Superintendencia de Industria y Comercio

RESOLUCIÓN NÚMERO 78798 DE 2025

(03 de octubre de 2025)

"Por la cual se impone una sanción y se imparten órdenes administrativas"

VERSIÓN ÚNICA

Radicación 24-240075

LA DIRECTORA DE INVESTIGACIONES DE PROTECCIÓN DE DATOS PERSONALES

En ejercicio de sus facultades legales, en especial las conferidas por el los literales a) y b) del artículo 21 la Ley 1581 de 2012, en concordancia con el numeral 4° del artículo 17 del Decreto 4886 de 2011, modificado por el artículo 7 del Decreto 092 de 2022, y

CONSIDERANDO

PRIMERO. Que, mediante Resolución No. 46436 del 16 de agosto de 2024, se inició una investigación administrativa y se formuló cargos a **WORLDCOIN FOUNDATION** y **TOOLS FOR HUMANITY CORPORATION**, como Responsables del tratamiento de datos personales por la presunta infracción a lo dispuesto en las normas que se relacionan a continuación:

(i) Literales a) y k) del artículo 17 de la Ley 1581 de 2012, en concordancia con el literal a) del artículo 4 de la misma Ley y el artículo 2.2.2.25.3.1 del Decreto 1074 de 2015.

(ii) Literales a) y b) del artículo 17 de la Ley 1581 de 2012 en concordancia con los literales a), c) y e) del artículo 4 de la misma Ley; el inciso primero del artículo 2.2.2.25.2.2, los artículos 2.2.2.25.2.4 y 2.2.2.25.2.5 del Decreto 1074 de 2015.

(iii) Literales a) y b) del artículo 17 de la Ley 1581 de 2012 en concordancia con los literales a), c) y e) del artículo 4 de la misma Ley; el inciso primero del artículo 2.2.2.25.2.2 y los artículos 2.2.2.25.2.3, 2.2.2.25.2.4 y 2.2.2.25.2.5 del Decreto 1074 de 2015.

(iv) Literales a) y c) del artículo 17 de la Ley 1581 de 2012 en concordancia con los literales a) y b) del artículo 4, los artículos 8 y 12 de la misma Ley y el inciso primero del artículo 2.2.2.25.2.2 del Decreto 1074 de 2015.

(v) Literales a), d) y k) del artículo 17 de la Ley 1581 de 2012 en concordancia con los literales a) y g) del artículo 4 de la misma Ley y el artículo 2.2.2.35.6.1 del Decreto 1074 de 2015.

(vi) Literales a) y k) del artículo 17 de la Ley 1581 de 2012 en concordancia con los literales a) y g) del artículo 4 de la misma norma y el artículo 2.2.2.25.6.1 del Decreto 1074 de 2015.

(vii) Literales a) y k) del artículo 17 de la Ley 1581 de 2012 en concordancia con el literal a) del artículo 4 de la misma Ley y el artículo 2.2.2.25.6.1 del Decreto 1074 de 2015.

Así mismo, de conformidad con lo establecido en el artículo 47 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, se corrió el traslado a Worldcoin Foundation y Tools For Humanity para que presentaran los descargos correspondientes.

SEGUNDO. Que mediante certificación No. 24-240075-33 del 23 de agosto de 2024, la Resolución No. 46436 del 16 de agosto de 2024, fue notificada personalmente por medio electrónico a WorldCoin Foundation y Tools For Humanity el día 22 de agosto de 2024, por lo que el término para presentar los descargos venció el día 12 de septiembre de 2024, sin que éstos hayan sido presentados.

TERCERO. Que mediante Resolución No. 58267 del 30 de septiembre de 2024, se incorporaron las pruebas allegadas a la presente actuación administrativa como se relaciona a continuación:

1. Oficios radicados con los números 24-240075-01 y 24-240075-02 del 11 de junio de 2024, mediante los cuales se requirió a **TOOLS FOR HUMANITY**, para que diera respuesta a unos requerimientos relacionados con la operación de **WORLDAPP** y/o **WORLD ID.**

2. Oficios radicados con los números 24-240075-05 y 24-240075-06 del 2 de julio de 2024 mediante los cuales el apoderado de Tools For Humanity, dio respuesta a las presuntas realizadas por este Despacho, relacionados anteriormente.

3. Acta de Preservación de Página Web No. 087 del 8 de julio de 2024, radicada en el sistema de trámites con el número 24-240075-27 mediante la cual el Grupo de Trabajo de Informática Forense y Seguridad Digital de la Oficina de Tecnología e Informática (en adelante GTIFSD) de esta Superintendencia, mediante la cual se realizó la preservación del sitio web https://es-es.worldcoin.org.

CUARTO. Que mediante Oficios Nos. 24-240075-40, 24-240075-41, 24-240075-43 y 24-240075-45 del 11 de octubre de 2024, los apoderados de **WORLDCOIN FOUNDATION** y **TOOLS FOR HUMANITY CORPORATION** presentaron solicitudes de Corrección de irregularidades en la actuación administrativa, así mismo presentaron un Incidente de Nulidad por indebida notificación de la Resolución No. 46436 del 16 de agosto de 2024 "Por la cual se inicia una investigación administrativa y se formulan cargos".

Sobre las citadas solicitudes el Despacho hará el respectivo pronunciamiento en el presente acto administrativo.

QUINTO. Que mediante oficio No. 24-240075-46 del 15 de octubre de 2024 los apoderados de **WORLDCOIN FOUNDATION** y **TOOLS FOR HUMANITY CORPORATION** presentaron escrito de alegatos de conclusión conforme el traslado hecho por este Despacho en la Resolución No. 58267 del 30 de septiembre de 2024, en el cual solicitaron se tuvieran en cuenta los siguientes documentos y enlaces:

Sitios Web

1. Sitio web de Términos y Condiciones de Usuario de Tools for Humanity, Versión 3.29: https://worldcoin.pactsafe.io/legal.html#contract-qx3iz24-o

2. Sitio web de Aviso de Privacidad de Tools for Humanity. Versión 4.25: https://worldcoin.pactsafe.io/legal.html#contract-9l-r7n2jt

3. Sitio web de Términos y Condiciones de Worldcoin Foundation. Versión 3.11: https://vault.pactsafe.io/s/8a18d792-fd76-44db-9b92-b0bb7981c248/legal.html?_gl=1*prn2v5*_gcl_au*MjgyODczNzM4LjE3Mjg2NTA5NTQ.#contract-byutjvtyt

4. Sitio web de Aviso de Privacidad de Worldcoin Foundation. Versión 3.14: https://vault.pactsafe.io/s/8a18d792-fd76-44db-9b92-b0bb7981c248/legal.html?_gl=1*prn2v5*_gcl_au*MjgyODczNzM4LjE3Mjg2NTA5NTQ.#contract-s1ytru6kk

5. Sitio web de Formulario de Consentimiento de Worldcoin Foundation para Datos Biométricos. Versión 1.18: https://vault.pactsafe.io/s/8a18d792-fd76-44db-9b92-b0bb7981c248/legal.html?_gl=1*prn2v5*_gcl_au*MjgyODczNzM4LjE3Mjg2NTA5NTQ.#contract-syn0uxpen

6. Sitio web de Términos y Condiciones de TFH Operator. Versión 1.0: https://worldcoin.pactsafe.io/hkyr3jgst.html#contract-hytuueeot

7. Sitio web de Portal de Solicitudes: https://tfh-privacy.zendesk.com/hc/en-us/requests/new?ticket_form_id=32124980246035

8. Sitio web de Worldcoin. ¿Qué es un operador de Worldcoin y cómo puedo convertirme en uno?: https://es-es.worldcoin.org/blog/worldcoin/what-is-worldcoin- operator

9. Sitio web de Worldcoin. Cumplimiento normativo, privacidad personal y acceso equitativo con Worldcoin: https://es-es.worldcoin.org/blog/worldcoin/regulatory-compliance-personal-privacy-equitable-access-worldcoin

10. Sitio web de Worldcoin. Privado por diseño: Una guía de los pilares de privacidad y el whitepaper de Worldcoin: https://es-es.worldcoin.org/blog/worldcoin/private- design-guide-worldcoin-privacy-pillars-whitepaper

11. Sitio web de Worldcoin. Privacidad: https://es-es.worldcoin.org/privacy

12. Sitio web de Worldcoin. Preguntas frecuentes sobre la privacidad de Worldcoin: https://es-es.worldcoin.org/blog/worldcoin/worldcoin-privacy-faqs

13. Sitio web de Worldcoin. El blog de Worldcoin (incluye vídeos explicativos sobre privacidad): https://es-es.worldcoin.org/blog

14. Sitio web de Worldcoin. Anuncio del programa de recompensas por detección de errores del Proyecto Worldcoin: https://es-es.worldcoin.org/blog/announcements/announcing-worldcoin-bug-bounty-program

Pantallazos:

15. Pantallazos de la sección de Seguridad y Privacidad de las Configuraciones de la World App.

16. Pantallazos del trayecto del usuario para acceder a la Orb App y ser operador de Orb.

17. Pantallazos del trayecto del usuario para acceder a la World App.

18. Pantallazos del trayecto del usuario para verificarse y obtener el World ID.

19. Pantallazo de materiales explicativos sobre el tratamiento de datos que realiza WF y que se ponen a disposición en distintas locaciones.

Whitepaper y Auditorías Externas

20. Whitepaper de Worldcoin. Privado por diseño: https://worldcoin.org/privatebydesign-whitepaper?_gl=1*1ddu53o*_gcl_au*MjgyODczNzM4LjE3Mjg2NTA5NTQ.

21. Auditoría del Protocolo de Worldcoin. Esta auditoría se elaboró de manera externa por Least Authority TFA GmbH, compañía enfocada en asuntos de privacidad en tecnología: https://leastauthority.com/wp-content/uploads/2024/05/Least-Authority- Worldcoin-MPC-Protocol-for-Uniqueness-Check-Final-Audit-Report.pdf

22. Auditoría de Revisión de Seguridad del Protocolo Worldcoin. Esta auditoría se elaboró de manera externa por Nethermind, compañía de investigación e ingeniería de software: https://github.com/NethermindEth/PublicAuditReports/blob/main/NM0122-FINAL_WORLDCOIN.pdf

23. Auditoría de Criptografía del Protocolo Worldcoin. Esta auditoría se elaboró de manera externa por Least Authority TFA GmbH, compañía enfocada en asuntos de privacidad en tecnología: https://leastauthority.com/wp-content/uploads/2023/07/Worldcoin_Protocol_Cryptography_Final_Audit_Report.p df

24. Auditoría del Software del Orb. Esta auditoría se elaboró de manera externa por Trail of Bits, una compañía que provee asesoría y análisis técnicos de seguridad: https://github.com/trailofbits/publications/blob/master/reviews/2023-08-worldcoin- orb-securityreview.pdf

Política de Seguridad de la Información

25. Política de Seguridad de la Información de Worldcoin de agosto del 2021.

Data Privacy Impact Assessment

26. Data Privacy Impact Assessment de la Worldcoin Foundation en relación con el procesamiento de datos a través del Orb en el contexto de la verificación de la Prueba de Humanidad.

Igualmente se solicitó un plazo para la presentación de los siguientes dictámenes:

a. Dictamen pericial de experto en informática, protección de datos y seguridad de la información, el cual será realizado por un perito experto en informática, protección de datos y seguridad de la información. Los objetivos del dictamen pericial serán entre otros:

- Determinar si el sitio web de Worldcoin (https://es-es.worldcoin.org) recolecta o no datos personales.
- Determinar si la funcionalidad de "Habilitación para la Custodia de Datos" está o no desactivada globalmente.
- Evidenciar cuáles son las medidas que toman las Entidades para salvaguardar la confidencialidad, integridad y disponibilidad de los datos.
- Ilustrar al Despacho sobre los aspectos técnicos que dieron lugar a la Resolución de Cargos.

b. Dictamen Pericial para realizar por un perito traductor oficial. Indica que su objetivo es aportar traducciones oficiales al español de los documentos aportados en el escrito de alegatos de conclusión.

SEXTO. Que mediante Resolución No. 70363 del 19 de noviembre de 2024, este Despacho reabrió el periodo probatorio, se incorporaron las pruebas relacionadas en el escrito de alegatos de conclusión y además decretó la práctica de unas pruebas, en los siguientes términos:

> *"**ARTÍCULO 1. ORDENAR** la reapertura del periodo probatorio establecido en el artículo 40 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.*
>
> ***ARTÍCULO 2.** Como consecuencia de lo anterior, este Despacho procede a:*
>
> 1. ***INCORPORAR** y tener como prueba todos los documentos y enlaces relacionados y allegados por los apoderados de **WORLDCOIN FOUNDATION** y **TOOLS FOR HUMANITY CORPORATION**, en el escrito de alegatos de conclusión radicado con el número 24-240075-46 de fecha 15 de octubre de 2024.*
> 2. ***CONCEDER** un término de treinta (30) días a los apoderados de **WORLDCOIN FOUNDATION** y **TOOLS FOR HUMANITY CORPORATION,** para que presenten los informes periciales sobre los cuales se hace referencia en el escrito de alegatos de conclusión y que fueran relacionados en la parte motiva del presente acto administrativo.*
> 3. ***DECRETAR** como prueba de oficio la preservación de la página web https://es-es.worldcoin.org así como de la aplicación APP – World App, para lo cual se hará la respectiva solicitud al Grupo de Trabajo de Informática Forense y Seguridad Digital de la Oficina de Tecnología e Informática de esta Superintendencia".*

SÉPTIMO. Que mediante los oficios No. 24-240075-42 y 24-240075-44 del 11 de octubre de 2024, los apoderados de Worldcoin Foundation y Tools For Humanity, presentaron solicitudes de revocatoria directa respecto de la Resolución No. 46436 del 16 de agosto de 2024 "Por la cual se inicia una investigación administrativa y se formulan cargos" y la Resolución No. 58267 del 30 de septiembre de 2024 "Por la cual se incorporan pruebas y se corre traslado para alegar", solicitudes que fueron **RECHAZADAS** por **IMPROCEDENTES** a través de la Resolución No. 71479 del 22 de noviembre de 2024.

OCTAVO. Que dentro del consecutivo No. 24-240075-64 del 30 de diciembre de 2024 se radicó en el sistema de trámites de la entidad el Acta No. 214-24 del 16 de diciembre de 2024 mediante la cual el Grupo de Trabajo de Informática Forense y Seguridad Digital de la Oficina de Tecnología e Informática de esta Superintendencia, realizó la preservación del sitio web https://world.org/es.es y la aplicación World App.

NOVENO. Que mediante Oficios No. 24-240075-65 y 24-240075-66 del 30 de diciembre de 2024, los apoderados especiales de **WORLDCOIN FOUNDATION** y **TOOLS FOR HUMANITY CORPORATION** presentaron escritos mediante los cuales allegan los informes periciales relacionados en el numeral 2 del artículo

2 de la Resolución No. 70363 del 19 de noviembre de 2024, así mismo allegaron la información que se relaciona a continuación:

Sitios Web

1. Sitio web de Términos y Condiciones de Usuario de Tools for Humanity, Versión 3.29: https://worldcoin.pactsafe.io/legal.html#contract-qx3iz24-o

2. Sitio web de Aviso de Privacidad de Tools for Humanity. Versión 4.25: https://worldcoin.pactsafe.io/legal.html#contract-9l-r7n2jt

3. Sitio web de Términos y Condiciones de Worldcoin Foundation. Versión 3.11: https://vault.pactsafe.io/s/8a18d792-fd76-44db-9b92-b0bb7981c248/legal.html?_gl=1*prn2v5*_gcl_au*MjgyODczNzM4LjE3Mjg2NTA 5NTQ.#contract-byutjvtyt

4. Sitio web de Aviso de Privacidad de Worldcoin Foundation. Versión 3.14: https://vault.pactsafe.io/s/8a18d792-fd76-44db-9b92-b0bb7981c248/legal.html?_gl=1*prn2v5*_gcl_au*MjgyODczNzM4LjE3Mjg2NTA 5NTQ.#contract-s1ytru6kk

5. Sitio web de Formulario de Consentimiento de Worldcoin Foundation para Datos Biométricos. Versión 1.18: https://vault.pactsafe.io/s/8a18d792-fd76-44db-9b92-b0bb7981c248/legal.html?_gl=1*prn2v5*_gcl_au*MjgyODczNzM4LjE3Mjg2NTA 5NTQ.#contract-syn0uxpen

6. Sitio web de Términos y Condiciones de TFH Operator. Versión 1.0: https://worldcoin.pactsafe.io/hkyr3jgst.html#contract-hytuueeot

7. Sitio web de Portal de Solicitudes: https://tfh-privacy.zendesk.com/hc/en-us/requests/new?ticket_form_id=32124980246035

8. Sitio web de Worldcoin. ¿Qué es un operador de Worldcoin y cómo puedo convertirme en uno?: https://es-es.worldcoin.org/blog/worldcoin/what-is-worldcoin- operator

9. Sitio web de Worldcoin. Cumplimiento normativo, privacidad personal y acceso equitativo con Worldcoin: https://es-es.worldcoin.org/blog/worldcoin/regulatory- compliance-personal-privacy-equitable-access-worldcoin

10. Sitio web de Worldcoin. Privado por diseño: Una guía de los pilares de privacidad y el whitepaper de Worldcoin: https://es-es.worldcoin.org/blog/worldcoin/private- design-guide-worldcoin-privacy-pillars-whitepaper

11. Sitio web de Worldcoin. Privacidad: https://es-es.worldcoin.org/privacy

12. Sitio web de Worldcoin. Preguntas frecuentes sobre la privacidad de Worldcoin: https://es-es.worldcoin.org/blog/worldcoin/worldcoin-privacy-faqs

13. Sitio web de Worldcoin. El blog de Worldcoin (incluye vídeos explicativos sobre privacidad): https://es-es.worldcoin.org/blog

14. Sitio web de Worldcoin. Anuncio del programa de recompensas por detección de errores del proyecto Worldcoin: https://es-es.worldcoin.org/blog/announcements/announcing-worldcoin-bug-bounty-program

Pantallazos

15. Pantallazos de la sección de Seguridad y Privacidad de las Configuraciones de la World App.

16. Pantallazos del trayecto del usuario para acceder a la Orb App y ser operador de Orb.

17. Pantallazos del trayecto del usuario para acceder a la World App.

18. Pantallazos del trayecto del usuario para verificarse y obtener el World ID.

19. Pantallazo de materiales explicativos sobre el tratamiento de datos que realiza WF y que se ponen a disposición en distintas locaciones.

Whitepaper y Auditorías Externas

20. Whitepaper de Worldcoin. Privado por diseño: https://worldcoin.org/privatebydesign-whitepaper?_gl=1*1ddu53o*_gcl_au*MjgyODczNzM4LjE3Mjg2NTA5NTQ.

21. Auditoría del Protocolo de Worldcoin. Esta auditoría se elaboró de manera externa por Least Authority TFA GmBH, compañía enfocada en asuntos de privacidad en tecnología: https://leastauthority.com/wp-content/uploads/2024/05/Least-Authority- Worldcoin-MPC-Protocol-for-Uniqueness-Check-Final-Audit-Report.pdf

22. Auditoría de Revisión de Seguridad del Protocolo Worldcoin. Esta auditoría se elaboró de manera externa por Nethermind, compañía de investigación e ingeniería de software: https://github.com/NethermindEth/PublicAuditReports/blob/main/NM0122-FINAL_WORLDCOIN.pdf

23. Auditoría de Criptografía del Protocolo Worldcoin. Esta auditoría se elaboró de manera externa por Least Authority TFA GmBH, compañía enfocada en asuntos de privacidad en tecnología:https://leastauthority.com/wp-content/uploads/2023/07/Worldcoin_Protocol_Cryptography_Final_Audit_Report.p df

24. Auditoría del Software del Orb. Esta auditoría se elaboró de manera externa por Trail of Bits, una compañía que provee asesoría y análisis técnicos de seguridad: https://github.com/trailofbits/publications/blob/master/reviews/2023-08-worldcoin- orb-securityreview.pdf

Política de Seguridad de la Información

25. Política de Seguridad de la Información de Worldcoin de agosto del 2021.

Data Privacy Impact Assessment

26. Data Privacy Impact Assessment de la Worldcoin Foundation en relación con el procesamiento de datos a través del Orb en el contexto de la verificación de la Prueba de Humanidad.

DECIMO. Que mediante Oficios Nos. 24-240075-67 y 24-240075-68 del 29 de enero de 2025, se corrió traslado para alegar a los apoderados de **WORLDCOIN FOUNDATION** y **TOOLS FOR HUMANITY CORPORATION.**

DECIMOPRIMERO. Que, previo a resolver de fondo la presente actuación administrativa, considera el Despacho necesario pronunciarse frente a los incidentes de nulidad presentados por los apoderados de las organizaciones, así como las solicitudes de corrección de irregularidades en los términos del artículo 41 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

11.1. Respecto del Incidente de Nulidad planteado por parte de los apoderados de WorldCoin y Tools for humanity.

Mediante los oficios número 24-245075-41 y 24-240075-45 del 11 de octubre de 2024, los apoderados de **WORLDCOIN FOUNDATION** y **TOOLS FOR HUMANITY CORPORATION** presentaron un **incidente de nulidad** por indebida notificación de la Resolución No. 46436 del 16 de agosto de 2024, teniendo en cuenta los siguientes argumentos:

Consideran que el incidente de nulidad procesal *"es plenamente procedente en el marco del presente trámite administrativo, habida cuenta de lo consagrado en el artículo 306 del CPACA, que dispone que, en los aspectos no contemplados en este código, se seguirá lo dispuesto por el Código de Procedimiento Civil, hoy CGP."*

Afirman que la nulidad procesal se encuentra consagrada en el artículo 132[1] y siguientes del CGP, de cuya lectura se desprende que este mecanismo se

[1] **ARTÍCULO 132. CONTROL DE LEGALIDAD.** Agotada cada etapa del proceso el juez deberá realizar control de legalidad para corregir o sanear los vicios que configuren nulidades u otras irregularidades del proceso, las cuales, salvo que se trate de hechos nuevos, no se podrán alegar en las etapas siguientes, sin perjuicio de lo previsto para los recursos de revisión y casación.

predica y aplica respecto de todo procedimiento en el cual intervenga una autoridad. Como causal se alega la contemplada en el numeral 8 del artículo 133[2] de la misma codificación.

Pues bien, respecto de la solicitud de nulidad invocada por parte de los apoderados de **WORLDCOIN FOUNDATION** y **TOOLS FOR HUMANITY CORPORATION**, este Despacho **no tiene competencia** para realizar pronunciamiento alguno, en la medida que esa potestad corresponde únicamente a la jurisdicción de lo contencioso administrativo. Sobre el tema en particular la doctrina[3] ha indicado:

> *"[l]a declaración de nulidad del Acto Administrativo le compete a la jurisdicción de lo contencioso administrativa, y es el resultado de una demanda, el proceso que debe seguirse, razones de hecho y de derecho que aporta el demandante, para finalizar con un fallo declarándolo o no la respectiva nulidad".*

En el mismo sentido[4], se ha manifestado lo siguiente:

> *"En Colombia, la nulidad de los actos administrativos solo es jurisdiccional y como tal la pueden declarar las autoridades contencioso-administrativas (los jueces administrativos, los tribunales administrativos y la Sala de lo Contencioso Administrativo del Consejo de Estado), según la distribución de competencia y las acciones señaladas en el CCA., hoy contenido en la Ley 1437 de 2011, en concordancia con la Ley 270 de 1996, en única o primera instancia según sea el caso.*
>
> *La anulación del acto administrativo solo se puede promover a través de acción judicial ante la jurisdicción contencioso administrativa, según las competencias fijadas en las disposiciones atrás mencionadas".*

Así las cosas, la solicitud realizada para efectos de la presente actuación administrativa, no requiere mayor desarrollo jurídico.

11.2. Respecto de las solicitudes de corrección de irregularidades de conformidad con lo establecido en el artículo 41 del CPACA.

A través de los Oficios No. 24-240075-40 y 24-240075-43 del 11 de octubre de 2024, los apoderados de WorldCoin Foundation y Tools For Humanity, solicitaron la corrección de irregularidades en la presente actuación administrativa, conforme lo establecido en el artículo 41 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, pues consideran que la Resolución No. 46436 del 16 de agosto de 2024, "Por medio de la cual se inicia una investigación administrativa y se formulan cargos", no fue notificada conforme las normas establecidas para el efecto.

Afirman los apoderados que, en el caso particular se debió seguir el procedimiento de notificación establecido en la Ley 1073 de 2006, *"Por medio de la cual se aprueba la convención sobre la notificación o traslado en el extranjero de documentos judiciales o extrajudiciales en Materia Civil o Comercial, hecha en La Haya el 15 de noviembre de 1965"*.

Asimismo, indican que no se tuvo en cuenta lo dispuesto en el artículo 291 del Código General del Proceso, el cual indica que cuando se realice una notificación al exterior se debe conceder un plazo de 30 días para comparecer a ser notificado.

---

[2] **ARTÍCULO 133. CAUSALES DE NULIDAD.** El proceso es nulo, en todo o en parte, solamente en los siguientes casos: 8. Cuando no se practica en legal forma la notificación del auto admisorio de la demanda a personas determinadas, o el emplazamiento de las demás personas aunque sean indeterminadas, que deban ser citadas como partes, o de aquellas que deban suceder en el proceso a cualquiera de las partes, cuando la ley así lo ordena, o no se cita en debida forma al Ministerio Público o a cualquier otra persona o entidad que de acuerdo con la ley debió ser citado.
Cuando en el curso del proceso se advierta que se ha dejado de notificar una providencia distinta del auto admisorio de la demanda o del mandamiento de pago, el defecto se corregirá practicando la notificación omitida, pero será nula la actuación posterior que dependa de dicha providencia, salvo que se haya saneado en la forma establecida en este código.

[3] PENAGOS, Gustavo. El Acto Administrativo Tomo II. Ediciones Doctrina y Ley. Bogotá D.C., 2008

[4] BERROCAL GUERRERO, Luis Enrique. Manual del Acto Administrativo. Librería Ediciones del Profesional Ltda. Sexta edición. Bogotá D.C. 2014.

Afirman que la notificación electrónica realizada al correo electrónico jannick.preiwisch@toolsforhumanity.com, no puede considerarse como válida, teniendo en cuenta que dicha dirección no pertenece Worldcoin Foundation. Frente a Tools For Humanity, corresponde a uno de sus funcionarios, situación que no lo convierte en un correo válido para efectuar las notificaciones judiciales ni extrajudiciales.

Finalmente, consideran que se vulneró el debido proceso de sus representadas teniendo en cuenta que la Resolución No. 46436 del 16 de agosto de 2024, por medio de la cual les fueron formulados los cargos, no fue notificada en debida forma.

Así las cosas, con el fin de pronunciarnos respecto de la solicitud elevada por los apoderados de las investigadas considera el Despacho necesario realizar un recuento sobre el trámite que se ha surtido dentro de la presente actuación administrativa:

(i) A través de los Oficios No. 24-240075-01 y 24-240075-02 del 11 de junio de 2024, se requirió a Tools For Humanity y WorldCoin Foundation para que brindaran información relacionada con la operación que se realiza respecto de la aplicación WORLD APP y/o WORLD ID. Solicitudes que se remitieron a los correos electrónicos legal@toolsforhumanity.com y dpo@worldcoin.org, respectivamente.

(ii) El señor Jannick Preiwisch actuando en calidad de apoderado, conforme el poder que allega como anexo, dio respuesta a las dos solicitudes mediante los oficios número 24-240075-05 y 24-240075-06 del 2 de julio de 2024.

TFH

WORLDCOIN
Contributor Company

VÍA CORREO ELECTRÓNICO
SOLICITAMOS CONFIDENCIALIDAD

2/07/ 2024

Dra.
Carolina García Molina
Directora de Investigaciones de Protección de Datos
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
Presentación en línea: contactenos@sic.gov.co

Referencia: Respuesta a requerimiento de información, Expediente No. 24-240075
Evento No.: 330

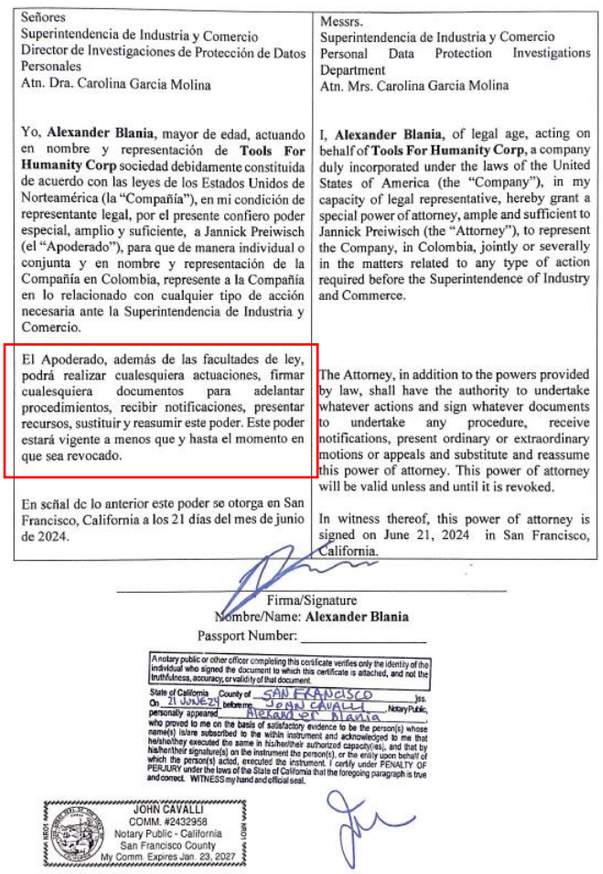
Estimada doctora García:

Quien suscribe, Jannick Preiwisch, identificado tal como figura después de mi firma, actuando en mi calidad de apoderado de TOOLS FOR HUMANITY CORPORATION ("TFH" o la "Sociedad"), conforme al poder adjunto a este documento (Anexos 1 y 2 con su respectiva traducción oficial), hago llegar la respuesta a la solicitud de información expedida por la Superintendencia de Industria y Comercio ("SIC") mediante el documento identificado con el número de expediente 24-240075, recibida el día 11 de junio. Por el presente, proporcionamos la información solicitada en apoyo a su trabajo y respondemos una a una sus preguntas detalladas en el Apéndice que encontrará a continuación.

El protocolo Wordlcoin es una infraestructura de código abierto de mejora de la privacidad concebida para Internet ("Worldcoin"). La esencia de Worldcoin es ser un pasaporte para Internet ("World ID"). Desde la perspectiva de la protección de datos, el punto clave es que

Imagen No. 1 Extraída del consecutivo 24-240075-05

A continuación, se relaciona el poder allegado como anexo en las citadas comunicaciones.



Señores
Superintendencia de Industria y Comercio
Director de Investigaciones de Protección de Datos Personales
Atn. Dra. Carolina García Molina

Yo, **Alexander Blania**, mayor de edad, actuando en nombre y representación de **Tools For Humanity Corp** sociedad debidamente constituida de acuerdo con las leyes de los Estados Unidos de Norteamérica (la "Compañía"), en mi condición de representante legal, por el presente confiero poder especial, amplio y suficiente, a Jannick Preiwisch (el "Apoderado"), para que de manera individual o conjunta y en nombre y representación de la Compañía en Colombia, represente a la Compañía en lo relacionado con cualquier tipo de acción necesaria ante la Superintendencia de Industria y Comercio.

El Apoderado, además de las facultades de ley, podrá realizar cualesquiera actuaciones, firmar cualesquiera documentos para adelantar procedimientos, recibir notificaciones, presentar recursos, sustituir y reasumir este poder. Este poder estará vigente a menos que y hasta el momento en que sea revocado.

En señal dc lo anterior este poder se otorga en San Francisco, California a los 21 días del mes de junio de 2024.

Messrs.
Superintendencia de Industria y Comercio
Personal Data Protection Investigations Department
Atn. Mrs. Carolina García Molina

I, **Alexander Blania**, of legal age, acting on behalf of **Tools For Humanity Corp**, a company duly incorporated under the laws of the United States of America (the "Company"), in my capacity of legal representative, hereby grant a special power of attorney, ample and sufficient to Jannick Preiwisch (the "Attorney"), to represent the Company, in Colombia, jointly or severally in the matters related to any type of action required before the Superintendence of Industry and Commerce.

The Attorney, in addition to the powers provided by law, shall have the authority to undertake whatever actions and sign whatever documents to undertake any procedure, receive notifications, present ordinary or extraordinary motions or appeals and substitute and reassume this power of attorney. This power of attorney will be valid unless and until it is revoked.

In witness thereof, this power of attorney is signed on June 21, 2024 in San Francisco, California.

Firma/Signature
Nombre/Name: **Alexander Blania**
Passport Number: _____

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

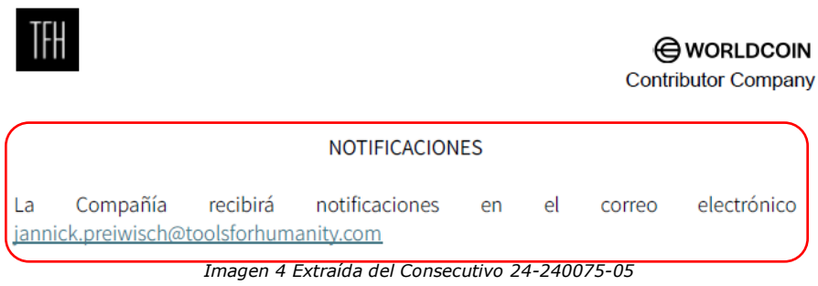
State of California County of SAN FRANCISCO
On 21 JUNE 24 before me JOHN CAVALLI, Notary Public,
personally appeared Alexander Blania
who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument. I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct. WITNESS my hand and official seal.

JOHN CAVALLI
COMM. #2432958
Notary Public - California
San Francisco County
My Comm. Expires Jan. 23, 2027

Imagen 2. Extraída del consecutivo 24-240075-05-09

Nótese que el apoderado fue autorizado para, entre otros, **recibir notificaciones respecto de la actuación administrativa que se adelanta** en esta Superintendencia.

Para tal efecto, en los escritos mediante los cuales se dio respuesta a los requerimientos antes mencionados, se informa que se recibirán las notificaciones en el correo electrónico jannick.preiwisch@toolsforhumanity.com.



TFH

WORLDCOIN
Contributor Company

NOTIFICACIONES

La Compañía recibirá notificaciones en el correo electrónico jannick.preiwisch@toolsforhumanity.com

Imagen 4 Extraída del Consecutivo 24-240075-05

Conforme lo establecido en el artículo 47 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, el acto administrativo que formula cargos deberá ser **notificado personalmente** a los interesados.

