Tecnológico de Monterrey

Reto Privacidad y Seguridad de los Datos

TC3007C.501

Inteligencia artificial avanzada para la ciencia de datos 2

Gpo 501

Docentes

Dr. Benjamín Valdés Aguirre

Ma. Eduardo Daniel Juárez Pineda

Dr. Ismael Solis Moreno

Dr. José Antonio Cantoral Ceballos

Dr. Carlos Alberto Dorantes Dosamantes

Integrante

Dafne Fernández Hernández

Introducción

Este reporte describe las políticas y regulaciones necesarias para el manejo seguro y ético de los datos en el proyecto de monitoreo de ganado bovino en CAETEC. La protección de datos personales es prioritaria, especialmente en proyectos que pueden capturar información sensible incidental. Este análisis examina las normativas vigentes, tanto en México como en la Unión Europea, y establece un marco para asegurar que el proyecto cumpla con los estándares de privacidad y seguridad.

1. Análisis de Normativas de Protección de Datos

LFPDPPP (México)

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) establece las bases para el manejo de datos personales en México. Para el proyecto, los aspectos relevantes son:

- **Artículo 8 (Consentimiento):** El consentimiento para el uso de datos personales debe ser expreso y puede revocarse en cualquier momento. En el contexto del proyecto, este consentimiento es esencial en caso de que los colaboradores del CAETEC aparezcan incidentalmente en las imágenes. Se deben establecer mecanismos que permitan a los colaboradores revocar su consentimiento fácilmente.

- **Artículo 19 (Medidas de seguridad):** Es necesario implementar medidas de seguridad para proteger los datos contra el acceso o uso no autorizado. Esto incluye políticas de cifrado, control de acceso y autenticación de dos factores. Estas medidas asegurarán que solo personal autorizado pueda acceder a los datos capturados en el proyecto.

- **Artículo 25 (Derecho de cancelación):** Los colaboradores deben tener derecho a cancelar su consentimiento y solicitar la eliminación de sus datos. Cualquier dato personal incidental (por ejemplo, imágenes de colaboradores) debe poder ser eliminado cuando ya no sea necesario para los fines del proyecto.

GDPR (Unión Europea)

El Reglamento General de Protección de Datos (GDPR) es una normativa de alto estándar en la protección de datos. Aunque es europeo, sus principios pueden guiar prácticas seguras en el proyecto.

- **Artículos 6-11 (Base legal para el procesamiento):** El GDPR establece que todo procesamiento de datos debe justificarse bajo una base legal específica. En este proyecto, si se utiliza el consentimiento, es crucial que los colaboradores tengan la opción de revocarlo en cualquier momento. Si se elige el interés legítimo como base, debe documentarse una evaluación de impacto en la privacidad.

- **Artículos 12-14 (Transparencia y comunicación):** Es esencial desarrollar una política de privacidad que explique detalladamente el propósito del procesamiento de datos, los métodos empleados y las medidas de seguridad implementadas. Esta política debe ser clara y estar disponible en el área de trabajo de CAETEC, especialmente para los colaboradores que podrían aparecer en las imágenes de forma incidental.

- **Artículo 25 (Protección de datos por diseño):** Este principio requiere minimizar la recolección de datos personales y aplicar medidas de protección desde la fase de diseño del proyecto. El equipo debe asegurar que las imágenes capturadas estén estrictamente orientadas al ganado y no incluyan personas a menos que sea accidental e inevitable.

2. Normativas y Políticas en Sistemas de Inteligencia Artificial

Regulación Europea de Inteligencia Artificial (AI Act)

El AI Act europeo clasifica los sistemas de IA en diferentes niveles de riesgo. Este proyecto se clasifica como de “riesgo limitado,” lo que implica:

- Transparencia y documentación: Informar a los usuarios sobre la interacción con el sistema de IA y documentar las capacidades y limitaciones del sistema. En el caso del CAETEC, esto significa que todos los colaboradores deben estar informados sobre el uso de visión artificial en su entorno de trabajo.
- Supervisión humana: Es fundamental que el sistema de IA sea monitoreado por personal capacitado, que pueda intervenir y ajustar el sistema si detecta problemas éticos o de privacidad.

Marco NIST para IA

El marco NIST para la gestión de riesgos en IA es una guía de mejores prácticas técnicas para asegurar la robustez y fiabilidad del sistema. En este proyecto:

- Evaluación de riesgos: El equipo debe realizar evaluaciones periódicas para identificar y mitigar riesgos potenciales en el uso de IA.
- Gestión del ciclo de vida: Este enfoque permite revisar y adaptar el sistema de IA a lo largo de su desarrollo, asegurando que se mantengan prácticas seguras y éticas en cada fase.

