Inteligencia artificial avanzada para la ciencia de datos II

(Gpo 501)

Módulo 4 - Momento de Retroalimentación

Integrantes del equipo:

Ana Lucía Cárdenas Pérez	A01284090
Diego Elian Rodriguez Cantú	A00829925
José Edmundo Romo Castillo	A01197772
Elías Garza Valdés	A01284041

Profesor

Ivan Mauricio Amaya Contreras

Hugo Terashima Marín

Monterrey, Nuevo León a 27 de Octubre del 2023

1. Verificar que los datos están anonimizados. Describir los atributos y razones por las que tienen que enmascarar.

La anonimización de datos es un proceso crucial para garantizar la privacidad y seguridad de la información personal de los individuos involucrados en el proyecto. Dado que el proyecto maneja datos sensibles de estudiantes, como nombres completos, edades, matrículas y fotografías, es imperativo implementar medidas de anonimización robustas. A continuación, se describen los atributos que requieren enmascaramiento y las razones para hacerlo:

1. Nombres completos:
   - Enmascaramiento: Los nombres reales se reemplazan con identificadores únicos o pseudónimos que no guardan relación con la identidad real de los estudiantes.
   - Razón: Esta medida previene la divulgación de la identidad de los estudiantes y protege su privacidad.

2. Edades:
   - Enmascaramiento: Las edades se generalizan en rangos (por ejemplo, 18-20, 21-23, etc.) en lugar de especificar la edad exacta.
   - Razón: Esta acción reduce la posibilidad de identificar a los individuos y mantiene una cierta privacidad mientras se retiene la utilidad de los datos.

3. Matrículas:
   - Enmascaramiento: Las matrículas se reemplazan con identificadores únicos que no están relacionados con los estudiantes.
   - Razón: Esta estrategia previene el riesgo de identificación y asegura la confidencialidad de la información personal de los estudiantes.

4. Fotografías:
   -Enmascaramiento: Se aplican técnicas de desidentificación facial, que alteran o difuminan las características faciales, o se substituyen las fotografías reales con avatares genéricos.
   -Razón: Esta medida evita la identificación de los estudiantes a partir de sus características faciales y garantiza su privacidad.

Respecto a la base de datos de Deta Space, es vital asegurar que los procesos de anonimización se realicen antes de almacenar o procesar los datos. Además, es prudente verificar las políticas de privacidad y seguridad de la plataforma, y considerar la implementación de medidas de seguridad adicionales, como el cifrado de datos, para garantizar una protección adecuada. Finalmente, es fundamental estar al tanto y cumplir con las regulaciones y leyes de privacidad de datos aplicables, como el Reglamento General de Protección de Datos (GDPR) en Europa o la Ley de Protección de Datos Personales (LFPDPPP) en México, entre otros, dependiendo de la jurisdicción en la que se encuentre el proyecto.

2. Consultar normativa para la privacidad de los datos y pasos comunes que se toman para garantizar la privacidad de los datos

La Ley de Protección de Datos en México regula cómo las empresas y organizaciones deben manejar la información personal. Requiere el consentimiento de las personas, garantiza sus derechos de acceso y seguridad de datos, y establece sanciones por incumplimiento. Su objetivo es proteger la privacidad de los datos personales en manos de particulares. Algunos puntos claves de la ley son:

- **Consentimiento**: se debe de solicitar consentimiento por parte del usuario sobre el uso de sus datos personales.
- **Derechos de los titulares de los datos**: Los titulares de los datos deberán tener derecho a acceder a sus datos, rectificarlos, cancelarlos y hasta oponerse al tratamiento
- **Seguridad de datos**: las organizaciones deben de implementar medidas de seguridad para proteger la información
- **Transferencia de datos**: la transferencia de datos está sujeta a restricciones y requisitos específicos
- **Responsable de datos**: la empresa deberá de designar un encargado para la protección de datos personales y supervisar el cumpliento de la ley
- **Notificación sobre violaciones de los datos**: la organización deberá de notificar a los titulares de datos y a las autoridades correspondientes si existe una brecha de seguridad que afecte la privacidad de los datos personales.
- **Sanciones**: esta misma ley establece sanciones y multas para quienes hagan incumplimiento de los puntos mencionados.

3. Proceso sobre cómo se trabaja con los datos

a. *Dónde se puede almacenar:* Se pueden guardar los datos en un servidor preferiblemente que tenga un entorno seguro y que se hagan copias de seguridad regularmente. También se puede hacer uso de servicios en la nube como Google Cloud Storage o Microsoft Azure Blob Storage para guardar las imágenes.
b. *En qué tipo de redes puede estar:* En una red privada, al ser información sensible. También se puede utilizar una VPN para acceder a los datos de forma segura desde ubicaciones remotas y para agregar un poco más de seguridad, pedir autenticación cada vez que se quiera ingresar a estos desde una red externa.
c. *Quién puede ver los datos:* Personas como profesores y personal administrativo deben de contar con permisos de acceso y visualización. Para esto se puede implementar un sistema de autenticación y autorización para garantizar que solo esas personas puedan acceder a la información.
d. *Documentos o reglamentos que se deben firmar antes de acceder a los datos:* Antes de que el personal tenga acceso a los datos, los usuarios deben firmar un acuerdo de confidencialidad y cumplimiento de las políticas de seguridad de datos.

4. Herramientas se pueden usar para quién y cuándo tuvo acceso a los datos

a. *Registro de acceso a la base de datos:* El sistema de registro de acceso guardará quién accede a la base de datos, cuándo lo hizo y qué realizó en el sistema.
b. *Sistemas de control de acceso:* Ayuda a gestionar quién puede acceder a qué datos y qué pueden hacer. Esto implica la definición de roles y permisos para los usuarios.
c. *Herramientas de auditoría de registros:* Herramientas de auditoría de registros permiten a los administradores supervisar y revisar las actividades de los usuarios.
d. *Monitoreo de seguridad:* Estas herramientas pueden alertar sobre intentos no autorizados o actividades sospechosas que se lleven a cabo dentro del sistema.
e. *Informes de acceso:* Generar informes regularmente con los accesos a los datos registrados, y así poder ver quién ha accedido a qué información y en qué momentos.