Por su parte el artículo 56 de la citada codificación dispone lo siguiente:

> ***ARTÍCULO 56. NOTIFICACIÓN ELECTRÓNICA.*** *<Artículo modificado por el artículo 10 de la Ley 2080 de 2021. El nuevo texto es el siguiente:> Las autoridades podrán notificar sus actos a través de medios electrónicos, siempre que el administrado haya aceptado este medio de notificación.*
>
> *Sin embargo, durante el desarrollo de la actuación el interesado podrá solicitar a la autoridad que las notificaciones sucesivas no se realicen por medios electrónicos, sino de conformidad con los otros medios previstos en el Capítulo Quinto del presente Título, a menos que el uso de medios electrónicos sea obligatorio en los términos del inciso tercero del artículo 53A del presente título.*
>
> *Las notificaciones por medios electrónicos se practicarán a través del servicio de notificaciones que ofrezca la sede electrónica de la autoridad.*

Los interesados podrán acceder a las notificaciones en el portal único del Estado, que funcionará como un portal de acceso.

La notificación quedará surtida a partir de la fecha y hora en que el administrado acceda a la misma, hecho que deberá ser certificado por la administración.

En concordancia con lo anterior, el artículo 67 también del CPACA, establece que las decisiones de la administración podrán ser notificadas a través de medios electrónicos.

Así las cosas, el trámite de notificación realizado por parte de esta Superintendencia respecto de la Resolución No. 46436 del 16 de agosto de 2024, se ajusta a los preceptos normativos antes mencionados, en la medida que (i) se autorizó que las notificaciones se surtieran de manera electrónica y (ii) se envió copia del acto administrativo a notificar.

En vista de lo anterior, y en la medida que la notificación de la resolución que formuló los cargos a WorldCoin Foundation y Tools For Humanity se realizó conforme las normas aplicables para el efecto, no existe irregularidad alguna que deba ser corregida por parte de este Despacho, en los términos del artículo 41 del CPACA[5].

Por otra parte, en lo que tiene que ver con el trámite de notificación establecido en la Ley 1073 de 2006, es necesario tener en cuenta que la naturaleza jurídica de la presente actuación es del orden **administrativo sancionatorio**, razón por la que, evidentemente no es posible su aplicación, por cuanto de acuerdo con lo establecido en el artículo 1 de la citada norma, **ésta sólo tiene aplicación para aquellos trámites o procesos de carácter civil o comercial.**

Ahora bien, respecto de la falta de notificación de la Resolución No. 46436 del 16 de agosto de 2024, alegada por los apoderados de WorldCoin Foundation y Tools For Humanity, llama la atención del Despacho que el mismo reclamo no se realizara respecto de la comunicación de la Resolución No. 58267 del 30 de septiembre de 2024 "Por medio de la cual se incorporaron pruebas y se corre traslado para alegar" y se hace esta observación en la medida que dicha comunicación se realizó también a los correos electrónicos dpo@worldcoin.org y jannick.preiswich@toolsforhumanity.com.

Y vencido el término de diez (10) días hábiles otorgado en el mismo, **los apoderados de Worldcoin Foundation y Tools For Humanity a través de los oficios Nos. 24-240075-46 y 24-240075-47 del 15 de octubre de 2024, presentaron los alegatos de conclusión correspondientes, pronunciándose respecto de cada uno de los cargos formulados en la Resolución No. 46436 del 16 de agosto de 2024 en contra de sus representadas.**

De lo anterior concluye el Despacho que, contrario a lo planteado por los apoderados, si tuvieron conocimiento desde un principio del contenido de la Resolución que formuló los cargos, pudiendo de esta manera presentar el escrito de descargos.

DECIMOSEGUNDO. Que mediante Oficios Nos. 24-240075-69 y 24-240075-70 del 11 de febrero de 2025, los apoderados de **WORLD FOUNDATION**[6] y **TOOLS FOR HUMANITY CORPORATION**, presentaron los alegatos de conclusión para lo cual tuvieron en cuenta los siguientes argumentos:

12.1. Afirman que en la presente actuación administrativa se violó el derecho al debido proceso de sus representadas, por las siguientes razones:

---

[5] "**ARTÍCULO 41. CORRECCIÓN DE IRREGULARIDADES EN LA ACTUACIÓN ADMINISTRATIVA.** La autoridad, en cualquier momento anterior a la expedición del acto, de oficio o a petición de parte, corregirá las irregularidades que se hayan presentado en la actuación administrativa para ajustarla a derecho, y adoptará las medidas necesarias para concluirla".

[6] De acuerdo con lo informado en el escrito de alegatos recientemente "Worldcoin Foundation" modificó su nombre comercial a "World Foundation".

a. La SIC no notificó en debida forma a las entidades de la resolución de cargos ni de las demás decisiones adoptadas en el presente trámite.

b. La SIC impidió a las entidades presentar descargos como lo exige la ley para efectuar una justa y adecuada defensa de sus intereses.

c. La Resolución de Cargos incumplió el deber de precisión y claridad sobre los hechos que la originaron y las disposiciones presuntamente vulneradas.

12.2. Sostienen que está probado que las Entidades han respetado las normas de protección de datos. Para sustentar este aspecto, los apoderados se pronuncian respecto de cada uno de los cargos formulados por el Despacho en la Resolución No. 46436 del 16 de agosto de 2024.

12.3. Solicitan que, para efectos de una improbable imposición de una sanción, la SIC deberá graduarla, en atención a los criterios aplicables consagrados en el artículo 24 de la Ley 1581 de 2012.

12.4. Se informa igualmente que Worldcoin Foundation modificó su nombre comercial a "World Foundation".

DECIMOTERCERO. Respecto de la violación al debido proceso de las Entidades.

Consideran los apoderados de World Foundation y Tools For Humanity Corporation que a lo largo de la presente actuación administrativa se ha vulnerado el debido proceso teniendo en cuenta que la SIC *"(i) no notificó en debida forma a las Entidades de las decisiones adoptadas en el presente trámite y aún no ha resuelto las solicitudes de nulidad por indebida notificación debidamente presentadas, (ii) no otorgó a las Entidades un periodo para presentar descargos como lo exige la ley para efectuar una justa y adecuada defensa de sus intereses, e (iii) incumplió con el deber de precisión y claridad en los hechos que originaron la actuación administrativa y las disposiciones presuntamente vulneradas".*

Notificación de la Resolución No. 46436 del 16 de agosto de 2024 y el término concedido para la presentación del escrito de descargos.

Los apoderados de World Foundation y Tools For Humanity Corporation, manifestaron lo siguiente:

> *"(…) a la fecha las Entidades no pueden considerarse válidamente notificadas de la Resolución de Cargos ni de ninguna las dichas determinaciones adoptadas por la SIC, pues estas no han sido notificadas conforme a las formas y procedimientos aplicables, indispensables para que las Entidades puedan ejercer su defensa y garantizar el debido proceso.*
>
> *Con motivo de lo anterior, y como primera actuación dentro de este trámite, el 11 de octubre de 2024 las Entidades presentaron sendos incidentes de nulidad por indebida notificación, solicitando que se declarara la nulidad de todo lo actuado a partir de la Resolución No. 46436 de 2024, inclusive.*
>
> *Sin embargo, los incidentes de nulidad antes presentados no han sido analizados, resueltos ni concedidos, pues la SIC continuó con el trámite, sin ajustar ni subsanar los errores cometidos en los procesos de notificación.*
>
> *En efecto, aunque posteriormente la Resolución No. 70363 de 2024 de fecha 19 de noviembre de 2024 menciona "Que este Despacho considera procedentes las solicitudes hechas por los apoderados de WORLDCOIN FOUNDATION y TOOLS FOR HUMANITY CORPORATION, y en aras de garantizar el derecho de defensa y de contradicción, ordenará la reapertura de la etapa probatoria dentro de la presente actuación administrativa…", la SIC omitió analizar y resolver los incidentes de nulidad por indebida notificación.*
>
> *(…)*
>
> *Además, la SIC indebidamente no otorgó a las Entidades la oportunidad de presentar descargos como lo exige la ley en este tipo de procedimientos, lo cual le ha impedido a las Entidades presentar una justa y adecuada defensa de sus intereses, y ha vulnerado su derecho al debido proceso.*
>
> *Primero, bajo el errado entendimiento de que las Entidades fueron notificadas "por correo electrónico" de la Resolución de Cargos el 23 de agosto de 2024, en la cual se habría concedido*

un término de 15 días para presentar descargos, mediante Resolución No. 58267 de 2024 la SIC determinó que dicho término habría vencido en silencio. Esto es equivocado, pues tal término nunca pudo considerarse otorgado, debido a que la resolución que lo otorgó no fue notificada en debida forma.

Como consecuencia de lo anterior, las Entidades investigadas por la SIC no tuvieron un término para presentar descargos dentro del presente procedimiento administrativo.

La oportunidad para presentar descargos es una etapa esencial del debido proceso administrativo, conforme al artículo 47 del CPACA, según el cual "Los investigados podrán, dentro de los quince (15) días siguientes a la notificación de la formulación de cargos, presentar los descargos y solicitar o aportar las pruebas que pretendan hacer valer". (Énfasis añadido)

Esta etapa no fue otorgada las Entidades, quienes a la fecha no han podido presentar descargos contra los cargos formulados.

Como se señaló, al declarar que el término para presentar descargos venció en silencio, cuando la resolución que lo concedió no fue debidamente notificada, la SIC transgredió directamente el derecho de defensa las Entidades, quienes por tal motivo no contaron con la oportunidad de presentar descargos.

Frente a la notificación de la Resolución No. 46436 del 16 de agosto de 2024, como se indicó en el aparte relacionado con la solicitud de corrección de irregularidades, ésta se realizó de manera electrónica de conformidad con lo establecido en el artículo 56 en concordancia con el artículo 67 del CPACA. Esto, teniendo en cuenta que en el poder otorgado en su momento al señor Jannick Preiswich en calidad de Oficial de Protección de datos se autorizó para recibir notificaciones al correo electrónico jannick.preiswich@toolsforhumanity.com

No comparte el Despacho lo manifestado por los apoderados de las investigadas cuando dicen que no pueden considerarse válidamente notificados dentro de la presente actuación administrativa, razón por la que no es posible ejercer en plena forma su derecho de defensa. Esto, por las siguientes razones:

- La Resolución No. 58267 del 30 de septiembre de 2024, que incorporó las pruebas y corrió traslado para alegar por el término de 10 días hábiles dentro de la presente actuación administrativa, fue comunicada a los mismos correos electrónicos a los cuales se notificó la Resolución No. 46436 del 16 de agosto de 2024.

- Frente a esta última actuación las investigadas a través de sus apoderados no sólo alegaron de conclusión[7] dentro del término de 10 días hábiles concedido, pronunciándose frente a cada uno de los cargos imputados por este Despacho, sino que además solicitaron la práctica de pruebas. Lo anterior, lleva a concluir que contrario a lo indicado, las investigadas conocieron el acto administrativo que formuló los cargos, por lo tanto, sabían el término legal para presentar el respectivo escrito de descargos.

- Con el fin de garantizar el debido proceso dentro de la actuación administrativa este Despacho a través de la Resolución No. 70363 del 19 de noviembre de 2024, ordenó la incorporación y práctica de las pruebas allegadas y solicitadas. Así mismo, se concedió nuevamente el término de 10 días hábiles para alegar de conclusión mediante los oficios 24-240075-67 y 24-240075-68 del 29 de enero de 2025.

- Mediante Oficio No. 24-240075-69 del 11 de febrero de 2025, las investigadas a través de sus apoderados presentaron alegatos de conclusión, pronunciándose nuevamente respecto de cada uno de los cargos formulados en la Resolución No. 46436 del 16 de agosto de 2024.

En consecuencia, y a pesar de que el trámite de la notificación de la Resolución que formuló los cargos se realizó conforme las normas establecidas para el efecto, no le asiste duda al Despacho que en el caso particular se perfeccionó la notificación por conducta concluyente en los términos establecidos en el artículo 72 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, el cual establece lo siguiente:

[7] Mediante Oficio No. 24-240075-46 del 15 de octubre de 2024 los apoderados de Worldcoin y Tools For Humanity presentaron alegatos de conclusión.

> *"**Artículo 72. Falta o irregularidad de las notificaciones y notificación por conducta concluyente, Sin el lleno de los anteriores requisitos no se tendrá por hecha la notificación, no producirá efectos legales la decisión, a menos que la parte interesada revele que conoce el acto**, consienta la decisión o interponga los recursos legales".*

Frente a la notificación por conducta concluyente, la doctrina[8] ha manifestado que:

> *"Cuando el particular conoce el acto administrativo que no se ha notificado o que se notificó irregularmente, prima este conocimiento sobre la falta o irregularidad de esta diligencia, de manera que el acto produce sus efectos a pesar de estos hechos. El conocimiento del acto por el particular se evidencia de una de res formas: porque esta revele que conoce el acto, porque consienta la decisión o porque interponga los recursos legales. Hay entonces notificación por conducta concluyente cuando se presenta una o varias de estas tres circunstancias".*

En línea con lo anterior, el Consejo de Estado indicó lo siguiente:

> *"Es de anotar que en el artículo 72[19]9 de la Ley 1437 de 2011, el legislador previó que sin el lleno de los requisitos no se tendrá por hecha la notificación, ni producirá efectos la decisión a menos que la parte interesada revele que conoce el acto, consienta la decisión o interponga los recursos legales. En este orden de ideas, la conducta concluyente es una modalidad igualmente válida de notificación de los actos administrativos y se erige en un mecanismo tendiente a subsanar las omisiones o irregularidades que se hayan presentado al intentar la comunicación por el mecanismo principal[20]10 esto es, el personal o cuando fracasó la notificación por aviso o por edicto".*

Así las cosas, en este punto de la discusión encuentra el Despacho que en la presente actuación administrativa se han respetado cada una de las garantías que constituyen el debido proceso.

DECIMOCUARTO. Competencia de la Superintendencia de Industria y Comercio.

El artículo 19 de la Ley 1581 de 2012, establece la función de vigilancia que le corresponde a la Superintendencia de Industria y Comercio para garantizar que en el tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la citada Ley.

Previo a referirnos sobre cada uno de los cargos formulados, este Despacho realizará una breve referencia al marco constitucional y legal

DECIMOQUINTO. Adecuación típica.

En relación con el principio de tipicidad en el derecho administrativo sancionatorio, la Corte Constitucional mediante sentencia C-748 de 2011[11], manifestó lo siguiente:

> *"En relación con el principio de tipicidad, encuentra la Sala que pese a la generalidad de la ley, es determinable la infracción administrativa en la medida en que se señala que la constituye **el incumplimiento de las disposiciones de la ley**, esto es, en términos específicos, la regulación que hacen los artículos 17 y 18 del proyecto de ley, en los que se señalan los deberes de los responsables y encargados del tratamiento del dato".*

Conforme lo anterior, corresponde a este Despacho establecer si las conductas investigadas en la presente actuación, dan lugar o no a la imposición de una sanción, para lo cual se deberán tener en cuenta las razones de hecho y de derecho aducidas por las investigadas en sus escritos de alegatos de conclusión, así como el conjunto de pruebas allegadas al expediente.

---

[8] ARBOLEDA PERDOMO, Enrique José. Comentario al Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Tercera Edición. Editorial Legis. 2021

[9] [19] ARTÍCULO 72. FALTA O IRREGULARIDAD DE LAS NOTIFICACIONES Y NOTIFICACIÓN POR CONDUCTA CONCLUYENTE. Sin el lleno de los anteriores requisitos no se tendrá por hecha la notificación, ni producirá efectos legales la decisión, a menos que la parte interesada revele que conoce el acto, consienta la decisión o interponga los recursos legales».

[10] [20] Consejo de Estado, Sección Tercera, C.P. Dr. Jaime Orlando Santofimio Gamboa, providencia de 9 de julio de 2014, radicado: 52001-23-31-000-2001-01115-01 (29.741).

[11] Corte Constitucional, Magistrado Ponente Jorge Ignacio Pretelt Chaljub.

15.1. Deber de adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la Ley 1581 de 2012.

El literal k) del artículo 17 de la Ley 1581 de 2012, establece lo siguiente:

> *"**ARTÍCULO 17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO.** Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:*
>
> *k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos";*

Por su parte, el artículo 2.2.2.25.3.1 del Decreto 1074 de 2015, estableció cuál es el contenido mínimo que debe contener el Manual de Políticas de la Información. Veamos:

> ***ARTÍCULO 2.2.2.25.3.1. Políticas de Tratamiento de la información.** Los responsables del tratamiento deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas.*
>
> *Las políticas de tratamiento de la información deberán constar en medio físico o electrónico, en un lenguaje claro y sencillo y ser puestas en conocimiento de los Titulares. Dichas políticas deberán incluir, por lo menos, la siguiente información:*
>
> *1. Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable.*
> *2. Tratamiento al cuál serán sometidos los datos y finalidad del mismo cuando esta no se haya informado mediante el aviso de privacidad.*
> *3. Derechos que le asisten cómo Titular.*
> *4. Persona o área responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización.*
> *5. Procedimiento para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.*
> *6. Fecha de entrada en vigencia de la política de tratamiento de la información y período de vigencia de la base de datos.*
> *Cualquier cambio sustancial en las políticas de tratamiento, en los términos descritos en el artículo 2.2.2.25.2.2. del presente Decreto deberá ser comunicado oportunamente a los titulares de los datos personales de una manera eficiente, antes de implementar las nuevas políticas.*

La Política de Tratamiento de Datos Personales define las pautas a través de las cuales el Responsable realiza el tratamiento de los datos personales recolectados. Esto con el fin de garantizar el pleno y efectivo ejercicio del derecho de Habeas Data del titular[12].

De conformidad con lo anteriormente indicado, este Despacho cuando formuló los cargos en la Resolución No. 46436 del 16 de agosto de 2024, verificó sí las políticas de tratamiento de la información publicadas por World Foundation y Tools For Humanity, cumplen con los requisitos mencionados. A continuación, se analizarán cada uno de ellos respecto de la Política de Tratamiento de la Información del sitio web https://es-es-worlcoin.org, Aviso de Privacidad World App – WorldCoin Wallet y Aviso de Privacidad de la Aplicación TFH y del Socio Operativo.

15.1.1. Respecto de la Política de Tratamiento de World Foundation. https://es-es-worlcoin.org

Se analizarán aquellos aspectos marcados como **NO** cumplidos, y sobre los cuales la apoderada de World Foundation se pronunció en su escrito de alegatos de conclusión:

[12] La Corte Constitucional en la sentencia C – 748 de 2011, respecto del derecho de Habeas Data, expresó: "(…) el reconocimiento del derecho al habeas data –identificado como un derecho fundamental autónomo tanto en el plano nacional como internacional- persigue la protección de los datos personales en un mundo globalizado en el que el poder informático es creciente. Esta protección responde a la importancia que tales datos revisten para la garantía de otros derechos como la intimidad, el buen nombre y el libre desarrollo de la personalidad. Sin embargo, el que exista una estrecha relación con tales derechos, no significa que no sea un derecho diferente, en tanto comprende una serie de garantías diferenciables y cuya protección es directamente reclamable por medio de la acción de tutela, sin prejuicio del principio de subsidiariedad que rige la procedencia de la acción".

	REQUISITOS LEGALES DE LAS POLÍTICAS DE TRATAMIENTO DE LA INFORMACIÓN		**COMENTARIO DIRECCIÓN RESOLUCIÓN No. 46436 del 16 de agosto de 2025**
a)	¿Utiliza un lenguaje claro y sencillo? (Art. 2.2.2.25.3.1 del Decreto 1074 de 2015).	No	La PTI no utiliza un lenguaje claro y sencillo.
b)	¿Contiene el nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable? (Artículo 2.2.2.25.3.1 del Decreto 1074 de 2015).	No	Únicamente se verifica una dirección, pero no es claro en indicar si se trata de su domicilio, no informa de manera clara un correo electrónico y tampoco un teléfono de contacto.
c)	¿Señala el tipo de Tratamiento –manual o automatizado- al cual serán sometidos los datos? (Núm. 2 del Artículo 2.2.2.25.3.1 del Decreto 1074 de 2015).	No	No informa de manera clara el tipo de tratamiento al cual serán sometidos los datos recopilados.
d)	¿Informa la finalidad del tratamiento de los datos? (núm. 2 del Artículo 2.2.2.25.3.1 Decreto 1074 de 2015).	No	La PTI informa los fines para los cuales son utilizados los datos recolectados, no obstante, no se indican cuáles son los datos que serán recolectados.
e)	¿Menciona de manera completa los derechos del Titular del dato? (Núm. 1 Artículo 2.2.2.25.3.1 Decreto 1074 de 2015 y art 8 Ley 1581 de 2012).	No	La PTI no menciona de manera completa los derechos del Titular del dato.
f)	¿Describe el procedimiento para que los Titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización? (Núm. 5 del Artículo 2.2.2.25.3.1 del Decreto 1074 de 2015, Artículos 2.2.2.25.3.6 y numeral 3 del artículo 2.2.2.25.6.2 de la misma norma.	No	La PTI no establece el procedimiento para que los Titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.
g)	¿Los anteriores canales prevén, por lo menos, la posibilidad de que el titular ejerza sus derechos a través del mismo medio por el cual fue recogida su información, dejando constancia de la recepción y trámite de la respectiva solicitud? (Art. 14 Ley 1581 del 2012).	No	
h)	¿Informa el período de vigencia de la base de datos? (Núm. 6, art 13 del Decreto 1377 de 2013 incorporado en el Artículo 2.2.2.25.3.1 Decreto 1074 de 2015).	No	La PTI no informa cuales son las bases de datos ni el período de vigencia de las mismas.

a) <u>La Política de Tratamiento de la Información, ¿Utiliza un lenguaje claro y sencillo? (Art. 2.2.2.25.3.1 del Decreto 1074 de 2015).</u>

"La SIC se limita a mencionar que el Aviso de Privacidad de WF no utiliza un lenguaje claro y sencillo, sin proporcionar una explicación detallada o argumento específico que justifique esta afirmación. Esta falta de claridad impide un ejercicio efectivo del derecho de defensa, dado que no es precisa la forma en que la SIC argumenta que el Aviso de Privacidad no es claro ni sencillo.

En todo caso, el Aviso de Privacidad de WF ha sido diseñado precisamente para facilitar la comprensión por parte de los titulares de los datos personales, utilizando un lenguaje accesible y un formato estructurado que fomenta la claridad y es sencillo:

El Aviso de Privacidad de WF se dirige al titular de los datos como "Usted", lo que genera un tono cercano y directo, evitando términos técnicos o ambiguos que puedan dificultar la interpretación del contenido.

El formato del Aviso de Privacidad de WF está dividido en preguntas frecuentes, tales como "¿Cómo utilizamos los datos personales que recopilamos?" o "¿Dónde tratamos sus datos?", simulando una conversación en la que la empresa responde de manera sencilla y detallada a las inquietudes más comunes que un titular de datos podría tener. Este enfoque conversacional está pensado específicamente para promover una lectura sencilla, amigable y comprensible.

El Aviso de Privacidad de WF cuenta con una tabla de contenido que permite a los usuarios navegar de manera sencilla por las distintas secciones del documento, asegurando que puedan encontrar fácilmente la información que les interesa.

Cada punto está detallado de manera precisa, explicando tanto el proceso de recolección y tratamiento de los datos como los derechos de los titulares, lo que garantiza que los usuarios tengan una visión completa y transparente".

Utilizar un lenguaje claro y sencillo no hace referencia únicamente a la manera cómo fue escrita la política de tratamiento de la información. El Responsable también debe tener en cuenta que la misma debe ser comprensible, es decir, que no exceda en términos técnicos o legales, que puedan llegar a confundir al titular. El fin último de las pautas publicadas es que se pueda saber exactamente cómo serán tratados sus datos personales.

b) ¿Contiene el nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable? (Artículo 2.2.2.25.3.1 del Decreto 1074 de 2015).

Respecto de este requisito manifestó la apoderada de World Foundation lo siguiente:

> *"La SIC se limita a mencionar que en el Aviso de Privacidad de WF únicamente se verifica una dirección, sin informar de manera clara un correo electrónico y tampoco un teléfono de contacto. Según la SIC, el Aviso de Privacidad de WF no es claro en indicar si esa dirección se trata del domicilio de WF.*
>
> *Sin embargo, la SIC no considera los siguientes apartados que cumplen con lo exigido por la norma de protección de datos personales en Colombia:*
>
> ***Nombre o razón social:** World Foundation. Esta información puede encontrarse en la introducción del Aviso de Privacidad de WF, cuando dice "Somos la World Foundation (…), el administrador detrás del desarrollo y crecimiento del protocolo World". Esta información queda evidente en la Sección 1 del Aviso de Privacidad de WF, "Responsable del tratamiento", cuando dice "Somos el Responsable del tratamiento de todos los Datos del Protocolo (…) y los Datos del Orb (…).*
>
> ***Domicilio:** Suite 3119, 9 Forum Lane, Camana Bay, PO Box 144, George Town, Grand Cayman KY1- 9006, Islas Caimán. Es claro que esa dirección es el domicilio de WF, dado que esta información puede encontrarse en la Sección 1 del Aviso de Privacidad de WF, "Responsable del tratamiento".*
>
> ***Dirección:** WF no cuenta con una dirección física en Colombia, por lo que el domicilio mencionado arriba cumple como dirección.*
>
> ***Correo electrónico:** En la Sección 4, el Aviso de Privacidad de WF dispone que el titular de los datos se puede comunicar a través de dpo@world.org. Ese correo electrónico permite la comunicación de los titulares de datos personales con WF, por lo que funge como el correo electrónico del responsable.*
>
> *Dado que WF no cuenta con un domicilio en Colombia, indicar un número de teléfono en el Aviso de Privacidad de WF es inoficioso. La comunicación a través de ese medio por parte de un titular residente en Colombia sería costosa. La indicación del Portal de Solicitudes y el correo electrónico cumplen el propósito de la norma de privacidad, que es garantizar el pleno y efectivo ejercicio del derecho de hábeas data".*
>
> *Debe mencionarse, en todo caso, que WF ofrece herramientas de autoservicio a través de la aplicación World App que permiten al usuario eliminar sus datos personales en cualquier momento. WF ofrece a los interesados formas fáciles de ejercer sus derechos de manera autónoma, entre ellas, la opción de suprimir sus datos en cualquier momento a través de la World App.*
>
> *Llamar a un número de teléfono de WF, entidad domiciliada en un país extranjero, además de ser costoso, implicaría entregar datos personales. Las posibilidades que ofrece WF son gratuitas y aseguran el principio de minimización de datos.*

Sobre este aspecto es indispensable especificar el nombre del Responsable del tratamiento de los datos personales que sean recolectados. Al verificar nuevamente la **Política de Tratamiento en su versión 3.12 del 12 de junio de 2024, encuentra el Despacho que en el numeral 1 "Responsable del tratamiento"**, no se indica de manera clara y expresa su nombre.

14/6/24, 14:51 WLD Production Legal Center

1. **Responsable del tratamiento**

Somos el Responsable del tratamiento de todos los Datos del Protocolo (definidos a continuación) y los Datos del Orb: Suite 3119, 9 Forum Lane, Camana Bay, PO Box 144, George Town, Grand Cayman KY1-9006, Islas Caimán. La Fundación tiene un único establecimiento en la Unión Europea ("**UE**").

"Datos del Protocolo" se refiere a todos los datos personales recopilados y tratados a través de su uso del protocolo de Worldcoin o los tokens de Worldcoin.

Imagen 5. Extraída de la Política de Tratamiento de Información de Worldcoin Foundation
Acta de Preservación No. 087 radicada en el consecutivo 24-240075-12

Si bien, es posible identificar la dirección de World Foundation, así como el correo electrónico para efectos de facilitar la comunicación entre su representada y los titulares, los mismos no son suficientes para garantizar que puedan ejercer sus derechos, el hecho que, por ejemplo, se considere que no es necesario informar un número telefónico porque se encuentra en el exterior y que podría ser costoso para el titular, no es excusa, en la medida que ese tipo de contacto debe ser gratuito para aquellos titulares que no tengan fácil acceso

a medios electrónicos y corresponde al responsable implementar mecanismos y herramientas que permitan dar cumplimiento a los requisitos mínimos de la política de tratamiento, como lo es en este caso, el teléfono de contacto del responsable garantizando el acceso a todos los titulares de los datos personales. Así mismo, las opciones de autoservicio que hace referencia la investigada no son suficientes para solicitar la eliminación de todos los datos personales del titular aportados a través de la aplicación y de la entrega del dato biométrico del iris.

c) ¿Señala el tipo de Tratamiento –manual o automatizado- al cual serán sometidos los datos? (Núm. 2 del Artículo 2.2.2.25.3.1 del Decreto 1074 de 2015).

> *"La SIC se limita a mencionar que el Aviso de Privacidad de WF no informa de manera clara el tratamiento al cual serán sometidos los datos recopilados, sin proporcionar una explicación detallada o argumento específico que justifique esta afirmación. Esta falta de claridad impide un ejercicio efectivo del derecho de defensa, dado que no es preciso el argumento de la SIC sobre que el Aviso de Privacidad no informa de manera clara el tratamiento al cual serán sometidos los datos recopilados.*
>
> *El numeral 2 del artículo 2.2.2.25.3.1. del Decreto 1074 de 2015 no exige que se mencione si el tratamiento es manual o automatizado en las políticas de tratamiento de información, sino que se refiere únicamente al tratamiento al cual serán sometidos los datos y la finalidad de este. Esto es lo suficientemente claro en el Aviso de Privacidad de WF.*
>
> *Según el Artículo 3 de la Ley 1581 de 2012, debe entenderse "Tratamiento" como cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. El Aviso de Privacidad de WF cuenta con secciones que describen la información que WF recopila (Sección 5), cómo utilizan los datos personales que recopilan (Sección 6), dónde tratan los datos del titular (Sección 7), cuándo comparten los datos del titular (Sección 8), cómo se registran los datos del titular en la cadena de bloques pública (Sección 9), cómo utilizan las cookies (Sección 10), y cuánto tiempo conservan los datos del titular (Sección 11). Cada una de estas secciones describe en detalle el Tratamiento de datos personales por parte de WF".*

La pregunta que realiza el Despacho hace referencia a la primera parte del requisito establecido en el numeral 2 del artículo 2.2.2.25.3.1 del Decreto 1074 de 2015, que se relaciona al tipo o manera en que serán tratados los datos personales, tal como se indica en la respectiva pregunta: manual o automatizado. Aspecto sobre el cual no existe claridad en la política estudiada.

No obstante, conforme a la descripción hecha por la apoderada de World Foundation, asume el Despacho que el tipo de tratamiento al cual serán sometidos los datos personales que sean recolectados en la página web analizada, es de carácter automatizado y no manual.

d) ¿Informa la finalidad del tratamiento de los datos? (núm. 2 del Artículo 2.2.2.25.3.1 Decreto 1074 de 2015).

Respecto de esta pregunta, indicó la apoderada de World Foundation manifestó:

> *"La SIC menciona que el Aviso de Privacidad de WF informa los fines para los cuales son utilizados los datos recolectados, pero no indica cuáles son los datos que serán recolectados. Sin embargo, hay una sección completa que se describe la información que WF recopila y las finalidades relacionadas (Sección 5).*
>
> *La Sección 5 divide la información que WF recopila en tres categorías principales: (i) los datos que el usuario proporciona, tales como los relacionados con el servicio de verificación de Proof of Personhood (PDP), que utiliza los datos del usuario para verificar su identidad única, (ii) los datos que recopilan de fuentes de terceros, tales como los datos de las cadenas de bloques para garantizar el cumplimiento de obligaciones legales, prevenir actividades ilegales en la plataforma, y analizar las tendencias de transacciones con fines de investigación y desarrollo, y (iii) los datos biométricos, que se recopilan después de que el titular acepta el formulario de consentimiento de datos". (…)*

Efectivamente, como lo señala la apoderada de World Foundation, la Sección 5 de la política de tratamiento informa los datos que son "recolectados". Sin embargo, no indica de manera específica a cuáles datos se está haciendo referencia, ni la finalidad especifica que se le dará a los mismos.

5.1 Datos que usted nos facilita

Es posible que tenga que facilitarnos ciertos datos para poder utilizar una función dentro de los Servicios. Dependiendo de la jurisdicción y la finalidad del tratamiento de los datos, la base jurídica para el tratamiento en los casos siguientes son el consentimiento del usuario, la ejecución de un contrato (nuestro compromiso de prestar los Servicios) y, en algunos casos, nuestro interés legítimo. A continuación encontrará una lista de los datos que puede facilitar y para qué podemos utilizarlos:

- **Servicio PDP**. El Servicio de verificación de Proof of Personhood (prueba de condición de persona) ("Servicio PDP") permite a otros desarrolladores aprovechar el protocolo de la World ID para verificar que sus usuarios son humanos únicos. Estos datos constituyen Datos del Protocolo.

5.2 Datos que recopilamos de fuentes de terceros

De cuando en vez, podemos obtener y analizar los datos públicos de la cadena de bloques para garantizar que las partes que utilizan nuestros Servicios no participan en actividades ilegales o prohibidas en virtud de las Condiciones del usuario, y para analizar las tendencias de las transacciones con fines de investigación y desarrollo. La base jurídica para el tratamiento de estos datos es el cumplimiento de las obligaciones legales. Estos datos constituyen Datos del Protocolo.

5.3 Datos biométricos

Solo recopilaremos y utilizaremos sus datos biométricos después de que usted acepte el **Formulario de consentimiento de datos**, que detalla los tipos de datos biométricos que tratamos y por qué lo hacemos. Los datos biométricos **no** están vinculados a los Datos del Protocolo.

Imagen 6. Extraída de la Política de Tratamiento de Información de Worldcoin Foundation
Acta de Preservación No. 087 radicada en el consecutivo 24-240075-12

e) ¿Menciona de manera completa los derechos del Titular del dato? (Núm. 1 Artículo 2.2.2.25.3.1 Decreto 1074 de 2015 y art 8 Ley 1581 de 2012).

Sostiene la apoderada de World Foundation lo siguiente:

> *"El Aviso de Privacidad de WF debe leerse en conjunto con el Portal de Solicitudes*[23][13] *referenciado en la Sección 4 sobre seguridad de los datos. Al seleccionar Colombia y darle clic a los tipos de solicitudes que se despliegan en el Portal de Solicitudes, se pueden encontrar los siguientes derechos: (i) solicitar la eliminación de los datos personales del titular, (ii) solicitar copia de los datos personales del titular, (iii) solicitar la actualización o rectificación de los datos personales del titular, (iv) solicitar los tipos de datos personales recolectados sobre el titular, (v) objetar el tratamiento de datos personales, y (vi) solicitar explicación sobre las prácticas de toma de decisiones automatizadas que utilizan datos personales".*

Encuentra el Despacho que para el momento en que se realizó la preservación de la página web https//es.es.worldcoin.org a través del Acta No. 087 del 8 de julio de 2024, la Sección 6 de la política de tratamiento de información que se revisa, menciona el portal de solicitudes worldcoin.org/requestportal, sin embargo, no existe claridad si en el mismo se enumeraran como lo indica la apoderada de World Foundation los derechos que tienen los titulares respecto del tratamiento de sus datos personales.

Ahora, conforme lo indicado en el escrito de alegatos, este Despacho ingreso al enlace proporcionado por la apoderada de Worldcoin relacionado con el portal de solicitudes, encontrando que, a pesar de seleccionar el idioma español en la página web, algunas de las preguntas se encuentran en idioma inglés.

Al desplegar el menú "Select Request Type", las opciones se encuentran igualmente en inglés, como puede verificarse a continuación:

[13] [23] Se puede acceder aquí: https://tfh-privacy.zendesk.com/hc/en-us/requests/new?ticket_form_id=32124980246035

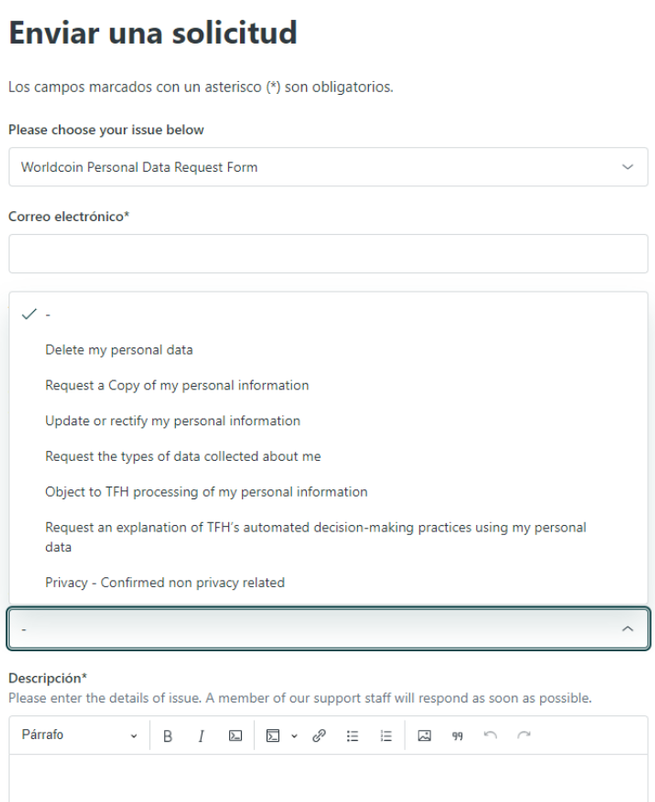


Imagen 7. Extradida del "portal de solicitudes" enlace https://tfh- privacy.zendesk.com/hc/en-us/requests/new?ticket_form_id=32124980246035

Conforme lo anterior, si bien existe un portal mediante el cual se puede presentar reclamos, considera el Despacho que al menos debería brindar la opción de que pueda desplegar el menú en idioma español, para que sea de total entendimiento de los titulares que entregan sus datos para que sean tratados por parte de World Foundation.

f) ¿Describe el procedimiento para que los Titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización? (Núm. 5 del Artículo 2.2.2.25.3.1 del Decreto 1074 de 2015, Artículos 2.2.2.25.3.6 y numeral 3 del artículo 2.2.2.25.6.2 de la misma norma.

Indicó la apoderada de World Foundation que,

> *"La Sección 13 del Aviso de Privacidad de WF dispone que para ejercer los derechos o ponerse en contacto con el Delegado de Protección de Datos ("DPD"), el titular puede enviar su solicitud a través del Portal de Solicitudes. El Aviso de Privacidad de WF, en la misma Sección 13, es claro en que responde a todas las solicitudes que reciben de personas que desean ejercer sus derechos de protección de datos de acuerdo con las normas de protección de datos aplicables.*
>
> *Para presentar una solicitud, el titular debe acceder al Portal de Solicitudes, completar los campos obligatorios (incluidos el asunto, la descripción y cualquier otra información pertinente), y enviar el formulario de manera que el equipo de asistencia se ponga en contacto lo antes posible".*

Como se dijo en el anterior ítem analizado, el portal de solicitudes al que hace referencia la apoderada de World Foundation, no se encuentra en idioma español, a pesar de haber escogido la preferencia en la parte inferior de la página, y de haber indicado como país de usuario "Colombia". Bajo estas condiciones, simplemente un titular no podrá ejercer sus derechos plenamente cuando existe una barrera que lo impide, como lo es el idioma.

Igualmente, el portal de solicitudes al que hace referencia la investigada no contempla el procedimiento que debe seguir un titular frente a las solicitudes de consultas o reclamos, por ejemplo, no se tiene certeza de la persona o área encargada de tramitar y dar respuesta oportuna. Es importante mencionar que lo manifestado por la investigada respecto a que "*el equipo de asistencia se ponga en contacto lo antes posible*", no se ajusta a los estándares establecidos en el régimen de protección de datos personales en Colombia, pues la ley

contempla los términos perentorios y las acciones que debe realizar el responsable del tratamiento de datos personales para atender las consultas y reclamos de los titulares, garantizando el ejercicio del derecho fundamental del habeas data.

g) ¿Los anteriores canales prevén, por lo menos, la posibilidad de que el titular ejerza sus derechos a través del mismo medio por el cual fue recogida su información, dejando constancia de la recepción y trámite de la respectiva solicitud? (Art. 14 Ley 1581 del 2012).

Frente al contenido de este requisito, la apoderada de World Foundation nuevamente hace referencia al portal de solicitudes implementado por su representada, y es a través de este canal que los titulares de la información pueden realizar las respectivas solicitudes o presentar los correspondientes reclamos.

No obstante, insiste el despacho que dicho portal no se adapta a las necesidades del titular colombiano, cuya lengua materna es el español. Por lo tanto, contrario a lo indicado en el escrito de alegatos, este requisito se cumple, pero de manera parcial, pues es necesario que se actualice y pueda ser consultado en idioma español y se dé cumplimiento a los requisitos mínimos que la normativa exige para la creación de las políticas de tratamiento.

h) ¿Informa el período de vigencia de la base de datos? (Núm. 6, art 13 del Decreto 1377 de 2013 incorporado en el Artículo 2.2.2.25.3.1 Decreto 1074 de 2015).

Afirma la apoderada de World Foundation lo siguiente:

> *"Al respecto, cabe mencionar que la Sección 5 divide la información que WF recopila en tres categorías/bases de datos principales: (i) los datos que el usuario proporciona, (ii) los datos que recopilan de fuentes de terceros, y (iii) los datos biométricos. Sobre la vigencia de las bases de datos, la Sección 11 dispone que WF conserva los datos durante el tiempo que sea razonablemente necesario para prestar los servicios, servir a legítimos fines comerciales, y cumplir con obligaciones legales y reglamentarias".*

Sobre este requisito es necesario que los Responsables de información indiquen de manera clara y precisa la vigencia que tendrá la base de datos. No indicarlo conllevaría a concluir que el tratamiento de la información no tiene un término definido en el tiempo.

En este orden de ideas, concluye el Despacho que la política de tratamiento de la información no se ajusta en su totalidad a las normas de protección de datos establecida para el territorio colombiano.

15.1.2. Aviso de Privacidad World App – Worldcoin Wallet.

Se analizarán aquellos aspectos marcados como **NO** cumplidos y parcialmente cumplidos y sobre los cuales la apoderada de World Foundation se pronunció en su escrito de alegatos de conclusión:

	REQUISITOS LEGALES DE LAS POLÍTICAS DE TRATAMIENTO DE LA INFORMACIÓN		**COMENTARIO**
a)	¿Utiliza un lenguaje claro y sencillo? (Art. 2.2.2.25.3.1 del Decreto 1074 de 2015).	No	La PTI **no** utiliza un lenguaje claro y sencillo.
b)	¿La PTI ha sido puesta en conocimiento de los titulares? (Artículo 2.2.2.25.3.1 del Decreto 1074 de 2015).	P	La PTI, si bien es accesible al público es necesario ingresar al Link Términos y Condiciones de Uso.
c)	¿Contiene el nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable? (Artículo 2.2.2.25.3.1 del Decreto 1074 de 2015).	No	Únicamente se verifica una dirección, pero no es claro en indicar si se trata de su domicilio, no informa de manera clara un correo electrónico y tampoco un teléfono de contacto.
d)	¿Señala el tipo de Tratamiento –manual o automatizado- al cual serán sometidos los datos? (Núm. 2 del Artículo 2.2.2.25.3.1 del Decreto 1074 de 2015).	No	No informa de manera clara el tipo de tratamiento al cual serán sometidos los datos recopilados.
e)	¿Informa la finalidad del tratamiento de los datos? (núm. 2 del Artículo 2.2.2.25.3.1 Decreto 1074 de 2015).	No	Al verificar el documento no es clara la finalidad del tratamiento de los datos personales.

f)	¿Menciona de manera completa los derechos del Titular del dato? (Núm. 1 Artículo 2.2.2.25.3.1 Decreto 1074 de 2015 y art 8 Ley 1581 de 2012).	P	La PTI menciona de manera parcial y condicionada sobre los derechos del Titular del dato.
g)	¿Describe el procedimiento para que los Titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización? (Núm. 5 del Artículo 2.2.2.25.3.1 del Decreto 1074 de 2015, Artículos 2.2.2.25.3.6 y numeral 3 del artículo 2.2.2.25.6.2 de la misma norma.	No	La PTI no establece el procedimiento para que los Titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización.
h)	Los anteriores canales prevén, por lo menos, la posibilidad de que el titular ejerza sus derechos a través del mismo medio por el cual fue recogida su información, dejando constancia de la recepción y trámite de la respectiva solicitud.? (Art. 14 Ley 1581 del 2012).	No	
i)	¿Informa el período de vigencia de la base de datos? (Núm. 6, art 13 del Decreto 1377 de 2013 incorporado en el Artículo 2.2.2.25.3.1 Decreto 1074 de 2015).	No	La PTI no informa cuales son las bases de datos ni el período de vigencia de las mismas.

a) La Política de Tratamiento de la Información, ¿Utiliza un lenguaje claro y sencillo? (Art. 2.2.2.25.3.1 del Decreto 1074 de 2015).

Frente al cumplimiento de este requisito, este Despacho reitera lo indicado cuando analizó su cumplimiento respecto de la Política de Tratamiento de la Información de World Foundation, en el numeral 15.1.1. (a)

b) ¿La PTI ha sido puesta en conocimiento de los titulares? (Artículo 2.2.2.25.3.1 del Decreto 1074 de 2015).

Respecto del cumplimiento de este requisito y teniendo en cuenta el Acta de Preservación No. 087 del 8 de julio de 2024, la política de tratamiento solo puede ser consultada accediendo al link de Términos y Condiciones de Uso.

c) ¿Contiene el nombre o razón social, domicilio, dirección, correo electrónico y teléfono del Responsable? (Artículo 2.2.2.25.3.1 del Decreto 1074 de 2015).

Sobre el cumplimiento de este requisito, el apoderado de Tools For Humanity Corporation, manifestó:

> *Sin embargo, la SIC no considera los siguientes apartados que cumplen con lo exigido por la norma de protección de datos personales en Colombia:*
>
> ***Nombre o razón social:*** *Tools for Humanity Corporation. Esta información puede encontrarse en la Sección 1 del Aviso de Privacidad de WF, "Responsable del tratamiento".*
>
> ***Domicilio:*** *548 Market Street, PMB 49951, San Francisco, CA 94104*
> *EE. UU. Es claro que esa dirección es el domicilio de TFH, dado que esta información puede encontrarse en la Sección 1 del Aviso de Privacidad de TFH, "Responsable del tratamiento".*
>
> ***Dirección:*** *TFH no cuenta con una dirección física en Colombia, por lo que el domicilio mencionado arriba cumple como dirección.*
> *Correo electrónico:*
>
> ***Versión 4.21 del 12 de junio de 2024:*** *Aun cuando las adendas son específicas para cada jurisdicción, hacen parte integral del Aviso de Privacidad de TFH. La sección E.1. de la Adenda E indica que el correo electrónico de TFH es dpo@toolsforhumanity.com. Ese correo electrónico es aplicable para todas las jurisdicciones, incluyendo Colombia. Este correo electrónico se menciona un total de tres veces en el Aviso de Privacidad de TFH, lo que permite que el titular lo pueda encontrar fácilmente.*
>
> *Versión 4.28 del 2 de diciembre del 2024: Para efectos de claridad y consistencia en el texto del Aviso de Privacidad de TFH, se incluye el correo electrónico dpo@toolsforhumanity.com en la Sección 13.*
>
> *Dado que TFH no cuenta con un domicilio en Colombia, indicar un número de teléfono en el Aviso de Privacidad de TFH es inoficioso. La comunicación a través de ese medio por parte de un titular residente en Colombia sería costosa. La indicación del Portal de Solicitudes (que se desarrolla abajo) y el correo electrónico cumplen el propósito de la norma de privacidad, que es garantizar el pleno y efectivo ejercicio del derecho de hábeas data.*

Es cierto que el correo electrónico dpo@toolsforhumanity.com se encuentra descrito en el numeral E1 de las adendas, específicamente la relacionada con Corea del Sur.

Respecto de las "Adendas", la política las definió de la siguiente manera:

> *"A continuación, varias adendas disponen información jurídicamente requerida para los mercados respectivos en los que desarrollamos nuestra actividad. Esta información forma parte del consentimiento dependiendo de la región en la que resida el interesado. Esta información puede diferir de la información de su ubicación porque determinadas jurisdicciones bloqueamos determinados servicios. En caso de cualquier incoherencia con lo anterior, prevalecerá la declaración más especial sobre la jurisdicción en particular.*

Conforme lo anterior, si bien es cierto que las adendas hacen parte de la política de tratamiento de Tools For Humanity Corporation, en el contexto presentado, sólo puede hacer referencia al país respecto del cual se menciona.

En este punto, vale la pena recordar que el fundamento que dio origen al análisis presentado en el acto administrativo que formuló cargos es la declaración de privacidad en su versión 4.21 efectiva a partir del 12 de junio de 2024.

Las actualizaciones que se hayan realizado con posterioridad reflejan que, a partir de la intervención de esta Superintendencia, se están realizando mejoras frente a la protección de datos personales.

Luego entonces, la Política de tratamiento de Tools For Humanity no cumplió con el citado requisito.

Finalmente, llama la atención de Despacho que en ninguna de las versiones de la política allegada por parte de los apoderados de World Foundation y Tools For Humanity Corporation, se contempla una adenda exclusiva para Colombia en la que se contemplen las mismas restricciones o prebendas indicadas para los otros países.

d) ¿Señala el tipo de Tratamiento –manual o automatizado- al cual serán sometidos los datos? (Núm. 2 del Artículo 2.2.2.25.3.1 del Decreto 1074 de 2015).

Sobre este aspecto, el Despacho reitera lo indicado sobre el cumplimiento del citado requisito cuando analizó la política de tratamiento de World Foundation.

e) ¿Informa la finalidad del tratamiento de los datos? (núm. 2 del Artículo 2.2.2.25.3.1 Decreto 1074 de 2015).

Manifestó el apoderado de Tools For Humanity Corporation lo siguiente:

> *"el Aviso de Privacidad de TFH informa de manera clara y sencilla las finalidades del tratamiento de los datos en la Sección 6, que se titula "¿Cómo utilizamos los datos que recopilamos?". Al respecto, el Aviso de Privacidad de TFH menciona que se utilizan los datos para, entre otros: (i) ofrecer y mantener los productos y servicios, (ii) permitir la publicación de información en una cadena de bloques y demostrar la singularidad del titular, (iii) mejorar y desarrollar productos y servicios, (iv) llevar a cabo investigaciones científicas de datos, (v) analizar el uso que el titular hace de los servicios, (vi) cumplir con las normas aplicables, (vii) gestionar solicitudes de servicio al cliente, quejas y consultas, (viii) resolver controversias, y (ix) ponerse en contacto con el titular en relación con actualizaciones de los servicios".*

Conforme lo indicado, si bien se enumeran una serie de finalidades, no se hace mención especial a la finalidad especifica de tratamiento en la captura del iris de los titulares y las acciones que realizará World Foundation y Tools For Humanity Corporation en todo el ciclo de vida del dato desde su recolección y hasta su destino final.

f) ¿Menciona de manera completa los derechos del Titular del dato? (Núm. 1 Artículo 2.2.2.25.3.1 Decreto 1074 de 2015 y art 8 Ley 1581 de 2012).

Afirma el apoderado de Tools For Humanity, lo siguiente:

> *El Aviso de Privacidad de TFH cuenta con una sección denominada "Sus derechos" (Sección 15 en la versión 4.21 y Sección 14 en la versión 4.28). Esta sección describe los derechos con los que cuenta el titular, e indica que son los siguientes: (i) obtener la información sobre los datos personales que tratan del titular, (ii) recibir los datos personales que le conciernen al titular, (iii) exigir que corrijan de inmediato los datos personales que le conciernen al titular si son incorrectos, (iv) exigir que eliminen los datos personales que le conciernen, (v) retirar libremente el consentimiento, y (vi) objetar el consentimiento.*
>
> *Los anteriores derechos se ajustan con los dispuestos por el Artículo 8 de la Ley 1581 de 2012. (…)*
>
> *En cualquier caso, el Aviso de Privacidad de TFH no limita ningún derecho de los titulares de datos. El titular cuenta con todos los derechos reconocidos por la regulación aplicable, y TFH procura garantizar el ejercicio de esos derechos.*

Establece el literal a) del artículo 4 de la Ley 1581 de 2012, *"el tratamiento a que se refiere la presente Ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen".*

Bajo esta premisa, los procedimientos y políticas que tenga implementados el Responsable frente al tratamiento de los datos personales recolectados, deben ceñirse a los presupuestos establecidos en la ya citada Ley 1581 de 2012.

El apoderado de Tools For Humanity realiza una comparación entre los "derechos", establecidos en la Sección 14 de la Política de Tratamiento de la Información, con aquellos establecidos en el artículo 8 de la Ley 1581 de 2012, con el fin de demostrar que los primeros, si bien no se describen al pie de la letra de la norma colombiana, se puede interpretar conforme su contenido que cumplen con la misma finalidad. Al respecto, es oportuno mencionar que la precitada ley señala claramente los derechos de los titulares de datos personales, los cuales no están contemplados en su integridad por parte de la investigada. Son normas positivas que no pueden ser interpretados y no puede pretender que el titular deduzca que sus derechos son respetados por el Responsable.

g) ¿Describe el procedimiento para que los Titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar y suprimir información y revocar la autorización? (Núm. 5 del Artículo 2.2.2.25.3.1 del Decreto 1074 de 2015, Artículos 2.2.2.25.3.6 y numeral 3 del artículo 2.2.2.25.6.2 de la misma norma.

Sobre este aspecto en particular, el apoderado de Tools For Humanity Corporation, manifestó en el escrito de alegatos de conclusión lo siguiente:

> *"La Sección 14 de la versión 4.21 (Sección 13 de la versión 4.28) del Aviso de Privacidad de TFH dispone que para ejercer los derechos o ponerse en contacto con el DPD, el titular puede enviar su solicitud a través del Portal de Solicitudes o al correo dpo@toolsforhumanity.com. El Aviso de Privacidad de TFH, en la misma Sección 14, es claro en que responde a todas las solicitudes que reciben de personas que desean ejercer sus derechos de protección de datos de acuerdo con las normas de protección de datos aplicables.*
>
> *Para presentar una solicitud, el titular debe acceder al Portal de Solicitudes, completar los campos obligatorios (incluidos el asunto, la descripción y cualquier otra información pertinente), y enviar el formulario de manera que el equipo de asistencia se ponga en contacto lo antes posible".*

Este Despacho a partir de lo indicado por parte del apoderado de Tools For Humanity Corporation, al verificar el portal de solicitudes, encuentra que se trata del mismo formulario relacionado en el literal e) del numeral 15.1.1 del presente acto administrativo este escrito, presentando igualmente las mismas falencias: a pesar de haber seleccionado el idioma español, algunas de sus preguntas se encuentran en idioma inglés tal y como puede ver en la imagen 7.

h) ¿Los anteriores canales prevén, por lo menos, la posibilidad de que el titular ejerza sus derechos a través del mismo medio por el cual fue recogida su información, dejando constancia de la recepción y trámite de la respectiva solicitud? (Art. 14 Ley 1581 del 2012).

Sobre este aspecto, el Despacho reitera lo indicado sobre el cumplimiento del citado requisito cuando analizó la política de tratamiento de World Foundation, en el literal g) del numeral 15.1.1. del presente acto administrativo.

i) ¿Informa el período de vigencia de la base de datos? (Núm. 6, art 13 del Decreto 1377 de 2013 incorporado en el Artículo 2.2.2.25.3.1 Decreto 1074 de 2015).

Indica el apoderado lo siguiente:

> *"Al respecto, cabe mencionar que la Sección 5 divide la información que TFH recopila en cuatro categorías/bases de datos principales: (i) los datos que el usuario proporciona, (ii) los datos que recopilan de fuentes de terceros, (iii) los datos que recopila de forma automática, y (iv) datos anonimizados y agregados. Sobre la vigencia de las bases de datos, la Sección 11 dispone que TFH conserva los datos durante el tiempo que sea razonablemente necesario para prestar los servicios, servir a legítimos fines comerciales, y cumplir con obligaciones legales y reglamentarias.*

Sobre este requisito el Despacho reitera lo indicado en el literal h) del numeral 15.1.1.

En este orden de ideas, concluye el Despacho que la política de tratamiento de la información no se ajusta en su totalidad a las normas de protección de datos establecida para el territorio colombiano.

15.1.3. Respecto de las "Adendas" incorporadas en las Políticas de Tratamiento de la información de World Foundation y Tools For Humanity Corporation.

El artículo 15 de la Constitución Política desarrolla dos premisas que orientan el ejercicio del derecho de habeas data. En primer lugar, otorga a las personas la potestad que tienen de conocer, actualizar y rectificar la información que pueda recolectarse sobre ellas en bases de datos o archivos en entidades públicas o privadas.

En segundo lugar, señala que las actividades relacionadas con la recolección, tratamiento y circulación de datos deben respetar, no sólo el principio de libertad, sino todas las garantías consagradas en la constitución.

Con el fin de desarrollar el derecho constitucional de habeas data, descrito en el artículo 15 de la Constitución antes citado, se expide la Ley 1581 de 2012.

El artículo 2 de la citada ley dispone:

> ***"ARTÍCULO 2o. ÁMBITO DE APLICACIÓN.*** *Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.*
>
> *La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al Responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales".*

El término "Tratamiento", definido por el literal g) del artículo 3 de la Ley 1581 de 2012, no solo se menciona en el artículo 15 de la Constitución Política, sino que, es determinante para establecer el campo de aplicación de la citada ley. Veamos:

> ***"Artículo 3. Definiciones.*** *Para los efectos de la presente ley, se entiende por:*
> (…)
> *g)* ***Tratamiento:*** *Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión."*

Así las cosas, la Ley Estatutaria 1581 de 2012 es aplicable, entre otras, cuando:

a) El Tratamiento lo realiza el Responsable o Encargado, domiciliados o no en territorio colombiano, que directa o indirectamente, a través de cualquier

medio o procedimiento, físico o electrónico, recolecta, usa, almacena o trata Datos personales en el territorio de la República de Colombia.

b) El Responsable o el Encargado no está domiciliado en la República de Colombia ni realiza Tratamiento de Datos dentro del territorio colombiano. Pero, existen normas o tratados internacionales que los obliga a cumplir la regulación colombiana.

La Corte Constitucional, por su parte, en relación con el ámbito de aplicación de ese artículo señaló en la Sentencia C-748 de 2011 lo siguiente:

> *"Para la Sala, esta disposición se ajusta a la Carta, pues amplía el ámbito de protección a algunos Tratamientos de datos personales que ocurren fuera del territorio nacional, en virtud del factor subjetivo. En un mundo globalizado en el que el flujo transfronterizo de datos es constante,* ***la aplicación extraterritorial de los estándares de protección es indispensable para garantizar la protección adecuada de los datos personales de los residentes en Colombia, pues muchos de los Tratamientos, en virtud de las nuevas tecnologías, ocurren precisamente fuera de las fronteras.*** *Por tanto, para la Sala se trata de una medida imperiosa para garantizar el derecho al habeas data".* (Subrayado fuera de texto).

Es necesario adicionalmente, tener en cuenta que, como se ha mencionado, el principio de legalidad en materia de protección de datos, se trata de una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen.

Conforme lo indicado, es dable concluir que cualquier persona natural o jurídica que realice tratamiento de datos personales en territorio Colombiano debe sujetarse a las normas establecidas para el efecto, cumpliendo igualmente con los deberes que conlleva dicha actividad.

Ahora, si bien World Foundation y Tools For Humanity Corporation cuentan con políticas de protección de la información, éstas no se ajustan del todo a lo establecido en la norma colombiana.

Como se advirtió en el acto administrativo que formuló los cargos, la Política de Tratamiento de la Información de World Foundation y Tools For Humanity Corporation, contienen una serie de "adendas", en las cuales se establece la manera cómo se aplicarán dichas políticas en los países que se relacionan en la misma.

Respecto de las adendas, en las Políticas analizadas se informa lo siguiente:

> *"A continuación, varias adendas disponen información jurídicamente requerida para los mercados respectivos en los que desarrollamos nuestra actividad. Esta información forma parte del consentimiento dependiendo de la región en la que resida el interesado. Esta información puede diferir de la información de su ubicación porque en determinadas jurisdicciones bloqueamos determinados servicios. En caso de cualquier incoherencia con lo anterior, prevalecerá la declaración más especial sobre la jurisdicción en particular".*

Es decir, determinadas cláusulas de las Políticas no son aplicadas en la Unión Europea, Reino Unido, Japón, Argentina, Singapur, Corea del Sur, California y Perú. Dependiendo de la jurisdicción o país las diferencias relacionadas con el tratamiento de datos personales son evidentes.

Worldcoin inició operaciones en Colombia sin haber ajustado sus políticas de tratamiento conforme el régimen de protección de datos personales establecido en la Ley 1581 de 2012 y sus normas reglamentarias, cuando está en la obligación de hacerlo teniendo en cuenta la actividad que realiza se centra en el tratamiento de datos personales sensibles.

15.1.4. Aviso de Privacidad de la Aplicación TFH y del Socio Operativo.

Frente al cumplimiento de los requisitos establecidos en el artículo 2.2.2.25.3.1 del Decreto 1074 de 2015, consideró el apoderado de Tools For Humanity, que el citado Aviso de Privacidad cumple con cada uno de ellos.

Al respecto es necesario indicar que, cuando se realizó la respectiva verificación por el Despacho al momento de la formulación los cargos, se evidenció que dicho aviso de privacidad no estaba redactado en idioma castellano[14], razón por la que es imposible determinar su efectivo cumplimiento.

15.2. Deber de solicitar y conservar, en las condiciones previstas en la Ley, copia de la respectiva autorización otorgada por el titular.

Respecto del cumplimiento de este deber, el Despacho abordará el análisis de los cargos segundo y tercero, relacionados con (i) la autorización previa, expresa e informada como cláusula general en el tratamiento de datos y (ii) la autorización correspondiente a los datos personales sensibles. Para lo cual, en primer lugar, se realizará una breve referencia respecto de la normatividad aplicable, los principios y deberes que la orientan.

15.2.1. Autorización previa, expresa e informada como cláusula general en el tratamiento de datos personales.

La Constitución Política de 1991, definió en el artículo 15 el derecho fundamental de Habeas Data en los siguientes términos:

> ***"ARTÍCULO 15.*** *Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo,* ***tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas****.*
>
> ***En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.***
>
> *La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.*

La Corte Constitucional, en la sentencia SU – 082 de 1995 estableció que el derecho de habeas se considera como un derecho autónomo, cuyo núcleo está compuesto por la autodeterminación informática y el principio de libertad. Adicionalmente comprende *a) El derecho a conocer las informaciones que a ella se refieren; || b) El derecho a actualizar tales informaciones, es decir, a ponerlas al día, agregándoles los hechos nuevos; || c) El derecho a rectificar las informaciones que no correspondan a la verdad.*

En el ámbito interno, la protección a los datos personales se materializa, principalmente, a través de las Leyes Estatutarias 1266 de 2008 y 1581 de 2012[15].

La Ley 1266 de 2008 tiene como propósito proteger los datos personales en materia financiera y crediticia. En este sentido, la Corte Constitucional señaló en la Sentencia C-1011 de 2008 lo siguiente:

> *"Como se expondrá en detalle en el apartado 1.1. del análisis material de la iniciativa, el Proyecto de Ley, considerado a partir de criterios sistemáticos, históricos y teleológicos, tiene por objeto particular establecer un sistema de reglas para la administración de datos personales relacionados con el comportamiento crediticio, excluyéndose otras materias, como es el caso del derecho a la información, el derecho a la intimidad y la regulación de otros escenarios del ejercicio del derecho al hábeas data, distinto al expuesto.*
>
> *(…)*
>
> *En efecto, en el apartado 1.1. del análisis material del Proyecto de Ley se demostró, a partir de argumentos de naturaleza sistemática, teleológica e histórica, que la iniciativa es una regulación del derecho al hábeas data con un carácter sectorial, en la medida en que los mecanismos concretos para la protección del derecho contenidos en el Proyecto respondían exclusivamente a la recopilación de datos personales de contenido financiero, comercial y crediticio, destinados al cálculo de riesgo crediticio. Dentro de ese análisis se dieron algunos ejemplos de cómo conceder carácter genérico al Proyecto, esto es,*

[14] **ARTICULO 10.** El castellano es el idioma oficial de Colombia. Las lenguas y dialectos de los grupos étnicos son también oficiales en sus territorios. La enseñanza que se imparta en las comunidades con tradiciones lingüísticas propias será bilingüe.

[15] Consejo de Estado, Sala de Consulta y Servicio Civil Radicación No. 11001-03-06-000-2020-00234-00 (2458) 6 de mayo de 2021.

> *extender sus reglas a todos los escenarios de administración de datos personales, llevaría a contrasentidos e, incluso, a vulneraciones de las normas constitucionales. Con base en lo anterior, se concluyó que el entendimiento acertado del Proyecto de Ley es el de un régimen particular y específico, dirigido a la fijación de reglas para la administración de datos personales financieros, comerciales y crediticios, con exclusión de otras modalidades de ejercicio del derecho al hábeas data. (Subrayas de la Sala).*

Ante el ámbito restringido de la Ley 1266 de 2008; y teniendo en cuenta el interés de que el país fuera considerado en la comunidad internacional como un país seguro en la protección de datos[16], y la necesidad de llenar el vacío jurídico existente en materia de protección de datos personales[17], fue promulgada la Ley Estatutaria 1581 de 2012.

La Ley 1581 de 2012 tiene como finalidad asegurar la protección efectiva de los datos personales, de tal manera que durante todo su tratamiento (recolección, almacenamiento, registro, uso o divulgación) se aseguren altos estándares de calidad en el manejo de la información. Con este propósito, establece una serie de límites para el uso y administración de los datos personales; impone responsabilidades y deberes respecto al tratamiento de los datos, y brinda a sus titulares herramientas para exigir su protección frente a cualquier vulneración. De esta suerte, la Ley 1581 de 2012 constituye el marco legal general para el tratamiento de los datos personales en nuestro país[18].

Una de las características más importantes de la Ley 1581 de 2012 es la incorporación de una serie de principios que contribuyen en la interpretación de sus disposiciones. Se trata de los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, los cuales, en palabras de la Corte Constitucional[19] definen el contexto axiológico dentro del cual debe moverse el proceso informático. Según este marco general, existen unos parámetros generales que deben ser respetados para poder afirmar que el proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo.

Para efectos del deber que se analiza, haremos referencia al principio de libertad establecido en el literal c) del artículo 4 de la ya citada Ley 1581 de 2012, establece:

> *c) **Principio de libertad:** El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento;*

La Corte Constitucional en la ya citada sentencia C – 748 de 2011, respecto del citado principio manifestó:

> *"Este principio, pilar fundamental de la administración de datos, permite al ciudadano elegir voluntariamente si su información personal puede ser utilizada o no en bases de datos. También impide que la información ya registrada de un usuario, la cual ha sido obtenida con su consentimiento, pueda pasar a otro organismo que la utilice con fines distintos para los que fue autorizado inicialmente.*

---

[16] Este proyecto incorpora en su articulado las mejores prácticas internacionales en materia de protección de datos contempladas en Convenio 108 de 1981 del Consejo de Europa, la Directiva Europea 95/46 de 1995, la Resolución 45/95 de 1990 de la ONU y la Resolución de Madrid de 2009, con el objetivo de lograr con esta ley la acreditación de Colombia por parte de la Unión Europea como un país seguro en protección de datos y así poder acceder al mercado europeo sin restricciones atrayendo inversión extrajera y generando nuevos empleos. Gaceta del Congreso núm. 488 del 4 de agosto de 2010.

[17] Este nuevo proyecto de ley busca llenar el vacío de estándares mínimos de protección de todos los datos personales –anunciado por la Corte Constitucional en la sentencia C-1011 de 2008, de ahí que su título sea precisamente "Por el cual se dictan disposiciones generales para la protección de datos personales". Esa intención también fue anunciada por el gobierno en la exposición de motivos, en la que afirmó: "(…) es necesario que el país cuente con una legislación integral y transversal que garantice la protección efectiva de los datos personales en todo el proceso de tratamiento". Corte Constitucional. Sentencia del 6 de octubre de 2011, C-748/11. Véase igualmente: Es importante señalar que este proyecto de ley complementa la Ley 1266 de 2008, que se refiere a un ámbito muy preciso de datos y responde a particulares necesidades de los usuarios del sector financiero que es necesario conservar. Este proyecto se encarga del universo de los demás datos personales que la Ley 1266 de 2008 no cobija. Gaceta del Congreso núm. 488 del 4 de agosto de 2010.

[18] El proyecto de ley pretende crear un marco legal general para el tratamiento de cualquier clase de dato personal, propone una visión transversal de los límites en el uso y administración de datos personales creando responsabilidades para quienes los reciban y administren describiendo quienes son los responsables del dato cuando el titular lo entrega y este es objeto de tratamiento. Gaceta del Congreso núm. 1023 del 2 de diciembre de 2010.

[19] C – 748 de 2011.

