisfacción de los ciudadanos latinoamericanos respecto a los servicios que les brinda el Estado, es decir, busca comprobar la existencia de brechas entre la gestión de los servicios y la experiencia que el ciudadano vive al utilizar alguno de ellos. Este estudio permite que, al desarrollar alguna iniciativa de optimización del servicio, esta pueda estar respaldada o validada por la necesidad o percepción que el ciudadano tenga acerca de la problemática que esta iniciativa quiera resolver, de manera de evitar la asignación de recursos a iniciativas que el ciudadano no valore o no resuelvan la dificultad identificada. El objetivo del estudio no es establecer planes de acción para cada trámite realizado en los países analizados sino determinar líneas de acción en función de un mismo formato de medición para todos los países y todos los trámites. Por ejemplo, bajo el mismo marco de evaluación se analizaron los procedimientos de registro de nacimiento y la renovación de los documentos de identidad. A pesar de que la evaluación tenga los mismos campos a evaluar, no todos los países necesitan implementar grandes proyectos tecnológicos para mejorar sus sistemas. Por ejemplo, Chile busca optimizar de manera electrónica más que implementar tecnología que robustezca el sistema; Panamá elige no solo modernizar la captura de la identidad, sino también otorgarle calidad al sistema de gestión de la identidad bajo la implementación de estándares internacionales (Pareja y Serale, 2017).

C

## Forma de medición

**Nivel** D C B A

El ciudadano registra frecuentemente quejas o reclamos respecto a los distintos procesos del ciclo de vida de la identidad, debido a que no se realiza ningún tipo de mejora a la experiencia del ciudadano.

### Factores clave de posicionamiento

- No existe ningún tipo de mejora aplicada a los procesos del ciclo de vida de la identidad.
- No existen definiciones de calidad de servicio: tiempos de espera, reimpresiones, etc.
- No existen mecanismos oficiales para que los ciudadanos puedan realizar sus reclamos o si existen no son conocidos por el público.

**Nivel** D C B A

El ciudadano registra frecuentemente quejas o reclamos en momentos particulares de alguno de los procesos de registro, emisión, uso y actualización. Esto sucede debido a que las mejoras que se ejecutan se diseñan e implementan de manera aislada, respondiendo a dificultades internas operacionales y no a las experimentadas por el ciudadano.

**Factores clave de posicionamiento**

- No se implementan iniciativas globales de mejora integrales, ya que no cubren los procesos de inicio a fin.
- Existen mecanismos oficiales para que los ciudadanos puedan realizar sus reclamos y son conocidos por el público.
- Existen criterios de calidad de servicio pero no existen mecanismos de medición de los mismos, como tiempos de espera, duración de las distintas operaciones (registro y emisión del documento, entre otros), etc.

**Nivel** 


El ciudadano no registra quejas o reclamos respecto a los procesos de registro, emisión y actualización. Sin embargo, las entidades competentes en la ejecución de estos procesos no realizan ningún tipo de medición de la experiencia del ciudadano.

**Factores clave de posicionamiento**

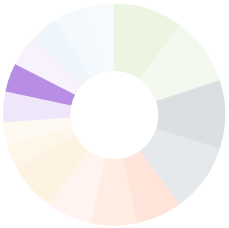
- Se realizan iniciativas de optimización en tópicos tales como reingeniería de procesos, automatización y aumento de desempeño, entre otros.
- Existen criterios de calidad de servicio y también mecanismos de medición de tiempos de espera y de duración de las distintas operaciones (registro, emisión del documento, etc.) pero los criterios de calidad no se alcanzan.

**Nivel** 


El ciudadano no registra quejas o reclamos respecto a los procesos de registro, emisión y actualización. Asimismo, las mediciones respecto a la perspectiva del ciudadano, que se realizan de manera periódica, es positiva y es el factor clave para diseñar o implementar alguna mejora en la operación de estos procesos.

**Factores clave de posicionamiento**

- Realización de encuestas a ciudadanos y medición de indicadores de satisfacción periódicas, lo que posibilita obtener muestras de trámites tanto en el ámbito privado como público que permitan implementar acciones tácticas de mejora.
- Existencia de criterios de calidad de servicio y también de mecanismos de medición de tiempos de espera y de duración de las distintas operaciones (registro, emisión del documento, etc.). Los criterios de calidad se alcanzan sistemáticamente.



# **Indicador 5.2:** Trazabilidad del uso de la identidad

## A
## Definición del indicador

El ciudadano tiene la posibilidad de consultar las transacciones en las que su identidad fue autenticada tanto en los servicios centralizados de los operadores certificadores de la identidad como en la institución de origen que realizó dicha consulta.

Es importante destacar que, si el proceso de autenticación se realiza sin interacción con los servicios de verificación del registro, no se espera que se genere ninguna traza. De hecho, sería una mala práctica que sí se generase.

## B
## Justificación de uso

El nivel de uso del mecanismo de identificación se manifiesta en la posibilidad que tiene el ciudadano de autenticar su identidad frente a distintas instituciones que lo requieran para realizar una transacción. En ese sentido, existen buenas prácticas que permiten al ciudadano conocer, de manera actualizada, qué personas naturales y/o jurídicas han realizado una consulta de verificación y/o autenticación de la identidad sobre la información que guardan los operadores certificadores de identidad.