3. Proceso de Manejo y Acceso a los Datos

Control de Acceso y Almacenamiento Seguro

Para el acceso a los datos:

- Autorización: Solo el personal que haya firmado los acuerdos de confidencialidad (NDA) y procesamiento de datos (DPA) puede acceder a los datos. Esto garantiza que el manejo de la información esté limitado a personal autorizado que comprende y respeta las políticas de uso.
- Almacenamiento en redes seguras: Los datos deben almacenarse en redes privadas o VPNs seguras con autenticación de dos factores. Se recomienda también el cifrado de los datos para protegerlos en caso de intentos de acceso no autorizado.

Documentación y Registro de Accesos

Un registro de acceso detallado debe ser implementado para mantener un rastro de auditoría. Este registro debe incluir:

- Fecha y hora de cada acceso.
- Nombre y rol de la persona que accede a los datos.
- Propósito del acceso.

Estos registros deben actualizarse regularmente y estar disponibles para auditorías internas, permitiendo un control estricto sobre el uso de datos en el proyecto.

4. Recomendaciones Prácticas para Cumplimiento y Evidencia

Anonimización de Imágenes

Se deben aplicar técnicas de anonimización (por ejemplo, difuminado o enmascaramiento de rostros) en imágenes que capturen personas de manera incidental. La eliminación o anonimización de estas imágenes debe llevarse a cabo cuando ya no sean necesarias, en alineación con la LFPDPPP y GDPR.

Capacitación en Seguridad y Privacidad

Todo el personal que tenga acceso a los datos debe recibir capacitación específica en políticas de privacidad y uso ético de IA. Esta capacitación debe incluir temas como:

- Uso seguro de contraseñas y autenticación de dos factores.
- Políticas de privacidad y gestión ética de datos.
- Procedimientos de manejo seguro del correo y comunicación sobre el proyecto.

Esta capacitación asegura que todos los involucrados en el proyecto comprendan y respeten las normativas y protecciones aplicables.

Administración y documentación de datos:

Este documento proporciona un registro detallado del uso y tratamiento de los datos de acuerdo con el procedimiento previamente establecido.

Gestion y Registro de Datos

Acuerdo de Políticas de Datos, Ética y Seguridad

Este documento establece las políticas de datos, ética y seguridad para el manejo del proyecto, el cual es esencial la firma de todos los involucrados como compromiso con el cumplimiento de las normativas.

Políticas de Datos, Ética y Seguridad

1. **Retención de datos limitada y eliminación segura**
   Las imágenes recolectadas serán almacenadas únicamente durante el tiempo estrictamente necesario para cumplir con los objetivos del proyecto. Una vez

cumplido el propósito, se procederá a su eliminación segura mediante métodos aprobados (como borrado criptográfico) o se anonimizarán para proteger los datos personales y garantizar su uso ético en análisis futuros.

2. **Control de acceso restringido**

   Solo tendrán acceso a los datos las personas autorizadas que hayan firmado los acuerdos de confidencialidad correspondientes. Esto incluye el uso de credenciales únicas, restricciones de acceso físico a los servidores, y la implementación de sistemas de monitoreo para detectar accesos no autorizados.

3. **Autenticación robusta y contraseñas seguras**

   Todo el equipo deberá usar autenticación de dos factores para acceder a los datos y sistemas relacionados. Las contraseñas deberán cambiarse periódicamente para una mayor seguridad.

4. **Capacitación continua en seguridad de datos**

   Todo el personal deberá participar en capacitaciones regulares sobre temas de privacidad y seguridad, tales como la gestión de incidentes, protección frente a phishing, y mejores prácticas para el manejo de datos sensibles.

5. **Verificación de cumplimiento normativo**

   Se deberán realizar auditorías periódicas para asegurar que las prácticas del proyecto cumplen con las normativas LFPDPPP (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) y GDPR (Reglamento General de Protección de Datos). Esto incluye realizar revisiones de los contratos con terceros y las medidas de protección implementadas.

6. **Gestión ética de datos personales**

   Todos los datos recopilados deberán ser tratados de acuerdo con principios éticos. En caso de que las imágenes capturen a personas de forma incidental, su identidad deberá ser protegida mediante técnicas de anonimización o difuminado. Se prohíbe el uso de los datos para cualquier fin que no esté explícitamente aprobado en el proyecto.

7. **Prohibición de compartir datos sin autorización**

   Está estrictamente prohibido compartir datos o imágenes fuera del equipo autorizado del proyecto sin previa autorización de los docentes y del socio formador.. Esto incluye tanto datos crudos como procesados.

8. **Registro de uso y manejo de datos**

   Se deberá mantener un registro detallado de todos los accesos, descargas y usos de los datos. Este registro incluirá la fecha, hora, propósito, y la identificación de la persona que accedió a los datos.

