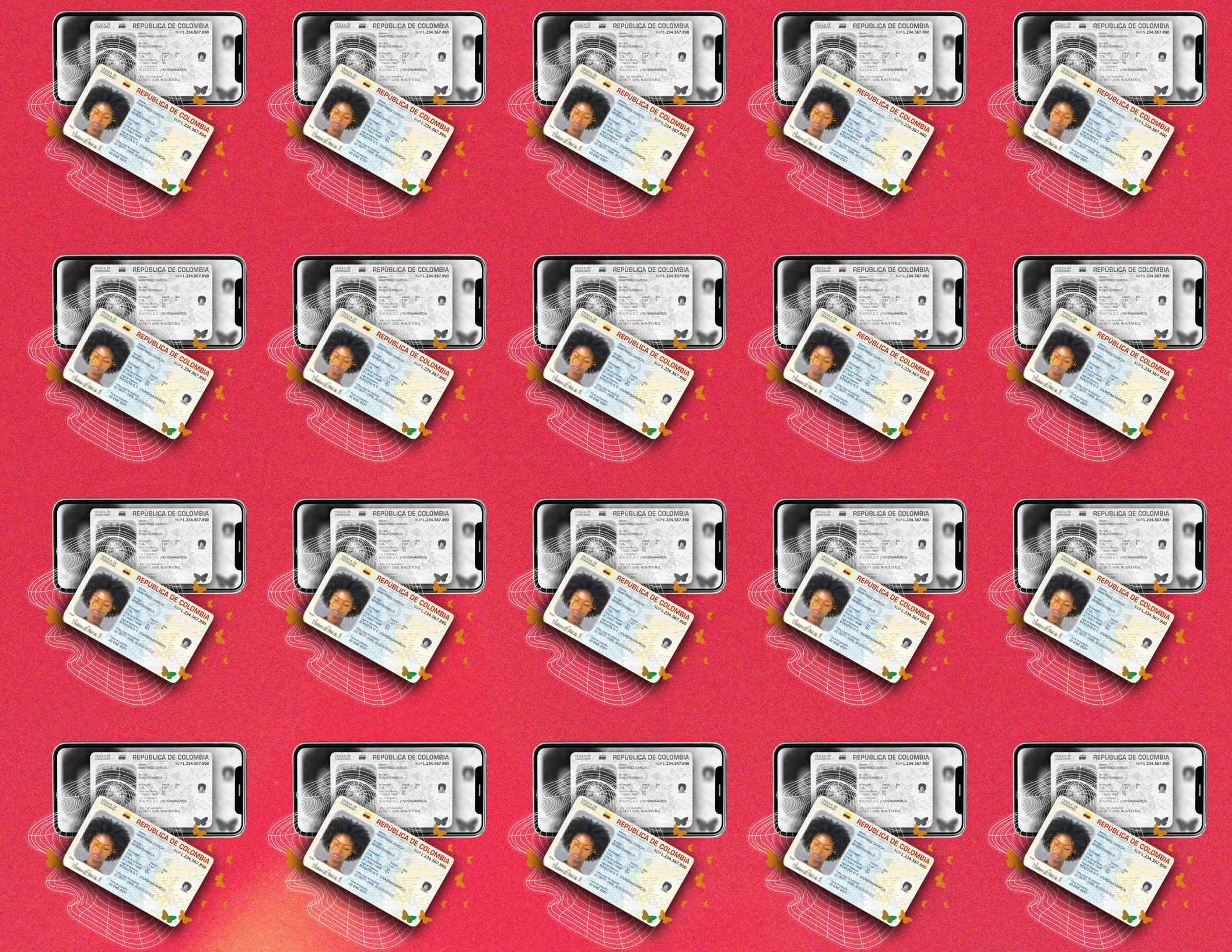
Informe de hallazgos

Análisis de la aplicación CÉDULA DIGITAL

<K+ LAB>

Fundación Karisma


REPÚBLICA DE COLOMBIA
CÉDULA DE CIUDADANÍA
NUIP 1.234.567.890
MARTÍNEZ GARCÍA
MARÍA ISABELA
BOGOTÁ D.C. (CUNDINAMARCA)
30 ENE 2021

Publicación: Septiembre del 2025

Análisis de la aplicación Cédula Digital

Informe de hallazgos

Este informe es resultado de las investigaciones realizadas por el Laboratorio de Seguridad Digital y Privacidad de la Fundación Karisma (K+Lab) durante el segundo semestre del 2024 y enero de 2025.

Fundación Karisma

Somos una organización de la sociedad civil que busca proteger y promover los derechos humanos y la justicia social en el diseño y uso de las tecnologías digitales. Trabajamos en la promoción de los derechos humanos en el mundo digital.

Autoría e Investigación

<K+LAB>

- Dirección de Karisma
  Catalina Moreno Arocha
  Juan Diego Castañeda
- Corrección de estilo
  Nelson La Rotta Marín
- Diseño editorial
  Daniela Moreno Ramírez
- Coordinación editorial
  Natalia Andrade Fajardo
- Apoyo editorial
  Laura Grisales Silva

Esta investigación fue posible gracias al apoyo de la organización Meedan para el desarrollo del análisis y de Open Society Foundation (OSF) para la incorporación de nuevas técnicas de análisis utilizadas en este estudio.

Meedan

OPEN SOCIETY FOUNDATIONS

Este informe está disponible bajo Licencia Creative Commons Atribución 4.0. Esta licencia permite a otros distribuir, mezclar, ajustar y construir a partir de su obra, incluso con fines comerciales, siempre que le sea reconocida la autoría de la creación original.
https://creativecommons.org/licenses/by-sa/4.0/deed.es

CONTENIDO

Resumen ejecutivo 6

1. Introducción 9

2. Metodología 12
2.1 Los ejes de la metodología 12
2.2 Dificultades en nuestra investigación 14

3. La aplicación de la Cédula Digital 16

4. Problemas de funcionalidad y de accesibilidad 20
4.1 Errores y problemas de funcionalidad reportados 20
4.2 Implementación de los nuevos servicios 22
4.3 Procedimiento de expedición de Cédula Digital sin cita 23
4.4 Requisitos de los dispositivos para usar la aplicación 23
4.5 El problema de accesibilidad para personas con ciertas discapacidades 23
Puntos clave del análisis de funcionalidad de Cédula Digital 27

5. Permisos y rastreadores 28
5.1 Permisos sin explicar 28
5.2 Rastreadores en la Cédula Digital: ¿estadísticas o marketing? 30
5.3 Cambios en rastreadores y permisos 33
Puntos clave sobre rastreadores y permisos en Cédula Digital 34

6. ¿Con quién habla y qué dice Cédula Digital? 35
6.1 Primer mapeo 35
6.2 El subdominio de la RNEC 36
6.3 Los dominios de IDEMIA: datos desconocidos y solicitud de permiso 36
6.4 Analíticas de datos y marketing 37
Puntos clave del análisis de tráfico de Cédula Digital 38

7. El papel de IDEMIA: branding local para experimentos globales 39
7.1 El archivo de configuración de Cédula Digital 39
7.2 ¿Una autorización para acceder y compartir datos? Los términos de uso y la política de privacidad “escondidos” de IDEMIA - Estado Unidos 41
7.3 Cuando la RNEC nos habla de IDEMIA 44
Puntos clave del análisis de datos personales y relación entre la RNEC e IDEMIA 48

8. La necesidad de una auditoría de seguridad digital externa, independiente y transparente 49
8.1 Recomendaciones estándar 49
8.2 Servicios abiertos: el interrogante del BGP 50
8.3 SDK de terceros y riesgos de fugas de datos 51
8.4 Cuando los logs siguen hablando (demasiado) 52
8.5 Las URL de configuración en libre acceso revelan debilidades en la autenticación biométrica 52
Puntos clave de la necesidad de una auditoría externa, independiente y transparente 53

9. Información pública: lo que hay y todo lo que falta 54
9.1 Información incompleta (Términos de uso y Política de privacidad) 54
9.2 Desde las tiendas de Apple y Google 56
Puntos clave sobre información pública y transparencia de Cédula Digital 59

Preguntas y preocupaciones para ampliar el debate 60

RESUMEN EJECUTIVO

Este informe es el resultado de una investigación y análisis técnico de la aplicación Cédula Digital de la Registraduría Nacional del Estado Civil (RNEC) de Colombia. El trabajo se llevó a cabo entre el segundo semestre de 2024 y enero de 2025, y fue posible gracias al apoyo financiero de la Fundación MEEDAN.

Durante la investigación, recopilamos y analizamos información pública, solicitamos datos directamente a la RNEC y realizamos distintos análisis funcionales y técnicos. Para ello, utilizamos metodologías replicables, éticas y no intrusivas, apoyadas en herramientas de código abierto, especialmente Pirogue Tool Suite que permite registrar, analizar y descifrar parte de los datos enviados y recibidos por la aplicación, con el fin de comprender su contenido y destinatarios. La implementación de esta herramienta fue posible gracias al apoyo de Open Society Foundations (OSF).

La Cédula Digital es la más reciente propuesta de identificación de la RNEC. Esta pretende convertirse en la llave maestra de la transformación digital en Colombia al permitir la interoperabilidad entre servicios digitales del Estado y su interconexión con servicios financieros, especialmente en la recepción de notificaciones y documentos oficiales.

Con este desarrollo, se busca transformar el paradigma de la identificación y autenticación en Internet mediante el uso de tecnologías biométricas, como el reconocimiento facial. Estas nuevas posibilidades en su implementación abren interrogantes que, desde Karisma, consideramos necesario abordar con una mirada crítica y reflexiva.

Uno de los hallazgos más importantes de esta investigación es el rol de la empresa multinacional IDEMIA en el desarrollo, mantenimiento

y administración de la aplicación y su infraestructura. La relación contractual entre la RNEC y la empresa IDEMIA ya fue analizada en una investigación previa de Karisma[1].

En este trabajo identificamos que la aplicación Cédula Digital es, en realidad, una adaptación local —un rebranding para Colombia— de una aplicación genérica llamada Mobile ID, desarrollada por la empresa IDEMIA, que además mantiene y administra los servidores asociados a las bases de datos correspondientes. También encontramos que Cédula Digital envía datos a dominios externos de IDEMIA y requiere autorizaciones y licencias específicas de sus servidores, en cada uno de sus componentes para poder funcionar.

De acuerdo con la legislación colombiana sobre protección de datos personales, IDEMIA actúa como "encargado del tratamiento de datos personales" para la RNEC, que es la entidad responsable. Sin embargo, en ninguno de los documentos públicos analizados, incluidos los términos y condiciones, la política de privacidad y la información disponible en las tiendas de aplicaciones de Apple y Google, se menciona a IDEMIA.

También identificamos que la aplicación Cédula Digital envía datos a otros servidores externos. Esto es resultado de la inclusión de cinco componentes de terceros que funcionan como rastreadores y están vinculados a fines de analítica de datos y marketing. Entre ellos se encuentran servicios como Localytics —de la empresa estadounidense Upland Software— y Google Ads. Esta práctica plantea serias preocupaciones en materia de privacidad y podría incluso generar riesgos de fuga de datos personales.

Así mismo, se examinó la seguridad digital de la aplicación con algunas limitaciones metodológicas. Destacamos puntos positivos en las implementaciones como la robusta infraestructura a priori y políticas estrictas de cifrado de los datos, entre otros.

1. Karisma (2022). El sistema de identidad administrado por la Registraduría Nacional del Estado Civil. Disponible en: https://digitalid.karisma.org.co/2022/11/27/el-sistema-de-identidad-administrado-por-la-Registraduri-a-Nacional-del-Estado-Civil/

Asimismo, se identificaron fragilidades en la implementación del HTTPS, algunos logs de la aplicación que divulgan datos que no deberían, páginas web de libre acceso que muestran detalles de la configuración técnica y, en particular, un nivel de seguridad de reconocimiento facial y autenticación en línea descrito como “LOW”. Estos elementos son suficientes para plantear que la aplicación necesita una auditoría de seguridad digital y privacidad externa independiente y transparente, de la misma manera que lo pedimos para el software de Elecciones.

Por último, la investigación resalta algunas barreras de accesibilidad para las personas usuarias; por ejemplo, la necesidad de tener equipos móviles muy recientes con un sistema operativo mínimo de Android 12 e iOS 17, lo que excluye a gran parte de la población colombiana. Por otro lado, la activación de la aplicación con reconocimiento facial presenta un alto nivel de dificultad para personas con discapacidad visual, incluso cuando es moderada. Ambos problemas de accesibilidad se heredan de la aplicación genérica de IDEMIA.

Con este informe queremos plantear una reflexión general sobre las consecuencias a largo plazo de cambiar el paradigma de autenticación en los servicios digitales, que brinda soluciones múltiples y variadas, para reemplazarlo por una identificación y autenticación mediante servicios centralizados basados en biometría y monopolizados por empresas multinacionales que controlan estas tecnologías. Por eso, desde Karisma, nos preguntamos si los problemas de soberanía, autonomía, exclusiones diversas, privacidad e incluso seguridad digital no serán superiores a los aparentes beneficios.

I. INTRODUCCIÓN

Fundación Karisma[2] es una organización de la sociedad civil dedicada proteger y promover los derechos humanos y la justicia social en el diseño y uso de las tecnologías digitales. A través del activismo con múltiples enfoques legales y tecnológicos, Karisma articula su trabajo colaborando con socios locales, regionales e internacionales mediante coaliciones estratégicas.

Desde hace años, el Laboratorio de seguridad digital y privacidad (K+Lab) analiza aplicaciones y sitios web de interés público con una perspectiva de derechos humanos. Sus análisis se centran en la protección de datos, la seguridad digital y la privacidad. Además, con la intermediación del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia[3] (MINTIC) hemos contribuido a mejorar sitios webs y aplicaciones en aspectos como la transparencia sobre el desarrollo, información pública sobre los permisos solicitados, términos y condiciones de uso, seguridad digital y privacidad. Este trabajo ha sido reconocido tanto por el Gobierno de Colombia como por organizaciones internacionales[4].

La aplicación Cédula Digital reviste un interés particular, ya que permite la identificación de la ciudadanía, la autenticación en servicios digitales del Estado o del sector financiero, así como la recepción de documentos y notificaciones oficiales, entre otras funciones.

2. Consultar: https://web.karisma.org.co

3. Consultar: https://web.karisma.org.co/wp-content/uploads/download-manager-files/INFORME%20CONJUNTO.pdf

4. Karisma (2021) Encouraging vulnerability treatment, responsible management, handling and disclosure of vulnerabilities, OECD, p. 71. Disponible en: https://web.karisma.org.co/wp-content/uploads/2022/06/DSTI-CDEP-SDE20203-FINAL.en_-1.pdf

Esta investigación se centra en la aplicación Cédula Digital[5] y, con ella, continuamos los trabajos de investigación e incidencia realizados previamente en ámbitos de identificación, uso de biometría, empresas privadas en sistemas tecnológicos vitales para el Estado colombiano y de principios de derechos humanos para el desarrollo de programas de identificación[6]. En "A promising playground": IDEMIA and the digital infrastructuring in Colombia, escrito en 2024, por López-Solano y Castañeda[7], se analiza cómo la RNEC se ha convertido en la entidad pública con el monopolio de la gestión de identificación y autenticación —ahora en conexión con la biometría— en Colombia y cómo la empresa francesa IDEMIA[8] ha tenido un papel central desde el año 2000. López-Solano y Castañeda resaltan que:

> el caso de IDEMIA y de la Registraduría expone un proceso mezclado en el cual no es fácil distinguir entre lo público (no comercial) y lo privado (comercial). Es casi imposible saber dónde empieza la Registraduría y dónde termina IDEMIA[9].

Esta investigación intenta **responder a la pregunta sobre el rol de la empresa IDEMIA (y otras empresas) en el desarrollo y el funcionamiento de aplicación Cédula Digital para abrir el debate sobre la soberanía estatal en contextos estratégicos.** También, analizamos problemáticas vinculadas con accesibilidad, inclusión, privacidad y seguridad digital de la aplicación, enfoques habituales de los trabajos realizados por el K+Lab estos últimos años.

En Karisma hemos explorado estos requisitos a través del micrositio *Identidad digital y Derechos Humanos*[10], planteando los siguientes principios para un sistema de identidad que proteja los derechos humanos:

- ***Privacidad y protección de datos personales:*** entender cuáles son los datos personales que emplea la aplicación, la finalidad de uso y las implicaciones en términos de privacidad para las personas usuarias. Nos centramos particularmente en los datos biométricos, considerados en Colombia como datos sensibles según la Ley de protección de datos personales[11].

5. Consultar: https://wapp.registraduria.gov.co/identificacion/cedula-digital/

6. Al respecto, revisar el programa de Karisma: digitalid.karisma.org.co

7. López-Solano y Castañeda (2024) "Un terreno de juego prometedor": IDEMIA y la infraestructura de identidad digital en Colombia, que hace alusión a una publicación de IDEMIA que califica así Colombia para experimentar nuevas formas de identidad digital a través de la aplicación Cédula Digital, como se verá más adelante. Disponible en inglés: https://www.tandfonline.com/doi/full/10.1080/1369118X.2024.2302995

8. Consultar: https://www.idemia.com/

9. López-Solano y Castañeda, op cit. Traducción nuestra.

10. Consultar: https://digitalid.karisma.org.co/2021/12/07/principios-id/

11. Ley estatutaria 1581 de 2012, artículo 5.

- *Seguridad digital:* verificar la implementación de estándares de seguridad digital como medidas de protección de alto nivel, teniendo en cuenta la cantidad de datos utilizados, la sensibilidad de estos y las funcionalidades particulares de la aplicación (capítulo 8).
- *Accesibilidad:* analizar cómo los requisitos o diseños técnicos imponen barreras arbitrarias o injustas a sectores de la población en razón de sus distintas condiciones, cuáles grupos pueden acceder a esta forma de identificación, teniendo en cuenta su diseño, la experiencia de usuario y configuraciones técnicas.

Finalmente, considerando el carácter aún experimental de esta aplicación, resulta necesario abrir el debate en torno al uso de tecnologías biométricas para la autenticación de identidad en servicios digitales públicos y privados, así como a la creciente delegación de esta función a actores privados.

Este documento está conformado por nueve capítulos. Luego de esta introducción, en el capítulo 2 describimos la metodología empleada para realizar el análisis, así como las dificultades encontradas para acceder a la información necesaria. En el capítulo 3 presentamos una descripción general de la aplicación Cédula Digital, y en el 4 abordamos algunos problemas de funcionalidad, tanto de la aplicación como del procedimiento de expedición del documento, especialmente desde una perspectiva de inclusión.

El capítulo 5 ofrece un análisis de los permisos y rastreadores que utiliza la aplicación, mientras que en el 6 se presentan los resultados del análisis de tráfico de datos. En el capítulo 7 comentamos la relación entre IDEMIA y la Registraduría Nacional del Estado Civil (RNEC), a partir de la información obtenida durante esta investigación. El capítulo 8 identifica varios problemas de seguridad digital que evidencian la necesidad de una auditoría externa, independiente y transparente en esta materia. En el 9 analizamos la información pública disponible sobre el sistema en su conjunto.

Finalmente, cerramos el documento con una serie de preguntas que invitan a reflexionar sobre el análisis realizado, especialmente desde las perspectivas de la soberanía digital, la intimidad, la protección de datos y la seguridad digital.

