



El futuro
es de todos

Consejería Presidencial
para asuntos económicos
y transformación digital



Industria y Comercio
SUPERINTENDENCIA

Sandbox sobre privacidad desde el diseño y por defecto en proyectos de Inteligencia Artificial



SANDBOX SOBRE PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO EN PROYECTOS DE INTELIGENCIA ARTIFICIAL

Versión para comentarios

El siguiente documento ha sido elaborado por la **Superintendencia de Industria y Comercio con insumos y guía técnica de la Consejería Presidencial de Asuntos Económicos y Transformación Digital**. La realización del sandbox y las condiciones de su funcionamiento son competencia exclusiva de la Superintendencia de Industria y Comercio.

Fecha:

Octubre 20, 2020

Entidades involucradas en la realización del documento



El futuro
es de todos

Gobierno
de Colombia



El futuro
es de todos

Consejería Presidencial
para asuntos económicos
y transformación digital



CONTENIDO

I | RESUMEN DE LOS PRINCIPALES
ASPECTOS DEL SANDBOX REGULATORIO
pág 4-6

II | DE LA PRIVACIDAD, LA ÉTICA Y LA SEGURIDAD
DESDE EL DISEÑO Y POR DEFECTO
pág 7-9

III | DE LOS ESTUDIOS DE IMPACTO DE
PRIVACIDAD
pág 10-11

IV | CONFIANZA
pág 12-13

V | MARCO REGULATORIO
pág 14-16

VI | DEL SANDBOX REGULATORIO
pág 17-22



I

RESUMEN DE LOS PRINCIPALES ASPECTOS DEL SANDBOX REGULATORIO



| SANDBOX SOBRE PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO EN PROYECTOS DE INTELIGENCIA ARTIFICIAL | |
|--|--|
| Marco legal | Ley Estatutaria 1581 de 2012 y Decreto 4886 de 2011 |
| Objetivos específicos | <ul style="list-style-type: none"> ○ Fijar criterios que faciliten el cumplimiento de la regulación sobre tratamiento de datos y señalar los procedimientos para su cabal aplicación ○ Sugerir o recomendar, en caso que sea necesario, los ajustes, correctivos o adecuaciones de la regulación colombiana a los avances tecnológicos. ○ Lograr que el debido tratamiento de datos personales sea un componente esencial del diseño y puesta en marcha de proyectos de inteligencia artificial. ○ Promover la creación de productos de inteligencia artificial que desde su diseño y durante su ejecución sea, entre otras, respetuosos de los derechos de las personas respecto de su información personal y acordes con la regulación sobre tratamiento de datos personales. ○ Acompañar y asesorar en en materia de protección de datos personales, a las empresas seleccionadas, con el fin de mitigar los riesgos asociados a la implementación de la inteligencia artificial. ○ Consolidar un enfoque preventivo / proactivo de protección de derechos humanos en proyectos de IA |
| Requisitos principales | Proyecto de inteligencia artificial en comercio electrónico, publicidad o marketing que se encuentre en etapa de diseño (no debe estar culminado ni haber sido puesto operación). |
| Criterios de elegibilidad | <ul style="list-style-type: none"> ○ Novedad e impacto tanto en los derechos de las personas como en el mercado ○ Idea o tecnología innovadora |

| SANDBOX SOBRE PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO EN PROYECTOS DE INTELIGENCIA ARTIFICIAL | |
|--|--|
| Presentación de propuestas | Febrero 1 a marzo 30 de 2021. |
| Informe de propuesta (s) seleccionada (s) | Mayo 31 de 2021. |
| Tiempo | Duración inicial de seis (6) meses. |
| Costos | La presentación de propuestas no tiene ningún costo. |
| Herramientas | Asesoría especializada de la SIC en aspectos jurídicos sobre tratamiento de datos personales y seguimiento del avance del proyecto . |





II

DE LA PRIVACIDAD,
LA ÉTICA Y LA
SEGURIDAD DESDE
EL DISEÑO Y POR
DEFECTO



La Global Privacy Assembly aprobó durante el mes de octubre de 2020 la **RESOLUTION ON ACCOUNTABILITY IN THE DEVELOPMENT AND THE USE OF ARTIFICIAL INTELLIGENCE**. Esa resolución, entre otras, insta a las organizaciones que desarrollan o utilizan sistemas de inteligencia artificial (IA) a considerar la implementación de las siguientes medidas:

