CHOUCAIR
Business Centric Testing

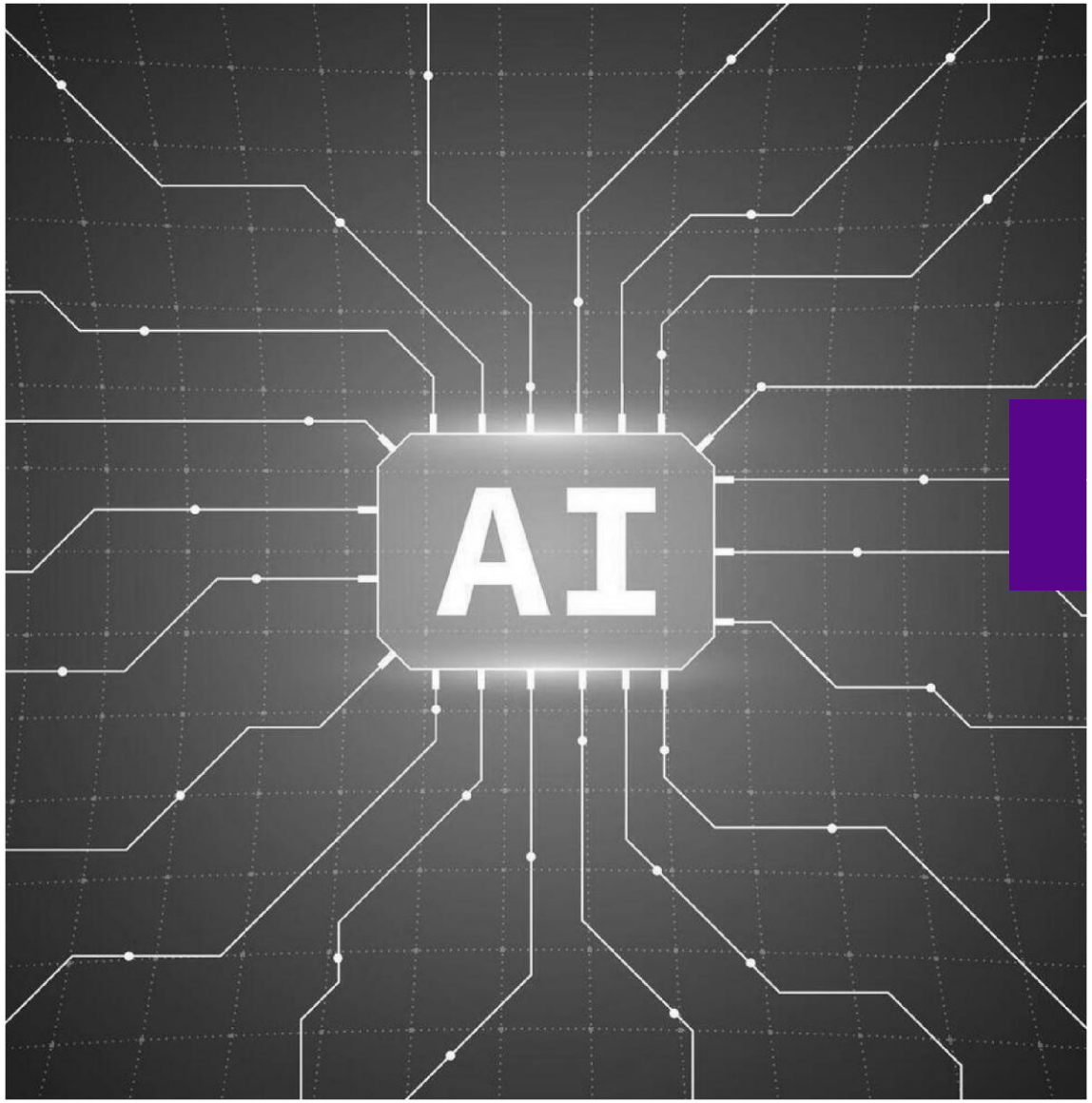
INTELIGENCIA ARTIFICIAL GENERATIVA

AUTOMATIZACIÓN INTELIGENTE

# Introducción a LLM

## + Model Context Protocol

Cómo se integran para crear agentes inteligentes y herramientas automatizadas



CHOUCAIR
Business Centric Testing

# Agenda del Día

01 ¿Qué es un LLM?

