LEVEL 3 · 심화 | AI 개발 · 도입 | 기업·단체 출강교육

우리 회사 전용 AI 챗봇 만들기 (RAG)

우리 데이터로 답하는 전용 챗봇

2일	16시간	8개	22개
교육 일수	총 교육 시간	단원 구성	실습 과제

1 과정 개요

규정·매뉴얼·FAQ 같은 우리 회사 문서로만 답하고 근거 문서를 함께 보여 주는 RAG 챗봇을 2일 동안 직접 만드는 실습 과정입니다. 1일차에는 문서 수집·정제부터 관리형 파일 검색으로 만든 기준 챗봇, n8n으로 청킹·임베딩·벡터 저장소를 직접 구성한 챗봇까지 두 가지를 만들어 비교합니다. 2일차에는 평가 질문 세트로 품질을 숫자로 재고 개선한 뒤, 열람 권한·프롬프트 인젝션·개인정보를 점검하고 사내 메신저나 웹 채팅으로 배포해 시연합니다. 코드를 작성하지 않는 노코드·로우코드 경로로 진행합니다.

교육 기간	2일 · 16시간
교육 수준	LEVEL 3 · 심화
교육 대상	실무·기획자
교육 형태	집체(출강) · 실습 중심(약 75%) · 1인 1노트북 · 참가자 조직 문서로 프로젝트
활용 도구	관리형 파일 검색 (OpenAI file search 등 — 벡터 저장소·인용 출처 자동 제공) n8n (데이터 로더·텍스트 분할기·임베딩·벡터 저장소·Chat Trigger) 벡터 저장소: Supabase(pgvector) 또는 실습용 Simple Vector Store 구글 시트 또는 엑셀 (평가 세트·결과 기록)
권장 인원	1인 1노트북 실습과 문서별 코칭이 가능한 소규모~중규모 운영 권장 (협의)

이런 분께 적합합니다

- 사내 규정·매뉴얼·FAQ를 묻고 답하는 일이 많은 부서의 실무자·기획자, 사내 AI 도입 담당자에게 맞춘 과정입니다.
- 프로그래밍은 필요 없습니다. 노코드 자동화 도구(n8n 등)를 한 번이라도 써 봤다면 2일차 실습이 한결 수월합니다.
- 외부 반출이 허용된 사내 문서 10~30개와 실제로 자주 받는 질문 목록을 준비해 오시면 그대로 챗봇과 평가 세트가 됩니다.

2 교육 목표

1. 문서 준비와 RAG 구축

- 수집→정제→청킹→임베딩→검색→답변 생성→출처 표시로 이어지는 RAG 전체 흐름을 각 단계의 결과물을 보며 이해합니다.
- 스캔 PDF·표·구버전 문서처럼 검색을 망치는 문서를 골라 정제하고, 문서명·부서·개정일·공개 범위 메타데이터를 붙입니다.
- 관리형 파일 검색과 n8n 직접 구축 두 가지 방식으로 챗봇을 만들어 조정 범위·운영 부담·데이터 보관 위치를 비교합니다.

2. 품질을 숫자로 관리

- 근거 문서·조항을 짝지은 평가 질문 세트를 만들어 검색 적중·근거 충실·거절 적절성을 기록합니다.
- 오답을 문서 부재·검색 실패·생성 오류·질문 모호로 나누고 청크 크기·메타데이터 필터·검색 개수·지시문을 조정해 전후를 비교합니다.
- 문서에 없는 질문에는 지어내지 않고 「확인되지 않습니다」와 담당 부서를 안내하도록 답변 규칙을 세웁니다.

3. 권한·보안·운영

- 공개 범위가 다른 문서를 검색 단계에서 거르는 방식(메타데이터 필터·행 수준 보안)을 설계하고 권한 없는 질문으로 시험합니다.
- OWASP LLM Top 10의 프롬프트 인젝션·민감정보 노출·벡터/임베딩 취약점을 기준으로 챗봇을 공격해 보고 대응합니다.
- 개정 문서 재색인·답변 불가 질문 로그·정기 재평가를 포함한 운영 계획을 세우고 사내에 배포합니다.

