Universidad de la Ciudad de Aguascalientes

Legalidad y Protección de la Información

Caso 3

Contexto: Una empresa de telecomunicaciones desea desarrollar un modelo de machine learning para predecir qué clientes tienen mayor probabilidad de cancelar su servicio. Para ello, se dispone de una amplia base de datos (Un metadato es información que describe y contextualiza otros datos, facilitando su organización y acceso. Los microdatos son unidades de información detalladas y específicas, como registros individuales en una base de datos. Los macrodatos, por otro lado, son grandes volúmenes de datos que suelen ser analizados para identificar patrones o tendencias. En conjunto, una base de datos es un sistema que utiliza metadatos para organizar tanto microdatos como macrodatos, asegurando su correcta gestión y análisis.) que incluye información personal de los clientes como edad, género, ingresos, historial de consumo, entre otras variables.

Marco ético y legal

- Privacidad: El modelo requiere el uso de datos personales sensibles que podrían revelar información privada sobre los clientes.
- Discriminación: Existe el riesgo de que el modelo perpetúe o incluso amplifique sesgos existentes en los datos, lo que podría conducir a decisiones discriminatorias contra ciertos grupos de clientes.
- Transparencia: Es importante garantizar que el modelo sea transparente y comprensible, tanto para los desarrolladores como para los reguladores.

Identificación y gestión de datos personales

- Inventario de datos: Se realiza una exhaustiva revisión de los datos para identificar qué información es considerada personal y sensible.
- Minimización de datos: Se seleccionan solo los datos necesarios para desarrollar el modelo, evitando el uso de información excesiva o irrelevante.
- Anonimización y seudonimización: En la medida de lo posible, se aplican técnicas de anonimización y seudonimización para proteger la identidad de los clientes.

  Técnicas de anonimización:
  - Seudonimización
  - Enmascaramiento de datos
  - Generalización
  - Agregación de datos
  - Supresión
  - Permutación
  - Perturbación

    - K-anonimato
    - L-diversidad y T-closeness
- Consentimiento informado: Se obtiene el consentimiento explícito de los clientes para el uso de sus datos en el proyecto, informándoles sobre los fines del tratamiento y sus derechos.

Generación de un modelo ético

- Evaluación de sesgos: Se realizan análisis exhaustivos para identificar y mitigar posibles sesgos en los datos y en el modelo.
- Transparencia algorítmica: Se utilizan técnicas de explicación de modelos para hacer comprensible el funcionamiento del modelo y las decisiones que toma.
- Accountability (responsabilidad y actitud): Se establecen mecanismos de rendición de cuentas para garantizar que el modelo se utilice de manera responsable y ética.

Métricas de seguridad

- Protección de datos: Se implementan medidas técnicas y organizativas para proteger los datos personales de accesos no autorizados, pérdidas, alteraciones o destrucciones.
- Cumplimiento normativo: Se garantiza el cumplimiento de la legislación vigente en materia de protección de datos, como el GDPR en la Unión Europea o la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) en México.

Aportaciones

- Mayor confianza de los clientes: Al garantizar la privacidad y seguridad de los datos, se fomenta la confianza de los clientes en la empresa.
- Mejora de la reputación: El cumplimiento de las normas de protección de datos contribuye a mejorar la imagen de la empresa.
- Desarrollo de modelos más robustos y fiables: La identificación y mitigación de sesgos conduce a modelos más precisos y justos.
- Evitar sanciones legales: El incumplimiento de la legislación en materia de protección de datos puede acarrear graves consecuencias legales y económicas.

Actividad colaborativa

¿Qué otras técnicas podrían utilizarse para garantizar la privacidad en este tipo de proyectos?

¿Cómo se puede conciliar la necesidad de desarrollar modelos precisos con la protección de los derechos individuales?

¿Cuál es el papel de los científicos de datos en la promoción de una ética de la inteligencia artificial?

Rol Arquitecto Tecnológico:

¿Qué otras técnicas podrían utilizarse para garantizar la privacidad en este tipo de proyectos?

Asegurarse de emplear conjuntos de datos diversos y representativos, aplicar técnicas de validación cruzada (Holdout, Estratificada, k-fold) a los modelos entrenados, además es recomendable fortalecer la seguridad y privacidad de los datos utilizados para el entrenamiento y operación del modelo así como aplicar técnicas de protección a cada uno de las etapas del ciclo de vida de los datos empleados en el entrenamiento.