02 Capacidades clave de los LLM

03 Limitaciones de los LLM sin herramientas

04 ¿Qué es MCP?

05 Componentes de MCP

06 ¿Cómo funciona MCP?

07 Ejemplos de Servidores MCP

08 ¿Cómo trabajan juntos LLM + MCP?

09 Caso práctico

10 Beneficios de combinar LLM + MCP

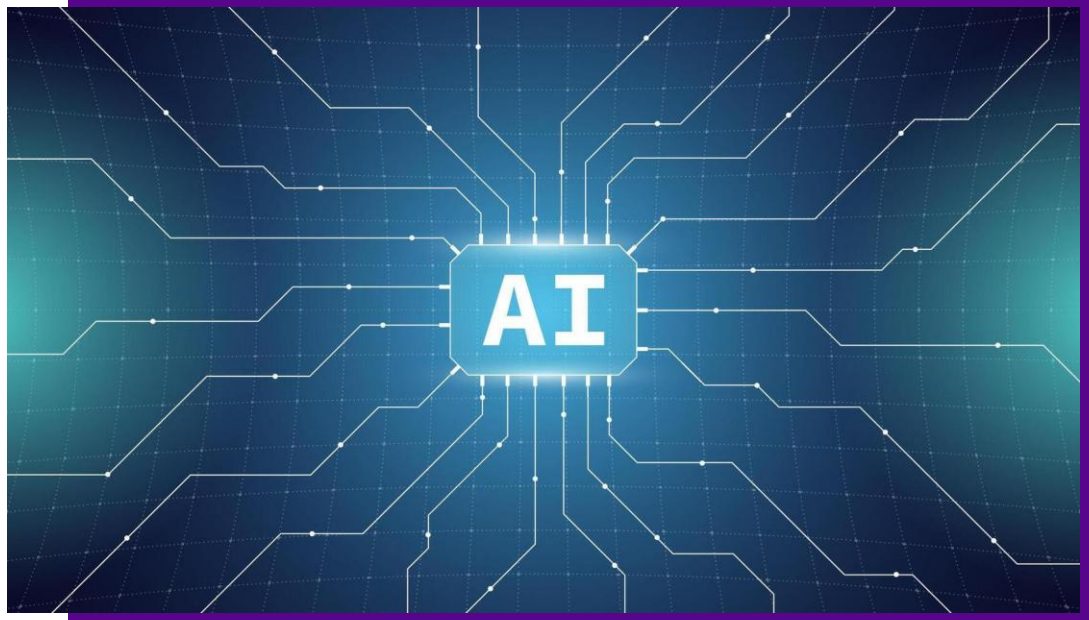
11 Riesgos y buenas prácticas

12 Casos de uso ideales

13 Conclusión y próximos pasos

# ¿Qué es un LLM?

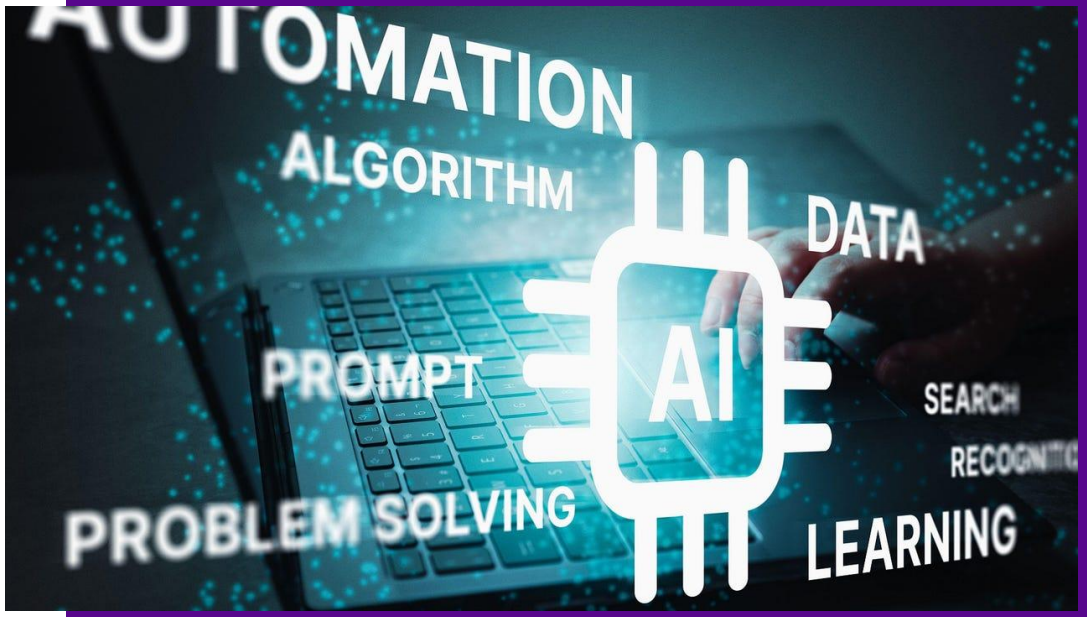
- Definición: Large Language Model (Modelo de Lenguaje Grande) - sistemas de IA entrenados con enormes cantidades de texto
- Propósito: Comprender, generar y razonar con lenguaje natural de forma similar a los humanos
- Ejemplos actuales: GPT-4, Claude, Gemini, LLaMA, Mistral
- Capacidades de razonamiento: Análisis de contexto, inferencia lógica, resolución de problemas complejos y toma de decisiones informadas
