<DAPROMPTED Series>

TECH TRENDS BY DACODES

GUÍA PASO A PASO

Evaluación técnica para migrar a MCP

Decide con evidencia si conviene migrar (total o parcial) a Model Context Protocol (MCP), qué alcance, costos, riesgos y un plan de siguiente paso.

PASO 1

Definir Alcance y Éxito

- **Casos de uso candidatos**
  (ej.: soporte, analítica, coding asistido, RAG).

- **KPI de éxito:**
  tiempo de integración, MTTR, % automatización, costo por integración, NPS interno.

- **Criterios de "go/no-go"** para pilotear: p.ej., reducción ≥40–60% del esfuerzo de integración, time-to-market en semanas, no meses.

Entregable
one-pager con objetivos, KPI y criterios de decisión

PASO 2

Inventario de Sistemas y Conectores

- Mapear fuentes de datos, herramientas y APIs críticas.
- Marcar **sensibles** (PII, PHI, financieros) y requisitos de compliance.

- Cruzar con el **ecosistema MCP:** servidores existentes para GitHub, Slack, GoogleDrive, Postgres, etc. y clientes compatibles.

Entregable
matriz sistemas ↔ conector MCP disponible; etiquetas de sensibilidad y dueños.

PASO 3

Arquitectura de Referencia (As-Is vs To-Be)

- **Pre-MCP:**
  integraciones punto a punto, frágiles, difícil de escalar y monitorear.

- **KPI de éxito:**
  estándar único (“USB-C para IA”), desacoplado, orquestación centralizada y contexto continuo entre herramientas.

- Definir patrón de **cliente MCP** (Claude Desktop/Apps, VS Code, ChatGPT, etc.) y servidores MCP a usar.

Entregable
diagrama lógico con flujos de datos, clientes/servidores MCP y límites de seguridad.

PASO 4

Seguridad, Autenticación y Cumplimiento

- Elegir transporte (SSE/HTTP streamable) y validar OAuth/OIDC para servidores remotos.

- Definir **scopes mínimos**, rotación de tokens, vault, y segregación por entorno

- Alinear con políticas de **data residency** y retención de contexto

Entregable
matriz de controles (auth, cifrado, logging), checklist de cumplimiento.

PASO 5

Selección de Piloto (30–60 días)

- Priorizar **1–2 flujos** con alto ROI (p.ej., conectar repos/Drive/Slack a un asistente para búsqueda contextual y ejecución de tareas).

- **Métricas del piloto:**
  - Tiempo de integración (objetivo: días, no meses).
  - Reducción de costos/desarrollo (objetivo: hasta 60%).
  - Trazabilidad y monitoreo centralizado.
  - Mejora de interoperabilidad/contexto entre herramientas.

Entregable
backlog del piloto, KPIs base y metas, plan de pruebas.

PASO 6

Implementación Técnica de Prueba

- **Conectar clientes** a servidores MCP y descubrir herramientas/recursos disponibles.

- Si usás **Claude vía API**, habilitar **MCP connector** con `mcp_servers`, tokens OAuth y lista de herramientas permitidas.

- Limitar herramientas por “allow-list”; configurar logs de **mcp_tool_use / mcp_tool_result** para auditoría.

Entregable
repo del piloto, config reproducible (infra-as-code), dashboard de logs.

PASO 6

Observabilidad y Gobierno

- Centralizar **telemetría:**
  éxito/fallo por herramienta, latencias, tasas de uso.

- Runbooks de incidentes y **SLOs** (disponibilidad de servidores MCP, errores de autorización, vencimiento de tokens).

- Catálogo de **prompts/recursos** versionados como parte del contexto compartido.

Entregable
panel de monitoreo y runbooks operativos.

PASO 7

Evaluación de Riesgos

- **Técnicos:** dependencia de servidores públicos vs internos, límites actuales (p.ej., solo tool calls en conector API).

- **Operativos:** cambios en APIs de origen, ownership difuso de conectores.

- **Seguridad:** fuga de contexto, permisos excesivos.

Entregable
registro de riesgos con mitigaciones y responsables

PASO 9

Análisis de Costo–Beneficio

- Baseline vs MCP: menos código personalizado, reutilización, escalado eficiente.
- Cuantificar ahorro por **tiempo de integración y menor dependencia de especialistas**.
- Valor estratégico: **time-to-market** acelerado y diferenciación funcional.

Entregable
planilla TCO/ROI con supuestos y sensibilidad.

PASO 10

Decisión y Roadmap

- **Go/Iterar/No-Go** según KPI y criterios iniciales
- Si es **Go:**
  - Endurecer seguridad (tokens, secrets), endurecer SLAs.
  - Ampliar cobertura de servidores (GitHub/Slack/Drive/DBs) y clientes compatibles.
  - Escalar a 3–5 casos de uso y formalizar centro de excelencia MCP.

Entregable
registro de riesgos con mitigaciones y responsables

Checklist rápido de “listos para pilotear”

- [ ] Casos de uso + KPI definidos
- [ ] Inventario de sistemas mapeado a servidores MCP
- [ ] Diagrama To-Be con límites de seguridad
- [ ] OAuth/token y logging configurados
- [ ] Métricas y panel de observabilidad activados
- [ ] Runbooks de incidentes publicados
- [ ] Matriz de riesgos con mitigaciones
- [ ] Plan de pruebas y rollback

Recursos de base (para tu equipo)

- Qué es MCP y ecosistema de clientes/servidores
- Anuncio y objetivos del estándar (open, dos-vías, contexto)
- Beneficios empresariales/ROI, time-to-market y escalabilidad
- Antes vs ahora: integración rígida vs desacoplada/robusta
- Conector MCP vía API (config, OAuth, tool calls)
- Enfoque de contexto compartido e interoperabilidad en flujos multi-agente