¿Cómo se puede conciliar la necesidad de desarrollar modelos precisos con la protección de los derechos individuales?

Establecer procedimientos que aseguren la actualización de modelos, y reglas de seguridad previamente establecidas, con esto se permitirá abordar y proteger ante nuevas vulnerabilidades y amenazas descubiertas.

¿Cuál es el papel de los científicos de datos en la promoción de una ética de la inteligencia artificial?

El científico de datos es el responsable del diseño e implementación de las técnicas y tecnologías de inteligencia artificial, por ello es su responsabilidad el conocer, difundir y aplicar las técnicas apropiadas que permitan el desarrollo ético de soluciones en el campo de la inteligencia artificial.

Rol Arquitecto de Visualizaciones:

¿Qué otras técnicas podrían utilizarse para garantizar la privacidad en este tipo de proyectos?

- **Privacidad diferencial**: Esta técnica añade ruido matemático a los datos antes de su análisis, asegurando que no se pueda reidentificar a los individuos.

- **Federated learning (aprendizaje federado)**: Permite el entrenamiento de modelos de machine learning en los dispositivos donde los datos son generados, sin que los datos personales sean centralizados, lo que protege la privacidad del usuario.
- **Control de acceso basado en roles**: Asegurarse de que solo los empleados con permisos específicos puedan acceder a los datos sensibles, aplicando técnicas como el control de acceso granular para minimizar el riesgo de violación de la privacidad.

¿Cómo se puede conciliar la necesidad de desarrollar modelos precisos con la protección de los derechos individuales?

El equilibrio entre precisión y privacidad puede lograrse a través de:

- **Minimización de datos**: Utilizar únicamente los datos que son estrictamente necesarios para el desarrollo del modelo, eliminando cualquier información irrelevante o excesiva.
- **Evaluación constante del sesgo**: Los modelos deben ser evaluados y ajustados para mitigar cualquier sesgo inherente que pueda surgir de los datos sensibles como género, edad o ingresos, asegurando que las decisiones automatizadas no perpetúen discriminaciones.
- **Modelos explicativos**: Desarrollar modelos que sean transparentes y cuyos resultados sean comprensibles tanto para los usuarios como para los reguladores. Esto asegura que los clientes puedan entender cómo se utilizan sus datos.
- **Actualización continua de los modelos**: Mantener los modelos en constante revisión y actualización para asegurar que las medidas de protección de datos estén alineadas con las nuevas normativas y tecnologías.

¿Cuál es el papel de los científicos de datos en la promoción de una ética de la inteligencia artificial?

Los científicos de datos tienen un rol crucial en la ética de la inteligencia artificial:

- **Diseño ético**: Son responsables de diseñar e implementar modelos que respeten la privacidad y los derechos de las personas. Esto implica aplicar técnicas para mitigar sesgos y garantizar la equidad en los resultados.
- **Divulgación y educación**: Deben promover prácticas éticas dentro de sus equipos, abogando por el uso responsable de la IA y educando a otros profesionales sobre los riesgos y beneficios de la tecnología.
- **Auditoría y transparencia**: Los científicos de datos deben trabajar activamente en garantizar la transparencia de los modelos, haciendo visibles y comprensibles las

decisiones automatizadas y asegurando que los sistemas de IA puedan ser auditados para verificar su equidad y precisión.

- **Responsabilidad**: Son responsables de anticipar las consecuencias sociales de los modelos que desarrollan, desde la discriminación hasta los impactos en la privacidad, y deben garantizar que sus prácticas se alineen con normativas legales y principios éticos claros.

Marco legal & BPM

¿Qué otras técnicas podrían utilizarse para garantizar la privacidad en este tipo de proyectos?

Para garantizar la privacidad en este proyecto, es crucial aplicar la anonimización y la sodomización para proteger la identidad de los clientes, utilizando técnicas como el anonimato. La empresa debe asegurar la minimización de datos, recolectando solo lo esencial, y obtener un consentimiento informado claro, cumpliendo con la Ley Federal de Protección de Datos Personales (LFPDPPP). Además, se deben evaluar y mitigar sesgos en el modelo, garantizar la transparencia algorítmica, y asegurar la rendición de cuentas, en línea con normativas internacionales como el GDPR. Esto refuerza la confianza y evita riesgos legales.

