Instituto Tecnológico y de Estudios Superiores de Monterrey
Inteligencia artificial avanzada para la ciencia de datos II

Reto: Privacidad y Seguridad de los Datos (Portafolio Análisis - Individual)

Profesores:

Ismael Solis Moreno

Benjamín Valdés Aguirre

José Antonio Cantorral Ceballos

Carlos Alberto Dorantes Dosamantes

Paul Park - A01709885

Equipo:
Los pochos hermanos

9 de noviembre de 2025

1. Contexto del proyecto

El proyecto tiene como objetivo desarrollar un modelo de visión artificial para identificar individualmente a las vacas del CAETEC a partir de imágenes capturadas por un robot.

Dado que estas imágenes pueden contener información visual sensible (como etiquetas de identificación o elementos reconocibles del entorno del CAETEC), es indispensable aplicar medidas de privacidad y seguridad de datos.

2. Anonimización de los datos

Con base en la política de acceso del equipo, las imágenes son anonimizadas antes de su uso. Este proceso incluye:

- Recorte o difuminado de etiquetas visibles en las vacas.
- Verificación manual para asegurar que no aparezcan nombres, códigos o personas.
- Asignación de identificadores internos (por ejemplo, *vaca_001*, *vaca_002*) que sustituyen los ID reales.

Gracias a este procedimiento, no es posible rastrear una vaca específica ni vincular las imágenes con información sensible del CAETEC.

3. Normas y estándares aplicados

El proyecto se desarrolló conforme a los siguientes lineamientos:

- **ISO/IEC 27001:** Sistema de gestión de seguridad de la información.
- **NOM-001-SAG/GAN-2015:** Sistema Nacional de Identificación Animal para Bovinos y Colmenas.
- **Política de acceso del equipo:** Documento interno alineado con los lineamientos institucionales y del socio formador.

4. Proceso de manejo y acceso a los datos

Los datos del proyecto se almacenan en **Google Drive**, con control de identidad y permisos restringidos.
Solo los miembros autorizados del equipo pueden acceder mediante sus cuentas institucionales.

Cada integrante debe:

- No compartir credenciales.
- Eliminar copias locales temporales tras su uso.
- Registrar sus acciones en la bitácora de cambios del equipo.

Flujo de manejo de datos:

1. El socio formador entrega las imágenes.
2. Se revisan y anonimizan antes de su uso.
3. Se almacenan en la carpeta compartida del proyecto.
4. Cada modificación o descarga se registra en la bitácora.

5. Registros y bitácora

El equipo mantiene trazabilidad de todas las acciones sobre los datos mediante dos mecanismos:

- **Automático:** historial de Google Drive.
- **Manual:** hoja de bitácora compartida (documento de control de cambios).

En mi caso personal, participé en la revisión de imágenes y en el registro de las acciones correspondientes bajo mi cuenta institucional.

6. Conclusiones personales

Durante la implementación confirmé que la anonimización visual y el control de acceso son esenciales para mantener la confidencialidad de los datos del CAETEC.
Asimismo, la trazabilidad mediante bitácoras garantiza que cualquier acción sobre los datos pueda ser auditada.

El proceso descrito cumple con las normas aplicables y representa una práctica responsable de manejo de datos en entornos académicos y productivos.

Referencias

- Siew, Bhola Randy (2024). *Strengthening Big Data Security and Privacy in Libraries: A Review of ISO Standards and Real-World Cyberattack Case Studies.* Journal of Information Studies & Technology.
- NOM-001-SAG/GAN-2015 – *Sistema Nacional de Identificación Animal para Bovinos y Colmenas*. https://www.gob.mx/cms/uploads/attachment/file/771729/NOM_001_SAG_GAN_2015.pdf
- *Política de Acceso del Proyecto CAETEC* (documento compartido del equipo). https://www.notion.so/Pol-tica-de-acceso-287a3ea0df618097b208f5f04539b31c?source=copy_link