> *El literal c) del Proyecto de Ley Estatutaria no sólo desarrolla el objeto fundamental de la protección del habeas data, sino que se encuentra en íntima relación con otros derechos fundamentales como el de intimidad y el libre desarrollo de la personalidad. En efecto, el ser humano goza de la garantía de determinar qué datos quiere sean conocidos y tiene el derecho a determinar lo que podría denominarse su "imagen informática".*
>
> *(…)*
> *De todo lo anterior, puede entonces deducirse: (i) los datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo, expreso e informado del titular. Es decir, no está permitido el consentimiento tácito del Titular del dato y sólo podrá prescindirse de él por expreso mandato legal o por orden de autoridad judicial, (ii) el consentimiento que brinde la persona debe ser definido como una indicación específica e informada, libremente emitida, de su acuerdo con el procesamiento de sus datos personales. Por ello, el silencio del Titular nunca podría inferirse como autorización del uso de su información y (iii) el principio de libertad no sólo implica el consentimiento previo a la recolección del dato, sino que dentro de éste se entiende incluida la posibilidad de retirar el consentimiento y de limitar el plazo de su validez".*

De acuerdo con lo anterior, el Responsable debe asegurar el cumplimiento del citado principio al momento de recolectar la autorización del titular, de acuerdo con lo establecido en el literal b) del artículo 17 de la Ley 1581 de 2012, que dispone:

> *b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;*

El artículo 9 de la Ley 1581 de 2012, define la autorización en los siguientes términos:

> ***Artículo 9°. Autorización del Titular.*** *Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.*

La autorización que otorga el titular para el tratamiento de sus datos personales debe ser **previa**, **expresa** e **informada**. La Corte Constitucional, respecto de estas características, indicó:

> *"En relación con el **carácter previo**, la autorización debe ser suministrada, en una etapa anterior a la incorporación del dato. Así por ejemplo, en la Sentencia T-022 de 1993, se dijo que la veracidad del dato no implica que el Responsable del Tratamiento no tenga el deber de obtener una autorización anterior. En igual sentido, la Sentencia T-592 de 2003 dijo que el derecho al habeas data resulta afectado cuando los administradores de la información recogen y divulgan hábitos de pago sin el consentimiento de su titular. La Corte expresó que el consentimiento **previo** del titular de la información sobre el registro de sus datos económicos "en los procesos informáticos, aunado a la necesidad de que aquel cuente con oportunidades reales para ejercer sus facultades de rectificación y actualización durante las diversas etapas de dicho proceso, resultan esenciales para salvaguardar su derecho a la autodeterminación informática."*
>
> *En relación con el carácter **expreso**, la autorización debe ser inequívoca, razón por la cual, al contrario de lo sostenido por algunos intervinientes, no es posible aceptarse la existencia, dentro del ordenamiento jurídico colombiano, de un consentimiento tácito. Lo anterior, por varias razones:*
>
> ***En primer lugar**, la jurisprudencia constitucional ha exigido tal condición y ha dicho que el consentimiento debe ser **explícito y concreto a la finalidad específica de la base de datos**.*
>
> *(…)*
>
> *En segundo lugar, de una interpretación armónica de todo el articulado se deduce que el legislador estatutario tuvo una intención inequívoca que el consentimiento siempre fuese expreso. Así, desde el artículo 3 se dice que éste debe ser "previo, expreso e informado". Esto mismo se repite en el artículo 4. Posteriormente, el artículo 8 ordinal b), garantiza al Titular el derecho de solicitar prueba de la autorización, y señala que ésta sólo puede considerarse exceptuada en los casos consagrados en el artículo 10. El artículo 9 ordena que la autorización sea "obtenida por cualquier medio que pueda ser objeto de consulta posterior*
>
> *Por otro lado, el artículo 10 señala, en forma taxativa, los casos en que no se requiere autorización, y no hace referencia alguna a la existencia de un consentimiento tácito, lo cual necesitaría expresa autorización legal.*
>
> *(…)*
>
> *En relación con el carácter **informado**, el titular no sólo debe aceptar el Tratamiento del dato, sino también tiene que estar plenamente consciente de los efectos de su autorización. En este mismo sentido, en la Sentencia T-592 de 2003, la Corte señaló que la autorización debe ser cualificada y debía contener una explicación de los efectos de la misma. Además, a pesar de que se presente la autorización, el Responsable y Encargado del Tratamiento debe actuar de buena fe.*

De todo lo anterior, puede entonces deducirse: (i) los datos personales sólo pueden ser registrados y divulgados con el consentimiento libre, previo, expreso e informado del titular. Es decir, no está permitido el consentimiento tácito del Titular del dato y sólo podrá prescindirse de él por expreso mandato legal o por orden de autoridad judicial, (ii) el consentimiento que brinde la persona debe ser definido como una indicación específica e informada, libremente emitida, de su acuerdo con el procesamiento de sus datos personales. Por ello, el silencio del Titular nunca podría inferirse como autorización del uso de su información y (iii) el principio de libertad no sólo implica el consentimiento previo a la recolección del dato, sino que dentro de éste se entiende incluida la posibilidad de retirar el consentimiento y de limitar el plazo de su validez. (...)"[20]

No existe, por tanto, otra interpretación legal y constitucional diferente a que el consentimiento debe cumplir con los requisitos de ser previo, expreso e informado para que el mismo, pueda considerarse que se ajusta a los lineamientos establecidos en la Ley, pues, de lo contrario, se estaría afectando, como lo señaló la Corte en la sentencia arriba citada, el derecho a la autodeterminación informática entendido como el núcleo esencial del derecho al habeas data y, en la práctica, el Titular perdería el control de sus datos personales.

Las definiciones de expreso, previo e informado contienen elementos claves que se analizan a continuación, con el fin de que se asegure que sólo el consentimiento que se interprete conforme a la Ley 1581 de 2012 será considerado como tal.

Elementos del consentimiento:

1. **Expreso:** El término expreso significa la manifestación de voluntad libre del Titular para permitir el tratamiento de sus datos personales por parte de un tercero. Así mismo, esa necesidad de manifestación por parte de la persona impide que la falta de actuación - o quizás mejor, el comportamiento pasivo – constituya un consentimiento válido bajo la Ley 1581 de 2012, pues, como lo señaló la Corte Constitucional en la Sentencia C-748 de 2011, "*no es posible aceptarse la existencia, dentro del ordenamiento jurídico colombiano, de un consentimiento tácito*". Así sucede, por ejemplo, con formularios de recolección de datos en línea que no cuentan con casillas de aceptación. Esta situación obliga a los Responsables del Tratamiento a crear procedimientos para garantizar que las personas otorguen su consentimiento y, a su vez, proporcionan pruebas al Responsable del Tratamiento de que se ha obtenido el consentimiento. Los ejemplos más clásicos son la firma manuscrita en la parte inferior de un formulario de papel y la selección de una casilla en un sitio web en Internet.

   El requisito de expreso para los datos sensibles se sustituye por un "consentimiento explícito", pues para este tipo de datos se considera adecuado que exista un elevado nivel de control sobre los datos personales por parte de su Titular.

2. **Informado:** El término informado significa que la persona debe conocer las finalidades específicas del tratamiento de sus datos, la persona natural o jurídica, pública o privada, que decidirá sobre el tratamiento de los datos concernidos, los derechos relativos al tratamiento de sus datos, así como del modo de hacer valer sus derechos en relación con el tratamiento y, en general, las condiciones en que se efectuarán las actividades de tratamiento de datos personales.

   En ese sentido, el artículo 12 de la Ley 1581 de 2012 establece que cuando se va a solicitar la autorización al Titular de la Información, el Responsable del tratamiento deberá informarle de manera clara y expresa lo siguiente: a) el tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo; b) el carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes; c) los derechos que le asisten como

[20] Cfr. Corte Constitucional, sentencia C 748 del 2011.

titular; y, d) la identificación, dirección física o electrónica y teléfono del responsable del tratamiento.

Si se trata de datos sensibles el Responsable del tratamiento también debe cumplir lo que ordena el artículo 2.2.2.25.2.3 del Decreto 1074 de 2015, a saber:

> *"Artículo 2.2.2.25.2.3. De la autorización para el Tratamiento de datos personales sensibles. El Tratamiento de los datos sensibles a que se refiere el artículo 5 de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6 de la citada ley.*
>
> *En el Tratamiento de datos personales sensibles, cuando dicho Tratamiento sea posible conforme a lo establecido en el artículo 6 de la Ley 1581 de 2012, deberán cumplirse las siguientes obligaciones:*
>
> *1. Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.*
>
> *2. Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.*
>
> *Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles".*

3. **Previo:** El término previo significa que la persona debe otorgar su consentimiento antes del comienzo del tratamiento de su información personal, debiendo cumplirse a más tardar en el momento en que el dato va a ser recogido, sin que sea admisible, en este punto, considerar su acatamiento con posterioridad a su recolección, pues sólo así quedaría garantizado el derecho de la persona a tener una apropiada información antes de otorgar su consentimiento. En este sentido, el artículo 2.2.2.25.2.2., del Decreto 1074 de 2015 establece lo siguiente:

> *"Artículo 2.2.2.25.2.2. Autorización. El Responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento. (…)".*

Visto lo anterior, el consentimiento, como uno de los fundamentos jurídicos del tratamiento de datos personales, para que sea válido bajo la Ley 1581 de 2012, debe cumplir los siguientes requerimientos legales:

a) El consentimiento debe ser expreso. El Titular debe realizar alguna acción positiva que indique su consentimiento y debe tener la libertad de no consentir.

b) El consentimiento debe estar informado. El artículo 12 de la Ley 1581 de 2012 enumera la información que debe suministrársele al Titular; esa información debe ser claramente visible, destacada y completa. No basta con ponerla a disposición en algún sitio de la página web, sin que la persona no la conozca.

c) El consentimiento debe ser previo. La obtención del consentimiento debe ser previa a la recolección de los datos.

Conforme las citadas características el consentimiento que otorga el titular debe responder únicamente a su propia voluntad y no a la entrega de cualquier tipo de contraprestación que pueda condicionarlo.

A continuación, teniendo en cuenta el análisis normativo y jurisprudencial que precede, este Despacho se pronunciará respecto de los formularios que fueran analizados por parte del GTIFSD a través del Acta No. 087 del 8 de julio de 2024, respecto de la página web World – https://es-es.worldcoin.org/. Se analizará si las investigadas a través de los citados formularios cumplen con la normatividad

relacionada con la autorización previa, expresa e informada que debe otorgar el titular del dato.

En la citada página se encontraron, entre otros, los siguientes formularios en los cuales se evidencia un eventual tratamiento de datos personales, como se relaciona a continuación:

a) "**Conviértete en Operador de Orb**", el cual se despliega al ingresar al link "Operador de Orb" ubicacado en su momento en la parte inferior de la página https://es-es.worldcoin.org/

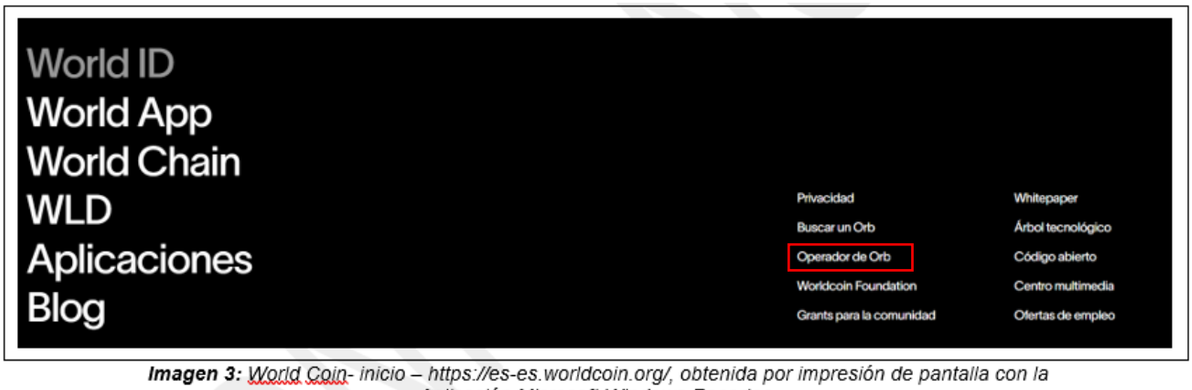
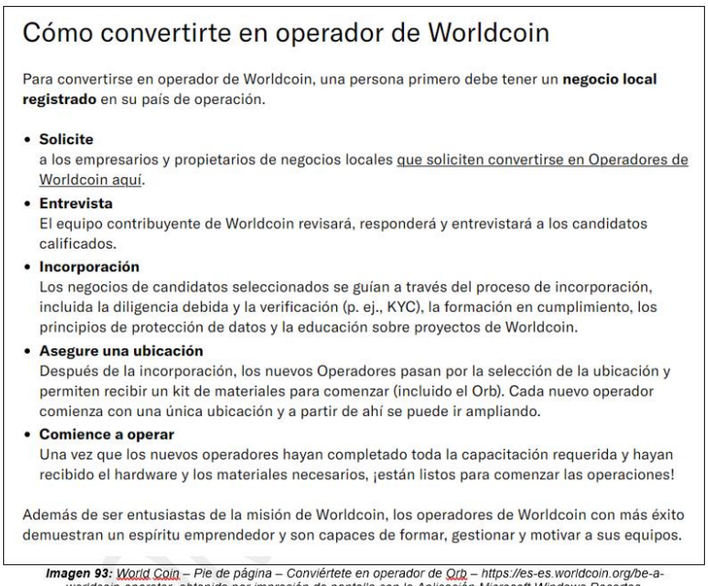


Imagen 3: *World Coin- inicio – https://es-es.worldcoin.org/, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*



Cómo convertirte en operador de Worldcoin

Para convertirse en operador de Worldcoin, una persona primero debe tener un **negocio local registrado** en su país de operación.

- **Solicite**
  a los empresarios y propietarios de negocios locales que soliciten convertirse en Operadores de Worldcoin aquí.
- **Entrevista**
  El equipo contribuyente de Worldcoin revisará, responderá y entrevistará a los candidatos calificados.
- **Incorporación**
  Los negocios de candidatos seleccionados se guían a través del proceso de incorporación, incluida la diligencia debida y la verificación (p. ej., KYC), la formación en cumplimiento, los principios de protección de datos y la educación sobre proyectos de Worldcoin.
- **Asegure una ubicación**
  Después de la incorporación, los nuevos Operadores pasan por la selección de la ubicación y permiten recibir un kit de materiales para comenzar (incluido el Orb). Cada nuevo operador comienza con una única ubicación y a partir de ahí se puede ir ampliando.
- **Comience a operar**
  Una vez que los nuevos operadores hayan completado toda la capacitación requerida y hayan recibido el hardware y los materiales necesarios, ¡están listos para comenzar las operaciones!

Además de ser entusiastas de la misión de Worldcoin, los operadores de Worldcoin con más éxito demuestran un espíritu emprendedor y son capaces de formar, gestionar y motivar a sus equipos.

Imagen 93: *World Coin – Pie de página – Conviértete en operador de Orb – https://es-es.worldcoin.org/be-a-worldcoin-operator, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

Al dar clic en el enlace "*Presentar Solicitud*", la página dirige al enlace "*https://orbapp.worldcoin.org/auth?callbackUrl=%2Fdashboard*", en este se encuentra un módulo nombrado "*Welcome to the Orb App*", como se puede ver a continuación:

Conviértete en operador de Orb

Por un enfoque más humano para dar la bienvenida a todos al protocolo Worldcoin.

Presentar solicitud →

Imagen 94: *World Coin – Pie de página – Conviértete en operador de Orb – https://es-es.worldcoin.org/be-a-worldcoin-operator, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

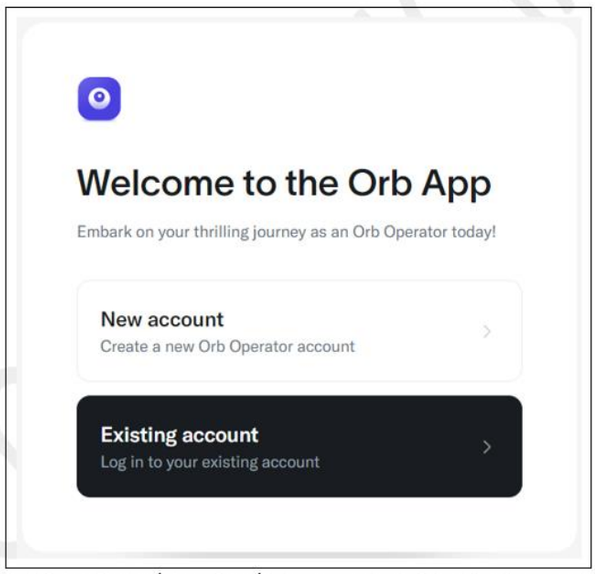


Imagen 95: *World Coin – Pie de página – Conviértete en operador de Orb – https://es-es.worldcoin.org/be-a-worldcoin-operator, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

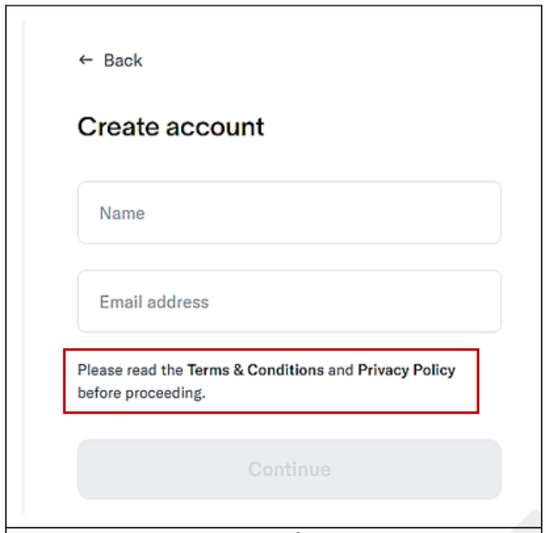


Imagen 96: *World Coin – Conviértete en operador de Orb – https://es-es.worldcoin.org/be-a-worldcoin-operator, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

Al momento de ingresar los datos de "nombre" y "correo electrónico", para continuar con el proceso se solicita la lectura de los Términos y Condiciones y la Política de Privacidad. Al seguir con el trámite correspondiente, solicita el formulario establecer una contraseña:

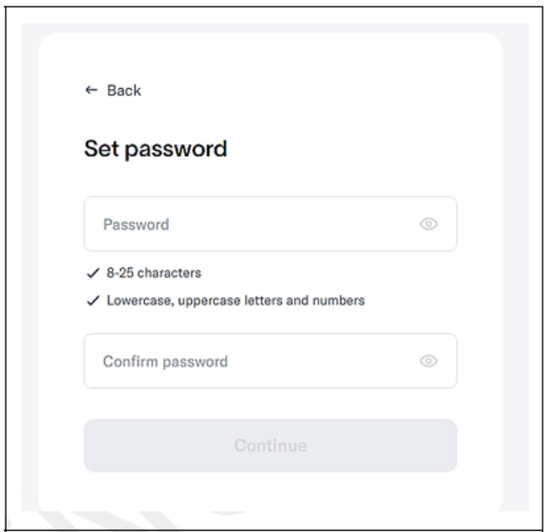


Imagen 97: *World Coin – Conviértete en operador de Orb – https://es-es.worldcoin.org/be-a-worldcoin-operator, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

Posterior a la inclusión de la contraseña, la cuenta es creada, e informa finalmente la posibilidad de seleccionar el idioma. Sobre este punto en particular, llama la atención que el formulario únicamente puede ser consultado en idioma Inglés:

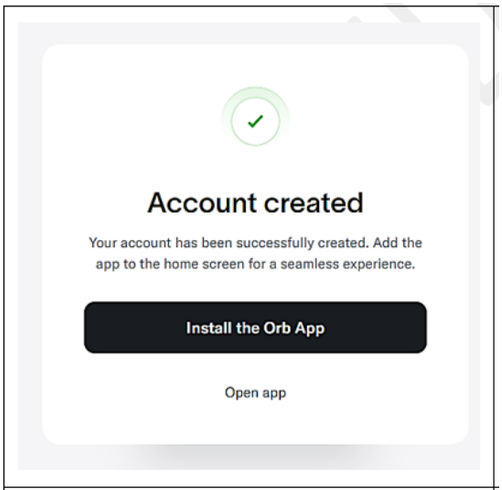


Imagen 98: *World Coin – Conviértete en operador de Orb – https://es-es.worldcoin.org/be-a-worldcoin-operator, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

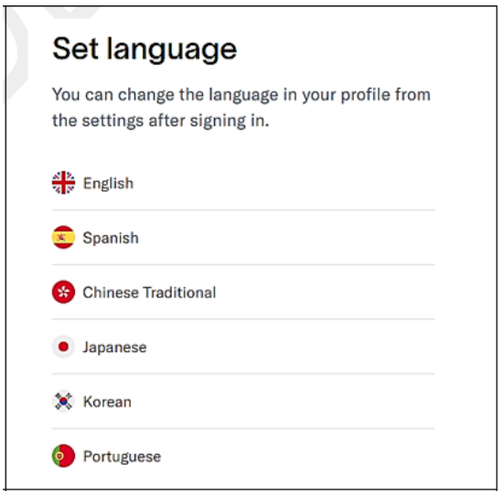
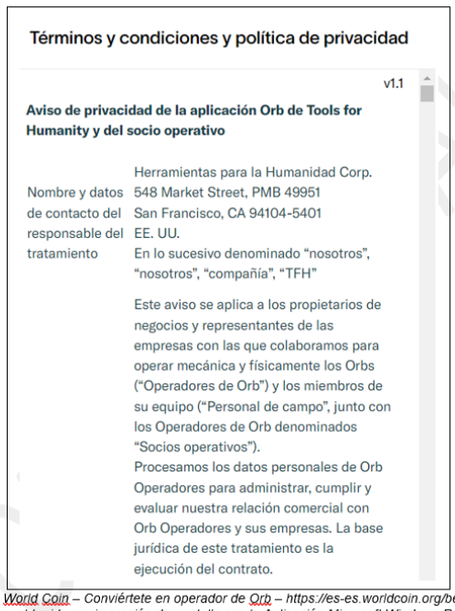


Imagen 99: *World Coin – Conviértete en operador de Orb – https://es-es.worldcoin.org/be-a-worldcoin-operator, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

Al seleccionar el idioma en el que se quiere usar la aplicación, se muestra un documento titulado "Terms & Conditions & Privacy Policy", como se puede ver a continuación:

ESPACIO EN BLANCO



Términos y condiciones y política de privacidad

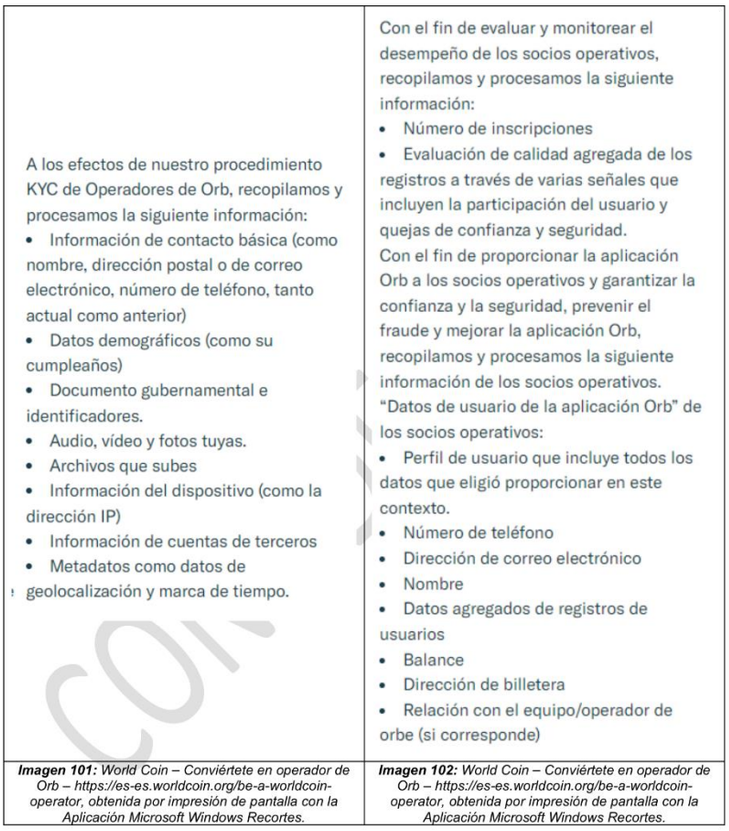
v1.1

Aviso de privacidad de la aplicación Orb de Tools for Humanity y del socio operativo

Nombre y datos de contacto del responsable del tratamiento	Herramientas para la Humanidad Corp. 548 Market Street, PMB 49951 San Francisco, CA 94104-5401 EE. UU. En lo sucesivo denominado "nosotros", "nosotros", "compañía", "TFH"
	Este aviso se aplica a los propietarios de negocios y representantes de las empresas con las que colaboramos para operar mecánica y físicamente los Orbs ("Operadores de Orb") y los miembros de su equipo ("Personal de campo", junto con los Operadores de Orb denominados "Socios operativos"). Procesamos los datos personales de Orb Operadores para administrar, cumplir y evaluar nuestra relación comercial con Orb Operadores y sus empresas. La base jurídica de este tratamiento es la ejecución del contrato.

Imagen 100: *World Coin – Conviértete en operador de Orb – https://es-es.worldcoin.org/be-a-worldcoin-operator, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

En este documento se encuentra que los datos personales que se recopila son los siguientes:



A los efectos de nuestro procedimiento KYC de Operadores de Orb, recopilamos y procesamos la siguiente información:

- Información de contacto básica (como nombre, dirección postal o de correo electrónico, número de teléfono, tanto actual como anterior)
- Datos demográficos (como su cumpleaños)
- Documento gubernamental e identificadores.
- Audio, vídeo y fotos tuyas.
- Archivos que subes
- Información del dispositivo (como la dirección IP)
- Información de cuentas de terceros
- Metadatos como datos de geolocalización y marca de tiempo.

Imagen 101: *World Coin – Conviértete en operador de Orb – https://es-es.worldcoin.org/be-a-worldcoin-operator, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

Con el fin de evaluar y monitorear el desempeño de los socios operativos, recopilamos y procesamos la siguiente información:

- Número de inscripciones
- Evaluación de calidad agregada de los registros a través de varias señales que incluyen la participación del usuario y quejas de confianza y seguridad.

Con el fin de proporcionar la aplicación Orb a los socios operativos y garantizar la confianza y la seguridad, prevenir el fraude y mejorar la aplicación Orb, recopilamos y procesamos la siguiente información de los socios operativos.

"Datos de usuario de la aplicación Orb" de los socios operativos:

- Perfil de usuario que incluye todos los datos que eligió proporcionar en este contexto.
- Número de teléfono
- Dirección de correo electrónico
- Nombre
- Datos agregados de registros de usuarios
- Balance
- Dirección de billetera
- Relación con el equipo/operador de orbe (si corresponde)

Imagen 102: *World Coin – Conviértete en operador de Orb – https://es-es.worldcoin.org/be-a-worldcoin-operator, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

Una vez se crea la cuenta al acceder se encuentran dos opciones, como se puede ver a continuación:

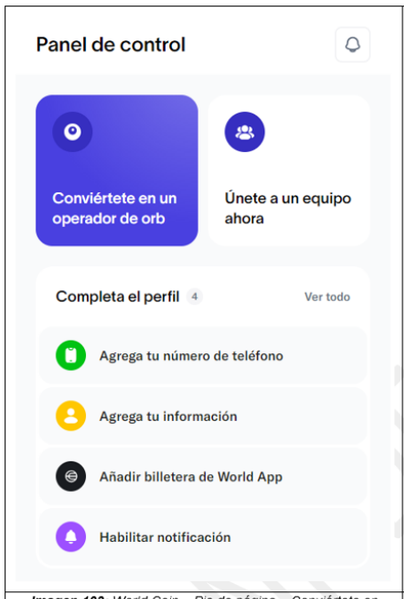


Imagen 103: *World Coin – Pie de página – Conviértete en operador de Orb – https://es-es.worldcoin.org/be-a-worldcoin-operator, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

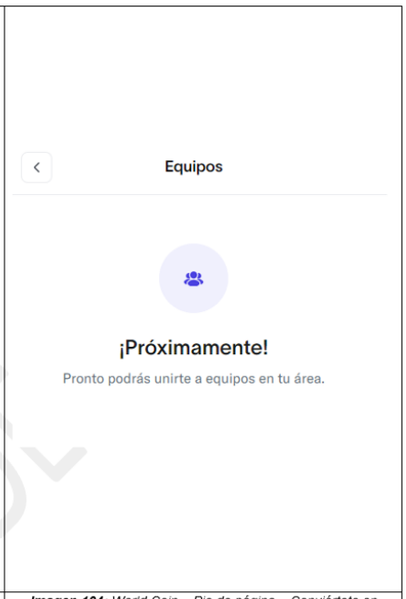


Imagen 104: *World Coin – Pie de página – Conviértete en operador de Orb – https://es-es.worldcoin.org/be-a-worldcoin-operator, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

Este Despacho, al verificar el Aviso de Privacidad de la aplicación TFH Orb y del socio operativo, en su versión 1.1. vigente a partir del 6 de febrero de 2024, evidenció que no se encuentra en idioma castellano, tal y como se indicó en el aparte correspondiente.

El formulario no ofrece la posibilidad de ser "aceptado" o un chequeo mediante el cual el titular de los datos autorice de manera previa, expresa e informada, el tratamiento de sus datos, de acuerdo a la finalidad especifica que el responsable del tratamiento pretenda realizar.

Ahora bien, el mismo formulario fue revisado por el GTIFSD cuando realizó la segunda preservación de la página World - https://world.org/es-es cuyos resultados fueron incluidos en el Acta No. 214 del 16 de diciembre de 2024. Y de la cual se destaca el siguiente procedimiento:

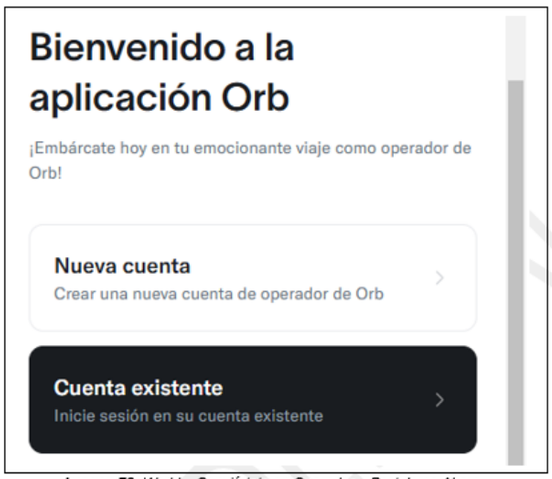


Imagen 78: *World – Conviértete en Operador – Postularse Ahora – https://orbapp.worldcoin.org/auth?callbackUrl=%2Fdashboard%3F_gl%3D1*1nbpxjx*_gcl_au*MTMzNDQ4OTUxNi4xNzMzMzI2NDMz, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

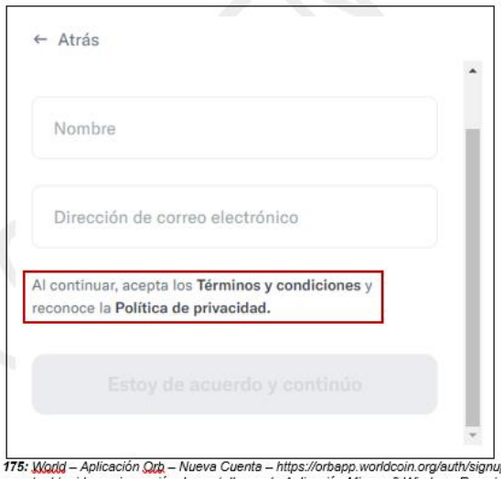
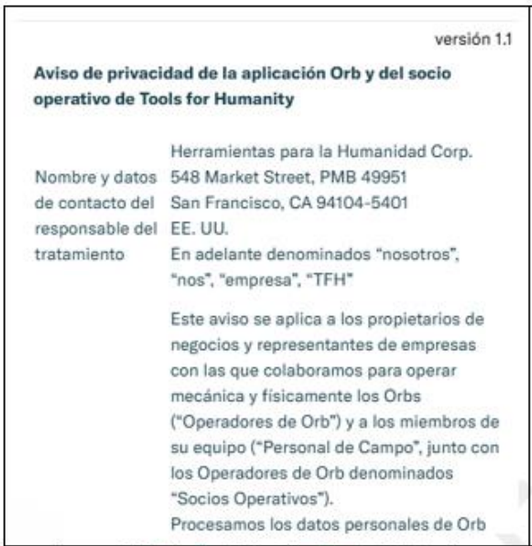


Imagen 175: *World – Aplicación Orb – Nueva Cuenta – https://orbapp.worldcoin.org/auth/signup/create-account, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

La opción "Al continuar, acepta los Términos y Condiciones y reconoce la Política de Privacidad", no estaba dispuesto en el anterior formulario.

Una vez creada la cuenta, al iniciar la sesión se solicita aceptar el "Aviso de Privacidad de la aplicación Orb y del socio operativo de Tools for Humanity" y el Aviso de Privacidad, como se puede observar a continuación:


versión 1.1

Aviso de privacidad de la aplicación Orb y del socio operativo de Tools for Humanity

Nombre y datos de contacto del responsable del tratamiento	Herramientas para la Humanidad Corp. 548 Market Street, PMB 49951 San Francisco, CA 94104-5401 EE. UU. En adelante denominados "nosotros", "nos", "empresa", "TFH"

Este aviso se aplica a los propietarios de negocios y representantes de empresas con las que colaboramos para operar mecánica y físicamente los Orbs ("Operadores de Orb") y a los miembros de su equipo ("Personal de Campo", junto con los Operadores de Orb denominados "Socios Operativos").
Procesamos los datos personales de Orb

Imagen 180: *World – Aplicación Orb – Iniciar Sesión – https://orbapp.worldcoin.org/auth/signin, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*


versión 1.0

Condiciones de uso del operador de Tools For Humanity

¡Bienvenido a la comunidad Worldcoin! *Worldcoin es un protocolo de código abierto respaldado por una comunidad global de desarrolladores, individuos y otros colaboradores. Tools for Humanity es una empresa global de desarrollo de software y hardware que crea las herramientas para llevar tecnologías y productos de blockchain e identidad digital a miles de millones de personas, incluso contribuyendo al desarrollo y crecimiento del ecosistema Worldcoin.*

Estos Términos entre usted y Tools for Humanity Corporation, una corporación de Delaware (colectivamente con nuestras afiliadas, "TFH", "nosotros" o "nos") rigen su uso y acceso a nuestros sitios web y aplicaciones, incluida World App y la aplicación Operator (colectivamente, las "Aplicaciones"), y toda la funcionalidad, el contenido y los servicios asociados que le brindamos (colectivamente, los

Imagen 181: *World – Aplicación Orb – Iniciar Sesión – https://orbapp.worldcoin.org/auth/signin, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

Imagen 182: *World – Aplicación Orb – Nueva Cuenta – https://orbapp.worldcoin.org/auth/signup/create-account, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

El Checkbox "Entiendo y acepto los Términos y condiciones de usuario del operador de TFH y el Aviso de la aplicación TFH Orb y el socio operativo", fue activada posterior a la revisión que se hiciera inicialmente.

Una vez se aceptan, solicita seleccionar idioma correspondiente, realizada la operación se muestra el panel de control de la aplicación:

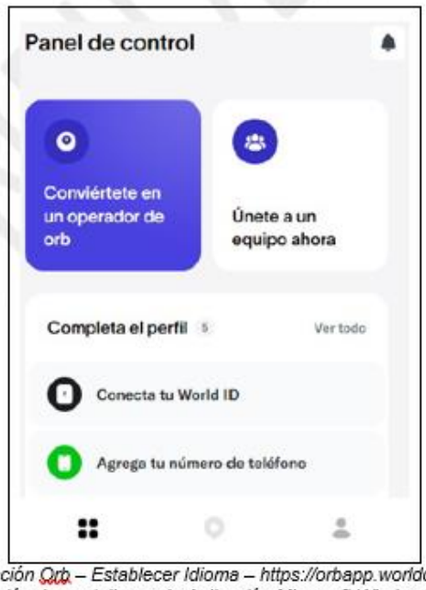


Imagen 184: *World – Aplicación Orb – Establecer Idioma – https://orbapp.worldcoin.org/auth/signin, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

Al seleccionar la opción *"Conviértete en un operador de Orb"*, se solicitan una serie de datos, a continuación, su descripción:

- Nombre completo.
- Correo electrónico.
- Número de teléfono.
- Linkedin (Opcional).
- Dirección de billetera (Opcional).
- ¿Cuál es tu Rol actual?
- ¿Cuál es tu industria actual?
- ¿Tienes una entidad comercial registrada?
  - Proporciona un breve resumen del negocio.
  - Sito web de negocios.
  - Si corresponde, sube un permiso de negocio minorista (Opcional).
  - Sube el certificado de registro de la empresa.
- ¿Estaría dispuesto a establecer una entidad comercial registrada para este proyecto?
- ¿Tienes un equipo?
  - ¿Cuál es el tamaño de tu equipo?
- ¿Tienes un espacio de oficina o comercio?
  - ¿Cuántas ubicaciones tiene?
  - Enlace de Google Maps.
  - Tamaño en metros cuadrados.
  - Sube una foto del espacio.
  - Agrega tus horas de trabajo.
  - ¿Tienes acceso a una conexión de internet confiable en tu ubicación?
- ¿Tienes experiencia en gestión de eventos, ventas y/o Marketing?

