



Campus Estado de México

Inteligencia artificial avanzada para la ciencia de datos II (Gpo 101)

Reto Privacidad y Seguridad de los Datos

Juan Pablo Castañeda Serrano A01752030
Aldo Daniel Villaseñor Fierro A01637907
Francisco Castorena Salazar A00827756
José Alfredo García Rodríguez A00830952

Atributos y las razones del enmascaramiento de datos.

Ya que nuestro proyecto se divide en tres (Frontend con react, backend con FLASK y la base de datos en MongoDB). Tomamos consideraciones en las tres tecnologías:

Seguridad en la API de Flask:

Autenticación y Autorización: Implementamos autenticación utilizando tokens dados en .env de AWS y nos aseguramos de que solo los usuarios o sistemas autorizados puedan acceder a nuestros endpoints.

HTTPS: Usaremos siempre HTTPS para transmitir datos entre el cliente y el servidor. Esto protege la información durante su transmisión. De este modo igual las conexiones sólo podrán conectarse de tener un certificado

Limitar la exposición de endpoints: No exponemos endpoints innecesarios y utilizamos técnicas de rate-limiting para prevenir ataques de fuerza bruta.

Seguridad en MongoDB:

Autenticación: Nos aseguramos de que MongoDB esté configurado para requerir autenticación.

Encriptación:

En Reposo: Utilizamos la encriptación at-rest para proteger los datos almacenados. con el seteo de contraseña de MongoDB Compass

En Tránsito: Nos aseguramos de que los datos transmitidos a y desde MongoDB están encriptados utilizando TLS/SSL.

Backup Seguro: Al hacer backups, nos aseguramos de que también están encriptados y almacenados de forma segura.

Seguridad en React

CORS (Cross-Origin Resource Sharing): Configuramos correctamente los headers de CORS en nuestro servidor Flask para que solo nuestra aplicación React pueda hacer solicitudes a la API. Esto implementado en la siguiente fase de nuestro proyecto para poder realizar pruebas con PostMan

Otras consideraciones generales:

Actualizaciones Regulares: Mantenemos todas las tecnologías (React, Flask, MongoDB, Yolo) actualizadas para asegurarte de tener las últimas correcciones de seguridad.

Entrenamiento y Concienciación: Aseguramos de que todos los involucrados en el desarrollo y mantenimiento del sistema están bien informados sobre las mejores prácticas de seguridad.

Normativa actual de la industria a la que esté sujeto el socio formador:

LFPDPPP. INAI

([https://inicio.inai.org.mx/English_Section_Documents/LFPDPPP%20ENG%20\(1\).pdf](https://inicio.inai.org.mx/English_Section_Documents/LFPDPPP%20ENG%20(1).pdf))