Prueba técnica Profesional Machine Learning

Punto 1

- Resolución del problema
    - Emplearía componentes de la nube de Azure para construir una solución que contemple temas de almacenamiento de datos, registro de logs, modelos de IA, gestión de repositorios de código, almacenamiento de secretos y desencadenadores de eventos
- Metodología:
    - Como paso cero, tendría creado un repositorio en Azure Devops con las ramas, pipelines de despliegue y CI/CD de la solución. Asimismo, un Azure Key Vault para almacenar las credenciales y secretos. En el correo tendría creadas 4 carpetas las cuales corresponden a los 4 tipos de de correos que identificará el modelo
    - Primero usaría un servicio de Azure (Logic App, Azure Function) que se encuentre monitoreando la bandeja de entrada (esperando que llegue un correo) y realice una notificación al momento de llegar un correo nuevo
    - Acto seguido pasaría el correo por el modelo de procesamiento de lenguaje natural (NLP) con el fin de realizar el análisis y comprensión del texto alojado en el correo, identificando la intención como comprar, vender, entidades como la empresa, productos, e información relevante que permita clasificar el correo en uno de los 4 tipos
    - Posterior guardaría la información extraída en una base de datos relacional. Los logs de errores los almacenaría en un Azure Storage
    - Finalmente, teniendo la clasificación del correo, clasificaría el correo en la carpeta que corresponde dependiendo de su tipo
- Modelos:
    - CLU (Conversational Language Understanding)
    - Azure Open AI (modelo de IA generativa)
- Arquitectura:
    - Correo electrónico
    - Azure Logic Apps (eventos al llegar un correo)
    - Modelo de IA para procesamiento
    - Azure SQL (almacenar datos del correo)
    - Azure Storage (almacenar logs de error de la solución)
    - Azure Devops (manejo de repositorios de código, CI/CD)
    - Azure Key Vault (manejo de secretos)

Punto 2

Sí, el modelo está sufriendo una deriva incremental (incremental drift). Esto se debe a que los datos con los que se entrenó no representan las condiciones actuales, por lo que ha perdido precisión en sus predicciones.

Para validar la deriva en el modelo, usaría pruebas estadísticas temporales las cuales me ayuden a detectar cambios en los datos a lo largo del tiempo y la observación del rendimiento del modelo para así detectar desviaciones en un momento determinado

Para evitar la deriva en el modelo, haría pruebas periódicas e intervenciones proactivas del rendimiento del modelo con el fin de tener un modelo que perdure en el tiempo y pueda afrontar los cambios. De igual forma, tendría presente cuales son los factores que provocan la deriva y tomaría medidas para evitarlos

Si el modelo presentó deriva, abordaría de 2 formas el problema:

- Si la deriva del modelo es reversible, lo que haría es volver a entrenarlo con los nuevos datos, y de ser necesario ajustar nuevos parámetros
- Si la deriva del modelo no es reversible, pensaría en cambiar el modelo por uno más robusto

Punto 3

Para evitar que el modelo genere texto aleatorio (alucinaciones) y se obtenga la información solicitada, tendría en cuenta 3 factores:

- Utilizar prompts específicos los cuales busquen delimitar la respuesta del modelo (plantillas de prompts que se pueden importar de librerías)
- Supervisión humana al tener una persona que esté evaluando y juzgando la calidad de las respuestas (sea el desarrollador o usuario final)
- Configurar parámetros como la temperatura del modelo a 0 para que el modelo sea preciso y reduzca la aleatoriedad en los textos generados