Desafío Abierto de Agente de IA: Asistente para Incubadoras

Por Santiago Panozzo, Milagros Kucharski, Cristian Rodriguez y Francisco Nasso

Fecha de entrega: Viernes 8 de Agosto de 2025

Universidad Católica del Uruguay

Índice

Introducción

Contexto del proyecto

El centro Ithaka es el Centro de Emprendimientos e Innovación de la Universidad Católica del Uruguay. Su objetivo es la generación de iniciativas que promueven la generación de una cultura de innovación y emprendimiento en la comunidad universitaria comprendida dentro de la UCU. (UCU, 2025)

Como parte de su programa de emprendimientos, el centro recibe decenas de propuestas de miembros de la comunidad universitaria sobre posibles emprendimientos que desean desarrollar con ayuda del centro.

Muchos de los postulantes, sin embargo, no disponen de las herramientas o la información necesaria para llevar a cabo la postulación de manera correcta y efectiva. Los procesos, criterios de aprobación, y otros factores que influencian las postulaciones, son puntos de fricción a la hora de realizar las postulaciones.

Es por esto por lo que se propuso llevar a cabo un proyecto de desarrollo de un agente conversacional con inteligencia artificial para brindar apoyo a los postulantes. Fundamentalmente, se busca mejorar así la experiencia del postulante resolviendo sus dudas y aportando información relevante para complementar sus postulaciones.

Contexto del equipo

El equipo fue compuesto por cuatro alumnos de la carrera de Ingeniería en Informática de la Universidad Católica del Uruguay. Cada miembro del equipo tiene experiencia real en distintos ámbitos del desarrollo de software, las ciencias computacionales y la gestión de proyectos. Esto se vio reflejado en las asignaciones de tareas y la organización general del proyecto.

Como parte de la preparación para el proyecto, se realizó una capacitación previa exhaustiva en el stack tecnológico de Google Cloud y sus servicios de inteligencia artificial con tecnologías como Gemini y Vertex AI.

Marco tecnológico

Dadas las habilidades adquiridas en la capacitación en Google Cloud, se decidió llevar a cabo el proyecto utilizando los servicios que ofrece el mismo.

En cuanto al desarrollo del agente, el proyecto se llevó a cabo en Python utilizando la librería de Pydantic AI para la conexión con Gemini, el modelo extenso de lenguaje (LLM) multimodal principal de Google.

Otros recursos tecnológicos utilizados de la suite de Google Cloud fueron: Cloud Storage para el almacenamiento de archivos, BigQuery para el almacenamiento estructurado de datos, y Vertex AI Studio para el diseño y experimentación de prompts.

Justificación del enfoque en inteligencia artificial

Se decidió utilizar inteligencia artificial en el proyecto debido a su capacidad de generar contenido en lenguaje natural que permite la fácil comunicación con los usuarios del centro Ithaka. Además de esto, el uso de estrategias de generación como RAG (retrieval-augmented generation) permiten brindar información verídica al usuario contrastada con documentos oficiales proporcionados por el centro.

El enfoque en la creación de agentes con inteligencia artificial permite también la automatización de flujos anteriormente llevados a cabo manualmente por trabajadores del centro. Por ejemplo, permite a los usuarios rellenar formularios estructurados a través de la carga de información desestructurada y solicitar automáticamente al usuario que proporcione cualquier dato faltante.

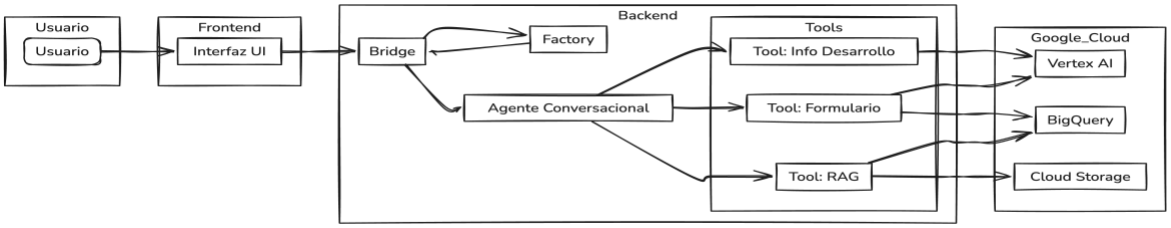
Esta comprensión avanzada facilita enormemente la comunicación con el usuario y la realización de tareas sin intervención humana de parte del centro Ithaka, ahorrando tiempo y recursos y brindando de igual forma una experiencia personalizada para el postulante.