- **Evaluar** el posible impacto en los derechos humanos (incluida la protección de datos personales y los derechos de privacidad) antes del desarrollo y/o uso de la IA;
- **Probar** la solidez, confiabilidad, precisión y seguridad de los datos de la IA antes de ponerla en uso, incluida la identificación de sesgos en los sistemas y los datos que se utilizan que pueden conducir a resultados injustos;
- **Implementar** medidas de Responsabilidad Demostrada que sean apropiadas con respecto a los riesgos de interferencia con los derechos humanos;

Durante 2019 la Superintendencia de Industria y Comercio expidió los siguientes documentos: (i) **Guía sobre el tratamiento de datos personales para fines de comercio electrónico**¹; (ii) **Guía sobre el tratamiento de datos personales para fines marketing y publicidad** y (iii) **Guía para la implementación del principio de responsabilidad demostrada en las transferencias internacionales de datos personales**². En todas ellas, se recomienda incorporar la privacidad, la ética y la seguridad desde el diseño y por defecto. Adicionalmente, se sugiere efectuar estudios de impacto de privacidad.

Estas pautas replican a cualquier actividad como, entre otras, la inteligencia artificial (en adelante IA). De hecho, esas recomendaciones son reiteradas en la **GUÍA DE TRATAMIENTO DE DATOS PERSONALES E INTELIGENCIA ARTIFICIAL**³ de la Red Iberoamericana de Protección de Datos (en adelante RIPD).

En esos documentos se plantea que la privacidad desde el diseño y por defecto (*Privacy by Design and by Default*), es considerada una medida proactiva para, entre otras, cumplir con el Principio de Responsabilidad Demostrada (Accountability). Al introducir la privacidad desde el diseño, se busca garantizar el correcto Tratamiento de los datos utilizados en los proyectos que involucren recolección, uso o tratamiento de datos personales. Así las cosas, el debido tratamiento de la información debe ser un componente esencial del diseño y puesta en marcha de proyectos de inteligencia artificial.

La Privacidad por Diseño "*promueve la visión de que el futuro de la privacidad no puede ser garantizada sólo por cumplir con los marcos regulatorios; más bien, idealmente el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado*

de una organización⁷⁴. Por eso, desde antes que se recolecte información y durante todo el ciclo de vida de la misma, se deberían adoptar medidas preventivas de diversa naturaleza (tecnológica; organizacional; humana; procedimental; entre otras) con el objeto de evitar vulneraciones al debido tratamiento de los datos personales.

Adicionalmente, también se ha puesto de presente que la ética desde el diseño y por defecto, deben irradiar el esquema, desarrollo y uso de los datos en proyectos de IA, teniendo que ser parte fundamental de cualquier aspecto relacionado con esa actividad.

Lo anterior también debe predicarse de la seguridad en el Tratamiento de datos personales. Sin seguridad y un cumplimiento activo de este principio, no habrá debido Tratamiento de los datos. Por lo tanto, es fundamental adoptar medidas tecnológicas; humanas; administrativas; físicas; contractuales y de cualquier otra índole que eviten:

- **Accesos indebidos o no autorizados a la información.**
- **Manipulación de la información.**
- **Destrucción de la información.**
- **Usos indebidos o no autorización de la información.**
- **Circular o suministrar la información a personas no autorizadas.**

Las medidas de seguridad deben ser apropiadas considerando varios factores como: (i) los niveles de riesgo del Tratamiento para los derechos y libertades de los Titulares de los datos; (ii) la naturaleza de los datos; (iii) las posibles consecuencias que se derivarían de una vulneración para los Titulares, y la magnitud del daño que se puede causar a ellos, al Responsable y a la sociedad en general; (iv) el número de Titulares de los datos y la cantidad de información; (v) el tamaño de la organización; (vi) los recursos disponibles, (vii) el estado de la técnica, y (viii) el alcance, contexto y finalidades del Tratamiento de la información.

Todas las medidas de seguridad, deben ser objeto de revisión, evaluación y mejora permanente.