2. METODOLOGÍA

2.1 Los ejes de la metodología

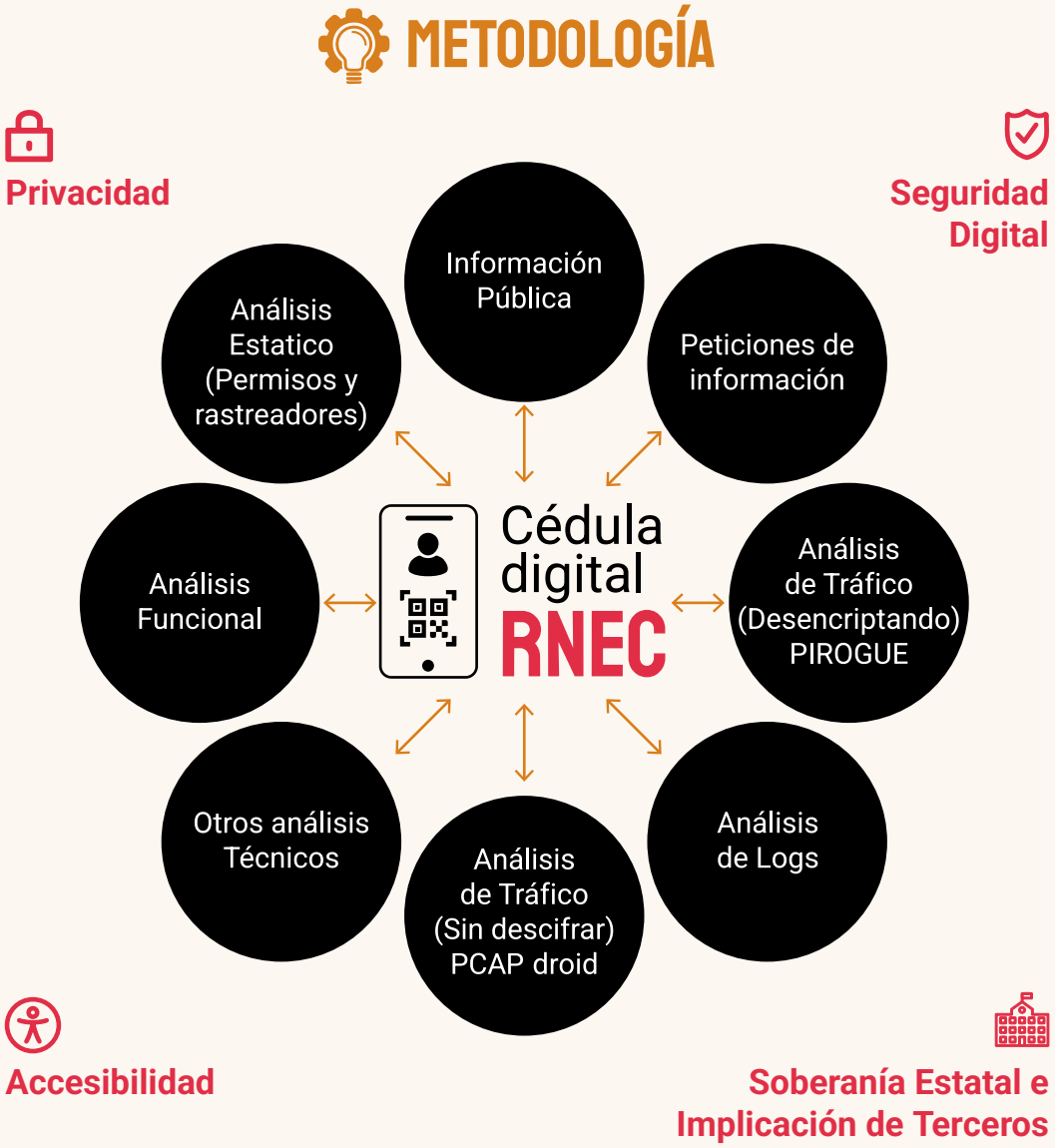


Figura 1. Metodología de investigación

En la figura 1 se presenta la estructura del análisis, basada en ocho ejes metodológicos que combinan aspectos técnicos y no técnicos. Es importante resaltar que los análisis técnicos realizados fueron no intrusivos, reproducibles y éticos. Los ocho ejes metodológicos se organizan de la siguiente manera:

1. **Información pública:** se analizó información pública del sitio web de la RNEC y de las empresas involucradas, también en las tiendas de Google y Apple, en la aplicación misma, e Internet en general. Esto sumado a los registros de dominios webs, de direcciones IP y certificados criptográficos.

2. **Solicitud de información:** se envió un derecho de petición a la RNEC el 25 de noviembre del 2024[12], que fue respondido parcialmente por la entidad el 8 de enero de 2025. Se mandó también un "Recurso de insistencia" a la RNEC el 22 de enero del 2025 que no fue respondido,

3. **Análisis funcional:** se realizaron pruebas funcionales sobre los procesos de registro, activación y uso de la aplicación con personas usuarias voluntarias, en entornos Android e iPhone.

4. **Análisis estático (permisos y rastreadores de la aplicación):** se analizaron (indirectamente y vía herramientas automatizadas) los permisos y rastreadores que se encuentran en el APK de la versión Android de la aplicación. Se usaron las herramientas de código abierto Exodus Privacy[13] y ClassyShark3xodus[14] que permiten listar los permisos de la aplicación y sus rastreadores.

5. **Análisis de logs:** se analizaron los registros de eventos (logs) generados por el uso de la aplicación. En Android por medio de la aplicación de código abierto Pidcat[15] y en iPhone con idevicesyslog, de la librería de código abierto libmobiledevice[16].

6. **Análisis de tráfico local y sin descifrar:** el primer análisis de tráfico generado por la aplicación en funcionamiento se realizó usando la aplicación de código abierto PCACdroid[17] instalada en un teléfono Android, esto aísla el tráfico de red generado por la aplicación y facilita grabarlo. Este análisis permite establecer los dominios y direcciones IP hacia los cuales se conecta la aplicación

12. Se registró con el radicado RNEC-E-2024-203754.

13. Consultar: https://exodus-privacy.eu.org/en/

14. Consultar: https://fossdd.gitlab.io/fdroid-website/en/packages/com.oF2pks.classyshark3xodus/

15. Consultar: https://github.com/JakeWharton/pidcat

16. Consultar: https://libimobiledevice.org

17. Consultar: https://play.google.com/store/apps/details?id=com.emanuelef.remote_capture&hl=es

7. **Análisis de tráfico cifrado:** se realizó un segundo análisis del tráfico generado por la aplicación en funcionamiento, descifrando el protocolo HTTPS[18]. Esto permite observar el contenido de los paquetes de datos y saber qué tipo de datos envía y recibe la aplicación. Para lograrlo, se usó la herramienta de código abierto Pirogue Tool Suite[19] instalada localmente en un raspberry Pi[20] y un teléfono Android con permisos de superusuario (root).

   Es importante resaltar que esta herramienta permite acceder a las llaves criptográficas en la memoria del teléfono donde está instalada la aplicación, sin necesidad de generar certificados criptográficos o modificar el código fuente de la aplicación. Por esto, es un método de investigación que incluso agencias de protección de datos y regulatorias usan para sus investigaciones[21]. Algunas partes del tráfico de la aplicación se descifraron y otras no[22]. Además, analizamos también el tráfico generado por los formularios web vinculados con Cédula Digital, en el sitio web de la RNEC.

8. **Otros análisis técnicos:** se realizó el estudio de los certificados criptográficos manejados por la aplicación o la identificación de tecnologías web con la herramienta Wappalyzer[23].

2.2 Dificultades en nuestra investigación

Además de los retos técnicos, varios factores dificultaron nuestro análisis: la falta de información pública, las respuestas incompletas a nuestra solicitud de información y el código propietario, que implica que no existe una forma libre de acceso al código fuente de la aplicación por la propiedad intelectual del desarrollador.

La información disponible públicamente sobre la aplicación es bastante limitada y omite puntos importantes, en particular en cuanto al papel de terceros, las empresas que la implementan, y la protección de los datos personales de las personas usuarias, como lo detallamos más adelante.

18. HyperText Transfer Protocol Secure de su sigla en inglés, en español “protocolo seguro de transferencia de hipertexto”. Consiste en la encapsulación del protocolo estándar HTTP en el protocolo cifrado SSL o su sucesor TLS.

19. Consultar: https://pts-project.org/

20. Un raspberry Pi es un pequeño computador, consutar: https://www.raspberrypi.com/

21. Consultar: https://pts-project.org/guides/g10/

22. En especial se tuvo problemas para descifrar el tráfico relacionado con el reconocimiento facial. La hipótesis principal es que esto se debe a la versión de Android o de componentes hardware de la cámara del teléfono usadas en estas pruebas. Para el correcto funcionamiento de estas funcionalidades, la aplicación necesita de versiones actualizadas del sistema operativo. Puede ser que la aplicación tenga contramedidas adicionales no identificadas que bloqueen el análisis de tráfico cifrado utilizando Pirogue/Frida.

23. Consultar: https://www.wappalyzer.com/

Por ello, solicitamos información[24] directamente a la RNEC, pero solo obtuvimos respuesta a 8 de las 20 preguntas planteadas. En general, la RNEC justifica la negativa a proporcionar información alegando reserva por motivos de seguridad nacional, sin explicar en qué fundamenta esta decisión ni explorar alternativas para entregar información sin comprometer la reserva, como exige la ley. Además, algunas respuestas fueron incompletas. Por esto, posteriormente, el 22 de enero del 2025, enviamos un Recurso de insistencia a la RNEC y que no ha respondido hasta la fecha.

Finalmente, elegir una **solución que es propiedad de la empresa IDEMIA para una aplicación tan sensible**, en lugar de una aplicación de código abierto, o cómo mínimo de propiedad del Estado[25], introduce limitaciones en cuanto al acceso al código fuente y las posibilidades de análisis y auditorías técnicas externas e independientes[26]. Además, la aplicación implementa barreras y contramedidas técnicas que son necesarias, pero dificultan los análisis técnicos. La aplicación implementa bloqueo de pantallazos, y parece implementar contramedidas como el certificate pinning[27] o la detección de root.

Es importante señalar que tener un teléfono en estado root, o para los iPhone con jailbreak, significa haber desbloqueado el acceso a funcionalidades del sistema operativo a las cuales normalmente no se puede acceder. Si bien en el caso de Apple, la condiciones de uso no permiten esta operación, en el caso de Android, muchas empresas (en particular Google) lo permiten, considerando que es una posibilidad legítima del cliente tener acceso a todas las funcionalidades de su dispositivo.

24. Carta del 8 de enero del 2025, en respuesta a nuestro derecho de petición del 25 de noviembre del 2024 (se extendió el periodo legal para responder pidiendo un tiempo adicional de 15 días hábiles). Está firmada por Álvaro Alfonso Araujo Oñate, director nacional de identificación de la RNEC.

25. En este aspecto de la propiedad de la aplicación y de su código fuente parece existir una ambigüedad. Si bien en la pantalla de inicio de la aplicación aparece “Copyright 2023, Todos los derechos reservados, Registraduría Nacional del Estado Civil / Colombia” los términos y condiciones de IDEMIA (que se estudian en el apartado 7) permiten sospechar sobre propiedad intelectual de la firma de la aplicación y su código fuente.

26. Es una problemática similar a la del software Elecciones que Karisma y otras organizaciones resaltaron en numerosas publicaciones. Por ejemplo, en un comunicado de prensa de 2023, lo expresamos: “Por otro lado, aunque entendemos que la negociación con el contratista DISPROEL en este aspecto puede ser complicada, queremos reiterar que para nosotros el hecho de que el software de escrutinio y su solución tecnológica no sean propiedad del Estado sino de una empresa privada sigue siendo un problema de fondo y que la propiedad intelectual no puede ser una barrera para la observación electoral.”. Comunicado de prensa 01: Observación técnica a las elecciones regionales de 2023. Continúan los problemas de acceso a información previa a los comicios. Disponible en: https://web.karisma.org.co/comunicado-de-prensa-01-observacion-tecnica-a-las-elecciones-regionales-de-2023-continuan-los-problemas-de-acceso-a-informacion-previa-a-los-comicios/.

27. Es una contramedida que introduce la verificación de las características de los certificados criptográficos de los servidores con los cuales la aplicación se comunica (en general con un hash). Impide los análisis de tráfico de la aplicación con métodos clásicos de tipo “Man in the Middle SSL” que usan certificados propios. Esta contramedida puede tener justificaciones de seguridad digital.

3. LA APLICACIÓN DE LA CÉDULA DIGITAL

La aplicación Cédula Digital fue anunciada el primero de diciembre de 2020 por el presidente Iván Duque, el Ministerio de Tecnologías de la Información y las Comunicaciones, a cargo de Karen Abudinen, y la Registraduría Nacional del Estado Civil, en cabeza de Alexander Vega. Su primera versión fue publicada en enero del 2021 en las tiendas de aplicaciones de iPhone y Android[28]. Inicialmente, la aplicación solo tenía la funcionalidad de **identificación de los ciudadanos colombianos**. Es decir, presentar una versión digital de la cédula de ciudadanía física para identificarse presencialmente. Sin embargo, el expresidente Duque ya anunciaba sus futuras metas y funcionalidades:

> Con este nuevo paso, Colombia sigue a la vanguardia y vamos por ese primer lugar (en el ranking de la OCDE), porque se habilitan los Servicios Ciudadanos Digitales y empezamos una plataforma que será la Carpeta Ciudadana Única de bases de datos interactivas entre todas las dependencias. Y esta cédula es el camino para materializarlo[29].

La aplicación fue desarrollada por medio de una adición a un contrato ya existente[30] entre la RNEC y la empresa IDEMIA[31].

La importancia de IDEMIA en el desarrollo de las funciones de la Registraduría ha aumentado de forma sostenida en la última década, con un crecimiento sin precedentes durante el periodo 2020-2021. Este incremento también se refleja en el monto de los contratos suscritos entre la RNEC y la multinacional.

28. Disponibles en: https://apps.apple.com/co/app/cedula-digital-colombia/id1543274615 y https://play.google.com/store/apps/details?id=co.gov.registraduria.ceduladigital&hl=es_CO

29. MINTIC. Comunicado de prensa, 1 de diciembre 2021. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/160459:Con-la-nueva-cedula-la-prestacion-de-los-Servicios-Ciudadanos-y-la-transformacion-tecnologica-Colombia-avanza-a-paso-firme-ministra-Karen-Abudinen

30. Adición No. 1 y Otrosí No 03. Al contrato de prestación de servicios No. 002 de 2020 sus condiciones adicionales y sus otrosí No. 1 y 2 de 2020, suscrito entre la Registraduría Nacional del Estado Civil e Idemia Identity & Security Sucursal Colombia.

31. https://www.lasillavacia.com/detector-de-mentiras/falso/detector-otra-vez-la-cedula-digital-ya-existe-y-smartmatic-no-esta-involucrada/

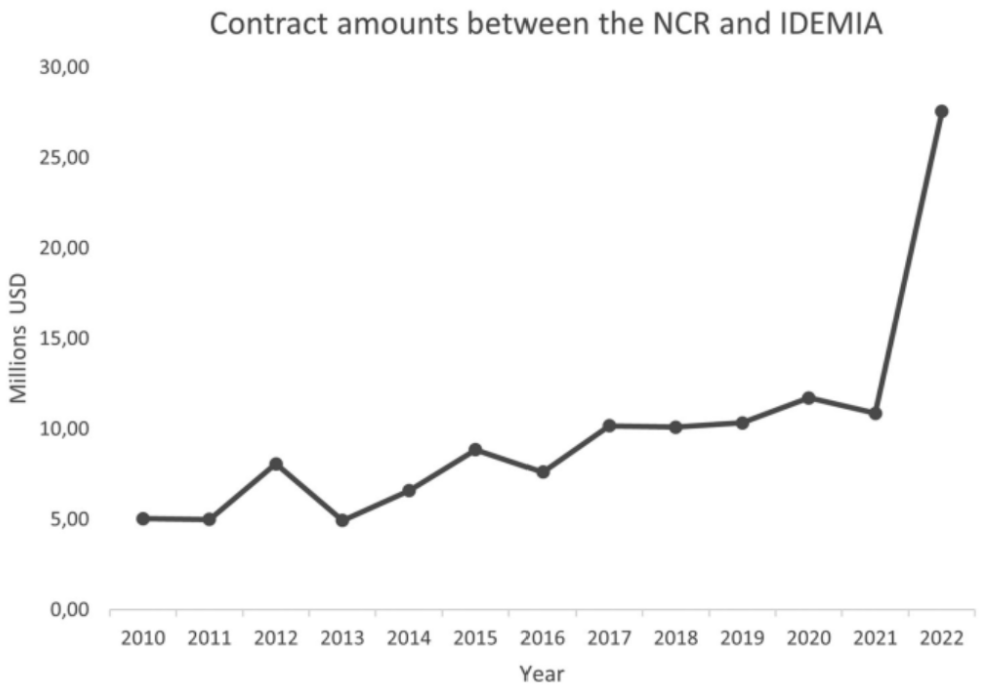


Figura 2. Monto de los contratos entre la RNEC e IDEMIA entre 2010 y 2022 en USD
Fuente: López-Solano y Castañeda (2024) usando los datos extraídos del Sistema Electrónico para la Contratación Pública (SECOP) de los contratos entre la RNEC e IDEMIA.

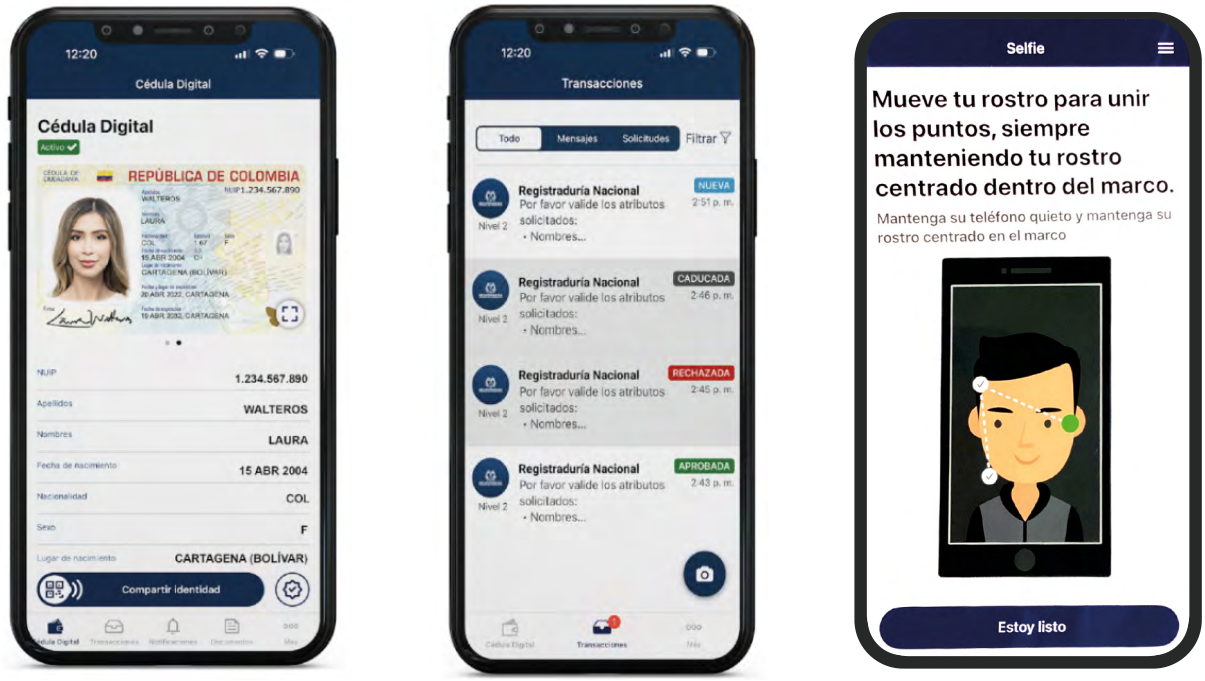
En noviembre 2023, la RNEC anunció oficialmente el lanzamiento de la versión 2 de la aplicación con nuevas funcionalidades[32]:

- **Autenticación en transacciones virtuales:** se podrán hacer mediante el protocolo de identidad OIDC[33], con altos niveles de seguridad a través de autenticación biométrica facial y PIN. La aplicación también usa biometría dactilar.
- **Notificaciones:** posibilidad de recibir y gestionar notificaciones de entidades públicas y financieras con la confirmación de lectura y documentos adjuntos.
- **Documentos:** capacidad de recibir documentos, leerlos y firmarlos con certificado digital, almacenarlos y posibilidad de compartirlos a terceros.