3 세부 시간표 (2일 · 16시간)

1일차	8시간
RAG 구조와 챗봇 범위 정하기 1시간	• RAG 흐름 한눈에 보기: 수집·정제·청킹·임베딩·검색·답변 생성·출처 표시, 일반 챗봇·긴 프롬프트·미세조정과의 차이 • 챗봇이 답할 것과 답하지 않을 것: 범위 밖 질문, 사람의 판단이 필요한 질문(인사·법무 결정 등) 구분 실습 우리 팀 챗봇의 사용자·사용 상황·예상 질문 20개 작성 — 2일차 평가 세트의 출발점 실습 답하면 안 되는 질문 5개와 그때의 안내 문구(담당 부서·연락 경로) 정하기

문서 수집·정제 2시간	• 검색을 망치는 문서 유형: 글자가 없는 스캔 PDF, 셀 병합 표, 머리글·바닥글 반복, 구버전·중복 문서 실습 준비한 문서 10~30개를 목록화 — 소유 부서·최신 개정일·공개 범위·폐기 여부 표시 실습 HWP는 PDF·DOCX로, 표는 행 단위 문장으로 풀고 개정 이력·폐기 조항을 정리한 텍스트/마크다운 정제본 만들기 실습 주민등록번호·연락처·개인 평가 등 개인정보와 기밀 포함 여부 점검 후 가림 처리 • 결과물: 정제 문서 묶음 + 문서 목록표(메타데이터 원본)
관리형 파일 검색으로 기준 챗봇 만들기 2시간	• 관리형 RAG의 구조: 파일 업로드 → 벡터 저장소 → 검색 → 답변에 인용 출처(파일명) 표시까지 서비스가 처리 실습 정제 문서를 벡터 저장소에 올리고 예상 질문 20개로 답변 받기 실습 인용된 파일이 실제 근거와 맞는지 ○/△/×로 채점해 기준선 기록 실습 답변 규칙 지시문 작성 — 근거 문서명 표기, 문서에 없으면 「확인되지 않습니다」 + 담당 부서 안내 • 관리형 방식에서 확인할 점: 세부 조정 범위, 데이터 보관·삭제 정책, 사내 반출 승인 절차
n8n으로 직접 구축: 청킹·임베딩·벡터 저장 3시간	• n8n RAG 구성: 데이터 로더 → 텍스트 분할기(Recursive Character 등) → 임베딩 모델 → 벡터 저장소(Insert Documents) • 청크 크기·겹침의 영향: 작은 청크는 정밀 검색, 큰 청크는 맥락 보존 — 저장과 질문에 같은 임베딩 모델 사용 실습 같은 문서를 청크 크기 2~3가지로 저장하고 동일 질문의 검색 결과(유사도 점수 포함)를 비교 실습 문서 목록표의 문서명·부서·개정일·공개 범위를 청크 메타데이터로 넣기 실습 Chat Trigger + AI Agent + 벡터 저장소 도구(Retrieve as Tool)로 질의응답 챗봇 연결, 검색 결과 개수 조정 • 결과물: 관리형·직접 구축 챗봇 2개를 같은 질문 20개로 비교한 결과표

2일차 — 8시간

평가 세트로 품질 측정하기 2시간	• 평가 기준 4가지: 검색 적중(맞는 조각을 가져왔나), 근거 충실(문서에 없는 말을 했나), 답변 유용성, 거절의 적절성 실습 1일차 질문을 근거 문서·조항과 짝지은 평가 세트 30개로 확장 — 범위 밖 질문·함정 질문·비슷한 조항 혼동 질문 포함 실습 시트 또는 n8n 평가 기능으로 평가 세트를 일괄 실행하고 기준 점수 기록 실습 틀린 답을 문서 부재·검색 실패·생성 오류·질문 모호 4가지 원인으로 분류