- Arquitectura: Basados en redes neuronales profundas con miles de millones de parámetros



CHOUCAIR
Business Centric Testing

# Capacidades Clave de los LLM

- Comprensión del lenguaje natural: Interpretan y entienden texto en múltiples idiomas con contexto semántico completo
- Razonamiento: Capacidad de análisis lógico, deducción e inferencia para resolver problemas complejos
- Ejecución de herramientas: Pueden invocar y utilizar APIs, funciones y servicios externos de forma estructurada
- Generación de código: Escriben, depuran y explican código en múltiples lenguajes de programación
- Toma de decisiones basada en contexto: Evalúan situaciones y generan respuestas adaptadas al contexto específico



CHOUCAIR
Business Centric Testing

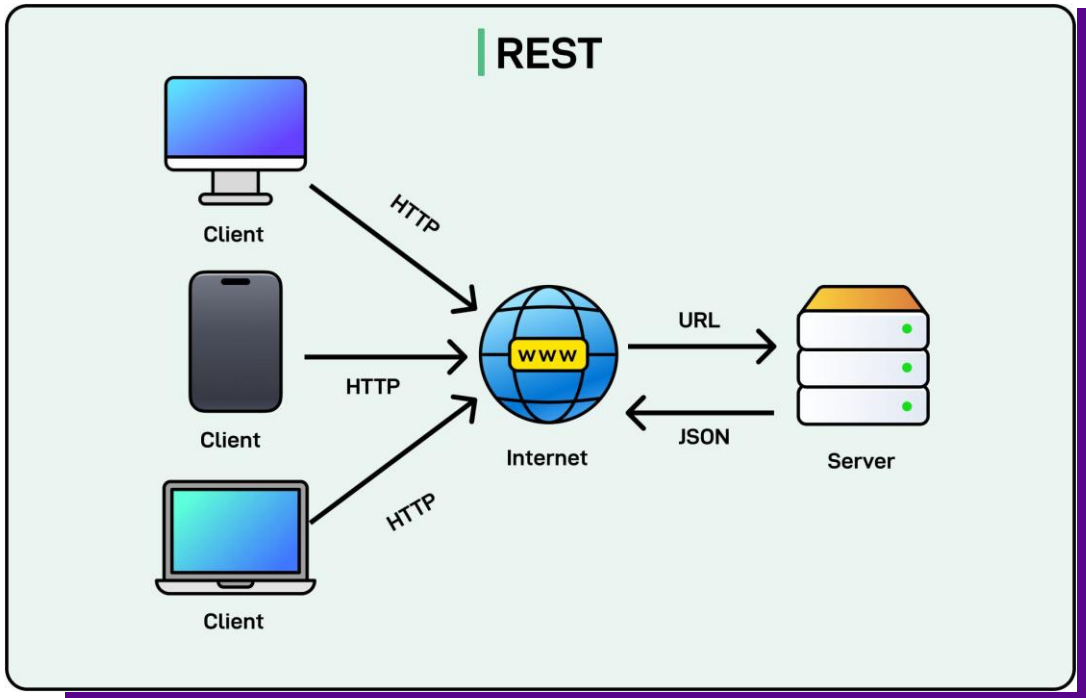
# Limitaciones de los LLM sin Herramientas

