IACADEMY

ENTERPRISE AGENT ENGINEERING

MÓDULO 04

Diseño de Agentes por Dominio

Principal

iacedemy.com — 2026

MÓDULO 04

Diseño de Agentes por Dominio

Nivel: Principal / Arquitecto

Autor: Alicia Sanz

Publicación: Julio 2026

Plataforma: iacedemy.com

Este material es parte del track Enterprise Agent Engineering de IAcademy.
Uso personal e intransferible.

> “No diseñas un agente genérico. Diseñas un especialista con rol, tools, memoria, políticas y KPIs.”

3.1 Anatomía de un Agente Enterprise

```yaml
agent:
  id: AGENT-{DOMAIN}-{NUM}
  version: "1.0"
  domain: soc | grc | sales | ops | training

identity:
  objective: "Qué debe lograr"
  role: "Quién es"
  tone: "Cómo comunica"

capabilities:
  tools: []        # Con risk_level, timeout, requires_hitl
  knowledge: []    # Fuentes de conocimiento (RAG, DB, API)
  memory:
    short_term: "context_window"
    long_term: "qdrant | postgresql"

policies:
  max_cost_per_execution: 0.50
  max_tool_calls: 10
  escalation_threshold: 0.7
  data_classification: "confidential"
  allowed_models: ["qwen3.5-27b"]

kpis:
  task_completion_rate: ">= 0.85"
  avg_latency_seconds: "< 5"
  cost_per_task_eur: "< 0.10"
  user_satisfaction: ">= 4.0"
```

3.2 Agentes SOC

Threat Hunter

```yaml
agent:
  id: AGENT-SOC-HUNTER-001
  objective: "Detectar amenazas avanzadas mediante hipótesis y búsqueda
proactiva"
  tools:
    - query_siem(query, timeframe) # risk: low
    - search_threat_intel(ioc) # risk: low
    - isolate_endpoint(hostname) # risk: critical, hitl: true
  knowledge: [mitre_attack, sigma_rules, yara_rules]
  kpis:
    true_positive_rate: ">= 0.80"
    hunt_hypotheses_per_week: ">= 5"
```

Incident Responder

```yaml
agent:
  id: AGENT-SOC-IR-001
  objective: "Contener y remediar incidentes de seguridad"
  tools:
    - get_alert_details(alert_id)
    - block_ip(ip, duration) # risk: high, hitl: true
    - disable_account(user_id) # risk: critical, hitl: true
    - create_incident_report(data)
  policies:
    escalation: "Siempre escalar si afecta >10 usuarios"
    max_containment_time: "30 minutos"
```

SIEM Analyst

```yaml
agent:
  id: AGENT-SOC-SIEM-001
  objective: "Triagear alertas del SIEM, reducir falsos positivos"
  tools:
    - query_siem(query, timeframe)
    - correlate_events(alert_id)
    - classify_alert(alert_id, severity)
    - auto_close_alert(alert_id, reason) # risk: medium
  kpis:
    false_positive_reduction: ">= 60%"
    avg_triage_time: "< 2 minutos"
```

3.3 Agentes GRC

Compliance Agent

```yaml
agent:
  id: AGENT-GRC-COMPLIANCE-001
  objective: "Evaluar cumplimiento y generar evidencias automáticamente"
  tools:
    - scan_controls(framework, scope)
    - generate_evidence(control_id)
    - create_finding(control_id, gap, recommendation)
    - export_report(format) # PDF, Excel
  knowledge: [ens_alto, iso_27001, nis2, ai_act, rgpd]
  kpis:
    controls_evaluated_per_day: ">= 50"
    evidence_accuracy: ">= 95%"
```

Risk Agent

```yaml
agent:
  id: AGENT-GRC-RISK-001
  objective: "Evaluar riesgos, calcular impacto y probabilidad"
  tools:
    - assess_risk(asset, threat, vulnerability)
    - calculate_risk_score(impact, probability)
    - suggest_mitigation(risk_id)
    - update_risk_register(risk_id, data)
```

3.4 Agentes Comerciales

SDR Agent

```yaml
agent:
  id: AGENT-SALES-SDR-001
  objective: "Cualificar leads y agendar reuniones"
  tools:
    - search_leads(criteria)
    - enrich_lead(company, domain)
    - score_lead(lead_id)
    - send_email(to, subject, body) # risk: high, hitl: true
    - schedule_meeting(lead_id, datetime)
  kpis:
    leads_qualified_per_day: ">= 20"
    meeting_conversion_rate: ">= 15%"
```

CRM Agent

```yaml
agent:
  id: AGENT-SALES-CRM-001
  objective: "Mantener CRM actualizado y generar insights de pipeline"
  tools:
    - update_deal(deal_id, fields)
    - get_pipeline_stats(period)
    - predict_close_probability(deal_id)
    - generate_forecast(quarter)
```

3.5 Agentes de Operaciones

Invoice Processing Agent

```yaml
agent:
  id: AGENT-OPS-INVOICE-001
  objective: "Procesar facturas: extraer datos, validar, aprobar o
escalar"
  tools:
    - extract_invoice_data(pdf_path)
    - validate_invoice(data, purchase_order)
    - approve_invoice(invoice_id) # risk: high, hitl: amount > 5000
    - flag_for_review(invoice_id, reason)
  kpis:
    processing_accuracy: ">= 98%"
    avg_processing_time: "< 30 segundos"
    auto_approval_rate: ">= 70%"
```

3.6 Agentes de Formación

Tutor Agent

```yaml
agent:
  id: AGENT-TRAIN-TUTOR-001
  objective: "Responder dudas del alumno adaptándose a su nivel"
  tools:
    - search_course_content(query, module_id)
    - get_student_progress(student_id)
    - suggest_next_topic(student_id)
    - create_practice_exercise(topic, difficulty)
  memory:
    long_term: "historial de preguntas y nivel por alumno"
  kpis:
    answer_accuracy: ">= 90%"
    student_satisfaction: ">= 4.2"
```

3.7 Ejercicios

Ejercicio 1: Spec por Dominio

Elige un dominio (SOC/GRC/Sales/Ops/Training). Escribe la System Spec completa para un agente: identity, 4+ tools con risk_level, 3+ behaviors, guardrails y KPIs.

Ejercicio 2: Multi-Agent por Dominio

Diseña un sistema de 3 agentes para un SOC: Detector + Investigador + Responder. Define la comunicación entre ellos (message passing o scratchpad).

Ejercicio 3: KPIs y Métricas

Define 5 KPIs para un agente GRC de compliance. Para cada KPI: métrica, threshold, cómo se mide, cada cuánto, y qué pasa si no se cumple.

Ejercicio 4: Cross-Domain

Diseña un agente que coordine entre dominios: un incidente de seguridad (SOC) que requiere notificación a clientes (Sales) y documentación de compliance (GRC). ¿Cómo se orquestan?

Módulo 3 v1.0 . Enterprise Agent Engineering . IAcademy 2026