## C
## Forma de medición

**Nivel** D C B A

En aquellos países que brindan un servicio de verificación centralizado, el ciudadano no puede acceder al registro de las autenticaciones de su identidad realizadas en el ecosistema, en caso que este exista.

**Factores clave de posicionamiento**

- En aquellos casos donde se brinda un servicio de verificación de identidad centralizado, no existe una base de datos que registre información sobre las condiciones en que se utilizó el servicio (qué organismo, fecha, hora, desde dónde, etc.)

**Nivel** D C B A

El ciudadano puede acceder al registro de las autenticaciones de su identidad realizadas en algunos ámbitos.

**Factores clave de posicionamiento**

- Las instituciones del sector público establecen convenios interinstitucionales con el registro civil o con los operadores certificadores de identidad, con el objetivo de autenticar la identidad de los ciudadanos que desean realizar transacciones en sus instituciones.

**Nivel** 


El ciudadano puede acceder al registro de las autenticaciones de su identidad realizadas en todos los ámbitos.

**Factores clave de posicionamiento**

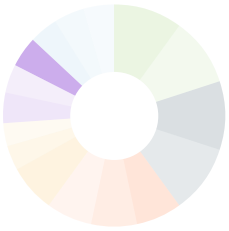
- Las instituciones de los sectores públicos y privados establecen convenios interinstitucionales o contratos de servicios con el registro civil o con los operadores certificadores de identidad, con el objetivo de autenticar la identidad de los ciudadanos que desean realizar transacciones en sus instituciones.

**Nivel** 


El ciudadano puede acceder al registro de las autenticaciones de su identidad realizadas en todos los ámbitos, a través de un portal o una aplicación web que además cuenta con datos actualizados. En términos prácticos, este nivel agrega sobre el nivel B la existencia de una plataforma que permite al usuario ver las transacciones de forma actualizada, ya que el nivel B implica que esto no existe y que, si el ciudadano quiere acceder a la información, debe solicitarlo.

**Factores clave de posicionamiento**

- Las instituciones de los sectores públicos y privados establecen convenios interinstitucionales o contratos de servicios con el registro civil o con los operadores certificadores de identidad, con el objetivo de autenticar la identidad de los ciudadanos que desean realizar transacciones en sus instituciones.
- Como parte de las iniciativas de gobierno electrónico, existe un portal del ciudadano en donde una de las consultas en línea que pueden hacerse es el estado de las autenticaciones que las instituciones, tanto del sector público como del privado, han realizado.



# **Indicador 5.3:** Cumplimiento del marco normativo

## A
## Definición del indicador

Grado de cumplimiento del marco normativo.

## B
## Justificación de uso

La importancia de este indicador reside en que, además de emitir y crear instrumentos legales que regulen e incorporen la política de **privacidad** y **datos personales** en el ecosistema de identidad, es aún más importante, por un lado, que las instituciones encargadas del tratamiento y uso de información las apliquen y, por otro, que el ciudadano conozca, sepa y también elija dentro de este marco.

Las consecuencias de que la legislación no tenga la correspondiente reglamentación y aplicación

podrían llevar a que la identidad sea una de las principales fuentes de fraude y delitos en sistemas más desarrollados, en los que los servicios están completamente integrados con la identidad fundacional a todo nivel y en todo ámbito.

C

## Forma de medición

**Nivel** 


No existe vinculación con el marco normativo. Cada institución define sus propios protocolos de operación para la gestión de la identidad.

**Factores clave de posicionamiento**

- No existe práctica legal o informal de cuidado de los datos relacionados a la identidad.

**Nivel** 


Existe vinculación con el marco normativo solo en el ámbito público, y se definen procedimientos técnicos para la gestión de la identidad para todas las instituciones del sector público.

**Factores clave de posicionamiento**

- Existen prácticas de cuidado de los datos relacionados a la identidad, pero no así estándares de protección de datos ni procedimientos para la protección y privacidad de datos.

**Nivel** 


Existe vinculación con el marco normativo en los ámbitos públicos y privados, y se establecen procedimientos estandarizados para la gestión de la identidad.

**Factores clave de posicionamiento**

- Existen procedimientos operativos de acuerdo a políticas de privacidad de datos, con respecto a los datos de identidad que las entidades públicas recogen en los trámites ofrecidos al ciudadano.

**Nivel** 


Además, se establecen procedimientos especializados por el rubro al que pertenece la institución que gestiona la identidad. Por ejemplo, leyes especializadas en salud, educación, etc.