¿Cómo se puede conciliar la necesidad de desarrollar modelos precisos con la protección de los derechos individuales?

Para conciliar la precisión de los modelos con la protección de los derechos individuales, es necesario aplicar técnicas de anonimización y seudonimización que protejan la identidad sin afectar la calidad de los datos, junto con la minimización de datos recolectando solo lo esencial. Además, realizar evaluaciones de sesgos y garantizar la transparencia algorítmica permite evitar discriminaciones y asegurar que los modelos sean comprensibles. Esto debe complementarse con el consentimiento informado de los usuarios y el cumplimiento de normativas como el GDPR o la LFPDPPP, estableciendo una clara rendición de cuentas.

¿Cuál es el papel de los científicos de datos en la promoción de una ética de la inteligencia artificial?

El rol de los científicos de datos en la promoción de una ética en la inteligencia artificial reviste una importancia fundamental, al ser los responsables de la creación y supervisión de algoritmos cuyo uso puede afectar derechos fundamentales. Es imperativo que velen por la

transparencia en los modelos desarrollados, previniendo prácticas discriminatorias y asegurando el cumplimiento normativo en el tratamiento de datos personales, conforme a marcos legales como el GDPR y la LFPDPPP. Asimismo, deben implementar técnicas de minimización de datos y anonimización para mitigar riesgos asociados a la privacidad, promoviendo siempre la rendición de cuentas y la equidad en las aplicaciones de IA, con el fin de garantizar que sus impactos sean beneficiosos y respetuosos de los derechos individuales.

Kevin Gustavo Domínguez López

3 Principales puntos del decálogo.
1.- Privacidad.
2.-Auditoría.
3.-Transparencia.

En es te caso es fundamental considerar principalmente 3 puntos del decálogo de ética para ciencia de datos como lo es:

1.- Privacidad. La “privacidad” es uno de los principales y más delicados conceptos que se manejan al trabajar con bases de datos que contienen información personal y sensible de las personas como lo son los ingresos,género e historiales.

2.-Auditoría. Se requiere mantener una seguridad en el proceso de trabajo por lo cual es de suma importancia tener “auditorías” constantes que mantengan un aseguramiento del manejo y protección de la información para poder evitar el mal uso de estos.

3.-Transparencia. Ya que el caso de trabajo menciona que la toma de decisiones se generará por distintos grupos de trabajo es muy necesario la óptima comprensión en todo momento y esto conlleva el tener una óptima “transparencia” y así todos puedan tener una plena confianza en el proceso.
(El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, n.d.)

Andrea Graciela López Segura

Con el fin de mejorar la experiencia de nuestros clientes y desarrollar un proyecto que nos permita identificar con mayor precisión sus necesidades, solicitamos su consentimiento explícito para el uso de ciertos datos personales, los cuales serán gestionados bajo estrictas medidas de seguridad y conforme a las regulaciones vigentes. Nos comprometemos a tratar

sus datos con la máxima confidencialidad, implementando altos estándares de privacidad que incluyen auditorías independientes para asegurar el cumplimiento de nuestras políticas de protección de datos.

Los datos proporcionados serán tratados de manera anónima y únicamente para los fines indicados en este proyecto, garantizando en todo momento la seguridad y protección de su información. Además, usted tendrá la posibilidad de consultar, en cualquier momento, cómo se están utilizando sus datos, asegurando una total transparencia en el proceso.

Es fundamental para la empresa que este tratamiento de datos se realice con el respaldo adecuado. Por lo tanto, solicitamos la firma de un consentimiento informado que autorice el uso de su información personal para el desarrollo del proyecto. Este consentimiento asegura el cumplimiento de todas las normativas de privacidad y protección de datos, como el Reglamento General de Protección de Datos (RGPD) o la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en caso de aplicar), y establece nuestro compromiso con un tratamiento seguro y responsable de su información.

Solicitamos a todos los equipos encargados de la recopilación, tratamiento y análisis de datos que verifiquen que los formatos de consentimiento informado sean debidamente firmados y almacenados de manera segura. Esto no solo garantizará el respaldo legal necesario para la ejecución del proyecto, sino que también asegurará el cumplimiento de las auditorías internas y externas que se llevarán a cabo para verificar la correcta gestión de la información de nuestros clientes.

Al proceder de esta manera, aseguramos que el proyecto se desarrollará dentro del marco legal vigente y bajo los principios de ética, responsabilidad y transparencia que rigen nuestra empresa.

Ulises Paz Vidales

Para este caso es necesario contar con la experiencia del Marco jurídico (BPM) y de procesos, para manejar de manera legal la información, además de un arquitecto tecnológico aunado al trabajo de un arquitecto de diseño de hardware y firmware para tener la seguridad que la base de datos sea segura y se manejen los principios antes mencionados; donde las responsabilidades serían:

Marco jurídico: garantiza que los datos sean manejados de manera conforme a las normativas vigentes.
Arquitecto Tecnológico: Diseñar la técnica de procesamiento de datos, asegurando escalabilidad, seguridad y eficiencia.
Arquitecto de diseño de hardware y firmware: generar la estructura y medios para asegurar que las bases de datos sean fiables, acesibles.

***Nota,** dependiendo del tamaño de la empresa, número de empleados, capacidades, es necesario la revaloración de los roles, agregando más para ajustarse a las necesidades de la empresa.

Mitsiu Alejandro Carreño Sarabia

Se requieren accesos empleando protocolos de red seguros (HTTPS) en formatos estructurados o semiestructurados, dichos accesos deben presentar alta disponibilidad, integración con accesos programáticos (automatizable), se recomienda emplear arquitecturas API (interfaz de programación de aplicaciones en inglés) y REST (transferencia de estado representacional en inglés). Además se espera contar con reportes detallando tiempos de inactividad, su duración así como su causa (actualización de servicio/arquitectura o respuesta a incidentes).

Marco Antonio Rodríguez Rangel

Para conseguir la visualización adecuada se necesita definir qué variables se mostrarán en el tablero de control resultante, protegiendo la privacidad de la información, no colocando datos confidenciales de manera directa, además de mantener un diseño estético y no cargado de información, siempre manteniendo la atención del usuario hacia lo que se desea presentar, además de incluir el cómo se usó la información para tener una transparencia de su uso.

Otro aspecto a considerar es evitar incluir maneras en que la información mostrada pueda ser sesgada por algún filtro (por ejemplo el género) para así mantener una imparcialidad correcta ante esta situación.

Andrés Daniel Pérez Rodríguez

Minimización de datos: En virtud de lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, se establece con claridad el principio de minimización de datos, el cual dispone que el tratamiento de datos personales debe circunscribirse únicamente a aquellos que resulten adecuados, pertinentes y estrictamente necesarios en relación con los fines para los cuales dichos datos son recabados. Tal principio se encuentra consagrado en diversos artículos de la mencionada ley, en particular en el Artículo 13, el cual prescribe que "El tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad. En particular para datos personales sensibles, el responsable deberá realizar esfuerzos razonables para limitar el periodo de tratamiento de los mismos a efecto de que sea el mínimo indispensable". Asimismo, en lo que respecta al tratamiento de datos

personales sensibles, el mismo artículo impone al responsable la obligación de "limitar el periodo de tratamiento de los mismos, de modo que este sea el mínimo indispensable".

Limitación del plazo de conservación: En el contexto jurídico, la limitación del plazo de conservación de datos personales resulta fundamental para garantizar el derecho a la protección de los datos de los titulares, conforme lo establece la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. De acuerdo con el Artículo 25 de dicha Ley, el titular tiene el derecho inalienable de cancelar sus datos personales en cualquier momento, lo que activa un periodo de bloqueo durante el cual dichos datos no podrán ser tratados, salvo para determinar responsabilidades relacionadas con su tratamiento. Este periodo de bloqueo, según lo estipulado, será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que originó el tratamiento de los datos. Posteriormente, y una vez cumplido el periodo de bloqueo, es obligación del responsable proceder a la cancelación definitiva de los datos en cuestión. Esta disposición subraya la importancia de que los datos personales no sean conservados más allá del tiempo necesario para cumplir con la finalidad para la cual fueron recabados, asegurando así el respeto a los derechos del titular y previniendo un tratamiento indebido o excesivo de la información.

Integridad y confidencialidad: En el ámbito de la protección de datos personales, la integridad y confidencialidad son pilares fundamentales para asegurar que la información sensible sea manejada con el más alto estándar de seguridad. De acuerdo con lo establecido en el Artículo 21 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, los responsables y terceros que participen en cualquier etapa del tratamiento de datos personales están obligados a mantener la confidencialidad de dicha información. Esta obligación no solo se extiende durante el curso de la relación con el titular de los datos, sino que persiste incluso después de la finalización de dicha relación, garantizando así una protección continua contra cualquier tratamiento no autorizado o ilícito, así como contra la pérdida, destrucción o daño accidental de los datos personales. El cumplimiento de estos principios no solo es un deber legal, sino un compromiso ético esencial en la salvaguarda de los derechos de privacidad de los individuos.

Limitación de Datos: En virtud de lo dispuesto por la Ley de Privacidad de 1974, 5 U.S.C. § 552a(e)(1), toda agencia gubernamental que recopile datos personales está legalmente obligada a asegurar que dicha recopilación sea estrictamente limitada a la información pertinente y necesaria para cumplir con los fines para los cuales dichos datos son obtenidos. Este principio, conocido como la limitación de datos, se erige como un pilar fundamental en la protección de la privacidad individual, garantizando que la recolección de datos no sea excesiva ni irrelevante en relación con el propósito declarado. La transgresión de este principio puede constituir una violación directa de la Ley, exponiendo a la entidad infractora a posibles acciones legales, sanciones administrativas y la invalidez de los procedimientos basados en la recolección indebida de datos. Por lo tanto, la adherencia

estricta a la limitación de datos no es sólo un imperativo legal, sino una salvaguarda esencial de los derechos de privacidad consagrados en la normativa federal.

Omar Franco Ramirez

- ¿Qué otras técnicas podrían utilizarse para garantizar la privacidad en este tipo de proyectos?

Homomorfismo completamente homomórfico: Esta técnica permite realizar cálculos sobre datos cifrados sin descifrarlos, manteniendo la privacidad de la información en todo momento.
Diferencial privacy: Agrega ruido aleatorio a los datos antes de su análisis, dificultando la identificación de individuos específicos a partir de los resultados.
Federated learning: Entrena el modelo de machine learning en los dispositivos de los usuarios, en lugar de centralizar los datos, reduciendo el riesgo de brechas de seguridad.

- ¿Cómo se puede conciliar la necesidad de desarrollar modelos precisos con la protección de los derechos individuales?

Selección cuidadosa de variables: Utilizar solo las variables estrictamente necesarias para el modelo, evitando aquellas que puedan revelar información sensible.
Reducción de dimensionalidad: Reducir el número de dimensiones de los datos para disminuir la cantidad de información que se procesa.
Generalización de los datos: Agrupar los datos en categorías más amplias para reducir la granularidad y proteger la identidad de los individuos.

- ¿Cuál es el papel de los científicos de datos en la promoción de una ética de la inteligencia artificial?

Concientización: Difundir los principios éticos de la IA y sensibilizar a sus colegas y a la sociedad en general sobre los desafíos y las implicaciones de esta tecnología.
Diseño ético: Incorporar consideraciones éticas en todas las etapas del desarrollo de un modelo de machine learning, desde la recopilación de datos hasta la implementación.
Colaboración: Trabajar en conjunto con expertos en ética, abogados y otros profesionales para garantizar que los proyectos de IA se desarrollen de manera responsable.

A N E X O S :

Técnicas de anonimización (continuación):

1. Seudonimización:

- **Descripción:** Consiste en reemplazar los identificadores personales directos (como nombres, direcciones, números de seguro social) con un seudónimo o código.
- **Ventajas:** Reduce el riesgo de identificación directa.
- **Desventajas:** Si se conoce el sistema de codificación, es posible revertir el proceso.

2. Enmascaramiento de datos:

- **Descripción:** Se ocultan ciertos datos sensibles mediante técnicas como la sustitución de caracteres, encriptación o la utilización de patrones (por ejemplo, reemplazar los números de una tarjeta de crédito por “XXXX-XXXX-XXXX-1234”).
- **Ventajas:** Protege los datos sensibles en su forma original.
- **Desventajas:** Dependiendo del enmascaramiento, puede ser reversible si se conocen los métodos usados.

3. Generalización:

- **Descripción:** Se reduce la precisión de los datos mediante la agrupación en categorías amplias. Por ejemplo, en lugar de almacenar la edad exacta, se almacena un rango de edades (20-30, 30-40, etc.).
- **Ventajas:** Disminuye el riesgo de reidentificación, manteniendo cierta utilidad analítica.
- **Desventajas:** Puede perderse información valiosa para el análisis.

4. Agregación de datos:

- **Descripción:** Los datos individuales se combinan en grupos o se resumen para evitar la identificación de individuos. Un ejemplo sería publicar solo estadísticas agregadas en lugar de datos individuales.
- **Ventajas:** Protege completamente la identidad individual.
- **Desventajas:** Pierde precisión y detalle, lo que puede limitar su utilidad.

5. Supresión:

- **Descripción:** Se eliminan o suprimen ciertos elementos de los datos que podrían llevar a la identificación de una persona. Por ejemplo, omitir nombres o direcciones específicas.
- **Ventajas:** Reduce significativamente el riesgo de identificación.
- **Desventajas:** Puede llevar a la pérdida de datos importantes.

6. Permutación:

- **Descripción:** Se reorganizan los valores de los datos de forma que se pierda la relación directa entre la identidad y los atributos. Por ejemplo, permutar las fechas de nacimiento en un conjunto de datos de pacientes.
- **Ventajas:** Mantiene la distribución general de los datos.
- **Desventajas:** Puede no ser efectiva si se pueden combinar otros datos externos.

7. Perturbación:

- **Descripción:** Se añade "ruido" a los datos, modificando ligeramente los valores reales. Por ejemplo, cambiar ligeramente los ingresos reportados o modificar las ubicaciones geográficas por unos cuantos kilómetros.
- **Ventajas:** Hace más difícil la reidentificación al modificar los datos reales.
- **Desventajas:** Puede afectar la precisión de los resultados si el ruido añadido es demasiado significativo.

8. K-anonimato:

- **Descripción:** Es un enfoque que garantiza que cualquier dato individual no pueda distinguirse de al menos otros *k-1* individuos dentro del conjunto de datos. Esto se logra mediante técnicas como la generalización y la supresión.
- **Ventajas:** Ofrece un equilibrio entre privacidad y utilidad de los datos.
- **Desventajas:** Puede ser vulnerable a ataques de homogeneidad o vinculaciones si no se implementa adecuadamente.

9. L-diversidad y T-closeness:

- **Descripción:** Son mejoras sobre el k-anonimato que intentan proteger contra ataques basados en la falta de diversidad dentro de los datos generalizados o la proximidad de valores sensibles a valores generales.
- **Ventajas:** Mejora la privacidad en comparación con k-anonimato.
- **Desventajas:** Aumenta la complejidad del proceso de anonimización.

10. BPM

La gestión de procesos de negocio, según la definición de Gartner , emplea métodos para detectar, modelar, analizar, medir, mejorar y optimizar la estrategia y los procesos del negocio.

11.B2B

Es una abreviatura que significa Business to Business, lo cual en español se traduce como de empresa a empresa. Se refiere a un modelo de negocio en el que las transacciones comerciales se llevan a cabo entre compañías, en lugar de entre una empresa y un consumidor final (B2C).

Bibliografía

Autoridad Nacional de Protección de Datos de Singapur. (Octubre de 2022). *Guía básica de anonimización.* Obtenido de https://www.aepd.es/documento/guia-basica-anonimizacion.pdf

Sánchez de la Calle, A. (25 de Noviembre de 2022). *Cómo aplicar correctamente las técnicas de anonimización y seudonimización y la reidentificación de los datos personales.* Obtenido de prodat.es: https://www.prodat.es/blog/como-aplicar-correctamente-las-tecnicas-de-anonimizacion-y-seudonimizacion-y-la-reidentificacion-de-los-datos-personales/

El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (n.d.). *de privacidad*. Normativa y legislación en PDP Leyes en México para la protección de datos personales. https://micrositios.inai.org.mx/marcocompetencias/?page_id=370#:~:text=El%20art%C3%ADculo%2016%20de%20la,como%20oponerse%20a%20su%20uso.