Una vez se diligencia la información solicitada, se envía la solicitud.

Al realizar la comparación correspondiente, encuentra el Despacho que, si bien frente a este formulario se introdujeron cambios, no es claro a partir de qué fecha se encuentran vigentes. La información que fuera recolectada con anterioridad a ellos se realizó de manera diferente tal como se indicó en líneas anteriores.

En este punto es necesario resaltar que "aceptar" o "entender" los términos o condiciones o la política de privacidad, no implica que el titular haya autorizado el tratamiento de sus datos personales, de esta manera iría en contra del principio de libertad antes desarrollado.

b) "**Suscríbete al Newsletter de Worldcoin**", de acuerdo con la imagen 107 del Acta de Preservación No. 087 del 8 de julio de 2024.

En el pie de página se encuentra un módulo para registrarse al "Newsletter" (Boletín informativo), para este proceso la página solicita únicamente el correo electrónico, como se puede ver a continuación:

Imagen 107: *World Coin – Pie de página – Suscríbete al newsletter de Worldcoin – https://es-es.worldcoin.org/, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

Se indicó en el Acta de Preservación No. 087 de 2024, indicó: *"en esta sección no se encuentra ningún chequeo para aceptar los términos y condiciones, Política de Privacidad, Aviso de privacidad o algún documento que haga referencia al tratamiento de datos personales. Sin embargo, en el pie de página se encuentran los enlaces para acceder a los Términos y Condiciones y Aviso de Privacidad".*

Sobre este aspecto en particular, si bien en la parte inferior de la página web se encuentran los enlaces para consultar las diferentes políticas de privacidad, lo cierto es que no se le informa de manera clara y expresa al titular que para efectos de suscribirse al "newsletter" puede consultar dichas políticas para otorgar su autorización en el tratamiento de los datos personales.

Independiente que se trate únicamente del correo electrónico de un titular, el formulario no es claro en indicar en cuál base de datos será registrado y si efectivamente se trata sólo para recibir el "boletín" de World, o que pueda ser utilizado para un fin diferente al inicialmente informado.

El mismo formulario fue evaluado en el Acta No. 214 del 16 de diciembre de 2024, y si bien introduce un cambio en su denominación, no es posible para el titular autorizar el tratamiento de su información.

c) Formulario World ID – para aplicaciones – Partner con World ID para su App. En la ya citada Acta de Preservación No. 087 del 7 de julio de 2024, el GTIFSD, describió el proceso para acceder a éste en los siguientes términos:

- *Al seleccionar esta opción, la página dirige al enlace "https://toolsforhumanity.typeform.com/partners?typeform-source=es-es.worldcoin.org", en este se encuentra el módulo mostrado en la imagen 22, página* ***Error! Bookmark not defined.****.*

- *Al dar clic en el botón "**Start**" (imagen 22, página **Error! Bookmark not defined.**), la página dirige a la primera parte del módulo, en esta solicita ingresar el nombre del titula que quiere usar el producto:*

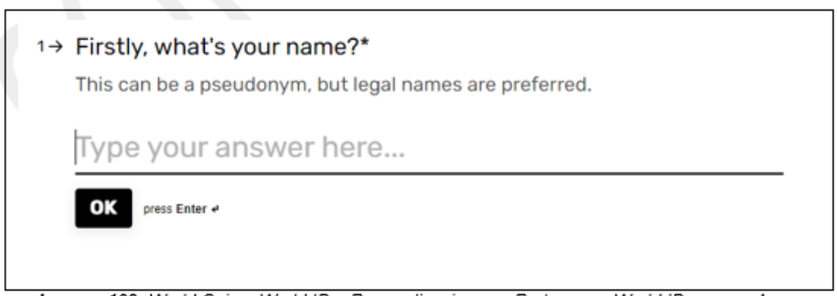


Imagen 109: *World Coin – World ID – Para aplicaciones – Partner con World ID para su App – https://toolsforhumanity.typeform.com/partners?typeform-source=es-es.worldcoin.org, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

- *Al ingresar la información solicitada y dar clic en el botón* ***"OK"****, el módulo solicita ingresar el correo electrónico:*

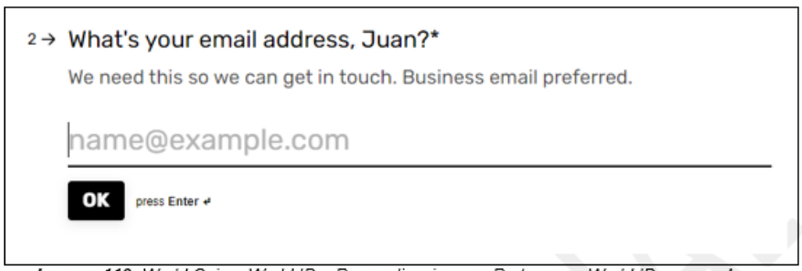


Imagen 110: *World Coin – World ID – Para aplicaciones – Partner con World ID para su App – https://toolsforhumanity.typeform.com/partners?typeform-source=es-es.worldcoin.org, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

- *Al ingresar la información solicitada y dar clic en el botón **"OK"**, el módulo solicita ingresar el proyecto que representa el titular:*

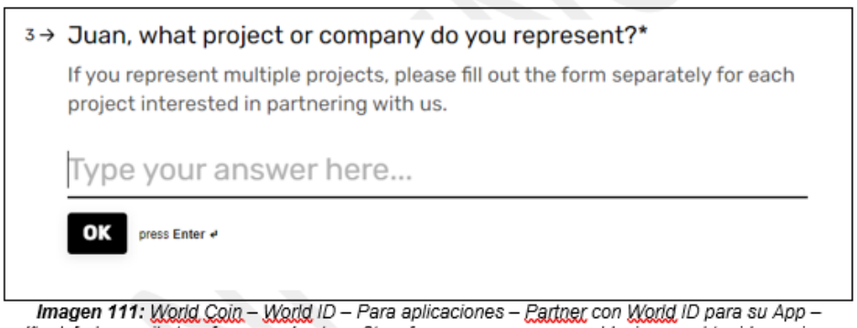


Imagen 111: *World Coin – World ID – Para aplicaciones – Partner con World ID para su App – https://toolsforhumanity.typeform.com/partners?typeform-source=es-es.worldcoin.org, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

- *Al ingresar la información solicitada y dar clic en el botón **"OK"**, el módulo solicita ingresar como World Coin puede conocer más acerca del proyecto del titular:*

Imagen 112: *World Coin – World ID – Para aplicaciones – Partner con World ID para su App – https://toolsforhumanity.typeform.com/partners?typeform-source=es-es.worldcoin.org, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

- *Al ingresar la información solicitada y dar clic en el botón **"OK"**, el módulo le solicita al titular seleccionar las opciones por las que está interesado en usar World ID en su proyecto:*

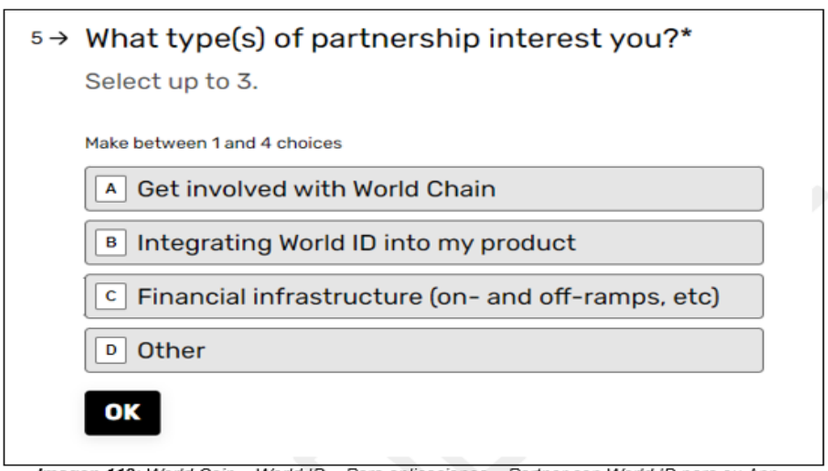


Imagen 113: *World Coin – World ID – Para aplicaciones – Partner con World ID para su App – https://toolsforhumanity.typeform.com/partners?typeform-source=es-es.worldcoin.org, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

- *Al ingresar la información solicitada y dar clic en el botón **"OK"**, el módulo le solicita al titular explicar en que se beneficiaría su proyecto con la implementación de WorldCoin.*

***Imagen 114:** World Coin – World ID – Para aplicaciones – Partner con World ID para su App – https://toolsforhumanity.typeform.com/partners?typeform-source=es-es.worldcoin.org, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

- *Al ingresar la información solicitada y dar clic en el botón **"OK"**, el módulo solicita enviar la información registrada oprimiendo el botón "Submit", al continuar se muestra el siguiente mensaje:*

***Imagen 115:** World Coin – World ID – Para aplicaciones – Partner con World ID para su App – https://toolsforhumanity.typeform.com/partners?typeform-source=es-es.worldcoin.org, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

Respecto del citado formulario, el GTIFSD informó lo siguiente: *"en esta sección no se encuentra ningún método para la consulta de Políticas de tratamiento de datos, Políticas de privacidad, Políticas de seguridad, Términos y condiciones, Avisos de privacidad o algún documento que haga referencia al tratamiento de datos. En esta sección tampoco se tiene acceso al pie de página".* Tampoco se encuentra algún tipo de sistema de chequeo con el que el titular pueda autorizar el tratamiento de sus datos personales.

Igualmente, es evidente que el formulario no se encuentra en idioma castellano, siendo éste de acuerdo con el artículo 10 de la Constitución Política, el idioma Oficial de la República de Colombia.

El citado formulario también fue revisado por el GTIFSD en el Acta No. 214 del 16 de diciembre de 2024, si bien presenta cambios menores en su forma, se encuentra redactado en inglés, situación que se convierte en una barrera para aquellas personas que no estén familiarizadas con ese idioma.

En este orden de ideas, los formularios que fueran verificados por el GTIFSD en el Acta de Preservación No. 87 del 8 de julio de 2024, y que, si bien les fueron introducidos algunos cambios, no le otorga al titular la posibilidad de autorizar el tratamiento de sus datos personales, de manera libre, expresa e informada.

En cuanto a los formularios "Solicitud de Eliminación de Datos" y "Pre – Ordena tu Orb – Pago", éstos no se encontraban desarrollados cuando se realizó la primera preservación de la página web de Worldcoin, por lo que, en virtud del debido proceso, este Despacho en el presente acto administrativo no hará pronunciamiento alguno, pues, no hicieron parte del Acto Administrativo que formuló los cargos.

Analizado el cumplimiento de la autorización previa como cláusula general para el tratamiento de los datos personales en los diferentes formularios dispuestos por las investigadas para el desarrollo de su objeto comercial en Colombia, este

Despacho procede a verificar el cumplimiento de la misma, frente al tratamiento los datos sensibles.

15.2.2. Autorización previa, expresa e informada para el tratamiento de datos personales sensibles.

El literal c) del artículo 3 de la Ley 1581 de 2012, definió el dato personal como *"cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables"*.

La jurisprudencia constitucional[21] en relación con el concepto de dato personal y sus tipologías se ha pronunciado de la siguiente manera:

> *"Esta definición, aunque es amplia, concuerda en términos generales con la línea jurisprudencial que esta Corte ha desarrollado en la materia, así como con la definición adoptada en la Ley 1266 sobre el dato personal financiero. Adicionalmente, la fijación de una definición de dato personal es un ejercicio legítimo de la libertad de configuración de la que goza el legislador, cuyos límites en este caso no han sido desconocidos.*
>
> *2.3.1.1 En efecto, la jurisprudencia constitucional ha precisado que las características de los datos personales –en oposición a los impersonales[184][22]- son las siguientes: "i) estar referido a aspectos exclusivos y propios de una persona natural, ii) permitir identificar a la persona, en mayor o menor medida, gracias a la visión de conjunto que se logre con el mismo y con otros datos; iii) su propiedad reside exclusivamente en el titular del mismo, situación que no se altera por su obtención por parte de un tercero de manera lícita o ilícita, y iv) su tratamiento está sometido a reglas especiales (principios) en lo relativo a su captación, administración y divulgación."[185]23*
>
> *(…)*
>
> *Por su parte, la Ley 1266, con el aval de esta Corporación, aunque en un contexto diferente, definió los datos personales de forma similar: "Dato personal: es cualquier pieza de información vinculada a una o varias personas natural o jurídica. (…)" (literal e del artículo 3).*
>
> *Los datos personales, a su vez, suelen ser clasificados en los siguientes grupos despendiendo de su mayor o menor grado de aceptabilidad de divulgación: datos públicos, semiprivados y privados o sensibles.[186]24*

En lo que tiene que ver con el dato personal sensible, la Corte Constitucional, en sentencia C – 1011 de 2008, indicó:

> *"[c]aso distinto se predica de la información sensible, relacionada, entre otros aspectos, con la orientación sexual, los hábitos del individuo y el credo religioso y político. En estos eventos, la naturaleza de esos datos pertenece al núcleo esencial del derecho a la intimidad, entendido como aquella "esfera o espacio de vida privada no susceptible de la interferencia arbitraria de las demás personas, que al ser considerado un elemento esencial del ser, se concreta en el derecho a poder actuar libremente en la mencionada esfera o núcleo, en ejercicio de la libertad personal y familiar, sin más limitaciones que los derechos de los demás y el ordenamiento jurídico".[129] En este caso, todo acto de divulgación mediante los procesos genéricos de administración de datos personales, distintos a las posibilidades de divulgación excepcional descritas en el fundamento jurídico 2.5. del presente análisis, se encuentra proscrita. Ello en la medida que permitir que información de esta naturaleza pueda ser objeto de procesos ordinarios de acopio, recolección y circulación vulneraría el contenido esencial del derecho a la intimidad.*

Nótese que, de acuerdo con su naturaleza, el tratamiento de la información sensible de un titular, el Responsable debe contar con un proceso reforzado y de diligencia de tratamiento tanto en su recolección como cualquier operación sobre los mismos.

Ahora bien, el artículo 5 de la Ley 1581 de 2012, definió el dato personal sensible en los siguientes términos:

---

[21] Sentencia C – 748 de 2011
[22] [184]Ver sentencia T-729 de 2002, M.P. Eduardo Montealegre Lynett.
[23] [185]*Cfr.* Sentencia T-414 de 1992, M.P. Ciro Angarita Barón.
[24] [186]Ver sentencias T-729 de 2002, M.P. Eduardo Montealegre Lynett; C-491 de 2007, M.P. Jaime Córdoba Triviño; y C-1011 de 2008, M.P. Jaime Córdoba Triviño, y artículo 3 de la Ley 1266.

> *"**ARTÍCULO 5o. DATOS SENSIBLES.** Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y **los datos biométricos**". (negrilla fuera de texto)*

El citado artículo categoriza el dato biométrico como un dato sensible, ya que por su naturaleza está en la capacidad de determinar la identidad de una persona a partir de aspectos relacionados con sus características biológicas.

La Superintendencia Financiera de Colombia, en la Circular Básica Jurídica cuando desarrolló los aspectos de Seguridad y Calidad que deben tenerse en cuenta en la realización de operaciones, dispuso:

> *2.2. Definiciones aplicables*
>
> *2.2.13. Característica biométrica: Atributo biológico o comportamental de un individuo del cual se pueden extraer propiedades distintivas y repetibles para su reconocimiento.*
>
> *2.2.14. Muestra biométrica: Representación que se obtiene de una característica biométrica capturada mediante un dispositivo vinculado a un sistema biométrico, como una imagen facial, una grabación de voz o una imagen de huella digital.*
>
> *2.2.15. Plantilla biométrica: Representación de una o varias muestras biométricas utilizadas para la comparación, reconocimiento e individualización de una persona, las cuales pueden construirse a través de métodos tales como vectores, datos numéricos y algoritmos criptográficos.*

En la regulación europea se definió el dato biométrico en los siguientes términos[25]:

> *"Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o conformen la identificación única de dicha persona (…)*

Respecto de los sistemas biométricos el Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales, creado en virtud de la Directiva 95/46/CE del Parlamento Europeo, indicó:

> *"Los sistemas biométricos son aplicaciones de las tecnologías biométricas que permiten la identificación automática, y/o la autenticación/comprobación de una persona. Se suelen utilizar aplicaciones de autenticación/comprobación para diversas tareas en campos muy distintos y bajo la responsabilidad de una amplia gama de entidades diferentes.*
>
> *Cada biometría, ya se utilice para autenticación/comprobación o para identificación, depende, más o menos, del elemento biométrico en cuestión, que puede ser:*
> *- **universal:** el elemento biométrico existe en todas las personas;*
> *- **único:** el elemento biométrico debe ser distintivo para cada persona;*
> *- y **permanente:** la propiedad del elemento biométrico es permanente a lo largo del tiempo para cada persona.*
>
> *Se puede distinguir entre dos categorías principales de técnicas biométricas, en función de que se utilicen datos estables o datos dinámicos sobre el comportamiento.*
>
> *En primer lugar, existen técnicas basadas en aspectos físicos y fisiológicos que miden las características fisiológicas de una persona e incluyen: comprobación de las huellas digitales, análisis de la imagen del dedo, reconocimiento del iris, análisis de la retina, reconocimiento facial, resultados de muestras de las manos, reconocimiento de la forma de la oreja, detección del olor corporal, reconocimiento de la voz, análisis de muestras del ADN y análisis de los poros de la piel, etc. (…)"*

A través del reconocimiento del iris, se proporcionan patrones que reflejan características físicas o fisiológicas del individuo. Estos patrones del iris vienen marcados desde el nacimiento y rara vez cambian, son muy complejos y contienen una gran cantidad de información, más de 200 propiedades únicas[26].

---

[25] Artículo 4 – 14 del Reglamento General de Protección de Datos de la Unión Europea

[26] Guía para el Tratamiento de Datos Biométricos. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales INAI.

El objeto del sistema biométrico es reconocer a las personas, es decir, "volver a conocer" a una persona que ha sido identificada y registrada previamente. En otras palabras, el reconocimiento implica comparar –de manera manual o automatizada- una muestra biométrica de una persona con plantillas previamente registradas y relacionadas con una identidad específica.

Bajo este entendido, el dato biométrico conserva su calidad y características físicas y/o fisiológicas de la persona a quien pertenece durante el tiempo que dure su tratamiento, es decir, desde el momento de su captura, almacenamiento y la posterior comparación que se realice por parte del Responsable.

Así las cosas, **el código de iris como dato biométrico a la luz de la legislación Colombiana es un dato personal sensible**, en la medida que permite la identificación de una persona por sus condiciones físicas y/o fisiológicas, **por lo que su tratamiento debe ajustarse al régimen de protección de datos personales vigente en el territorio colombiano.**

El artículo 6 de la Ley 1581 de 2012 **prohíbe el tratamiento de los datos personales sensibles.** Sin embargo, establece una serie de excepciones, entre las cuales se encuentra la **autorización explicita a dicho tratamiento por parte del titular.**

Efectivamente, de conformidad con el principio de libertad, es posible que las personas naturales den su consentimiento, por supuesto, expreso e informado, para que sus datos personales sean sometidos a tratamiento. En estos casos deberán cumplirse con todos los principios que rigen el tratamiento de datos personales, en especial cobrará importancia el principio de finalidad, según el cual el dato sensible solamente podrá ser tratado para las finalidades expresamente autorizadas por el titular y que en todo caso deben ser importantes desde el punto de vista constitucional (…)[27] (Subraya fuera de texto)

El artículo 2.2.2.25.2.3. del Decreto 1074 de 2015, reglamenta la autorización de que trata el artículo 5 de la Ley 1581 de 2012, en los siguientes términos:

> ***ARTÍCULO 2.2.2.25.2.3. De la autorización para el Tratamiento de datos personales sensibles.*** *El Tratamiento de los datos sensibles a que se refiere el artículo 5 de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6 de la citada ley.*
>
> *En el Tratamiento de datos personales sensibles, cuando dicho Tratamiento sea posible conforme a lo establecido en el artículo 6 de la Ley 1581 de 2012, deberán cumplirse las siguientes obligaciones:*
>
> *1. Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.*
> *2. Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.*
> ***Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles***

Se trata entonces de una autorización reforzada, pues busca proteger el derecho constitucional de habeas data del titular frente a los datos personales sensibles que sean recolectados por parte de un Responsable, y considerando su naturaleza de identificar física o fisiológicamente a una persona, deberá informar las finalidades específicas para las cuales serán utilizados.

Así mismo, **el Responsable no podrá condicionar el desarrollo de su actividad, al consentimiento que sobre el mismo deba otorgar el titular.**

El Acta de Preservación de la página web No. 087 del 8 de julio de 2024, se verificó el "Formulario de Consentimiento de Worldcoin Foundation para datos Biométricos". Versión 1.16 efectiva a partir del 12 de junio de 2024.

[27] C-748 de 2011

Con el citado formulario, se informa a las personas interesadas en participar en la operación, que el tratamiento de los datos biométricos recolectados se realizará al momento de hacer su verificación en el Orb. A continuación, se describen las etapas:

(i) Al iniciar con la descarga de la aplicación, ésta se encuentra en idioma inglés, indica un Checkbox en el cual se le pregunta al titular si está de acuerdo con los Términos y Condiciones de Uso y Aviso de Privacidad de World App proveída por Tools For Humanity Corporation.

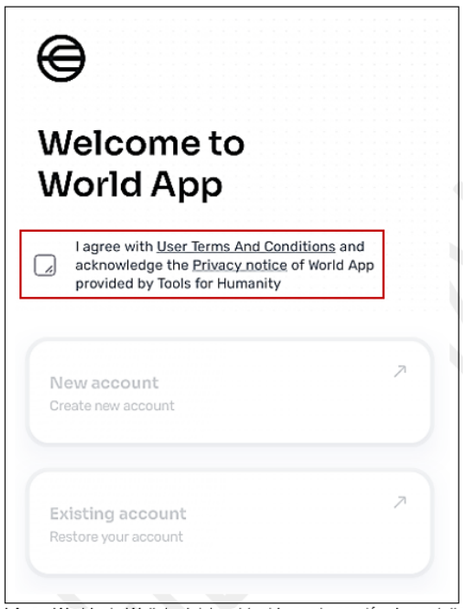


Imagen 53: *World App - Worldcoin Wallet – Inicio, obtenida por impresión de pantalla con la Aplicación Microsoft Windows Recortes.*

(ii) En este punto debe aclararse que los términos y condiciones y Aviso de privacidad, están relacionados únicamente con la descarga de la aplicación en cualquiera de las tiendas habilitadas para el efecto. Aún no se trata del tratamiento de datos personales sensibles.

Y si bien se da la posibilidad de ingresar y verificar las políticas de privacidad, "estar de acuerdo" con las mismas, no quiere decir que se acepte el tratamiento de los datos personales que son recolectados para su funcionamiento.

ESPACIO EN BLANCO

Imagen 55: *Aplicación World App - Worldcoin Wallet – Creación cuenta, obtenida con impresión de pantalla por la Aplicación de Microsoft Windows Recortes.*

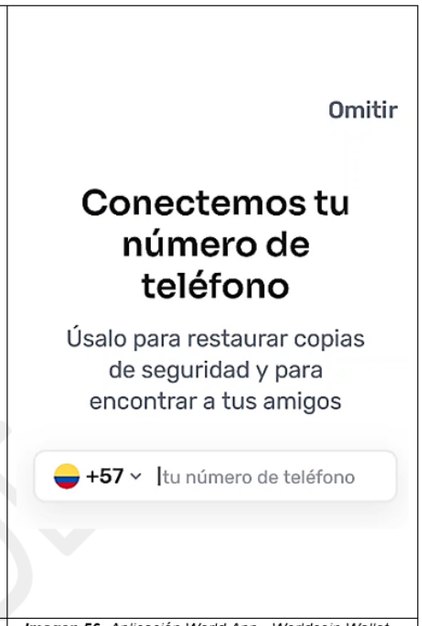


Imagen 56: *Aplicación World App - Worldcoin Wallet – Creación cuenta, obtenida con impresión de pantalla por la Aplicación de Microsoft Windows Recortes.*

(iii) Al omitir el registro de un número de teléfono, la aplicación solicita la creación de una contraseña. Una vez creada la contraseña la aplicación muestra un mensaje en el que informan que se realizará una copia de seguridad de la cuenta, como se puede ver a continuación:

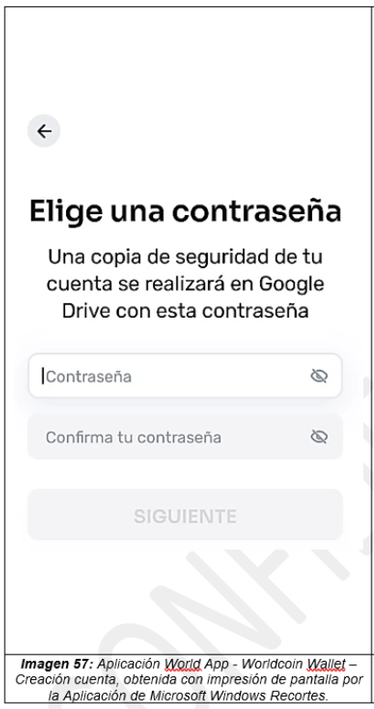


Imagen 57: *Aplicación World App - Worldcoin Wallet – Creación cuenta, obtenida con impresión de pantalla por la Aplicación de Microsoft Windows Recortes.*

Imagen 58: *Aplicación World App - Worldcoin Wallet – Creación cuenta, obtenida con impresión de pantalla por la Aplicación de Microsoft Windows Recortes.*

(iv) La aplicación solicita seleccionar la cuenta de correo electrónico con la que se realizará la copia de seguridad de la cuenta, una vez se selecciona la cuenta y se otorgan los permisos de acceso a esta se puede acceder al inicio de la aplicación, como se puede ver a continuación:

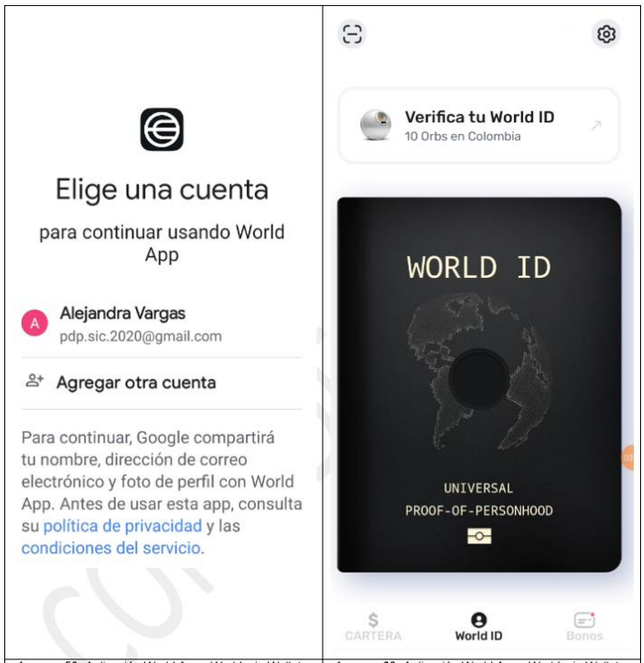


Imagen 59: *Aplicación World App - Worldcoin Wallet – Creación cuenta, obtenida con impresión de pantalla por la Aplicación de Microsoft Windows Recortes.*

Imagen 60: *Aplicación World App - Worldcoin Wallet – Creación cuenta, obtenida con impresión de pantalla por la Aplicación de Microsoft Windows Recortes.*

(v) Una vez se accede a la aplicación, esta solicita seleccionar la moneda que el usuario quiere configurar, mostrando por defecto el peso colombiano, al seleccionar la moneda y continuar se muestra el inicio de la aplicación, como se puede ver a continuación:

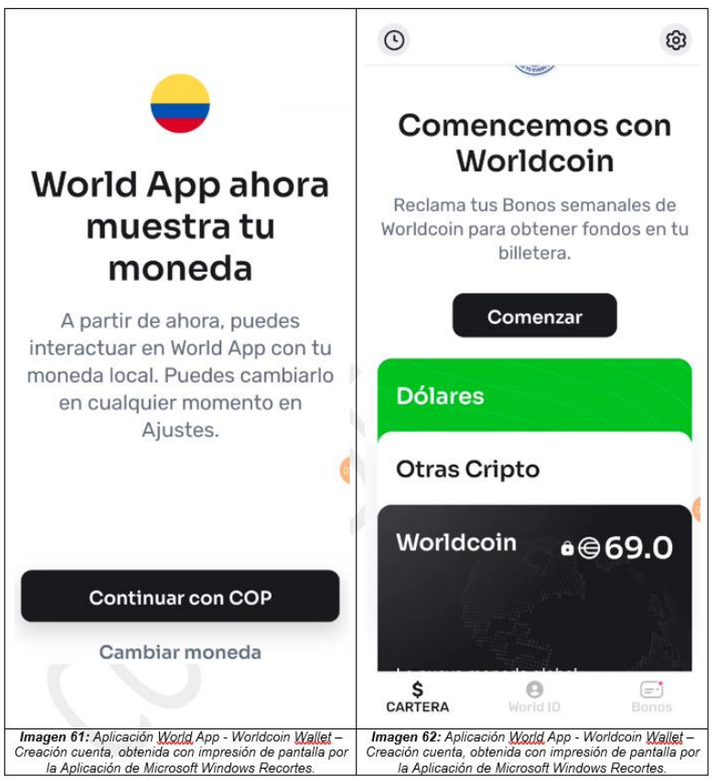


Imagen 61: *Aplicación World App - Worldcoin Wallet – Creación cuenta, obtenida con impresión de pantalla por la Aplicación de Microsoft Windows Recortes.*

Imagen 62: *Aplicación World App - Worldcoin Wallet – Creación cuenta, obtenida con impresión de pantalla por la Aplicación de Microsoft Windows Recortes.*

(vi) Al seleccionar la opción "**Wordcoin", se muestran los bonos que se encuentran disponibles y su valor en pesos colombianos. Este valor podrá ser reclamado por el titular cuando realice la comprobación y verificación de su iris con un Orb, para lo cual se debe realizar el agendamiento de una cita, como se puede ver a continuación.**

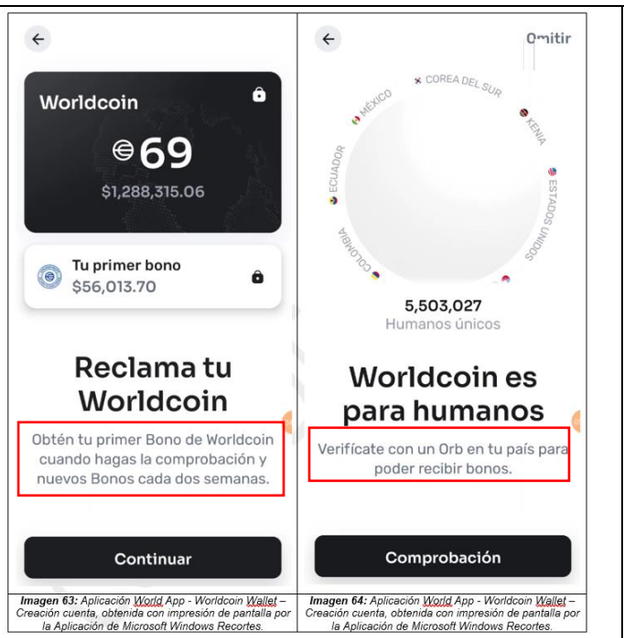


Imagen 63: *Aplicación World App - Worldcoin Wallet – Creación cuenta, obtenida con impresión de pantalla por la Aplicación de Microsoft Windows Recortes.*

Imagen 64: *Aplicación World App - Worldcoin Wallet – Creación cuenta, obtenida con impresión de pantalla por la Aplicación de Microsoft Windows Recortes.*

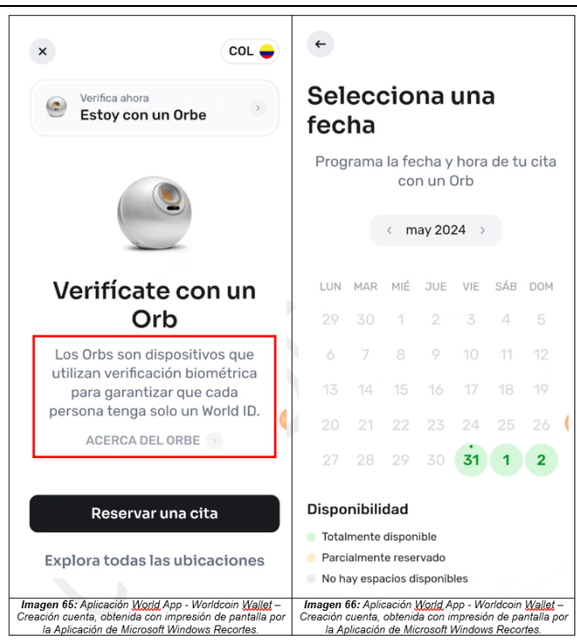


Imagen 65: *Aplicación World App - Worldcoin Wallet – Creación cuenta, obtenida con impresión de pantalla por la Aplicación de Microsoft Windows Recortes.*

Imagen 66: *Aplicación World App - Worldcoin Wallet – Creación cuenta, obtenida con impresión de pantalla por la Aplicación de Microsoft Windows Recortes.*

(vii) Una vez se encuentra la disponibilidad para asistir a la verificación del iris con un Orb, se asigna igualmente la hora para asistir a la cita, tal como puede observarse a continuación:

Imagen 67: *Aplicación World App - Worldcoin Wallet – Creación cuenta, obtenida con impresión de pantalla por la Aplicación de Microsoft Windows Recortes.*

Finalmente, el titular asiste a la cita programada para realizar la respectiva verificación ante el Orb. **En esta etapa, antes de que se realice el escaneo del iris, el titular debe tener la oportunidad de leer el "Formato de Consentimiento de World Foundation para datos biométricos". Actividad que sólo puede realizarse una vez sea descargado de la respetiva aplicación.**

Una vez se realice la verificación del iris y por consiguiente su comparación, conforme el modelo de negocio manejado por Worldcoin, se realiza la entrega al titular de la compensación económica.