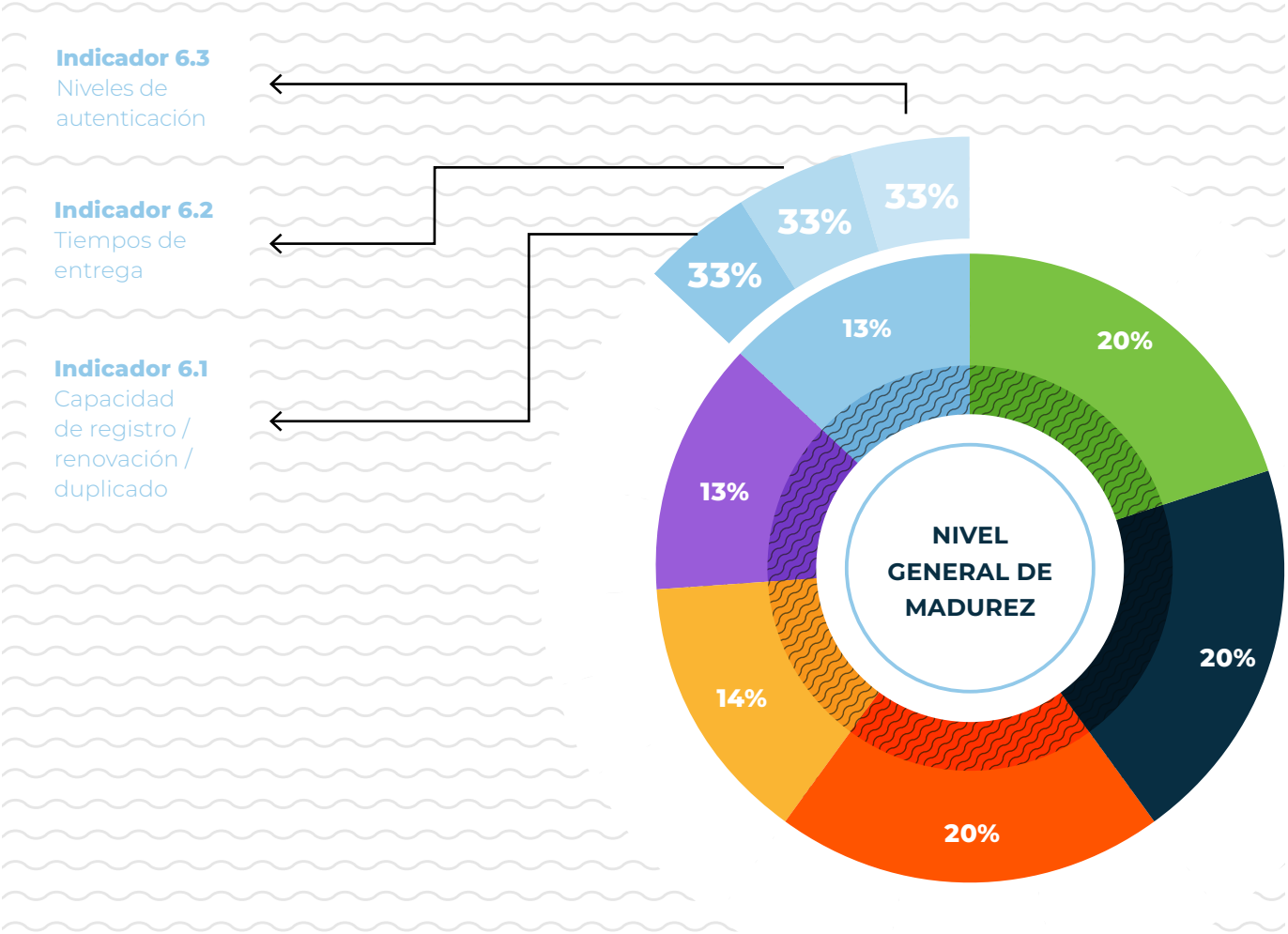
**Factores clave de posicionamiento**

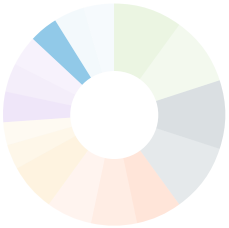
- Existen estándares de protección de datos y procedimientos aplicados para la protección y privacidad de datos.
- Existe un organismo regulador de la aplicación de estos estándares, que tiene la potestad de sanción, auditoría y verificación.

# 3.6. DIMENSIÓN 6: DESEMPEÑO

La dimensión 6, **Desempeño**, tiene un peso del 13% dentro del Modelo de Madurez, y está compuesta por tres indicadores: 6.1: **Capacidad de registro/renovación/duplicados**, 6.2: **Tiempos de entrega** y 6.3: **Niveles de autenticación**. Los tres indicadores tienen el mismo peso dentro de la dimensión, es decir, el 33%.

**Gráfico 3.6.**
Peso de la dimensión Desempeño y de sus tres indicadores





# Indicador 6.1:
# Capacidad de registro/ renovación/duplicado

A

## Definición del indicador

- Capacidad de registro / Número de nacimientos
- Capacidad de renovación / Número de solicitudes
- Capacidad de emisión de duplicado / Número de solicitudes – renovación – duplicado

B

## Justificación de uso

La capacidad para **registrar** por primera vez, **renovar** el mecanismo y otorgar el **duplicado** a los ciudadanos es unas de las principales mediciones de desempeño de un sistema de identidad. Se relaciona, por un lado, con la estrategia de registro que las instituciones reguladoras implementen y, por otro, con la tecnología que se ponga a disposición en los puntos de registro. Finalmente, el resultado se verá reflejado en la cobertura demográfica que se obtenga.