32. Noticia completa: https://www.registraduria.gov.co/Cedula-digital-2-0-nueva-actualizacion-contiene-la-autenticacion-de-la-firma-de.html

33. El protocolo OIDC para OpenID Connect permite centralizar la identificación y autenticación, delegando a un servidor. Según Wikipedia es "una capa de identidad sobre el protocolo de autenticación OAuth 2.0, el cual permite a los clientes verificar la identidad de un usuario basado en la autenticación realizada por un servidor de autorización, así como para obtener información de perfil del usuario utilizando un esquema REST". El protocolo es desarrollado por la OpenID Foundation, para más información consultar: https://openid.net/.

Los siguientes pantallazos de la aplicación Cédula Digital ilustran estas funcionalidades:



a. Identificación

b. Autenticación en línea y recepción de notificaciones

c. Activación de la Cédula Digital con reconocimiento facial

Figura 3. Pantallazos de la aplicación Cédula Digital
Fuentes: Tienda de Google para a y b[34], c es una foto nuestra.

Sin embargo, hasta la fecha, no encontramos información pública específica que detalle cuáles entidades públicas o financieras en Colombia han implementado la autenticación a través de Cédula Digital en sus trámites y servicios. Adicionalmente, la RNEC no respondió este punto cuando solicitamos información[35]. **Si bien la implementación de esta funcionalidad ya existe en la aplicación, no conocemos desarrollos o implementaciones en posibles entidades usuarias.**

34. Disponibles en: https://play.google.com/store/apps/details?id=co.gov.registraduria.ceduladigital&hl=es&pli=1

35. Pregunta 2 del Derecho de Petición del 25 de noviembre de 2024: "Indique detalladamente ¿Cuáles son los servicios digitales públicos y/o de entidades privadas que están usando el protocolo de autenticación OIDC -al día de hoy- a través de la nueva aplicación Cédula Digital? Adjunte el acto administrativo o la norma, cualquiera sea su naturaleza, que otorga competencia a las entidades privadas para usar ese tipo de protocolos". Respuesta: "No se suministra información ya que la misma cuenta con carácter de reserva según lo establecido en el artículo 24, literal primero, de la Ley 1755-2025".

Hay que resaltar que, a nivel mundial, el uso de una aplicación de identidad digital con biometría para identificar y autenticar a la ciudadanía es todavía novedosa y plantea importantes problemas de protección de datos. La multinacional IDEMIA, especializada en estas tecnologías está experimentando sus nuevas tecnologías de identificación y autenticación en Colombia, Marruecos, Estonia y Lituania[36], y en algunos estados de Estados Unidos para licencias de conducción[37].

Además de la propia aplicación, también analizamos tres formularios **web vinculados con Cédula Digital que están en el sitio web de la RNEC.**

Finalmente, la función de identificación de los ciudadanos colombianos de la aplicación Cédula Digital se usa en conexión con otra aplicación llamada **Verificación de Identidad[38]**. Esta aplicación es una adaptación para Colombia de la aplicación Verify de IDEMIA[39] y es usada por la policía colombiana para realizar verificaciones de identidad[40] usando el protocolo Bluetooth[41]; resaltamos que esta segunda aplicación no se analizó en el marco de esta investigación.

36. "Our documents are widely acknowledged for the high security level they provide. Since 2019, our eID cards in Estonia, Latvia, Morocco and Colombia, have been awarded as best new ID cards by the industry during the High Security Printing conferences". Identity week (2023) Julien DROUET, VP Identity Solutions at IDEMIA. Disponible en: https://identityweek.net/julien-drouet-vp-identity-solutions-at-idemia/

37. Estas tecnologías de identificación/autenticación fueron probadas por IDEMIA inicialmente en Colombia y en los estados de Oklahoma, Delaware y Arizona. Información disponible en: https://www.idemia.com/wp-content/uploads/2022/02/mobile-id-based-approach-to-digital-id-idemia-brochure-202202.pdf

38. Consultar: https://play.google.com/store/apps/details?id=co.gov.registraduria.verificar&hl=es_CO

39. Consultar: https://idemia-mobile-id.com/about-mobileidverify

40. Consultar: https://www.registraduria.gov.co/Registraduria-Nacional-desarrolla-aplicativo-movil-de-verificacion-de-identidad.html

41. En la respuesta al derecho de petición que hicimos, la RNEC menciona, en cuanto al uso del permiso Bluetooth, que "Bluetooth: se solicita al usuario, su uso es para compartir atributos con la aplicación de Verify".

4. PROBLEMAS DE FUNCIONALIDAD Y DE ACCESIBILIDAD

4.1 Errores y problemas de funcionalidad reportados

Al analizar los comentarios en las tiendas de aplicaciones móviles, confirmamos la recurrencia de problemas técnicos en distintas versiones de la aplicación. La mayoría de los reportes señalan la falta de información clara sobre su funcionamiento y la ausencia de pruebas previas al lanzamiento de nuevas funcionalidades. En la App Store de Apple, al momento de redactar este informe, la aplicación tenía una calificación promedio de apenas 1.8 sobre 5.

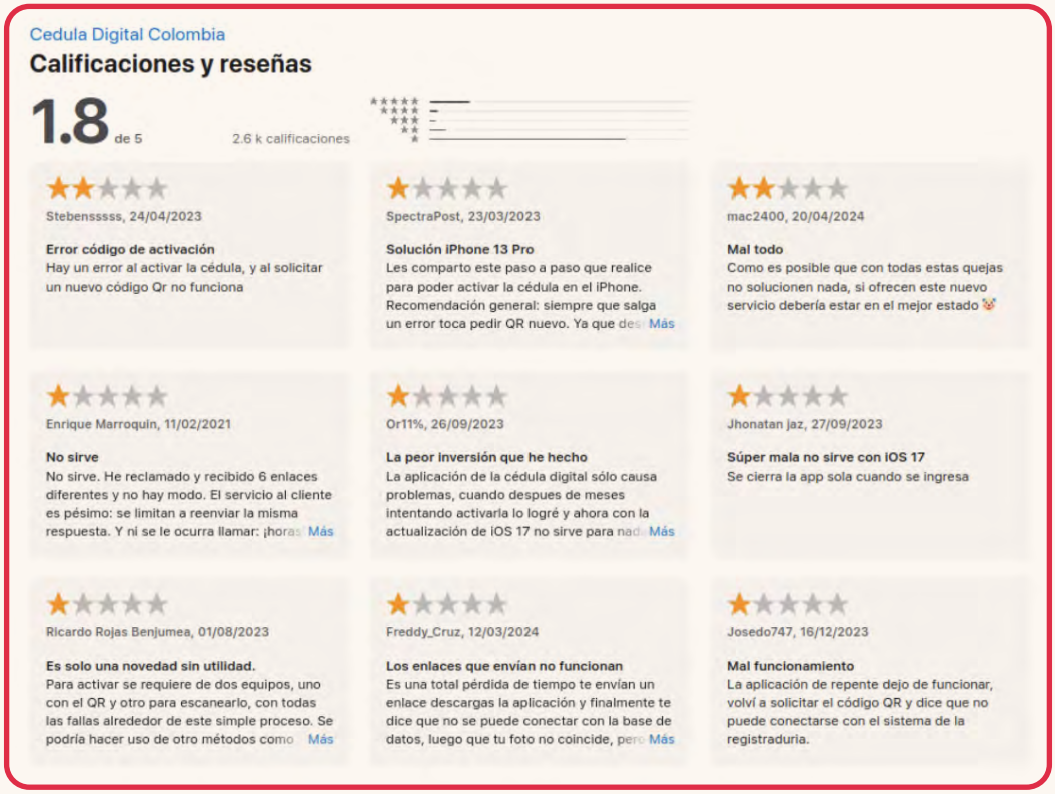


Figura 4. Calificaciones de Cédula Digital en la tienda de Apple Fuente: App Store[42].

42. Calificaciones disponibles en: https://apps.apple.com/co/app/cedula-digital-colombia/id1543274615

En la tienda de Google la clasificación es mejor, pero las personas usuarias también señalan bastantes problemas.

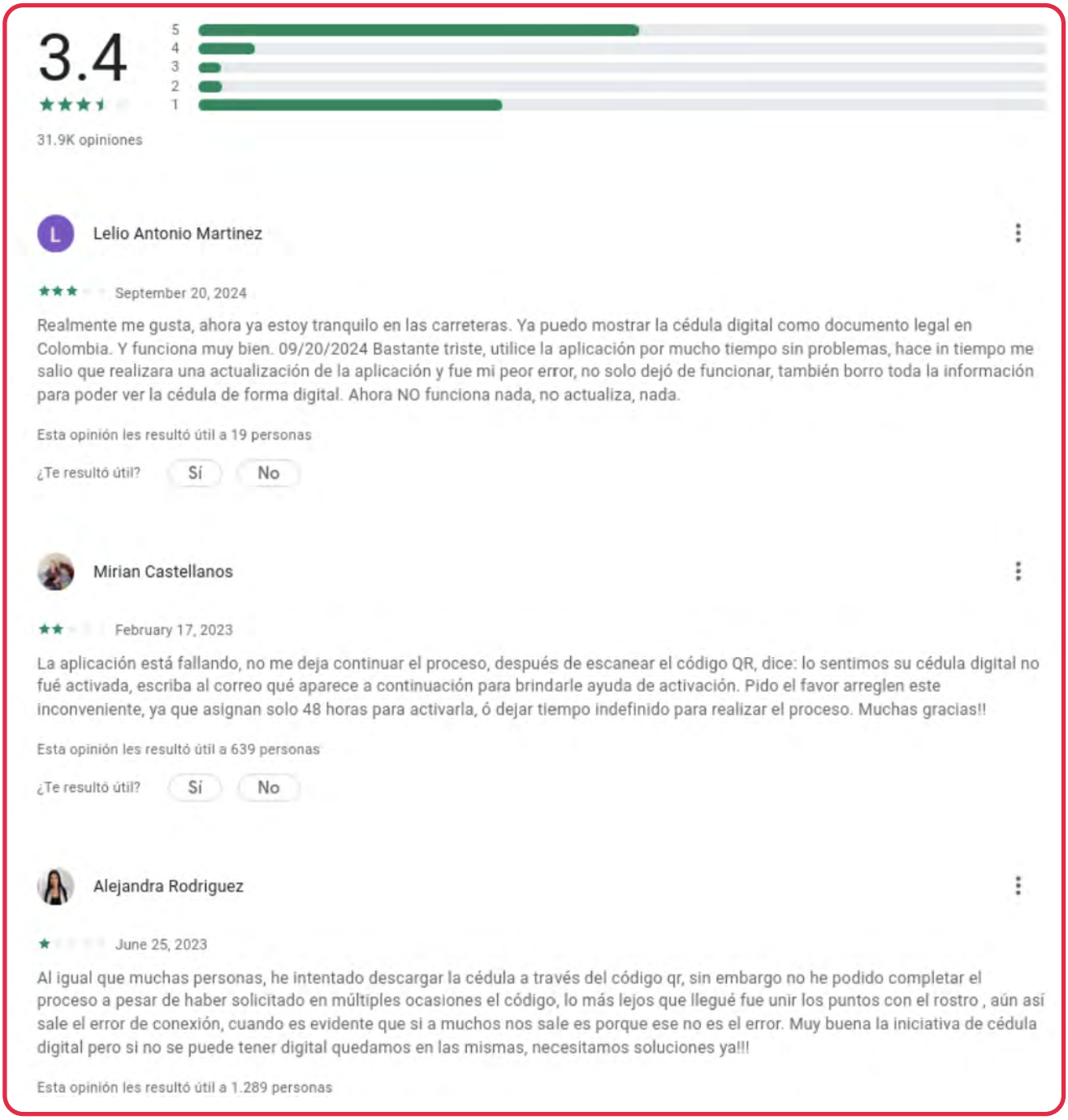


Figura 5. Extracto de las calificaciones de Cédula Digital en la tienda de Google
Fuente: Play Store de Google[43]

43. Se pueden consultar en su totalidad aquí: https://play.google.com/store/apps/details?id=co.gov.registraduria.ceduladigital&hl=es_CO

4.2 Implementación de los nuevos servicios

Según la información pública de la tienda de Apple y las notificaciones que nos aparecieron en Android, la aplicación parece integrar ya la nueva funcionalidad de autenticación en línea para servicios de terceros.

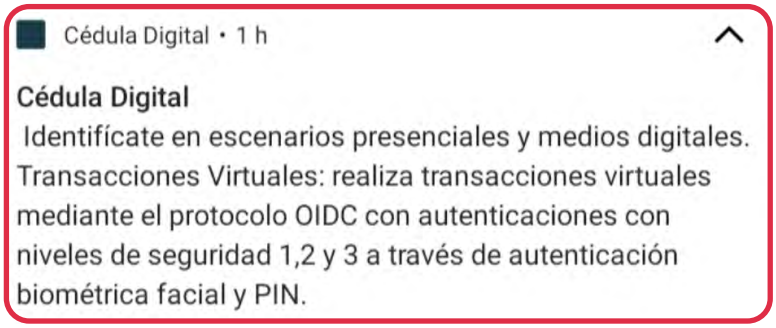


Figura 6. Notificación recibida el 23 de septiembre 2024
Fuente: Captura de pantalla.

La aplicación parece poder también recibir mensajes, notificaciones oficiales y documentos:

Figura 7. Sección de mensajes y solicitudes de la aplicación
Fuente: Captura de pantalla.

Sin embargo, al momento de redactar este informe no se identificaron entidades públicas o privadas que estén usando estas nuevas funcionalidades.

4.3 Procedimiento de expedición de Cédula Digital sin cita

El sitio web de la RNEC dedicado a la Cédula Digital se denomina “Tu Cédula Digital sin cita”[44] y el formulario web “Tramita la Cédula Digital sin agendar cita” permiten inferir que la aplicación se puede activar directamente en línea y sin agendar cita. Sin embargo, en realidad, el proceso exige ir presencialmente a oficinas habilitadas de la RNEC por lo menos dos veces[45].

Figura 8. Formulario web “Tramita la Cédula Digital sin agendar cita”
Fuente: Sitio web de la RNEC.

44. Consultar: https://wapp.registraduria.gov.co/identificacion/cedula-digital/#inicio

45. Se requiere ir a la oficina al comienzo del trámite para registrar datos personales (incluyendo dirección física), información biométrica (fotografía y huellas de los diez dedos de las manos) y verificar la cédula física de la persona. Posteriormente, cuando se completa el trámite, se debe ir una segunda vez para recibir la nueva cédula física y un código QR de activación de la aplicación.

El formulario web "Tramita la Cédula Digital sin agendar cita" solo permite hacer el pago en línea de la solicitud por PSE. Sin embargo, en las dos pruebas realizadas, no funcionó para este proceso. En la pregunta 12 de la solicitud de información pedimos a la RNEC confirmar si se trataba de un error técnico en el formulario web, pregunta que no fue respondida:

> La página web del sitio de la Registraduría "Tu Cédula Digital sin cita" apunta a través de su link de pago a un formulario web titulado "Tramita la Cédula Digital sin agendar cita". Sin embargo, cuando intentamos llenar este formulario con datos de personas voluntarias (desde distintas configuraciones) nunca funcionó. Confirme si se trata de un error técnico e indique:
>
> - ¿Cuál es el objetivo de este formulario web?
> - ¿Es posible tramitar la Cédula Digital sin agendar cita?
>
> La RNEC nos responde:
> "En atención a su petición, es pertinente mencionar que el formulario 'Tramita la Cédula Digital sin agendar cita' es con el fin través (SIC) de este link https://ceduladigital.registraduria.gov.co/index es con el fin de realizar directamente el pago de la Cédula Digital[46]".

Además, las personas que nos ayudaron en las pruebas funcionales llenaron el formulario sin recibir ninguna confirmación en la pantalla después de registrarse y la página las regresaba al formulario vacío. No recibieron correo de confirmación y tampoco fue posible acceder a la página de "Inicio de sesión" asociada[47] con el correo y la contraseña diligenciados en el formulario.

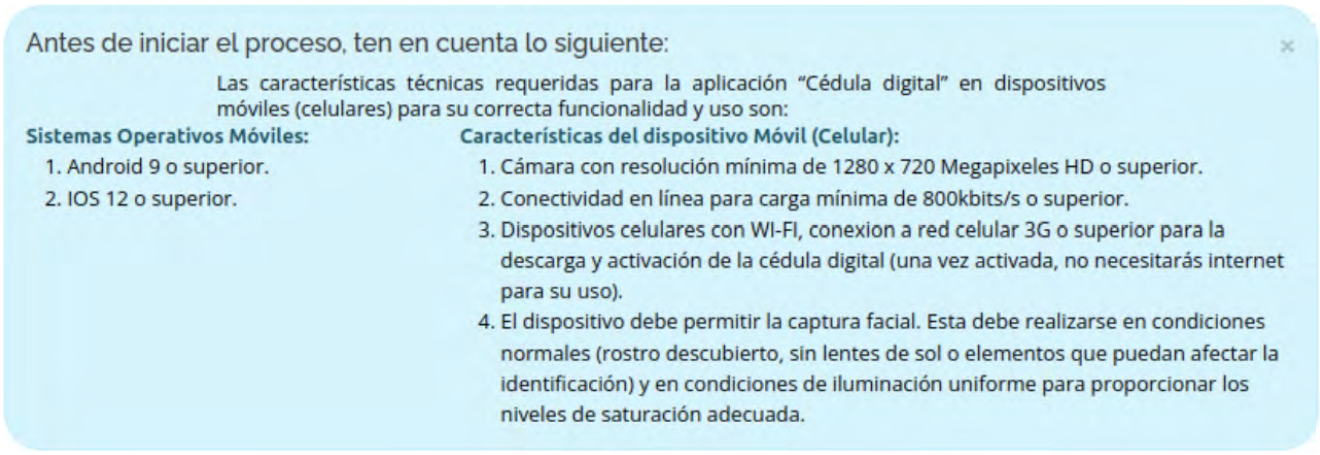
Finalmente, los análisis técnicos realizados sobre los datos enviados por el formulario y las respuestas de los servidores mostraron que efectivamente **el formulario tiene errores técnicos,** uno de ellos generando un bucle que no permite su correcto funcionamiento y que explica porque siempre vuelve al formulario vacío después de mandarlo. (anexo 2).

46. Respuesta a nuestro derecho de petición, pregunta 12.

47. Consultar: https://ceduladigital.registraduria.gov.co/login

4.4 Requisitos de los dispositivos para usar la aplicación

En la página del formulario “Tramita la Cédula Digital sin agendar cita” encontramos esta información sobre los requisitos de la aplicación:


Antes de iniciar el proceso, ten en cuenta lo siguiente:

Las características técnicas requeridas para la aplicación “Cédula digital” en dispositivos móviles (celulares) para su correcta funcionalidad y uso son:

Sistemas Operativos Móviles:

1. Android 9 o superior.
2. IOS 12 o superior.

Características del dispositivo Móvil (Celular):

1. Cámara con resolución mínima de 1280 x 720 Megapixeles HD o superior.
2. Conectividad en línea para carga mínima de 800kbits/s o superior.
3. Dispositivos celulares con WI-FI, conexion a red celular 3G o superior para la descarga y activación de la cédula digital (una vez activada, no necesitarás internet para su uso).
4. El dispositivo debe permitir la captura facial. Esta debe realizarse en condiciones normales (rostro descubierto, sin lentes de sol o elementos que puedan afectar la identificación) y en condiciones de iluminación uniforme para proporcionar los niveles de saturación adecuada.

Figura 9. Características requeridas para la aplicación Cédula Digital
Fuente: Sitio web de la RNEC.

En Colombia, imponer este tipo de requisitos deja por fuera a buena parte de la población. En su respuesta a la solicitud de información, la RNEC plantea que para que la aplicación tenga un funcionamiento óptimo se debe contar, **como mínimo, con una versión de Android 12 (de octubre de 2021) o de iOS 17 (de septiembre de 2023)**[48]. Esto reduce todavía más el acceso a la aplicación. Además, como vimos, la probable implementación de contramedidas de detección de root excluye también a las personas que han elegido usar un dispositivo “rooteado”.

4.5 El problema de accesibilidad para personas con ciertas discapacidades

La activación de la Cédula Digital exige un reconocimiento facial relativamente complejo, en el que la persona debe mover su rostro siguiendo un punto que recorre tres círculos en la pantalla. Además, no se permite usar gafas durante el proceso.