- Falta de estado persistente: No pueden recordar información entre sesiones ni mantener datos a largo plazo sin sistemas externos
- Alucinaciones: Pueden generar información incorrecta o inventada que parece convincente pero no es verificable
- Dependencia de contexto limitado: Tienen una ventana de contexto finita que restringe la cantidad de información que pueden procesar simultáneamente
- Incapacidad de ejecutar acciones reales por sí solos: Solo generan texto; no pueden interactuar directamente con sistemas, bases de datos o aplicaciones externas

CHOUCAIR
Business Centric Testing

# ¿Qué es MCP (Model Context Protocol)?

- Protocolo abierto: Estándar diseñado para conectar LLM con herramientas y servicios externos de forma universal
- Ejecución segura: Permite que los modelos ejecuten acciones reales de forma estructurada y controlada
- Independiente de proveedor: MCP no depende de ningún proveedor específico, garantizando interoperabilidad
- Puente inteligente: Actúa como intermediario entre la capacidad de razonamiento del LLM y sistemas externos



CHOUCAIR
Business Centric Testing

# Componentes de MCP

| Servidor MCP | Cliente MCP | LLM | Proveedores de Herramientas | Contextos Declarativos |
|---|---|---|---|---|
| Expone herramientas y recursos disponibles. Ejecuta acciones solicitadas por el cliente. Gestiona conexiones y permisos de forma segura. | Conecta el LLM con servidores MCP. Traduce peticiones del LLM a llamadas estructuradas. Devuelve resultados al modelo. | Cerebro del sistema. Decide qué herramientas usar. Interpreta resultados y genera respuestas contextuales. | Servicios externos conectados vía MCP: navegadores, bases de datos, APIs, sistemas de archivos, contenedores. | Definiciones de capacidades disponibles. Esquemas de entrada/salida. Permisos y restricciones de seguridad. |

CHOUCAIR
Business Centric Testing

# ¿Cómo funciona MCP? - Flujo Completo

1. El LLM recibe una petición del usuario
2. El LLM detecta que necesita una herramienta externa
3. El Cliente MCP genera una solicitud estructurada
4. El Servidor MCP ejecuta la acción en el sistema externo
5. El Servidor MCP devuelve datos limpios y estructurados
6. El LLM procesa los datos y produce una respuesta contextual

CHOUCAIR
Business Centric Testing

# Ejemplos de Servidores MCP

## Playwright MCP


Automatización web avanzada y testing de navegadores

## Selenium MCP


Control de navegadores y automatización de pruebas

## Podman MCP


Administración de contenedores y orquestación

## Filesystem MCP

Gestión de archivos y directorios del sistema

## Git MCP

Control de versiones y operaciones de repositorios

## Database MCP

Consultas y operaciones en bases de datos

# ¿Cómo trabajan juntos LLM + MCP?

## LLM como Agente Inteligente

El LLM se transforma en un agente capaz de:

- Tomar decisiones autónomas
- Ejecutar acciones complejas
- Interactuar con sistemas reales

## MCP como Puente Seguro

MCP actúa como intermediario que:

- Controla permisos y accesos
- Valida y estructura peticiones
- Garantiza ejecución segura

## Automatización en Lenguaje Natural

Permite automatizar tareas mediante:

- Instrucciones en lenguaje humano
- Ejecución de acciones reales
- Respuestas contextuales inteligentes

