

**¿QUÉ  
BUSCAR EN  
LOS SISTEMAS  
DE IDENTIDAD  
DIGITAL?**

**Una tipología  
de etapas**

**Esta tipología se basa en una investigación realizada por The Engine Room, con el apoyo de Omidyar Network, Open Society Foundations y Yoti Foundation de octubre de 2018 a octubre de 2019.**

**Investigadores:** Sharid Bin Shafique, Chennai Chair, Kittima Leeruttanawisut, Koliwe Majama, Chuthathip Maneepong, Precious Ogbuji, Berhan Taye

**Redacción:** Sara Baker, The Engine Room

**Revisión y Edición:** Zara Rahman, Laura Guzmán, Madeleine Maxwell, Sivu Siwisa, The Engine Room

**Traducción:** Global Voices

**Diseño gráfico:** Julie Saw, Little by Little Studios

El texto de este trabajo está bajo licencia Creative Commons Attribution-Share Alike 4.0 International Licence. Para ver el detalle de esta licencia, visite:

[http://creativecommons.org/licenses/by-sa/4.0/.](http://creativecommons.org/licenses/by-sa/4.0/)

**THE ENGINE ROOM**

# Antecedentes del proyecto

A fines de 2018, The Engine Room inició un proyecto para entender las experiencias de las personas con los sistemas de identidad digital. Para los fines de este proyecto, hemos definido sistemas de identidad digital como sistemas estatales o humanitarios que recopilan y usan datos digitales – los cuales a menudo incluyen datos biométricos como huellas dactilares y escaneos de iris – para identificar a ciudadanos, residentes y beneficiarios.

Trabajamos con investigadores en terreno en cinco locaciones, enfocados en sistemas nacionales de Nigeria, Zimbabue y Tailandia, así como sistemas humanitarios en campos de refugiados rohinyá en Bangladesh y campos de refugiados en Etiopía. Para entender mejor el amplio ecosistema de identidad digital, el proyecto incluyó una revisión de literatura que se extendió más allá de estos cinco lugares para explorar sistemas en otras partes del mundo.

Esta tipología de etapas es el primero de nuestros hallazgos del proyecto. Próximamente publicaremos más reflexiones, incluido un informe global y casos de estudio.

# Cómo usar esta tipología

Esta tipología explica las etapas de planificación, desarrollo, implementación y mantenimiento del sistema de identificación digital de acuerdo a lo que identificamos en nuestros estudios de campo e investigación de escritorio. Está dirigida a la sociedad civil, activistas y periodistas que buscan mejorar su comprensión de estos sistemas, educar o hacer incidencia al respecto.<sup>1</sup>

Esta herramienta te ayudará a:

- > Identificar en qué etapa está un sistema de identificación digital
- > Entender qué esperar de cada etapa
- > Elaborar estrategias de incidencia para influenciar a desarrolladores y tomadores de decisiones

**Cada etapa enumera actividades claves que pueden emprender los creadores de los sistemas, pero no todos los sistemas que examinamos incluyeron todas las actividades.**

Cada actividad está seguida por una lista de **preguntas a realizar** al sistema de identificación digital de tu comunidad, y cada etapa incluye un breve **caso de estudio** de incidencia. Las etapas de planificación y desarrollo también enumeran **documentos** claves a revisar. Estos son documentos típicamente producidos por desarrolladores del sistema de identificación digital y pueden aclarar sus motivaciones, planes y objetivos. Hay más información sobre los temas mencionados en las referencias al final de este documento.

# Etapa 1 Planificación

En esta etapa, los creadores del sistema de identificación están sentando las bases señalando problemas que el sistema debe resolver y creando marcos de trabajo necesarios. Las preguntas claves se enfocan en indagar en los argumentos presentados para impulsar un sistema de identificación digital, y buscan entender las referencias legales y de políticas que podrían darle sustento.