Este requisito representa una barrera de acceso para personas con discapacidad visual y para quienes tienen otras discapacidades, como dificultades psicomotrices. Una persona con discapacidad visual que emplea herramientas tecnológicas para su autonomía digital

48. Respuesta la pregunta 8: “Las versiones Android 9 y IOS 12 actualmente no son soportadas por los fabricantes, se adjunta información de las versiones soportadas actualmente por los fabricantes, las cuales son las versiones recomendadas para el óptimo funcionamiento de la Aplicación de Cédula Digital”. Después se muestra una tabla donde la versión mínima de Android es la 12 y la mínima de iOS es la 17. La respuesta completa a esta pregunta, incluyendo esta tabla, se encuentra en el anexo 3.

y laboral nos apoyó en la solicitud de la Cédula Digital. Sin embargo, la persona no logró completar el trámite por sí misma.

Tras varios intentos fallidos, tuvo que solicitar nuevos códigos QR a la RNEC mediante el formulario web para, finalmente, activar la aplicación Cédula Digital con asistencia.

Los siguientes pantallazos ilustran parte del proceso de registro[49]:

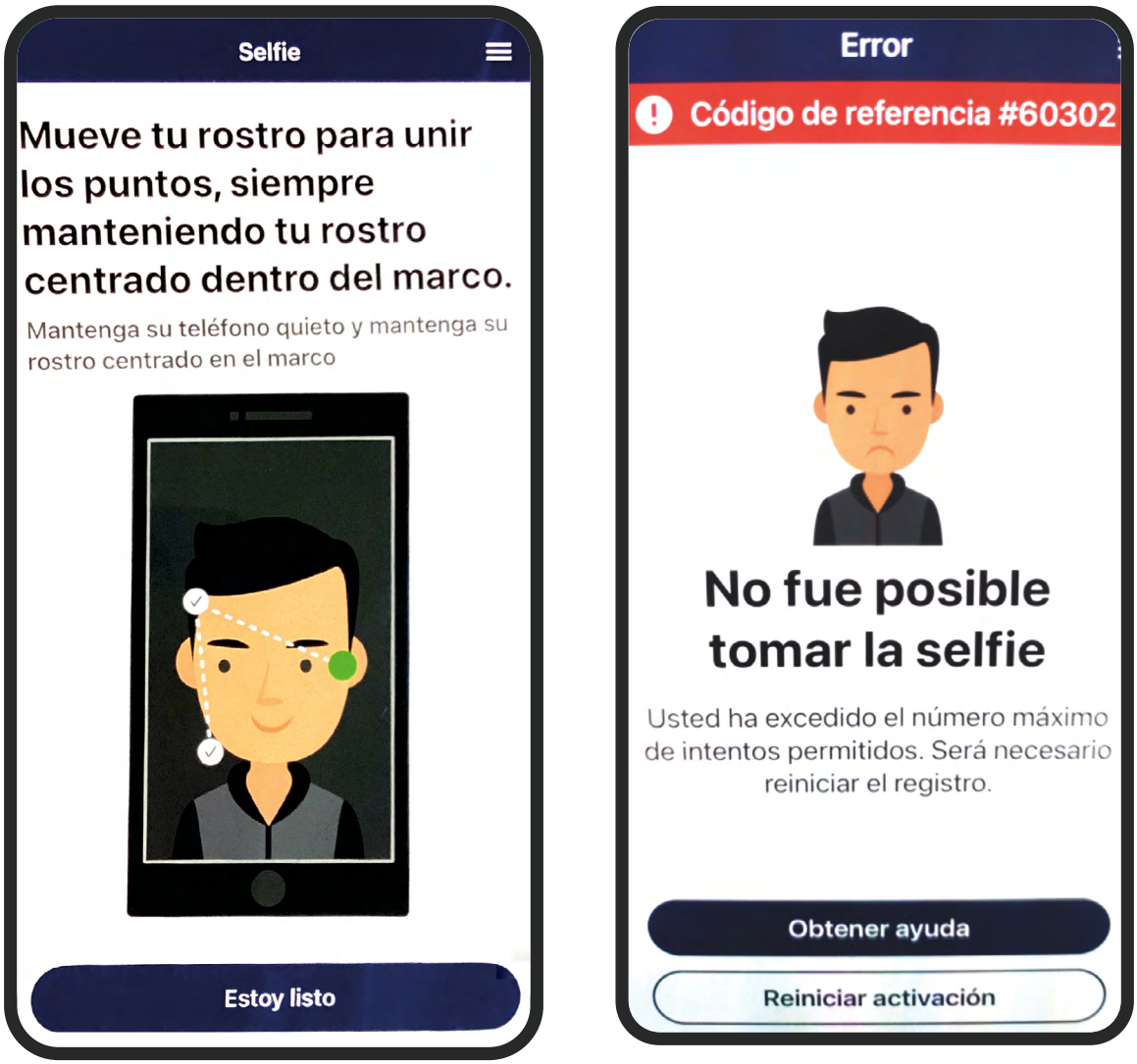


Figura 10. Fotografías de pantalla en el proceso de reconocimiento facial
Fuente: Capturas de pantalla.

49. En el sitio web de IDEMIA también se puede acceder a una explicación en video de un proceso equivalente, el proceso está en el minuto 00:42: https://na.idemia.com/dmv-2/mobile-id/

En la solicitud de información a la RNEC presentamos estas fallas como un problema de accesibilidad de la aplicación y consultamos por alternativas. La respuesta se centró en la cédula física como alternativa, a pesar de que la pregunta era clara sobre la cédula en su versión digital y la aplicación[50].

Puntos clave del análisis de funcionalidad de Cédula Digital

- **Necesita más desarrollo**

La aplicación fue lanzada sin pruebas de funcionalidad suficientes y con falta de instructivos claros para su uso. Actualmente, no ha incorporado algunas de las funcionalidades previstas, como la autenticación en servicios digitales de terceros o la recepción de notificaciones y documentos oficiales, posiblemente porque aún no hay terceros que la hayan adoptado.

- **Dificultades en el proceso de obtención y activación**

Aunque se han implementado formularios web para facilitar la activación y el pago en línea, estos presentan dificultades que pueden afectar la experiencia de las personas usuarias y retrasar el acceso a la aplicación.

- **Desafíos de accesibilidad**

El proceso de reconocimiento facial, requerido para la activación inicial, puede representar una barrera para personas con ciertas discapacidades, como la visual, al no contar con alternativas accesibles.

- **Requisitos tecnológicos y su impacto en la inclusión**

La necesidad de usar modelos recientes de celulares para el correcto funcionamiento de la aplicación podría limitar su acceso a ciertos sectores de la población. Adicionalmente, la restricción en dispositivos Android con root puede representar un obstáculo adicional para algunas personas usuarias.

50. Respuesta a las pregunta 9 y 10 del derecho de petición, pregunta 9: “Indique y justifique ¿cuáles son las opciones de acceso que brinda la RNEC a las personas que no cuentan con un teléfono inteligente actualizado a las versiones requeridas por la aplicación Cédula Digital?”. Respuesta: “La cédula de ciudadanía digital equivale funcionalmente a la cédula de ciudadanía física, con la cual los colombianos pueden identificarse plenamente en escenarios presenciales y no presenciales, con los más altos estándares y condiciones para garantizar la seguridad de sus datos, acreditando una plena identificación y mitigando el riesgo de suplantación. La cédula de ciudadanía digital se entrega en dos versiones:
•La versión física de seguridad en policarbonato, que una vez sea expedida y entregada a su titular se habilitará la generación de la segunda versión.
•La cédula de ciudadanía en su versión digital, que activará el o la colombiana en su smartphone, con sistema operativo Android o IOS, será visualizada de la misma manera que la versión física. Esto quiere decir que, si un colombiano desea adquirir la cédula de ciudadanía digital, debe previamente contar con la cédula de seguridad en policarbonato. Es importante indicar que la cédula de ciudadanía digital es un documento de identificación que permite a los colombianos acceder a servicios de manera rápida, ágil y confiable, aprovechando las tecnologías de la información y las comunicaciones que permiten el acceso a diferentes servicios para los que antes se requería de la presencialidad. Expuesto lo anterior, la cédula de ciudadanía en cualquiera de sus dos (2) formatos en que se expide, es decir, amarilla con hologramas y digital en sus dos versiones, goza de plena validez para realizar trámites ante entidades públicas o privadas”.
Pregunta 10: “Indique cuáles son las alternativas de accesibilidad, para la autenticación en su activación inicial (que se hace por defecto con reconocimiento facial en una forma que puede dificultarse a personas con discapacidades visuales, por ejemplo), con las que cuenta la aplicación Cédula Digital”.
Respuesta: “Se resolvió en la pregunta anterior.”

5. PERMISOS Y RASTREADORES

5.1 Permisos sin explicar

La versión más reciente para Android de Cédula Digital (de noviembre de 2024) **tenía 43 permisos en total**[51]. La solicitud de permisos se justifica, en parte, por las múltiples funcionalidades de la aplicación, como el reconocimiento facial, la biometría dactilar y la interconexión Bluetooth con dispositivos de control de identidad, como el celular de un policía. Sin embargo, no se explican todos los permisos requeridos.

En la respuesta de la RNEC sobre la finalidad de algunos permisos indican:

> Los permisos solicitados por la App de Cédula Digital son tres (3) y su finalidad es la siguiente:
> - *Cámara:* se solicita al usuario para lectura del QR y autenticación facial.
> - *Notificaciones:* se solicita al usuario para notificar cambios de estado en el documento digital.
> - *Bluetooth:* se solicita al usuario para compartir atributos con la aplicación de Verify.

La respuesta sobre los permisos Bluetooth, cinco en total[52], es interesante y muestra la conexión entre la aplicación Cédula Digital con la aplicación de control de identidad -Verify-, usada por la Policía Nacional.

Sin embargo, la respuesta de la RNEC sobre los permisos está incompleta. No se mencionan varios, por ejemplo, el de **biometría dactilar** y el de **acceso a la ubicación fina**, que aparecieron en las pruebas funcionales.

51. El último reporte realizado con Exodus Privacy se puede consultar en el siguiente enlace: https://reports.exodus-privacy.eu.org/es/reports/532946

52. Los siguientes: BLUETOOTH (pair with Bluetooth devices), BLUETOOTH_ADMIN, (access Bluetooth settings), BLUETOOTH_ADVERTISE (advertise to nearby Bluetooth devices), BLUETOOTH_CONNECT (connect to paired Bluetooth devices), y BLUETOOTH_SCAN (discover and pair nearby Bluetooth devices).

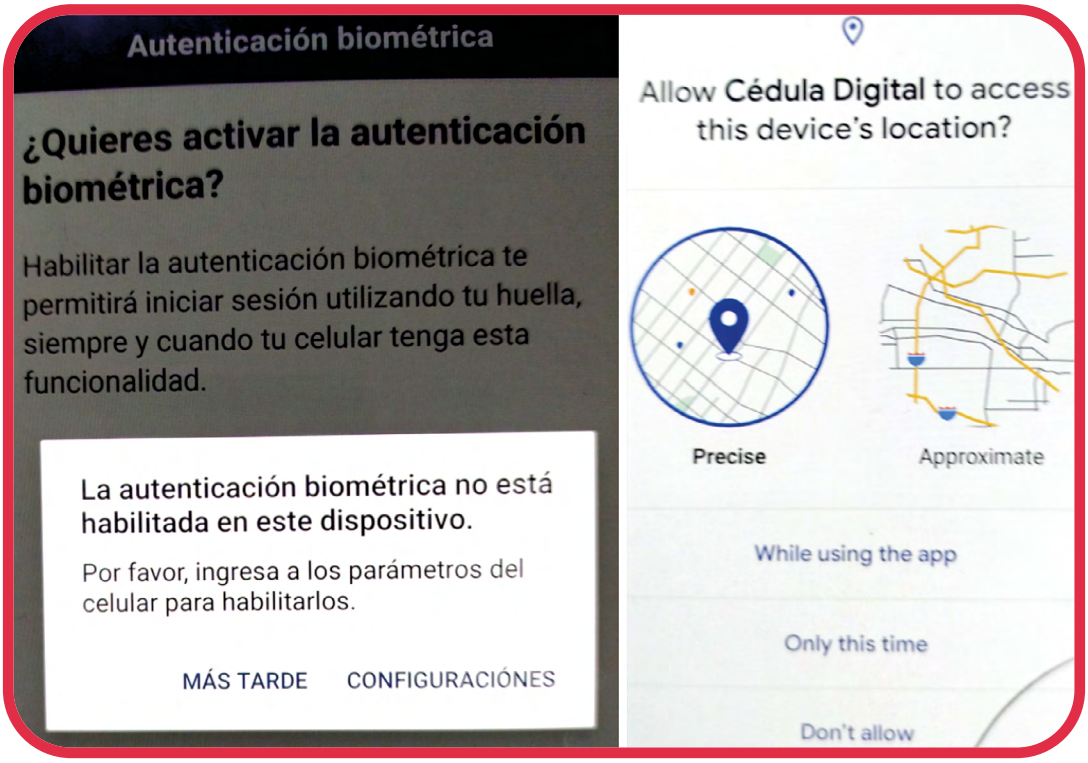


Figura 11. Solicitudes de permisos para autenticación biométrica y acceso a la ubicación precisa
Fuente: Capturas de pantalla.

Si bien la finalidad del primer permiso se entiende: autenticación en la aplicación mediante la biometría dactilar. **No encontramos la finalidad del permiso de acceso a la ubicación fina[53], dado que este tipo de permisos sí tienen importantes implicaciones de privacidad de las personas.**

Encontramos permisos que permiten que la aplicación siempre esté corriendo en el celular, por ejemplo:

- **FOREGROUND_SERVICE run foreground service:** da la posibilidad a la aplicación de correr como tarea de fondo.
- **RECEIVE_BOOT_COMPLETED run at startup:** permite que la aplicación se inicie automáticamente cuando el teléfono se enciende, sin que la persona usuaria tenga que abrirla manualmente.

Si la aplicación se ejecuta en todo momento, con acceso a la ubicación fina, podría representar un riesgo al derecho a la intimidad. Ya que podría rastrear continuamente la ubicación de la persona usuaria sin su conocimiento o consentimiento explícito en cada sesión.

53. Aunque pueda relacionarse con la sincronización con un dispositivo de control cercano integrando la aplicación Verificación de identidad, pero no encontramos ninguna información al respecto y es solo una hipótesis.

5.2 Rastreadores en la Cédula Digital: ¿estadísticas o marketing?

Como se muestra en el anexo 4, los análisis realizados con Exodus Privacy y ClassyShark3xodus permitieron identificar cinco rastreadores presentes en la versión 4 para Android de la aplicación Cédula Digital.

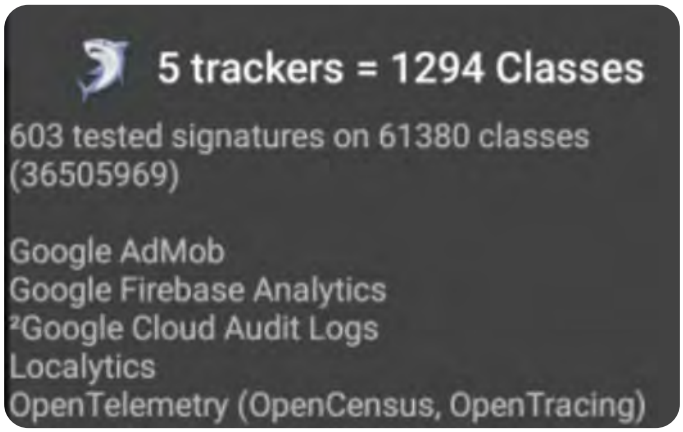


Figura 12. Rastreadores "trackers" detectados con la aplicación ClassyShark3xodus
Fuente: Captura de pantalla.

Los cinco rastreadores identificados consisten en lo siguiente:

- **Google Ad Mob**
  Es un servicio de Google[54] que facilita la integración de anuncios en aplicaciones tanto para Android como iOS, permitiendo generar ingresos a partir de la publicidad. Es necesario entender detalladamente por qué y cómo se usa para evaluar potenciales impactos a la protección de datos e intimidad, entre otros derechos fundamentales[55].
  Disponible en: https://admob.google.com/intl/es-419/home/

- **Google Firebase Analytics**
  Es el servicio de analítica de datos de Google, que lo ofrece a cambio de datos personales valiosos para sus servicios de publicidad dirigida. La política de privacidad de Google autoriza expresamente a la empresa para utilizarlos.
  Disponible en: https://firebase.google.com/docs/analytics?hl=es

54. Consultar: https://admob.google.com/intl/es-419/home/

55. Sin embargo, esto permite entender por qué, como veremos más adelante, los términos de uso de la aplicación Mobile ID de IDEMIA —de la cual la Cédula Digital es una adaptación local— incluyen una sección titulada "Links to Third Party Sites, Advertising", en la que se menciona expresamente la posibilidad de rastreo y la inclusión de publicidad a través de la aplicación.

Es importante señalar que la política de privacidad del servicio Firebase remite principalmente a la política de privacidad de Google: “Google utiliza los datos del servicio de Firebase de conformidad con nuestra Política de Privacidad y las condiciones aplicables”. Ver: https://firebase.google.com/support/privacy?hl=es-419.

> Usamos la información que recopilamos de todos nuestros servicios para los siguientes propósitos: [...] Proporcionar servicios personalizados, incluidos el contenido y los anuncios [...] En función de sus parámetros de configuración, es posible que le mostremos anuncios personalizados según sus intereses y su actividad en los servicios de Google[56].

- **Google Cloud Audit Logs**

Según Google, “los servicios de Google Cloud escriben registros de auditoría que registran actividades y accesos administrativos dentro de tus recursos de Google Cloud. Los registros de auditoría te ayudan a responder ‘¿quién hizo qué, dónde y cuándo?’ dentro de tus recursos de Google Cloud con el mismo nivel de transparencia que en los entornos locales”.

Es necesario saber si Cédula Digital está usando esta herramienta para almacenar datos y, de ser así, qué servicios de Google Cloud se están usando. No hay certeza de su implementación, pero existe la posibilidad de que aún no esté activo y podría implementarse a futuro.
Disponible en: https://cloud.google.com/logging/docs/audit?hl=es-419

- **Localytics**

Es también un servicio de analítica de datos y marketing de la empresa Estadounidense Upland[57]. En su sitio web se describe como “Mobile app marketing and analytics software”.
Disponible en: https://uplandsoftware.com/localytics/

- **Open Telemetry**

Es un servicio apoyado por la Cloud Native Computing Foundation[58] y descrito en el sitio web como “a collection of APIs, SDKs, and tools. Use it to instrument, generate, collect, and export telemetry data (metrics, logs, and traces) to help you

56. Consultar: https://policies.google.com/privacy?hl=es-419 .

57. Consultar: https://uplandsoftware.com/about/

58. Consultar: https://www.cncf.io/

> analyze your software's performance and behavior"[59]. El SDK es considerado como un rastreador porque puede generar envío de datos. Sin embargo, no identificamos el envío de datos a terceros generados para ello. Es posible que hasta ahora solo haya sido utilizado para generar logs de aplicación[60].
> Disponible en: https://opentelemetry.io/

La presencia de estos rastreadores no es accidental, sino producto de una integración deliberada por parte del desarrollador de la aplicación (RNEC/IDEMIA) mediante componentes externos (SDK), con el fin de habilitar los cinco servicios previamente descritos. Su presencia puede permitir el rastreo de las personas usuarias y la transmisión de datos a empresas del sector del marketing, lo cual plantea riesgos importantes en términos de privacidad y protección de datos personales.

Así se explicó en el informe Datos y AdTech: ¿A dónde van los ductos del petróleo digital?, publicado recientemente por Karisma:

> Además, las tecnologías de seguimiento en internet funcionan de una forma muy similar: realizando cruces de la información recolectada en bases de datos por diversas compañías.En el mundo digital se utilizan métodos como cookies, identificadores de publicidad y fingerprinting de dispositivos que permiten recolectar información sobre quién está navegando, qué está buscando o dónde se ubica. Posteriormente, como si fueran una refinería, los algoritmos de procesamiento desarrollados por las compañías convierten estos datos crudos en el recurso más valioso del siglo: información sobre quiénes somos, qué hacemos y en qué estamos interesados[61].

