Integrantes:

Diana Avelino
Johana Correa
Ricardo Rivera
Adriana Hernandez

TALLER 2. COMPROBANDO LA VIABLIDAD DE NUESTRA INICIATIVA

Actividad 1. Repitiendo el live

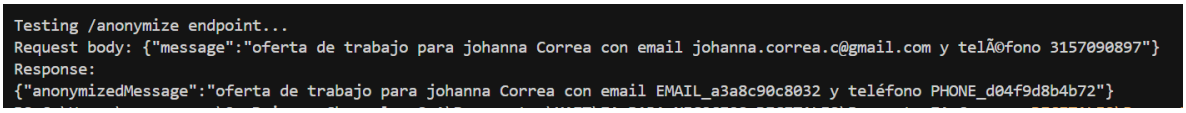
Link del repositorio: https://github.com/Adrianahernandezbejarano/BancoAndino-Onboarding-PoC/tree/main/LiveDemo

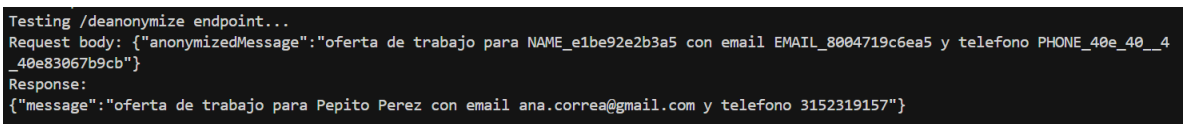
Prompts

- Instala Node.js
- Crea un Data Privacy Vault para que la informacion PII (Informacion de identificación personal) se anonimice usando node.js.
- Desarrolla un endpoint que reciba una cadena con un mensaje que contenga PII como nombres, correos electrónicos y números de teléfono, y que devuelva el mensaje anonimizado, reemplazando el nombre, correo y teléfono por un token alfanumérico.
- Por favor, actúa como un desarrollador senior en Node.js y dime paso a paso cómo lo harías. Pregúntame la información que necesites y utiliza buenas prácticas de codificación y comentarios en las funciones.
- Un ejemplo de request es:
    - curl -X POST http://localhost:3001/anonymize -H "Content-Type: application/json" -d '{"message":"oferta de trabajo para Dago Borda con email dborda@gmail.com y teléfono 3152319157"}'
    - el response sería:
    - {
    - "anonymizedMessage": "oferta de trabajo para d7e8e0bf bd673df2 con email b09bde30 y teléfono dd195b6c"

    - }
- curl -X POST http://localhost:3001/anonymize -H "Content-Type: application/json" -d '{"message":"oferta de trabajo para johanna Correa con email johanna.correa.c@gmail.com y teléfono 3157090897"}'
    - The response to that request would be: { "anonymizedMessage": "oferta de trabajo para d7e8e0bf bd673df2 con email b09bde30 y teléfono dd195b6c" }
- Gracias. Ahora, implementemos el endpoint de desanonimización donde la llamada debería ser así: curl -X POST http://localhost:3001/deanonymize \ -H "Content-Type: application/json" \ -d '{"anonymizedMessage":"oferta de trabajo para NAME_e1be92e2b3a5 con email EMAIL_8004719c6ea5 y telefono PHONE_40e83067b9cb"}' Y debería devolver el mensaje original: {"message":"oferta de trabajo para Pepito Perez con email ana.correa@gmail.com y teléfono 3152319157"}
- Verifica que el servicio esté arriba y funcionando
- Ajusta el manejo de errores añadiendo bloques catch para la gestion de errores controlado
- Incluye las pruebas unitarias del servicio para verificar que se cumplan todos los escenarios (200, 400 y 500)
- modifica el Código incluyendo Archivos de internacionalización para el manejo de mensajes y ajusta el Código
- Crea un módulo dedicado constants.js y exporta las constantes desde ahí el lineamiento es cero constantes regadas por el código.

Evidencia:



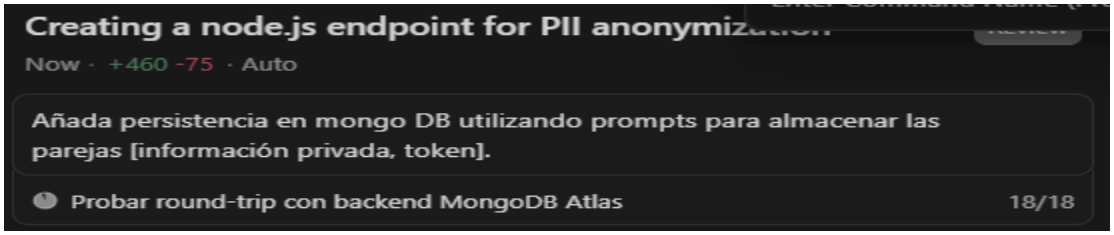


Actividad 2 – Añadiendo persistencia

Link del repositorio: https://github.com/Adrianahernandezbejarano/BancoAndino-Onboarding-PoC/tree/main/taller%202

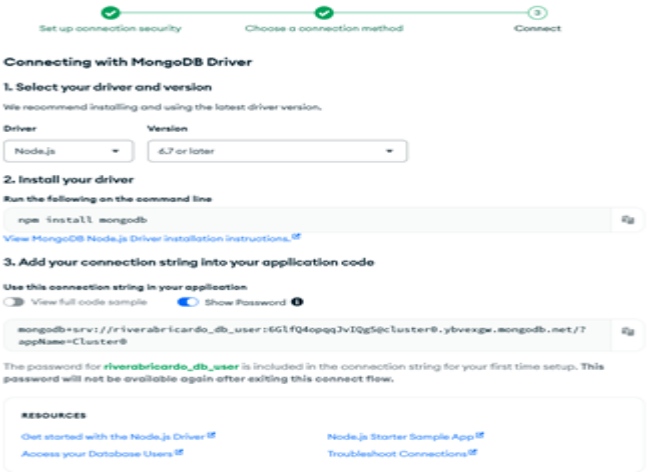
1. Añada persistencia en mongo DB utilizando prompts para almacenar las parejas [información privada, token].

Se procede a ejecutar el siguiente prompt en Cursor

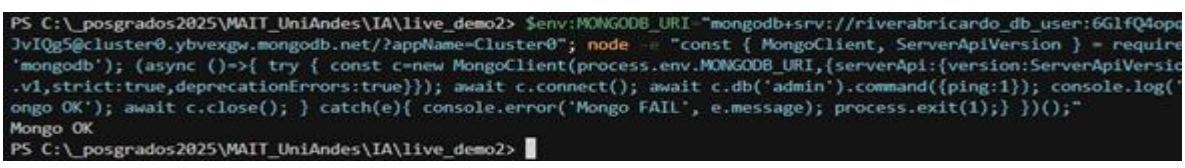


2. Cree una cuenta en MongoDB Atlas

Se realizar la creación de la base de datos identificando la cadena de conexión entre otros datos



Se arranca el servidor mongodb y se comprueba que la instancia esté arriba



3. Conecte su aplicativo con la persistencia cambiando la cadena de conexión donde el asistente de IA puso la conexión.

```
PS C:\_posgrados2025\MAIT_UniAndes\IA\live_demo2> $env:VAULT_BACKEND="mongo"
PS C:\_posgrados2025\MAIT_UniAndes\IA\live_demo2> $env:MONGODB_URI="mongodb+srv://riverabricardo_db_user:6GlfQ4opqq
ybvexgw.mongodb.net/?appName=Cluster0"
PS C:\_posgrados2025\MAIT_UniAndes\IA\live_demo2> $env:DATA_KEY_HEX="0123456789abcdef0123456789abcdef0123456789abcd
ef"  # 64 hex
PS C:\_posgrados2025\MAIT_UniAndes\IA\live_demo2> $env:TOKEN_SALT="tu-salt"
PS C:\_posgrados2025\MAIT_UniAndes\IA\live_demo2> $env:PORT="3001"
PS C:\_posgrados2025\MAIT_UniAndes\IA\live_demo2> node src/server.js
```

4. Pruebe nuevamente el servicio de anonimizar y desanonimizar.

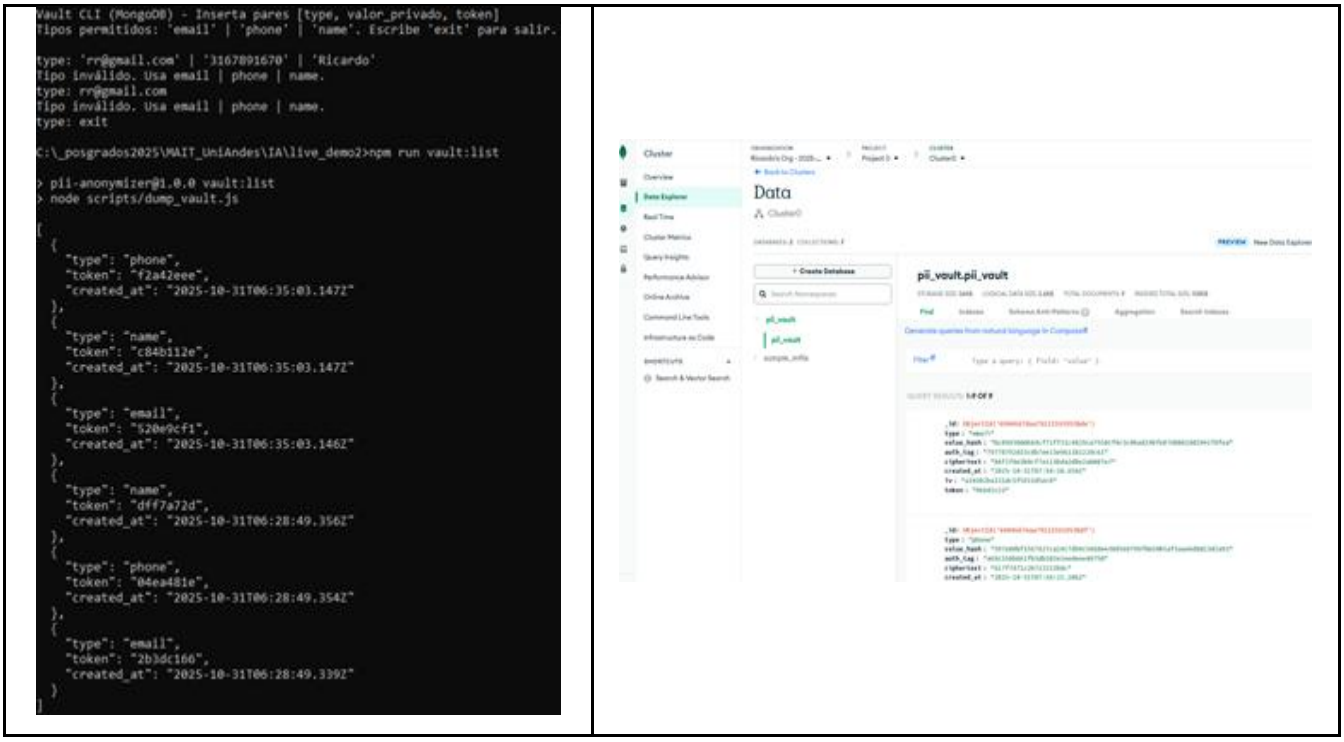
Se validaron servicios activos

Se cargan variables de entorno y se procede a ejecutar el curl para almacenar varios ejemplos de anonimización

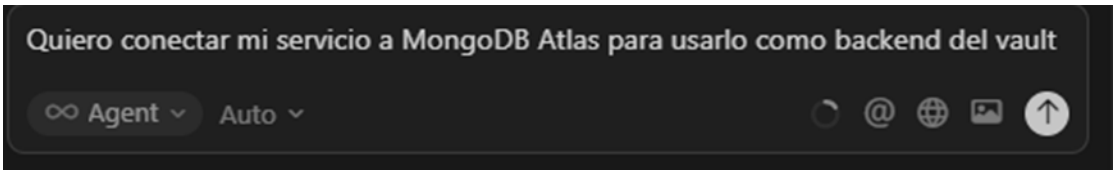
```
C:\_posgrados2025\MAIT_UniAndes\IA\live_demo2>curl.exe -X POST "http://localhost:3001/anonymize" -H "Content-Type: a
pplication/json" -d "{\"message\":\"oferta de trabajo para Ricardo Rivera con email rrivera@gmail.com y teléfono 316
7891670\"}"
{"anonymizedMessage":"oferta de trabajo para c84b112e con email 520e9cf1 y teléfono f2a42eee"}
```

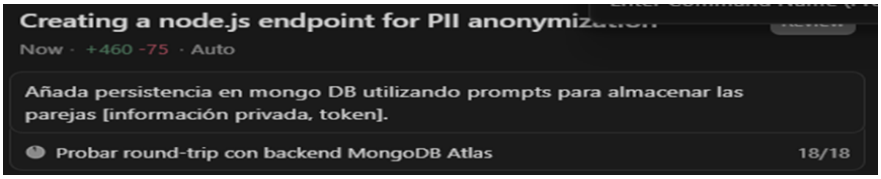
5. Incluya el resultado de su prueba en el documento con sus prompts.
   Se puede observar la persistencia de los datos en mongoDB tanto desde consola como desde la interfaz

Consola	Interfaz MongoDb



Los prompts utilizados fueron los siguientes:



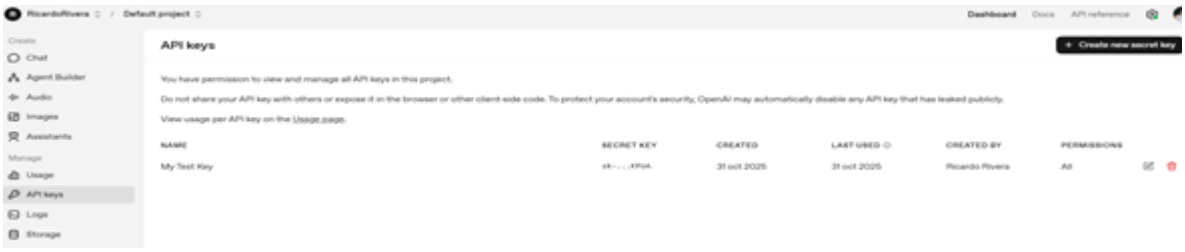


Actividad 3 – Comunicación con la IA

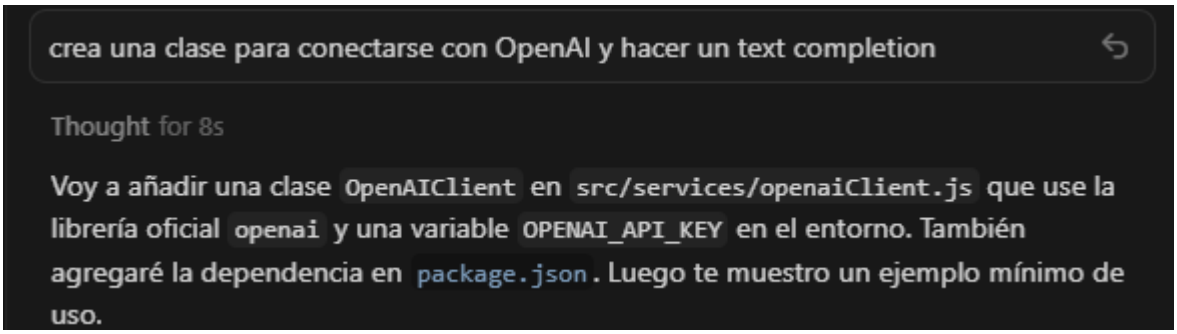
Link del repositorio:
https://github.com/Adrianahernandezbejarano/BancoAndino-Onboarding-PoC/tree/main/taller%202

1. Si aún no tiene cuenta en OpenAI, cree una y cree su developer API key en https://platform.openai.com/docs/overview

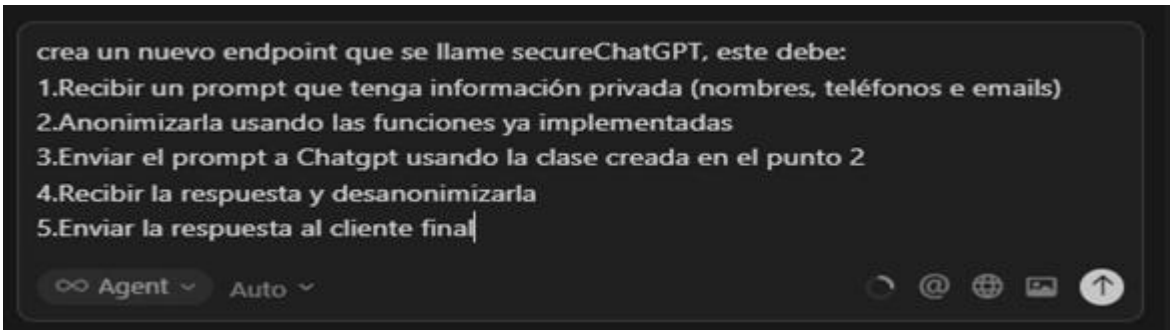
Se crea la cuenta en OpenIA y se genera la API Key



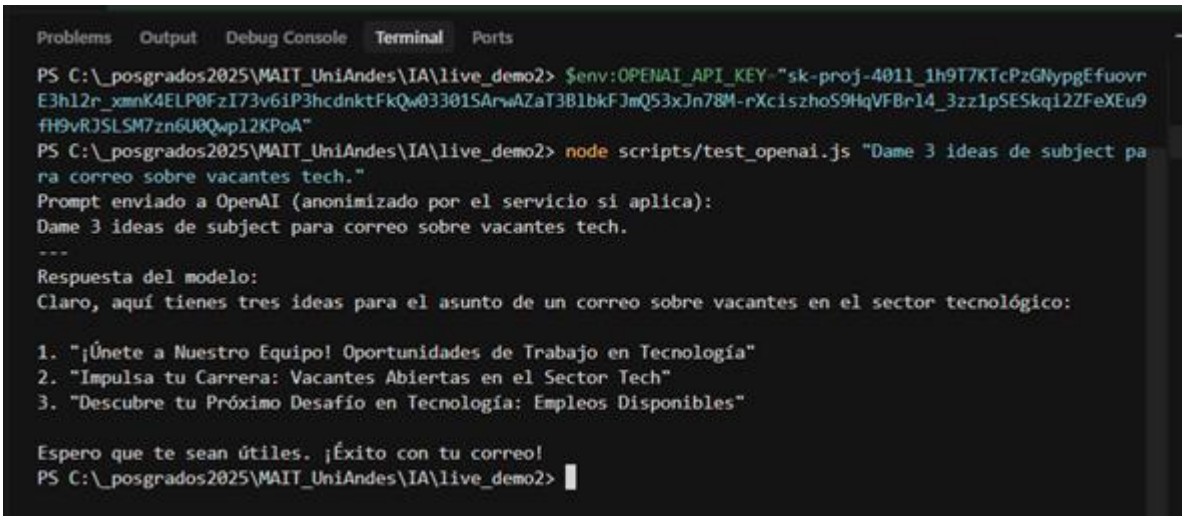
2. Solicite a Cursor que le cree una clase para conectarse con OpenAI y hacer un text completion



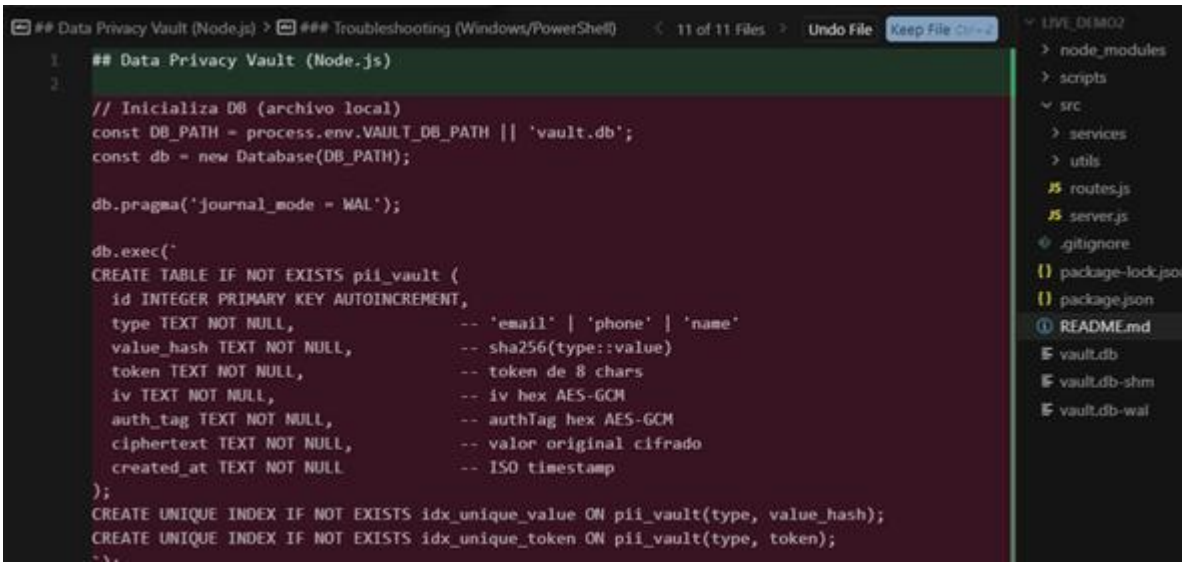
3. Ahora haga un nuevo endpoint que se llame secureChatGPT, este debe:
   - Recibir un prompt que tenga información privada (nombres, teléfonos e emails)
   - Anonimizarla usando las funciones ya implementadas
   - Enviar el prompt a Chatgpt usando la clase creada en el punto 2
   - Recibir la respuesta y desanonimizarla
   - Enviar la respuesta al cliente final



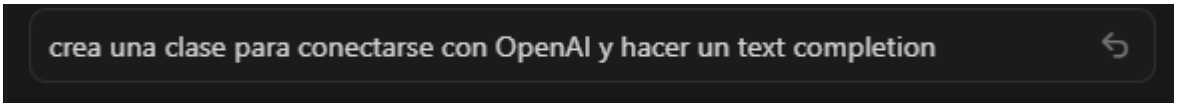
Para probar la funcionalidad del endpoint secureChatGPT se creó el script test_openai.js y se procedió a su ejecución:

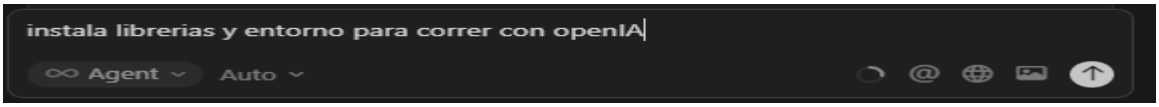


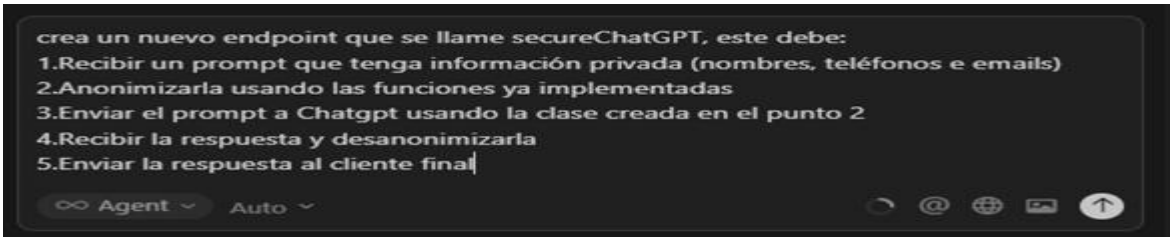
4. Pídale a cursor que le genere un archivo Readme.md con la descripción del proyecto y los pasos para instalarlo.
   Incluya un archivo en la raíz indicando los prompts que usó para llegar hasta este punto.

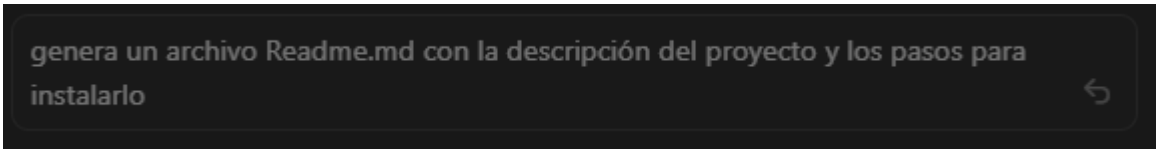


Los prompts utilizados fueron los siguientes:









Actividad 4. Conclusiones y entrega

- Con las herramientas de inteligencia artificial tenemos una aceleración significativa en el ciclo de desarrollo de software desde la conceptualización hasta el despliegue lo que antes tomaba semanas ahora toma días.

- Con las herramientas de inteligencia artificial generativa y la democratización del conocimiento hace posible que el desarrollo de aplicaciones no sea exclusivo para equipos técnicos (acotado proyectos complejidad baja), ya que para proyectos de complejidad media o alta vemos que se debe tener un conocimiento por lo menos de bases técnicas.

- No solo los ingenieros y perfiles técnicos deben prepararse para usar esta tecnología, ya que conocer como realizar los prompt para generar proyectos y otras tareas en general, seguramente se va a extender a diferentes áreas de conocimiento y de trabajo, lo que va a potenciar lo que se puede hacer y va a crear nuevas formas de trabajar.

- En relación con el valor a negocio, permite iterar y probar rápidamente hipótesis que puedan ser relevantes para el negocio y el cumplimiento de los objetivos estratégicos, mitigando el riesgo de los inversionistas de perdida.

- Aunque el valor de la inteligencia artificial generativa en el ciclo de software es invaluable, se debe tener en cuenta que la autogeneración de código y análisis de los requerimientos puede tener sesgos, o bugs, por lo que es importante validar las salidas a los prompts

- Para proyectos grandes se debe considerar la supervisión de un experto, así como la mantenibilidad y escalabilidad a largo plazo.

- Saber alimentar con el contexto correcto al LLM para el trabajo y conocer cómo realizar los prompt aumenta la posibilidad de éxito en los resultados

- Construir instrucciones claras y contextuales se vuelve clave para maximizar la capacidad de las herramientas de IA, reduce el retrabajo y acelera la entrega de valor.

- En la clase y en el taller la IA da un valor agregado ya que sugieren mejoras y pasos a seguir lo cual mejora la experiencia y la solución, con el prerrequisito de un contexto detallado para evitar “alucinaciones”

- La demo se hace en un escenario controlado donde están todas las herramientas para ejecutar, pero en cuanto se va ejecutando el taller se requiere complejidades del desarrollo de software normales.

- Hay que buscar como organizar la información que va generando la herramienta de IA, porque se puede extender y luego se pierde el objetivo inicial de la tarea