# Caso Práctico: Automatización con Playwright MCP

## 1. Prompt del Usuario

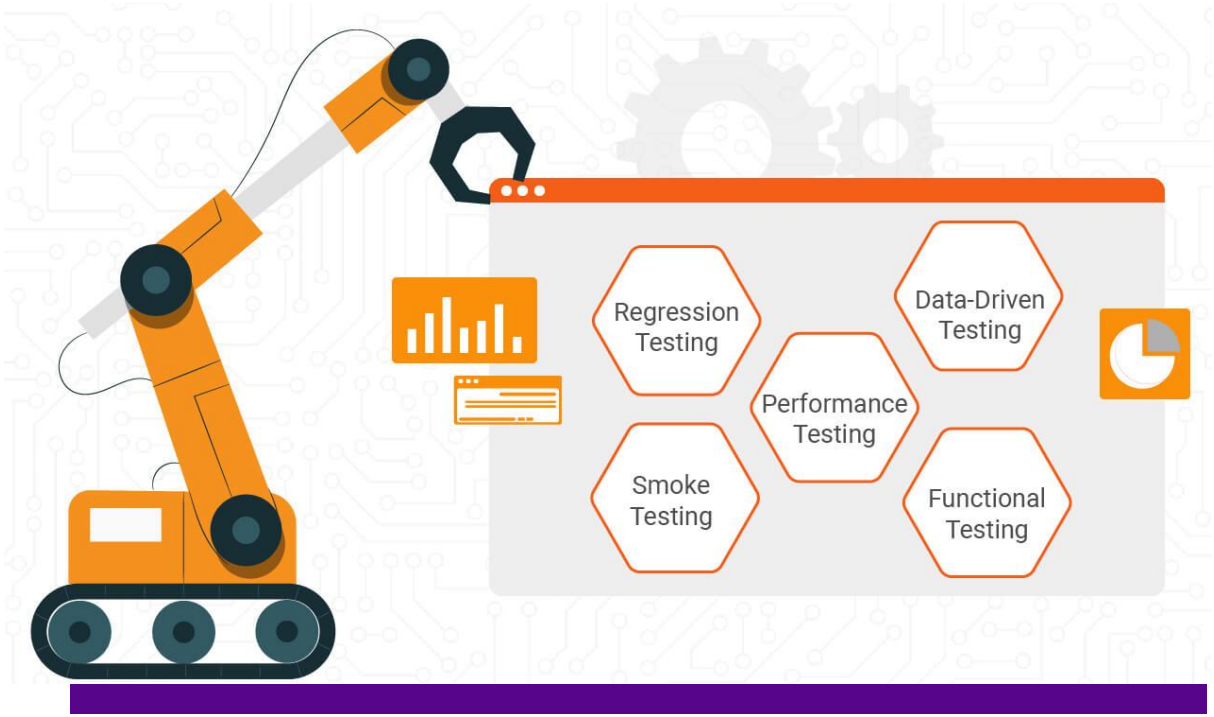
*"Inicia sesión en el portal con usuario: admin@empresa.com y contraseña: Pass123"*

## 2. Llamada MCP Generada

```
playwright.navigate("portal.com")
playwright.fill("#email", "admin@empresa.com")
playwright.fill("#password", "Pass123")
playwright.click("#login-button")
```

## 3. Resultado Devuelto

"Inicio de sesión exitoso. Usuario autenticado y redirigido al dashboard principal."



CHOUCAIR
Business Centric Testing

# Beneficios de combinar LLM + MCP

## Automatización Avanzada

Tareas complejas ejecutadas mediante lenguaje natural, sin necesidad de programación manual

## Ejecución de Acciones Reales

Los LLM pueden interactuar con sistemas externos y ejecutar operaciones concretas