Por tanto, es fundamental evaluar los riesgos previo a integrar estos componentes, en especial cuando se trata de aplicaciones con datos sensibles como Cédula Digital[62]. Implementar en la aplicación estos cinco servicios externos crea riesgos de privacidad altos y —al menos en el caso de Google Firebase Analytics y Localytics— supone transferencias de datos a empresas dedicadas al marketing. Algo imposible de aceptar en una aplicación del Estado, dado que:

59. Traducción: "una colección de API, SDK y herramientas. Utilízalo para instrumentar, generar, recopilar y exportar datos de telemetría (métricas, registros y trazas) que te ayudarán a analizar el rendimiento y el comportamiento de tu software".

60. Analizamos los logs generados localmente por la aplicación, algunos se muestran en el anexo 11.

61. Karisma (2024) Datos y AdTech: ¿a dónde van los ductos del petróleo digital? Disponible en: https://web.karisma.org.co/wp-content/uploads/2024/05/PIA-informe.pdf

62. En el mismo informe, se explica así: "En el artículo Fuga de datos por rastreo publicitario habíamos alertado de una situación común que pone en riesgo la privacidad de las personas usuarias: los y las desarrolladoras suelen integrar librerías o SDKs de terceros porque ofrecen funcionalidades pero sin considerar las posibles consecuencias de la transmisión de datos, sin realizar un análisis de las políticas de privacidad de los terceros asociados y sin tener en cuenta el consentimiento de las personas usuarias.", Ibid.

- La integración de este tipo de servicio de terceros puede generar rastreo de la persona usuaria y transmisiones de datos personales a estos terceros, el caso de Cédula Digital se aborda en los capítulos 6 y 8.
- La actual implementación de la aplicación implica que el uso de un servicio público esencial, como lo es la identificación y autenticación ciudadana, esté condicionado a la transferencia de datos personales a terceros privados con finalidades ajenas a los fines constitucionales del Estado. Esta situación contraviene los principios fundamentales de la Ley de Habeas Data, especialmente aquellos relativos al derecho a la información y al consentimiento previo, expreso e informado en cada tratamiento de datos.
- Finalmente, una mala integración de estos servicios genera riesgos de seguridad digital y posibles fugas de datos personales, por lo cual es urgente un análisis de riesgo previo y cuidadoso (capítulo 8).

5.3 Cambios en rastreadores y permisos

Los análisis que se hicieron sucesivamente en la plataforma de análisis automáticos Exodus Privacy, sobre los permisos y los rastreadores Cédula Digital en las tres versiones sucesivas de la aplicación (2022, 2023 y 2024) muestran un aumento significativo en el tiempo:

Figura 13. Rastreadores y permisos detectados por Exodus Privacy en versiones de la Cédula Digital de 2022, 2023 y 2024
Fuente: Sitio web de Exodus Privacy[63].

63. Disponible en: https://reports.exodus-privacy.eu.org/es/reports/search/co.gov.registraduria.ceduladigital/

En la versión 4.0.0, la herramienta ClassyShark3xodus detectó no tres sino **cinco rastreadores**. Dentro los permisos nuevos que aparecieron, y cuyo fin desconocemos, están el NFC[64] y "BLUETOOTH_ADVERTISE" (advertise to nearby Bluetooth devices) relacionado con publicidad por Bluetooth. Este es "un método de marketing móvil que utiliza la tecnología Bluetooth para enviar contenido, como mensajes, información o publicidad, a dispositivos móviles como teléfonos celulares o tabletas"[65].

Esto resulta especialmente preocupante, ya que se vincula con los nuevos rastreadores y con la posibilidad de que empresas del sector del marketing digital integren, de diversas formas, mecanismos de publicidad y seguimiento a través de la aplicación Cédula Digital.

Puntos clave sobre rastreadores y permisos en Cédula Digital

- **Falta de transparencia sobre permisos y rastreadores**

Cédula Digital solicita 43 permisos y contiene 5 rastreadores, sin que exista suficiente información pública sobre su propósito y alcance.

- **Permisos con implicaciones en privacidad**

Si bien algunos permisos pueden estar justificados por las funcionalidades de la aplicación, como el reconocimiento facial, la biometría dactilar y la interconexión Bluetooth con la Policía Nacional, otros generan interrogantes. No queda claro por qué la aplicación requiere acceso a la ubicación precisa del dispositivo o cuál es la finalidad del permiso de publicidad vía Bluetooth.

- **Uso de rastreadores de terceros**

La presencia de rastreadores vinculados a servicios de analítica y marketing, como **Localytics, Google AdMob y Firebase Analytics**, resulta preocupante y no es apropiado para una aplicación estatal.

64. Near Field Contact, o comunicación de campo cercano que es una tecnología de comunicación inalámbrica, de corto alcance y alta frecuencia que permite el intercambio de datos entre dispositivos, https://es.wikipedia.org/wiki/Comunicaci%C3%B3n_de_campo_cercano

65. Según Wikipedia: https://en-m-wikipedia-org.translate.goog/wiki/Bluetooth_advertising?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

6. ¿CON QUIÉN SE COMUNICA Y QUÉ DICE LA CÉDULA DIGITAL?

6.1 Primer mapeo

Los análisis de tráfico que hicimos usando la aplicación permitieron establecer tres familias de dominios con los cuales se conecta:

1. El dominio principal de la aplicación pertenece a la RNEC.
2. Dominios que pertenecen a IDEMIA.
3. Dominios de empresas estadounidenses con actividades de analítica de datos y marketing.

Los anexos 5 y 6 muestran y analizan estas conexiones con detalles técnicos. La figura 14 sintetiza los resultados de dicho análisis:

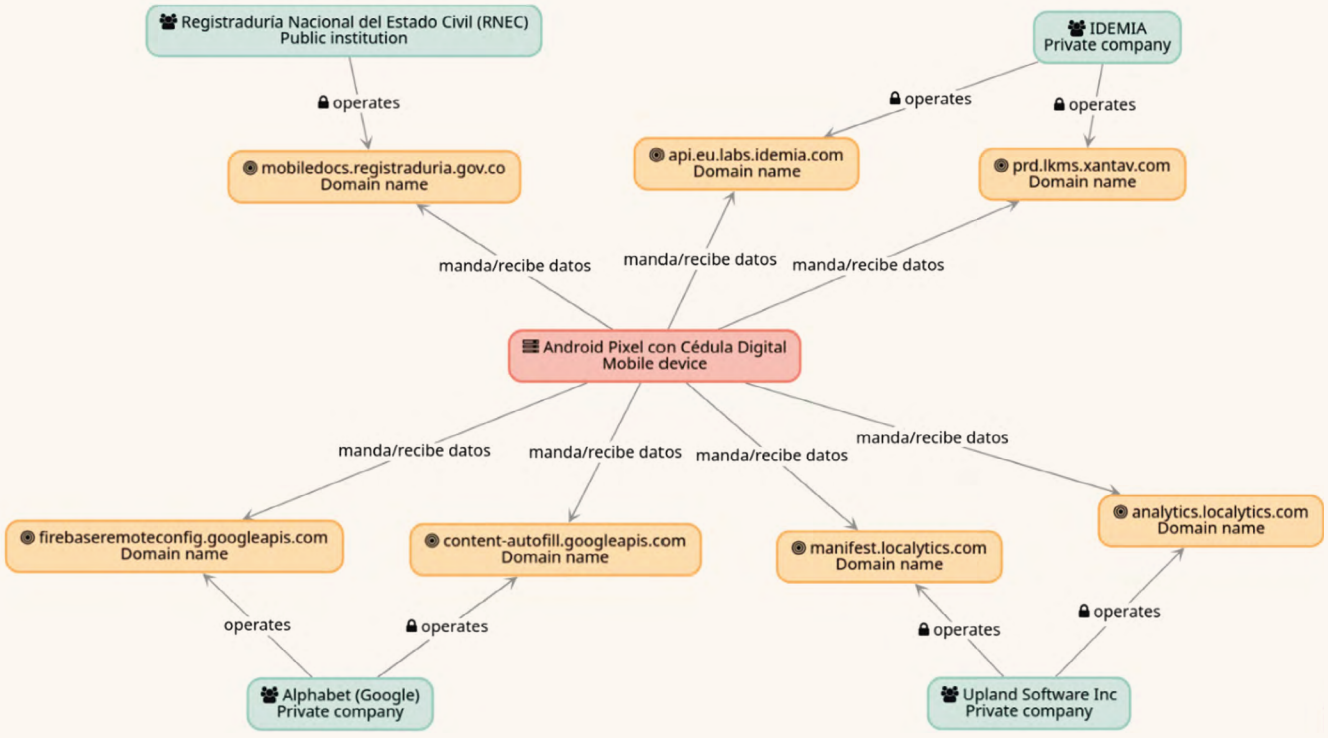


Figura 14. Comunicación de Cédula Digital con dominios externos
Fuente: Elaboración propia usando Colander (de Pirogue Tool Suite).

6.2 El subdominio de la RNEC

La aplicación se comunica principalmente con el dominio **"mobiledocs.registraduria.gov.co"** de la RNEC (un subdominio de su dominio principal). La gran mayoría de los datos enviados y recibidos por la aplicación se relacionan con este dominio (anexo 5). A priori los servidores correspondientes también son de la RNEC.

Son a priori porque el análisis de la dirección IP que corresponde al dominio "mobiledocs.registraduria.gov.co" evidencia que es un servidor de la RNEC ubicado un centro de datos de la empresa EMCALI, de Cali (anexo 6). Sin embargo, el análisis detallado de los paquetes muestra que se usa un servidor intermediario (Reverse Proxy[66] de tipo Envoy) junto con un balanceador de carga[67], tipo "F5 / Big IP", (anexo 8). Esto significa que no se puede verificar el destino final de la conexión encubierto en este intermediario.

El análisis con Pirogue permitió capturar, descifrar y analizar el tráfico de las primeras fases de activación de la Cédula Digital: arranque, envío de código QR y reconocimiento facial, que se hacen con el dominio "mobiledocs.registraduria.gov.co" (anexo 7). Allí evidenciamos cómo:

La aplicación busca un archivo de configuración que permite configurar la aplicación genérica de IDEMIA en la Cédula Digital Colombiana (capítulo 7).
Después, la aplicación inicia la fase de validación del código QR de activación y después la de reconocimiento facial.

6.3 Los dominios de IDEMIA: datos desconocidos y solicitud de permiso

La aplicación también intercambia directamente datos con dominios de IDEMIA: "api.eu.labs.idemia.com" y "prd.lkms.xantav.com", que aparecieron en los análisis de tráfico (anexo 5). En el primero, se relaciona con servidores alquilados a la empresa estadounidense Amazon, ubicados en Europa: Suecia y Alemania. El segundo dominio se relaciona con la dirección IP 143.204.23.30 que también corresponde a un servidor alojado en Amazon, pero en Estados Unidos (anexo 6).

66. Tomando la definición de Wikipedia: "En redes de computadoras, un proxy inverso es un tipo de servidor proxy que recupera recursos en nombre de un cliente externo, desde uno o más servidores internos. Estos recursos se devuelven al cliente como si se originaran en el propio servidor Web.", https://es.wikipedia.org/wiki/Proxy_inverso

67. Un balanceador o equilibrador de carga (en inglés "load balancer") es "una solución que actúa como un proxy de tráfico y distribuye el flujo de red o de aplicaciones entre los puntos de conexión de varios servidores. Su principal función es equilibrar la capacidad durante los picos de tráfico y mejorar la fiabilidad de las aplicaciones. Al reducir la carga en servicios o nubes individuales, optimizan el rendimiento general de las aplicaciones. Además, distribuyen la demanda entre distintas superficies de computación, lo que ayuda a mantener la continuidad de las sesiones tanto de aplicaciones como de red." tomando la definición del sitio web de la empresa F5, que es la solución que se usa aquí.

Usando Pirogue se pudo descifrar el tráfico (datos enviados y recibidos) hacia el dominio "prd.lkms.xantav.com" pero no hacia el dominio "api.eu.labs.idemia.com". Hacia el primero se mandan y reciben datos técnicos relacionados con la aplicación.

La comunicación con el dominio de IDEMIA "prd.lkms.xantav.com" corresponde al proceso mediante el cual la aplicación Cédula Digital recibe autorización para utilizar la tecnología Mobile ID de IDEMIA (anexo 10). Esta autorización se otorga a través de la entrega de licencias específicas para cada componente, así como de certificados criptográficos (X.509) emitidos a nombre de IDEMIA Identity & Security France. La validación de estas licencias también puede observarse en los eventos (logs) generados por la aplicación (anexo 11).

En otras palabras, para que la aplicación Cédula Digital funcione, debe recibir previamente una "autorización técnica" desde un servidor de IDEMIA. **Si bien este procedimiento no es inusual desde el punto de vista operativo, evidencia una dependencia técnica y operativa significativa de la RNEC frente a la infraestructura de esta empresa privada.**

En cuanto al segundo dominio de IDEMIA "api.eu.labs.idemia.com", no hemos obtenido respuesta en la solicitud de información a la RNEC sobre cuáles son los datos que se envían y reciben.

6.4 Analíticas de datos y marketing

La aplicación envía con regularidad, e incluso antes de conectarse al dominio principal, datos a un subdominio de la empresa **Localytics**, de analítica de datos y marketing, que desde 2020 pertenece a Upland Software[68] (anexo 12). Estos datos siempre incluyen características del dispositivo móvil, de la aplicación, la zona geográfica y varios identificadores que permiten reconocer a la persona usuaria, habilitando así mecanismos de rastreo.

En ciertos envíos se remiten datos relacionados con el contenido de la aplicación y la etapa en la cual se encuentra la persona usuaria (anexo 12). No se detectaron envíos de datos personales, aunque, en función de cómo se parametriza Localytics, el servicio lo permite[69]. Además, como ya se explicó, la parte del tráfico que se descifró con Pirogue no incluye las etapas posteriores a la activación por reconocimiento facial, momento en el que la aplicación despliega los datos personales asociados a Cédula Digital. Por tanto, no se puede determinar con certeza qué información se transmite a Localytics en esa fase, lo que implica un riesgo potencial de fuga de datos personales sensibles.

Por otra parte, la aplicación manda y recibe datos del dominio "googleapis.com", en los

68. Consultar: https://info.uplandsoftware.com/upland-acquires-localytics.html

69. Documentación técnica: https://help.uplandsoftware.com/localytics/dev/android.html#collected-data-android (Android) y https://help.uplandsoftware.com/localytics/dev/ios.html#ios (iPhone).

subdominios *"firebaseremoteconfig"* y *"content-autofill"*. Firebase es la plataforma de hosting y desarrollo de aplicaciones de Google entres sus funcionalidades están: análisis de errores, analítica de datos e, incluso, envío de notificaciones y publicidad. El tráfico hasta este dominio no es parte del tráfico que se pudo descifrar y, por ello, no se logró conocer qué datos se envían. En cuanto a "content-autofill" se remiten datos relacionados con las características de la aplicación (anexo 12).

Puntos clave del análisis de tráfico de Cédula Digital:

- **Servidor principal**

La aplicación Cédula Digital envía la mayoría de sus datos al dominio "*mobiledocs.registraduria.gov.co*" que pertenece a la RNEC. Aunque la dirección IP pertenece a la RNEC y está alojada en un centro de datos de EMCALI en Cali, el análisis técnico no permite determinar con certeza la ubicación de los servidores finales que reciben los datos. Esto se debe a la presencia de una arquitectura con un **servidor proxy reverso** y un **balanceador de carga**, que funcionan como intermediarios y ocultan el servidor aplicativo final.

- **Intercambio de datos con IDEMIA**

La aplicación intercambia datos con dos dominios webs de IDEMIA. En el primero ("xantav.com"), se emiten licencias de uso y certificados para autorizar la aplicación y sus componentes, evidenciando una vez más **la fuerte dependencia de la Cédula Digital con IDEMIA**. En cuanto al segundo dominio ("api.eu.labs.idemia.com"), no se pudo establecer qué datos envía/recibe la aplicación.

- **Analíticas de datos y marketing**

La aplicación envía también datos al dominio "googleapis.com" y, con regularidad, a *"localytics.com"*. La integración de Localytics, un servicio de marketing y analítica de datos de **Upland Software**, planteando un **riesgo significativo para la privacidad**. Esta plataforma no solo recopila información sobre la aplicación y el dispositivo; sino también su contenido y varios identificadores de la persona usuaria. Además, según su documentación técnica, **Localytics** permite la exportación de grandes volúmenes de datos, incluidos datos personales, aumentando el riesgo de fuga de datos o uso no autorizado de la información.

7. EL PAPEL DE IDEMIA: BRANDING LOCAL PARA EXPERIMENTOS GLOBALES

7.1 El archivo de configuración de Cédula Digital

Al poner en marcha la aplicación Cédula Digital, la primera acción que ejecuta[70] es ir a buscar su **archivo de configuración general**, este proceso es invisible para la persona usuaria. Esto se estableció capturando, descifrando y analizando los flujos de datos enviados y recibidos por la aplicación, usando Pirogue (anexo 1). Este archivo de configuración, tipo JSON, se compone de cinco partes que se ven en la figura siguiente.

Figura 15. Estructura y extracto del archivo de configuración de Cédula Digital
Fuente: Elaboración propia.

70. Antes de esto hay conexiones hasta el dominio de analítica de datos y marketing Localytics pero es una comunicación originada por una componente (SDK) de tercero. La primera conexión de la aplicación en sí es para ir a buscar el archivo de configuración.

Sobre la información en el archivo encontramos:

- La información del *"tenantID"*, o "identificador del arrendatario", es descrita en el archivo como "genérico", indica probablemente que Cédula Digital es una versión genérica de Mobile ID.
- Detalles de configuración y características de la aplicación como su nombre, el nombre del cliente (o "business process" que es *"COLOMBIA_RNEC"*), los tipos de autenticación aceptados, etc.
- Tres URL que contienen otros archivos de configuración específicos sobre el reconocimiento facial, los tipos de datos personales que deben contener el documento de identidad[71] (que dependen del país y tipo de documento), y los atributos del consentimiento.
- Varias URL que contienen **términos y condiciones, política de privacidad de la aplicación; sin embargo no es no de Cédula Digital, sino de la aplicación Mobile ID de IDEMIA.**

Todo indica que el propósito de este archivo es proporcionar elementos de configuración específicos para adaptar la solución genérica Mobile ID de IDEMIA a la aplicación Cédula Digital. En ese sentido, Cédula Digital operaría como una versión local, rebranding, de la solución Mobile ID[72], implementada por la RNEC en el contexto colombiano.

El análisis del sitio de IDEMIA sobre Mobile ID, y de sus vídeos promocionales, muestra además que Cédula Digital es casi idéntica, en su funcionamiento[73] y diseño. Igualmente, la aplicación tiene que conectarse a un dominio web de IDEMIA, "xantav.com", para obtener licencias de uso para varios de estos componentes tecnológicos (anexo 10). Los eventos técnicos (logs) generados por la aplicación muestran lo mismo y es interesante ver que, en el caso de los análisis en iPhone, empiezan con **"mID_CO"** (abreviación probable de "Mobile ID Colombia") que es el nombre con el que se identifica técnicamente la aplicación (anexo 11).

Hay también otro detalle llamativo que se observó en las comunicaciones con este dominio de IDEMIA. Allí se mencionan varios nombres (de paquete) de la aplicación. El oficial, que ya vimos, "co.gov.registraduria.ceduladigital" y tres adicionales. Dos podrían ser versiones de prueba o de desarrollo[74]: *"com.idemia.mobileid.colombia.rnec"*, "com.idemia.mobileid.colombia.rnec.dev" y "com.idemia.mobileid.colombia.rnec.dev.pl" (anexo 10).

71. Lo llaman "privacy-views-col".

72. Consultar: https://www.idemia.com/mobile-id y https://na.idemia.com/dmv-2/mobile-id/

73. Principalmente en activación con código QR y el tipo de reconocimiento facial, la presentación del documento de identidad, la interconexión Bluetooth con la aplicación Verify para la verificación de identidad y la autenticación en servicios digitales de terceros.

74. "dev" en informática se suele usar para devolpment (desarrollo). Cuando hay una versión de una aplicación todavía en prueba se suele usar nombres o dominios con el prefijo o sufijo "dev".

Esto sugiere que, en las etapas iniciales del desarrollo, se habría propuesto —e incluso comenzado a trabajar— con una aplicación cuyos nombres de paquete hacían explícita la relación con IDEMIA y su solución Mobile ID, como ocurre con las versiones utilizadas en otros países, por ejemplo en Estados Unidos. Es probable que, en fases posteriores, la RNEC optara por adoptar un nombre de paquete más personalizado y alineado con la identidad institucional local.

Además, al final del archivo de configuración se incluyen enlaces a dos documentos legales que no hacen referencia a Cédula Digital, sino a Mobile ID, lo cual será analizado en la siguiente sección.

En conjunto, estos elementos permiten inferir que Cédula Digital es, en esencia, una adaptación —o rebranding local— de la aplicación genérica Mobile ID desarrollada por IDEMIA, utilizada por la RNEC en el contexto colombiano.

7.2 ¿Una autorización para acceder y compartir datos? Los términos de uso y la política de privacidad "escondidos" de IDEMIA - Estado Unidos

En los archivos de configuración se encuentran hipervínculos hacia estos documentos:

1. Los términos de usos de la aplicación Mobile ID (IDEMIA MOBILE ID TERMS OF USE)[75].
2. Declaración de privacidad *(Privacy Statement)*[76].

El segundo tiene un enlace hacia un tercer documento, de información y consentimiento para la colecta de datos personales biométricos y sensibles (*CONSENT TO COLLECT BIOMETRIC AND SENSITIVE PERSONAL INFORMATION)*[77]. Estos tres documentos están a nombre de la sucursal Estadounidense de *IDEMIA, IDEMIA IDENTITY & SECURITY USA LLC*[78].

En la declaración de privacidad de IDEMIA, **se menciona claramente que la empresa IDEMIA IDENTITY & SECURITY USA LLC puede usar y almacenar los datos personales de la persona usuaria, incluyendo datos sensibles y biométricos, entre otros.**

75. Consultar: https://idemia-mobile-id.com/enduserterms

76. Consultar: https://idemia-mobile-id.com/policies/di

77. Consultar: https://idemia-mobile-id.com/policies/di/biometricsconsent

78. Consultar: https://www.idemia.com/usa

Los servicios IDEMIA pueden recopilar IIP (Información de Identificación Personal) y Datos que pueden incluir lo siguiente:

- IIP del usuario proporcionada durante la descarga y uso de los Servicios, incluyendo nombre, dirección, contraseñas, fecha de nacimiento, documentos de identidad e información relacionada (por ejemplo, licencias de conducir, pasaportes, etc.) e información biométrica (por ejemplo, rostro, huellas dactilares).
- Datos sobre el uso de los Servicios por parte de un usuario, incluidos registros de caídas y estadísticas de uso.
- Datos sobre el dispositivo de un usuario y su interacción con los Servicios, incluyendo el tipo de dispositivo móvil, ID de usuario único, dirección IP y sistema operativo, y tipo de navegador(es) en uso.
- Análisis y estadísticas como el número de documentos de identidad procesados en un intervalo de tiempo, la tasa de aprobados/no aprobados de un tipo de documento de identidad o de un proceso de autenticación de documentos, códigos de aprobados/no aprobados, fecha y/o lugar de emisión del documento[79].

También, en las preguntas de uso frecuente de la página de IDEMIA sobre Mobile ID, se menciona:

¿Qué hace IDEMIA con mis datos?

IDEMIA no recopila, almacena ni guarda sus datos personales de forma permanente. Los únicos lugares en los que se almacena su información completa son el DMV[80] de su estado, y de forma encriptada en tu teléfono -hasta que decida compartirla. Para más información, lea la declaración de privacidad de IDEMIA aquí[81].

IDEMIA indica que no recolecta, almacena o posee datos personales **de forma permanente** y lo aclara en la declaración de privacidad que define las políticas de retención de datos personales:

- Durante el periodo de uso y hasta 30 días después de la cancelación de los servicios para los datos personales que necesitan almacenamiento a largo plazo (stateful services) como los datos biométricos.

79. Traducción propia tomada de: https://idemia-mobile-id.com/policies/di

80. Las DMV (Department of motor vehicle) son agencias gubernamentales estadounidenses que manejan, entre otras, las licencias de conducción. Actualmente, en Estados Unidos la aplicación Mobile ID solo se está usando en ese contexto. En el extracto de la FAQ mencionada, olvidan modificar la respuesta para actualizarla y extenderla a otros tipos de documentos (como la cédula colombiana) que ahora maneja Mobile ID.

81. Traducción propia tomada de: https://na.idemia.com/dmv-2/mobile-id/

- 30 días para los datos personales que no necesitan almacenamiento a largo plazo (stateless services).
- De manera indefinida para los datos “anonimizados”, aunque se deberían denominar datos seudonimizados[82].

Los términos de uso mencionan algo preocupante: la posibilidad de que IDEMIA directamente, vía la aplicación o indirectamente, comparta datos personales con terceros. Incluso, se presenta la posibilidad de que la aplicación muestre publicidad, generando riesgos de rastreo asociados al marketing digital. Esto provoca preguntas sobre la soberanía, protección de datos personales, intimidad y seguridad digital. Aquí, dos extractos de los términos de uso sobre estos puntos:

> **Enlaces a sitios de terceros, publicidad.** La App puede contener información, enlaces y/o anuncios de sitios web operados por Partes Relacionadas u otras partes (los “Sitios de Terceros”).
> [...]
> **Consentimiento para el uso de datos:** Privacidad. [...] El usuario puede tener la posibilidad de compartir cierta información de identificación personal u otra información sensible («Información») con las Partes de Confianza u otros terceros.[83]”

Estos elementos indican que IDEMIA tendría la capacidad de acceder a la totalidad de los datos personales de las personas usuarias de la Cédula Digital, incluidos datos sensibles y biométricos. Además, existe la posibilidad de que se habiliten canales de comunicación con terceros, incluso con actores del sector del marketing y la publicidad.

A pesar de la normativa de protección de datos vigente en Colombia, estos documentos brindan más información sobre el funcionamiento y tratamiento de datos de la aplicación que los propios términos de uso y la política de privacidad de la **Cédula Digital**. Además, esta información tampoco ha sido proporcionada en las respuestas de la **RNEC** a la solicitud de información.

82. La “anonimización” de datos es un tema complejo, muchos estudios han mostrado que los “datos anonimizados” como los de ubicación, se podían “des-anonimizar”; ya que se reconectan repetidamente a sus propietarios. Es más preciso, en la mayoría de casos, hablar de “seudonimazión”, que dificulta la conexión entre datos y una persona; que de “anonimización”, que impide la conexión entre datos y una persona.

83. Traducción propia tomada de: https://idemia-mobile-id.com/enduserterms

7.3 Cuando la RNEC nos habla de IDEMIA

El hecho que los datos de las y los colombianos sean administrados por la empresa IDEMIA es algo que el propio Registrador ha afirmado anteriormente:

Figura 16. Trino de 5 de junio de 2024 de la cuenta de X de la RNEC
Fuente: Cuenta de X de RNEC[84].

Por tanto, es necesario aclarar cómo está dividida la administración de los datos entre IDEMIA y la RNEC: si se extiende también a la nueva base de datos de Cédula Digital, que tiene un alcance mayor al de la cédula tradicional. Al mismo tiempo, si la aplicación pretende ser la llave de acceso a servicios digitales de entidades terceras públicas y privadas, así como recibir notificaciones y documentos oficiales, además de manejar datos biométricos de reconocimiento facial[85].

84. Disponible en: https://x.com/Registraduria/status/1798424805135229245?utm_source=chatgpt.com&mx=2

85. Los datos biométricos de reconocimiento facial son más sensibles, desde el punto de la privacidad, que una simple foto. Incluyen datos derivados de imágenes de la cara desde varios ángulos, para permitir un reconocimiento facial incluso si la cara no está de frente a la cámara.

Las respuesta de la RNEC a la solicitud de información presentada por Karisma sobre el papel de IDEMIA y su eventual acceso a los servidores que almacenan las bases de datos de Cédula Digital apuntan a un rol más importante de IDEMIA dentro del sistema de identificación nacional:

> **16. ¿Cuál es el papel de la empresa IDEMIA en el desarrollo, mantenimiento y funcionamiento de la aplicación Cédula Digital?**
>
> Rta.: IDEMIA como contratista de la Registraduría Nacional del Estado Civil, como función principal debe prestar y brindar el soporte y respectivo mantenimiento sobre la aplicación de Cédula Digital Colombia.
> [...]
>
> **18. ¿IDEMIA tiene acceso a los servidores informáticos que almacenan las bases de datos de la Cédula Digital u otros servidores involucrados en su funcionamiento?**
>
> Rta.: Para el cumplimiento de las obligaciones del contrato **el contratista IDEMIA tiene acceso a los servidores informáticos que almacenan las bases de datos de la Cédula Digital y otros servidores involucrados con su funcionamiento**.
> No obstante, se indica que, el contratista en el marco de sus competencias contractuales suscribió un compromiso de confidencialidad y no divulgación de la información, en aras de salvaguardar así lo consignado en las bases de datos"[86].

En la respuesta a la pregunta 19, la RNEC afirma:

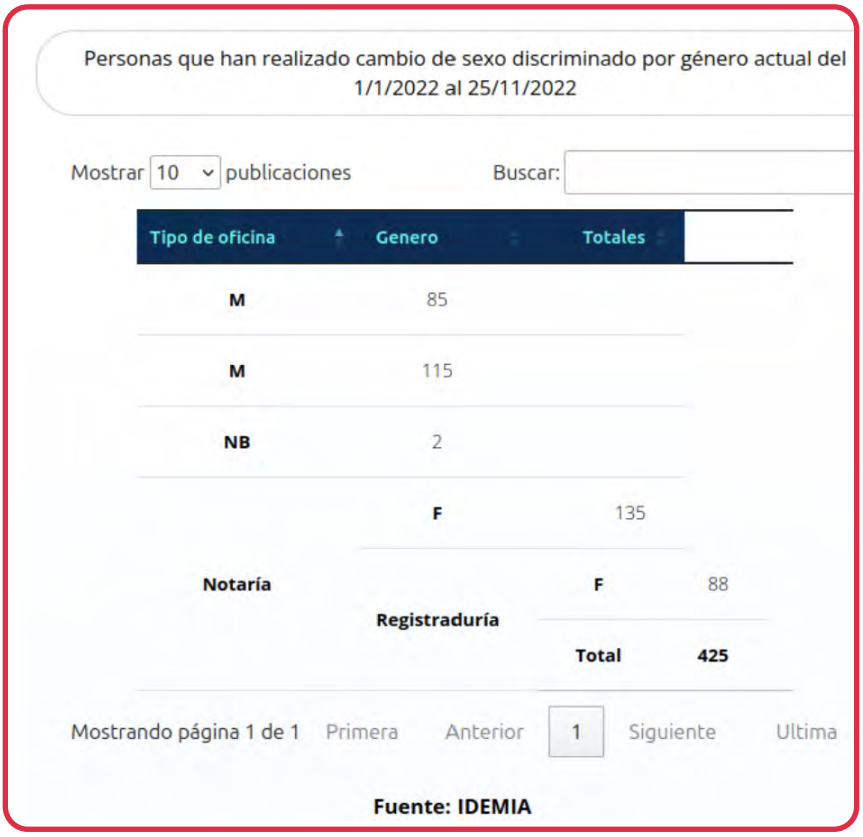
> Los datos de los ciudadanos no son transmitidos a la empresa IDEMIA, toda vez que, la información de los ciudadanos se encuentra en las bases de datos que compone y administra Registraduría Nacional del Estado Civil y se encuentran ubicados dentro de la infraestructura de la misma Entidad.

Sin embargo, en la parte previa de este informe se estableció que los análisis técnicos muestran cómo encontramos que la aplicación sí transmite datos hacía dominios web que pertenecen a IDEMIA (aunque no sean necesariamente datos personales).

Si bien la base de datos principal que almacena los datos personales y biométricos de los ciudadanos colombianos se ubica en la infraestructura de la RNEC, la respuesta a la pregunta 18 y otros elementos que se desarrollan a continuación indican que **no es la RNEC, sino IDEMIA la que administra esa base de datos**. En el artículo titulado Registraduría Nacional

86. Respuesta al Derecho de Petición, carta de la Dirección de Identificación de la Registraduría, 8 de enero del 2025.

expide las primeras cédulas digitales con enfoque diferencial a personas trans, la RNEC presenta una tabla en la que se indica que la fuente es IDEMIA.



Personas que han realizado cambio de sexo discriminado por género actual del 1/1/2022 al 25/11/2022

Mostrar 10 publicaciones Buscar:

Tipo de oficina	Genero	Totales
M	85	
M	115	
NB	2	
	F	135
Notaría	F	88
Registraduría	Total	425

Mostrando página 1 de 1 Primera Anterior 1 Siguiente Ultima

Fuente: IDEMIA

Figura 17. Tabla de la RNEC
Fuente: Registraduría Nacional expide las primeras cédulas digitales con enfoque diferencial a personas trans[87].

Como se ve en la figura, la fuente de esta tabla es IDEMIA, esto sugiere que esta empresa, mas no la RNEC, es la que está en capacidad de producir la información sobre la administración de la identidad legal de las personas. En el peor de los casos, esto explicaría porque la RNEC accede a la base de datos de la Cédula Digital de forma indirecta, a través de una aplicación interna, sin acceso directo al servidor de la base de datos. Este acceso directo permitiría realizar consultas más detalladas, incluyendo solicitudes inusuales, y, sobre todo, representa un aspecto particularmente sensible en términos de seguridad[88].

Esto también se expresa, implícitamente, en que sea IDEMIA y no la RNEC, la que puede hacer ciertas modificaciones o correcciones sobre la base de datos correspondiente, el portal web o la "Herramienta Logística de Entrega de documentos vía web" (HLED-WEB). Esto se

87. Disponible en: https://registraduria.gov.co/Registraduria-Nacional-expide-las-primeras-cedulas-digitales-con-enfoque.html#!/servicios/comunicados.htm

88. Ya que puede permitir acceder y modificar directamente los datos, así como hacer búsquedas, extracciones y réplicas completas de la base de datos.

muestra en un documento público de 2023, la Modificación Circular Única de Registro Civil e Identificación – Versión 8, señalamos los extractos correspondientes:

> La actualización-reconstrucción del material de cedulación de Primera Vez, Renovación o Rectificación en casos excepcionales consiste en un proceso que inicia en el lugar donde el usuario se presenta a realizar un trámite de identificación y la Estación Integrada de Servicios-EIS advierte que no es posible realizar dicho trámite; **en este caso, el Registrador debe solicitar mediante correo electrónico a la Mesa de ayuda del PMT soporte, a través del correo electrónico soporte_pmt@idemia.com** enviando la información sobre el NUIP del usuario, y si se le informa que es un caso de "No Migrada", se deberá confirmar con el usuario que haya tenido cédula amarilla de hologramas, para posteriormente corroborar con la Coordinación de Recepción - DNI la consistencia de la información.
> [...]
> Con respecto a las novedades o inconvenientes que se presenten en la actualización realizada a la herramienta Web Service, pueden comunicarse con la mesa de ayuda al teléfono 7957620 **o correo electrónico soporte_pmt@idemia.com**.
> [...]
> Excepcionalmente, cuando se requiera realizar mantenimiento correctivo al dispositivo de entrega "Morphotablet" o al equipo en el cual se encuentra instalado el HLED-WEB, o cuando el titular del documento es sujeto de una situación de fuerza mayor debidamente comprobada, el registrador pondrá en conocimiento el caso ante los Delegados Departamentales, quienes deben verificar que dicho dispositivo efectivamente se haya remitido a través del contrato de mantenimiento correctivo, **evidenciando la solicitud a través de un caso abierto en la mesa de ayuda de nuestro aliado tecnológico IDEMIA**, o en su defecto evaluarán la circunstancia referida, autorizando o no la entrega del documento.
> [...]
> Para la opción b, si existen cédulas de ciudadanía (plásticos) que no figuren en el reporte del portal Hled-Web, se debe enviar un correo electrónico a soporte@idemia.com, con máximo cinco (5) cédulas de ciudadanía para que sean incluidas y actualizados en la herramienta[89].

Otros elementos que muestran la dependencia de la aplicación con IDEMIA aparecen en el análisis de tráfico en la sección 6.3 de este informe: la aplicación se conecta con dominios webs que pertenecen a IDEMIA y en particular pide licencias y autorizaciones técnicas para poder funcionar. Además, en los datos mandados aparecen nombres anteriores y de pruebas que se usaron por la aplicación en donde expresamente aparece el nombre de IDEMIA[90].

89. Consultar: Consultar: https://wapp.registraduria.gov.co/identificacion/cedula-digital/files/pdf/20230327_circular-unica-de-rc-e-identificacion_version-8_23-de-marzo-de-2023.pdf

90. Ver la sección 7.1, se trata de los nombres "com.idemia.mobileid.colombia.rnec", "com.idemia.mobileid.colombia.rnec.dev" y "com.idemia.mobileid.colombia.rnec.dev.pl". Hoy el nombre identificador de la aplicación es "co.gov.registraduria.ceduladigital" y solo deja aparecer la registraduría.

Puntos clave del análisis de datos personales y relación entre la RNEC e IDEMIA

- **Adaptación local de una aplicación genérica**

La aplicación Cédula Digital parece ser una adaptación local de Mobile ID, desarrollada por la empresa IDEMIA. Esta empresa no solo creó la aplicación, también gestiona su mantenimiento y administra las bases de datos asociadas.

- **Rol de IDEMIA en el tratamiento de datos**

Dada su participación en la gestión y almacenamiento de datos, IDEMIA debería ser considerada la encargada del tratamiento de datos, mientras que la RNEC actuaría como la responsable del tratamiento, según la normativa colombiana de protección de datos.

- **¿De quién es la propiedad intelectual del desarrollo?**

Es altamente probable que IDEMIA Estados Unidos (IDEMIA IDENTITY & SECURITY USA LLC) posea la propiedad intelectual total o parcial de la aplicación y su código fuente, aunque no hay claridad al respecto.

- **Riesgos para la soberanía y la transparencia**

La posible titularidad extranjera del código fuente plantea un riesgo en términos de soberanía nacional, dificultando el control del Estado sobre la aplicación. Además, la falta de transparencia en su infraestructura y código podría limitar e impedir auditorías externas, independientes y técnicas.

- **Impacto en la confianza pública**

La dificultad al realizar auditorías adecuadas, en particular a causa de propiedad intelectual de IDEMIA de todo o parte del código fuente de la aplicación, afecta la confianza tanto de la sociedad civil como de las propias instituciones del Estado colombiano en la seguridad, integridad y funcionamiento de la Cédula Digital.

8. LA NECESIDAD DE UNA AUDITORÍA DE SEGURIDAD DIGITAL EXTERNA, INDEPENDIENTE Y TRANSPARENTE

En este capítulo analizamos algunas características de seguridad de la aplicación y de sus servidores mediante análisis externos con metodologías no intrusivas. Sin embargo, se requieren más indagaciones para corroborar si una aplicación como Cédula Digital cumple con la protección de la intimidad, datos personales y requisitos de seguridad digital. Para una evaluación más amplia y profunda de la aplicación y su infraestructura, se necesita de otros análisis de seguridad como: código fuente, pruebas de penetración en los servidores, arquitectura, actualizaciones de cada componente y de configuración internas, de logs de los servidores, entre otros; y que por ahora no podemos realizar dadas nuestras capacidades y recursos.

De Cédula Digital se esperan los más altos estándares de protección de derechos humanos y seguridad digital por la importancia estratégica de la identificación de las personas, por los recursos dedicados a este proyecto (casi 30 millones de USD en el 2022, ver figura 2) y por el tamaño del contratista encargado de ella. De ahí que sea necesaria una auditoría externa que pueda realizar los análisis y recomendaciones necesarias para asegurar la protección de los derechos de las personas y la seguridad de la aplicación.

8.1 Recomendaciones estándar

Los análisis de seguridad que hicimos y que se detallan en el anexo 13, muestran en general un buen nivel de seguridad, dentro de lo que se puede observar con las limitaciones de nuestra metodología. En particular se puede destacar:

- La implementación del protocolo cifrado HTTPS en el dominio principal de la aplicación (mobiledocs.registraduria.gov.co), con una política de seguridad estricta (HSTS) y con una versión reciente de TLS v 1.2[91] aunque no la última que es TLS 1.3.
- El uso de la tecnología de reverse proxy Envoy junto con un balanceador de carga, que siendo unos intermediarios pueden proteger el servidor aplicativo y permiten también absorber una gran cantidad de solicitudes.
- La instalación de dos cookies técnicas asociadas al dominio[92] con atributos de seguridad (Secure y HTTP Only) que ayudan a protegerse contra robos de cookies[93].

91. El protocolo HTTPS (Hypertext Transfer Protocol Secure) consiste en la encapsulación del protocolo HTTP en el protocolo cifrado SSL (Secure Socket Layer) o su sucesor TLS (Transport Layer Security).

92. Son las cookies “rnec_id” y “TS01aa88df” respectivamente de identificación de sesión y de load balancing.

93. HTTPOnly permite asegurar que las cookies solo puedan acceder vía el protocolo HTTP, y no desde una función javascript de un tercero por ejemplo. Secure garantiza que solo se transmite la cookie con el protocolo HTTPS.

Una prueba sobre la implementación del HTTPS/TLS en la plataforma SSL Labs[94] en el dominio *"mobiledocs.registraduria.gov.co"* muestra una buena nota de B[95]. Sin embargo, hay defectos que se deben corregir (anexo 13).

Igualmente, el análisis de las respuestas del servidor web usado para los formularios vinculados con la Cédula Digital, en el dominio *"ceduladigital.registraduria.gov.co"*, muestra características de seguridad similares: el uso de cabeceras de seguridad y el enmascaramiento de las versiones de los servidores. Además, en cuanto a la implementación del HTTPS, la evaluación está mejor, con una nota de A+ (anexo 13).

En cuanto a las versiones y actualizaciones de los componentes usados en el dominio de la aplicación, el uso de intermedios como el Proxy Reverso o el balanceador de carga, junto con el enmascaramiento de las versiones de los servidores en las respuestas HTTP, no se pudo identificar las versiones de la mayoría de los componentes tecnológicos usando solo nuestra metodología. Esto es positivo porque dificulta las fases de reconocimiento ante un eventual ataque. Sin embargo, se lograron identificar las versiones para dos componentes: el framework de aplicación web (Bootstrap) y una librería Javascript (anexo 8). El primero está en una versión un poco antigua pero sigue manteniendo las actualizaciones de seguridad. Es necesario garantizar que, de manera general, todos los componentes de la infraestructura de Cédula Digital cuenten con sus actualizaciones de seguridad digital.

En términos generales, parece que hay una voluntad de cumplir con las recomendaciones estándares de seguridad y en particular las Condiciones mínimas técnicas y de seguridad digital para sitios webs anexos a la Resolución MinTIC 1519 del 2020[96].

8.2 Servicios abiertos: el interrogante del BGP

Un análisis de los servicios (puertos) abiertos del servidor que corresponde al dominio *"mobiledocs.registraduria.gov.co"* muestra que, sumados a los puertos estándares usados para una aplicación web (dominio, HTTPS) y de un servicio de autenticación (*"ident"*), hay dos más que están abiertos (anexo 9).

- BGP (Border Gateway Protocol) es un protocolo con que se intercambia información de encaminamiento entre sistemas autónomos (AS)[97], que son grandes sistemas o porciones de redes, generalmente de operadores de internet o grandes empresas.
- Un puerto no estándar que, en este caso, podría vincularse con la implementación de equipos de seguridad de la empresa Fortinet.

94. Consultar: https://www.ssllabs.com/ssltest/

95. Las notas en SSL LAB van de "A+" (lo mejor) hasta "F" (lo peor) y evalúan la calidad de implementación del protocolo cifrado SSL/TLS, que es la capa de cifrado del protocolo HTTPS (Hyper Text Transfer Secure). También existe la nota "T" cuando el certificado criptográfico no está firmado por una autoridad reconocida (no es "Trusted")

96. Consultar: https://gobiernodigital.mintic.gov.co/portal/Noticias/160997:MinTIC-publica-la-Resolucion-1519-del-2020-sobre-transparencia-en-el-acceso-a-la-informacion-accesibilidad-web-seguridad-digital-web-y-datos-abiertos

97. Consultar: https://es.wikipedia.org/wiki/Border_Gateway_Protocol

En cuanto al primero (BGP), resulta sorprendente su aparición en este contexto, ya que es difícil entender “desde el exterior” como funciona la infraestructura de la Cédula digital. Dejándonos un interrogante sobre en qué y cómo se usa el BGP en este caso. También cabe la posibilidad de que el puerto o servicio BGP haya quedado expuesto por negligencia, error de configuración o simple descuido.

Por tanto, es importante que la RNEC explique por qué y cómo se usa el puerto/servicio BGP y, en caso de que no se use, que lo cierre para cumplir con las buenas prácticas de seguridad digital y reducir la superficie de ataque.

8.3 SDK de terceros y riesgos de fugas de datos

Como se mostró en los capítulos 7 y 8, además de los componentes externos (SDK) de IDEMIA, la aplicación cuenta con otros cinco componentes externos para desarrollo, analítica de datos y de marketing, en particular las de Localytics y de Google Ads; algunos de estos enviaron datos durante nuestros análisis.

El uso de este tipo de componentes externos rastrea a las personas usuarias y genera problemas de privacidad, un riesgo en el marco de una aplicación sensible del Estado y que no debería estar relacionada con marketing. Como lo hemos mencionado antes[98], la presencia y ejecución de estos SDK de terceros puede generar fugas de datos personales sensibles hacia terceros que no están autorizados para recibirlos. En este caso, el problema de privacidad se podría convertir en un problema de seguridad digital grave.

La inclusión de SDK de terceros, especialmente cuando están vinculados con el ámbito del marketing, requiere un análisis de riesgo previo a su implementación y configuración en la aplicación. Además, es fundamental poder auditar posteriormente los efectos de su inclusión para garantizar que no genere impactos negativos en términos de privacidad y seguridad digital. Esta pregunta del análisis de riesgo previo, la hicimos a la RNEC pero no obtuvimos respuesta[99].

98. Ver estas dos publicaciones: Fugas de datos por rastreo publicitario (https://web.karisma.org.co/fuga-de-datos-por-rastreo-publicitario/) y Datos y AdTech (https://web.karisma.org.co/wp-content/uploads/2024/05/PIA-informe.pdf).

99. Pregunta 14: “¿Se hizo un análisis de impacto en protección de datos para evaluar cuáles son las consecuencias de la integración de las componentes “Firebase analytics” y “Localytics” en la aplicación y conocer cuáles son los datos del usuario que se transmiten a las empresas Google y Localytics y el rastreo generado por ello? En caso afirmativo adjunte el documento que soporta dicho análisis de impacto. En caso negativo, indique las razones por las cuáles aún no lo ha realizado.
Rta.: No se suministra información ya que la misma cuenta con carácter de reserva según lo establecido en el artículo 24 literal primero de la Ley 1755-2025.”

8.4 Cuando los logs siguen hablando (demasiado)

Como ya vimos, la aplicación parece implementar contramedidas estrictas que dificultan descifrar el tráfico, incluso cuando se hace desde un teléfono controlado. Se trata del certificate pinning y de la detección de root.

Por esto, cuando empezamos a analizar los eventos (logs) de Android generados localmente por Cédula Digital, fue una sorpresa descubrir todo lo que contenían y en particular las solicitudes HTTP descifradas hacia el dominio de la RNEC “mobiledocs.registraduria.gov.co” (anexo 14).

Si bien en las fases de desarrollo de la aplicación es normal y útil incluir muchos eventos en los logs, la mayoría se deben quitar cuando la aplicación sale a producción y se distribuye, dado que pueden revelar demasiado y vulnerar la seguridad.

Por lo tanto, parece que los desarrolladores han omitido desactivar algunos logs que “hablan demasiado” (y se habían activado para las fases de desarrollo) en la aplicación publicada.

8.5 Las URL de configuración en libre acceso revelan debilidades en la autenticación biométrica

La aplicación utiliza varias URL de acceso público para su configuración (anexo 1), en particular:

- La URL de configuración de la aplicación.
- La URL de configuración de reconocimiento facial (“facecaptureconfiguration”).

Aunque la mayoría de la información del primer archivo debería ser pública, también incluye otras como la política de PIN, detalles sobre las firmas de la aplicación y la segunda URL. En esta, el archivo JSON pone en evidencia que **el nivel de seguridad del reconocimiento facial y de autenticación online están ambos configurados en un nivel bajo (“LOW”)**[100]. Sería necesario investigar a qué corresponden exactamente los niveles marcados como “LOW” por parte de IDEMIA. Sin embargo, es muy probable que ni IDEMIA ni la RNEC tengan la intención de que la información accesible desde estas URL públicas —encontradas tanto en el tráfico de red como en los logs de Android, mucho más fáciles de consultar— esté expuesta.

La presencia de configuraciones de seguridad en niveles “LOW” plantea serios interrogantes sobre la seguridad del sistema de autenticación en línea y del uso de biometría, que constituyen el núcleo de funcionamiento de Cédula Digital.

100. Además de dos otros procesos (“UNLOCK” y “MIGRATION”) que también se encuentran en nivel “LOW”.

Puntos clave de la necesidad de una auditoría externa, independiente y transparente

- **Aspectos positivos y mínimos requeridos**

La seguridad digital de la aplicación Cédula Digital presenta varios puntos positivos, lo cual es fundamental para una herramienta de este alcance y sensibilidad. Sin embargo, estos estándares deberían ser el mínimo esperado en una aplicación con carácter público.

- **Deficiencias técnicas preocupantes**

A pesar de los avances, identificamos algunas negligencias que deben corregirse:

- Defectos en la implementación de HTTPS, aunque sean menores.
- Registros de actividad (logs) que deberían haberse desactivado.
- URL sin control de acceso adecuado.

- **Interrogantes sobre la seguridad biométrica**

El archivo de configuración de la aplicación indica que el reconocimiento facial y la autenticación en línea están configurados en un nivel de seguridad "bajo" ("LOW"). Esto genera dudas sobre la robustez de estos mecanismos, que son elementos clave en la seguridad de la aplicación.

- **Interrogante sobre un servicio abierto del servidor**

Detectamos un puerto/servicio (BGP) abierto en el servidor del dominio principal de la aplicación. Si no se está utilizando, debería cerrarse. En caso contrario, la RNEC debería explicar su función y justificación en este contexto.

- **Necesidad de una auditoría independiente**

Nuestro análisis, basado en metodologías específicas, tiene un alcance limitado y muestra solo una parte del panorama general. Sin embargo, los hallazgos son suficientes para evidenciar la necesidad de una auditoría técnica e independiente sobre la seguridad digital y la privacidad de Cédula Digital, con total transparencia en sus resultados[101].

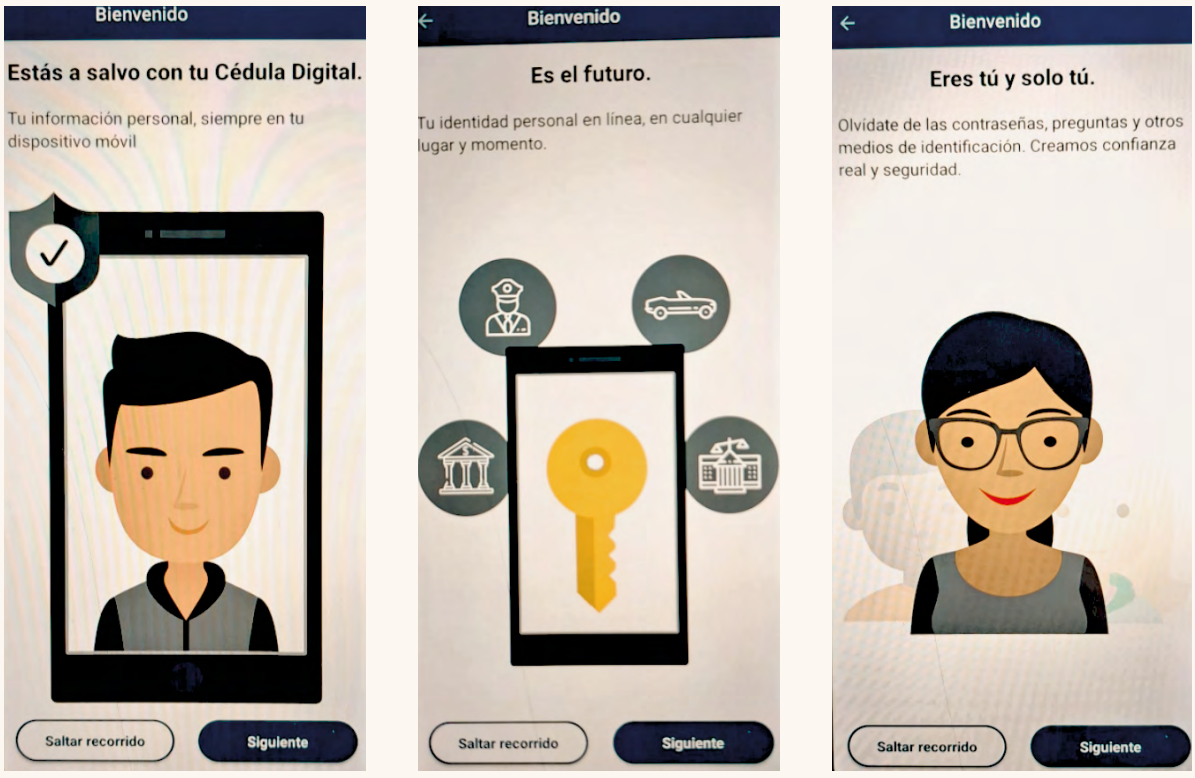
101. Obviamente sin publicar detalles técnicos que puedan vulnerar más la aplicación.

9. INFORMACIÓN PÚBLICA: LO QUE HAY Y TODO LO QUE FALTA

La información oficial sobre Cédula Digital se encuentra principalmente en sus Términos de uso, que se presentan antes de iniciar la aplicación; además, la aplicación incluye una breve Política de privacidad. También hay información disponible en las tiendas de Google y Apple, así como en el sitio web de la RNEC, enfocada principalmente en su uso.

9.1 Información incompleta (Términos de uso y Política de privacidad)

La información que se despliega al iniciar la aplicación es la única que se presenta de forma sistemática, ya que el resto de información mencionada este informe necesita una búsqueda activa por parte de la persona usuaria o interesada.



A B C

Figura 18: Fotografías de las pantallas de inicio de Cédula Digital (a, b y c)
Fuente: Capturas de pantalla Cédula Digital.

Al iniciar la aplicación, se presentan estas imágenes que expresan, explícita o implícitamente, que:

1. Cédula Digital gestiona la información personal de forma segura siempre.
2. Cédula Digital permite gestionar la identidad personal en línea y autenticarse frente a la policía o entes de control, servicios comerciales, del Estado o financieros.
3. La prueba de identidad, autenticación, no se hace con contraseñas sino con biometría.

Después, la aplicación muestra los términos de uso, que se deben aceptar. Esta información no ha cambiado durante nuestro periodo de análisis (segundo semestre 2024 y hasta enero 2025).

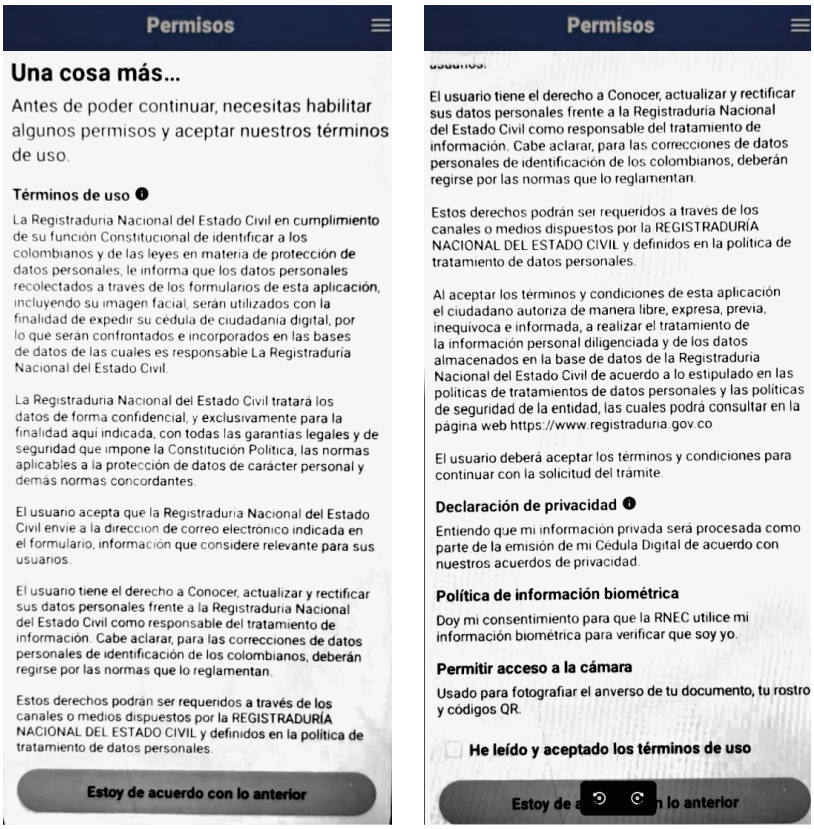


Figura 19. Información y consentimiento inicial de Cédula Digital (Términos de uso)
Fuente: Capturas de pantalla Cédula Digital.

Aunque se titula “Permisos”, son los términos de uso que también se puede encontrar en: https://wapp.registraduria.gov.co/identificacion/cedula-digital/files/pdf/terminos-de-uso_10-05-2022.pdf

Encontramos que los elementos del documento son más de la política de privacidad que de los términos de uso de una aplicación. Los Términos de uso de Cédula Digital se asemejan más a una política de privacidad que a un verdadero documento de términos y condiciones. Su enfoque principal es declarar a la RNEC como responsable del tratamiento de datos personales y solicitar el consentimiento para el uso de la cámara y los datos biométricos. Sin embargo, la política de privacidad disponible es sumamente limitada[102] y no cumple con los requisitos mínimos de la Ley de protección de datos en Colombia.

Nuestra investigación identificó varios elementos fundamentales que no están contemplados en el documento de Términos de uso ni en la Política de privacidad de la aplicación, a pesar de que deberían estarlo. Entre ellos se encuentran nuevas funcionalidades introducidas a partir de la versión 2 de la aplicación, como la autenticación OIDC hacia servicios de terceros, la recepción de notificaciones oficiales del Estado y el almacenamiento de documentos oficiales, funcionalidades anunciadas públicamente por la RNEC en comunicados oficiales. Sin embargo, estas no se describen ni se informa cómo será el tratamiento de los datos personales que implican. Además, en respuesta a un derecho de petición que buscaba confirmar si dichas funcionalidades habían sido efectivamente integradas, la RNEC se negó a responder, alegando que la información era “reservada”; a pesar de que algunas de estas funciones están mencionadas incluso en la descripción de la aplicación en la tienda de Apple.

Podemos afirmar que IDEMIA tiene un papel central en el desarrollo, la gestión y administración de la aplicación y de los servidores que almacenan sus bases de datos. En su respuesta al derecho de petición la RNEC reconoció que IDEMIA es la contratista y que tiene acceso a los servidores y bases de datos, pero esta información no es pública ni detalla el rol específico de IDEMIA. De acuerdo con nuestra investigación, IDEMIA es la “encargada de tratamiento de datos personales” en el sentido de la ley Habeas Data[103] (capítulo 7). IDEMIA además de desarrollar y controlar la aplicación, también podría tener un rol más relevante en la administración de la base de datos correspondiente; por lo que la RNEC podría ser solo la responsable, mas no la encargada del tratamiento de los datos personales capturados para producir la identidad legal.