## Desarrollo de estrategia: Determinar la necesidad de un sistema de identificación digital

### Preguntas a realizar

- ¿Qué problema pretende solucionar este sistema de identificación digital? ¿Es este un problema real y significativo? ¿Hay evidencia que demuestre que la identificación digital resolverá dicho problema?
  - Argumentos comunes de los Estados incluyen:
    - › Mejora la seguridad nacional
    - › Mejora la prestación de servicios y entrega de derechos
    - › Inclusión financiera
  - Los argumentos comunes de las organizaciones<sup>2</sup> humanitarias incluyen:
    - › Distribución de ayuda más rápida y eficiente
    - › Disminución de fraude
- ¿Quién se beneficia más con este sistema? ¿Los beneficios superan los riesgos?
- ¿El desarrollador ha llevado a cabo consultas profundas con una diversidad de partes interesadas?

# Desarrollo de políticas y legislación: Crear marcos regulatorios para la implementación de un sistema de identificación digital

## Documentos claves

- Legislación de protección de datos
- Ley de identificación digital (u otra ley que disponga la existencia de un sistema nacional)

## Preguntas a realizar

- ¿Qué leyes existentes permiten o impiden la recopilación de datos, como datos biométricos, a través de este sistema?
- ¿Qué proyectos de ley relacionados están evaluando los legisladores? ¿Estos proyectos incluyen un periodo de comentarios del público?
- ¿Ya está vigente alguna ley de protección de datos?<sup>3</sup> ¿Cómo afecta, si es que afecta, al sistema planificado de identificación digital? ¿Aborda problemas como intercambio de datos o retención de datos?

## Caso de estudio

La defensoría legal puede ser un método efectivo para enfrentar posibles violaciones a la privacidad y otros problemas. Cuando el secretario general del Partido Popular Nacional presentó una demanda en la que sostenía que la propuesta de sistema de identificación digital de Jamaica era inconstitucional, la Corte Suprema jamaicana



resolvió<sup>4</sup> a su favor y el sistema quedó descartado. Aunque una demanda similar en India, previa al caso jamaicano, no logró detener a su sistema nacional (Aadhaar), las iniciativas indias tuvieron un impacto crítico en Jamaica, donde los jueces se basaron mucho en la opinión discordante del juez de la Corte Suprema india DY Chandrachud.<sup>5</sup>

# Etapa 2 Desarrollo

En esta etapa, los desarrolladores están trabajando con socios para definir los parámetros e infraestructura del sistema de identificación digital. Las preguntas claves examinan la naturaleza de estas sociedades y la protección de datos del usuario.

**Compras: Encontrar y contratar a un socio del sector privado para desarrollar, y posiblemente mantener, un sistema de identificación digital**

## Documentos claves

- Licitación de propuestas o términos de referencia para contratar a un tercero
- Un acuerdo de intercambio de datos entre Gobiernos anfitriones y organizaciones de asistencia

## Preguntas a realizar

- ¿Hay un proceso de compras? Si es así, ¿es abierto y transparente?<sup>6</sup>
- ¿Quién es el proveedor comercial y cómo se beneficia?
- ¿A qué datos puede acceder el proveedor comercial y qué hará con esos datos?
- ¿El proveedor comercial tiene vínculos con comunidades nacionales o internacionales de inteligencia y fuerzas del orden?
- Si una organización como ACNUR está implementando un sistema en nombre de un Gobierno anfitrión, ¿se intercambia algún dato con el país de origen de los refugiados?

# Diseño y planificación: Crear la arquitectura y protocolos asociados a un sistema de identificación digital

## Documentos claves

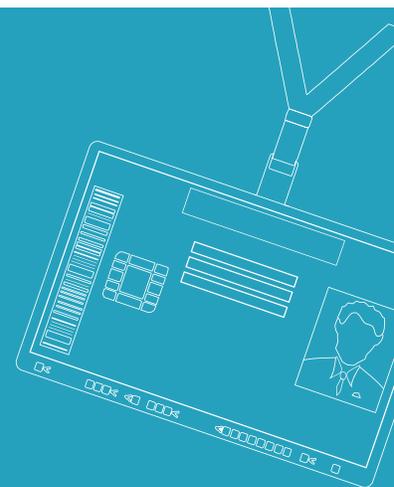
- Diagrama de arquitectura u otra descripción que explique cómo funcionará el sistema
- Procesos que rigen el consentimiento, registro, retención de datos, etc.
- Evaluación de riesgos o evaluación de impacto a la privacidad

## Preguntas a realizar

- El diseño de la arquitectura del sistema sigue prácticas cada vez más recomendadas, como la Privacidad por diseño,<sup>7</sup> el Diseño centrado en los humanos<sup>8</sup> y el Diseño participativo.<sup>9</sup>
- ¿Los procesos de registro y consentimiento están diseñados con aportes de grupos vulnerables?
- ¿Qué documentos de identidad se usarán para el proceso de registro? ¿Todos tienen ya estos documentos? ¿Quién podría quedar fuera?
- ¿Cómo se almacenarán los datos? ¿La base de datos está centralizada? ¿Quién tendrá acceso?
- ¿Hay políticas de seguridad apropiadas y protocolos basados en evaluaciones de riesgos?
- ¿Hay políticas de retención de datos?

## Caso de estudio

Cuando Túnez propuso una tarjeta de identidad biométrica, no había información sobre dónde se almacenarían los datos personales o quién tendría acceso, y nunca se mencionó al contratista comercial.<sup>10</sup> La sociedad civil convenció a los legisladores para que adoptaran reformas a la protección de datos que salvaguardarían la base de datos biométricos.<sup>11</sup> En una victoria sin precedentes, cuando las reformas fueron aprobadas, el ministro del Interior descartó el proyecto completamente. Al parecer no podría seguir adelante sin que la empresa anónima tuviera acceso a datos ciudadanos.



# Etapa 3 Implementación

Esta etapa incluye el despliegue y funcionamiento de un sistema de identificación digital. Las preguntas claves enfatizan la importancia de la difusión pública y buscan entender las experiencias de las personas con el sistema.

## Campañas de sensibilización: Informar a la población sobre el propósito, función y proceso de registro de un sistema de identificación digital

### Preguntas a realizar

- ¿De qué forma han involucrado al público los desarrolladores?
  - Las tácticas comunes incluyen:
    - › Divulgación en medios
    - › Participación de líderes comunitarios
    - › Anuncios en campos de refugiados
- ¿Se ha contactado a grupos vulnerables?
- ¿Tiene la gente suficiente información para sustentar e interactuar con sistemas de identificación digital o hacer incidencia efectiva para lograr cambios fundamentales?
- ¿Las personas pueden conectar privacidad de datos a otros temas urgentes como pobreza y discriminación?

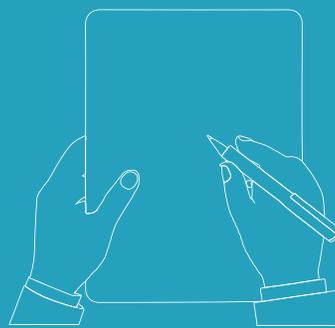
# Registro y uso: Inscribir usuarios a un sistema de identificación digital y habilitar servicios de capacitación

## Preguntas a realizar

- ¿Se ha consultado a las comunidades marginadas para evitar barreras en el registro?
  - Las barreras comunes incluyen:
    - › Falta de lugares de registro accesibles para personas con discapacidades y personas en zonas rurales
    - › Discriminación contra personas transgénero y no binarias (por ejemplo, falta de opciones de género apropiadas en los formularios, incapacidad de reconocer transiciones de género)
    - › Desconocimiento del idioma o de las herramientas digitales usadas
    - › Incapacidad de reconocer normas culturales (por ejemplo, pedir que las mujeres en comunidades conservadoras se registren independientemente)
    - › Costos asociados a la obtención o corrección de documentos de identidad iniciales
- ¿Las organizaciones humanitarias han evaluado el impacto del trauma en refugiados recién registrados?
- ¿Todas las poblaciones están teniendo los mismos beneficios?
  - ¿Hay alguna que esté siendo más perjudicada que otra?

## Caso de estudio

En Tailandia, la sociedad civil está haciendo el trabajo de ayudar a los migrantes a pasar por el registro de identificación. Esta cercana conexión entre trabajadores migrantes y las oficinas de identificación de migrantes del Gobierno crea una valiosa oportunidad de incidencia.



Las organizaciones de la sociedad civil tienen un conocimiento único de las necesidades de los migrantes y de las barreras y riesgos que enfrentan, lo que puede permitirles presionar para lograr cambios que beneficien a esta población marginada.

# Etapa 4 Mantenimiento

En esta etapa, las entidades encargadas de manejar el sistema de identificación digital gestionan su uso y problemas relacionados con él. Aunque el registro suele captar la mayor atención, el mantenimiento es crítico para el éxito a largo plazo de un sistema de identificación digital. Las preguntas a hacer abordan los conflictos de las personas con el sistema y qué tan seriamente toman estas entidades el fuerte peso de la seguridad.

## Actualizaciones: Abordar los cambios en la vida y errores de registro en el sistema de identificación digital

### Preguntas a realizar

- ¿Cuál es el proceso para actualizar o enmendar errores en los datos?
- ¿Hay evidencia de la efectividad o fallas de este proceso? Por ejemplo, ¿hay personas que no hayan podido hacer cambios necesarios causando la negación de servicio, ayuda o la capacidad de ejercer sus derechos?
- ¿Cómo se manejan los falsos positivos y falsos negativos?<sup>12</sup>

## Informe de quejas: Remitir y abordar quejas sobre un sistema de identificación digital

### Preguntas a realizar

- ¿Cómo pueden las personas presentar quejas sobre el sistema? ¿El proceso es fácil, intuitivo y accesible?

- ¿Se trata a las personas de manera justa y respetuosa cuando presentan quejas?
- ¿Las personas confían en los departamentos encargados de responder las quejas?
- ¿Se necesita supervisión independiente?

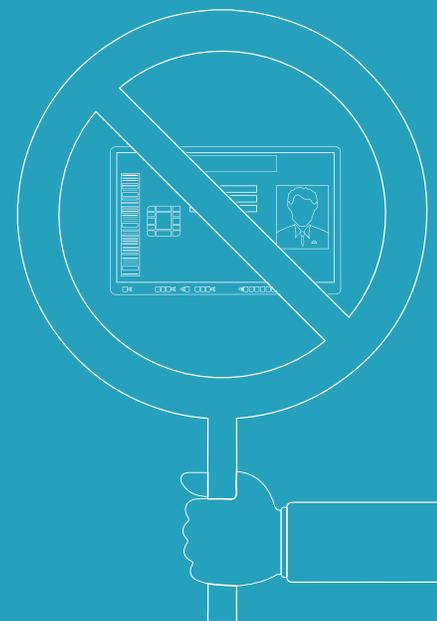
## Seguridad: Proteger los datos del sistema de identificación digital conforme pasa el tiempo

### Preguntas a realizar

- ¿El desarrollador está siguiendo las políticas y protocolos diseñados para evitar incidentes de seguridad?
- ¿Hay protocolos claros y viables para gestionar fuga, filtraciones y fallas de datos?
- ¿El desarrollador es transparente sobre la cantidad y daños causados por los incidentes de seguridad?
- ¿Existen formas para que las personas busquen rectificar perjuicios originados por incidentes de seguridad?

### Caso de estudio

Cuando no se abordan las quejas, una acción colectiva puede tener impacto. En Bangladesh, con pocos recursos de presión, los refugiados rohinyá hicieron una huelga para protestar por las cédulas inteligentes que catalogan a cada persona como “ciudadano de Myanmar desplazado forzosamente” en vez de rohinyá, y para pedir que las autoridades se nieguen a compartir datos biométricos de los refugiados con el Gobierno de Myanmar.<sup>13</sup>



# Referencias

- 1** Para mejores prácticas de identificación digital, ten en cuenta el movimiento Good ID (<https://www.good-id.org/en/>), el marco de trabajo de la evaluación del CIS (<https://digitalid.design/evaluación-framework-01.html>), la hoja de ruta de UIT ([https://www.itu.int/en/ITU-D/ICT-Applications/Documents/Guides/ITU\\_eID4D\\_DIGITAL%20IDENTITY\\_ROAD\\_MAP\\_GUIDE\\_FINAL\\_Under%20Review\\_Until-05-10-2018.pdf](https://www.itu.int/en/ITU-D/ICT-Applications/Documents/Guides/ITU_eID4D_DIGITAL%20IDENTITY_ROAD_MAP_GUIDE_FINAL_Under%20Review_Until-05-10-2018.pdf)) y los principios del Banco Mundial (<http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identificación-for-sustainable-development-toward-the-digital-age.pdf>).
- 2** The Engine Room y Oxfam. (2018). Biométrica en el sector humanitario. <https://www.theengineroom.org/wp-content/uploads/2018/05/Oxfam-Report-May2018.pdf>
- 3** El artículo de KJ Dearie sobre transparencia, rendición de cuentas y control del usuario en leyes de privacidad ofrece ejemplos de leyes estrictas de privacidad de datos. <https://www.good-id.org/en/articles/new-age-data-privacy-3-core-concepts-privacy-laws-around-world/>
- 4** Robinson v. Fiscal general de Jamaica, JMFC Full 04 (Corte Suprema, 2019). <https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf>
- 5** Bhatia, G. (2019, 15 de abril). La otra vida del desacuerdo de Aadhaar: La Corte Suprema jamaicana deroga un sistema biométrico nacional. Medianama. <https://www.medianama.com/2019/04/223-the-afterlife-of-the-aadhaar-dissent-the-jamaican-supreme-court-strikes-down-a-nacional-biometric-identificación-gautam-bhatia/>
- 6** Conoce más sobre licitaciones abiertas para compras en: <https://standard.open-contracting.org/infrastructure/latest/en/>
- 7** Lee más sobre privacidad por diseño en <https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/>

**8** Lee más sobre diseño centrado en los humanos <https://www.ideo.org/herramientas>

**9** Sinni, G. (2017). Diseño participativo para servicios públicos: Innovación en Administración Pública. The Design Journal, 20(1), S3368-S3379, <https://doi.org/10.1080/14606925.2017.1352841>

**10** Mzalouat, P.H. (2018, 22 de marzo). Documento de identidad biométrico: Crónica de un proyecto de ley descartado. Inkyfada. <https://inkyfada.com/fr/2018/03/22/carte-identite-biometrique-tunisie/>

**11** Sayadi, E. (2018, 11 de enero). Identificación biométrica vs. privacidad: ¡Los tunecinos ganan privacidad! Pero la lucha aún no termina. <https://www.accessnow.org/biometric-id-vs-privacy-tunisians-stood-privacy-not-yet/>

**12** Falso positivo: cuando el sistema identifica una coincidencia donde no la hay. Falso negativo: cuando el sistema no logra identificar una coincidencia donde debería.

**13** Islam, M. N. (2018, 26 de noviembre). Bangladesh enfrenta la rabia de los refugiados por el término 'rohinyá', recopilación de datos. Reuters. <https://www.reuters.com/article/us-myanmar-rohingya-bangladesh/bangladesh-faces-refugee-anger-over-term-rohingya-data-collección-idUSKCN1NV1EN>