III

DE LOS ESTUDIOS DE IMPACTO DE PRIVACIDAD



Previo al diseño y desarrollo del proyecto de IA, la SIC y la RIPD sugieren efectuar una evaluación de impacto en la privacidad (*Privacy Impact Assessment - PIA* por sus siglas en inglés). Con el fin de poner en funcionamiento un sistema efectivo de manejo de riesgos y controles internos, para garantizar que los datos se tratarán debidamente y conforme con la regulación existente.

Dicha evaluación debería incluir, como mínimo, lo siguiente:

- Una descripción detallada de las operaciones de Tratamiento de datos personales que involucra el proyecto de IA.
- Una evaluación de los riesgos específicos para los derechos y libertades de los Titulares de los datos personales. La identificación y clasificación de riesgos, así como la adopción de medidas para mitigarlos, son elementos cardinales del Principio de Responsabilidad Demostrada. Es fundamental que las organizaciones desarrollen y pongan en marcha, entre otros, un **“sistema de administración de riesgos asociados al tratamiento de datos personales”**⁵ 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”**⁶.
- Las medidas previstas para afrontar los riesgos, incluidas garantías; medidas de seguridad; diseño de *software*; tecnologías y mecanismos que garanticen la protección de datos personales, teniendo en cuenta los derechos e intereses legítimos de los Titulares de los datos y de otras personas eventualmente afectadas.

Los resultados de este estudio, junto con las medidas para mitigar los riesgos, hacen parte de la aplicación del principio de privacidad desde el diseño y por defecto.





IV

CONFIANZA



Desde hace algunas décadas se ha sostenido que la confianza es factor crucial para el crecimiento y consolidación de cualquier otra actividad que se realice a través del uso de las tecnologías⁷, lo cual ha sido reiterado al establecer que **“las actividades continuas de creación de confianza deben ser una de las prioridades estratégicas más importantes para cada organización”⁸**.

La confianza se entiende como la expectativa de que **“se puede contar con la palabra del otro”** y de que se emprenderán acciones positivas y beneficiosas entre las partes de manera recíproca. Cuando existe confianza, la persona cree que la empresa es fiable, cumple su palabra, es sincera, íntegra y cumple con las acciones prometidas⁹.

Implementar la privacidad desde el diseño y por defecto son evidencia de que las organizaciones están comprometidas con el debido tratamiento de los datos personales y los derechos de las personas.





V

MARCO REGULATORIO



Este Sandbox se realiza dentro del marco de las siguientes competencias legales de la Superintendencia de Industria y Comercio:

Decreto 4886 de 2011 **“Por medio del cual se modifica la estructura de la Superintendencia de Industria y Comercio, se determinan las funciones de sus dependencias y se dictan otras disposiciones”**.

Artículo 1. FUNCIONES GENERALES

“La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:

1. Asesorar al Gobierno Nacional y participar en la formulación de las políticas en todas aquellas materias que tengan que ver con la protección al consumidor, la promoción y protección de competencia, a propiedad industrial, la **protección de datos personales** y en las demás áreas propias de sus funciones.

(...)

61. Impartir instrucciones en materia de protección al consumidor, protección de la competencia, propiedad industrial, administración de datos personales y en las demás áreas propias de sus funciones, **fijar criterios que faciliten su cumplimiento y señalar los procedimientos para su cabal aplicación.**

(...)

65. Adelantar actividades de divulgación, **promoción** y capacitación, en las materias de competencia de la entidad. (...).”

ARTÍCULO 30. FUNCIONES DEL DESPACHO DEL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO.

Son funciones del Despacho del Superintendente de Industria y Comercio:

1. Asesorar al Gobierno Nacional y participar en la formulación de las políticas en todas aquellas materias que tengan que ver con la protección al consumidor, la promoción y protección de la competencia, la propiedad industrial, **la protección de datos personales** y en las demás áreas propias de sus funciones.

(...)

5. Impartir instrucciones en materia de protección al consumidor, protección de la competencia, propiedad industrial, **la protección de datos personales** y en las demás áreas propias de sus funciones, así como **fijar los criterios que faciliten su cumplimiento y señalar los procedimientos para su cabal aplicación.**

ARTÍCULO 16. FUNCIONES DEL DESPACHO DEL SUPERINTENDENTE DELEGADO PARA LA PROTECCIÓN DE DATOS PERSONALES.

Son funciones del Despacho del Superintendente Delegado para la Protección de Datos Personales:

- 1. Asesorar al Superintendente de Industria. y Comercio en la formulación de las políticas en lo que se relaciona con su área.*
- 2. Velar por el cumplimiento de las normas y leyes vigentes **y proponer nuevas disposiciones.** (...)*

○ Ley Estatutaria 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”

“ARTÍCULO 21. FUNCIONES.

La Superintendencia de Industria y Comercio ejercerá las siguientes funciones:

(...)

- i) Sugerir o recomendar los ajustes, correctivos o adecuaciones a la normatividad que resulten acordes con la evolución tecnológica, informática o comunicacional; (...)*





VI

DEL SANDBOX REGULATORIO



Este sandbox regulatorio busca ser un escenario preventivo y de experimentación, para que las empresas o entidades interesadas en desarrollar proyectos de inteligencia artificial creen soluciones de cumplimiento colaborativo a través del acompañamiento no vinculante de la autoridad de datos en la implementación de herramientas como los estudios de impacto de privacidad, la privacidad por diseño y la responsabilidad demostrada, entre otras medidas que consideren apropiadas.

La SIC propone esta arenera regulatoria para que sea un espacio para acompañar desde el inicio algunos proyectos de inteligencia artificial con miras a que los mismos no sólo sean exitosos científica o económicamente, sino amigables y respetuosos de los derechos de las personas respecto de la recolección, almacenamiento, uso o circulación de su información.

En este sentido la SIC acoge la definición de inteligencia artificial prevista en el Conpes 3975 de 2019: **“Inteligencia artificial: es un campo de la informática dedicado a resolver problemas cognitivos comúnmente asociados con la inteligencia humana o seres inteligentes, entendidos como aquellos que pueden adaptarse a situaciones cambiantes. Su base es el desarrollo de sistemas informáticos, la disponibilidad de datos y los algoritmos.”**¹⁰

Durante el desarrollo de la arenera se activa un ejercicio de creación colaborativa de soluciones en materia de protección de datos e inteligencia artificial. Este sandbox será positivo para los emprendedores y sus clientes porque la innovación tecnológica estará acompañada de asesoría especializada para ser compatible con la protección de datos personales de manera que sus productos sean, entre otros, respetuosos de los derechos de las personas sobre la recolección y uso de su información.

Transversalidad del sandbox y participación de otras entidades públicas y privadas

La SIC considera que los aprendizajes y elementos que se obtengan de este espacio de experimentación pueden ser muy positivos para otras entidades públicas o privadas. En términos generales, se ha determinado que las características de la Inteligencia Artificial y su impacto en distintas regulaciones y materias hacen necesario que distintas organizaciones estén involucradas en un ejercicio de estas características. Las entidades involucradas pueden obtener un conocimiento adecuado sobre herramientas para desarrollar la Privacidad desde el diseño en los proyectos transformacionales que está desarrollando y el uso de sistemas IA en su entidad. Así mismo, se reducen las asimetrías de información sobre la tecnología para tomar decisiones regulatorias informadas y se logra conocer la posición de la SIC en la materia, para evitar posibles contradicciones con otros entes de supervisión o regulación.

Lo anterior ya ha sido señalado en distintos documentos técnicos en la materia, tal como el *Modelo conceptual para el diseño de Regulatory Sandboxes & Beaches en IA*, publicado por la Consejería Presidencia de Asuntos Económicos y Transformación Digital en el año 2020:

“Por lo tanto, considerar que una tecnología de estas características puede ser analizada desde una sola disciplina o desde una sola autoridad de vigilancia y control puede resultar bastante limitado. Tecnologías así de disruptivas tienen efectos transversales y requiere de distintos profesionales y autoridades que brinde un enfoque multidisciplinar. Ahora bien, basta sólo imaginar los efectos ambiciosos de un único *sandbox* transversal que brinde lecciones y enseñanzas a distintos sectores y entidades dentro del Estado. No solo los beneficios se ven en términos de eficiencia para el sector público, sino que sirve de base para considerar la construcción futura de una regulación transversal de tecnologías emergentes como la inteligencia artificial, que evita una aproximación sectorizadas que incluso puedan llegar a ser contradictorias.”

Por consiguiente, el modelo de sandbox regulatorio propuestos presentará un mecanismo específico para la participación de otras entidades públicas o privadas como participantes activos y observadores del trabajo que se realice al respecto.

La SIC invitará a participar a las organizaciones dependiendo de su objeto social o competencias legales de manera que sean pertinentes o conexas con el proyecto que se seleccione para realizar el sandbox.

Objetivos específicos

- Fijar criterios que faciliten el cumplimiento de la regulación sobre tratamiento de datos y señalar los procedimientos para su cabal aplicación.
- Sugerir o recomendar, en caso de que sea necesario, los ajustes, correctivos o adecuaciones de la regulación colombiana a los avances tecnológicos.
- Lograr que el debido tratamiento de datos personales sea un componente esencial del diseño y puesta en marcha de proyectos de inteligencia artificial.
- Promover la creación de productos de inteligencia artificial que desde su diseño y durante su ejecución sean, entre otras, respetuosos de los derechos de las personas respecto de su información personal y acordes con la regulación sobre tratamiento de datos personales.

- Acompañar y asesorar en materia de protección de datos personales, a las empresas seleccionadas, con el fin de mitigar los riesgos asociados a la implementación de la inteligencia artificial.
- Consolidar un enfoque preventivo / proactivo de protección de derechos humanos en proyectos de IA.

Beneficios

Para el país:

- Promover la innovación respetuosa de las normas sobre tratamiento de datos personales de los ciudadanos.
- Liderar la generación de proyectos de IA que sean referentes para futuros emprendimientos.

Para las empresas participantes:

- Reducción de riesgos legales en el tratamiento de datos personales.
- Acompañamiento especializado de la autoridad en el desarrollo de herramientas para la protección de datos desde el diseño y por defecto.
- Generación de confianza en el mercado, sus clientes y la sociedad.
- Evidenciar medidas de responsabilidad demostrada (accountability) que serán relevantes frente a eventuales investigaciones e imposición de sanciones¹².

Para los ciudadanos:

- Ser usuarios de productos de IA respetuosos de sus derechos como titulares de datos personales o, según el caso, saber que sus datos están siendo recolectados y usados por empresas que implementaron la privacidad desde el diseño y por defecto.
- Más confianza porque saben que la autoridad de protección de datos participó en el proyecto.

Para la SIC:

- Los “sandboxes” son una alternativa preventiva para cumplir el mandato del artículo 15 de la Constitución según el cual: *“En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.”*
- Promover tratamientos de datos respetuosos de los derechos humanos.
- Comprender y conocer de primera mano las innovaciones de las empresas objeto de control y vigilancia.
- Evaluar “en tiempo real” la eficacia de las estrategias de la entidad para la protección de derechos.

- Replicar el conocimiento adquirido mediante la creación de guías sobre tratamiento de datos personales que podrán ser útiles para otras empresas que emprendan proyectos de inteligencia artificial

Requisitos

Podrán participar empresas, universidades, nacionales o extranjeras que vayan a desarrollar o estén desarrollando procesos de IA en los siguientes temas:

- **Comercio electrónico**
- **Publicidad o marketing**

Es importante que el proyecto no esté culminado ni que se haya puesto en operación porque el objetivo del sandbox no es avalar tecnologías o proyectos preexistentes.

Período de consultas

El documento será publicado para consulta ciudadana durante el mes de noviembre de 2020. Se dará un plazo para remitir comentarios a la SIC. Después de este término se analizarán todos los comentarios recibidos.

Durante la segunda y tercera semana de diciembre de 2020 se organizarán dos sesiones para escuchar las eventuales dudas que surjan sobre el sandbox.

Se podrán realizar sesiones adicionales para dicho efecto dependiendo del número de interesados o de la complejidad del proyecto.

Presentación de propuestas

Las propuestas deben presentarse dentro de los meses de febrero y marzo del año 2021. Para el efecto, quienes deseen presentar sus proyectos deberán diligenciar el formulario que diseñará la SIC.

La SIC podrá solicitar información adicional en caso de ser necesario.

Selección

La SIC podrá seleccionar una o varias propuestas. Los resultados se publicarán en la última semana del mes de mayo de 2021. De ser necesario, se ampliará dicho plazo para adoptar la decisión.

La SIC podrá no seleccionar ninguna de las propuestas presentadas.

Ejecución del proyecto

El sandbox iniciará en el mes de junio de 2021 y la asesoría de la SIC será de máximo seis (6) meses. No obstante, en caso de ser necesario se podrá ampliar dicho término.

Previo al inicio de operaciones de la arenera se realizarán reuniones con la (s) empresa (s) seleccionada (s) y la SIC para establecer aspectos concretos de la ejecución del sandbox como, entre otros, el calendario de trabajo, la delimitación de las expectativas y las responsabilidades de las partes.

Durante la ejecución, la Delegatura realizará los controles correspondientes, los cuales incluyen, pero no están limitados a reportes con retroalimentación, recomendaciones y observaciones.

Fechas claves

| ACTIVIDAD | FECHAS |
|---|--------------------------------|
| Publicación de la propuesta de sandbox | ▶ Noviembre 6 de 2020 |
| Fecha límite para presentar observaciones | ▶ Noviembre 30 de 2020 |
| Publicación de la convocatoria | ▶ Diciembre 15 de 2020 |
| Sesión virtual de eventuales aclaraciones para las organizaciones interesadas en participar | ▶ Enero 15-22 de 2021 |
| Presentación de propuestas | ▶ Febrero 1 a marzo 30 de 2021 |
| Informe de propuesta (s) seleccionada (s) | ▶ Mayo 31 de 2021 |
| Ejecución del proyecto | ▶ Junio a diciembre de 2021 |



Referencias

- 1 Cfr. [https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20SIC%20Tratamiento%20Datos%20Personales%20ComercioElectronico\(1\).pdf](https://www.sic.gov.co/sites/default/files/files/pdf/Guia%20SIC%20Tratamiento%20Datos%20Personales%20ComercioElectronico(1).pdf)
- 2 Cfr. [https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales\(1\).pdf](https://www.sic.gov.co/sites/default/files/files/pdf/Gu%C3%ADa%20%20SIC%20para%20la%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%20en%20las%20transferencias%20internacionales(1).pdf)
- 3 El texto de la guía fue aprobado el 21 de junio de 2019 y puede consultarse en: <https://www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf>
- 4 Cfr. Cavoukia, Ann. *Privacidad por Diseño: Los 7 principios fundamentales*. Disponible en: <http://mediascope.nl/wp-content/uploads/2015/08/privacidad-por-dise%C3%B1o.pdf>
<https://www.mediascope.es/wp-content/uploads/2016/10/privacidad-por-disen%C3%A1o-1.pdf>
Ana Brian Nougreres también explica este tema en su artículo de 2012 publicado en la Revista Internacional de Protección de Datos Personales (RIPDP) y titulado “La protección inteligente de los datos personales: Privacy by Design (PbD)”. El texto puede consultarse en: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok6_-Ana-Brian-Nougreres_FINAL.pdf
- 5 Superintendencia de Industria y Comercio (2015) “*Guía para implementación del principio de responsabilidad demostrada (accountability)*”. Págs 16-18.
- 6 Ibid. Pág. 16
- 7 Cfr. Reichel & Shefter. Harvard Business Review. Jul-Ago, 2000
- 8 Cfr. Edelman Trust Barometer de 2019, <https://www.edelman.com/trust-barometer>
- 9 Cfr. Barrera Duque, Ernesto (2018) *Diseño organizacional centrado en el cliente. Teoría y práctica en empresas sociales*. Universidad de la Sabana y Ecoe ediciones.
- 10 Documento Conpes 3975 de 2019. Pg. 20. Disponible en: <https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3975.pdf>



Referencias

- 11 Guío Español, Armando. Modelo conceptual para el diseño de Regulatory Sandboxes & Beaches en IA. Corporación Andina de Fomento y la Consejería Presidencia de Asuntos Económicos y Transformación Digital, 2020. Pg. 10. Disponible en: <https://dapre.presidencia.gov.co/AtencionCiudadana/DocumentosConsulta/consulta-200820-MODELO-CONCEPTUAL-DISENO-REGULATORY-SANDBOXES-BEACHES-IA.pdf>
- 12 En efecto, el último párrafo del artículo 27 del decreto 1377 de 2013 (incorporado en el decreto 1074 de 2015) dice lo siguiente: *“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 tomada 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 decreto.”*

Sandbox sobre privacidad desde el diseño y por defecto en proyectos de Inteligencia Artificial



El futuro
es de todos

Consejería Presidencial
para asuntos económicos
y transformación digital