Gobernanza de Datos

Uso Ético de los Datos

SECRETARÍA DE INNOVACIÓN Y TRANSFORMACIÓN DIGITAL

SUBSECRETARÍA DE POLÍTICAS PÚBLICAS BASADAS EN EVIDENCIA

Buenos Aires Ciudad

Jefe de Gobierno
Horacio Rodríguez Larreta
Jefe de Gabinete
Felipe Miguel
Secretario de Innovación y Transformación Digital
Diego Fernández
Subsecretaria de Políticas Públicas Basadas en Evidencia
Melisa Breda

Índice

En la era digital, los datos se han convertido en uno de los activos más valiosos para las organizaciones ya que desempeñan un rol fundamental en la gestión de procesos y toma de decisiones.

Reconociendo su importancia, el Gobierno de la Ciudad Autónoma de Buenos Aires (GCABA), a través de la Secretaría de Innovación y Transformación Digital (SECITD), ha adoptado una política de datos que busca fortalecer los procesos de obtención, integración y almacenamiento, con el objetivo de tomar decisiones basadas en evidencia y mejorar la vida de los vecinos que viven y transitan por la Ciudad.

Para lograr este propósito, el GCABA ha establecido una política de interoperabilidad como parte de su enfoque de gobernanza de datos. Estos lineamientos, basados en las mejores prácticas internacionales y el modelo DAMA-DMBOK, definen un marco común de gobernanza de datos que abarca todas las etapas del ciclo de vida de los mismos.

Con el objetivo de integrar y disponibilizar todos los datos del GCBA, en 2021 se implementó la Plataforma Inteligente de Buenos Aires (PIBA), a través de un data lake, que consiste en una herramienta de inteligencia aumentada.

En tanto, en 2022 se creó el Sistema de Interoperabilidad de la Ciudad de Buenos Aires (SI) con la intención de eficientizar los procesos y servicios de cara al ciudadano.

A continuación, se transmiten los lineamientos que rigen el data lake y que determinan los estándares que deben aplicarse en el ciclo de vida de gestión de datos. Los mismos establecen procesos claros y universales sobre cómo GCABA clasifica, comparte, accede, gestiona y protege los datos.

1. Introducción

Uno de los retos más relevantes para todo tipo de organizaciones y especialmente para el sector público es el de asegurar un marco ético del uso de los datos que prevenga de todo posible daño y que aumente el bienestar social. Por lo tanto, entendemos que en toda estrategia de transformación digital, donde los datos son la materia prima, debe contemplarse la dimensión ética. Mucho más cuando entramos en escenarios de toma de decisiones algorítmica.

¿Qué es la ética de datos?

El Open Data Institute define la ética de los datos como: "Una rama de la ética que evalúa las prácticas, recopilación, creación, análisis y envío de datos tanto estructurados como no estructurados. Que pueden afectar negativamente a las personas y la sociedad si no son tratados de forma correcta y con el mayor cuidado posible.".

Abarca el tratamiento, la recolección, la transparencia, así como las acciones y decisiones en relación con los datos en general y los datos personales, en particular.

El presente trabajo está dirigida a cualquier persona que trabaje directa o indirectamente con datos en el sector público, incluidas todas las personas que se desempeñen en distintas áreas como ser los profesionales de datos, como estadísticas, [1] analistas y científicos de datos, responsables, personal operativo y quienes ayudan a producir una visión informada de los datos, también a aquellas personas funcionarias e instituciones públicas que tienen planificado desarrollar proyectos tecnológicos que [2] involucran el uso tratamiento intensivo y el análisis de datos para mejorar su gestión o entrega de productos y servicios a las personas.

2. Ética de datos

2.1 ¿Qué es el uso ético de los datos?

El uso ético de datos se refiere a aquellas pautas de comportamiento que promueven juicios apropiados, responsabilidad, principios y valores al momento en el que se adquieren, gestionan o utilizan esos datos, con el objetivo de proteger los derechos y privacidad de las personas y minimizar los riesgos potenciales para promover una auténtica transparencia en los proyectos y sistemas que conlleven una gestión de datos y de esa manera evitar la corrupción y el daño que pueda resultar en caso de dejar de lado dicha ética de uso.

De esa manera, los procesos de gestión de datos deben ser diseñados como soluciones sostenibles que beneficien en primer lugar a las personas, desarrollando activamente productos e infraestructuras que mejoren y respeten la privacidad.

2.2 ¿Cuál es su finalidad?

El objetivo de esta Guía es proveer las bases para el uso adecuado y responsable de los datos, además de brindar conocimientos sobre los fundamentos éticos que deberán considerarse para el desarrollo de proyectos de sistemas de toma o soporte de decisión y en el diseño de algoritmos que utilicen los modelos de datos, donde existen potenciales

riesgos éticos y legales, como el uso sesgado de los datos, para fomentar de esa manera la innovación responsable.

2.3 ¿Cuál es su importancia?

Dado el escenario actual, existen diferentes situaciones en las que el marco jurídico puede no ser suficiente para evitar el uso de los datos de forma que conlleve un riesgo para la autonomía individual, el bienestar y la dignidad de los seres humanos, entre otras circunstancias.

La ética de datos puede ayudar a ilustrar e instruir sobre los criterios de recolección, el intercambio y el uso responsable de los datos por parte de las personas y los sistemas desarrollados al respecto, al mismo tiempo, intenta mejorar la capacidad de cumplimiento de las diferentes normativas que le sean aplicables.

Esta Guía brinda un marco sobre el cual se deben deslindar enfoques para el diseño y la implementación de iniciativas o proyectos que impliquen sistemas de toma de decisión y ciencia de datos. Es necesario entonces, considerar la ética de datos como una base dinámica para la evaluación y orientación de las tecnologías, contemplando la dignidad humana, el bienestar y la prevención de daños.

2.4 De la guía

Los datos deben ser recopilados solamente para finalidades legítimas y por medios legales. En principio, la recopilación de datos debería ser limitada y realizarse con el conocimiento o el consentimiento de la persona. No deberían recopilarse datos sobre personas excepto en las situaciones y con los métodos permitidos o autorizados por ley y (por lo general) deberían darse a conocer a las personas afectadas en el momento en que se recopilen.

El requisito de legitimidad abarca el concepto de legalidad y excluye el tratamiento arbitrario y caprichoso de Datos. Implica transparencia y una estructura jurídica a la cual pueda tener acceso la persona cuyos datos estén recopilándose. En la mayoría de los contextos se puede cumplir el requisito de legitimidad si el recopilador o encargado de los Datos informa al Titular sobre las bases jurídicas de la solicitud de los Datos en el momento de su recopilación (por ejemplo, “se solicita su número de identificación personal de conformidad con la Ley Nacional de tránsito”). En otros casos podría necesitar una explicación diferente, como “se requiere esta información para garantizar que el reembolso se envíe a la dirección correcta del reclamante”. En tales casos, se deberían indicar claramente las finalidades para las cuales se recopilan los datos, a fin de que la persona pueda entender cómo se recopilarán, usarán o divulgarán los datos.

Los datos deben ser tratados con responsabilidad y buenas prácticas para evitar lo que a continuación veremos.

A los fines de ampliar los conceptos asociados a qué tipos de datos pueden tratarse y los requisitos para ello, recomendamos la lectura de la Guía de Clasificación de Datos.

2.5 ¿A quién va dirigida?

Esta Guía está dirigida a cualquier persona que trabaje directa o indirectamente con datos en el sector público, incluidos los profesionales de datos como estadistas, analistas y científicos de datos, responsables, personal operativo y quienes ayudan a producir una visión informada de los datos, también a aquellos funcionarios e instituciones públicas que tienen planificado desarrollar proyectos tecnológicos que involucran el uso intensivo y el análisis de datos para mejorar su gestión o entrega de servicios a las personas.

2.6 ¿Cómo utilizarla?

