Promptior Chatbot

El objetivo es hacer un chatbot con Langchain que implemente una arquitectura RAG, para retornar informacion que se encuentra en <u>promptior.ai</u> y que sea capaz de responder preguntas acerca de Promptior, como por ejemplo "Que servicios ofrece Promptior?" y "Cuando fue fundada la empresa?. Y que ese mimo chatbot se pueda interactuar desde Langserve Playground.

Las Tecnologias utilizadas fueron:

- Python
- Langchain
- LangSmith (Evaluador)
- LangServe
- Redis (Chat History)
- Pinecone (Vector Store)
- Replit (IDE y Cloud provider)

A continuacion te presentare las etapas de la implementacion, anexandote imagenes, codigo y comentarios de los problemas que tuve en el camino y como los resolvi.

Preprocessing

1. **Webscraping**: Obtener el HTML del website, asi como sus links asociados. Uno de los principales razones por la que no use la clase de langchain para hacer Scraping es porque no me retornaba el HTML completo. Decidi construir funciones que retornara correctamente el html de la pagina principal y de la de los links asociados, ignorando los links que retornaban a la misma pagina y los que eran links externos.

Resolucion de Problema: El primer problema fue que no me cargaba bien el sitio y le agregue una condicion para que esperara a que un Xpath estuviera presente, despues de eso que me retornara el HTML. El segundo fue que cuando queria que retornara el HTML de los links asociados, excepto los externos y los de la pagina principal.

```
class WebScraper:
    def __init__(self, url):
        self.main url = url
        self.browser = None
        self.page = None
    def setup_browser(self, playwright):
        self.browser = playwright.chromium.launch(headless=Ti
        self.page = self.browser.new_page()
    def navigate_and_extract(self):
        self.page.goto(self.main url, wait until="networkidle"
        self.page.wait_for_selector("xpath=//div[@id='root']'
        html_content = self.page.content()
        title = self.page.title()
        links = self.page.query_selector_all("a")
        hrefs = [self.page.evaluate("el => el.getAttribute('l
        main domain = urlparse(self.main url).netloc
        for href in hrefs:
            if href.startswith("/") and not href.startswith('
                href = self.main_url.rstrip("/") + href
            if urlparse(href).netloc == main_domain:
                print(f"Navegando a {href}")
                try:
                    self.page.goto(href, wait_until="network:
                    page_content = self.page.content()
```

Retrieval System

- 1. Text Processing: Despues de obtener el HTML, se proceso a texto con

 HTML2TextTransform y al ver que el Texto me lo entrego con los titulos y los
 subitulos con el formato markdown (# , ##, ###).
- 2. Split in Chunks: Se uso MarkdownHeaderTextSplitter para obtener los chunks, y que cada chunk correspondiera al tema que le corresponde. En este caso como el contexto de la informacion no era muy grande, elegi por dividirlo solo por el header ##, por ejemplo:

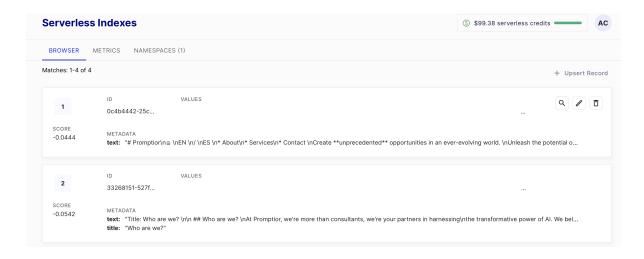
```
## Who are we?
```

At Promptior, we're more than consultants, we're your partners in harnessing the transformative power of AI. We believe the real magic happens not just through technology implementation, but when it's fully embraced within every corner of your organization. We're committed to fostering an ecosystem where innovation isn't merely applied, but seamlessly integrated, becoming an essential part of your daily processes, strategic decisions, and operational framework. We're here to guide you every step of the way on this transformative journey, ensuring it's not just smooth, but truly empowering. With Promptior by your side you're stepping confidently into a future full of unprecedented possibilities.

```
def transform_and_split(self, html_content, page_content, til
        doc_1 = Document(page_content=html_content)
        doc 2 = Document(page content=page content)
        html2text_transformer = Html2TextTransformer()
        transformed docs = html2text transformer.transform do
        promptior_content = f"# {title} \n {transformed_docs
        headers_to_split_on = [
            ("##", "title")
            # ("###", "sub_title"),
        1
        markdown_splitter = MarkdownHeaderTextSplitter(header
        docs = markdown_splitter.split_text(promptior_content
        for doc in docs:
            if 'title' in doc.metadata:
                doc.page_content = f"Title: {doc.metadata['t:
        return docs
```

De igual forma a los metadata se le agrego el titulo del header que el corresponde.

- 3. Embed Chunks: Se uso el modelo de OpenAl text-embedding-3-small con dimension de 1536.
- 4. Vector Store: Use Pinecone (PineconeVectorStore), por sus diferentes formas de hacer busqueda y tambien por calidad y precio en su mejora de Serverless.



Resolucion de Problemas: En esta etapa tuve problemas con definir de que manera era mas eficiente hacer splits de la informacion, ya que que al implementar el RAG, hacia busqueda por similaridad y me retornaba chunks que no deberia (Los retornaba porque en ciertos chunks contenia la palabra "Services", que era parte del header o footer del html). Eso pasaba cuando realizaba la pregunta "Que servicios ofrece la empresa?". Por lo tanto al estar analizando bien la situacion, no era necesario que en mi retrival se retornaran 2 documentos de contexto, y por el caso de es muy poca la informacion porcedi con el aumento del top_k=4. Tambien aplique Rerank con Cohere (Para hacer un filtrado de la informacion y en ves de 4 chunks, fueran 2 o 3), pero vi que no era necesario el Rerank y lo deje en top_k = 4.

Agent

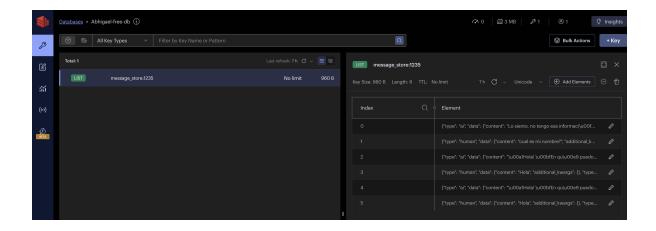
Se creo un Agente con Chat History, para mejorar la conversacion entre Usuario-Agente, tambien agregandole capacidades para ejecutar Tools en el momento que sea requerida.

```
def create_agent(self):
  prompt = ChatPromptTemplate.from_messages(
      E
          (
              "system",
              "You are very powerful assistant."
              "Talk with the user as normal. "
          ),
          MessagesPlaceholder(variable_name="chat_history"),
          ("user", "{input}"),
          MessagesPlaceholder(variable_name="agent_scratchpad"),
      ]
  )
  11m = ChatOpenAI(temperature=0, model="gpt-3.5-turbo-0125")
  agent = create_openai_functions_agent(llm, self.tools, prompt)
  agent executor = AgentExecutor(agent=agent, tools=self.tools,
  return agent executor
def run(self):
    agent_with_chat_history = RunnableWithMessageHistory(
        self.agent,
        self.get_message_history,
        input_messages_key="input",
        history messages key="chat history",
    ).with_types(input_type=Input, output_type=Output).with_conf
    return agent_with_chat_history
```

- Tools ←→ search_promptior → Retrieval(→ Input Query → List[Documents]):
 Se creo para que cuando el usuario realice una pregunta acerca de Promptior,
 haga busqueda por similaridad y retorne una lista de documentos para el
 contexto.
- 2. Model \rightarrow gpt-3.5-turbo-0125 : Se uso este modelo por fines de calidad-precio.

3. Chat history: Aqui implemente *Redis* para almacenar y consultar el historial de las conversaciones, dependiendo del "session_id" (Para identificar a quien pertenece).

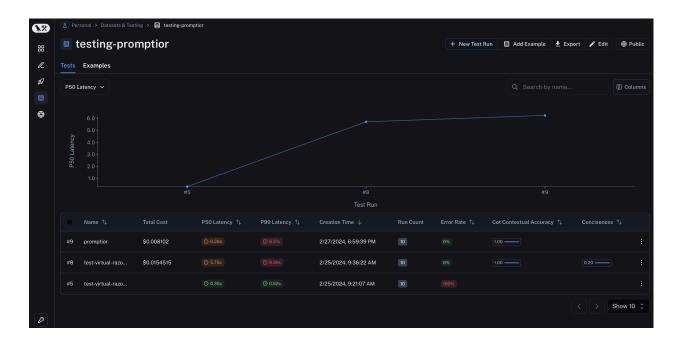
```
def get_message_history(self, session_id: str):
    return RedisChatMessageHistory(session_id, url=self.
```



Resolucion de Problemas: Aqui el porblema que tuve fue al principio la integracion con Redis, me sucedian problemas de Autentificacion por la URL ingresada, pero ya al estar leyendo documentacion tenia que agregarles mas parametros como la password dentro de la URL, despues de eso el historial de las conversaciones lo registra correctamente dependiendo del "session_id" que se asigne.

Evaluation Benchmark

Cree una evaluacion para evaluar la capacidad de pregunta y respuesta del Chatbot con LangSmith.

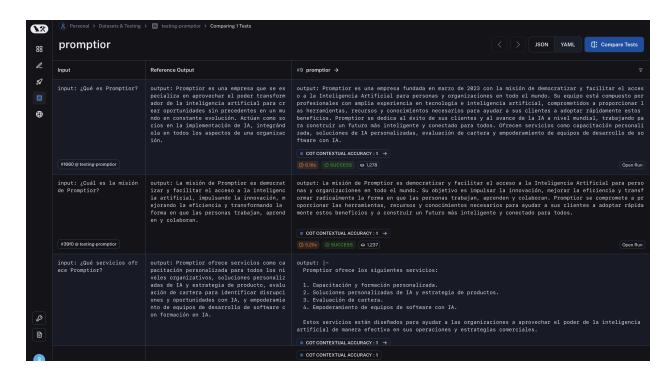


Genere una lista de preguntas y respuestas esperadas. Despues con RunEvalConfig use la metrica de "Cot Contextual Accuracy", para evaluar que lo que responda el chatbot este dentro del contesto de la respuesta correcta.

```
def evaluation_agent(self, dataset_name="testing-promptior", pro
      eval config = RunEvalConfig(
          evaluators=[
              "cot_qa"
          ٦,
          custom_evaluators=[],
          eval_llm=ChatOpenAI(model="gpt-3.5-turbo-0125", temper
      )
      client = langsmith.Client()
      chain_results = client.run_on_dataset(
          dataset name=dataset name,
          llm_or_chain_factory=self.agent,
          evaluation=eval_config,
          project_name=project_name,
          concurrency_level=5,
          verbose=True,
```

) return chain_results

Con gpt-3.5-turbo-0125, evalue si la respuesta generada estaba bien o mal.



Link de la prueba: https://smith.langchain.com/public/4cf46e18-3b0e-4a46-8ef6-601413d9af80/d

Deployment

- Langserve:
- UI → Langserve Playground: Se ingresa el ID para la conversacion que quieren almacenar y el input.



• Cloud provider → Replit

Uno de los problemas que tuve al principio fue la integracion del agente que cree a la app de langserve, para que las dependencias no tuvieran conflicto. Pasando un momento de respiro me puse a leer la documentacion y langserve pudo correr perfectamente. Tambien el otro fue al querer hacer el deploy con AWS, intente

realizar la configuracion y obtuve unos errores, pero me puse a buscar y vi que se podia usar LangServe en Replit (Es donde normalmente hago el deploy de mis aplicaciones), y el despliegue fue muy rapido.