



Tecnológico de Monterrey

Campus Querétaro

Política de Datos y Regulaciones de Privacidad

Gamaliel Marines Olvera	A01708746
Uri Jared Gopar Morales	A01709413
José Antonio Miranda Baños	A01611795
María Fernanda Moreno Gómez	A01708653
Oskar Adolfo Villa López	A01275287
Luis Ángel Cruz García	A01736345

Inteligencia artificial avanzada para la ciencia de datos II
Grupo 501

Introducción

La presente **Política de Datos y Regulaciones de Privacidad** tiene como finalidad establecer las directrices que regirán la recolección, almacenamiento, uso y protección de los datos en nuestro proyecto. El compromiso del equipo es garantizar la privacidad y seguridad de los datos de nuestros clientes, cumpliendo con las normativas legales aplicables y adoptando las mejores prácticas para la protección de la información.

Objetivo

El objetivo de esta política es garantizar que los datos sean gestionados de manera segura, transparente y conforme a las normativas legales, protegiendo la confidencialidad, integridad y disponibilidad de la información. Para ello, se establecen procedimientos claros que guían la recolección, tratamiento, almacenamiento y eliminación de los datos, al mismo tiempo que se garantiza el respeto a la privacidad de los individuos y organizaciones involucradas.

Los principales objetivos de esta política incluyen:

1. **Proteger la privacidad** de los datos recopilados durante la operación del proyecto.
2. **Establecer procedimientos claros** para el manejo seguro de los datos.
3. **Cumplir con las normativas** nacionales e internacionales sobre la protección de datos.
4. **Garantizar la transparencia** y el consentimiento informado de las partes involucradas en el uso de los datos.

Alcance

Esta política aplica a todos los datos que se recopilan, almacenan, procesan o transmiten en el marco de los proyectos de machine learning relacionados con la ganadería. Afecta tanto al personal interno como a cualquier tercero que participe en el tratamiento de la información, incluyendo proveedores y colaboradores externos.

Específicamente, esta política abarca:

1. **Datos personales y no personales** relacionados con las operaciones ganaderas.
2. **Datos sensibles** cuya protección es crítica debido a su naturaleza confidencial.
3. **Consentimiento de los usuarios** y transparencia en el tratamiento de la información.

4. **Cumplimiento normativo** de leyes de protección de datos, como el Reglamento General de Protección de Datos (GDPR) o las leyes locales correspondientes.

El alcance de esta política incluye todas las etapas del ciclo de vida de los datos: desde su recolección inicial, almacenamiento, procesamiento, hasta su eliminación final.

Términos y Definiciones

Para garantizar una interpretación clara y coherente de esta política, se definen los siguientes términos clave:

1. **Datos personales:** Cualquier información que permita identificar directa o indirectamente a una persona física, como nombre, número de identificación, datos de ubicación, entre otros.
2. **Datos sensibles:** Información que, por su naturaleza, requiere un nivel de protección mayor, como datos financieros, información de salud, datos de bienestar animal, o datos que puedan afectar la seguridad de las operaciones.
3. **Tratamiento de datos:** Cualquier operación realizada sobre datos personales o no personales, tales como recolección, almacenamiento, modificación, consulta, uso, transmisión, o destrucción de la información.
4. **Responsable del tratamiento:** La persona física o jurídica, autoridad pública, u organismo que determina los fines y medios del tratamiento de los datos.
5. **Encargado del tratamiento:** La persona física o jurídica que trata los datos personales en nombre del responsable del tratamiento.
6. **Consentimiento informado:** Permiso explícito otorgado por el cliente o usuario final para la recolección y procesamiento de sus datos, después de haber sido informado de manera clara y comprensible sobre el uso que se dará a los mismos.
7. **Cifrado:** Proceso de codificación de datos para protegerlos del acceso no autorizado, garantizando la confidencialidad de la información.
8. **Normativas de protección de datos:** Conjunto de leyes, regulaciones y directrices que rigen la protección de la privacidad y seguridad de los datos, tales como el GDPR u otras normativas locales.

Datos

Recopilación de datos

La recopilación de datos es un proceso crítico para el desarrollo y funcionamiento de nuestro proyecto. Nos comprometemos a recolectar únicamente la información necesaria para cumplir con los fines legítimos establecidos en esta política.

1. Tipos de datos recopilados:

Recopilamos datos tanto personales como no personales, que incluyen información sobre las operaciones ganaderas, así como datos de rendimiento y productividad. Esto puede incluir:

- Datos de identificación (como nombres o identificadores únicos).
- Datos operacionales (relacionados con el rendimiento de los animales, alimentación, etc.).
- Información técnica (como la ubicación GPS o el uso de maquinaria).

2. Fuentes de datos:

Los datos serán obtenidos directamente del cliente, cámaras web, registros internos, bases de datos y fuentes legítimamente autorizadas. Principalmente, estamos obteniendo los datos a través de imágenes capturadas por una cámara web en el área de camas de un corral del CAETEC, enviadas a una raspberry pi y almacenadas en la nube.

3. Finalidad de la recopilación:

Los datos serán recolectados y procesados exclusivamente para los fines que se hayan comunicado claramente al cliente.

4. Mínima recolección:

Nos comprometemos a recopilar solo los datos que sean estrictamente necesarios para cumplir con los objetivos definidos. Cualquier dato que no sea esencial será excluido del proceso.

5. Transparencia en la recopilación:

Se informará claramente al cliente sobre qué datos serán recolectados y con qué fines. El proceso de recopilación será transparente, y los usuarios podrán decidir qué datos comparten de acuerdo con sus preferencias y necesidades.

Datos sensibles

Los datos sensibles, por su naturaleza, requieren un mayor nivel de protección. En nuestra operación, estamos comprometidos a manejar estos datos de manera que se respete la privacidad y la seguridad de todas las partes involucradas.

1. Definición de datos sensibles:

Consideramos como datos sensibles aquellos que pueden revelar

información personal altamente confidencial o que, en caso de ser comprometidos, podrían tener un impacto significativo en la privacidad de las personas o la operación de los clientes. Esto incluye:

- Datos de salud o bienestar animal.
- Datos de ubicación precisa que revelen detalles críticos sobre la infraestructura o las operaciones.
- Dato ajeno a la identificación de la vaca en las camas (como la identificación de personas que puedan salir en las fotos).
- Cualquier otro dato que pueda implicar un riesgo elevado en caso de exposición o mal manejo.

2. **Consentimiento explícito:**

Antes de recolectar datos sensibles, se solicitará un consentimiento explícito y separado por parte del cliente. Los clientes serán informados claramente sobre qué datos sensibles se recolectarán y cómo se utilizarán.

3. **Retención limitada:**

Los datos sensibles se conservarán solo durante el tiempo necesario para cumplir con los fines específicos por los que fueron recopilados. Una vez que estos datos ya no sean necesarios, serán eliminados de manera segura y permanente.

Consentimiento y Transparencia

Consentimiento

El consentimiento es fundamental y debe ser otorgado de manera **informada, explícita y voluntaria**.

1. **Consentimiento informado:**

Se proporciona a los usuarios información clara sobre los datos recibidos y cómo se utilizarán. Los usuarios entenderán plenamente el uso que se hará de sus datos, incluyendo si estos se compartirán con terceros o se usarán para fines adicionales como análisis de machine learning.

2. **Consentimiento explícito:**

El consentimiento será otorgado mediante una acción afirmativa clara.

3. **Retiro del consentimiento:**

Los usuarios tendrán el derecho de retirar su consentimiento en cualquier momento, si los datos proporcionados fueron usados de una manera no ética. Para ello, el cliente deberá presentar la justificación del retiro de su consentimiento para una primera evaluación de la situación con los profesores de reto: Dr. Benjamín Valdés y el Mtro. Eduardo Juárez.

Posteriormente, si se identifica una falta ética con el uso de los datos proporcionados (llámese falta ética a la venta de la información dada, distribución de la información en canales no autorizados, uso de esta para fines personales o la alteración de la información para fines engañosos), se deberá presentar la situación con el comité de ética del ITESM campus Querétaro para que se siga el proceso indicado por ellos. Si de lo contrario, los profesores deliberan que no se realizó una falta ética por parte del equipo, el equipo continuará con sus actividades sin represalias y sin resentimientos.

Transparencia

La transparencia es clave para que los usuarios comprendan cómo se utilizan sus datos y puedan ejercer control sobre ellos. Nos comprometemos a ofrecer información clara y accesible sobre nuestras prácticas de manejo de datos.

1. **Información clara y comprensible:**

Toda la información proporcionada a los usuarios estará redactada de manera sencilla, evitando el uso de tecnicismos.

2. **Finalidad del procesamiento:**

Los datos se almacenarán y procesarán únicamente para los fines específicos y legítimos informados a los usuarios. No se utilizarán los datos para otros propósitos sin el consentimiento explícito del usuario.

Protección de Privacidad

Las políticas que se pueden incluir en este proyecto son las siguientes:

1. **Política de Privacidad de Datos:** Describir cómo se recopilan, procesan y almacenan los datos proporcionados.
2. **Política de Control de Acceso:** Definir claramente los roles y permisos de acceso a los datos, así como los procedimientos para otorgar, modificar y revocar accesos.
3. **Política de Retención de Datos:** Especificar el tiempo que se conservarán los datos y las condiciones bajo las cuales se destruirán de manera segura.

Acceso a Datos

El equipo se compromete a garantizar que el acceso a los datos sea gestionado de manera estricta y conforme a los principios de **control y restricción**. Estas medidas aseguran que solo el personal autorizado pueda acceder a la información, de acuerdo con sus responsabilidades y necesidades operativas.

Acceso Controlado

El acceso a los datos será gestionado bajo un esquema de control riguroso, garantizando que solo los individuos que necesitan los datos para llevar a cabo su trabajo tengan acceso a ellos. Para asegurar este control:

1. Roles y permisos:

Todos los accesos estarán vinculados dentro del equipo, quienes tienen permiso de lectura y escritura. Se asignan niveles de acceso únicamente de lectura a profesores, compañeros de otros equipos de la misma materia académica y a los clientes. Usuarios extras a los mencionados anteriormente no tendrán acceso a ninguno de estos datos, por lo que no tendrán permisos de escritura y/o lectura.

2. Registro de accesos:

Se mantendrán registros detallados de quién ha accedido a los datos y cuándo lo ha hecho. Estos registros permitirán realizar auditorías periódicas en un futuro para garantizar el cumplimiento de las políticas de acceso y detectar cualquier uso indebido.

Almacenamiento y Seguridad

El proyecto, al estar delimitado y teniendo como propósito el que se use de manera local (es decir, una aplicación de escritorio), no mantendrá bases de datos en servidores de la nube, cuyos servicios se tengan que financiar. Por ello, se recomiendan prácticas avanzadas y un poco más robustas cuando se haga el uso de este proyecto en situaciones que requieran de resistencia a fallos, escalabilidad y alta disponibilidad:

1. Seguridad del almacenamiento:

Que los datos sean almacenados de manera segura en servidores o fuentes de almacenamiento que cumplan con estándares avanzados de seguridad. Esto incluye la utilización de tecnologías de encriptación tanto para los datos en tránsito como para los datos en reposo, a fin de proteger la información frente a accesos no autorizados.

2. Medidas de cifrado:

Que los datos sensibles estén cifrados mediante algoritmos robustos para garantizar que la información no pueda ser interpretada por personas no autorizadas, incluso si se accediera indebidamente a los sistemas de almacenamiento.

3. Copias de seguridad (backups):

Se deben realizar copias de seguridad periódicas de los datos con el fin de proteger la información frente a pérdidas accidentales o daños. Estas copias

de seguridad estarán almacenadas en ubicaciones seguras y también estarán cifradas para proteger la confidencialidad de los datos.

4. **Gestión de acceso físico:**

El acceso a las instalaciones donde se almacena la infraestructura de datos debe estar controlado de manera estricta. Solo el personal autorizado podrá acceder a los servidores físicos, y se deben aplicar medidas de seguridad adicionales, como cámaras de vigilancia, cerraduras electrónicas y registros de acceso.

5. **Protección contra ciberataques:**

Se deben considerar soluciones avanzadas de seguridad, tales como firewalls, sistemas de detección de intrusiones (IDS) y software antivirus actualizado regularmente para proteger los sistemas frente a ciberataques, malware y otras amenazas.

6. **Actualización de seguridad:**

Todos los sistemas y aplicaciones utilizadas para almacenar y procesar datos se deben mantener actualizados con los últimos parches de seguridad. Se tienen que llevar a cabo revisiones periódicas para identificar vulnerabilidades y aplicar las correcciones necesarias de manera oportuna.