Esta Guía presenta en primer lugar, los conceptos, principios, consideraciones legales y éticas, además de las acciones específicas sobre la ética en el uso de datos para que aquellas personas que desarrollen o participen en proyectos que impliquen una gestión de datos, tengan una base fundamental para mitigar posibles impactos negativos y riesgos que puedan derivarse de ellos.

En adición, esta Guía proporciona tablas de evaluación práctica y preguntas de orientación sobre la actualidad y estado en que se encuentre la persona parte del proyecto o sistema en cuestión respecto al uso ético de datos. En esos términos, cualquier persona que requiera indicaciones o fundamentos para analizar y evaluar su presente frente al uso ético de datos, puede recurrir a esta Guía y obtener los resultados existentes, además de oportunidades de mejora.

2.7 Estado del arte

La ética en el uso de los datos involucra a todo tipo de datos de muy diferentes maneras.

Por ejemplo, si publicamos datos sobre contaminación en una ciudad y lo hacemos únicamente para las zonas menos contaminadas estaríamos haciendo un uso claramente poco ético y responsable de esos datos.

Si cumplimos con las directivas y leyes de protección de datos correspondientes podemos pensar que ya tenemos garantizado un uso ético y responsable de los datos que gestionamos. Sin embargo, aunque la legislación sobre protección de datos es muy variada entre los distintos países y en algunos casos también muy completa, no suele generalmente cubrir aspectos éticos más generales.

El Open Data Institute[1] define una serie de pautas éticas a través del Esquema de la ética de los datos, estableciendo los principales elementos a plantearse:

- Descripción de nuestras fuentes de datos:
    - ✔ ¿Cuáles son sus características principales?
    - ✔ ¿Quién tiene derechos y permisos sobre ellas y con quiénes se comparten?
    - ✔ ¿Qué limitaciones pueden tener en la actualidad?
    - ✔ ¿Qué políticas y legislación son aplicables?

[1] Open Data Institute

- ✔ ¿Se comprende cuál es su propósito?
- ✔ ¿Quiénes pueden verse positivamente o negativamente afectados?
- ✔ ¿Cómo podríamos minimizar el impacto negativo?
- ✔ ¿Cómo podrían los afectados interactuar con la organización?

● Gestión de riesgos:

- ✔ ¿Se están comunicando los riesgos adecuadamente?
- ✔ ¿Cuál es la política de revisión de riesgos?
- ✔ ¿Qué acciones están previstas?

La ética deberá estar presente en todas las etapas del ciclo de vida y gestión de los datos, ya que si por ejemplo ignoramos a ciertos grupos durante la fase de recolección de datos (por ejemplo, en base a su etnia, posición social o género), esto tendrá graves consecuencias posteriormente ya que dichos grupos simplemente no existirán como parte de la población representada en esos datos y serán por tanto discriminados en cualquier uso posterior que se haga de los mismos.

Cada organización deberá establecer sus propias pautas éticas específicas en base al uso de los datos que hagan en cada caso. Existen también organizaciones globales que trabajan para establecer pautas de referencia en sus respectivas áreas de conocimiento que podríamos adoptar directamente, como por ejemplo las pautas éticas para la protección de los datos y la privacidad de la Comisión Europea[2] el grupo de interés en aspectos éticos y sociales de los datos de la Research Data Alliance[3] o el framework ético de la ciencia de los datos del Gobierno de Reino Unido[4].

2.8 Sesgos y discriminación

En cuanto a los riesgos más conocidos que conlleva el uso y gestión de los datos, el esgo y la discriminación son los que más preocupan, por suponer o implicar un agravio muy grave contra los derechos de las personas.

En primer lugar, la discriminación se caracteriza por la posibilidad de involucrar tanto a una persona como a un grupo de personas, las cuales, a causa de la misma, resultan posicionadas en una situación menos ventajosa o diferente respecto de otra persona o personas, basado en razones, como su origen étnico, género, religión, orientación sexual, opiniones políticas, entre otras. Esta discriminación puede darse de una forma tanto directa como indirecta, es decir, que a pesar de que una decisión aparente ser neutral, suponga un perjuicio al sujeto discriminado.

Un sesgo, en cambio, es aquel error que favorece repetidamente a un grupo, siendo el error sistemático en una dirección o en un subconjunto específico de datos, se trata de un sesgo.

Una de las materias en las que más se encuentran sesgos y discriminaciones es el género,

[2] Data protection and privacy ethical guidelines (europa.eu)
[3] RDA – Ethics and Social Aspects of Data (ESAD) Interest Group Case Statement | RDA (rd-alliance.org)
[4] Data_science_ethics_framework_v1.0_for_publication__1_.pdf (publishing.service.gov.uk)

debido a la falta de la aplicación de una real perspectiva de género a la hora de construir los datasets y durante todo el ciclo de vida de los datos. Desde la SSPPBE construimos una guía sobre Datos con Perspectiva de Género (agregar link de la guía de Data Género), con herramientas para aplicar en organizaciones.

2.8.1 Sesgos

El sesgo puede presentarse en los modelos de decisión automáticos, más comúnmente como resultado de un algoritmo desarrollado, de manera intencional o no con ese sesgo, o que este se origine directamente de la base de datos utilizada. A continuación, se presentan las diferentes circunstancias en las cuales se puede presentar un sesgo dentro de lo habitual desde el desarrollo hasta la implementación de un sistema de toma de decisiones.

Creación de un sistema de toma de decisiones:

El problema de sesgo que se presenta cuando se quiere implementar un sistema de decisión automático o semiautomático, surge por la falta de un análisis del impacto que pueda derivar del mismo para la población en un momento y lugar determinados.

Esto es así por porque, si bien el objetivo de instituir un sistema de decisión es resolver un problema específico, en un primer aproximamiento no se cuenta con un examen o visión global que incorpore a todas las personas que puedan ser potencialmente impactadas por el problema, sin estimar e identificar específicamente si existen subgrupos de la población para los cuales se quiere garantizar equidad.

Entrenar un modelo de toma de decisiones:

En este punto se utilizan promedios sin considerar los diferentes subgrupos que posea la población. En la gran mayoría de estos casos, los responsables utilizan datos históricos sin tener en cuenta diferentes factores y contextos, lo cual puede implicar un problema grave, ya que esto puede favorecer a grupos de la población que son mayoría, dejando plenamente de lado las necesidades particulares de grupos minoritarios. Un ejemplo que se viene repitiendo desde hace tiempo se trata de los sistemas automáticos de contrataciones, el cual por diferentes factores favorece constantemente a los hombres. Estos factores corresponden a la manera en que el sistema aprende diversas características, como el hecho de que históricamente en ciertas industrias los empleados eran siempre hombres, es decir, al utilizarse datos de contrataciones de los últimos años, la herramienta aprende a favorecer a los hombres.

El sistema no sesga por género de manera directa e intencional, pero a causa de los datos históricos que le enseñaron, deja por fuera a mujeres.

Recopilación sesgada de datos:

La recopilación de datos se realiza directamente de manera sesgada, aunque sea de forma no intencional. Como ejemplo de este sesgo, se pueden mencionar las encuestas realizadas en el ámbito público que son reflejadas en una base de datos, y que se utilizan luego para toma de decisiones, sea para otorgar o quitar beneficios, realizar estadísticas o desarrollar algún proyecto. En este sentido, cuando se lleva a cabo una encuesta, por ejemplo, para recopilar información sobre profesiones por hogar y en la pregunta sobre ocupación se otorga como opción “ama de casa”, se indica que sólo la mujer tendrá esta ocupación ya que es femenino, por lo cual los hombres que ejerzan labores domésticas, es decir, que posean esa profesión no figuraran en los resultados de dicha encuesta. Como resultado, se producirá un sesgo en la recopilación de datos e impactará potencialmente en los proyectos que utilicen esta base de datos.

Sesgo en sistemas de reconocimiento:

Los sistemas de reconocimiento por imágenes pueden sesgar en cuanto las bases de datos otorgan definiciones de imágenes a gran escala, que luego se utilizarán para desarrollar modelos de reconocimiento facial, proyectos de inteligencia de actividad humana, entre otros. El problema allí resulta de la desigualdad de representación de esas imágenes según un contexto, por ejemplo, cuando las imágenes de búsqueda arrojan resultados que muestran ciertas etnias o razas para profesiones específicas. Esto último resulta en un sesgo por cuanto no se representa la diversidad que pueda existir en las profesiones en cuanto a género, edad y raza, entre otros y este sesgo será luego replicado en el sistema o proyecto que se va a desarrollar sobre esa base de datos.

De dichas tecnologías de reconocimiento facial también pueden derivarse algunos sesgos en los resultados que devienen del entrenamiento que se ha otorgado. Para educar o entrenar un sistema, se utilizan datos o imágenes que reflejan personas de determinada edad, raza y género, por lo cual dichos modelos poseen mayores tasas de error en los demás grupos de la población que no pertenezcan a las que allí son reflejadas.

Con todo lo anterior, se manifiestan los sesgos potenciales que pueden resultar de los datos utilizados para la ejecución y desarrollo de un proyecto, incluso antes de que se introduzca para la población general. Por este motivo, es sumamente necesario que sean tenidos en cuenta desde la etapa de formulación de esos proyectos, es decir, apenas se proponga su objetivo, para poder estimar el impacto que pueda llegar a tener y afectar a la población y en ese caso, para buscar soluciones a esas potenciales consecuencias no deseadas del sistema.

Cuando se toman decisiones de carácter público en base a sesgos, forzosamente resultará en una discriminación contra determinados grupos de la población, lo cual se verá a continuación.

2.8.2 Discriminación

Actualmente, existen legislaciones que reconocen que puede existir discriminación producto de la toma de decisiones automatizadas[5]. A este tipo de discriminación se la llama "discriminación algorítmica", una de sus características reside en que reproduce tipos de discriminación existentes en el mundo real. La misma puede tener su origen en una variedad de razones que incluyen que los datos recopilados representan solo a una fracción de la población, que se haya desarrollado o entrenado sobre una base de datos sesgada, o que exista una falta de actualización en los datos, entre otras cosas.

Este tipo de discriminación se la califica de "algorítmica" porque lo que permite que esta se instale y se propague en los sistemas informáticos es el uso del aprendizaje automatizado y de la inteligencia artificial (IA).

La discriminación algorítmica es aquella que refleja en sus procesos distintos tipos de diferencia, exclusión, preferencia o segregación que suelen ocurrir en la cotidianeidad y se reproducen en el entorno de datos, o que surgen de ellos, como por ejemplo, cuando los sistemas de reconocimiento facial los cuales fueron expuestos en el punto anterior, reportan mayores errores al procesar rostros que no se asemejen a los rasgos de las personas en las imágenes más frecuentes en las búsquedas las cuales no reflejan la diversidad que existe.

De esta manera, se suele referir a estos datos como "imperfectos", "incorrectos", "inexactos" o "incompletos" ya que estos revelan los sesgos en que incurrieron las personas que realizaron su recopilación. Además, como ya se ha presentado, los datos pueden revelar potenciales problemas de insuficiencia, error, carencia en cuanto a la falta de representación de algunos grupos de la sociedad como las minorías, y exceso en caso de representación de las mayorías, lo cual puede llevar a que puede derivar en una decisión algorítmica equivocada.

Las consecuencias de reproducir algorítmicamente procesos discriminatorios que reflejan aquellos existentes en el mundo real, tiene que ver con los posibles impactos negativos, es decir, los perjuicios que puedan resultar en contra de la población.

Comúnmente se describe a estos sistemas señalando que su capacidad predictiva resulta simplemente de la extrapolación en el futuro de dinámicas identificadas en el pasado. De esta forma, un algoritmo aprenderá y llevará impregnado los errores discriminaciones del pasado, por ejemplo, que ciertas razas o etnias sean consideradas de tener una mayor tendencia a cometer delitos.

A pesar de todo esto, es menester recordar que la discriminación existe también en el proceso humano de toma de decisiones. Allí, puede ser un desafío incorporar algoritmos, aprendizaje automatizado y la IA para evitar sesgos de producto humano, y cuidar de que no sean reproducidos. Desafortunadamente, en la mayoría de los casos, los algoritmos no han aportado una mejora, sino que, por el contrario, han contribuido a la discriminación y sesgos.

En este contexto, y para contrarrestar la incidencia negativa que trae el desarrollo de nuevas tecnologías, se han instituido nuevos derechos apuntando a la transparencia de los

[5] artículo 22, General Data Protection Regulation (GDPR)

algoritmos y abocando por los derechos humanos.

Actualmente, la discriminación digital deriva en la posibilidad de restringir el acceso a servicios, empleos, y variedad de herramientas digitales, provocando un grave perjuicio en la población. Es por esta razón que deberá considerarse desde el principio en el diseño de algoritmos, tener un enfoque preventivo y de supervisión.

Algunas de las medidas que se deberán tener en consideración son, la necesidad de incluir la disminución de sesgos en los procesos de aprendizaje algorítmico, la generación de habilidades en funcionarios, y que estos se encuentren capacitados para prevenir actos de discriminación, además de velar por enseñar el desarrollo de la no discriminación desde el diseño de los proyectos.

2.9 Paso a paso para identificar sesgo o discriminaciones en datos

En línea con lo explicado en los puntos anteriores se recomienda realizar los siguientes pasos para evitar el uso sesgado de los datos:

a. **Paso 1: Advertir el sesgo en la creación de un sistema de toma de decisiones:**

   Se recomienda realizar un examen o visión global que tenga en consideración a todas las personas que puedan ser potencialmente impactadas por los resultados del proyecto y evaluar los posibles escenarios en los que el sistema derive en un efecto no deseado. Es imprescindible identificar específicamente si existen subgrupos de la población para los cuales se requiere garantizar equidad.

b. **Paso 2: Prevenir la recopilación sesgada de datos:**

   Se propone verificar que la recopilación de datos se realice observando cuidar la terminología, el sentido, y el propósito o finalidad con la que se utilizarán los mismos, además de las cuestiones que se consideren necesarias para mitigar el impacto negativo que pueda resultar para las personas. Además, se aconseja revisar las bases de datos adquiridas de un tercero, en su caso, para evitar el uso de datos incompletos, erróneos y potencialmente discriminatorios.

c. **Paso 3: Evaluar sesgos a la hora de entrenar un modelo de toma de decisiones:**

   Para entrenar un modelo de toma de decisiones, es necesario cerciorarse de que no se refleje en el diseño, es decir desde su algoritmo, un potencial sesgo que afecte a las personas o grupo de personas. Además, en caso de utilizar datos históricos para los sistemas de toma de decisión, se recomienda comprobar si los mismos puedan llegar a impactar de manera negativa en detrimento de los derechos de los diferentes grupos que puedan existir en la población.

d. **Paso 4: Evitar el sesgo en el desarrollo y sucesión del proyecto:**

   Una vez que se ha establecido el objetivo del proyecto, se ha realizado la recopilación de datos o se ha utilizado una base de datos preexistente y se ha efectuado el entrenamiento del sistema o modelo, se recomienda revisar que este último se encuentre en línea con los objetivos preestablecidos desde su comienzo y a su vez, examinar si el propósito es alcanzado sin perpetrar un sesgo potencial para las personas o grupo de personas. Por último, es necesario comprobar que el modelo o

sistema se mantenga actualizado y en caso de ser imprescindible se debe velar por modificar el algoritmo para evitar que se produzca un daño potencial en caso de que el mismo pueda sesgar o discriminar a un grupo de personas.

2.10 Responsabilidades en el uso de datos

Quienes traten datos, como fue mencionado anteriormente, se encuentran obligados y son responsables.

En primer lugar, se entiende que son responsables de resguardar la licitud de su desarrollos, siendo que las mismas siempre se encontrarán bajo un marco jurídico determinado, y comprendiendo dicho marco tanto a las regulaciones locales como a las fuentes de derecho internacional. En este sentido, deberán verificar que se cuente con la base legal requerida para poseer, operar y utilizar una base de datos, con el objetivo de adecuarse a dichos estándares normativos aplicables.

Dentro del tratamiento de los datos, se sostiene que deberán identificar si existe dicha base, datos personales o datos personales sensibles, según la clasificación de nuestro cuerpo normativo, y a partir de allí brindar la protección y cuidado que la misma legislación en vigor requiere para resguardar la privacidad. Para tal fin se recomienda recurrir a la Guía de Clasificación de Datos.

En este sentido, aquellas personas que gestionan datos personales tienen la responsabilidad de tener en cuenta las limitaciones del uso de los datos, en la medida que una mala gestión puede implicar un daño en una persona o un grupo de personas. En segundo lugar, y como complemento al punto anterior, existe la responsabilidad de utilización de principios éticos, durante todo el ciclo de vida de los datos. Dichos principios implican que, aunque las regulaciones no llegarán al punto de tratar un determinado punto, se deberían tener en cuenta las normas éticas de la sociedad, al obrar sobre dichos puntos.

Los funcionarios públicos, por su parte, tienen la responsabilidad de garantizar la gestión ética de los datos, adoptando las medidas necesarias para ello. De esta forma, deberían tener en cuenta los aspectos éticos de los datos durante los períodos de contrataciones, de la misma forma que deberían exigir que quienes gestionan datos se pongan en contacto con estas autoridades en casos de posibles lesiones a derechos, o para determinar el alcance y los límites de los intercambios de datos.

En línea con esto, se deberá asegurar y garantizar siempre que la gestión de datos genere confianza y transparencia en las distintas etapas del ciclo de vida de los datos, es decir, en la generación, recolección, almacenamiento, eliminación, acceso, intercambio y finalmente, durante su uso.

Por ese motivo, es necesario gestionar esos datos conforme con los instrumentos normativos aplicables, tanto de la legislación nacional como internacional, las directrices o recomendaciones formales, códigos de conducta, hasta las herramientas de autoevaluación y códigos de integridad o ética.

Por último, se considera que quienes controlen datos deberán garantizar la robustez de los sistemas que los almacenan. La robustez, como responsabilidad, insta a los

desarrolladores a intentar lograr el funcionamiento confiable de los sistemas, así como a tomar las medidas de protección necesarias para evitar cualquier efecto adverso imprevisto.

Se establece, además, como responsabilidad de las personas involucradas en los procesos que hagan uso de los datos, conocer las bases de gobernanza, los mecanismos y herramientas recomendadas para el acceso y el intercambio con la finalidad de garantizar que sean respetados los lineamientos establecidos al respecto, por lo cual se aconseja que tengan en cuenta, apliquen y utilicen las siguientes Guías:

2.11 Otras consideraciones éticas

Además de las responsabilidades mencionadas anteriormente, existen otras consideraciones éticas, las cuales deben ser consideradas a lo largo de todo el proceso. Las mismas son la proporcionalidad y la aceptación social.

✔ Proporcionalidad: teniendo en cuenta los costos de los proyectos de ciencia de datos, se considera relevante tener en cuenta otras posibilidades, que pudieran atender a la necesidad actual sin el uso de un modelo. De esta forma, deberá evaluarse si este medio es el más adecuado, como así también, debe ponderarse que los beneficios sean mayores a los posibles riesgos.

✔ Aceptación social: se considera a la aceptación social de un proyecto como un punto a tener en cuenta ya que esta aceptación no es solo una opinión, sino que tiene también aplicaciones prácticas que pueden definir el futuro de un desarrollo, de una tecnología. Este punto se encuentra íntimamente ligado con el principio de transparencia, en tanto es central en esta consideración explicar quién y con qué finalidad utilizará los datos, así como la forma en la que se los tratará durante todo el proceso.

2.12 Big Data y el uso ético de datos

¿Por qué debemos tener mayor precaución respecto del tratamiento de datos cuando es Big Data que en Small data?

El incremento en la capacidad de procesamiento de datos generado por el Big data deja la toma de decisiones casi totalmente en manos de la IA. Sin embargo, deberá entenderse que los algoritmos entrenados con el fin de realizar predicciones, las toman en base a probabilidades, y siempre existirá un marco de error. Un ejemplo de esto es un correo electrónico de spam que no es clasificado automáticamente por el algoritmo de detección.

Con el fin de limitar los efectos negativos, existen diferentes métodos aplicables:

✔ Evaluación de algoritmos: consiste en reportes periódicos que permiten desarrollar un mapeo constante de los programas del sector público, de cómo se están implementando los principios éticos y de los desafíos encontrados en este proceso.

✔ Limpieza de datos: es un método que consiste en limitar los prejuicios y los errores en los datos que se utilizan en el desarrollo de las IA. Dicho método puede estar compuesto por acciones como monitorear los errores, mejorar la calidad de los datos, buscar datos duplicados, y la estandarización de procesos.

✔ Evaluación de legitimidad: es un modelo relacionado por la Web foundation para evaluar la legitimidad de aplicación de los sistemas de inteligencia artificial, considerando como legítimos a aquellos procedimientos explicables y que contengan responsabilidades rastreables.

✔ Códigos internos de conducta y/o ética: tienen el fin de establecer los comportamientos esperados de quienes, a lo largo del ciclo de vida de estas tecnologías, cumplan con los principios éticos para las iniciativas de datos: respeto a las personas, respeto a los derechos humanos, participación y responsabilidad por las decisiones.

3. Principios generales de la ética de datos

Con el fin de manipular los datos recolectados de acuerdo con las buenas prácticas, se entiende que aquellos a cargo de realizar este manejo, deberán actuar teniendo en cuenta ciertos principios, con el objetivo de implementar buenas prácticas de uso. Dichos principios deberán tener en cuenta, especialmente, el tipo de datos con los que se trabajará; es decir, si se tratará datos personales, datos personales sensibles o alguna categoría especial de datos, de acuerdo con lo establecido en la Guía de Clasificación de Datos.

Estos principios comprenden la transparencia, la rendición de cuentas, la equidad, la sustentabilidad, la acción y supervisión humana, la solidez técnica y seguridad, y la protección y privacidad de datos. Los mismos se encuentran definidos a continuación:

3.1 Transparencia

El principio de transparencia se encuentra mencionado en la Ley 104-CABA-1998 de Acceso a la Información Pública. La misma obliga a los responsables a facilitar el acceso a los interesados, presentando la información pública de forma clara, estructurada y entendible.

Deberá ser considerado como la apertura para brindar información significativa sobre el diseño, funcionamiento, e impacto que tienen los sistemas de toma de decisiones automatizados para aquellos individuos que pueden verse afectados por sus decisiones y resultados. De esta forma, la información deberá ser de fácil acceso y comprensible, con el fin de promover la participación activa de la población durante el ciclo de vida de los sistemas de Inteligencia Artificial.

Por otro lado, deberá presentarse información comprensible sobre la posibilidad de los falsos positivos o falsos negativos que puede dar como resultado un algoritmo, así como sus indicadores de desempeño. Se considera que incluso en los sistemas denominados “Black Box”, donde se dificulta la comprensión, se deberá explicar su denominación y sus posibles efectos. Es decir, se deberá presentar información clara sobre los objetivos que persigue este sistema.

Como fue mencionado anteriormente, la aceptación de la población general es un componente que se deberá encontrar presente a la hora de implementar un proceso en que se realice este tipo de gestión de datos. La importancia de la transparencia reside, en

este caso, en la necesidad de la formación de una opinión por parte de la ciudadanía. Se entiende que la retención de información puede derivar en una crisis de confianza entre el gobierno y la ciudadanía.

Se entiende que, en virtud de preservar el principio de transparencia, deberá evitarse la opacidad sobre el funcionamiento de los algoritmos, es decir, el desconocimiento o la negativa a explicar. Dicha Opacidad puede ser intencional, intrínseca o analfabeta:

✔ Opacidad intencional: ocurre en aquellos casos en los que los propietarios carecen de transparencia por voluntad propia. Estos casos pueden darse tanto por motivos de propiedad intelectual como por una necesidad de mantener la opacidad para asegurar el funcionamiento del sistema

✔ Opacidad intrínseca: se da en los casos en los que la complejidad del mismo sistema no permite su explicación. Con el crecimiento de los proyectos de Big Data, y el incremento en el volumen de los datos procesados, comienzan a aparecer casos en los que incluso los desarrolladores de los sistemas son incapaces de entender el funcionamiento de los mismos.

✔ Opacidad analfabeta: se denomina tal a aquellos casos en los que el funcionamiento de un sistema no puede realizarse sobre la base de que la población general no se encuentra debidamente educada para comprender. Se entiende que, si bien un sistema puede ser explicable en la teoría, y quienes lo desarrollan pueden ser abiertos respecto de su funcionamiento, bien puede generarse opacidad frente a una sociedad que no maneja el lenguaje técnico requerido para una adecuada comprensión del mismo.

3.2 Rendición de cuentas (accountability)

La rendición de cuentas o “Accountability” indica que quienes controlen datos, serán sujetos obligados frente a las normativas, originando responsabilidades y dando lugar a posibles sanciones ante un incumplimiento.

La rendición de cuentas no solo refiere a la responsabilidad, sino también a la capacidad de demostrar que se encuentran en cumplimiento con las regulaciones vigentes.

La rendición de cuentas trae como consecuencia que el sistema deberá ser auditable, es decir, que sea posible evaluar los algoritmos, datos y procesos de diseño.

Se considera que el sistema deberá ser “auditable”, entendiéndose como tal a la capacidad para evaluar los algoritmos, datos y etapas de diseño. Con el fin de aumentar la confianza en los sistemas desarrollados, se considera buena práctica contar con informes de auditoría a su disposición.

Otra directriz que compone la rendición de cuentas es la notificación de los efectos negativos, siendo tarea del obligado informar sobre las acciones que hayan tenido impactos negativos en los sujetos, así como responder por las consecuencias de este resultado. En concordancia con este principio y con el fin de aumentar la confiabilidad, es relevante mencionar que las personas que sufran un perjuicio como resultado de una mala gestión, deben tener derecho a recibir una compensación proporcional al daño.

De esta manera, se considera que también debe posibilitar la “trazabilidad”, entendiéndose como tal a la posibilidad de rastrear los eventos. Como concepto, tiene la función de complementar a la auditabilidad y a la notificación de los efectos negativos, facilitando las tareas de identificar posibles errores o fallas durante el proceso.

3.3 Equidad

El principio de equidad apunta a reducir la reproducción de los sesgos al mínimo posible. Se entiende que a lo largo de la realización de todos los proyectos de implementación de algoritmos se deberán tener en cuenta posibles sesgos que pueden manifestarse. Este punto se encuentra desarrollado en la siguiente cláusula.

3.4 Sesgos y discriminación

Este principio deberá tenerse presente ante la existencia de grupos vulnerables, para los cuales deberá resaltarse la equidad y tener en cuenta dichas vulnerabilidades al momento de la toma de decisiones. En este punto, es considerado buena práctica que los equipos de trabajo encargados de gestionar datos tengan una composición diversa, en aras de obtener una perspectiva amplia.

Es necesario aclarar a su vez que, si bien la no discriminación como principio es válida, no resulta ser suficiente en los casos que se deba solucionar una desigualdad preexistente, o donde las tomas de decisiones se encuentren previamente sesgadas.

En estos casos, por lo tanto, se volverá válido favorecer, en una medida razonable, a los individuos o grupos perjudicados.

Uno de los aspectos esenciales en cuanto a evitar los sesgos y discriminaciones, es la construcción y tratamiento de datos con perspectiva de género.

Desde la SSPPBE construímos una guía que brinda herramientas para estos casos en particular.

3.5 Sustentabilidad

En el contexto actual de creciente aumento poblacional y cambio climático, con el objetivo de beneficiar a todos los seres humanos, incluyendo a las generaciones futuras y teniendo en cuenta el principio de equidad, se entiende que tanto el conjunto de la sociedad como el medio ambiente son partes interesadas. Consecuentemente, se considera que, al realizar un proyecto, no se puede dejar de tener en cuenta la sustentabilidad y la responsabilidad ecológica. Se deberá contribuir en la generación de un ambiente sano, equilibrado y que satisfaga las necesidades presentes sin comprometer a las generaciones futuras.

A su vez, si bien los sistemas de toma de decisiones son utilizados para resolver problemáticas actuales, dicho uso debería armonizar con el medio ambiente, en la medida de lo posible.

Las tres dimensiones de la sostenibilidad: protección ambiental, justicia social y economía equitativa. Ahora necesitamos saber cuáles son estos criterios, cuándo aplicarlos y cómo

hacerlo.

Cuando hablamos de criterios sostenibles nos referimos a aquellas pautas que evitan o, en su defecto, minimizan el impacto ambiental, económico y social que se esté planificando, desarrollando o explotando.

Estos criterios hacen compatible cada Acción con la preservación del valor del Capital Natural y, por ende, los servicios de los ecosistemas, asegurando el bienestar humano.

3.6 Acción y supervisión humanas

La acción y supervisión humanas, como principio, tiene la finalidad de evitar la obstaculización de los derechos fundamentales. Se entiende como acción humana a aquellas decisiones realizadas con conocimientos y herramientas necesarias para comprender los sistemas, teniendo la capacidad de evaluarlos o cuestionarlos.

Por otra parte, la supervisión humana ayuda a garantizar que un sistema no menoscabe la autonomía humana o provoque otros efectos adversos.

La supervisión en gobierno deberá ser: por un lado, modelos supervisados y por otro, la supervisión humana posterior, la que puede consistir en mecanismos de gobernanza, tales como el mando humano. El mismo refiere a la capacidad de supervisar la actividad general de un sistema, así como la libertad de decidir cómo y cuándo utilizar un sistema en una decisión particular. De esta manera, se puede decidir no utilizar un sistema en una situación en la que se considere innecesario, permitiendo que se ejerza la discrecionalidad humana durante el uso del sistema, o habilitar la posibilidad de ignorar una decisión adoptada por un sistema.

3.7 Solidez técnica y seguridad

Se entiende por solidez técnica a la necesidad de desarrollar sistemas con enfoques preventivos en relación con los riesgos, minimizando así daños involuntarios e imprevistos.

Los sistemas deberán ser protegidos frente a las vulnerabilidades que pudieran ser explotadas. Esto puede darse en forma de ataques por parte de agentes malintencionados contra los datos, el modelo o la infraestructura informática subyacente. Tales ataques pueden afectar la forma de toma de decisiones del sistema, o incluso detener su funcionamiento.

De esta misma forma, se recomienda intentar lograr el mayor nivel de precisión posible, efectuando las predicciones, recomendaciones, o tomando decisiones correctas en la mayoría de los casos. El fin de la precisión se encuentra relacionado con mitigar posibles errores en los procesos mencionados anteriormente o, de no ser así, indicar la probabilidad de que se produzcan estos errores.

A su vez, se requiere que el sistema sea fiable y confiable, siendo la primera característica la capacidad de funcionar adecuadamente con un conjunto de información y en diversas situaciones; y la segunda, la repetición de un comportamiento en las mismas condiciones.

3.8 Gestión de la privacidad de los datos

Se considera que los sistemas deberán garantizar la protección de la intimidad y de los datos a lo largo de todo el ciclo de vida de un sistema. Esto incluye la información inicialmente otorgada por el usuario, así como la información obtenida sobre el usuario como producto de las interacciones constantes con el sistema.

Se entiende que los registros digitales del comportamiento humano pueden otorgar la posibilidad a los sistemas de inferir aquellos datos personales sensibles, como orientación sexual u opiniones políticas y religiosas.

3.9 Big data y el uso ético de datos

Debido a esto, se deberá asegurar que toda información recabada de esta manera no se utilizará para generar una discriminación injusta o ilegal.

Se entiende que los datos utilizados deberán ser de calidad, en la medida que no contengan sesgos sociales, imprecisiones o errores. Por otra parte, se deberá garantizar la integridad de los datos, ya sea mediante sistemas desarrollados internamente como los adquiridos externamente.

A su vez, se debe mencionar la importancia de limitar el acceso a los datos. Éstos deberían ser, en principio, manipulados solamente por aquellas personas necesarias para tal fin, con el propósito de reducir el riesgo de causar un perjuicio al sujeto. Adicionalmente, se recomienda contar con personal debidamente calificado para procesar datos, con conciencia del impacto que podría tener un incidente, y con un amplio conocimiento de la legislación y buenas prácticas en materia de ética.

3.10 ¿Cómo se aplican?

Se considera que los principios desarrollados anteriormente deberían, en la medida de lo posible, tener una aplicación práctica.

Se deberían documentar las decisiones del proceso de a lo largo de todo el proceso de desarrollo e implementación, con el fin de facilitar la transparencia de los algoritmos, así como la rendición de cuentas.

En lo relativo a la equidad, se entiende que la mejor forma de garantizarla es definiendo posibles subgrupos que puedan sufrir sesgos. Al entrenar modelos, se deberán tener en cuenta no solo datos históricos, sino también a aquellos grupos minoritarios que podrían ser dejados de lado.

Por lo tanto, se considera una buena práctica presentar los resultados de diferentes subgrupos a las herramientas implementadas, buscando que no surjan diferencias entre éstos (por ejemplo, las posibles diferencias en estadísticas anteriores al separar por género).

Con el fin de regirse de acuerdo con el principio de sustentabilidad durante el desarrollo de sistemas, deberán evaluarse en su totalidad el proceso de desarrollo, despliegue y utilización de sistemas, así como toda su cadena de suministro, a través, por ejemplo, de un

seguimiento del uso de recursos y del consumo de energía durante la formación, dando prioridad a las opciones menos perjudiciales. Se deberían promover medidas que garanticen el respeto del medio ambiente por parte de todos los eslabones de la cadena de toma de decisiones. A su vez, se indica realizar Evaluaciones de Impacto Ambiental; mantener controlada la huella de carbono, en caso de tratarse de una organización; y realizar Análisis del Ciclo de Vida de un producto, teniendo en cuenta que los mismos se encuentran en declive en un marco de práctica masiva de obsolescencia programada.

Con el fin de salvaguardar la acción y supervisión humanas, deberá llevarse a cabo una evaluación del impacto sobre los derechos fundamentales. Esta evaluación deberá llevarse a cabo antes del desarrollo de los sistemas en cuestión e incluir una evaluación de las posibilidades de reducir dichos riesgos o de justificar estos como necesarios en una sociedad democrática para respetar los derechos y libertades de otras personas. Además, deberían crearse mecanismos que permitan conocer las opiniones externas sobre los sistemas que pueden vulnerar los derechos

fundamentales.

Se recomienda, para garantizar la Seguridad y la Solidez Técnica, realizar un Plan de repliegue y seguridad general, es decir, medidas que posibiliten un plan de repliegue en el caso de que surjan problemas. Además, se deberán establecer procesos dirigidos a aclarar y evaluar los posibles riesgos asociados con el uso de sistemas en los diversos ámbitos de aplicación. El nivel de las medidas de seguridad requeridas depende de la magnitud del riesgo que plantee un sistema, que a su vez depende de las capacidades del sistema. Cuando se prevea que el proceso de desarrollo o el propio sistema planteará riesgos particularmente altos, es crucial desarrollar y probar medidas de seguridad de forma proactiva.

En lo que respecta a la privacidad de los datos, en cualquier organización que maneje datos personales (con independencia de si alguien es usuario del sistema o no) deberán establecerse protocolos que rijan el acceso a los datos. En esos protocolos deberán describirse quién puede acceder a los datos y en qué circunstancias.

4. Conclusión

A lo largo de esta guía, se han determinado los retos más relevantes para el sector público en cuanto al uso ético y gestión de los datos y, como consecuencia, se advierte la necesidad de instituir un marco que facilite el uso adecuado y responsable de los datos, como así también, brindar conocimientos fundamentales para el desarrollo de proyectos de sistemas de toma o soporte de decisiones y en el diseño de algoritmos que utilicen los modelos de datos.

Tal como se ha desarrollado en el presente documento, existe actualmente un contexto donde regularmente se presentan situaciones que pueden llevar un riesgo para la autonomía individual, el bienestar y la dignidad de las personas.

Es por esto que también se incorporó la importancia de plasmar el uso de datos con perspectiva de género. Ya que es necesario observar y tener presentes los principios, normas, reglamentos, regulaciones y/o prácticas éticas, contenidos en esta guía, que

ofrezcan las herramientas necesarias para evitar cualquier tipo de sesgo, discriminación o cualquier otro perjuicio a los derechos fundamentales de las personas.

ANEXO I

APLICACIÓN EN UN PROYECTO

1. ACCIONES ESPECÍFICAS

1.1 DEFINIR Y ENTENDER LA NECESIDAD DE LOS USUARIOS

Previo a la recolección de datos, deberá realizarse las siguientes preguntas con el objeto de concluir si es efectivamente necesario la recolección de dichos datos:

1.1.1 COMPRENDER EL BENEFICIO PÚBLICO EN GENERAL

✔ ¿Cuáles son los beneficios directos para individuos en este proyecto? (por ejemplo, ahorrar tiempo al solicitar un servicio gubernamental servicio gubernamental)

✔ ¿De qué manera el proyecto ofrece resultados sociales positivos para el público en general?

✔ ¿Cómo puede medir y comunicar los beneficios de este proyecto al público?

✔ ¿Cuáles son los grupos que se verían desfavorecidos por el proyecto/ que no se benefician del proyecto?

✔ ¿Qué se puede hacer al respecto?

✔ ¿Qué individuos, grupos, grupos demográficos u organizaciones se verán afectados positivamente por este proyecto? ¿Cómo?

1.1.2 COMPRENDER LAS CONSECUENCIAS INVOLUNTARIAS Y/O NEGATIVAS DE SU PROYECTO

✔ ¿Cuál sería el perjuicio de no utilizar los datos?

✔ ¿Qué resultados sociales podrían no alcanzarse?

✔ ¿Cuáles son los posibles riesgos o consecuencias negativas del proyecto, frente al riesgo de no seguir adelante con el proyecto?

✔ ¿Podría el mal uso de los datos o el mal diseño, contribuir a reforzar los problemas sociales, éticos y las desigualdades?

✔ ¿Qué tipo de mecanismos puede poner en marcha para evitar que esto ocurra?

✔ ¿Qué grupos específicos se benefician del proyecto?

✔ ¿Qué grupos pueden verse privados de oportunidades o sufrir consecuencias negativas por culpa del proyecto?

✔ ¿Qué medidas puede tomar para minimizar el daño?

✔ ¿Cómo podría reducir las limitaciones en sus fuentes de datos? ¿Cómo mantiene segura la información personal y otra información confidencial?

✔ ¿Cómo está midiendo, informando y actuando sobre los posibles impactos negativos de su proyecto?

✔ ¿Qué beneficios aportarán estas acciones a tu proyecto?

1.1.3 JUSTIFICAR EL USO ADECUADO DE RECURSOS PÚBLICOS EN SU PROYECTO

✔ ¿Cómo puede demostrar la rentabilidad de su proyecto?

✔ ¿Existe una gobernanza eficaz y una supervisión de la toma de decisiones para garantizar el éxito del proyecto?

✔ ¿Tiene pruebas que demuestren todo lo anterior?

1.1.4 BENEFICIO PÚBLICO TRANSPARENTE

✔ ¿Puede publicar información sobre cómo el proyecto ofrece resultados sociales

positivos para el público?

✔ ¿Las personas entienden su propósito, especialmente las personas de las que se tratan los datos o que se ven afectadas por su uso?

✔ ¿Cómo pueden las personas interactuar con el responsable del proyecto?

✔ ¿Cómo pueden las personas corregir la información, apelar o solicitar cambios en el proyecto?

✔ ¿Son razonables y bien entendidos los mecanismos de apelación?

✔ ¿Qué tan abierto puedes ser sobre este proyecto? ¿Podría publicar su metodología, metadatos, conjuntos de datos, código o mediciones de impacto?

✔ ¿Va a compartir datos con otras organizaciones? Si es así, ¿quién?

1.2 CUMPLIMIENTO DE LA LEY

Deberá conocer las leyes, reglamentos y códigos de buenas prácticas usuales relacionados con el uso de los datos. En caso de duda, deberá consultar a los expertos pertinentes.

1.2.1 OBTENER ASESORAMIENTO JURÍDICO

✔ ¿Ha hablado con un asesor jurídico dentro de su organización?

✔ ¿Ha hablado con su equipo de seguridad de la información o ciberseguridad?

✔ ¿Ha consultado al responsable de protección de Datos de su organización?

✔ ¿Qué asesoramiento jurídico ha recibido?

✔ ¿Qué códigos éticos existentes se aplican a su proyecto?

✔ ¿Qué legislación, políticas u otras regulaciones determinan cómo usar los datos?

✔ ¿Qué requisitos introducen?

Es su deber y obligación obedecer la ley en cualquier proyecto de datos. Deberá dar cumplimiento a la Ley CABA No 1845/2006 sobre Protección de Datos Personales.

Un aspecto importante del cumplimiento de la Ley de protección de datos, es ser capaz de demostrar qué medidas técnicas y organizativas son utilizadas, con el objeto de garantizar que todo está documentado, y el tratamiento que es realizado sobre los datos.

1.2.2 OTRAS RECOMENDACIONES LEGALES-PROTECCIÓN DE DATOS DESDE EL DISEÑO: Si bien es un principio que no se encuentra, actualmente, legislado en nuestro país, es una práctica recomendable incorporar este principio de protección de datos desde el diseño y por defecto, con el objeto de poder analizar si el nuevo proyecto se ajusta al cumplimiento de la ley y la gobernanza de los datos.

EVALUACIÓN DE IMPACTO: Otro punto importante y recomendable para realizar es, previo a la puesta en marcha del proyecto, una evaluación de impacto, con el objeto de analizar si existe un alto riesgo para los derechos de las personas, especialmente cuando se utilizan nuevas tecnologías.

1.3 REVISAR LA CALIDAD Y LAS LIMITACIONES DE LOS DATOS

Cuando hablamos de calidad de datos, hacemos referencia a que los datos personales deberán ser relevantes para el propósito de su uso y, como así también, exactos, completos y actuales.

Cuando hablamos de limitaciones de los datos, hacemos referencia a tres tipos de limitaciones:

✔ Limitación en la recolección de los datos, donde deberán existir límites para la recolección de datos personales y cualquiera de estos datos deberán obtenerse por medios legales y justos y, contar con el consentimiento del sujeto implicado.

✔ Limitación del propósito, es decir que, el propósito de la recolección de datos se deberá especificar a más tardar en el momento en que se produce dicha recogida, y su uso se verá limitado al cumplimiento de los objetivos u otros que no sean incompatibles con el propósito original, especificando en cada momento el cambio de objetivo.

✔ Limitación de uso, es decir, que no se deberá divulgar, poner a disposición o usar los datos personales para propósitos que no cumplan lo expuesto anteriormente, excepto que:

- Se cuente con el consentimiento del sujeto implicado,
- por imposición legal o de las autoridades (por ejemplo, se puede disponer que los datos recopilados con fines de toma de decisiones administrativas puedan estar disponibles para investigación, estadísticas y planificación social),

- Fuentes de acceso público de datos,
- tus datos están en listados que se limitan a datos de nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio,
- tus datos fueron obtenidos por una relación contractual, científica o profesional y son necesarios para su desarrollo o cumplimiento,
- se trata de las operaciones que hacen las entidades financieras y de las informaciones que reciben de sus clientes,
- un organismo público que obtuvo tus datos en ejercicio de sus funciones los cede a otro organismo público para que los use con una finalidad que está dentro de sus funciones.

De esta manera, deberán asegurarse de que los datos recolectados en el proyecto sean precisos, representativos, proporcionales a la finalidad para la cual son recolectados, de buena calidad y que se pueda explicar cuáles son sus limitaciones.

✔ ¿Estoy recolectando estrictamente los datos que necesito en función de mi finalidad?

✔ ¿Existen finalidades conexas y compatibles que requieran de otro tipo de datos?

✔ ¿Estoy ofreciendo opciones al titular de datos para comunicar un tipo de datos personales y no otros?

✔ ¿Se informó debidamente a los titulares de los alcances de la información que se recolectarán?

✔ ¿La información es clara y completa?

1.3.1 FUENTES DE DATOS

Previo al inicio en la recolección de datos se deberá determinar cuáles son las fuentes de obtención de los datos, ya sea que esté realizando la recolección directamente, o esté utilizando una fuente de datos externa.

Asimismo, deberá identificar cuál es la norma o base legal que autoriza el tratamiento.

De esta forma, deberá preguntarse:

✔ ¿Hay algún dato personal involucrado, o datos considerados sensibles?

✔ ¿Qué fuente(s) de datos se utiliza(n)?

✔ ¿Obtengo la información directamente de los titulares? En caso contrario, ¿mis fuentes son fuentes públicas de acceso irrestricto? ¿Obtengo la información de cesiones o comunicaciones, en cumplimiento de la ley local?

✔ ¿Son los individuos y/o las organizaciones que proporcionan los datos conscientes de cómo se utilizarán? Si el usuario está reutilizando los datos para su análisis sin el consentimiento individual, ¿cómo se ha garantizado que la nueva finalidad es compatible con el motivo original de la recolección?

✔ ¿Se entienden claramente todos los metadatos y los nombres de los campos?

✔ ¿Entiende cómo se generan los datos para el proyecto?

✔ ¿Los datos se recopilan para este proyecto o para otro propósito?

✔ ¿Qué procesos tiene en marcha para garantizar y mantener la integridad de los datos?

✔ ¿Cuáles son las advertencias? ¿Cómo se tendrán en cuenta las advertencias para cualquier política o servicio futuro que utilice este trabajo como base de pruebas?

✔ ¿Por qué medios se realiza la recolección de datos?

✔ ¿Se realiza por algún mecanismo automatizado?

✔ ¿Qué empleados de la organización o eventual personal tercerizado están involucrados en el proceso de recolección?

Asegúrese de conocer la procedencia y el linaje de los datos (orígenes de los datos y cómo y por qué se recopilaron), especialmente cuando los datos provienen de una fuente externa.

Al trabajar con múltiples fuentes, podría ser útil realizar un inventario de datos para ayudar a identificar, organizar y describir las diferentes fuentes de datos que recopila, accede y mantiene.

1.3.2 SESGO EN LOS DATOS

¿Cómo se han evaluado los datos? ¿Se han evaluado para detectar posibles sesgos?

✔ En este punto se deberá considerar:

✔ Si los datos puedan llegar a reflejar (con exactitud) una práctica histórica sesgada que no se desea reproducir en el nuevo proyecto (sesgo histórico).

✔ Si los datos pueden ser una representación errónea y sesgada de la práctica histórica, por ejemplo, porque sólo ciertas categorías de datos se registraron adecuadamente en un formato accesible para el proyecto (sesgo de selección).

✔ Si se utilizan datos sobre personas, ¿es posible que su modelo o análisis pueda identificar variables de características protegidas que puedan conducir a un resultado discriminatorio?

✔ Dichas variables pueden ser potencialmente una causa de discriminación indirecta; deberá considerar si el uso de estas variables es apropiado en el contexto de su proyecto.

✔ ¿Qué medidas ha tomado para mitigar el sesgo?

Para mayor información se remite a la cláusula correspondiente a este tema 2.8 Sesgos y discriminación

1.3.3 DETERMINACIÓN DE LA PROPORCIONALIDAD

En este criterio deberá:

✔ Identificar que solamente se traten los datos necesarios para la finalidad del tratamiento.