9.2 Desde las tiendas de Apple y Google

En la tienda de Google aparece información incompleta e incluso contradictoria sobre Cédula Digital. Menciona que la aplicación “no recopila datos del usuario” y a la vez da una lista de datos que se comparten que incluye información personal. Esta información es suministrada por los responsables de la aplicación, sin perjuicio del cuidado que la propia plataforma debería tener a la hora de publicarla.

102. Consultar:
https://wapp.registraduria.gov.co/identificacion/cedula-digital/files/pdf/politicas-de-privacidad_10-05-2022.pdf

103. Encargado del tratamiento: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. Artículo 2, Ley Estatutaria 1581 de 2012.

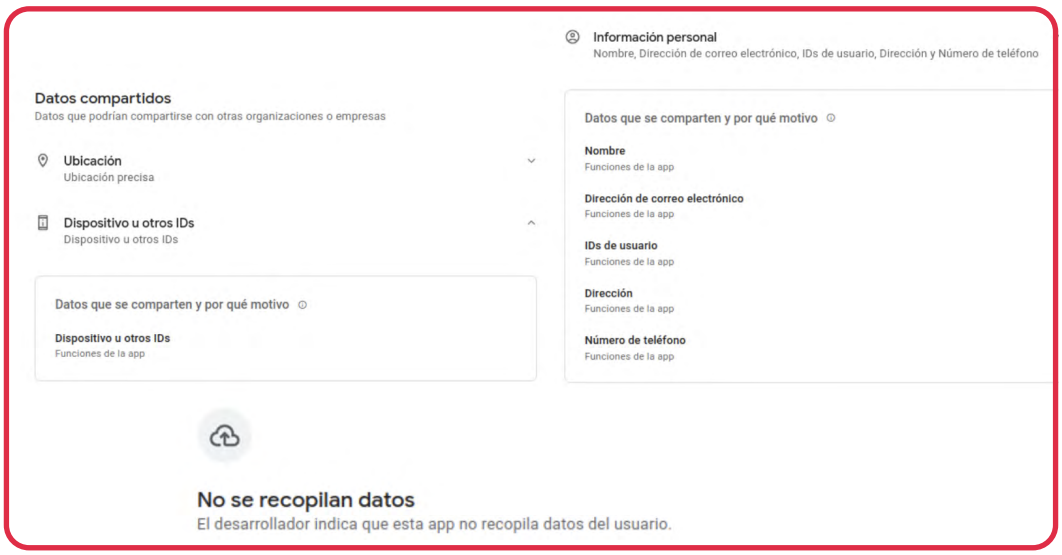


Figura 20. Información de la tienda Google sobre los datos compartidos, la información personal y la recopilación de datos
Fuente: Play Store de Google[104].

Esto indica, también, que los datos están cifrados en tránsito, algo necesario para la seguridad digital y que pudimos verificar, pero que el desarrollador no ofrece forma de borrar los datos.

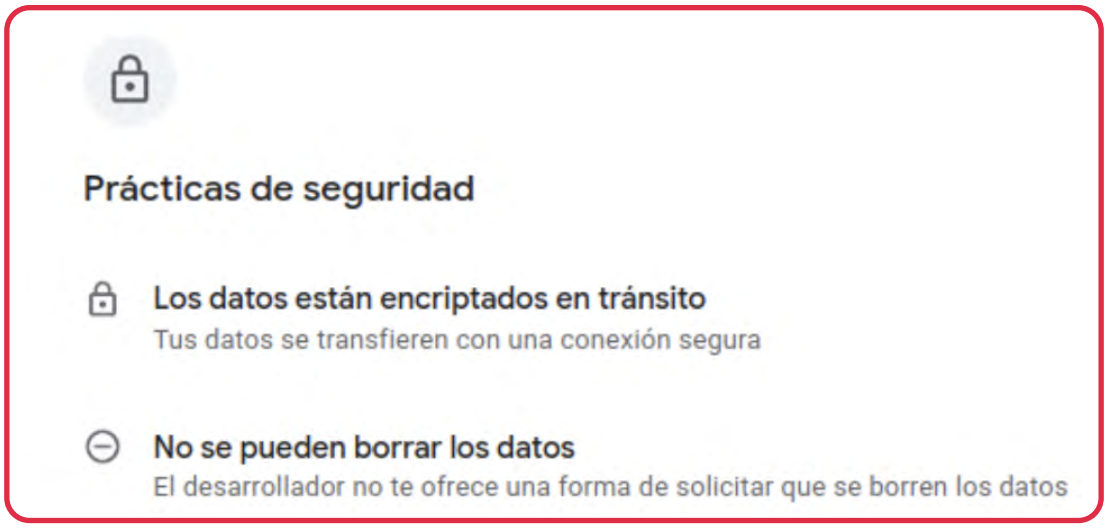


Figura 21. Información de la tienda Google sobre las prácticas de seguridad digital
Fuente: Play Store de Google.

En contraste, la tienda de Apple brinda más información que la Play Store sobre las finalidades y funcionalidades de la Cédula Digital y su historial de actualizaciones.

104. Consultar: https://play.google.com/store/apps/datasafety?id=co.gov.registraduria.ceduladigital&hl=es_CO

La cédula de ciudadanía digital es el formato de identificación por medios electrónicos que expide la Registraduría Nacional del Estado Civil desde diciembre del año 2020 para los mayores de 18 años en Colombia, la cual se activa una vez se reclame su versión física, denominada "cédula de seguridad personalizada en policarbonato".

Puedes instalarla en tu iPhone, siendo viable aún en escenarios offline (sin acceso a internet), **permitiendo la autenticación de la identidad e incrementando la accesibilidad de todos los colombianos y en escenarios online (con acceso a internet) para acceder a servicios digitales seguros.**

Servicios principales:

Identificación: identifícate en escenarios presenciales y medios digitales.

Transacciones Virtuales: realiza transacciones virtuales mediante el protocolo OIDC con autenticaciones con niveles de seguridad 1,2 y 3 **a través de autenticación biométrica facial y PIN**[105].

En su historial de actualizaciones, confirma la implementación de autenticación para servicios de terceros (OIDC) a partir del 20 de noviembre del 2023.

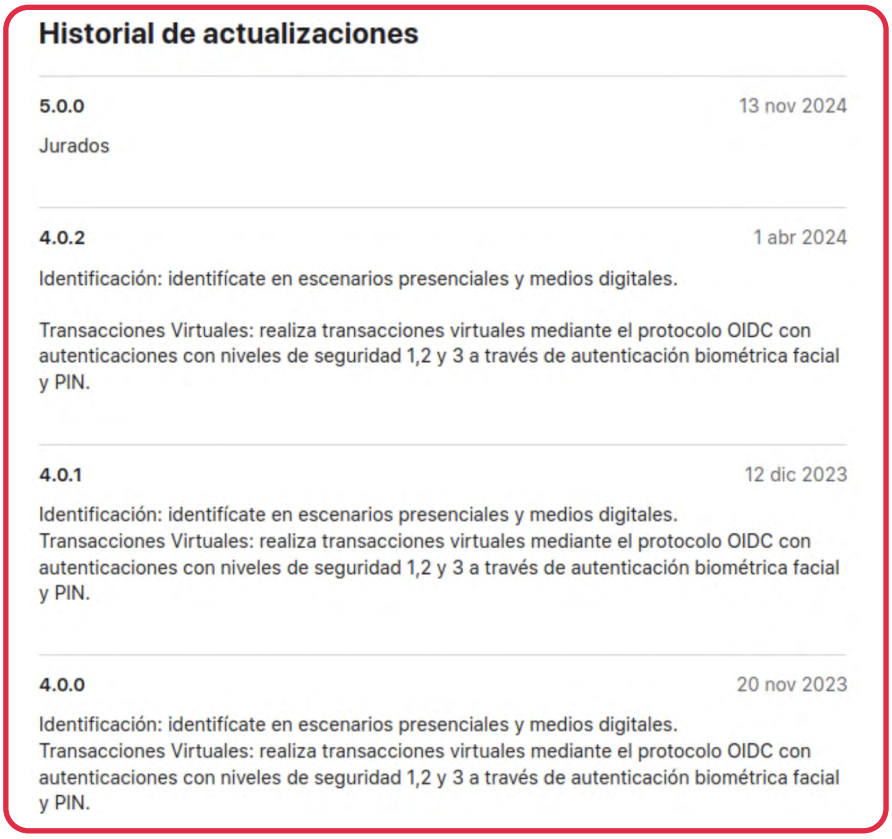


Figura 22.
Historial de actualizaciones de la Cédula Digital en la tienda Apple
Fuente: App Store[106].

105. Consultar: https://apps.apple.com/co/app/cedula-digital-colombia/id1543274615

106. Consultar: https://apps.apple.com/co/app/cedula-digital-colombia/id1543274615

Además, la figura 23 **confirma que la aplicación puede recolectar identificadores, usados para rastrear a la persona usuaria, y datos de ubicación, pero no asociados a la identidad.**

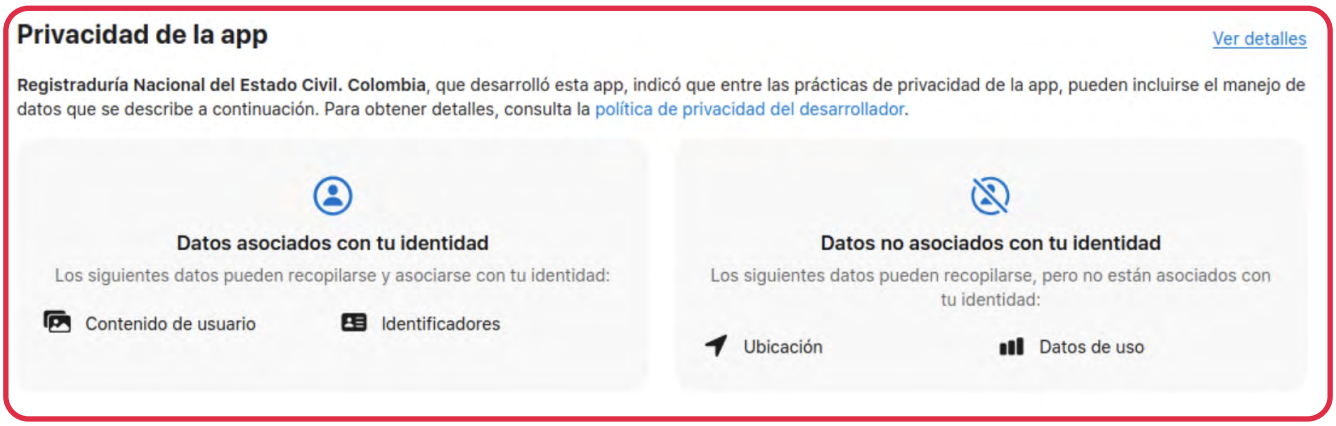


Figura 23. Privacidad de Cédula Digital en la tienda Apple
Fuente: App Store.

Así, los análisis técnicos han mostrado que, efectivamente, la aplicación envía datos no solo a IDEMIA sino también a Google y a la empresa de marketing y analítica que entrega el servicio Localytics (capítulos 5 y 6).

Puntos clave sobre información pública y transparencia de Cédula Digital:

La información pública dada por la RNEC sobre Cédula Digital en sus Términos y condiciones, Política de privacidad, en la App Store de Apple y la Play Store Google es insuficiente y a veces incorrecta o contradictoria. Los términos y condiciones y la política de privacidad no mencionan las nuevas funcionalidades de autenticación para servicios digitales de terceros, la recepción de notificaciones y documentos oficiales. Tampoco mencionan el papel de la empresa IDEMIA que desarrolló, mantiene y administra la aplicación y su base de datos y que debe ser considerada como encargada de tratamiento de datos personales en el sentido de la Ley de Habeas Data.

Esta falta de información y transparencia genera una opacidad sobre la aplicación Cédula Digital que no contribuye a generar la confianza necesaria.

PREGUNTAS Y PREOCUPACIONES PARA AMPLIAR EL DEBATE

Como lo hemos afirmado a lo largo del informe, la Cédula Digital es un proyecto que busca ser no solo un documento de identidad oficial en línea; sino también la llave de acceso a servicios del estado, especialmente al servicio de notificaciones y gestión documental.

Por este motivo, es clave discutir los alcances de la aplicación en el contexto que describe este informe; ya que la relación estrecha entre IDEMIA y la RNEC deja muchas preguntas sobre la aplicación Cédula Digital.

Con este informe, desde Karisma lanzamos el interrogante sobre dónde empieza la RNEC y dónde termina IDEMIA, ya que es más difícil de identificar de lo que se esperaría en una relación entre una entidad pública y una empresa privada. Por ello, planteamos algunas preguntas clave que consideramos esenciales para enriquecer el debate público y orientar futuras decisiones en materia de digitalización estatal.

- ¿Quién debe definir, y con base en qué criterios, el nivel de dependencia aceptable de una entidad pública respecto de una empresa privada para el cumplimiento de funciones constitucionales y legales?
- Cuando dicha dependencia se considere excesiva o inaceptable, ¿cómo puede reducirse sin afectar la continuidad del servicio ni comprometer la seguridad y privacidad de los datos de las personas?
- ¿Qué principios deben guiar el diseño de relaciones sostenibles y transparentes entre el sector público y el privado en la provisión de servicios digitales del Estado?

En relación con la función de identificación y autenticación de personas, surgen interrogantes fundamentales:

- ¿Es preferible una solución centralizada y dependiente de una empresa extranjera, como Cédula Digital, frente a modelos descentralizados y bajo control público?
- ¿Cuándo y con qué criterios se tomó esta decisión estratégica? ¿Hubo discusión pública o evaluación de alternativas?
- ¿Qué opciones existen para la identificación y autenticación en línea que no recurran a datos biométricos?
- ¿Cuáles de estas alternativas podrían implicar menores riesgos para los derechos fundamentales de las personas, especialmente en términos de privacidad, autonomía y no discriminación?

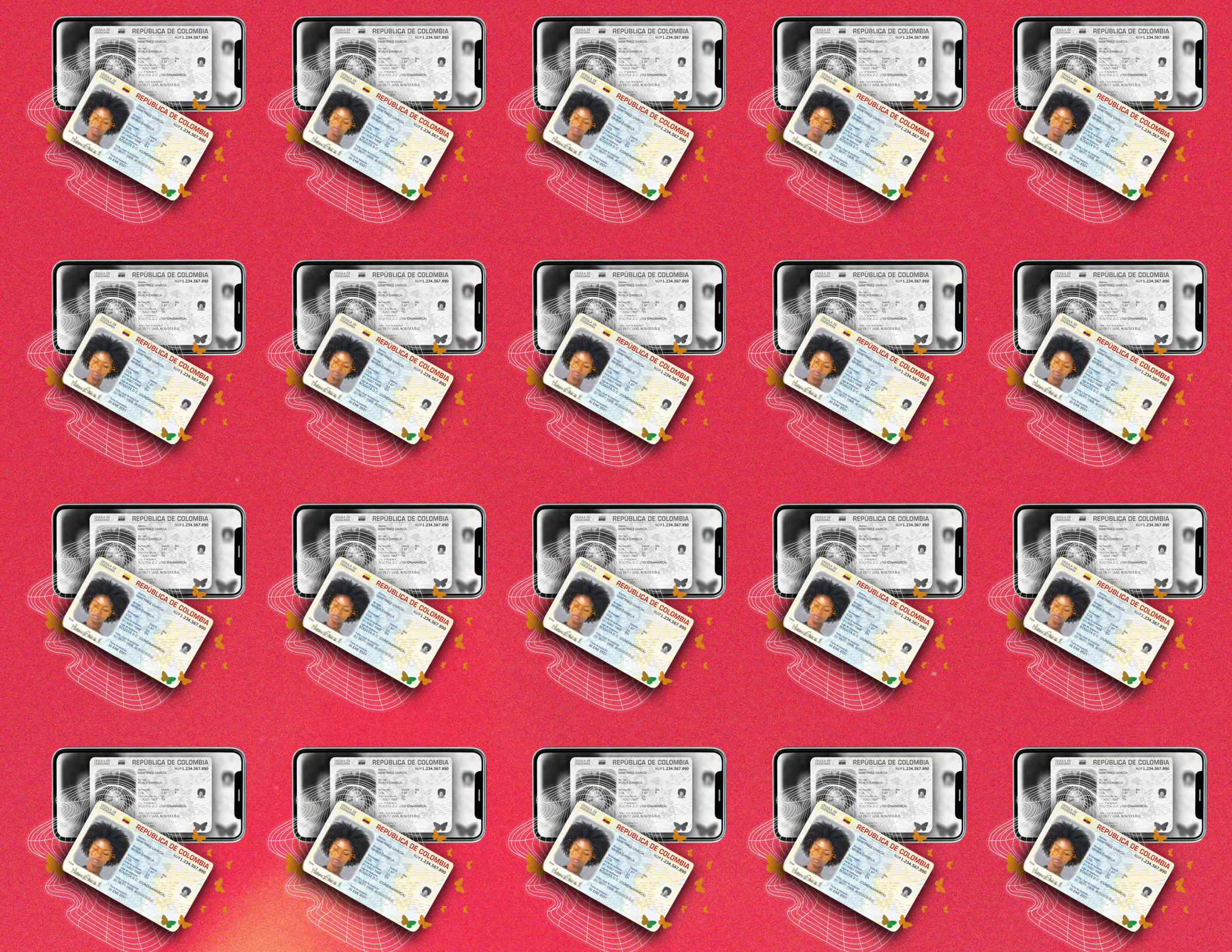
Estrechamente relacionado con el punto anterior y desde la perspectiva del derecho a la intimidad y la protección de datos personales, surgen preguntas que deben ser consideradas en el diseño y la evaluación de aplicaciones estatales:

- ¿Cómo garantizar que estas aplicaciones incorporen desde su concepción la privacidad y la protección de datos personales por defecto?
- ¿Cuál es el papel de las empresas de marketing en el ecosistema de la Cédula Digital?
- ¿Qué tipo y volumen de datos personales pueden estar obteniendo sobre la ciudadanía colombiana a través de esta aplicación?
- ¿Cómo se justifica el tratamiento de estos datos por parte de actores privados, especialmente cuando se trata de finalidades comerciales ajenas a los fines constitucionales del servicio?
- ¿Qué desafíos plantea esta situación para nuestro régimen jurídico en materia de tratamiento de datos personales, en particular frente a los principios de finalidad, proporcionalidad, consentimiento informado y las reglas sobre transferencias transfronterizas?

Finalmente, desde el punto de vista de la seguridad digital, el informe plantea algunas preguntas fundamentales que deberían orientar futuras decisiones tecnológicas en el sector público:

- ¿Cómo fortalecer el diseño y la implementación de tecnologías públicas para que la seguridad digital orientada a la protección de derechos esté en el centro del proceso y no sea una preocupación secundaria o reactiva?
- ¿Cómo institucionalizar auditorías externas, independientes y técnicamente robustas en proyectos estatales que han sido tercerizados o que involucran propiedad intelectual privada, de modo que se genere confianza pública y se garanticen los derechos de las personas?
- En relación con la decisión de incorporar biometría facial como mecanismo de autenticación, ¿cómo mitigar los riesgos asociados al uso de datos biométricos —que, a diferencia de una contraseña, no pueden cambiarse— en caso de fuga, mal uso o robo?

Desde Karisma, esperamos abrir un debate informado y plural sobre el rumbo que deben tomar las infraestructuras digitales del Estado. Frente a tecnologías que tocan funciones esenciales como la identificación ciudadana, resulta indispensable pensar en modelos que prioricen la soberanía tecnológica, la transparencia institucional, la seguridad digital y la protección efectiva de los derechos.


REPÚBLICA DE COLOMBIA
NUP 1.234.567.890

<K+ LAB>

Fundación Karisma

karisma.org.co