## Seguridad Controlada

Permisos granulares y validación de acciones antes de su ejecución

## Escalabilidad

Arquitectura modular que crece según las necesidades del proyecto

## Modularidad

Componentes independientes que se integran fácilmente sin acoplamiento fuerte

## Reutilización de Herramientas

Servidores MCP compartibles entre múltiples proyectos y equipos

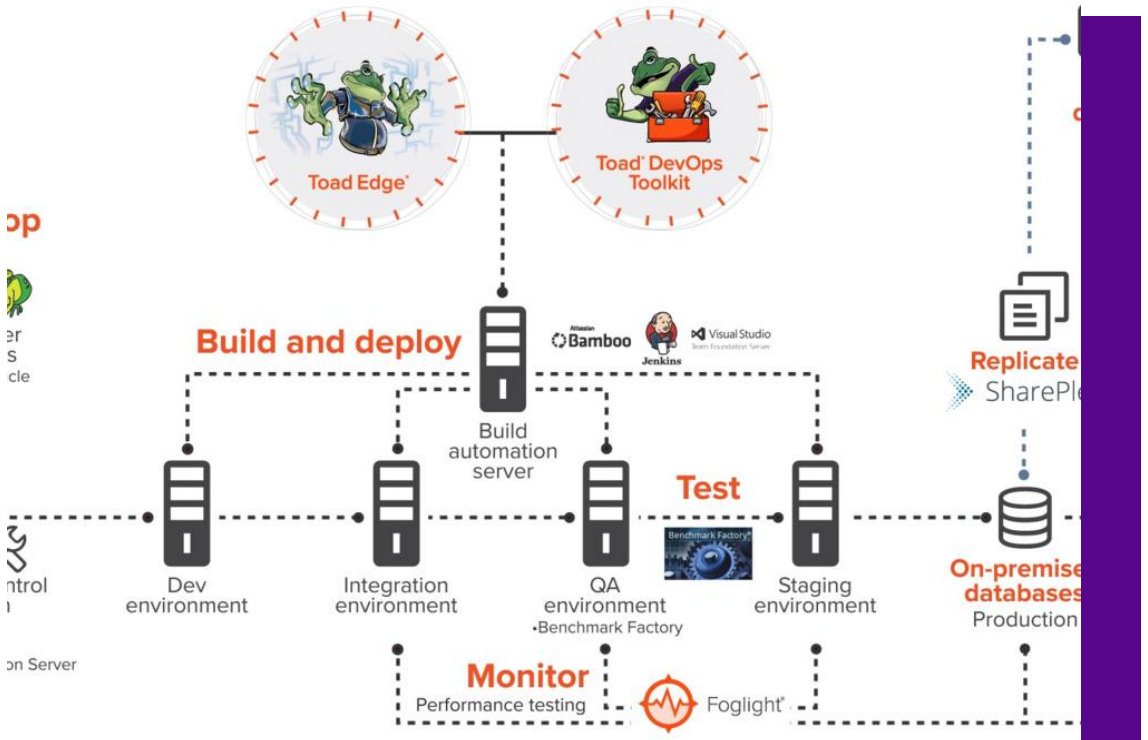
# Riesgos y Buenas Prácticas

- Control de permisos: Definir qué acciones puede ejecutar cada servidor MCP
- Timeouts: Establecer límites de tiempo para evitar bloqueos
- Logging: Registrar todas las acciones para auditoría y debugging
- Validación de entrada: Verificar y sanitizar datos antes de ejecutar
- Contención de acciones peligrosas: Sandboxing y restricciones de sistema

CHOUCAIR
Business Centric Testing

# Casos de uso ideales

- Automatización web: Navegación inteligente, scraping dinámico, interacción con formularios complejos
- Infraestructura (DevOps): Gestión de contenedores, despliegues automatizados, monitoreo inteligente
- Testing automatizado: Generación de casos de prueba, ejecución adaptativa, análisis de resultados
- Agentes empresariales: Asistentes inteligentes que ejecutan tareas complejas en sistemas corporativos
- ETL inteligentes: Extracción, transformación y carga de datos guiada por lenguaje natural
- RPA moderno impulsado por IA: Automatización de procesos robóticos con capacidad de razonamiento



CHOUCAIR
Business Centric Testing

# ¡Gracias!

## Resumen Final

- Los LLM son modelos poderosos de comprensión y generación
- MCP conecta LLM con herramientas reales de forma segura
- Juntos crean agentes inteligentes que automatizan tareas complejas

## Próximos Pasos:

Explora MCP en tus proyectos reales y descubre el potencial de la automatización inteligente