Pues bien, de la lectura del citado formato, considera el Despacho que su redacción no es clara y concreta frente al tratamiento de los datos personales sensibles para

quienes participan de la operación en Colombia, y es así, porque las reglas dispuestas en este no se aplican de la misma manera en otros países o regiones.

Al verificar la Sección 10 del citado formulario, evidencia el Despacho que coincide con lo dispuesto en la Sección 14 de la Política de Privacidad de World.

> *"A continuación, varias adendas disponen información jurídicamente requerida para los mercados respectivos en los que desarrollamos nuestra actividad. Esta información forma parte del consentimiento dependiendo de la región en la que resida el interesado. Esta información puede diferir de la información de su ubicación porque en determinadas jurisdicciones bloqueamos determinados servicios. En caso de cualquier incoherencia con lo anterior, prevalecerá la declaración más especial sobre la jurisdicción en particular".*

Es decir, determinadas cláusulas del formulario de consentimiento de World para datos biométricos, no son aplicadas en la Unión Europea, Reino Unido, Japón, Argentina, Singapur, Corea del Sur, y Perú pero si lo son en Colombia.

Un ejemplo de ello, y tal vez la más importante es la función de "custodia de datos", de que trata el numeral 3 del formulario de consentimiento. Indica explícitamente, que la misma puede estar desactivada en ciertas jurisdicciones, debido a requisitos normativos, lo cual evidentemente no se ajusta al principio de transparencia establecido en el literal e) del artículo 4 de la Ley 1581 de 2012.

La custodia de datos se especifica en el formulario de consentimiento de la siguiente manera:

3. **Habilitación de la Custodia de datos.**

Tenga en cuenta que la Custodia de datos podrá estar desactivada en algunas jurisdicciones debido a requisitos normativos. Consulte el apartado Adendas a continuación para confirmar si esta opción está disponible para usted.

3.1 Estado actual del proyecto Worldcoin

Para mejorar la precisión de las determinaciones de elegibilidad del sistema, necesitamos seguir entrenando a nuestro software de algoritmos. Por "entrenar" se entiende utilizar imágenes de personas reales como usted para ayudar al software a "aprender" a distinguir a los humanos de los no humanos y diferenciar a una persona de todas las demás. Actualizaremos el software periódicamente según se vaya entrenando y mejorando. Cuando eso ocurra, es posible que tengamos que volver a verificar su identidad digital única, y para ello será necesario usar sus Datos de imagen de nuevo.

3.2 Custodia de datos.

Si otorga su consentimiento para este Formulario de consentimiento de datos biométricos, en la aplicación se le pedirá que "**Habilite la Custodia de datos**." Si decide optar por la Custodia de datos, nos permitirá:

1. conservar los Datos de imagen y Derivados recopilados y calculados por el Orb;
2. enviar los Datos de imagen a nuestros equipos de la Unión Europea y Estados Unidos; y
3. utilizar los Datos de imagen para seguir desarrollando y mejorando el software, como se describe a continuación.
4. Etiquetar sus Datos de imagen con el sexo, el rango de edad y el color de la piel percibidos y aproximados para entrenar en la equidad algorítmica a la luz de la diversidad en el mundo.

Esto probablemente le ayudará a evitar inconvenientes porque, si tenemos sus Datos de imagen, no tendrá que volver a un Orb para verificar de nuevo su identidad digital cuando actualicemos el software. También nos ayudará, porque podemos usar sus Datos de imagen para mejorar el sistema y que Worldcoin se ponga a disposición más rápido. Una vez más, no es necesario que habilite la Custodia de datos, pero hacerlo puede ser conveniente tanto a usted como a nosotros, por lo que se lo agradecemos enormemente.

3.3 Datos que recopilamos al habilitar la Custodia de datos.

Cuando da su consentimiento en el Formulario de consentimiento de datos biométricos, recopilamos Datos de imágenes de sus iris e imágenes de su rostro, tal como se describe en el apartado II.1 anterior. Los Datos de imagen que recopilamos no cambian si acepta la Custodia de datos.

3.4 Qué hacemos con estos datos cuando habilita la Custodia de datos.

Cuando acepta el Formulario de consentimiento de datos biométricos, utilizamos los datos anteriores para los fines descritos en el apartado 2.2. Cuando también habilita la Custodia de datos, utilizamos los datos para los siguientes fines adicionales:

- actualizar automáticamente su Código de iris en caso de que actualicemos el algoritmos que calcula los Códigos de iris;
- optimizar y mejorar el cálculo del Código de iris y los Derivados;
- etiquetar los datos recopilados;
- utilizar los datos para formar y seleccionar al personal de etiquetado;
- desarrollar y entrenar algoritmos para reconocer, segmentar y diferenciar entre imágenes de iris y rostros humanos;
- probar los algoritmos con los resultados etiquetados por humanos;
- detectar y eliminar el sesgo de nuestros algoritmos (como el entrenamiento en equidad algorítmica etiquetando el sexo, el rango de edad y el color de piel aproximados);
- desarrollar, entrenar y probar un sistema para detectar si un usuario es un ser humano que presenta un ojo humano real o si un registro es válido;
- desarrollar, entrenar y probar modelos que utilicen imágenes de iris artificiales para, a su vez, entrenar aún más a los algoritmos;
- desarrollar, entrenar y probar modelos que mejoren el rendimiento y la experiencia del usuario del Orb; y
- formar y evaluar al personal que trabaja en estos sistemas.

No venderemos sus datos nunca. Tampoco utilizaremos ningún dato enumerado en este formulario para hacerle un seguimiento o para enviarle anuncios de productos de terceros.

Nótese que los datos que pueden ser recolectados son de naturaleza sensible. Su tratamiento no coincide con el objeto mismo del protocolo, según el cual no se trata de identificar a una persona por sus características físicas o fisiológicas.

Por ejemplo, si se autoriza la custodia de datos por el titular, de acuerdo con el formulario *"probablemente le ayudará a evitar inconvenientes porque, si tenemos Datos de imagen, no tendrá que volver a un Orb para verificar de nuevo su identidad digital cuando actualicemos el software".* Igualmente, se podrá *"actualizar automáticamente su código de iris en caso de que actualicemos el algoritmo que calcula los códigos de iris."*

Autorizar la custodia de datos tal como está redactada en el formato analizado, condiciona el consentimiento del titular respecto del tratamiento de sus datos personales sensibles.

Ahora bien, de acuerdo con lo informado por la apoderada de World en el escrito de alegatos de conclusión, la opción de custodia de datos se encuentra hoy en día, deshabilitada a escala global.

> *"En todo caso, y de acuerdo con el peritaje de Juan Diego Jiménez, la funcionalidad de "Habilitación para la Custodia de Datos" está desactivada globalmente en este momento. Los usuarios hoy en día no tienen la opción de activar esta opción:*

ESPACIO EN BLANCO

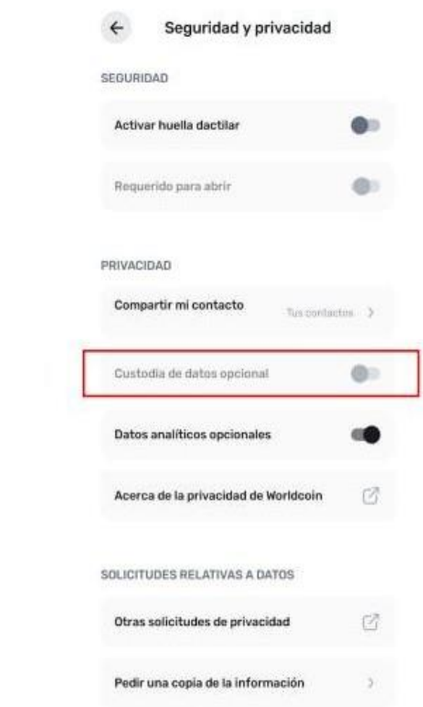


Figura 23. Opción de Custodia de Datos deshabilitada.

De acuerdo con lo anterior, si la opción fue desactivada a nivel global, ¿a partir de qué fecha? ¿qué razones tuvieron para desactivarla? ¿qué sucedió con los datos personales de los titulares que optaron por habilitar su custodia conforme lo indicado en el formulario? ¿por qué sigue siendo una opción en el formulario de consentimiento? Son preguntas que de acuerdo con las pruebas allegadas no tienen respuesta y que para esta Dirección es la confirmación de que a pesar de existir una prohibición expresa para el tratamiento de datos personales sensibles, como lo es código de iris de las personas, World Foundation y Tools For Humanity inician sus operaciones sin tener en cuenta el régimen de protección de datos personales, imponiendo su modelo de negocio por encima de los derechos fundamentales de origen constitucional que tienen los titulares residentes en Colombia.

En lo que tiene que ver con la obligación de conservar la autorización para ser consultada de manera posterior, en el formulario se indica que el titular *"tiene derecho a obtener de nosotros en cualquier momento, previa solicitud,* ***información sobre los datos personales*** *que tratamos sobre usted. Tiene derecho a recibir de nosotros los datos personales que le conciernen".*

La apoderada de World Foundation indica *que "la prueba de autorización es un dato personal (i.e., información vinculada o que puede asociarse a una o varias personas naturales determinadas o determinables)"*, por lo que, el titular puede solicitarla a través del medio establecido para ello.

Como se ha dicho, la autorización otorgada por el titular en los términos establecidos por el artículo 9 de la Ley 1581 de 2012, legitima al Responsable para el tratamiento de los datos personales solicitados. Sus requisitos son la de ser previa, expresa e informada y deberá *ser "obtenida por cualquier medio que pueda ser objeto de consulta posterior."*

Así, el Responsable del tratamiento debe estar en la capacidad de demostrar que cuenta con la autorización del titular, esto con el fin de verificar si ésta se dio bajo los términos establecidos en la Ley.

El numeral 9 del citado formulario hace relación a los derechos que tiene el titular frente al tratamiento de sus datos personales. Y éstos se pueden aplicar ***"en la medida en que podamos identificar al solicitante en nuestra base de datos"***. Luego entonces, si un titular o la autoridad de protección de datos

personales solicita la copia de la autorización, es probable que ésta no pueda ser consultada o entregada, en el caso que no se logre identificar a esa persona.

Y esos derechos se refieren únicamente a los datos personales que son recolectados y no frente a la autorización previa otorgada por el titular. Por lo tanto, tal y como se consideró en la formulación de cargos no es posible determinar si el Responsable del tratamiento pueda demostrar que las autorizaciones puedan ser consultadas posteriormente a solicitud del mismo titular que la otorgó.

Como se dijo en líneas anteriores, *el Responsable está en la obligación de adoptar los mecanismos aptos e idóneos para obtener la autorización del tratamiento por lo menos al momento en que se recolecte la información. Así mismo deberá garantizar que la misma pueda ser consultada posteriormente, tal y como lo establece el literal b) del artículo 17 de la Ley 1581 de 2012.*

Finalmente, se pregunta en este punto el Despacho, si los Operadores del Orb, que solo fungen como terceros colaboradores, cuentan con la capacitación necesaria para acompañar durante todo el proceso al titular, indicándole, por ejemplo, y entre otras cosas, cuáles son los derechos que le asisten conforme la Ley. De acuerdo con los pasos que debe seguir el titular desde la descarga de la World App y la recolección de su información biométrica, para adquirir el World ID, el tiempo con el que cuenta el titular para conocer y sobre todo entender el formato de consentimiento de datos biométricos, no es suficiente. Luego entonces, la promesa de un beneficio económico a cambio del dato biométrico puede acelerar el proceso para que el titular otorgue su autorización, sin que haya necesidad de una explicación adicional.

Esta forma de obtener la autorización previa expresa e informada del titular, no se ajusta a los estándares establecidos en el régimen de protección de datos en Colombia. La entrega de un beneficio económico a cambio de la imagen del iris significa que la operación de World Foundation se fundamenta en la monetización de los datos biométricos recolectados, estableciendo un determinado valor ya sea en bonos o en pesos colombianos (COP). Por lo tanto, a consideración del Despacho, se convierte en una figura dominante, en cuya relación, el titular se verá abocado a aceptar todas y cada una de las condiciones que imponga frente al tratamiento de la información entregada, desconociendo que el consentimiento debe obedecer a la voluntad libre del titular, quien debe estar en la capacidad de decidir conscientemente si está de acuerdo o no con el tratamiento de sus datos personales, en especial cuando se trata de aquellos de naturaleza sensible. La promesa de una contraprestación cualquiera que sea el tipo puede condicionar el juicio del titular y llevarlo tomar una decisión desinformada y prematura.

Bajo este contexto, está claro para el Despacho que el consentimiento o la autorización que otorgue el titular respecto del tratamiento de sus datos personales biométricos bajo estas condiciones no puede considerarse como libre, espontáneo o voluntario en los términos del principio de libertad.

15.3. Deber de informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.

Establece el literal c) del artículo 17 de la Ley 1581 de 2012, lo siguiente:

> ***"ARTÍCULO 17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO.*** *Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:*
>
> *c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;*

Por su parte, el literal b) del artículo 4 de la citada Ley, define el principio de finalidad de la siguiente manera:

> ***ARTÍCULO 4º. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES.*** *En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:*
>
> ***b) Principio de finalidad:*** *El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular;*

En lo que tiene que ver con los derechos de los titulares, estableció el legislador:

> ***ARTÍCULO 8o. DERECHOS DE LOS TITULARES.*** *El Titular de los datos personales tendrá los siguientes derechos:*
>
> ***a)*** *Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado;*
> ***b)*** *Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la presente ley;*
> ***c)*** *Ser informado por el Responsable del Tratamiento o el Encargado del Tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales;*
> ***d)*** *Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen;*
> ***e)*** *Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento el Responsable o Encargado han incurrido en conductas contrarias a esta ley y a la Constitución;*
> ***f)*** *Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.*
> *(…)*

Respecto del citado artículo la Corte Constitucional mediante sentencia C-748 de 2011, indicó:

> *"En realidad, los derechos enunciados en el Proyecto, son un desarrollo concreto de los principios enunciados en el artículo 4. En efecto, en virtud del principio de legalidad el Titular tiene derecho a que sus datos sean tratados de conformidad con los límites establecidos en la normatividad vigente, especialmente tomar acciones cuando su Tratamiento esté expresamente prohibido (ordinal a). En razón de la finalidad, el Titular tiene el derecho a ejercer un control constante sobre el dato, con el fin de determinar si el mismo está siendo utilizado para los fines frente a los cuales prestó su autorización y solicitar al Responsable o al Encargado informaciones sobre el uso que ha dado de sus datos personales (ordinales b, c y e). En razón del principio de libertad, el Titular tiene la garantía de comprobar que los datos que circulen sobre él, han sido previamente autorizados, solicitar prueba de ello y también puede revocar su autorización (ordinales a, b, c y e). Por el principio de veracidad o calidad, el Titular tiene el derecho a conocer, actualizar y rectificar sus datos personales en los casos en que estos sean inexactos, incompletos o fraccionados, que induzcan a error o cuyo Tratamiento se encuentre prohibido (ordinal a). Por el principio de transparencia, el Titular tiene derecho a conocer los datos que sobre él reposan en las bases de datos, solicitar prueba de la autorización brindada, ser informado del manejo que se ha hecho de sus datos y acceder en forma gratuita a sus datos personales (ordinales a, b y f). En aras del principio de acceso y circulación restringida, seguridad y confidencialidad, el Titular tiene derecho a exigir que su información sea tratada de conformidad con los límites impuestos por la Ley y la Constitución y que en caso de incumplimiento existe un recurso efectivo para lograr el restablecimiento de sus derechos (ordinales a y d).*
>
> *De la misma manera, cabe señalar que al igual que los principios, no puede considerarse que esta es una lista taxativa de garantías, sino que se encuentran incluidas todas aquellas prerrogativas que sean consecuencia de la garantía amplia del derecho fundamental al habeas data. De la misma manera, la rapidez del surgimiento de nuevos sistemas de información también hace necesario que los derechos sean integrados a los propios de cada sistema de información".*[28]

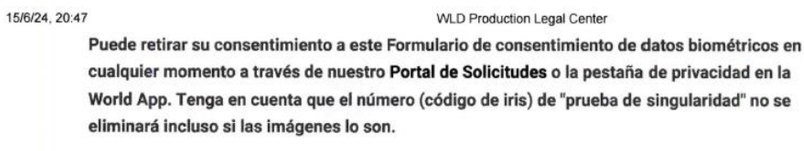
Adicionalmente el artículo 12 de la Ley 1581 de 2012, establece:

---

[28] Por ejemplo, en materia de redes sociales empiezan a dibujarse nuevos derechos. Así, el Grupo de Trabajo sobre Protección de Datos de la Unión Europea sostiene que en estos sistemas se deberían adoptar las siguientes medidas: "*Obligaciones de los SRS1. Los SRS deberían informar a los usuarios de su identidad y proporcionarles información clara y completa sobre las finalidades y las distintas maneras en que van a tratar los datos personales. 2. Los SRS deberían establecer parámetros por defecto respetuoso de la intimidad. 3. Los SRS deberían informar y advertir a sus usuarios frente a los riesgos de atentado a la intimidad cuando transfieren datos a los SRS. 4. Los SRS deberían recomendar a sus usuarios no poner en línea imágenes o información relativa a otras personas sin el consentimiento de éstas. 5. Como mínimo, en la página inicial de los SRS debería figurar un enlace hacia una oficina de reclamaciones, tanto para miembros como para no miembros, que cubra cuestiones de protección de datos. 6. La actividad comercial debe ajustarse a las normas establecidas por la Directiva relativa a la protección de datos y la Directiva sobre la protección de la vida privada en el sector de las comunicaciones electrónicas. 7. Los SRS deben establecer plazos máximos de conservación de los datos de los usuarios inactivos. Las cuentas abandonadas deben suprimirse. 8. Por lo que se refiere a los menores, los SRS deberían adoptar medidas adecuadas con el fin de limitar los riesgos.*"

> ***ARTÍCULO 12. DEBER DE INFORMAR AL TITULAR.*** *El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:*
>
> ***a)*** *El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;*
> ***b)*** *El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;*
> ***c)*** *Los derechos que le asisten como Titular;*
> ***d)*** *La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.*

En lo que tiene que ver con el Formato de Consentimiento para datos biométricos en sus versiones 1.16 del 12 de junio de 2024 y 1.18 del 30 de septiembre de 2024, indican que el número del código de iris o prueba de singularidad no se eliminará incluso si las imágenes que se tengan del titular son suprimidas.


15/6/24, 20:47 WLD Production Legal Center

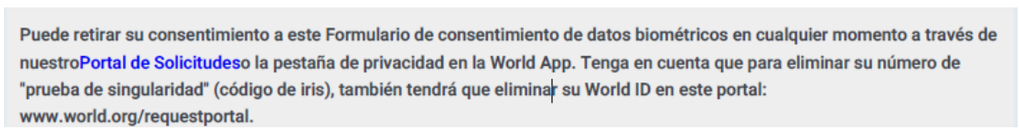
Puede retirar su consentimiento a este Formulario de consentimiento de datos biométricos en cualquier momento a través de nuestro Portal de Solicitudes o la pestaña de privacidad en la World App. Tenga en cuenta que el número (código de iris) de "prueba de singularidad" no se eliminará incluso si las imágenes lo son.

Se cuestiona el Despacho ¿existe una finalidad específica para ello?, si la hay ésta no le es informada al titular de manera clara y transparente.

La autorización que otorga un titular para el tratamiento de sus datos personales debe abarcar todos y cada uno de sus aspectos, desde el momento de su recolección hasta cuando cumpla con su propósito. El Responsable no puede limitar el consentimiento del titular para ciertas actividades del tratamiento, el derecho constitucional que tiene el titular respecto de la información que repose de él en una base de datos incluye solicitar la eliminación de ésta.

Nuevamente se cuestiona el Despacho ¿qué sucede con los datos personales sensibles de los titulares que solicitan la eliminación de su información incluyendo el código de su iris? ¿World Foundation aún conserva los códigos de iris respecto de los cuales se solicitó eliminación y no se accedió a ésta?

En la versión 1.22 del 2 de diciembre de 2024, se modifica lo relacionado con la eliminación de la información, en el entendido que si el titular quiere eliminar su código de iris deberá hacerlo también respecto de la World ID.


Puede retirar su consentimiento a este Formulario de consentimiento de datos biométricos en cualquier momento a través de nuestroPortal de Solicitudeso la pestaña de privacidad en la World App. Tenga en cuenta que para eliminar su número de "prueba de singularidad" (código de iris), también tendrá que eliminar su World ID en este portal: www.world.org/requestportal.

Ahora bien, una de las finalidades descritas por World Foundation, para obtener la información del código de iris de las personas es crear la prueba de singularidad, un código que identifique su unicidad. Así se podrá evitar el doble registro o un fraude respecto de la operación. Esto se logra a través de la comparación que se realice entre esos códigos, para lo cual necesariamente se debe conservar el código de iris correspondiente.

Si bien se le otorga al titular la posibilidad de solicitar la eliminación de su código de iris y su World ID ¿qué medidas tiene implementadas el responsable para continuar con la comparación de los códigos de iris? Es lógico concluir que la información biométrica no es suprimida completamente.

Por las razones anteriormente anotadas este Despacho considera que el Formato de Consentimiento de Datos Biométricos dispuesto por Worldcoin para el tratamiento de los datos personales sensibles no cumple con los parámetros establecidos en la Ley 1581 de 2012 y sus normas reglamentarias, en lo que tiene que ver con la información que debe entregar el responsable sobre las finalidades del tratamiento.

15.4. Deber de contar con la Política de Seguridad en el Tratamiento de los Datos Personales.

Mediante Oficio No. 24-240075-01 de fecha 11 de junio de 2024, esta Dirección, solicitó a las investigadas se aportara copia de la Política de la Seguridad de La información desarrollada e implementada por las investigadas. Así mismo informaran si dicha política es objeto de revisión, evaluación y seguimiento permanente.

El Oficial de Protección de Datos de Tools For Humanity Corporation, mediante Oficio No. 24-240075-05 del 2 de julio de 2024, dio respuesta en los siguientes términos:

> *"Algunas políticas de privacidad y seguridad están siendo revisadas y puestas a punto en este momento en vista de recientes adiciones de nuestro Director de Seguridad de la Información y nuestro Director de Privacidad. Por ello, tan pronto como culmine ese trabajo, estaremos más que dispuestos a proporcionarle las políticas actualizadas".*

Los apoderados de las entidades investigadas, en el escrito de alegatos de conclusión, respecto de las medidas de seguridad implementadas por sus representadas, indicaron:

> *"Aun cuando el régimen de protección de datos en Colombia no exige específicamente una Política de Seguridad en el Tratamiento de los Datos Personales ni determina el contenido que debe contener**, se aporta como prueba una política escrita que describe los procedimientos y los lineamientos desarrollados para asegurar que los datos relacionados con los Servicios de World se protegen. Esta política se aplica estableciendo estándares e implementando procedimientos para garantizar la confidencialidad, integridad y disponibilidad de los datos.***
>
> *Las Entidades, **conforme al principio de seguridad dispuesto por la Ley 1581 de 2012, han adoptado medidas técnicas y organizacionales para reducir el riesgo y prevenir la adulteración, la pérdida, la consulta, el uso o el acceso no autorizado o fraudulento a información.** Las Entidades llevan a cabo una revisión periódica de todas las medidas de seguridad para asegurar que sean adecuados y de vanguardia, considerando la naturaleza, el alcance, el contexto y los propósitos del tratamiento, así como la variabilidad en el riesgo de probabilidad y la separabilidad de los derechos y las libertades de personas naturales. A continuación, encontrará una lista general de algunas medidas técnicas y organizacionales ("TOM")" (Negrilla fuera de texto)*

RECOPILACIÓN DE DATOS – DATOS PERSONALES		
TOM	**Descripción**	**Cómo la Prueba de Humanidad del Orb cumple con esto**
Garantizar que los datos estén completos	Verificar que los campos que componen el formulario de recogida de datos permiten el registro completo de los datos requeridos.	Pruebas de detección de fraude y pruebas de calidad de imagen realizadas por modelos de IA en el Orb.
Minimizar los errores de registro de datos	Indicar de forma clara y específica el tipo de información que se va a registrar y su formato.	El proceso automatizado de recopilación de datos que no permite el registro manual de datos minimiza los riesgos de errores de registro de datos.
Garantizar la integridad	Verificar la exactitud de los datos introducidos si el tipo de registro lo permite (por ejemplo, formato de fecha: DD/MM/AAAAA).	Pruebas de detección de fraude y pruebas de calidad de imagen realizadas por modelos de IA en el Orb.
Garantizar la confidencialidad durante el proceso de recolección de datos	Cifrar la comunicación cliente-servidor durante la recopilación.	Toda la comunicación entre el Orb y el backend del Orb o el dispositivo del usuario y el backend del Orb está encriptada con TLS.
Limitar el acceso a la recolección de datos	Limitar la caché del formulario al cliente solo en el momento de la carga de datos. Limitar la carga de datos al cliente a una sola sesión de usuario.	No hay caché posible en el Orbe. La carga de datos se limita a una sesión de verificación en particular.
Limitar el acceso no autorizado durante la recolección de datos	Utilizar certificados digitales seguros validados por entidades autorizadas.	El firmware de Orb se audita y se basa en HSM estándar de la industria validados por entidades autorizadas.
Para datos sensibles: limitar el acceso no autorizado durante la recolección	Cifrar la comunicación durante la transferencia desde la aplicación del servidor a la base de datos.	Los Códigos de Iris se transmiten a través del cifrado TLS.

CONTROL DE ACCESO – DATOS PERSONALES	
TOM	**Cómo la Prueba de Humanidad del Orb cumple con esto**
Gestión de accesos	Los derechos y roles de acceso a los datos sensibles de los usuarios se otorgan en un proceso formalizado. Evitamos la escalada no autorizada de privilegios de acceso y roles en el contexto de datos sensibles de usuarios al requerir que dos personas separadas confirmen cada escalada de privilegios. Esto evita el abuso de privilegios. Todos los derechos y roles de acceso a los datos confidenciales de los usuarios se revisan cada tres meses.
Permisos de acceso	Implementamos un servicio central de gestión de acceso a la identidad (IAM) que integra el inicio de sesión único (SSO) en todos los flujos de autenticación para el acceso a las bases de datos y los servicios que acceden a esas bases de datos. Esto permite una restricción de acceso basada en roles para garantizar la limitación de acceso. No se puede acceder a ningún recurso interno sin que se le asigne previamente el acceso al recurso, lo que evita el acceso no autorizado. El inicio de sesión en el SSO requiere el uso de una contraseña segura y el uso de una clave de hardware con un segundo factor.
Autorización de acceso	Todos los miembros del equipo se autentican en el SSO con autenticación multifactor. Los dispositivos de los miembros del equipo reciben controles de seguridad antes de obtener acceso a cualquier información confidencial. Todo el acceso y la autorización se registra y supervisa para detectar comportamientos abusivos y para garantizar que se aplique el principio de acceso con privilegios mínimos.
Control de acceso	Todo el acceso a los recursos internos solo se concede en función de la necesidad de conocerlos. Cada privilegio de acceso se otorga a través de un proceso formalizado en el que se revisa que el miembro del equipo en cuestión requiere acceso al recurso en particular.
Monitoreo de acceso	Cada intento de acceso a los recursos que contiene datos confidenciales del usuario se registra y analiza en busca de irregularidades.

COPIA DE SEGURIDAD Y RECUPERACIÓN: DATOS PERSONALES	
TOM	**Cómo la Prueba de Humanidad del Orb cumple con esto**
Garantizar una copia de seguridad formal y proceso de recuperación	• Se ha puesto en marcha un plan de continuidad del negocio • Los proveedores de alojamiento con certificación ISO 27001 y SOC2 garantizan las copias de seguridad
Garantizar el acceso a los medios de comunicación control	• Los proveedores de alojamiento con certificación ISO 27001 y SOC2 garantizan el almacenamiento seguro de las copias de seguridad
Garantizar el acceso a los medios de comunicación control	• Se ha puesto en marcha un plan de continuidad del negocio • Los proveedores de alojamiento con certificación ISO 27001 y SOC2 garantizan las copias de seguridad • La ubicación de almacenamiento principal de los datos de Orb es el dispositivo del usuario individual (descentralización).

GESTIÓN DE VULNERABILIDADES – DATOS PERSONALES	
TOM	**Cómo la Prueba de Humanidad del Orb cumple con esto**
Evitar exfiltraciones de datos desde el diseño	• Cifrado en tránsito, en reposo y a nivel de datos • Control de acceso • Formación y sensibilización
Detectar posibles exfiltraciones de datos	Registro estricto e implementación de un sistema de gestión de información de seguridad. Existen políticas y protocolos de violación de datos.
Garantizar una adecuada protección	• SMPC anonimiza los datos de los datos del iris • Las pruebas de conocimiento cero evitan la vinculación de datos • Los filtros de inyección de código no son relevantes ya que la entrada de datos no es manual • La intrusión en la red se aborda a través de firewalls • La detección de intrusos se aborda mediante un registro estricto y la implementación de un sistema de gestión de información de seguridad
Garantizar la eficacia y duradero de las medidas	Auditorías internas y externas periódicas. Por ejemplo, las auditorías publicadas a continuación: • Auditoría SMPC (Informe de Auditoría de Autoridad Mínima)[69]. • Auditorías de protocolo y ZKPs (Nethermind)[70] y (Least Authority)[71].
	• Auditorías de Orbs (Informe de auditoría de Trail of Bits)[72].

- **Política de Seguridad de la Información Escrita. Tools For Humanity Corporation.**

En primer lugar, se describen los objetivos y finalidades de la política, de lo cual se destaca:

> *Esta Política de seguridad de la información escrita ("PSIE") es una representación de los estándares establecidos en Worldcoin (o la "Empresa") para garantizar la confidencialidad, integridad y disponibilidad de los datos de Worldcoin. Los procedimientos y directrices establecidos en esta PSIE se desarrollaron para garantizar que los datos de Worldcoin permanezcan protegidos de una manera consistente con los estándares de la Empresa. La protección de los sistemas en los que se procesan, almacenan o transmiten los datos de Worldcoin es de igual importancia para la Empresa. Como tal, cualquier referencia a datos en esta PSIE incluye los sistemas de la Empresa.*
>
> *El desarrollo de políticas es necesario para apoyar la gestión de riesgos en las operaciones diarias de la Empresa. Esta PSIE es un reflejo de las políticas bajo las cuales Worldcoin opera y salvaguarda sus datos para minimizar los riesgos. Worldcoin se esforzará por identificar posibles riesgos de forma continua y, cuando sea apropiado, desarrollará políticas para minimizar la exposición a dichos riesgos.*

Así mismo, indica que la política se aplica a (i) todo personal, contratista, colaborador o cualquier otra persona de Worldcoin que esté involucrada en los negocios de la organización. (ii) todas las ubicaciones definidas del negocio de Worldcoin, así como otras ubicaciones mientras se trabaja con copias físicas o digitales de datos; (iii) cualquier sistema o software utilizado para el procesamiento de datos de World Foundation incluidos, entre otros: extremos administrados (PC, portátiles, dispositivos móviles) servidores y redes, servicios en la nube y SaaS.

En lo que tiene que ver con datos, la citada política indica lo siguiente:

> *"Los empleados deben comprender los criterios de la Empresa sobre lo que se considera confidencial para poder gestionar adecuadamente los datos de la Empresa. En la siguiente tabla se clasifican los datos de Worldcoin para proporcionarles a los empleados una comprensión de los tipos de datos clasificados como confidenciales en la Empresa. Los datos identificados a continuación no son una lista exhaustiva de los tipos de datos que la Empresa mantiene, de los cuales es responsable o que gestiona. Para reducir cualquier margen de error, cualquier dato no clasificado específicamente a continuación, el cual sea creado en Worldcoin o recibido por los empleados de Worldcoin en el desempeño de sus labores, debe tratarse como confidencial.*

Se realiza en este punto alusión a los datos personales y sensibles del usuario (sin que se pueda determinar a tipo de usuario se refiere), así:

DATOS PERSONALES Y SENSIBLES DEL USUARIO	
Definición: información de identificación personal y datos biométricos confidenciales (como imágenes del iris y código de iris) que pueden atribuirse a una persona. Se trata de información confidencial (véase a continuación), pero está sujeta a un escrutinio gubernamental adicional.	Posible impacto de la pérdida: además de los impactos que se indican a continuación para la Información Confidencial, es probable que Worldcoin esté sujeto al escrutinio de la autoridad de privacidad de datos pertinente si se produce una violación de datos relacionada con esta clase de datos.
• Información de identificación personal de nuestros usuarios. • Información recopilada durante el proceso de registro (correo electrónico, ID de usuario y otros datos de la cuenta).	• Datos biométricos (imagen del iris, código de iris). • Imágenes faciales y otros metadatos (en la medida en que sean información de identificación personal).
CONFIDENCIAL	
Definición: datos muy valiosos y altamente sensibles que podrían afectar negativamente a Worldcoin si se pusieran a disposición del público.	**Posible impacto de la pérdida:** el impacto puede afectar negativamente la posición competitiva de Worldcoin, violar requisitos legales o regulatorios, violar requisitos contractuales, dañar la reputación de la Empresa y causar pérdidas financieras.
• Información de identificación personal (PII) que no está en la categoría anterior. • Plan de negocios y estrategia de mercadeo. • Datos financieros relacionados con la generación de ingresos y la elaboración de presupuestos. • Promociones de mercadeo en desarrollo • Combinaciones de nombre de usuario y contraseña. • Tokens de hardware o software (autenticación multifactor). • Configuración del sistema. • Direcciones IP internas. • Acuerdos entre terceros y empleados. • Datos financieros estratégicos u operativos. • Datos de la declaración del impuesto de sociedades.	• Documentación legal y facturación. • Datos de fusiones y adquisiciones no anunciados. • Secretos comerciales (por ejemplo, diagramas de diseño, datos competitivos, etc.). • Propiedad Intelectual. • Datos de pago electrónico (pago por transferencia bancaria o ACH). • Cheques de pago. • Incentivos o bonificaciones (montos o porcentajes). • Acuerdos de compra de tokens. • Datos de la cuenta bancaria. • Actividad relacionada con la inversión. • Información de la cuenta. • Información sobre montos de deuda.
PÚBLICA	
Definición: los datos han sido aprobados para su divulgación al público en general o están generalmente disponibles para el público.	**Posible impacto de la pérdida:** el impacto no sería perjudicial ni representaría un riesgo para las operaciones comerciales.
• Sitios web con acceso a Internet (por ejemplo, sitio web de la empresa. • Notas de Prensa aprobadas (redes sociales, blogs, etc.).	

Finalmente hace referencia a los siguientes aspectos:

- Derechos de acceso y administración, en el que se informa que los datos de Worldcoin se almacenan en soluciones de terceros.
- Incorporación y Cese, refiriéndose a los movimientos de personal que se realice al interior de la empresa.
- Acceso a la información de manera remota y al correo electrónico.
- Teletrabajo, y el horario de trabajo de los empleados de Worldcoin.
- Directrices generales relacionadas con el uso de contraseñas.
- Restricciones en el acceso.
- Almacenamiento de información confidencial.
- Gestión de datos confidenciales fuera de las instalaciones.
- Manejo de los computadores y cuentas personales.
- Gestión de contraseñas.
- Gestión de Dispositivos móviles.
- Gestión de activos.
- Gestión de inventario de hardware.
- Gestión de inventario de Software.
- Medios extraíbles.
- Acceso físico.
- Seguridad de redes y sistemas.
- Copia de seguridad y retención de datos.
- Destrucción de datos.
- Gestión de riesgos de terceros.

Conforme lo anterior, encuentra el Despacho, en primer lugar, que dicha política tiene fecha de expedición agosto de 2021, sin que pueda determinarse si ha tenido algún tipo de actualización desde que se inició la operación de World en Colombia.

Así mismo, hace referencia a los códigos de conducta que deben seguir los empleados de Worldcoin frente a la información que se maneje al interior de la empresa, pero no menciona lo relacionado con la recolección y procesamiento de los datos personales biométricos.

- **Privado por Diseño.**

En el citado documento, se relacionan los principios de privacidad de World. Este documento tuvo su última actualización el 18 de septiembre de 2024

Respecto a la seguridad de la información se informa lo siguiente:

> ***Seguridad.***
>
> *Worldcoin se trata de permitir que las personas estén en línea sin que se expongan sus identidades y capacitarlas para distinguir entre interacciones con bots e interacciones humanas. La seguridad ayuda a garantizar que se alcance ese nivel de privacidad, siempre y sin falta.*
>
> *World ID utiliza muchas técnicas de seguridad para garantizar la seguridad de los datos de los titulares de World ID.*
>
> *Un conjunto incluye herramientas humanas como el código abierto y las auditorias (consulte sección "Transparencia"), que ayudan a validar y poner a prueba las medidas de seguridad que se han creado e implementado.*
>
> *El otro conjunto incluye herramientas criptográficas, como ZKP y SMPC (consulta la sección "Anonimato"), que utilizan matemáticas avanzadas para proteger los datos, cifrarlos y mantenerlos privados o hacerlos anónimos.*
>
> *SMPC es uno de los pocos resultados en criptografía que puede proporcionar un secreto perfecto. Los ZKP, por su parte, usan hash de anulación o valores únicos para cada aplicación, de modo que no se pueda rastrear el historial.*
>
> ***Anonimato.***
>
> ***Computación multipartita segura (SMPC)***

> *Solo se necesita un teléfono inteligente para crear un World ID, pero probar que el titular es un humano único que no ha creados varios World ID mientras mantiene su identidad privada es un desafío complicado.*
>
> *Los datos biométricos, cuando se anonimizan adecuadamente, proporcionan la solución. La utilidad misma de los datos biométricos significa que deben ser recogidos y utilizados mínimamente y, cuando es el único camino viable, debe ser manejado con cuidado.*
>
> *Worldcoin lo hace a través de la SMPC.*
>
> *Cuando una persona verifica su World ID a través de un Orb, el Orb toma fotos de su iris y cara. Utiliza estas imágenes para hacer un código de iris, que es esencialmente una serie de números 1 y 0. No hay dos códigos de iris iguales ni revelan identificadores directos como nombre, sexo, edad, etc.*
>
> *Este código de iris se divide en diferentes piezas y se cifra permanentemente mediante la SMPC, lo que hace que los datos sean anónimos, dividiéndolos en múltiples valores abstractos (participaciones en SMPC) y almacenándolos en ubicaciones separadas administradas por dos entidades legalmente distintas. En un futuro próximo se añadirán socios de almacenamiento adicionales (incluidas universidades y organizaciones sin fines de lucro), lo que significa que los códigos de iris se dividirán en valores aún más abstractos almacenados y gestionados por entidades aún más independientes. Ninguna parte tiene acceso a una parte de un código de iris. Más bien, solo tienen acceso a la parte de la SMPC almacenada bajo su control y gestión.*
>
> *Si bien almacenar los datos en varias ubicaciones aparentemente aumentaría la probabilidad de que esos datos sean robados, lo cierto es todo lo contrario. Las acciones de SMPC se almacenan de tal manera que, si un actor malintencionado tuviera acceso a una acción de SMPC, sería indescifrable; solo tienen sentido cuando se juntan todas las piezas.*

De acuerdo con el citado documento, la implementación del **SMPC**[29] brinda la seguridad requerida para evitar cualquier circunstancia que ponga en riesgo la integridad del código de iris almacenado. **No obstante, no impide que se realice la comparación entre diferentes códigos para evitar un doble registro en la World ID o algún tipo de fraude relacionado con el modelo de negocio de World Foundation.**

Pero, si el código de iris es fragmentado y enviado a repositorios manejados por terceros, ¿qué método utiliza World para realizar la comparación de la cual se hizo mención anteriormente? ¿Existirá una base de datos paralela que contenga la información completa para ser consultada y realizar la comparación? Este es un aspecto que no es objeto de pronunciamiento por parte de World Foundation.

Independientemente de la división que del código de iris se realice, entiende el Despacho que cada fragmento deberá contener información biométrica suficiente para realizar una eventual comparación, por lo que siempre estará vinculado a la persona a quien pertenece, y siempre podrá ser consultada.

Adicionalmente, teniendo en cuenta la naturaleza de la Computación Multipartita Segura (SMPC), es perentorio que el titular tenga conocimiento sobre cómo será tratada y almacenada su información biométrica.

Al respecto, este Despacho pudo verificar que en el formato de consentimiento de datos biométricos en sus versiones 1.16 del 12 de junio de 2024[30] y 1.18 del 30 de septiembre de 2024[31], no se informa a los titulares respecto del protocolo **SMPC** utilizado por World. Sin embargo, de acuerdo con el Estudio de Impacto realizado por Least Authority, éste se encuentra en funcionamiento desde el mes de mayo de 2024, fecha en la cual inició su operación en Colombia.

---

[29] **SMPC:** "*Este es un protocolo criptográfico que, mediante la Compartición Aditiva de Secretos, permite segmentar un dato secreto en distintas partes, de manera que, al compartirse los datos, no pueda ser revelado el dato original por ninguna de las fuentes.*" **Consultado en:** https://www.aepd.es/prensa-y-comunicacion/blog/privacidad-desde-el-diseno-computacion-segura-multi-parte-comparticion. 22-09-2025.

[30] Este formato de consentimiento de datos biométricos fue revisado en el Acta de Preservación No. 087 del 8 de julio de 2024.

[31] Este formato de consentimiento fue allegado por los apoderados con el escrito de Alegatos de conclusión, presentado el 15 de octubre de 2024.

H.4	**Fugas biométricas**	**Computación segura multipartita (SMPC):** Al implantar SMPC, la Compañía garantiza que los datos biométricos se almacenan de forma anónima e irreversible, de modo que incluso si se filtrara una base de datos de SMPC, los datos serían inútiles y no podrían utilizarse para identificar al titular de los datos.	**Plena aplicación desde mayo de 2024** ☑

Sólo hasta la versión No. 1.22 del 2 de diciembre de 2024[32], se incluyó información relacionada con el citado protocolo de cifrado de los códigos de iris recolectados, para lo cual el titular deberá acceder a un link, tal como puede observarse a continuación:

> **¡Importante!** Recopilamos estos Datos de imagen para determinar que usted sea un ser humano único. En otras palabras, el sistema está diseñado para confirmar que usted es un ser humano real (vitalidad) y que esta es la primera vez que visita un Orb (singularidad).**No utilizamos los Datos de imagen para saber *quién* es usted (identificación).**
>
> **Anonimizamos su código de iris dividiéndolo en fragmentos que almacenan terceros de confianza en un cálculo multiparte. Puede encontrar aquí más información al respecto:**https://world.org/blog/announcements/worldcoin-foundation-unveils-new-smpc-system-deletes-old-iris-codes
>
> Los datos que recopilamos (descritos anteriormente) pueden considerarse o no datos personales o biométricos dependiendo de las leyes aplicables en su lugar de residencia. Sin embargo, en lo que respecta a la seguridad, los tratamos como datos biométricos y los gestionamos con un mayor grado de seguridad y cuidado. La base jurídica para la recopilación de Datos de imágenes es su consentimiento explícito. La base jurídica para calcular los Derivados de esos Datos de imágenes (como el Código de iris) y anonimizarlos para compararlos activamente con nuestra base de datos es su consentimiento explícito.

Lo que no resulta claro para el Despacho es, en lo que respecta al principio y deber de seguridad, qué tipos de medidas preventivas, han sido implementadas por las investigadas respecto de los terceros que intervienen en la custodia de los fragmentos de los códigos de iris. Tampoco se indican los tipos de riesgos que este tipo de protocolo traería para el tratamiento de los datos personales sensibles.

En lo que tiene que ver con el principio de seguridad y el deber que respecto de su ejercicio tienen los Responsables, los literales a), d) y k) del artículo 17 de la Ley 1581 de 2012, disponen lo siguiente:

> ***ARTÍCULO 17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO.*** *Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:*
>
> *a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;*
>
> *d)* ***Conservar la información bajo las condiciones de seguridad*** *necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;*
>
> *k)* ***Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley*** *y en especial, para la atención de consultas y reclamos;*

Los literales a) y g) respecto de los principios del tratamiento de datos personales, disponen:

> ***ARTÍCULO 4o. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES.*** *En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:*
>
> *a)* ***Principio de legalidad en materia de Tratamiento de datos:*** *El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen;*
>
> *g)* ***Principio de seguridad:*** *La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;*

[32] Este formato de consentimiento de datos biométricos fue revisado en el Acta de Preservación No. 214 del 16 de diciembre de 2024.

Por su parte el artículo 2.2.2.25.6.1 del Decreto 1074 de 2012, determina:

> ***ARTÍCULO 2.2.2.25.6.1. Demostración.*** *Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que* ***han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este capítulo, en una manera que sea proporcional a lo siguiente:***
> *1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.*
> *2. La naturaleza de los datos personales objeto del tratamiento.*
> *3. El tipo de Tratamiento.*
> *4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.*
> *En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, cómo también la descripción de las finalidades para las cuáles esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso.*
> ***En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas.***

Efectivamente, de conformidad con lo establecido en el literal g) del artículo 4 de la Ley 1581 de 2012, la información sujeta a tratamiento por el Responsable, debe ser manejada con las medidas técnicas, humanas y administrativas necesarias para otorgar **seguridad** a los registros, y así evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Nótese que **el principio de seguridad tiene un criterio eminentemente preventivo**, lo cual obliga a los Responsables o Encargados a adoptar medidas apropiadas y efectivas para **evitar** afectaciones a la seguridad de la información sobre las personas.

Frente al citado principio la Corte Constitucional, mediante Sentencia C-748 de 2011, manifestó lo siguiente:

> ***" 2.6.5.2.7. Principio de seguridad:*** *Al amparo de este principio, la información sujeta a tratamiento por el responsable o encargado, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*
>
> *De este principio se deriva entonces la responsabilidad que recae en el administrador del dato. El afianzamiento del principio de responsabilidad ha sido una de las preocupaciones actuales de la comunidad internacional, en razón del efecto "diluvio de datos"[240][33], a través del cual día a día la masa de datos personales existente, objeto de tratamiento y de ulterior transferencias, no cesa de aumentar. Los avances tecnológicos han producido un crecimiento de los sistemas de información, ya no se encuentran sólo sencillas bases de datos, sino que surgen nuevos fenómenos como las redes sociales, el comercio a través de la red, la prestación de servicios, entre muchos otros. Ello también aumenta los riegos de filtración de datos, que hacen necesarias la adopción de medidas eficaces para su conservación. Por otro lado, el mal manejo de la información puede tener graves efectos negativos, no sólo en términos económicos, sino también en los ámbitos personales y de buen nombre.*
>
> *En estos términos, el Responsable o Encargado del Tratamiento debe tomar las medidas acordes con el sistema de información correspondiente. Así, por ejemplo, en materia de redes sociales, empieza a presentarse una preocupación de establecer medidas de protección reforzadas, en razón al manejo de datos reservados. En el año 2009, el Grupo de Trabajo Sobre Protección de Datos de la Unión Europea señaló que en los Servicios de Redes Sociales" o "SRS debe protegerse la información del perfil en el usuario mediante el establecimiento de "parámetros por defecto respetuosos de la intimidad y gratuitos que limiten el acceso a los contactos elegidos". [241][34]*

---

[33] [240] El término es utilizada por el Dictamen 3/2010 sobre el principio de responsabilidad, emitido por el Grupo de Protección de Datos de la Unión Europea.

[34] [241] La seguridad, es uno de los elementos que debe contar con las garantías necesarias de protección de datos personales en los SRS. En consecuencia, el Grupo de Trabajo diseñó ciertos parámetros bajo los cuales el acceso a la información personal en redes sociales debe estar protegido, pues de no ser así, generaría desconfianza en el usuario, al no tener la certeza de que su información no va a ser tratada adecuadamente. Al especto se indicó: "Los SRS deberían pues establecer parámetros por defecto respetuosos de la intimidad, que permitan a los usuarios aceptar libre y específicamente que personas distintas a sus contactos elegidos accedan a su perfil, con el fin de reducir el riesgo de un tratamiento ilícito por terceros. Los perfiles de acceso ilimitado no deberían ser localizables por los motores de búsqueda internos, incluso por la función de búsqueda por parámetros como la edad o el lugar (…)".

Concordante con lo anterior, el principio acceso y circulación restringida[35] establece que el Tratamiento se sujeta a los límites que se derivan de la naturaleza de los Datos personales, de las disposiciones de la ley y la Constitución Política. En este sentido, el Tratamiento solo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la ley.

En la mencionada sentencia, en lo que tiene que ver con el citado principio, precisó:

> ***2.6.5.2.6. Principio de acceso y circulación restringida:*** *En razón de esta directriz, el Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, éste sólo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la presente ley. Además, se prohíbe que los datos personales, salvo información pública, se encuentren disponibles en Internet, a menos que se ofrezca un control técnico para asegurar el conocimiento restringido.*
>
> *En relación con* ***el primer inciso****, deben hacerse las siguientes precisiones. Como se explicó anteriormente, esta Ley Estatutaria, al establecer las condiciones mínimas en el manejo de la información, no agota la regulación en materia de habeas data, y por tanto, el Tratamiento estará también sujeto a la normatividad que se expida posteriormente.*
>
> *En cuanto* ***al segundo inciso****, la norma debe entenderse que también se encuentra prohibida toda conducta tendiente al cruce de datos entre las diferentes bases de información, excepto cuando exista una autorización legal expresa, es decir, lo que la jurisprudencia ha denominado el* ***principio de individualidad*** *del dato. Como consecuencia de lo anterior, queda prohibido generar efectos jurídicos adversos frente a los Titulares, con base,* ***únicamente*** *en la información contenida en una base de datos.*
>
> *De otra parte, y en relación con ese segundo inciso, uno de los interviniente solicita a esta Corporación, declarar su constitucionalidad bajo los siguientes condicionamientos:* ***(i)*** *se debe evitar que los datos privados, semiprivados, reservados o secretos puedan estar junto con los datos públicos, y por tanto, los primeros no pueden ser objeto de publicación en línea, a menos que se ofrezcan todos los requerimientos técnicos y* ***(ii)*** *se debe eliminar cualquier posibilidad de acceso indiscriminado, mediante la digitación del número de identificación a los datos personales del ciudadano.*
>
> *Considera la Sala que tales condicionamientos no son necesarios, por cuanto la misma norma elimina estas posibilidades. En efecto:* ***(i)*** *prohíbe que los datos no públicos sean publicados en Internet y* ***(ii)*** *sólo podrían ser publicados si se ofrecen todas las garantías. De lo anterior se infiere que si el sistema permite el acceso con la simple digitación de la cédula, no es un sistema que cumpla con los requerimientos del inciso segundo del literal f) del artículo 4.*
>
> *Sin embargo,* ***debe reiterarse que el manejo de información no pública debe hacerse bajo todas las medidas de seguridad necesarias para garantizar que terceros no autorizados puedan acceder a ella. De lo contrario, tanto el Responsable como el Encargado del Tratamiento serán los responsables de los perjuicios causados al Titular.***
>
> *De otra parte, cabe señalar que aún cuando se trate de información pública, su divulgación y circulación está sometida a los límites específicos determinados por el objeto y finalidad de la base de datos.*

Por su parte, el principio de confidencialidad agrega un sentido más de responsabilidad a quienes realizan el tratamiento de datos personales, pues, de acuerdo con su definición, *"[t]odas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento[36]"*

Bajo este entendido es que, los Responsables del tratamiento de datos personales deben tener implementadas las medidas necesarias para que incidentes de seguridad, no ocurran. Resulta necesario entonces, la

---

[35] ARTÍCULO 4o. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES. En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:
f) Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente ley y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la presente ley;
Los datos personales, salvo la información pública, no podrán estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o terceros autorizados conforme a la presente ley;

[36] Literal h) del artículo 4 de la Ley 1581 de 2012.

reglamentación y desarrollo de diferentes mecanismos que comprometan a los colaboradores en la labor de proteger el derecho de Habeas Data.

Respecto de la Política de Seguridad de la Información escrita de Tools For Humanity Corporation, sobre la cual hace referencia los apoderados en su escrito, tal como atrás se dijo, no se establecen las medidas de seguridad requeridas para el tratamiento de los datos personales en la operación misma de Worldcoin respecto de la recolección de los datos biométricos de los titulares.

Adicionalmente, en lo que tiene que ver con el SMPC (Computación Multipartita Segura), implementado por Worldcoin como medida de seguridad de los códigos de iris recolectados, en primer lugar, no le fue informado a los titulares, que sus códigos de iris serían divididos en partes y que serían entregados para su custodia a terceros de los cuales no se tiene conocimiento, la implementación del protocolo SMPC dificulta el conocimiento de los datos biométricos por parte de un tercero no autorizado, sin embargo, si este logra conseguir suficientes partes del código podría reconstruir el dato biométrico, por ejemplo, mediante la materialización de un incidente de seguridad, además se adquiere una dificultad técnica en lo relacionado con la supresión completa de los datos que se encuentran en entornos distribuidos. Tampoco se detalla los procedimientos implementados para supervisar y así determinar que los datos personales sensibles no se encuentran bajo algún riesgo que pueda afectar su integridad.

Se debe tener en cuenta que cada entidad participante, que actualmente son: "*University of Erlangen-Nuremberg, UC Berkeley center for Responsible Decentralized Intelligence y la empresa Nethermind*" (empresas, universidades, ONG) tendrán diferentes capacidades técnicas y presupuestales, por lo que no todas podrán contar con altos niveles de seguridad, por lo que, si no se establecen medidas de seguridad estrictas y controles, auditorías y sistemas de monitoreo claros se puede ver comprometida la información almacenada por ese tercero, lo que puede llevar a un compromiso de toda la red de encargados actuales y futuros.

15.5. Deber de contar con la Política de Gestión del Riesgo en el Tratamiento de los Datos Personales.

Sostiene la apoderada de World Foundation respecto del cargo formulado lo siguiente:

> *"La SIC sostiene que, en la respuesta al requerimiento de información, el Oficial de Protección de Datos de TFH indica que "el Responsable" no tiene implementada una política de gestión del riesgo de la información que cumpla con los postulados descritos en las normas de protección de datos personales. Sin embargo, en la respuesta al requerimiento de información en ningún momento se hizo un reconocimiento al respecto, sino que se mencionó que algunas políticas de privacidad y seguridad están siendo revisadas y puestas a punto por parte del Director de Seguridad de la Información y el Director de Privacidad de TFH[73]. Este equipo supervisa los programas de privacidad y seguridad que garantizan el tratamiento adecuado de los datos personales, incluidas las políticas, la formación, la respuesta a incidentes, la gobernanza y las medidas de información.*
>
> *Las normas de protección de datos en Colombia no exigen una Política de Gestión del Riesgo en el Tratamiento de Datos Personales, por lo que no es claro qué debe contener una de estas políticas en criterio de la SIC. Tampoco encontramos precedentes que sancionen a una compañía por no contar con este documento, y ningún análisis de la SIC como autoridad de protección de datos al respecto.*
>
> *Sin embargo, debe mencionarse que WF llevó a cabo una evaluación del impacto de la protección de datos ("DPIA") relacionado con los datos sensibles que se procesan en el contexto de la verificación del Orb. Este DPIA inició el 05 de mayo de 2024 y terminó el 17 de septiembre de 2024. El DPIA se enfoca en la verificación de la Prueba de Humanidad mediante el Orb, que permite que el usuario obtenga la World ID.*
>
> *El DPIA cumple la función de una Política de Gestión del Riesgo del Tratamiento de Datos Personales. Este documento se centra en evaluar el impacto que un proyecto, proceso o tecnología tiene sobre la privacidad y la protección de datos, lo que permite anticipar posibles vulnerabilidades y adoptar medidas preventivas para minimizar dichos riesgos. Esta función de evaluación es uno de los pilares esenciales de cualquier política de gestión del riesgo.*
>
> *Asimismo, el DPIA establece un marco estructurado para analizar los riesgos. Esto incluye una evaluación detallada de las posibles amenazas que puedan surgir en el ciclo de vida*

> *del tratamiento de datos, como la recolección, almacenamiento, uso y eliminación de la información personal (Sección G, Evaluación del impacto)75. El DPIA no solo identifica los riesgos, sino que también evalúa su severidad y la probabilidad de que ocurran, permitiendo priorizar las medidas de mitigación.*
>
> *El DPIA ofrece recomendaciones claras y prácticas para mitigar los riesgos identificados, lo cual es un componente clave de cualquier política efectiva de gestión de riesgos (Sección H, Soliciones). Estas recomendaciones incluyen la implementación de medidas técnicas y organizativas encaminadas a salvaguardar los datos de los titulares".*

Teniendo en cuenta lo indicado por los apoderados de World Foundation y Tools For Humanity Corporation, este Despacho procedió a analizar las diferentes auditorias relacionadas con los posibles riesgos que se puedan presentar en el tratamiento de los datos personales.

- **Informe de Auditoría de seguridad del Protocolo MPC para la verificación de unicidad.**

La citada auditoria tuvo como fecha final de elaboración el 4 de abril de 2024 y consiste en la realización de una auditoria de seguridad de su protocolo MPC para la verificación de unicidad.

Frente al **Alcance** de la auditoria el equipo encargado de realizar la auditoria informó:

> *"Nuestro equipo revisó la primera versión del Protocolo MPC, que aún carece de ciertos componentes relevantes para la seguridad. El equipo de Worldcoin señaló que está prevista una segunda versión del Protocolo MPC, que introducirá, por ejemplo, el cifrado de las consultas que contienen partes del código de iris. Por lo tanto, recomendamos realizar una auditoría de seguridad exhaustiva y de seguimiento del Protocolo MPC una vez que se complete el desarrollo de la versión 2. Además, nuestro equipo no verificó la exactitud de la especificación. También, recomendamos realizar una auditoría de especificaciones de la versión final de la especificación del protocolo MPC, que debe incluir una prueba de seguridad".*

Respecto de los problemas específicos y frente a las sugerencias realizadas, se indica que las mismas fueron resueltas por el equipo de Worldcoin.

- **Informe de auditoría de seguridad de la criptografía del protocolo Worldcoin.**

Para la auditoría la compañía Least Authority encargada por Tools For Humanity Corporation, realizó una investigación, indagación y revisión de la implementación criptográfica del protocolo de World. La fecha final de entrega fue el 26 de julio de 2023.

De acuerdo con el documento allegado, la siguiente imagen representa los problemas o sugerencias evidenciados y el estado de los mismos:

PROBLEMA o SUGERENCIA	ESTADO
Problema A: los valores secretos no se reducen a cero	Resuelta
Problema B: la curva BN254 no proporciona suficiente seguridad	Sin resolver-Planificado
Problema C: la generación actual de la CRS hace que las pruebas sean inseguras	Resuelta
Sugerencia 1: no almacenar ni acceder a secretos en las variables de entorno	Resuelta
Sugerencia 2: configurar los parámetros de la función hash de Poseidon para un nivel de seguridad de 128 bits	Sin resolver-Planificada
Sugerencia 3: eliminar código no utilizado de la base de código	Resuelta
Sugerencia 4: crear una Especificación Técnica de Semaphore para el caso de uso de Worldcoin	Resuelta
Sugerencia 5: cambiar el mecanismo de firma del servicio de administración de claves de AWS	Sin resolver-Planificada
Sugerencia 6: resolver los elementos *TODO* en la base de código	Parcialmente resuelta

Llama la atención del Despacho que el problema B no fue resuelto, al igual que las sugerencias 2 y 5, mientras que la número 6 fue parcialmente resuelta, por

lo que para este Despacho la investigada no solucionó los problemas y sugerencias recomendadas por la auditoría sobre la implementación criptográfica del protocolo de World Foundation.

- **Revisión del código de seguridad de aplicaciones del Orb. Evaluación de seguridad.**

La citada evaluación fue realizada por la firma Trail of Bits.[37] El informe final de dicha evaluación se realizó el día 20 de febrero de 2024.

Realizado el análisis conforme los parámetros determinados a la evaluación de la seguridad del software del Orb de World Foundation, fueron detectados 12 problemas:

ID	Título	Gravedad	Dificultad	Estado
1	Los datos de usuario pueden permanecer en el disco si el espacio de intercambio se configura en algún momento.	Informativa	Alta	Parcialmente resuelto
2	Riesgo de que se notifique un espacio de comprobación del estado de SSD incorrecto debido a un desbordamiento de enteros	Baja	Baja	Resuelto
3	Un token caducado para una API inexistente comprobado en el código fuente	Informativa	Indeterminada	Resuelto
4	Problemas de seguridad de memoria en la biblioteca ZBar	Alta	Alta	Resuelto
5	El escáner de códigos QR del Orb está configurado para detectar todos los tipos de códigos.	Media	Alta	Resuelto
6	Los volcados de memoria no están desactivados.	Informativa	Alta	Resuelto
7	Sockets de escritura y lectura de acceso general	Indeterminada	Alta	No resuelto
8	Oportunidades para reforzar la configuración estática del kernel y los parámetros de tiempo de ejecución	Informativa	Alta	Parcialmente resuelto
9	No se verifica la lista descargada de componentes que se deben actualizar.	Informativa	Alta	Resuelto
10	Problemas de seguridad en la configuración de cliente HTTP	Media	Alta	Parcialmente resuelto
11	Las versiones externas de las acciones CI/CD de GitHub no están fijadas.	Media	Media	Resuelto
12	La función *deserialize_message* puede entrar en pánico.	Informativa	Alta	No resuelto

De acuerdo con la gráfica presentada, los riesgos evaluados relacionados en los números 1, 7, 8, 10 y 12, aunque su nivel de gravedad fue clasificado como informativa[38] o indeterminada[39], por lo que no se tiene la certeza de sí para el momento en que inició la operación de World Foundation en Colombia fueron objeto de revisión por parte de las personas encargadas, llegando a su completa solución.

---

[37] Trail Of Baits ofrece servicios de asesoramiento y evaluación técnica de seguridad de algunas organizaciones más específicas del mundo. Combina la investigación de seguridad de alto nivel con una mentalidad de ataque del mundo real para reducir el riesgo y fortalecer el código.

[38] De acuerdo con lo informado en el resultado de la auditoria describe este nivel de gravedad como "El problema no plantea un riesgo inmediato, pero es relevante para las mejores prácticas de seguridad.

[39] Frente al nivel de gravedad indeterminada, se indicó que el alcance el riesgo no se determinó durante este encargo.

- **Evaluación de Impacto de Dato (DPIA) de Worldcoin Foundation sobre el "procesamiento Orb" en el contexto de una Prueba de Identidad Personal.**

La fecha final de la evaluación realizada fue el 17 de septiembre de 2024, la cual se centró "exclusivamente en la verificación de la Prueba de Identidad Personal a través de un dispositivo avanzado de cámara diseñado específicamente ("Orb") y en cómo los datos se procesan de manera segura.

Observa el Despacho que la normativa aplicada para la realización de la evaluación de impacto es el Reglamento General de Protección de Datos aplicable en la Unión Europea. Sería entonces necesario que se realizara una evaluación de impacto del dato, en la cual se tenga en cuenta la normatividad de protección de datos aplicable en el territorio colombiano.

- **Informe de Revisión de Seguridad NM-0112 WORLDCOIN**

Se trata de la evaluación que se realizó respecto de los códigos desarrollados para el funcionamiento del protocolo World ID, auditoría que se llevó a cabo en el mes de julio de 2023.

No es posible determinar si se tuvieron en cuenta las recomendaciones realizadas por la empresa, así mismo, es necesario identificar que los códigos revisados aún se encuentran activos o si han sufrido algún tipo de modificación.

Así las cosas, evidencia el Despacho que, a pesar de contar con una evaluación de riesgos que podría mejorar las medidas de seguridad, su implementación parcial no demuestra su compromiso de mantener la información recolectada bajo las condiciones de seguridad necesaria para evitar riesgos que pongan en peligro, la información biométrica recolectada de los titulares, ni cuentan con medidas robustas, efectivas, eficientes, oportunas, apropiadas útiles y demostrables en el tratamiento de los datos sensibles, que por su naturaleza requieren mayor diligencia y cuidado por parte de los responsables y encargados del tratamiento.

15.6. Deber de contar con el Manual para la Atención y respuesta a las consultas, peticiones y reclamos de los titulares, relacionado con cualquier aspecto del Tratamiento de los Datos Personales.

Respecto del cumplimiento del citado deber, indicaron los apoderados de las investigadas lo siguiente:

> *(…) las Entidades cuentan con un manual interno de políticas y procedimientos denominado "Data Subject Rights Policy" (el "Manual") que se aporta como anexo.*
>
> *El Manual cuenta con procedimientos claros para garantizar el ejercicio efectivo de los derechos de los titulares de datos, en cumplimiento de la normativa colombiana y otros marcos internacionales aplicables. Este documento es de obligatorio cumplimiento para todos los empleados y colaboradores, quienes deben seguir sus lineamientos al atender consultas, peticiones y reclamos relacionados con datos personales.*
>
> *Para asegurar una gestión eficiente y transparente, las Entidades han estado implementado distintos canales de atención. El principal punto de contacto es el Zendesk Privacy Center, una plataforma supervisada por un Privacy Manager y gestionada por un equipo especializado, donde las solicitudes son categorizadas y priorizadas según su naturaleza. Además, cuentan con un formulario de privacidad que recoge la información esencial para procesar cada requerimiento de manera precisa. De manera complementaria, la aplicación World App permite a los usuarios ejercer directamente sus derechos, como la eliminación o rectificación de datos. También disponen de direcciones de correo electrónico para recibir solicitudes, las cuales se integran al sistema Zendesk para garantizar su adecuada gestión.*
>
> *El Manual establece un marco de cumplimiento estricto respecto a los tiempos de respuesta exigidos en cada jurisdicción, incluyendo Colombia, asegurando que todas las solicitudes sean atendidas en los plazos legales establecidos. Con estas medidas, las Entidades garantizan que los derechos de los titulares sean respetados de manera oportuna, transparente y en un lenguaje claro, reafirmando el compromiso de TFH y WF con la protección de datos personales.*
>
> *Adicionalmente, aun cuando las normas de protección de datos personales en Colombia no establecen el detalle de lo que debe contener este manual, las Entidades cuentan con*

> *lineamientos que se reflejan en el formulario de solicitudes y los avisos de privacidad. Por ejemplo, la Sección 13 del Aviso de Privacidad de WF y del Aviso de Privacidad de TFH dispone que para ejercer los derechos o ponerse en contacto con el DPD, el titular puede enviar su solicitud a través del Portal de Solicitudes, a los correos electrónicos pertinentes, o incluso a los domicilios pertinentes.*
>
> *En el formulario de solicitud de datos se puede encontrar que el equipo de soporte se debe comunicar con el titular "lo antes posible" una vez se recibe el formulario. Asimismo, los avisos de privacidad son claros en que responden a todas las solicitudes que reciben de personas que desean ejercer sus derechos de protección de datos de acuerdo con las normas de protección de datos aplicables, lo que demuestra que el equipo de asistencia y los DPDs tienen la instrucción interna de responder las consultas, peticiones y reclamos de los titulares.*
>
> *Para presentar una solicitud, el titular debe acceder al Portal de Solicitudes, completar los campos obligatorios (incluidos el asunto, la descripción y cualquier otra información pertinente), y enviar el formulario de manera que el equipo de asistencia se ponga en contacto lo antes posible. Los Servicios de World también proveen recursos para que los titulares puedan comunicarse y hacer efectivos sus derechos en relación con datos personales a través del Help Center. Según el Help Center, las Entidades cuentan con un dedicado equipo de soporte de privacidad para resolver cualquier pregunta (e.g., consulta, petición, reclamo) de titulares de datos personales (…)*

El literal k) del artículo 17 de la Ley 1581 d 2012, dispone:

> ***ARTÍCULO 17. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO.*** *Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:*
>
> *k)* ***Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;***

Por su parte el literal a) del artículo de la misma ley, establece:

> ***ARTÍCULO 4o. PRINCIPIOS PARA EL TRATAMIENTO DE DATOS PERSONALES.*** *En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:*
>
> *a)* ***Principio de legalidad en materia de Tratamiento de datos:*** *El Tratamiento a que se refiere la presente ley es una actividad reglada que debe sujetarse a lo establecido en ella y en las demás disposiciones que la desarrollen;*

Por su parte el artículo 2.2.2.25.6.2 del Decreto 1074 de 2015, indica:

> ***ARTÍCULO 2.2.2.25.6.2. Políticas internas efectivas.*** *En cada caso, de acuerdo con las circunstancias mencionadas en los numerales 1, 2, 3 y 4 del artículo 2.2.2. 25.6.1. las medidas efectivas y apropiadas implementadas por el Responsable deben ser consistentes con las instrucciones impartidas por la Superintendencia de Industria y Comercio. Dichas políticas deberán garantizar:*
> *1. La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del responsable para la adopción e implementación de políticas consistentes con la Ley 1581 de 2012 y este capítulo.*
> *2. La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.*
> *3.* ***La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del tratamiento.***
> *La verificación por parte de la Superintendencia de Industria y Comercio de la existencia de medidas y políticas específicas para el manejo adecuado de los datos personales que administra un Responsable será tenida en cuenta al momento de evaluar la imposición de sanciones por violación a los deberes y obligaciones establecidos en la ley y en el presente capítulo.*

Conforme las citadas normas, el Responsable debe tener implementado un manual en el cual se establezca el procedimiento para la atención y respuesta a consultas, peticiones y reclamos de los titulares, con respecto al cualquier aspecto del tratamiento de sus datos personales.

Se allegó con el escrito de alegatos de conclusión el documento "Data Subjects Rights (Derechos de los titulares de datos) – Internal Procedures Policy (Política de Procedimientos Internos), del cual esta Despacho encuentra lo siguiente:

1. No se allega una versión en español.

2. Su objetivo es establecer los procedimientos basados en la legislación de protección de datos respecto de los derechos de los titulares, con el cual

se asegura el cumplimiento de la misma por parte de Worldcoin Project. Busca igualmente cumplir con el marco de privacidad en la transferencia de datos entre Área económica Europea y los Estados Unidos de América.

3. Debe ser aplicada por los empleados y colaboradores de Worldcoin Foundation.

4. El proceso para dar respuesta a requerimientos está adaptado para ser aplicado dependiendo del plazo legal establecido en las diferentes jurisdicciones, procurando de esta manera dar respuesta a todos.

5. En el numeral 6 relacionado con el cumplimiento de los derechos de los titulares de los datos, la norma legal aplicable es el Reglamento General de Protección de Datos aplicable en la Unión Europea.

6. La Ley 1581 de 2012 sólo es tenida en cuenta para efectos del término para dar respuesta a los requerimientos que se realicen por parte de los titulares colombianos.

Conforme lo anterior, el Manual (como es citado por los apoderados de World) no se ajusta a la normatividad colombiana, como se ha dicho a lo largo de la presente decisión, el tratamiento de los datos que se realice en territorio colombiano debe necesariamente realizarse conforme las normas establecidas en la Ley 1581 de 2012.

DECIMOSEXTO. Principio de Responsabilidad Demostrada

Frente al principio de responsabilidad demostrada, el artículo 2.2.2.25.6.1 del Decreto 1074 de 2015, dispone lo siguiente:

> ***"ARTÍCULO 2.2.2.25.6.1. Demostración.*** *Los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y este capítulo, en una manera que sea proporcional a lo siguiente:*
> *1. La naturaleza jurídica del responsable y, cuando sea del caso, su tamaño empresarial, teniendo en cuenta si se trata de una micro, pequeña, mediana o gran empresa, de acuerdo con la normativa vigente.*
> *2. La naturaleza de los datos personales objeto del tratamiento.*
> *3. El tipo de Tratamiento.*
> *4. Los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares.*
> *En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, los Responsables deberán suministrar a esta una descripción de los procedimientos usados para la recolección de los datos personales, cómo también la descripción de las finalidades para las cuáles esta información es recolectada y una explicación sobre la relevancia de los datos personales en cada caso.*
> *En respuesta a un requerimiento de la Superintendencia de Industria y Comercio, quienes efectúen el Tratamiento de los datos personales deberán suministrar a esta evidencia sobre la implementación efectiva de las medidas de seguridad apropiadas"*

Sobre este particular, la Corte Constitucional mediante la sentencia C-32 de 2021 reconoció la existencia de la **responsabilidad demostrada** en los siguientes términos:

> *"219. El principio de responsabilidad demostrada, conocido en el derecho comparado como accountability en la protección de datos personales, es incorporado por la legislación interna por el Decreto 1377 de 2013, reglamentario de la Ley 1581 de 2013 (sic). El artículo 26 de esa normativa determina que los responsables del tratamiento de datos personales deberán demostrar, a petición de la Superintendencia de Industria y Comercio, entidad que obra como autoridad colombiana de protección de datos, que han implementado medidas apropiadas y efectivas para cumplir con las citadas normas jurídicas. Esto de manera proporcional a: (i) la naturaleza jurídica del responsable y, cuando sea el caso, su tamaño empresarial; (ii) la naturaleza de los datos personales objeto de tratamiento; (iii) el tipo de tratamiento; y (iv) los riesgos potenciales que el referido tratamiento podrían causar sobre los derechos de los titulares del dato personal. Con este fin, los responsables deben informar a la SIC acerca de los procedimientos usados para el tratamiento de datos. A esta medida se suma lo previsto en el artículo 27 ejusdem, que estipula la obligación del responsable de establecer políticas internas que garanticen: (i) la existencia de una estructura administrativa proporcional a la*

> *estructura y tamaño empresarial del responsable; (ii) la adopción de mecanismos internos para poner en práctica dichas políticas; y (iii) la previsión de procesos para la atención y respuesta a consultas, peticiones y reclamos de los titulares, respecto de cualquier aspecto del tratamiento de datos personales.*
>
> ***El principio de responsabilidad demostrada, de acuerdo con lo expuesto, consiste en el deber jurídico del responsable del tratamiento de demostrar ante la autoridad de datos*** *que cuenta con la institucionalidad y los procedimientos para garantizar las distintas garantías del derecho al habeas data, en especial, la vigencia del principio de libertad y las facultades de conocimiento, actualización y rectificación del dato personal."*[40] *(Destacamos)*

Para el adecuado cumplimiento de la Ley 1581 de 2012, es necesario que, en la adopción de las políticas y procedimientos establecidos en el artículo 2.2.2.25.61 y siguientes del Decreto 1074 de 2015, concurran una serie de presupuestos que permitan evidenciar que aquellos implementados, en la práctica son además de efectivos, comprobables.

Así, la regulación colombiana le impone al Responsable del tratamiento la responsabilidad de garantizar la eficacia de los derechos del titular del dato, la cual no puede ser simbólica ni formal, sino real y demostrable. Téngase presente que según nuestra jurisprudencia *"existe un deber constitucional de administrar correctamente y de proteger los archivos y las bases de datos que contengan información personal o socialmente relevante"*[41].

Esto, en la medida que el Responsable no puede actuar como si los datos personales que se encuentren almacenados en sus bases de datos le pertenecieran. Si bien, tienen la facultad de decidir respecto de la información recolectada, ésta debe realizarse de manera correcta, apropiada y acertada. Su negligencia afectaría el derecho fundamental de habeas data de los titulares.

Para efectos de lo anterior, los artículos 2.2.2.25.6.1 y 2.2.2.25.6.2 del Decreto 1074 de 2015 reglamenta algunos aspectos relacionados con el principio de responsabilidad demostrada.

El citado artículo 2.2.2.25.6.1, establece que "los responsables del tratamiento de datos personales deben ser capaces de demostrar, a petición de la Superintendencia de Industria y Comercio, que han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012". Resulta imposible entonces para ese Responsable, ignorar la forma en que debe probar que pone en funcionamiento medidas adecuadas, útiles y eficaces para cumplir la regulación.

Es decir, se reivindica que un administrador no puede utilizar cualquier tipo de políticas o herramientas para dicho efecto, sino solo aquellas que tengan como propósito lograr que los postulados legales sean realidades verificables, y no solo se limiten a creaciones teóricas e intelectuales.

Con el propósito de dar orientaciones sobre la materia, esta Superintendencia expidió la "Guía para la implementación del principio de responsabilidad demostrada (accountability)"[42]

El término "accountability", a pesar de contar con diferentes acepciones, ha sido entendido en el campo de la protección de datos como el modo en que una organización debe cumplir (en la práctica) las regulaciones sobre el tema, y la manera en que debe demostrar que lo puesto en práctica es útil, pertinente y eficiente.

---

[40] Cfr. Corte Constitucional, sentencia C-032 del 18 de febrero de 2021. M.P. Dra Gloria Stella Ortiz. El texto de la sentencia puede consultarse en: https://www.corteconstitucional.gov.co/relatoria/2021/C-032-21.htm

[41] Corte Constitucional, Sentencia T-227 de 2003

[42] El texto de la guía puede consultarse en https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf

Conforme con ese análisis, las recomendaciones que trae la guía a los obligados a cumplir la Ley 1581 de 2012, consisten principalmente en diseñar y activar un Programa Integral de Gestión de Datos Personales (en adelante PIGDP). Esto, exige compromisos y acciones concretas de los directivos de la organización. Igualmente, requiere la implementación de controles de diversa naturaleza, desarrollar un plan de revisión, supervisión, evaluación y control del PIGDP, y demostrar el debido cumplimiento de la regulación sobre tratamiento de datos personales.

El principio de responsabilidad demostrada -accountability- demanda por parte del Responsable:

(i) Diseñar procedimientos apropiados, efectivos y verificables que permitan determinar el cumplimiento efectivo de los principios que orientan el tratamiento de datos personales. Éstos deberán ser objeto de revisión y evaluación permanente para medir su nivel de eficacia y el grado de protección de los datos personales.

(ii) Implementar acciones de diversa naturaleza para garantizar el correcto cumplimiento de todos y cada uno de los deberes que imponen la Ley 1581 de 2012 como regulación aplicable al tratamiento de datos personales.

Ahora bien, el principio de responsabilidad demostrada se articula con el concepto de "compliance." Éste hace referencia "al conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y establecer mecanismos internos de prevención, gestión, control y reacción frente a los mismos"[43].

Así las cosas, la identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos son elementos cardinales del "compliance" y de la efectiva aplicación del principio de responsabilidad demostrada (accountability).

De ahí que, se considere fundamental que las organizaciones desarrollen y pongan en marcha, entre otros, un sistema de administración de riesgos asociados al tratamiento de datos personales, que les permita identificar, medir, controlar y monitorear todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo a que están expuestos en desarrollo del cumplimiento de las normas de protección de datos personales.

Aunado a lo anterior, el cumplimiento de tal principio implica necesariamente garantizar y velar por el cumplimiento estricto de la normatividad aplicable al caso y poder demostrar que los documentos elaborados han sido diligenciados e implementados para que, a través de estos, se pueda demostrar el cumplimiento de la normatividad consagrada en el régimen de protección de datos personales contenido en la Ley 1581 de 2012.

Además de lo anterior, el cumplimiento de este principio busca que el Responsable del Tratamiento, demuestre que dentro de su organización se cuenta con:

a. Una estructura de gobierno corporativo en el sentido de que la formulación de políticas y procedimientos para el tratamiento reflejen una cultura de respeto a la protección de los datos personales;

b. Un programa corporativo que tenga controles efectivos, que responda al tamaño y estructura de la organización, destinado al cumplimiento, implementación y consolidación del régimen de protección de datos; y

c. Una evaluación y revisión continúa de los controles que lo integran, con el fin de determinar la pertinencia y eficacia del plan de gestión para lo cual deberán desarrollarse auditorías internas para evaluar, en una fase preliminar, el grado de cumplimiento con la normatividad de protección de datos.

[43] Cfr. World Compliance Association (WCA). http://www.worldcomplianceassociation.com/que-es-compliance.php

Así las cosas, este Despacho se permite reiterar que no basta con tener una cultura que propenda por el respeto en la teoría, sino que dicha cultura debe materializarse en la práctica a través del efectivo cumplimiento de la Ley 1581 de 2012, más allá de que esta autoridad requiera a la investigada sobre su cumplimiento, ya que es un deber de la organización dar pleno cumplimiento a tal normatividad y es un derecho constitucional del ciudadano que se le respeten sus datos personales, situación que adquiere mayor relevancia cuando se trata de información catalogada como sensible por la Ley.

DECIMOSÉPTIMO. Conclusiones.

(i) Por disposición expresa de la Constitución Política, en Colombia el tratamiento de los datos personales goza de especial protección y es a partir de este mandato que a través de la Ley 1581 de 2012 se positivizaron los principios, los deberes y los derechos de quienes intervienen en el tratamiento de los datos personales.

(ii) Conforme lo dispone el artículo 2, la Ley 1581 de 2012 será aplicada al responsable o encargado que, aun cuando su domicilio no se encuentre en Colombia, **realice el tratamiento de los datos personales de los titulares residentes en territorio colombiano**. Esta condición debe analizarse en conjunto con el principio de legalidad en materia de protección de datos personales. Esto en la medida que dicho tratamiento deberá ajustarse a los preceptos de la citada ley y sus disposiciones reglamentarias, es decir, ese responsable o encargado debe estar en la condición de asumir, cumplir y acatar, entre otros, los principios y los deberes descritos en los artículos 4 y 17 de la mencionada norma.

(iii) El tratamiento de datos personales de carácter sensible requiere un mayor cuidado y diligencia por parte de los responsables y encargados de tratamiento durante todo el ciclo de tratamiento, desde su recolección y hasta la finalización del mismo. Esta Dirección verificó el incumplimiento en varios aspectos, de la normatividad en materia de protección de datos personales en Colombia, conforme a la Ley 1581 de 2012 y sus decretos reglamentarios, concretamente: i) al no contar con políticas de tratamiento de datos personales con el cumplimiento de los requisitos mínimos, (ii) no cuentan con los procedimientos relacionados con la presentación y atención de consultas o reclamos por parte de los titulares de los datos personales, que les permitan el ejercicio del derecho fundamental de habeas data, (iii) no cuentan con las medidas de seguridad necesarias para prevenir los riesgos que conlleva el tratamiento de datos personales sensibles, y (iv) los formatos de autorización para el tratamiento de datos personales no se ajusten con el principio de libertad y requisitos exigidos por las leyes colombianas.

(iv) De acuerdo con la definición dispuesta en el artículo 5 de la Ley 1581 de 2012, **la imagen del iris como dato biométrico es por su naturaleza misma un dato personal sensible**, en la medida que permite la identificación de una persona por sus condiciones físicas y/o fisiológicas, **por lo que su tratamiento se encuentra expresamente prohibido, salvo que, el titular así lo autorice.**

(v) Por expreso mandato constitucional, en materia de protección de datos personales, el principio de libertad se erige como una garantía para que la información no pueda ser recolectada y tratada por el Responsable o Encargado sin la autorización previa y expresa del titular. El consentimiento que otorgue ese titular debe ser libre, sin ningún tipo de condicionamiento que pueda nublar su voluntad y lo lleve a tomar una decisión respecto de la cual pueda arrepentirse después.

(vi) La entrega de un beneficio económico condiciona a que el titular autorice el tratamiento de su información, sin conocer de antemano, por ejemplo,

cómo será almacenada, que tipo de medidas de seguridad tienen implementadas para asegurar su integridad.

El consentimiento como expresión del principio de libertad debe obedecer a la voluntad libre del titular, que pueda estar en la capacidad de decidir si está de acuerdo o no con el tratamiento de sus datos personales, en especial cuando se trata de aquellos de naturaleza sensible. La promesa de una contraprestación cualquiera que sea el tipo puede condicionar el juicio del titular y llevarlo tomar una decisión desinformada y prematura.

(vii) Se constató que Worldcoin para el desarrollo de su operación ofrece a las personas una compensación económica para la creación de una cuenta y la adquisición del World ID. Dicha compensación es entregada una vez se realice la verificación de la imagen del Iris por parte de la persona interesada. Es evidente entonces que Worldcoin vulnera el principio de libertad en la medida que el consentimiento que otorgue esa persona para el tratamiento de sus datos personales sensibles no es el producto del juicio interno que lo lleva a decidir finalmente, si acepta o no que su información sea almacenada y tratada por Worldcoin. Se vulnera el principio de finalidad, porque el tratamiento de los datos personales sensibles que realiza Worldcoin no obedece a una "finalidad" legítima. Se parte del hecho que ese tratamiento no cuenta con el consentimiento libre de sus titulares, tal como lo exige el artículo 6 de la Ley 1581 de 2012.

(viii) Si bien el titular de la información puede solicitar la eliminación de su información, inclusive las imágenes de su iris codificadas, considera el Despacho que dicha supresión no puede entenderse como definitiva. Y se llega a esta conclusión porque una de las funcionalidades de ese código es evitar un doble registro por parte de una misma persona en el protocolo, luego entonces Worldcoin mantiene una base de datos con dicha información, condición que no es informada al titular de la información.

(ix) Por mandato expreso de la Ley 1581 de 2012, el tratamiento de los datos personales sensibles está prohibido, salvo que el titular de la información recolectada lo autorice de manera previa, expresa e informada. En el presente caso, conforme el análisis realizado a lo largo del presente acto administrativo el modelo de negocio implementado por Worldcoin en Colombia no se ajusta al régimen de protección de datos personales, pues la autorización por ellos implementada no cumple con los requisitos exigidos para legitimar el tratamiento de los datos biométricos recolectados, razón por la cual la sanción a imponer cumple con los requisitos de legalidad y proporcionalidad desarrollados en el debido proceso.

(x) Las medidas que toma esta Dirección están dirigidas únicamente a proteger el derecho constitucional de habeas data de los colombianos, evitando que la información sea tratada por fuera de las normas que regulan la materia, tanto por Responsables y Encargados establecidos en territorio colombiano y aquellos que se encuentren en el extranjero, con lo cual, no se pretende desincentivar el desarrollo tecnológico ni la libre empresa de acuerdo con lo establecido en el artículo 333 de la Constitución Política, sino que las actividades comerciales que involucren el tratamiento de datos personales, incluyendo aquellos sensibles, verdaderamente se ajusten y estén en consonancia con el régimen de protección de datos personales establecido en la Ley 1581 de 2012 y sus normas reglamentarias, garantizando los derechos fundamentales de los titulares e incentivando que los responsables en la creación de nuevos negocios de innovación, lo realicen de manera responsable, ética y en estricto cumplimiento de la normativa colombiana.

DECIMOCTAVO. Imposición de la Sanción.

En términos generales, el derecho administrativo sancionador, pretende garantizar la preservación y restauración del ordenamiento jurídico, mediante la imposición de una sanción que no sólo repruebe, sino que también prevenga la realización de todas aquellas conductas contrarias al mismo. Se trata, en esencia, de un poder de sanción ejercido por las autoridades administrativas que opera ante el incumplimiento de los distintos mandatos que las normas jurídicas imponen a los administrados y aún a las mismas autoridades públicas"[44]

En un pronunciamiento reciente, la Corte Constitucional[45] sostuvo que el derecho administrativo sancionador "es una manifestación del ius puniendi estatal"[46], esto es, de la facultad que tiene el Estado para sancionar las conductas que se consideran reprochables. Dada su naturaleza, es una rama del derecho público que está sometida a unos principios "que operan como límite"[47], entre ellos, los principios de legalidad y tipicidad[48].

Dicha potestad se desarrolla materialmente bajo el procedimiento administrativo establecido en el CPACA, encontrándose de esta manera, sujeta a los principios establecidos en el artículo 3 de la citada codificación.

De conformidad con lo establecido en el citado artículo[49], las actuaciones sancionatorias definidas en el artículo 47 y siguientes del CPACA, se desarrollarán, con arreglo al principio del **debido proceso**[50], en virtud del cual, se tendrán en cuenta las normas de procedimiento y competencia establecidas en la Constitución y la Ley, con plena garantía de los derechos de representación, defensa y contradicción, así como del **principio de legalidad de las faltas y de las sanciones**.

En lo que tiene que ver con el **principio de legalidad**, la doctrina ha indicado que su finalidad es garantizar la libertad de los titulares y controlar la arbitrariedad judicial y administrativa mediante el señalamiento legal previo de las penas aplicables. Y aunque la doctrina y la jurisprudencia han reconocido que en el derecho administrativo sancionador no tiene la misma rigurosidad exigible en materia penal, aun así, el comportamiento sancionable debe estar precisado inequívocamente, como también la sanción correspondiente a fin de garantizar el derecho al debido proceso a que laude el artículo 29 Superior[51].

Respecto al **principio de tipicidad**, se ha dicho que el legislador está obligado a describir la conducta o comportamiento que se considera ilegal o ilícito en la forma más clara y precisa posible, de modo que no quede duda alguna sobre el acto, el hecho, la omisión o la prohibición que da lugar a sanción, e igualmente debe predeterminar la sanción indicando todos aquellos aspectos relativos a ella, esto es, la clase, el término, la cuantía, o el mínimo y el máximo dentro del cual

---

[44] Cfr. Corte Constitucional, sentencia C-818 del 9 de agosto de 2005. MP. Dr. Rodrigo Escobar Gil. En: https://www.corteconstitucional.gov.co/relatoria/2005/C-818-05.htm

[45] Sentencia C- 094 de 2021

[46] Sentencia C-412 de 2015.

[47] Ib.

[48] La Corte Constitucional también ha considerado como principios del derecho administrativo sancionador el debido proceso, el principio de proporcionalidad y la independencia entre la sanción administrativa y la sanción penal (cfr., sentencia C-748 de 2011, citada por la sentencia C-412 de 2015).

[49] La aplicabilidad general de los principios previstos en el artículo 3° del CPACA, como desarrollo directo de la Constitución Política, conlleva a que dichos principios deban observarse para cualquier actuación administrativa, incluidas las reguladas en leyes especiales. Así las cosas, el intérprete deberá utilizarlos directamente o hacer un ejercicio de integración normativa, entre los principios de la actuación administrativa previstos en la ley especial y los señalados en el CPACA. Laverde A. JUAN MANUEL. Manual de Procedimiento Administrativo Sancionatorio. Ed. Legis S.A. Bogotá Colombia Segunda Edición 2018.p. 51

[50] Efectivamente, el artículo 29 de la Constitución Política, establece que el "debido proceso" se aplicará a toda clase de actuaciones judiciales y administrativas, así mismo indica que "nadie podrá ser juzgado sino conforme a leyes preexistentes al acto que se le imputa, ante juez o tribunal competente y con observancia de la plenitud de las formas propias de cada juicio", aspectos que se materializan en los principios de legalidad y tipicidad.

[51] Restrepo Medina, MANUEL ALBERTO. Nieto Rodríguez MARÍA ANGELICA. El Derecho Administrativo Sancionador en Colombia. Editorial Universidad del Rosario. Legis. Bogotá Colombia Primera Edición 2017.

ella puede fijarse, la autoridad competente para imponerla y el procedimiento que ha de seguirse para su imposición[52].

En materia de protección de datos personales, la potestad sancionadora de esta Superintendencia se concreta en el artículo 22 de la Ley 1581 de 2012, el cual establece que, para la imposición de una sanción, deberá determinarse que hubo una vulneración efectiva a las disposiciones descritas en la citada Ley.

Mediante sentencia C – 748 del 6 de octubre de 2011, la Corte Constitucional cuando estudió la constitucionalidad del artículo 22 antes mencionado, manifestó:

> *"Esa potestad es una manifestación del jus punendi, razón por la que está sometida a los siguientes principios: **(i) el principio de legalidad**, que se traduce en la existencia de una ley que la regule; es decir, que corresponde sólo al legislador ordinario o extraordinario su definición. (ii) El **principio de tipicidad** que, si bien no es igual de riguroso al penal, sí obliga al legislador a hacer una descripción de la conducta o del comportamiento que da lugar a la aplicación de la sanción y a determinar expresamente la sanción285. (iii) El **debido proceso** que exige entre otros, la definición de un procedimiento, así sea sumario, que garantice el debido proceso y, en especial, el derecho de defensa, lo que incluye la designación expresa de la autoridad competente para imponer la sanción. (iv) El **principio de proporcionalidad** que se traduce en que la sanción debe ser proporcional a la falta o infracción administrativa que se busca sancionar286. (v) **La independencia de la sanción penal**; esto significa que la sanción se puede imponer independientemente de si el hecho que da lugar a ella también puede constituir infracción al régimen penal.*
>
> *Estos principios son los que debe cumplir cada una de las normas del capítulo en revisión.*
>
> *El artículo 22, inciso primero, cumple con el principio del debido proceso, en la medida en que señala que le corresponderá a la Superintendencia de Industria y Comercio adoptar las medidas y sancionar a los responsables y encargados del tratamiento de datos. Por tanto, se cumple con la obligación de designar la autoridad competente para imponer las sanciones por el desconocimiento de las normas de protección del dato.*
>
> *En relación con el principio de tipicidad, encuentra la Sala que pese a la generalidad de la ley, es determinable la infracción administrativa en la medida en que se señala que la constituye **el incumplimiento de las disposiciones de la ley**, esto es, en términos específicos, la regulación que hacen los artículos 17 y 18 del proyecto de ley, en los que se señalan los deberes de los responsables y encargados del tratamiento del dato.*
>
> *De esta misma generalidad adolecía el proyecto que dio origen a la Ley 1266 de 2008, y la Corte, en la sentencia C-1011 de 2008, interpretó que la infracción administrativa la constituía el desconocimiento de los deberes de los usuarios, fuentes y operadores. Esa interpretación será la misma que empleará en esta oportunidad la Sala para declarar la exequibilidad del inciso primero del artículo 22, cuando se refiere al "incumplimiento de las disposiciones de la presente ley por parte del Responsable del Tratamiento o el Encargado del Tratamiento".*

La facultad sancionadora de la cual se ha hecho referencia, además de encontrarse sujeta a los principios de legalidad y tipicidad, lo está también del principio de proporcionalidad, en desarrollo del cual, la sanción a imponer debe ser "proporcional" a la falta o infracción que se quiere sancionar, esto dentro de un marco de referencia que permita la determinación de la sanción en el caso en concreto.

Ese juicio de proporcionalidad o de ponderación busca que la sanción que vaya a ser impuesta sea consecuente y equilibrada respecto de la conducta reprochada, es decir, debe ser las más adecuada a la norma que le da sustento, pues lo que se pretende con su imposición es promover y garantizar el cumplimiento del Régimen de Protección de Datos Personales.

En desarrollo de los citados principios, la Ley 1581 de 2012 en sus artículos 23 y 24 establece las clases de sanciones y los criterios que deben ser tenidos en cuenta para efectos de su graduación.

> ***ARTÍCULO 23. SANCIONES.** La Superintendencia de Industria y Comercio podrá imponer a los Responsables del Tratamiento y Encargados del Tratamiento las siguientes sanciones:*

[52] Ibidem

a) Multas de carácter personal e institucional hasta por el equivalente de dos mil (2.000) salarios mínimos mensuales legales vigentes al momento de la imposición de la sanción. Las multas podrán ser sucesivas mientras subsista el incumplimiento que las originó;
b) Suspensión de las actividades relacionadas con el Tratamiento hasta por un término de seis (6) meses. En el acto de suspensión se indicarán los correctivos que se deberán adoptar;
c) Cierre temporal de las operaciones relacionadas con el Tratamiento una vez transcurrido el término de suspensión sin que se hubieren adoptado los correctivos ordenados por la Superintendencia de Industria y Comercio;
d) Cierre inmediato y definitivo de la operación que involucre el Tratamiento de datos sensibles;

ARTÍCULO 24. CRITERIOS PARA GRADUAR LAS SANCIONES. *Las sanciones por infracciones a las que se refieren el artículo anterior, se graduarán atendiendo los siguientes criterios, en cuanto resulten aplicables:*
a) La dimensión del daño o peligro a los intereses jurídicos tutelados por la presente ley;
b) El beneficio económico obtenido por el infractor o terceros, en virtud de la comisión de la infracción;
c) La reincidencia en la comisión de la infracción;
d) La resistencia, negativa u obstrucción a la acción investigadora o de vigilancia de la Superintendencia de Industria y Comercio;
e) La renuencia o desacato a cumplir las órdenes impartidas por la Superintendencia de Industria y Comercio;
f) El reconocimiento o aceptación expresos que haga el investigado sobre la comisión de la infracción antes de la imposición de la sanción a que hubiere lugar.

18.1. Literal a): La dimensión del daño o peligro a los intereses jurídicos tutelados por la ley.

De la lectura del literal a) del artículo 24 de la Ley 1581 de 2012, de la norma citada, resulta claro que para que haya lugar a la imposición de una sanción por parte de este Despacho, basta con que la conducta desplegada por la investigada haya puesto en peligro los intereses jurídicos tutelados por la Ley 1581 de 2012.

El juicio de antijuridicidad que debe realizar el operador jurídico recae sobre la infracción misma de la norma. En este punto en particular, resulta necesario traer a colación lo dicho por el Consejo de Estado[53] en materia de **antijuridicidad**.

"El segundo presupuesto ***para imponer una sanción administrativa es que el comportamiento además de ser típico sea antijurídico****. En la construcción tradicional del derecho penal se ha exigido que la conducta no sólo contradiga el ordenamiento jurídico (antijuridicidad formal) sino que además dicha acción u omisión lesione de manera efectiva un bien jurídico o por lo menos lo coloque en peligro (antijuridicidad material). Esta construcción constituye el punto de partida para la delimitación de este presupuesto en el derecho administrativo sancionatorio, sin embargo, como ocurre con otras instituciones y principios es inevitable que sea objeto de matización y por ende presente una sustantividad propia [94]54.*

Siempre se ha sostenido que el derecho penal reprocha el resultado, incluso en los denominados delitos de peligro, comoquiera que se requiere una puesta efectiva en riesgo del bien jurídico objeto de protección. ***Esta situación no se presenta en el ámbito administrativo en el que por regla general la "…esencia de la infracción radica en el incumplimiento de la norma*** *[95]55", de allí que se sostenga que el reproche recae sobre "la mera conducta".* ***En derecho sancionatorio, interesa la potencialidad del comportamiento, toda vez que el principal interés a proteger es el cumplimiento de la legalidad, de forma tal que tiene sustancialidad (antijuridicidad formal y material) "la violación de un precepto que se establece en interés colectivo, porque lo que se sanciona es precisamente el desconocimiento de deberes genéricos impuestos en los diferentes sectores de actividad de la administración*** *[96]56."*

A partir de lo anterior, basta con el incumplimiento de la norma para que la administración pueda ejercer su poder sancionatorio.

---

[53] Consejo de Estado – Subsección C). Radicación número: 05001-23-24-000-1996-00680-01(20738) Bogotá, D.C., veintidós (22) de octubre de dos mil doce (2012). Consejero ponente: ENRIQUE GIL BOTERO.

[54] [94] RINCÓN CÓRDOBA, Jorge Iván. Derecho Administrativo Laboral. Bogotá, Universidad Externado de Colombia. Pág. 595.

[55] [95] *Ibídem.*

[56] [96] BIELSA, Rafael. Derecho Administrativo. Tomo IV. El Poder de Policía. Limitaciones Impuestas a la Propiedad Privada en Interés Público. Administración Fiscal. Buenos Aires, Depalma. 1956. Pág. 69.

En el caso particular, conforme al análisis jurídico y probatorio que antecede, se demuestra que la operación de World Foundation en Colombia, se desarrolla a través del tratamiento de los datos personales de carácter sensible, desde su recolección y posterior almacenamiento de las personas que acceden a participar en el protocolo, dicha actividad, se encuentra expresamente prohibida por la ley y solo puede ser justificada a través del consentimiento previo, libre, expreso e informado que el titular otorgue para ello.
No obstante, como se indicó en el aparte correspondiente World Foundation condicionó la voluntad del titular de escoger si accede o no al tratamiento de su información sensible, cuando ofrece un incentivo económico para su entrega. Adicionalmente no brindó la información de manera clara, transparente y sencilla al titular sobre las finalidades específicas del tratamiento desconociendo el derecho de los titulares a la autodeterminación informática, que le permitiera conocer las condiciones en las que se llevaría a cabo el tratamiento de sus datos personales y que le permitiera tomar una decisión consciente sobre sus datos. Estas conductas a todas luces vulneran el régimen de protección de datos personales establecido en Colombia, dando lugar a la imposición de una sanción.

DECIMONOVENO. Que mediante Oficio No. 24-240075-71 del 24 del 21 de febrero de 2025, el abogado Juan Nicolás Laverde Garzón, informa al Despacho la sustitución del poder que le fuera otorgado por Tools For Humanity Corporation, al Doctor Sergio Pablo Michelsen Jaramillo, para lo cual este Despacho reconocerá personería en la parte resolutiva del presente acto administrativo.

VIGESIMO. Que, con el fin de garantizar los derechos de defensa y contradicción, esta Dirección ha concedido el acceso digital del presente expediente a los apoderados especiales de **WORLD FOUNDATION** y **TOOLS FOR HUMANITY CORPORATION,** María Victoria Munévar Torrado y Sergio Pablo Michelsen Jaramillo respectivamente, con los correos electrónicos elai@bu.com.co y smichelsen@bu.com.co quienes deberán registrarse en **CALIDAD DE PERSONA NATURAL** en el siguiente enlace https://servicioslinea.sic.gov.co/servilinea/ServiLinea/Portada.php.

Una vez registrados, en el mismo enlace podrá iniciar sesión a servicios en línea, donde deberá ingresar al vínculo denominado *"ver mis trámites"* y luego seleccionar *"De protección de datos personales",* donde podrá visualizar el presente proceso radicado bajo el No. **24-240075**.

Los citados apoderados son responsables de la seguridad y utilización correcta de su **USUARIO** y **CONTRASEÑA** y deberá adoptar las medidas necesarias para que sean estrictamente confidenciales y sean utilizados únicamente por aquellas personas que estén debidamente autorizadas para ello.

Si tiene alguna duda o presenta algún inconveniente para la consulta del expediente o requiere más información relacionada con la Protección de Datos Personales, favor comunicarse con el *contact center* (601) 592 04 00, para que la misma sea atendida en el menor tiempo posible.

En mérito de lo expuesto,

RESUELVE

ARTÍCULO 1. IMPONER como sanción a **WORLD FOUNDATION** y **TOOLS FOR HUMANITY CORPORATION** el **CIERRE INMEDIATO Y DEFINITIVO DE SU OPERACIÓN EN COLOMBIA QUE INVOLUCRE TRATAMIENTO DE DATOS PERSONALES**, teniendo en cuenta que la misma involucra el tratamiento de datos personales sensibles conforme con lo indicado en la parte considerativa del presente acto administrativo.

ARTÍCULO 2. ORDENAR a **WORLD FOUNDATION** y **TOOLS FOR HUMANITY CORPORATION**, la supresión de los datos personales sensibles, incluidos los códigos de iris, de las bases de datos, repositorios o servidores que tengan dispuestos para su almacenamiento, y que hayan sido recolectados

desde el inicio de operaciones en Colombia hasta la fecha de ejecutoria del presente acto administrativo.

ARTÍCULO 3. Para demostrar el cumplimiento de la citada orden **WORLD FOUNDATION** y **TOOLS FOR HUMANITY CORPORATION**, deberán allegar dentro del mes siguiente a la ejecutoria del presente acto administrativo un informe expedido por una entidad externa en la que se certifique que los datos personales sensibles incluidos los códigos de iris fueron eliminados, para lo cual deberá anexarse la evidencia técnica que así lo compruebe.

ARTÍCULO 4. Tanto el informe como la evidencia técnica que se remita será analizada por los ingenieros forenses dispuestos para el efecto por esta Dirección.

ARTÍCULO 5. Reconocer al Doctor Sergio Pablo Michelsen Jaramillo identificado con la cédula de ciudadanía No. 19.389.091 y Tarjeta Profesional No. 45.253 del C. S. de la J. como apoderado de Tools For Humanity Corporation, conforme a la sustitución del poder allegado a la presente actuación administrativa.

ARTÍCULO 6. NOTIFICAR la presente Resolución a **WORLD FOUNDATION** y **TOOLS FOR HUMANITY CORPORATION**, a través de sus apoderados entregándoles copia de esta e informándoles que contra ella procede recurso de reposición, ante la Directora de Investigaciones de Protección de Datos Personales y de apelación ante el Superintendente Delegado para la Protección de Datos Personales dentro de los diez (10) días siguientes a su notificación.

ARTÍCULO 7. La Superintendencia de Industria y Comercio se permite recordar que los canales habilitados para que los investigados ejerzan sus derechos, den respuesta a requerimientos, interpongan recursos, entre otros, son:

- Correo de la Superintendencia de Industria y Comercio: contactenos@sic.gov.co.

- Sede principal: Calle 24 No. 7 – 43 Local 108 en la Ciudad de Bogotá de lunes a viernes de 8:00 a.m. a 4:30 p.m.

NOTÍFIQUESE Y CÚMPLASE
Dada en Bogotá, D.C., 03 de octubre de 2025

LA DIRECTORA DE INVESTIGACIONES DE PROTECCIÓN DE DATOS PERSONALES

CAROLINA GARCIA MOLINA

Firmado digitalmente por CAROLINA GARCIA MOLINA
Fecha: 2025.10.03 10:14:02 -05'00'

CAROLINA GARCÍA MOLINA

Proyectó: NT
Revisó: CG
Aprobó: CG