Instituto Tecnológico y de Estudios Superiores de Monterrey

Inteligencia Artificial Avanzada para la Ciencia de Datos II (Gpo 501)

Momento de Retroalimentación:
Reto Privacidad y Seguridad de los Datos

Jorge Eduardo De León Reyna - A00829759

Octubre 27, 2023

Datos utilizados

Los datos que se están almacenando en este proyecto están relacionados con la información de las asistencias y participaciones de los alumnos en los diferentes cursos. Con esto en cuenta, se identificaron los siguientes datos en base a la naturaleza del proyecto:

1. Datos biométricos de reconocimiento facial:

a) Imágenes faciales de estudiantes.
b) Características biométricas como rasgos faciales y puntos clave.

2. Datos de identificación personal:

a) Nombres de estudiantes.
b) Números de identificación, como códigos de estudiante o números de identificación personal.

3. Datos de asistencia:

a) Fechas y horarios de las clases.
b) Registro de la presencia o ausencia de estudiantes en cada clase.

4. Datos de participación:

a) Información sobre la postura y posición de los estudiantes durante las clases.

5. Datos de usuario de la plataforma web:

a) Nombres de usuario y contraseñas.
b) Datos de contacto, como direcciones de correo electrónico.

6. Datos de informes y estadísticas:

a) Datos agregados sobre la asistencia y participación de los estudiantes.
b) Información utilizada para generar informes y métricas relacionadas con el rendimiento de los estudiantes.

Como se puede ver, la mayoría de la información es altamente sensible por lo que se tiene que manejar bajo un proceso de anonimización y extrema seguridad para evitar cualquier violacion en los mismos.

Normativa a seguir

Gracias a la naturaleza de los datos, es pertinente manejarlos bajo la normativa vigente, de manera que no se violen los estándares establecidos para este tipo de datos. En México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) es la regulación principal relacionada a la protección de datos personales y privacidad. A continuación se enlistan los principales puntos a considerar de la misma así como acciones claves para su cumplimiento:

Normativa	Acciones a seguir
Aviso de privacidad	Proporcionar a los estudiantes un aviso de privacidad que explique de manera clara y sencilla cómo se recopilarán, utilizarán y protegerán sus datos personales en la plataforma.
Consentimiento informado	Obtener el consentimiento informado de los estudiantes o sus padres/tutores legales antes de recopilar y procesar sus datos personales. El consentimiento debe ser libre, informado, expreso y revocable.
Seguridad de datos	La normativa de la LFPDPPP requiere que se tomen medidas técnicas, administrativas y físicas para proteger los datos personales contra el acceso no autorizado, la divulgación y la pérdida.
Derechos de los titulares de datos	Establecer un proceso para que los estudiantes ejerzan estos derechos los cuales consisten en el acceso, rectificación, cancelación y oposición de sus datos personales.
Registro de datos personales	Debido a la naturaleza de los datos, es posible que se deba registrar la base de datos de datos personales ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).
Retención de datos	La ley establece períodos de retención para los datos personales, por lo que se debe tener un plan para la eliminación segura de datos cuando ya no sean necesarios.

Debido a que el proyecto se encuentra en una fase de prototipo se implementarán solamente las medidas necesarias para la protección de datos acorde a esta etapa del proyecto. A continuación se enlistan las acciones finales a implementar durante esta etapa del proyecto:

1. **Definición de roles y responsabilidades:** Para un mejor y más seguro manejo de los datos se implementará un sistema de roles y responsabilidades dentro de la plataforma que permita un manejo y acceso a los datos más controlado por parte de los usuarios. Con esto se busca evitar el uso indebido de los mismos por parte de usuarios o personas no autorizadas.
2. **Aviso de privacidad:** A través de la firma en un documento se proporcionará a los estudiantes y demás usuarios un aviso de privacidad donde se explique de manera clara y sencilla cómo se recopilarán, utilizarán y protegerán sus datos personales en la plataforma.
3. **Consentimiento informado:** A través de la firma de un documento se les solicitará el consentimiento informado de los estudiantes o sus padres/tutores legales antes de recopilar y procesar sus datos personales. El consentimiento debe ser libre, informado, expreso y revocable.
4. **Seguridad de datos:** se tomarán medidas técnicas, administrativas y físicas para proteger los datos personales contra el acceso no autorizado, la divulgación y la pérdida.

Anonimización de datos

Con el fin de preservar la confidencialidad y seguridad de los datos se siguieron una serie de acciones que permiten proteger la privacidad de los datos personales de los estudiantes y demás usuarios de la plataforma. A continuación se enlistan las acciones tomadas:

1. **Identificación de datos sensibles:** Como primer paso se hizo un mapeo de los datos generados y utilizados de manera que pudiéramos identificar cuales representaban un mayor riesgo para la privacidad de los usuarios. De esta manera pudimos concentrarnos en estos mismos para su protección.
2. **Uso de IDs e información Dummy:** Para esta fase del proyecto donde el objetivo principal es el prototipado de la plataforma se implementó el uso de IDs e información Dummy de los usuarios. De esta manera en ningún momento se guardan datos reales que puedan relacionarse a la información personal de los usuarios.

3. **Cifrado de datos (en desarrollo):** con el fin de mantener la seguridad de los datos, se implementará un sistema de cifrado de los mismos de manera que no sean accesibles sin las claves y permisos necesarios.

Mecanismo de acceso a los datos

El control en el acceso a los datos es sumamente importante para la protección de estos asi como de la privacidad de los usuarios por lo que se tomaron las siguientes medidas como parte del mecanismo de acceso a los datos.

1. **Control de acceso:** se estableció un sistema de roles el cual permite un acceso controlado a los datos por parte de los miembros del equipo de desarrollo y bloqueando el mismo a cualquier otra persona o usuario de la plataforma.
2. **Solicitud de acceso a los datos:** debido a la etapa de desarrollo del proyecto, se definió el siguiente proceso para el acceso a los datos por parte de los miembros del equipo de desarrollo con el fin de respetar la normatividad asociada:
    a. Solicitud de Acceso: se debe enviar una solicitud al resto del equipo la cual debe incluir el propósito del acceso y la justificación del mismo.
    b. Acceso Limitado: se accede únicamente a los datos especificados en la solicitud de acceso del paso previo bajo supervisión de otro miembro del equipo.
    c. Informe a miembros del equipo: se deberá informar sobre las acciones realizadas en los datos accesados.
    d. Registro de acciones tomadas: se deberá llevar un registro de las acciones tomadas en los datos.