Cada una de las operaciones del ciclo de vida de la identidad está limitada por la capacidad para realizar dicha operación:

- En la fase de **registro** la captura de datos está limitada a la cantidad de oficinas y oficiales que realizan la tarea, y también a la duración de dicho proceso.
- En la fase de **prueba de identidad** existe la misma limitación de personal, a la que además se puede añadir la capacidad de los sistemas para operar (por ejemplo, cuántas búsquedas biométricas soporta el sistema en un intervalo de tiempo dado).
- En la fase de **emisión** importa la capacidad del sistema para generar las credenciales correspondientes y también los tiempos asociados a la entrega de dichos certificados.
- En la fase de **uso** se considera la capacidad de los sistemas para procesar las consultas en línea.
- En la fase de **actualización**, al igual que en la de registro, importa la cantidad de oficiales y oficinas disponibles para realizar la transacción, así como la duración de la misma.

C

## Información a obtener

**Relativas al registro:**

- Duración de un trámite de registro en minutos o cuántos procesos de registro puede llevar adelante el organismo por día (considerando que también tiene que llevar a cabo otros procesos).

- Tiempo de espera de un trámite de registro.
- Capacidad de búsqueda 1 a N del sistema biométrico.

**Relativas a la renovación y/o duplicado:**

- Duración de un trámite de renovación en minutos o cuántos procesos de renovación puede llevar adelante el organismo por día (considerando que también tiene que realizar otros procesos).
- Volumen de renovaciones (se puede estimar a partir del registro y del período de validez).

**Relativas a la emisión del documento:**

- Capacidad de personalización de certificados (documento de identidad) por día.

**Relativas al uso:**

- Capacidad de los servicios en línea para satisfacer consultas:
  - → Simultáneas,
  - → Por día.
- Cantidad de acuerdos y estimación del volumen acordado por día y en forma simultánea.

D

## Forma de medición

**Nivel** 


Es menor que 0,1.

**Factores clave de posicionamiento**

- El proceso de registro se basa en cumplimentar formularios no estandarizados y de forma analógica.
- No existe una lista definida de documentos requeridos para proceder con el proceso de registro.
- No se dispone de bases de datos que generen búsquedas automáticas para la validación de datos demográficos.
- No existen procedimientos de interoperabilidad con los principales puntos de registro de nacimiento: hospitales públicos y privados.

**Nivel** 


Está entre 0,1 y 0,9.

**Factores clave de posicionamiento**

- Se cuenta con formularios estandarizados con información definida a solicitar al ciudadano.

- Existe mapeo de documentos que provean información material de la identidad del ciudadano con la que realizar el procedimiento de verificación.
- Hay procedimientos de interoperabilidad con los principales puntos de registro de nacimiento: hospitales públicos y privados.

**Nivel** D C **B** A

Es igual o mayor a 1.

**Factores clave de posicionamiento**

- Existen bases de datos que generan búsquedas automáticas para la validación de datos demográficos.
- Hay procedimientos de captura biométrica y automatizada.

**Nivel** D C B **A**

Es mayor a 2.

**Factores clave de posicionamiento**

- Existen procedimientos de captura biométrica y automatizada.
- Hay aplicaciones *online* para el registro de identidad.

# Indicador 6.2:
# Tiempos de entrega

A

## Definición del indicador

Tiempos de entrega de mecanismos/herramientas que le permiten al ciudadano hacer uso del mecanismo de identificación.

B

## Justificación de uso

Como se muestra en estudios que ha realizado el Banco Mundial, como *The State of Identification Systems in Africa: A Synthesis of Country Assessments* (2017b), la complejidad de los sistemas de verificación en el proceso de emisión de la identidad y la no disponibilidad de sistemas de registro, validación y emisión de las identidades lo suficientemente avanzados tecnológicamente producen un proceso de emisión de la identidad ineficiente y que conlleva un período de tiempo excesivamente alto para su conclusión.

Por ejemplo, en Guinea los datos sobre nacimientos y defunciones en áreas rurales se completan en formularios en papel y se envían físicamente al registro civil, y en Costa de Marfil el proceso de emisión de un documento de identidad toma entre dos y tres meses debido a que se requiere la verificación manual de los documentos recibidos.

Si se mejoran los procesos de registro, emisión y actualización del sistema de identidad de un país, se puede conseguir un menor tiempo de entrega, lo cual representa un indicador de madurez del sistema de emisión.

Por ejemplo, el Registro Civil de Namibia implementó una mejora en el proceso de emisión de la identidad de sus ciudadanos, que redujo el tiempo de entrega de su documento de identidad de 100 días en 2014 a 16 días en 2015. Según este indicador, Namibia habría pasado del nivel D al nivel C.

C

## Forma de medición

**Nivel** D C B A

El proceso de validación se realiza de manera analógica y sin estandarización. El proceso de emisión dura más de 30 días y el mecanismo de identificación es analógico.

### Factores clave de posicionamiento

- El proceso de captura de la información se basa en formularios en papel que el ciudadano completa a mano.
- No se dispone de interconexión con las fuentes biográficas o demográficas que permitan verificar de forma automática la identidad de la persona que se está enrolando.