검색·답변 품질 개선 2시간	• 개선 수단 고르기: 문서 정제 보강, 청크 크기·겹침 조정, 메타데이터 필터, 검색 결과 개수, 답변 지시문 실습 오답 상위 원인 2가지를 골라 개선하고 같은 평가 세트로 다시 실행해 전후 비교 — 다른 질문이 나빠지지 않았는지 확인 실습 출처 표시 강화 — 답변 끝에 문서명·개정일·조항 표기, 원문 위치 안내 실습 후속 질문(「그럼 계약직은?」)을 위해 대화 메모리를 켜고 끈 결과 비교 • 결과물: 개선 전후 점수표와 변경 기록
권한·보안·개인정보 점검 2시간	• OWASP LLM Top 10 중 RAG에 직접 해당하는 위험: 프롬프트 인젝션(LLM01), 민감정보 노출(LLM02), 벡터·임베딩 취약점(LLM08), 잘못된 정보(LLM09) • 열람 권한을 검색 단계에서 거르기: 메타데이터 필터, Supabase pgvector + 행 수준 보안(RLS)으로 사용자별 문서 제한하는 구조 실습 공개 범위가 다른 문서 2종을 넣고 권한 없는 사용자 질문에 기밀 내용이 섞여 나오지 않는지 시험 실습 문서에 숨긴 지시문(간접 프롬프트 인젝션)과 지시문 유출 요청으로 공격해 보고 방어 지시문·문서 등록 검토 절차 마련 • 개인정보보호위원회 「생성형 AI 개발·활용을 위한 개인정보 처리 안내서」를 바탕으로 한 도입 전 점검표 작성
종합 프로젝트: 우리 조직 챗봇 배포·시연·피드백 2시간	실습 참가자 조직 문서로 최종 챗봇 완성 — n8n 공개 채팅(접근 인증 설정) 또는 사내 메신저 연결로 배포 실습 문서 갱신 절차 정하기 — 개정 문서 재색인, 구버전 삭제, 담당자·주기 지정 실습 운영 지표 설계 — 답변 불가 질문 기록, 사용자 피드백 버튼, 월 1회 평가 세트 재실행 • 시연·피드백: 평가 점수 전후와 함께 시연하고 강사·동료 피드백으로 사내 적용 전 보완 목록 확정

4 교육 후 손에 남는 산출물

- ✓ **우리 조직 문서로 답하고 근거 문서를 표시하는 RAG 챗봇 1개(배포본)**
- ✓ **정제 문서 묶음과 메타데이터 문서 목록표**
- ✓ **평가 질문 세트 30개와 개선 전후 점수표**
- ✓ **권한·보안·개인정보 점검표와 문서 갱신·운영 계획**

5 수료 후 이렇게 달라집니다

항목	수강 전	수강 후
정보 찾기	폴더·게시판을 뒤지거나 담당자에게 문의	챗봇에 물으면 답과 근거 문서를 함께 확인
답변 신뢰	일반 챗봇은 근거 없이 그럴듯하게 답함	문서에 없으면 「확인되지 않습니다」로 답하고 출처 표시
품질 관리	써 보고 느낌으로 판단	평가 세트 점수로 개선 전후 비교
권한	문서를 올리면 누구나 볼 위험	공개 범위에 따라 검색 단계에서 제한

6 운영 안내

참가자 준비사항

- 노트북 지참 (필수)
- LLM API 계정·n8n 계정 (사전 안내에 따라 생성, 기관 정책상 사용 가능한 서비스 사전 확인)
- 외부 반출이 승인된 사내 문서 10~30개 (규정·매뉴얼·FAQ, 개인정보 가린 사본)
- 실제로 자주 받는 질문 20개 내외 목록

교육장 요건

- 프로젝터 또는 대형 스크린
- 고속 인터넷(Wi-Fi) — 외부 AI API 접속이 사내 방화벽에서 허용되는지 사전 확인
- 1인 1노트북 사용 가능한 좌석과 전원

맞춤 구성 옵션

- 주 1일씩 나눠 2회 운영 (사이 기간에 문서 정제·평가 세트 보강 과제)
- 사내 시스템·문서로 실습 (보안 승인 범위 내, 사전 협의)
- 보안 등급별 열람 권한 설계 심화 (사내 인증 체계 연동 범위 협의)
- 사후 1회 기술 점검 세션 — 배포 후 평가 세트 재측정·개선 (협의)

문서를 외부 AI 서비스에 올려도 되는지 사내 보안·개인정보 담당 부서의 확인을 먼저 받아 주세요. 승인이 어려우면 공개 가능한 문서나 가상 문서로 실습하고, 사내 구축 방식은 별도 협의합니다.

nuguna

기업·단체 출강교육 문의

전화 010-6395-3043 · 카카오톡 @nuguna · nugunapass@gmail.com
www.nugunapass.com/onsite — 인원·대상·희망 일정을 알려 주시면 맞춤 커리큘럼과 견적을 제안드립니다.