Propuesta Hitos curso Proyecto de Título I 2025-10

Nombre Alumno: Gianfranco Bobadilla.
Nombre Guía Externo: Claudio Álvarez.
Tema Memoria: Generación automática de reportes individuales en plataforma de gestión de factores humanos de ciberseguridad HFShield.

Hito 1: 03/10

Objetivo: Investigación sobre aspectos teóricos y modelado de procesos y datos

En síntesis, las tareas del primer hito son:

1. Revisión bibliográfica sobre factores humanos en ciberseguridad y ciberhigiene. Lectura de artículos científicos y técnicos aportados por el profesor guía y su correspondiente síntesis.
2. Realizar una investigación sobre enfoques arquitectónicos para utilizar LLMs con la finalidad de generar análisis cualitativos sobre la base de datos cuantitativos.
3. Construir una tabla comparativa de LLMs para la aplicación de generación de reportes individuales personalizados.
4. Proponer un modelo de proceso para la generación de reportes individuales personalizados.
5. Proponer un esquema de datos (definición y descripción de recursos) para efectos del servicio (API) que generará los reportes que son objetivo del presente trabajo.

El desarrollo del hito 2 será evaluado con base a un documento que debe contener: (i) Síntesis de conceptos sobre factores humanos y ciberhigiene en relación a lo visto en las lecturas, (ii) Investigación sobre enfoques arquitectónicos, (iii) Tabla comparativa de LLMs, (iv) Modelo de proceso, (5) Esquema de datos.

Hito 2: 31/10

Objetivo: Implementación de prototipo de sistema de reportes individuales personalizados

Las principales tareas del segundo hito son las siguientes:

1. Realizar un muestreo de casos para realizar prototipado de reportes, por ejemplo, utilizando *clustering*.
2. Desarrollar una primera versión de un conjunto de prompts alineados con el modelo de proceso de H1.4 que permita realizar análisis y generación de recomendaciones personalizadas a una muestra de casos seleccionados.
3. Implementar en forma prototípica una base de conocimiento de ciberhigiene que pueda ser accedida por un orquestador (p.ej., langgraph) para utilizar con un LLM. Implementar la orquestación para que esto sea funcional (RAG).

El desarrollo del hito 2 será evaluado con base a un repositorio Git que debe contener: (i) proyecto en R o Python con la selección de casos (output csv o xlsx), (ii) prompts en formato texto para análisis y generación de recomendaciones junto el código de prototipo utilizado para realizar los análisis (repositorio GitHub), (iii) demostración de una integración entre un LLM y una base de conocimiento sobre ciberhigiene (repositorio GitHub).

Claudio Álvarez Gómez
RUT 15.384.296-5
Guía Externo