AB-100 · CHEAT SHEET · CERTIFYDECK

# Microsoft Certified: Agentic AI Business Solutions Architect Expert

Dominios, pesos oficiales y habilidades clave del temario de AB-100, para repasar antes del examen.

Nivel: Advanced (Expert) Duración: 100 min Nota de corte: 700/1000 Fuente: guía de estudio oficial de Microsoft Learn

## 1. Plan AI-powered business solutions

35–40%

### Analyze requirements for AI-powered business solutions

- El Cloud Adoption Framework distingue tres enfoques: la automatización basada en reglas para tareas fijas y predecibles, la RAG para responder a partir del conocimiento sin ejecutar acciones, y los agentes cuando hay que razonar y elegir acciones. Cuanta más autonomía, mayor impacto de los errores: las acciones difíciles de deshacer requieren aprobación humana, y los flujos de agente aportan pasos deterministas.
- La fundamentación se revisa en cinco dimensiones: exactitud (hechos verificados por expertos), relevancia (contenido acotado al caso de uso), actualidad (sin versiones caducadas), limpieza (sin duplicados ni ruido) y disponibilidad (indexado y accesible). Microsoft 365 Copilot y los agentes solo usan datos que el usuario puede ver, así que conviene revisar permisos y corregir el uso compartido excesivo.
- Para que otros sistemas de IA usen los datos de negocio sin duplicarlos: los Copilot connectors sincronizados indexan datos externos en Microsoft Graph con sus permisos y los federados los consultan en vivo por MCP; la Retrieval API fundamenta soluciones propias en SharePoint sin copiarlo; Link to Fabric lleva Dataverse a OneLake, y los servidores MCP de Dataverse y del ERP exponen registros y lógica de negocio.

### Design overall AI strategy for business solutions

- El proceso de adopción de IA del Cloud Adoption Framework parte de la estrategia (dónde aporta valor la IA), sigue con el plan (casos de uso desde problemas de negocio, madurez, prioridades y pruebas de concepto internas), AI Ready para cargas en Azure con la jerarquía de zonas de aterrizaje existente, y Govern, Secure y Manage AI como procesos continuos.
- La estrategia del Cloud Adoption Framework elige la solución con menor responsabilidad operativa: agentes predefinidos si bastan, Copilot Studio para poco código, Microsoft Foundry para código e infraestructura de Azure solo si hace falta control. El área de negocio es responsable del agente y de su riesgo residual; se combinan financiación central y local, formación por roles, privilegios mínimos y estándares de desarrollo comunes.
- En Copilot Studio, los agentes secundarios agrupan partes de un solo agente y los agentes conectados sirven cuando hay gobernanza, configuración o ALM propias o reutilización; A2A conecta agentes externos y MCP expone herramientas. En Microsoft Foundry, los agentes hospedados ejecutan orquestación propia. Conviene una fuente de conocimiento por subagente y visibilidad central con el registro de Microsoft Agent 365.
- Según Cloud Adoption Framework, conviene empezar por agentes precompilados (Dynamics 365, Microsoft 365 Copilot, Fabric, GitHub Copilot) cuando cumplen los requisitos: reducen el desarrollo aunque personalizan menos. Cada agente tiene su caso de uso, como Sales Qualification Agent para clientes potenciales o Case Management Agent para el ciclo de vida de casos, y se valida en un entorno de prueba antes de producción.
- Las reglas se reparten en capas: directivas de datos de Power Platform para limitar conectores, canales, HTTP o agentes sin autenticación; instrucciones y temas para acotar el ámbito del agente; moderación de contenido por agente, tema o solicitud. En Foundry, las barreras de protección combinan controles de daños, Prompt Shields y material protegido, y el mensaje del sistema fija rol, límites y comportamiento de reserva.

### Evaluate the costs and benefits of an AI-powered business solution

- Los criterios de ROI se agrupan en cuatro impulsores de valor (eficiencia, calidad, ingresos y estratégico), con indicadores adelantados y retrasados. El TCO suma implementación y operación: licencias y consumo, integraciones, hospedaje de dependencias como servidores MCP, gobierno, supervisión, soporte y retirada. Las horas ahorradas son capacidad, no ahorro financiero automático, y el coste por tarea completada mide la eficiencia.
- Un análisis de ROI creíble parte de una línea base medida antes del lanzamiento (tiempo por tarea, tasa de error, coste por interacción) con datos de sistemas, no solo encuestas. Las horas productivas se valoran con FTE, horas y tarifa con todos los costes; se prioriza con la matriz de impacto y esfuerzo y se mide con la calculadora de ahorros, Agent Assisted Hours y revisiones a 30 y 90 días.
- Empieza por los agentes y Copilot precompilados (Dynamics 365, Microsoft 365 Copilot) cuando cumplan los requisitos; si no, amplía Copilot con agentes declarativos o crea agentes con Copilot Studio (bajo código) o Microsoft Foundry (code-first). La infraestructura de Azure no es la opción predeterminada: elige la solución con la menor responsabilidad operativa y valora hospedaje, cumplimiento y esfuerzo.
- Model router en Microsoft Foundry analiza cada solicitud y la envía al modelo más adecuado: Balanced (predeterminado), Cost para volumen y presupuesto ajustado, Quality para tareas críticas. Un subconjunto de modelos actúa como control de cumplimiento y limita la conmutación por error; Data Zone Standard mantiene los datos en la zona. Para audio o un modelo fijo, usa una implementación directa y evalúa antes de producción.

