Instituto Tecnológico y de Estudios Superiores de Monterrey

Inteligencia Artificial Avanzada para la Ciencia de Datos

Los concentrados v2

Política de Datos y Acceso

Daniel Queijeiro Albo - A01710441

Diego Alfaro Pinto - A01709971

Diego Isaac Fuentes Juvera - A01705506

Jesus Ramirez Delgado - A01274723

Mauricio Anguiano Juarez - A01703337

Luis Adrián Uribe Cruz - A01783129

Índice

Objetivo y alcance del proyecto

Objetivo

Esta política establece los lineamientos para la gestión, protección y uso de los datos generados y utilizados en el proyecto de inteligencia artificial para la ganadería de precisión en el CAETEC

Alcance

Esta política aplica a:

- Datos generados por el sistema DeLaval (robot de ordeño BMC3)
- Imágenes de vacas capturadas por cámaras en corredor de salida
- Datos derivados y modelos generados
- Todo el personal y estudiantes del proyecto

Clasificación de Datos

Datos Públicos

- Estadísticas agregadas del hato (sin identificación individual)
- Papers académicos y publicaciones
- Modelos open source desarrollados
- Código y metodologías (repositorio GitHub)

Restricciones: Ninguna, pueden compartirse libremente tras finalizar el proyecto

Datos Confidenciales

- Registros individuales por vaca (ID, producción, salud)
- Imágenes originales de las vacas
- Archivos CSV del robot DeLaval
- Métricas de calidad de leche
- Datos que puedan afectar relaciones comerciales

Restricciones: Acceso limitado a equipo del proyecto, profesores y personal autorizado de CAETEC

Principios Fundamentales

1. **Confidencialidad comercial**
   Los datos son propiedad de CAETEC. No se compartirán fuera del equipo autorizado sin consentimiento expreso.
2. **Transparencia y apertura académica**
   Se promoverá el desarrollo de modelos open source. Los resultados serán compartidos con la comunidad académica respetando la confidencialidad de datos sensibles.

3. **Calidad y confiabilidad**
   Los datos serán validados, limpiados y documentados antes de su uso. Se mantendrán registros de todas las transformaciones realizadas.
4. **Ética y bienestar animal**
   El uso de datos no comprometerá el bienestar del ganado bovino. Todas las decisiones basadas en datos priorizarán la salud y el bienestar animal.

Protección de datos

Acceso autorizado

Únicamente los integrantes del equipo listados arriba, profesores del curso y personal del CAETEC tienen acceso a estos datos.

Anonimización de datos

El dataset de vacas utilizado en este proyecto no requiere anonimización, ya que los identificadores contenidos (ID de vaca, métricas de salud y producción) no constituyen datos personales ni sensibles conforme a la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Estos registros corresponden a animales de producción y no permiten rastrear información vinculada a personas físicas o productos específicos.

Normativa actual de la industria

En la industria ganadera y de agricultura de precisión, la gestión de datos se rige principalmente por marcos de trazabilidad y confidencialidad técnica más que por normativas de privacidad personal, ya que los registros se refieren a animales y operaciones productivas, no a personas físicas. En México, el marco aplicable es el establecido por el SINIIGA/SENASICA, que regula la identificación y trazabilidad pecuaria, mientras que a nivel internacional destacan la norma ISO 22005 (trazabilidad en la cadena alimento-pienso) y las directrices del ICAR (Animal Data Exchange) para intercambio seguro de datos entre sistemas.

En conjunto, estos lineamientos aseguran la confidencialidad y seguridad de la información sin requerir procesos de anonimización, dado que los identificadores del hato (ID de vaca, métricas de salud o producción) no son datos personales y su tratamiento se rige por criterios de trazabilidad técnica y confidencialidad comercial.

Almacenamiento seguro

Usaremos servicios de Amazon Web Services (AWS) para guardar nuestros datos de forma segura:

Amazon S3:

- Los datos están encriptados automáticamente
- Solo nuestro equipo tiene acceso mediante credenciales únicas
- Configuramos permisos específicos para cada tipo de archivo

Control de acceso:

- Cada miembro del equipo tiene su propio usuario con permisos limitados

- Usamos autenticación de dos factores (2FA)
- Los accesos quedan registrados automáticamente
- Configuramos políticas que sólo permiten acceso desde redes específicas

Configuración de seguridad:
- Bucket privado
- Encriptación en reposo activada
- Versionado de archivos para recuperación
- Logs de acceso habilitados
- Políticas de IAM restrictivas.

Tiempo de conservación de los datos
Durante el semestre mantendremos todos los datos necesarios para completar el trabajo. Tras la finalización del semestre, eliminaremos los datos originales pero se conservará el modelo entrenado.

Bases legales
Esta política está fundamentada bajo la Ley Federal de Protección de Datos Personales en Posesión de Particulares de México, especialmente lo establecido en los artículos 9, 60 y 61:

- Artículo 9: Los responsables del tratamiento de datos deben cumplir con 9 principios rectores para la protección de los datos
    - Licitud
        - El responsable está obligado a hacer el tratamiento con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional
    - Consentimiento
        - El responsable deberá obtener el consentimiento para el tratamiento de los datos personales, a menos que no sea exigible
    - Información
        - El responsable deberá dar a conocer al titular la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales a través del aviso de privacidad
    - Calidad
        - Se cumple con el principio de calidad cuando los datos personales tratados sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados
    - Finalidad
        - Los datos personales sólo podrán ser tratados para el cumplimiento de la finalidad o finalidades establecidas en el aviso de privacidad
    - Lealtad
        - Establece la obligación de tratar los datos personales privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad,

    - Proporcionalidad
        - Sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido
    - Responsabilidad
        - El responsable deberá adoptar medidas para garantizar el debido tratamiento, privilegiando los intereses del titular y la expectativa razonable de privacidad
- Artículo 60: El responsable deberá determinar las medidas de seguridad aplicables a los datos que maneje de acuerdo a 4 factores
    - El riesgo inherente por tipo de dato personal
    - La sensibilidad de los datos personales tratados
    - El desarrollo tecnológico, y
    - Las posibles consecuencias de una vulneración para los titulares
    - Tomar en cuenta los siguientes aspectos
        - El número de titulares
        - Las vulnerabilidades previas ocurridas en los sistemas de tratamiento
        - El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión, y
        - Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al responsable
- Artículo 61: El responsable debe realizar 9 acciones para garantizar la seguridad de los datos
    - Elaborar un inventario de datos personales y de los sistemas de tratamiento
    - Determinar las funciones y obligaciones de las personas que traten datos personales
    - Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales
    - Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva
    - Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales
    - Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha
    - Llevar a cabo revisiones o auditorías
    - Capacitar al personal que efectúe el tratamiento
    - Realizar un registro de los medios de almacenamiento de datos personales

Incidentes y contingencias

Incidente	**Acción inmediata**

Pérdida de datos	Recuperar desde los respaldos versionados y documentar la causa de la pérdida de datos.
Divulgación accidental	Notificar al CAETEC inmediatamente, evaluar el impacto, aplicar las medidas correctivas correspondientes
Falla de infraestructura	Utilizar respaldos, documentar y evaluar la migración del sistema

DECLARACIÓN DE CONFORMIDAD

Los miembros del equipo declaran haber leído, entendido y aceptado cumplir con esta política de datos:

- Daniel Queijeiro Albo - A01710441
- Diego Alfaro Pinto - A01709971
- Diego Isaac Fuentes Juvera - A01705506
- Jesus Ramirez Delgado - A01274723
- Mauricio Anguiano Juarez - A01703337
- Luis Adrián Uribe Cruz - A01783129