7. **Manejo de incidentes de seguridad:**

En el caso de que ocurra un incidente de seguridad que ponga en riesgo la integridad, confidencialidad o disponibilidad de los datos, se necesita contar con un plan de respuesta adecuado. Este plan debe incluir la identificación rápida del incidente, la mitigación del impacto y la notificación inmediata a las partes afectadas si es necesario, cumpliendo con las normativas aplicables.

8. **Almacenamiento limitado:**

Los datos no se deben almacenar más allá del tiempo necesario para cumplir con los fines establecidos en esta política. Una vez que los datos ya no sean necesarios, se deben eliminar de manera segura y permanente.

Normativas

Entre las normativas que tienen relación con el proyecto o el giro económico de nuestro cliente, se encuentran:

1. **Normativa GDPR (Reglamento General de Protección de Datos de la UE):** Si el proyecto involucra ciudadanos de la UE, debe seguir las regulaciones sobre el consentimiento, el derecho al olvido, la portabilidad de datos, entre otros.

2. **CCPA (California Consumer Privacy Act):** Si los datos incluyen ciudadanos de California, seguir las normas sobre transparencia, control del usuario sobre sus datos, y el derecho a solicitar la eliminación de datos.
3. **ISO/IEC 27001 (Seguridad de la Información):** Normativa internacional para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).
4. **HIPAA (Health Insurance Portability and Accountability Act):** Si los datos incluyen información de salud, cumplir con los requisitos de protección de datos sensibles relacionados con la salud.
5. **Ley Federal de Protección de Datos Personales (México):** Si el proyecto involucra datos de personas mexicanas, asegurarse de cumplir con esta ley, que regula la recopilación, uso, y tratamiento de datos personales.
6. **Política de Transferencia de Datos:** Definir claramente las condiciones bajo las cuales los datos pueden ser transferidos a terceros o a otras jurisdicciones, y cómo se asegura la protección de los datos durante la transferencia.
7. **Política de Anonimización y Pseudonimización:** Describir los procesos utilizados para anonimizar o pseudonimizar datos sensibles, garantizando así que los datos personales no puedan ser vinculados a individuos específicos sin información adicional.
8. **Normativa PCI-DSS (Payment Card Industry Data Security Standard):** Si el proyecto implica el procesamiento de pagos, seguir esta normativa que establece estándares de seguridad para proteger los datos de tarjetas de crédito.

Prevención

1. **Evaluaciones de riesgos:**
Se realiza una evaluación de riesgos y pruebas a la aplicación para auditar, identificando riesgos potenciales y solucionándolos. Eventualmente, se recomienda realizar auditorías y evaluaciones periódicas de seguridad para identificar vulnerabilidades y prevenir incidentes antes de que ocurran. **Nota:** Dependiendo del alcance del proyecto y de quién lo esté utilizando, es la frecuencia en que se recomiendan estas pruebas, pues cada empresa o proyecto tiene necesidades y especificaciones distintas.

Acuerdos

El equipo garantiza que cualquier tratamiento de datos personales estará sujeto a **acuerdos** adecuados con todas las partes involucradas, asegurando el cumplimiento de las normativas de protección de datos.

1. Acuerdos con terceros:

Cualquier acceso o tratamiento de datos por parte de terceros, como proveedores de servicios o socios comerciales, estará regulado mediante acuerdos que incluyan cláusulas de confidencialidad y de protección de datos. Estos acuerdos definirán las obligaciones de los terceros respecto al manejo seguro y responsable de los datos, así como las sanciones en caso de incumplimiento.

2. Acuerdos de confidencialidad (NDA):

El personal interno y cualquier colaborador que tenga acceso a datos confidenciales o personales deberá firmar un acuerdo de confidencialidad (NDA). Estos acuerdos garantizan que la información no se compartirá ni utilizará para fines no autorizados.

Al firmar el documento, las siguientes personas confirman estar enterados de los puntos detallados en el documento y estar de acuerdo en el cumplimiento de estos mismos.

Gamaliel Marines Olvera



Uri Jared Gopar Morales



José Antonio Miranda Baños



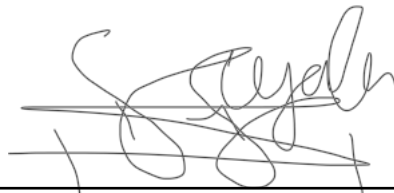
María Fernanda Moreno Gómez



Oskar Adolfo Villa López



Luis Ángel Cruz García



Ivo Neftalí Ayala García