- No se dispone de sistemas de verificación biométrica para evitar deduplicaciones y realizar una consulta *online* para asegurar la veracidad de la identidad del postulante.
- El centro de registro, el de validación y el de emisión están separados o los procesos se realizan en diferentes momentos.
- En el caso de los países que emiten registros digitales, la tecnología que caracteriza a los mecanismos de identificación no son fabricadas en el lugar de origen, por lo que es necesario realizar procedimientos de importación desde el extranjero.
- En el caso de los países que emiten mecanismos de identidad físicos, las entidades de registro no tienen la competencia y/o capacidad de imprimir las tarjetas de identificación, ya sea por factores de protección y seguridad física de las tarjetas o por falta de impresoras de tarjetas.

**Nivel** 


El proceso de validación se realiza de manera analógica, con un proceso estandarizado. El proceso de emisión dura entre 6 y 30 días y el mecanismo de identificación es analógico.

**Factores clave de posicionamiento**

- El proceso de captura es electrónico pero no se dispone de enlaces con fuentes biográficas o demográficas que permitan verificar la información introducida.
- La información es enviada electrónicamente al centro de validación pero, al no realizarse en el mismo momento de forma automática, se requiere un proceso posterior.
- Se recoge la información biométrica pero no se utiliza para emitir el mecanismo de identidad.
- La información de emisión del mecanismo de identidad no se realiza en la misma entidad.
- En el caso de los países que emiten mecanismos de identidad físicos, las entidades de registro no tienen la competencia y/o capacidad de imprimir las tarjetas de identificación, ya sea por factores de protección y seguridad física de las tarjetas o por falta de impresoras de tarjetas.

**Nivel** 


El proceso de validación se realiza de manera electrónica con un proceso estandarizado, pero no se lleva a cabo de forma *online*. El proceso de emisión dura entre dos y cinco días y el mecanismo de identificación es analógico.

**Factores clave de posicionamiento**

- El proceso de enrolamiento o el de emisión asumen el rol de validación, por lo que se reducen los tiempos del proceso en general.
- Aunque el proceso es fundamentalmente electrónico, al no estar integradas todas las funciones del ciclo de vida en la misma enti-

dad o al faltar algún proceso por interconectar de forma automática, el proceso no puede iniciar y terminar en el mismo instante (esto puede deberse a la necesidad de comprobación de la información presentada por el usuario).

- En el caso de los países que emiten mecanismos de identidad físicos, las entidades de registro no tienen la competencia y/o capacidad de imprimir las tarjetas de identificación, ya sea por factores de protección y seguridad física de las tarjetas o por falta de impresoras de tarjetas.

**Nivel** 


El proceso de validación se realiza de manera electrónica con un proceso estandarizado y de forma *online*. El proceso de emisión es automático y el mecanismo de identificación es analógico y digital necesariamente.

**Factores clave de posicionamiento**

- Todo el proceso es electrónico y la misma entidad asume los tres roles del ciclo de vida de emisión de la identidad: enrolamiento, validación y emisión.

- El punto de enrolamiento es capaz de introducir la información de enrolamiento de forma electrónica (metadatos, información biométrica y otros datos), validarla *online* con las bases de datos de verificación (registro civil u otros) y emitir el mecanismo de identificación en el medio adecuado. Esta identidad debe ser tanto presencial como digital para estar en este nivel.



# Indicador 6.3:
# Niveles de autenticación

A

## Definición del indicador

Nivel de complejidad de autenticación requerido para la comprobación de la identidad.

B

## Justificación de uso

Las transacciones realizadas por los ciudadanos requieren **distintos niveles de complejidad, dependiendo de la clasificación de sensibilidad de la información que se precisa validar**. Los niveles de complejidad de autenticación están muy vinculados a la protección de datos, debido a que cuanto más críticos de proteger sean los datos, mayor será el nivel de autenticación requerido para proceder con la transacción. Es usual que estos niveles se estructuren en categorías jerárquicas. Por ejemplo, la reglamentación europea eIDAS propone tres niveles de seguridad: **bajo**, **sustancial** y **alto**.

- **Nivel de seguridad bajo:** se refiere a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado limitado de confianza en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo (por ejemplo, los controles técnicos), y cuyo objetivo es reducir el riesgo de uso indebido o alteración de la identidad.

- **Nivel de seguridad sustancial:** se refiere a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado sustancial de confianza en la identidad pretendida o declarada de una persona y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo (por ejemplo, los controles técnicos), y cuyo objetivo es reducir sustancialmente el riesgo de uso indebido o alteración de la identidad.

- **Nivel de seguridad alto:** se refiere a un medio de identificación electrónica, en el contexto de un sistema de identificación electrónica, que establece un grado de confianza en la identidad pretendida o declarada de una persona superior al medio de identificación electrónica con un nivel de seguridad sustancial, y se describe en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo (por ejemplo, los controles técnicos), cuyo objetivo es evitar el uso indebido o alteración de la identidad.

En general, se asume que el nivel 1 del estándar ISO/IEC 29115 está fuera del alcance de un sistema de identidad nacional, por lo cual no está mapeado a las definiciones de eIDAS. A continuación, se usará el criterio definido por eIDAS como base para el análisis.

Es muy importante recalcar que diferentes aplicaciones pueden requerir distintos tipos de autenticación. En el Cuadro 3.1 se presenta a modo de ejemplo una lista de transacciones en la que se considera el tipo de autenticación requerida por transacción.