✔ Evaluar la pertinencia de recabar datos con fines históricos, científicos o estadísticos.

✔ Definir si existen mecanismos de actualización de datos.

✔ Identificar cuál es el procedimiento para eliminar los datos una vez agotada la finalidad.

✔ Analizar la necesidad de mantener los datos bloqueados y en ese caso definir los procedimientos de disociación. Es decir, que deberá utilizar el mínimo de datos necesarios para lograr el resultado deseado.

Los datos personales deberán ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se procesan.

✔ ¿Cómo se puede cumplir el objetivo del proyecto utilizando los datos personales

mínimos posibles?

✔ ¿Hay alguna manera de lograr el mismo objetivo con menos datos identificables,

por ejemplo, datos seudonimizados?

✔ Si se utilizan datos personales que identifican a los individuos, ¿qué medidas se aplican para controlar el acceso?

✔ ¿Los datos de entrada son adecuados y necesarios para alcanzar el objetivo?

✔ ¿El uso propuesto de los datos para fines secundarios hace que sea menos probable que las personas quieran volver a dar esos datos para el propósito principal para el que se recogieron?

✔ ¿Cómo puede explicar por qué necesita utilizar estos datos?

✔ ¿Este uso de los datos interfiere con los derechos de los individuos? En caso afirmativo, ¿existe una forma menos intrusiva de lograr el objetivo?

1.3.4 DATOS ABIERTOS Y COMPARTIBLES

Si los datos no son sensibles, y si los acuerdos de intercambio de datos con el proveedor lo permiten, deberá hacer que los datos sean abiertos y compartibles, de acuerdo a lo especificado en la siguiente Guía.

1.4 CANVAS DE ÉTICA DE DATOS

El Data Ethics Canvas es una herramienta para cualquier persona que recopile, comparta o use datos, cuyo objeto consiste en identificar y gestionar problemas éticos, tanto al comienzo de un proyecto que utiliza datos, como dentro de su desarrollo.

Es una herramienta utilizada para gestionar las preguntas a realizarse, como así también a reflexionar sobre dichas respuestas.

El Data Ethics Canvas se basa en el Ethics Canvas[i], un marco de alto nivel para evaluar las implicaciones éticas de cualquier proyecto, desarrollado por el Centro ADAPT para la Tecnología de Contenidos Digitales.

La presente Guía fue confeccionada utilizando las premisas impartidas por el Fata Ethics Canvas, por esta razón, para mayor información se solicita ingresar en The Odi.

ANEXO II

CUADROS DE AUTOEVALUACIÓN

2.1 CUADROS DE AUTOEVALUACIÓN PARA LOS 7 PRINCIPIOS GENERALES

A continuación, se presenta el cuadro de evaluación del estado de madurez de cada uno de los principios generales de la ética de datos, expuestos previamente.

En los siguientes cuadros se deberá indicar la situación en la que se encuentra respecto a la gestión ética de los datos, donde se describen los siguientes criterios para los puntajes detallados en cada uno de los principios.

2.1.1 TRANSPARENCIA

La transparencia significa que sus acciones, procesos y datos están abiertos a la publicación de forma completa, de fácil acceso y en formato gratuito.

Criterios establecidos:

Puntaje uno (1): La información sobre el proyecto, sus métodos y resultados no está disponible públicamente. Existe un amplio desconocimiento de los datos existentes y una fuerte negativa a explicar.

Puntaje dos (2): La información sobre el proyecto, sus métodos y resultados se encuentra disponible en forma limitada y se realiza la explicación parcial.

Puntaje tres (3): Se facilita el acceso a los interesados, presentando la información pública de forma clara, estructurada y entendible.

TRANSPARENCIA		
PUNTAJE		
1	2	3

2.1.2 RENDICIÓN DE CUENTAS (ACCOUNTABILITY)

La rendición de cuentas o “Accountability” indica que quienes controlen datos, serán sujetos obligados frente a las normativas, originando responsabilidades y dando lugar a

posibles sanciones ante un incumplimiento.

Criterios establecidos:

Puntaje uno (1): No se han establecido mecanismos de control, gobernanza o revisión del proyecto.

Puntaje dos (2): se han establecido mecanismos de control, gobernanza o revisión del proyecto limitados.

Puntaje tres (3): Integración de mecanismos de control público en el ciclo de vida del proyecto.

RENDICIÓN DE CUENTAS		
PUNTAJE		
1	2	3

2.1.3 EQUIDAD

El principio de equidad apunta a reducir la reproducción de los sesgos y discriminación al mínimo posible.

Criterios establecidos:

Puntaje uno (1): existe un riesgo significativo de que el proyecto resulte en daño o discriminación del público o ciertos grupos.

Puntaje dos (2): existe un riesgo parcial de que el proyecto resulte en daño o discriminación del público o ciertos grupos.

Puntaje tres (3): existe un riesgo bajo de que el proyecto resulte en daño o discriminación del público o ciertos grupos.

EQUIDAD		
PUNTAJE		
1	2	3

2.1.4 SUSTENTABILIDAD

Al hablar de sustentabilidad se considera que, al realizar un proyecto, no se puede dejar

de tener en cuenta la sustentabilidad y la responsabilidad ecológica.

Criterios establecidos:

Puntaje uno (1): no tienen en cuenta el impacto ambiental, económico y social durante la toma de decisiones para el desarrollo del proyecto.

Puntaje dos (2): tienen en cuenta parcialmente el impacto ambiental, económico y social durante la toma de decisiones para el desarrollo del proyecto.

Puntaje tres (3): promueven medidas que garantizan el respeto del medio ambiente por parte de todos los eslabones de la cadena de toma de decisiones.

SUSTENTABILIDAD		
PUNTAJE		
1	2	3

2.1.5 ACCIÓN Y SUPERVISIÓN HUMANAS

Se entiende como acción humana a aquellas decisiones realizadas con conocimientos y herramientas necesarias para comprender los sistemas, teniendo la capacidad de evaluarlos o cuestionarlos.

Criterios establecidos:

Puntaje uno (1): no se realiza una evaluación de impacto sobre los riesgos a afectar derechos fundamentales.

Puntaje dos (2): se tiene en cuenta el impacto a derechos fundamentales; sin embargo, no se realiza una evaluación formal

Puntaje tres (3): se realizan evaluaciones de impacto y seguimientos de posibles riesgos de afectar derechos fundamentales.

ACCIÓN Y SUPERVISIÓN HUMANAS		
PUNTAJE		
1	2	3

2.1.6 SOLIDEZ TÉCNICA Y SEGURIDAD

Se entiende por solidez técnica a la necesidad de desarrollar sistemas con enfoques

preventivos en relación con los riesgos, minimizando así daños involuntarios e imprevistos.

Criterios establecidos:

Puntaje uno (1): no cuentan con una protección para los riesgos presentes en los sistemas

Puntaje dos (2): cuentan con una protección baja o ineficiente frente a posibles riesgos.

Puntaje tres (3): los sistemas se encuentran debidamente protegidos frente a vulnerabilidades.

SOLIDEZ TÉCNICA Y SEGURIDAD		
PUNTAJE		
1	2	3

2.1.7 GESTIÓN DE LA PRIVACIDAD DE LOS DATOS

Se considera que los sistemas deberán garantizar la protección de la intimidad y de los datos a lo largo de todo el ciclo de vida de un sistema. Esto incluye la información inicialmente otorgada por el usuario, así como la información obtenida sobre el usuario como producto de las interacciones constantes con el sistema.

Criterios establecidos:

Puntaje uno (1): no existen protocolos efectivos de control de acceso a los datos

Puntaje dos (2): existen protocolos de control de acceso a los datos, pero los mismos se gestionan informalmente

Puntaje tres (3): existen protocolos eficaces de control de acceso a datos.

GESTIÓN DE LA PRIVACIDAD DE DATOS		
PUNTAJE		
1	2	3