

| CÓDIGO   | AUTOR                | DURACIÓN ESTIMADA | NIVEL DE FORMACIÓN |
|----------|----------------------|-------------------|--------------------|
| 01B06C05 | Carlos Ojeda Sánchez | 25 h              | Avanzado           |

**Dirigido a**

*Profesionales con conocimientos básicos sobre agentes de IA y perfiles técnicos, de automatización o transformación digital que quieran conectarlos con herramientas y servicios externos.*

**Descripción**

*Con este contenido de curso profesional el alumnado aprenderá a configurar agentes conectados capaces de utilizar herramientas, servicios y fuentes de información. Se priorizarán MCP, la selección de capacidades y permisos, la orquestación de tareas y la gestión de la memoria y del contexto. La parte práctica se centrará en configurar y probar un agente con herramientas reales en una tarea profesional delimitada.*

**COMPETENCIAS**

1. Interpretar MCP como estándar de conexión entre agentes y herramientas para valorar su papel en arquitecturas interoperables.
2. Configurar capacidades de un agente seleccionando herramientas, permisos y servicios externos para ejecutar tareas con control operativo.
3. Diseñar mecanismos de orquestación y memoria en agentes para coordinar tareas, conservar contexto y controlar decisiones sucesivas.

**CRITERIOS DE EVALUACIÓN (Objetivos)**

1. Explicar el problema de interoperabilidad que aborda MCP y relacionarlo con la conexión entre agentes y herramientas. Describir la arquitectura cliente-servidor de MCP identificando funciones, responsabilidades y flujo básico de intercambio. Diferenciar recursos, herramientas y prompts dentro de MCP mediante ejemplos aplicables a entornos profesionales. Valorar beneficios y límites de MCP para diseñar agentes conectados con mayor seguridad, trazabilidad y reutilización.
2. Aplicar el principio de mínimo privilegio al seleccionar permisos y herramientas disponibles para un agente. Categorizar herramientas según función, criticidad, datos tratados y nivel de riesgo asociado a su uso. Definir criterios de autorización, registro y supervisión para reducir errores, accesos innecesarios o acciones no deseadas. Justificar la selección de herramientas relacionándola con el objetivo del agente, el contexto y los controles requeridos.
3. Diferenciar patrones de orquestación secuencial, condicional e iterativa, indicando cuándo resulta adecuado cada uno. Explicar el ciclo de planificación, ejecución, observación y replanteamiento en agentes con tareas de varios pasos. Diseñar una estrategia de memoria distinguiendo contexto inmediato, historial útil, datos persistentes y límites de conservación. Identificar riesgos asociados a memoria y orquestación y proponer controles para evitar errores acumulativos o pérdida de contexto.

**CONTENIDOS****Unidad 1. Model Context Protocol (MCP)**

1. El problema que resuelve MCP: USB para agentes
2. Arquitectura: cliente, servidor, JSON-RPC
3. Ciclo: descubrimiento → invocación → respuesta
4. 4 tipos de capacidades: Tools, Resources, Prompts, Sampling
5. Servidores disponibles; anatomía de un servidor; MCP en la práctica (Claude Desktop); walkthrough guiado

**Unidad 2. Herramientas y capacidades del agente**

1. Principio de mínimo privilegio
2. 5 categorías: comunicación, datos, búsqueda, ejecución, especializada
3. Permisos por herramienta; documentar el toolbox
4. Config práctica: agente con email + calendario + búsqueda
5. Gestión de credenciales y secretos; testing antes de producción

**Unidad 3. Orquestación y memoria**

1. Orquestación: coordinar pasos y herramientas; patrones (secuencial, condicional, paralelo, iterativo)
2. El loop agéntico; planificación (ReAct, CoT agéntico)
3. Memoria de trabajo / corto plazo / largo plazo
4. RAG y bases vectoriales [intro desde cero]
5. Gestión de contexto; estado y persistencia

***Unidad Práctica. Configurar agente con herramientas reales***