**Cuadro 3.1.**
Ejemplos de tipo de autenticación por transacción

| Clasificación de dato | Transacción a realizar (ejemplo) | Dato a autenticar | Tipo de autenticación |
|---|---|---|---|
| Nivel básico | Compra comercial | UIN | Consulta electrónica del UIN<br>Código de barras del DNI |
| Nivel intermedio | Transacciones bancarias (por ejemplo, préstamos) | Huellas electrónicas<br>Verificación de voz (si la compra se realiza a través del canal telefónico) | Verificación de coincidencia de huella electrónica<br>Verificación de coincidencia de voz |
| Nivel alto | Presentación de declaración jurada | Firma electrónica | Certificación de firma electrónica |

La importancia de medir los niveles de autenticación requeridos para las transacciones reside en que la autenticación esté soportada en mecanismos electrónicos y tecnológicos que eviten o reduzcan los casos de fraude o accesos inadecuados. En ese sentido, aún existen muchos ámbitos en los que, si bien se requiere la autenticación de la identidad, estos mecanismos siguen siendo físicos por comparación y mantienen un porcentaje alto de error humano.

C

## Forma de medición

**Nivel** D C B A

Los procedimientos de autenticación, a través del mecanismo de identificación fundacional requerido, comprenden solo la visualización y comprobación física de alguno de los elementos del mecanismo de identificación portable. Es decir, no existe otro mecanismo que la comprobación física de la credencial correspondiente.

Alternativamente, los mecanismos de Gestión de Medios de Identificación Electrónica (sección 2.2) y Autenticación (sección 2.3) definidos por eIDAS (Reglamento de Ejecución (UE) 2015/1502 de la Comisión del 8 de septiembre de 2015), no alcanzan el nivel **bajo** de seguridad.

### Factores clave de posicionamiento

- El proceso de autenticación se realiza solo con base en la comprobación o la comparación física y no hay disponibles mecanismos de verificación automática o en línea.
- Las consultas que formen parte de la autenticación se realizan en bases de datos físicas o electrónicas. En el caso de esta última, no son bases de datos creadas bajo estándares.

**Nivel** 


Los procedimientos de autenticación, a través del mecanismo de identificación fundacional requerido, incluyen la verificación electrónica de datos biográficos y del número identificador.

Es importante destacar que a medida que aumenta el nivel, se agregan mecanismos de autenticación a los ya existentes, pero no se excluyen mecanismos previos. A modo de ejemplo, el nivel C se alcanza si los procedimientos de autenticación incluyen verificación electrónica y también permiten la verificación física de la identidad.

Alternativamente, los mecanismos de Gestión de Medios de Identificación Electrónica (sección 2.2) y Autenticación (sección 2.3) definidos por eIDAS (Reglamento de Ejecución (UE) 2015/1502 de la Comisión del 8 de septiembre de 2015), alcanzan el nivel **bajo** de seguridad.

**Factores clave de posicionamiento**

- La consulta de autenticación permite el cotejo de los datos biográficos, así como la verificación del número identificador.
- Los procesos electrónicos de autenticación electrónica no son obligatorios lo que genera que en ciertos ámbitos aún coexistan la comprobación o comparación física con las verificaciones electrónicas.

**Nivel** 


Los procedimientos de autenticación, a través del mecanismo de identificación fundacional, requeridos comprenden verificación electrónica de un número identificador, firma electrónica y huellas biométricas.

Alternativamente, los mecanismos de Gestión de Medios de Identificación Electrónica (sección 2.2) y Autenticación (sección 2.3) definidos por eIDAS (Reglamento de Ejecución (UE) 2015/1502 de la Comisión del 8 de septiembre de 2015), alcanzan el nivel **sustancial** de seguridad.

**Factores clave de posicionamiento**

- Aunque el proceso es fundamentalmente electrónico, al no estar integradas todas las funciones del ciclo de vida en la misma entidad o al faltar algún proceso por interconectar de forma automática, el proceso no puede iniciar y terminar en el mismo instante (esto puede deberse a la necesidad de comprobación de la información presentada por el usuario).

**Nivel** 


Los procedimientos de autenticación, a través del mecanismo de identificación fundacional, requeridos comprenden la verificación electrónica de uno de los siguientes elementos: número identificador, firma electrónica, y en aquellos países donde esté reglamentado, el uso de biometría.

Alternativamente, los mecanismos de Gestión de Medios de Identificación Electrónica (sección 2.2) y Autenticación (sección 2.3) definidos por eIDAS (Reglamento de Ejecución (UE) 2015/1502 de la Comisión del 8 de septiembre de 2015), alcanzan el nivel **alto** de seguridad.

**Factores clave de posicionamiento**

- Todo el proceso es electrónico y la misma entidad asume los tres roles del ciclo de vida de la identidad: entidad de registro, proveedor de credenciales y parte confiable.

- El punto de enrolamiento es capaz de introducir la información de enrolamiento de forma electrónica (metadatos, información biométrica y otros datos), validarla *online* con las bases de datos de verificación (registro civil u otros) y emitir el mecanismo de identificación en el medio oportuno. Esta identidad debe ser tanto presencial como digital para considerarse en este nivel.