9. **Protección contra incidentes de seguridad**
   Todo el equipo está obligado a reportar inmediatamente cualquier incidente de seguridad, como accesos no autorizados, pérdida de datos, o posibles vulnerabilidades. Se implementarán medidas para mitigar riesgos futuros, como parches de seguridad y revisiones de los protocolos.
10. **Acuerdos de confidencialidad con terceros**
    Los proveedores o colaboradores externos deberán firmar un DPA (Acuerdo de Procesamiento de Datos) que estipule las medidas de seguridad requeridas y las consecuencias legales por incumplimiento.
11. **Revisión continua y mejora de políticas**
    Las políticas de seguridad serán revisadas y actualizadas regularmente para adaptarse a cambios tecnológicos, normativos, o de contexto en el proyecto. Se espera la participación activa del equipo para proponer mejoras.
12. **Transparencia y comunicación clara**
    Toda la información relacionada con el tratamiento de datos deberá ser comunicada de manera clara y accesible a todas las partes involucradas. Esto incluye las finalidades del tratamiento, las medidas de seguridad implementadas, y los derechos de los titulares de los datos.

Responsabilidad y cumplimiento

13. **Acuerdo de cumplimiento y NDA**

    Todo miembro del equipo y los representantes del socio empresarial deberán firmar un acuerdo en el que se comprometan a cumplir con estas políticas de manejo de datos. Este acuerdo incluirá un acuerdo de confidencialidad (NDA) que especificará las obligaciones de cada parte y la prohibición de divulgar datos o imágenes fuera del proyecto.

14. **Compromiso con el cumplimiento**

    A través de la firma del acuerdo, todos los involucrados en el proyecto reafirman su compromiso de tratar los datos con la máxima responsabilidad, en alineación con las normativas aplicables y los principios éticos detallados en estas políticas.

Incumplimiento de la Norma

En caso de que alguna de las políticas descritas en este documento no sea cumplida por los involucrados, se procederá conforme a los siguientes puntos:

1. **Responsabilidad académica**

   Se evaluarán las implicaciones académicas del incumplimiento, y se tomarán las acciones necesarias conforme a las normativas vigentes. Esto incluye la notificación a las autoridades correspondientes y, en caso de ser necesario, la aplicación de sanción con el respectivo comité educativo donde se reportará como FIA (Falta de Integridad Académica) al estudiante que no cumpla con las normas establecidas.

2. **Acciones correctivas inmediatas**

   Se implementarán medidas correctivas para mitigar los efectos del incumplimiento. Esto incluye, pero no se limita a:

   - La suspensión temporal o permanente del acceso a los datos.
   - La rectificación inmediata de las vulneraciones a la seguridad o privacidad.
   - La reparación de daños ocasionados, si aplica.

3. **Revisión de procedimientos**

   El equipo de trabajo llevará a cabo una revisión exhaustiva de los procedimientos para identificar posibles fallos en la implementación de las políticas y proponer mejoras que prevengan futuros incumplimientos.

4. **Compromiso renovado**

   El involucrado deberá firmar un compromiso adicional que garantice la alineación de su conducta con las políticas descritas. En casos graves, se evaluará la continuidad de su participación en el proyecto.

5. **Notificación a partes interesadas**

   Se informará a los responsables del proyecto y, de ser necesario, a los socios o terceros afectados sobre el incumplimiento, detallando las acciones tomadas para solventarlo.

Nosotros, como equipo de desarrollo, nos comprometemos a cumplir con las políticas descritas:

- **Nombre y firma: _____ Fecha: _____**

- **Nombre y firma: _____ Fecha: _____**

- **Nombre y firma: _____ Fecha: _____**

- **Nombre y firma: _____ Fecha: _____**

- **Nombre y firma: _____ Fecha: _____**

Yo, como socio formador del proyecto, confirmo estar de acuerdo con las políticas descritas:

- **Nombre y firma: _____ Fecha: _____**

Referencias:

Reglamento general de protección de datos (RGPD) - GDPR-Text.com. (2019, October 28). GDPR-Text.com - GDPR Text, Translation and Commentary. https://gdpr-text.com/es/

Reglamento general de protección de datos (RGPD) - GDPR-Text.com. (2019, October 28). GDPR-Text.com - GDPR Text, Translation and Commentary. https://gdpr-text.com/es/

Reglamento general de protección de datos (RGPD) - GDPR-Text.com. (2019, October 28). GDPR-Text.com - GDPR Text, Translation and Commentary. https://gdpr-text.com/es/

Cámara De Diputados Del Congreso De La Unión. (2010). *LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES*. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf