Tecnológico de Monterrey

Campus Querétaro

Privacidad y Seguridad de los Datos

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

El presente documento plantea definiciones, prácticas, procesos e investigaciones acerca de las prácticas de seguridad y privacidad de datos implementadas en nuestro proyecto, así como prácticas o normativas que se han planteado los países para manejar proyectos como este.

Datos anonimizados

Para garantizar que nuestros datos estuvieran libres de información personal o sensible para nuestro socio formador, en nuestro proceso de clasificación de las imágenes (vaca acostada, vaca parada o no hay vaca), nos permitió tener una visión completa del conjunto de imágenes y asegurarnos de que no contenían ningún dato que pudiera comprometer la privacidad o seguridad de nuestro socio u organización asociada. Cuando se identificaba alguna imagen que podría poner en riesgo la anonimidad de la persona o empresa, esta era eliminada.

Normativas

Como parte de la descripción de las normativas y el tratamiento de los datos sensibles en nuestro proyecto, realizamos una Política de Datos y Regulaciones de Privacidad, todo esto basados en prácticas que han hecho otros proyectos o empresas con un giro similar a nuestro enfoque.

En dicho documento, se presenta el alcance de nuestra política de protección de datos, términos, tratamiento de los datos, definición de datos sensibles, transparencia, acceso basado en roles, almacenamiento, seguridad y normativas (tanto en México como extranjeras). Las normativas fueron recopiladas a través de investigaciones individuales de los miembros del equipo y se escogieron las que se tomaron relevantes y con un enfoque similar al de nuestro proyecto.

Proceso para trabajar con el dataset

Propósito

Establecer cómo asegurar la seguridad y protección de los datos al manipular el dataset dado por el socio formador.

Notas introductorias

Entendemos la importancia de la protección de los datos de nuestro socio formador. Asegurarnos que los datos sean correctamente manipulados nos permite garantizar al socio formador que sus datos no serán vistos o utilizados para otros fines que no sean los especificados y que no sean manipulados por terceros.

Involucrados

- Equipo de desarrollo (Equipo “TC”)
- Equipo compañero “No Name”

Entradas

- Dataset de imágenes proporcionado por el socio formador y previamente clasificado por ambos equipos de camas. Link
- Bitácora de Buenas Prácticas. Link
- Política de Datos y Regulaciones de Privacidad

Salidas

- Bitácora de Buenas Prácticas actualizada

Descripción

Fase	Actividades	Responsable(s)
Preparación Inicial del Dataset	Verificar la clasificación del dataset (Sensibles / No sensibles) según las categorías definidas en la política.	Equipo TC Equipo No Name
Preparación Inicial del Dataset	Documentar la fecha y hora del primer acceso al dataset en la sección “Clasificación de Datos” en la Bitácora de Buenas Prácticas	Equipo TC
Registro de Acceso y Manipulación	Cada vez que se accede o se manipula el dataset, registrar la actividad en la Bitácora de Buenas Prácticas.	Equipo TC
Registro de Acceso y Manipulación	Registrar la práctica realizada (por ejemplo, acceso, modificación, eliminación) y la fecha correspondiente (Asegurar que cualquier modificación al dataset (como cambios en la clasificación o eliminación de datos) se registre en la sección correspondiente de la bitácora).	Equipo TC
Documentación de Prácticas de Seguridad	Cada actividad realizada con el dataset debe revisarse para verificar que se cumplen todas las medidas de seguridad propuestas por el equipo en la Política de Datos y Regulaciones de Privacidad.	Equipo TC
Monitoreo de	Si aplica, documentar el “Monitoreo de Actividad” de	Equipo TC

Actividades	la Bitácora de buenas prácticas, registrando el nombre de la persona que realizó la actividad, la fecha y la actividad que se realizó de monitoreo.	
Registro de Incidentes y Respuestas	En caso de un incidente de seguridad, documentarlo en la "Bitácora de Incidentes". Describir el impacto, quién lo detectó, quién lo resolvió y las fechas de detección y solución.	Equipo TC
Revisión y auditoría.	Cada dos semanas, se debe revisar cada bitácora de cada práctica de la Bitácora de Buenas Prácticas para garantizar que todas las prácticas se están cumpliendo y que los registros están actualizados.	Equipo TC

Debemos recordar que…

- **Almacenamiento**. El almacenamiento se realiza en Google Drive después de recibir las imágenes. La carpeta de Google Drive es compartida, con acceso solo para los miembros del equipo. Esto se decidió por la seguridad de la infraestructura de Google.
- **Redes.** Se puede acceder a la carpeta desde cualquier red. No manejamos datos sensibles, por lo que no es indispensable controlar las redes desde las que se accede a la carpeta.
- **Acceso.** Solo los miembros del equipo, profesores y miembros de otros equipos pueden ver las imágenes. La carpeta del equipo no se puede compartir con ninguna persona ajena al equipo.
- **Documentos.** Debido a la naturaleza de los datos y el acuerdo realizado con el socio formador, no es necesario firmar un NDA nosotros con el socio formador, sin embargo, se deberá firmar la Política de Datos y Regulaciones de Privacidad por ambas partes, es decir, nosotros como equipo desarrollador (TC) y nuestro socio, el Mtro. Ivo Ayala.

Bitácora de buenas prácticas

Con el fin de tener trazabilidad y transparencia con la manipulación de datos en el proyecto, se implementó una Bitácora de Buenas Prácticas donde se ingrese cada que se audite alguna de las prácticas, así como los registros de cada una de las personas que hayan trabajado en cada una de ellas, con el fin de tener registro de cuándo y quiénes trabajaron en cada una de ellas para aclaraciones que se pudieran tener en un futuro.