4

# REFERENCIAS

1 2 3 4

# 4.1. REFERENCIAS

## A


ADB (Banco Asiático de Desarrollo). 2016. Identity for Development in Asia and the Pacific. Disponible en: **https://www.adb.org/sites/default/files/publication/211556/identity-development-asia-pacific.pdf**

Asamblea General de las Naciones Unidas. 2015. Declaración Universal de Derechos Humanos. Disponible en: **http://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf**


## B


Banco Mundial. 2015. Identification for Development (ID4D) Integration Approach. Disponible en: **https://www.biometricupdate.com/wp-content/uploads/2015/09/ID4D-report-World-Bank-Accenture.pdf**

Banco Mundial y GSMA (Global System for Mobile Communications). 2016. Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation. Disponible en: **http://documents.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf**

Banco Mundial. 2017a. Technical Standards for Digital Identity Systems. Disponible en: **http://pubdocs.worldbank.org/en/579151515518705630/ID4D-Technical-Standards-for-Digital-Identity.pdf**

Banco Mundial. 2017b. *The State of Identification Systems in Africa: A Synthesis of Country Assessments*. Disponible en: **https://documents1.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf**

BID (Banco Interamericano de Desarrollo). 2017. RG-T3070: Simplificando vidas a través de la identidad digital. Disponible en: **https://www.iadb.org/es/proyecto/RG-T3070**

Bujoreanu, L., A. Mittal y W. Noor. 2018. Desmitificar las tecnologías de identificación digital. *Blog Voces del Banco Mundial*. Disponible en: **https://blogs.worldbank.org/es/voices/desmitificar-las-tecnologia-de-identificacion-digital**

# C

CAF (Banco de Desarrollo de América Latina y el Caribe). 2014. Hacia la transformación digital de América Latina y el Caribe: Las infraestructuras y los servicios TIC de la región. Disponible en: **https://scioteca.caf.com/bitstream/handle/123456789/490/informe_tecnologiacaf.pdf?sequence=1&isAllowed=y**

————. 2017. Hacia la transformación digital de América Latina y el Caribe: El observatorio CAF del ecosistema digital. Disponible en: **https://scioteca.caf.com/bitstream/handle/123456789/1059/Observatorio%20CAF%20del%20ecosistema%20digital.pdf?sequence=7&isAllowed**

Comisión Europea. 2015. Decisión de Ejecución (UE) 2015/1506 de la Comisión del 8 de septiembre de 2015, *Diario Oficial de la Unión Europea*. Disponible en: **https://www.boe.es/doue/2015/235/L00037-00041.pdf**

# E

E-Governance Academy, 2014. Implementation of E-Government in Cross-Border Regions. Disponible en: **https://issuu.com/e-governanceacademy/docs/handbook_implementation_of_e-govern**

Estados Unidos Mexicanos. 1917. Constitución Política de los Estados Unidos Mexicanos. Disponible en: **http://www.sct.gob.mx/JURE/doc/cpeum.pdf**

# F

Fundación Telefónica. 2012. Tendencias pan-europeas en gestión de identidad digital. Disponible en: **https://telos.fundaciontelefonica.com/archivo/numero091/tendencias-pan-europeas-en-gestion-de-identidad-digital/**

————. 2013. Identidad Digital: El nuevo usuario en el mundo digital. Disponible en: **https://publiadmin.fundaciontelefonica.com/index.php/publicaciones/add_descargas?tipo_fichero=pdf&idioma_fichero=_&pais=Espa%C3%B1a&title=Identidad+Digital%3A+El+nuevo+usuario+en+el+mundo+digital&code=229&lang=es&file=identidad_digital.pdf**

# G

Global Delivery Initiative. 2017. e-Government for Better Civil Services: How the Korean Government Implemented the e-Registration System. Disponible en: **https://www.effectivecooperation.org/system/files/2021-08/errs_mobile_system_5-17-17_final.pdfhttp://www.globaldeliveryinitiative.org/sites/default/files/case-studies/errs_mobile_system_5-17-17_final.pdf**

# K

Kim, H. 2004. National Identity in Korean Curriculum. Disponible en: **https://files.eric.ed.gov/fulltext/EJ1073922.pdf**

# M

Mittal, A. 2022. Catalog of Technical Standards for Digital Identification Systems. Banco Mundial. Disponible en: **https://documents.worldbank.org/en/publication/documents-reports/documentdetail/707151536126464867/catalog-of-technical-standards-for-digital-identification-systems**

# N

NIST (Instituto Nacional de Estándares y Tecnología). 2017. Digital Identity Guidelines Enrollment and Identity Proofing, NIST Special Publication 800-63A. Disponible en: **https://doi.org/10.6028/NIST.SP.800-63a**

# P

Pareja, A., C. Fernández, B. Blanco, K. Theobald y A. Martínez. 2015. Simplificando vidas: Calidad y satisfacción con los servicios públicos. Banco Interamericano de Desarrollo. Disponible en: **https://publications.iadb.org/bitstream/handle/11319/7975/Simplificando-vidas-Calidad-y-satisfaccion-con-los-servicios-publicos.pdf**