Arquitectura de la solución

Componentes

El sistema presenta una arquitectura modular compuesta por los siguientes componentes principales:

- Agente Conversacional (Bot): la interfaz principal del sistema, encargada de recibir las consultas de los usuarios y generar respuestas usando modelos de lenguaje avanzado.
- Vector Store: almacena representaciones semánticas de documentos y datos, permitiendo una recuperación rápida y contextual de información relevante para el usuario.
- Scrapers: módulos encargados de extraer información actualizada desde las fuentes oficiales del centro Ithaka para alimentar el vector store y garantizar que los datos estén siempre vigentes.
- Servicios Google Cloud:
  - Vertex AI Studio: para la experimentación y diseño de prompts y modelos.
  - Cloud Storage: para almacenamiento de archivos.
  - BigQuery: para manejo estructurado de datos relacionados a los usuarios, conversaciones, mensajes y formularios.

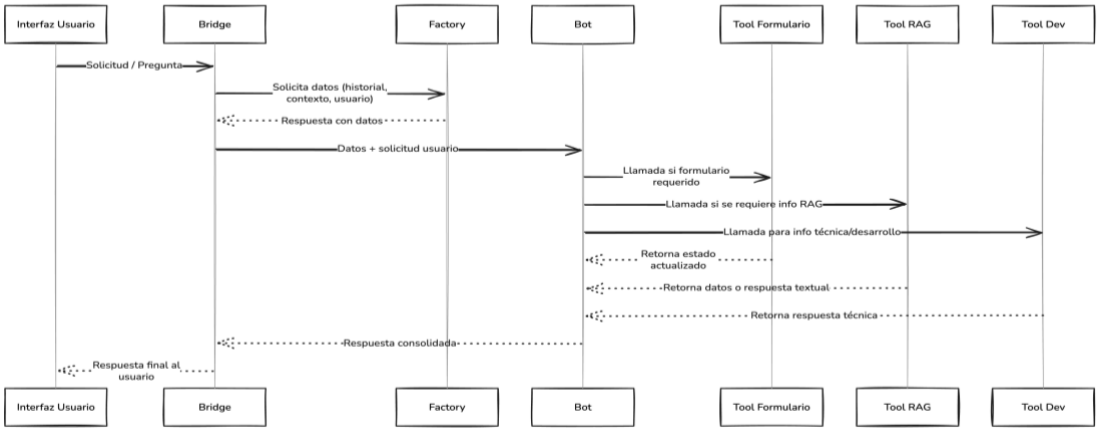


Flujo de datos y llamadas entre módulos

1. El usuario interactúa a través de la interfaz (UI), enviando preguntas o respuestas.
2. Estos datos pasan al módulo Bridge, que actúa de intermediario con el backend.
3. El Factory recibe la petición desde el Bridge y recopila datos relevantes: historial de conversación, contexto actual, entorno y datos específicos del usuario.
4. De vuelta al Bridge, estos datos enriquecidos se envían al bot conversacional.
5. El bot utiliza un enfoque no lineal; en lugar de un flujo secuencial rígido, dispone de varias "tools" o herramientas especializadas:
   - Tool de manejo de formularios: guía al usuario interno para concretar formularios necesarios para postulaciones.
   - Tool RAG: recupera información verídica de documentos almacenados en el vector store para fundamentar las respuestas.

- Tool para obtener información técnica o desarrolladores (Dev): para consultas que requieren datos específicos o internos.

6. Cada tool puede modificar el estado del bot y la conversación según la interacción, permitiendo adaptabilidad y flexibilidad en el diálogo.



Diseño de prompts

En cuanto al diseño de prompts, se utilizó la plataforma de Vertex AI Studio para una mejor experiencia de pruebas con diferentes parámetros. Dentro de esta, se puede configurar para una misma prompt de sistema diversas combinaciones de parámetros, permitiendo así encontrar la que de los mejores resultados.

La prompt de sistema se creó con la consideración de que el agente conversacional debía ser capaz de responder en un contexto multilenguaje, con restricciones a la hora de responder a consultas de temas no relacionados a la universidad o al centro.

Tras repetidas pruebas con distintos valores, se llegó a la siguiente prompt de sistema, la cual arrojaba los mejores resultados:

You are a multilingual chatbot that supports users at the Ithaka Center at the Catholic University of Uruguay. Your job is to provide relevant and accurate information to answer users' questions.

Today is {{ date }}. The user is a potential entrepreneur looking for information to help them develop their project proposal.

You can respond in text format in any language the user speaks, generate mermaid diagrams, and provide links to information that can help the user organize their thoughts and complement their proposal. Do not create invalid links or provide inaccurate information. Use

whatever means you deem best to illustrate your point to the user and improve their understanding.

Focus on the region or country of Uruguay unless the user specifies that the project is for another country. If the user asks a question unrelated to the Ithaka Center or a potential project, tell them you are not equipped to answer that type of question. Only answer questions related to Ithaka and the user's project.

Keep your response concise to keep the user's attention. You can suggest general ideas and wait for them to ask you in detail about a specific topic.

It is imperative that you respond only in the same language as the last message fragment you received from the user.

Módulos y alternativas consideradas

Base de agente conversacional

La base del sistema es un agente conversacional configurado para responder a las consultas básicas del usuario y ejecutar automáticamente las funcionalidades necesarias para completar las distintas posibles acciones que el mismo solicite.

Las consideraciones tomadas en cuenta para este agente son las especificadas en el diseño de prompts para la prompt de sistema que rige las conversaciones.

Respuestas por RAG

El módulo de respuestas por RAG es la funcionalidad que amplía las capacidades conversacionales del agente base, permitiendo la búsqueda de respuestas a las consultas de los usuarios en la documentación proporcionada por el centro Ithaka.

Permite además la incorporación de citas para aumentar la confianza del usuario en el contenido generado a partir de los documentos relevantes encontrados.

Se consideró también implementar una funcionalidad de recomendación de material basada en el módulo de RAG, pero su implementación no fue priorizada y se considera como una posible mejora o expansión de capacidades a futuro.

Funcionalidad de formularios

Una de las funcionalidades clave del agente es su capacidad para asistir a los usuarios en el llenado de formularios necesarios para completar su postulación al programa de emprendimientos. Esta funcionalidad fue diseñada con el objetivo de reducir la fricción que experimentaban los postulantes al enfrentarse con formularios complejos o poco claros.

El agente permite que el usuario proporcione información en lenguaje natural, incluso si esta está desestructurada o incompleta. Utilizando técnicas de comprensión de lenguaje natural y validación de datos, el agente interpreta la intención del usuario, extrae la información relevante y la organiza en los campos estructurados correspondientes. En los casos en que faltan datos necesarios o los datos ingresados no cumplen con los formatos requeridos, el agente interactúa proactivamente con el usuario para solicitar las correcciones o completar los campos pendientes.

La automatización de este proceso no solo mejora la experiencia del postulante, sino que también reduce significativamente la carga operativa sobre el equipo de soporte del centro Ithaka, permitiendo enfocar sus recursos en tareas de mayor valor estratégico.

Funcionalidades de audio

Otra de las funcionalidades implementadas en el agente conversacional es la capacidad de interactuar con los usuarios a través de mensajes de audio. Esta funcionalidad tiene como objetivo brindar una experiencia más accesible e inclusiva para los usuarios que prefieren o necesitan comunicarse mediante voz en lugar de texto.

Adicionalmente, se integró una funcionalidad de síntesis de voz (Text-to-Speech) para que las respuestas del agente puedan ser entregadas también en formato de audio. Esto permite que los usuarios escuchen las respuestas sin necesidad de leer, facilitando así la interacción en contextos donde la lectura no es práctica, como en movimiento o en situaciones que requieren accesibilidad visual.

Validaciones y Responsible AI

El proyecto pone especial énfasis en la confiabilidad, precisión y responsabilidad ética del agente conversacional, dado que atiende a usuarios que dependen de la información para realizar postulaciones importantes en el Centro Ithaka. Por ello, se implementaron diversos mecanismos y políticas que combinan controles técnicos y prácticas de diseño responsable para minimizar riesgos y potenciar una experiencia segura y adecuada.

Verificación de la información

Uso de fuentes oficiales: El agente se entrena y consulta sobre documentos oficiales, protocolos y manuales del Centro Ithaka que han sido previamente validados por

responsables del centro. Esto se asegura mediante scrapers que actualizan el vector store únicamente con información autorizada y vigente.

Retrieval-Augmented Generation (RAG): La arquitectura combina la generación de texto con la recuperación efectiva de documentos relevantes, garantizando que las respuestas estén fundamentadas y no sean meramente generativas sin respaldo.

Almacenamiento y consulta en BigQuery: Dado que los embeddings y datos se guardan en BigQuery, se aprovechan sus capacidades de control de acceso y auditoría para proteger la integridad de la información y evitar consultas no autorizadas o corruptas.

Filtrado y control de contexto

Restricción temática: El bot está configurado para responder únicamente a temas relacionados con el Centro Ithaka y los procesos de postulación. Cualquier consulta fuera del ámbito es manejada con mensajes que informan al usuario sobre la limitación, evitando así generar respuestas incorrectas o irrelevantes.

Validación de entradas de usuario: Se incorporaron validaciones para detectar preguntas ambiguas, imprecisas o fuera de contexto, solicitando aclaraciones al usuario en lugar de producir respuestas potencialmente erróneas.

Chequeo de coherencia y detección de incertidumbre: El sistema detecta cuándo la confianza en la respuesta es baja y, en esos casos, informa al usuario que no puede proveer una respuesta precisa, evitando improvisaciones y desinformación.

Medidas de mitigación de sesgos y contenido inapropiado

El modelo base utilizado para el agente conversacional incluye, por defecto, varias medidas de seguridad diseñadas para prevenir la generación de contenido violento, racista o discriminatorio. Estas opciones de seguridad forman parte de las configuraciones y protocolos de los modelos de lenguaje de Google Cloud, como Gemini y Vertex AI, y se activan automáticamente para mantener un comportamiento ético y responsable.

Durante la fase de pruebas en Vertex AI Studio, se verificó que el agente respetara estos parámetros de seguridad, realizando evaluaciones específicas para garantizar que no generara respuestas con sesgos o lenguaje ofensivo.

Estas medidas aseguran que el bot mantenga un trato respetuoso, inclusivo y seguro para todos los usuarios, alineado con los principios de Responsible AI.

Enfoque ético y privacidad

Transparencia: Cuando el bot no sabe o no puede responder con certeza, comunica al usuario la limitación y sugiere recurrir a soporte humano, promoviendo la confianza en el sistema.

Privacidad y protección de datos: Se respetan estrictamente normativas y buenas prácticas en el manejo de datos personales de los postulantes y usuarios, asegurando que la información sensible no sea divulgada ni usada incorrectamente.

Limitaciones del MVP

Dado que este proyecto se desarrolló como un MVP (Producto Mínimo Viable), no se implementaron mecanismos de retroalimentación humana ni procesos automáticos de actualización documental. Esto significa que el monitoreo, revisión y actualización continua del contenido quedan para etapas posteriores de desarrollo.

Pese a estas limitaciones, el diseño actual incorpora suficientes controles técnicos para garantizar una base sólida de funcionamiento confiable y ético.

Pruebas y Resultados

Se realizaron pruebas de las funcionalidades durante todo el desarrollo, lo cual incluyó pruebas unitarias para todo lo relacionado a carga de datos a BigQuery y Google Cloud Storage.

Además de esto, durante el diseño de las prompts utilizadas se realizaron también pruebas experimentales en Vertex AI Studio para asegurar que las respuestas del bot tuviesen consideración del idioma del usuario, fuesen concisas, y no tolerasen contenido violento, sexual o discriminatorio.

Finalmente, luego de integrar todas las partes del proyecto, se realizaron pruebas de integración y del funcionamiento de todas las funcionalidades comprendidas.

Conclusiones y Futuras Mejoras

A través de la integración de tecnologías avanzadas como Gemini, Vertex AI y otros servicios de Google Cloud, se logró diseñar en poco tiempo una solución robusta, accesible y adaptable a las necesidades reales de los usuarios.

El agente no solo ofrece respuestas contextuales y precisas mediante técnicas de recuperación aumentada (RAG), sino que también automatiza procesos clave como la asistencia en el llenado de formularios y la interpretación de mensajes de voz, ampliando así los canales de interacción con los postulantes. Esto permite reducir la

carga operativa sobre el personal del centro, optimizar recursos y ofrecer una atención personalizada a escala.

El proyecto demuestra cómo el uso estratégico de la inteligencia artificial puede transformar procesos institucionales, facilitando el acceso a la información y mejorando la eficiencia de las organizaciones. Además, sienta las bases para futuras expansiones funcionales del sistema, como la recomendación automatizada de recursos, el seguimiento inteligente del progreso del postulante o la integración con plataformas externas.

Algunas de las posibles mejoras a implementar en futuras etapas de desarrollo:

- **Incorporación de feedback humano:** Establecer un sistema donde el personal del centro pueda revisar y ajustar las respuestas del bot, mejorando la precisión y relevancia a partir de la experiencia real de uso.
- **Automatización y actualización documental dinámica:** Implementar mecanismos automáticos para que los scrapers actualicen de forma regular las fuentes oficiales y la base de conocimiento del bot, garantizando información vigente en todo momento.
- **Mayor personalización:** Integrar análisis del perfil y comportamiento del usuario para ofrecer respuestas más adaptadas a cada etapa del proceso de postulación y características individuales.
- **Integración de más fuentes de datos:** Conectar el bot a bases de datos internas adicionales o servicios complementarios del centro, para enriquecer las respuestas con datos técnicos, financieros o administrativos más completos, a modo de ayudar a los usuarios con sus postulaciones.
- **Análisis y monitoreo avanzado:** Diseñar paneles de control para monitorear métricas de uso, desempeño y satisfacción del usuario, permitiendo tomar decisiones informadas para actualizaciones y mejoras continuas.
- **Ampliación de funcionalidades:** Desarrollar nuevas tools que puedan asistir en tareas como la elaboración de propuestas, gestión de citas o seguimientos personalizados, aumentando la utilidad del agente para usuarios internos y externos.

Referencias

Google Cloud. (2025). *Google Cloud Skill Boost*. Obtenido de Beginner: Introduction to Generative AI Learning Path: https://www.cloudskillsboost.google/paths/118

Google Cloud. (2025). *Google Cloud Skill Boost*. Obtenido de Advanced: Generative AI for Developers Learning Path: https://www.cloudskillsboost.google/paths/183

Google Cloud. (2025). *Google Cloud Skill Boost*. Obtenido de Gemini for Google Cloud Learning Path: https://www.cloudskillsboost.google/paths/236

UCU. (2025). *Ithaka: Univeridad Católica del Uruguay*. Obtenido de Portal Web Universidad Católica del Uruguay: https://www.ucu.edu.uy/categoria/Ithaka-340