Pareja y Serale, 2017. Calidad y satisfacción ciudadana con el registro civil y la gestión de la identidad. *Blog GobernArte del Banco Interamericano de Desarrollo.* Disponible en: **https://blogs.iadb.org/gobernarte/2017/01/24/calidad-y-satisfaccion-ciudadana-con-el-registro-civil-y-la-gestion-de-la-identidad/**

Pedak, M. 2013. eID Estonian Experience. Disponible en: **https://nvvb.nl/media/cms_page_media/758/13%20Mari%20Pedak%20eID%20Estonian%20experience.pdf**

# R

República Constitucional del Perú. 1993. Constitución Política del Perú. Disponible en: **https://www.gob.pe/institucion/presidencia/informes-publicaciones/196158-constitucion-politica-del-peru**

# U

USAID (Agencia de los Estados Unidos para el Desarrollo Internacional). 2017. Identity in a Digital Age: Infrastructure for Inclusive Development. Disponible en: **https://www.usaid.gov/sites/default/files/2022-05/IDENTITY_IN_A_DIGITAL_AGE.pdf**

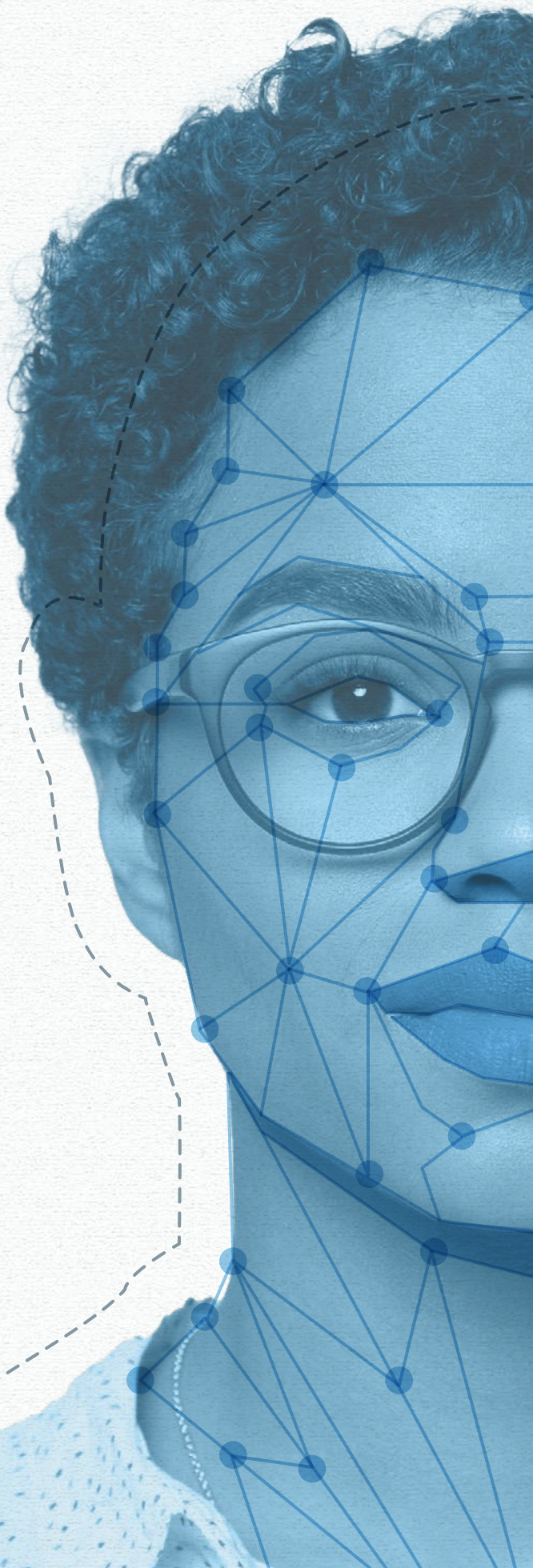
Universidad de Toronto. 2016. Case Study: Aadhaar – Providing Proof of Identity to One Billion. Disponible en: **https://static1.squarespace.com/static/5769a0b5f7e0ab7b91a3362b/t/5a2576f5419202014ee6d6b7/1512405956013/INDIA_CaseStudy_ReachProject2017.pdf**

# +ID

El concepto de identidad refiere al conjunto de información que caracteriza y reconoce a una persona en un determinado ecosistema; alrededor del concepto de identidad existe una serie de atributos que acompañan su definición. Uno de los desafíos más importantes de los sistemas de identificación es lograr que la totalidad de los ciudadanos se encuentren debidamente identificados por las administraciones de sus países.

A partir de la información disponible, se estima que hasta 2018 existían 1.100 millones de personas en el mundo que no contaban con un documento oficial para autentificar su identidad (Bujoreanu, Mittal y Noor, 2018).

Asociado a ello, el desafío de la cobertura ha sido la principal problemática hasta el momento. Sin embargo, el concepto de identidad ha evolucionado a una complejidad mayor en la que la autenticación de la identidad necesita de mecanismos robustos que permitan un espectro más amplio de uso por parte del ciudadano, así como una mejor experiencia del usuario final. De esta manera, se requiere de una visión holística que permita observar de manera global los ámbitos relevantes en la madurez de un sistema de identidad.



BID