## 2. Design AI-powered business solutions

30–35%

### Design AI and agents for business solutions

- Los términos de negocio enseñan a Copilot el vocabulario de la organización: los sinónimos dan nombres alternativos a columnas y el glosario define términos, siglas y reglas en función de tablas y columnas. En Sales se añaden en Copilot Studio y sirven para Sales agent y Copilot en Dynamics 365 Sales; en Customer Service, en la configuración de preguntas sobre datos. Alinéalos con los campos de clasificación y asigna responsables.
- Copilot en Customer Service se adapta con perfiles de experiencia por grupo de representantes, instrucciones personalizadas (solo con la base de conocimiento de Dynamics 365), solicitudes de la organización, filtros de conocimiento y respuesta determinista. Con Extend agent with Copilot Studio se añaden conocimiento, herramientas, agentes, temas y contexto personalizado; no se pueden cambiar el modelo ni las instrucciones del bot administrado.
- Para llevar datos externos a Sales se crea un conector personalizado de Power Platform (OAuth 2.0 con Microsoft Entra ID, en un entorno con aplicaciones de Dynamics 365) y una acción en Copilot Studio con las descripciones que Sales agent usa para asociarla. Un administrador de Sales la habilita y la certificación la abre a todos los usuarios. Revisa el cumplimiento de los datos de terceros.
- Los agentes de Copilot Studio se integran con Dynamics 365 Contact Center sin código específico por canal: un agente por flujo de trabajo basado en inserción, reglas de enrutamiento por contexto y transferencia al representante con todo el historial. En voz se usan DTMF, gramáticas y aviso de IA; con orquestación generativa, NLU+ procesa los datos dentro de Dynamics 365; las variables de contexto personalizan la conversación.
- Un agente de tareas completa acciones concretas con objetivos acotados, herramientas (conectores, flujos de agente, solicitudes, REST, MCP, computer use), conocimiento gobernado y reglas de seguridad. La orquestación generativa elige las herramientas por su descripción; usa flujos de agente para pasos deterministas y aprobaciones, pide confirmación en acciones sensibles y aplica el mínimo privilegio en la autenticación.

### Design extensibility of AI solutions

- En Microsoft Foundry, RAG se usa cuando las respuestas dependen de datos privados o cambiantes, y el fine-tuning (SFT, DPO o RFT) cuando hay que cambiar el comportamiento, el estilo o el uso de herramientas. El tipo de entrenamiento decide la residencia de datos, y los modelos ajustados pasan evaluaciones de seguridad. Un modelo de Foundry puede usarse en solicitudes de Copilot Studio mediante su endpoint de chat completions.
- Microsoft 365 Copilot admite dos enfoques: agentes declarativos, que usan el orquestador y los modelos de Copilot con instrucciones, conocimiento y acciones, y agentes de motor personalizado, con orquestación y modelos propios, mensajes proactivos y alojamiento externo. Los Copilot connectors sincronizados indexan datos en Microsoft Graph; los federados consultan en tiempo real mediante MCP.
- Un agente de Copilot Studio se amplía con temas, conocimiento, herramientas (conectores precompilados o personalizados, flujos de agente, solicitudes, MCP, computer use) y otros agentes. La orquestación generativa elige herramientas por su nombre y descripción. Los agentes secundarios agrupan capacidades de un mismo equipo; los conectados permiten modelo, ALM y publicación independientes.
- Con Model Context Protocol, un agente de Copilot Studio usa las herramientas y los recursos que publica un servidor MCP, y los cambios del servidor se reflejan automáticamente. Requiere orquestación generativa y el transporte Streamable, admite API key u OAuth 2.0 y queda sujeto a las directivas de datos de conectores. Conviene usar servidores de confianza y activar solo las herramientas necesarias.
- Computer use permite a un agente de Copilot Studio manejar sitios web y aplicaciones de escritorio de Windows con ratón y teclado virtuales cuando no hay API, y se adapta a cambios de interfaz. Requiere orquestación generativa y se configura con instrucciones, entradas, máquina, credenciales, control de acceso, Enforce HTTPS y supervisión humana, que no es una garantía. Conviene usar máquinas dedicadas y cuentas con privilegios mínimos.

### Orchestrate configuration for prebuilt agents and apps

- Las aplicaciones de finanzas y operaciones ofrecen Copilot en panel lateral, funciones integradas como resúmenes y análisis de planes de demanda, y agentes como Account Reconciliation Agent o el de comunicación con proveedores. Requieren Power Platform Integration y, si hace falta, mover datos entre regiones. El servidor Dynamics 365 ERP MCP da herramientas de datos, formularios y acciones limitadas por el rol de seguridad.
- Dynamics 365 Customer Service y Contact Center combinan agentes autónomos (Case Management Agent para el ciclo de vida del caso, Customer Knowledge Management Agent para crear artículos, Customer Intent Agent y Quality Evaluation Agent) con funciones de Copilot para el representante. El rollout manager activa los agentes de forma escalonada. En Sales, Sales Qualification Agent ofrece los modos Research only y Research and engage.
- Para extender Microsoft 365 Copilot se elige entre agentes declarativos, que usan el orquestador y los modelos de Copilot sin hospedaje adicional y heredan el cumplimiento de Microsoft 365, y agentes de motor personalizado, con orquestación y modelos propios, mensajería proactiva y uso en grupo. Agent Builder sirve para agentes guiados; Copilot Studio, para canales externos, acciones y flujos.
- Sales agent (antes Microsoft 365 Copilot for Sales) consulta Dynamics 365 Sales o Salesforce respetando la seguridad del CRM; se configuran las entidades, sinónimos, términos de glosario e instrucciones de IA de los resúmenes. Service Agent (antes Copilot for Service) requiere que el administrador de Microsoft 365 instale la aplicación Service y que el de Dynamics 365 añada Copilot al entorno.
- Power Platform ofrece AI Builder, con modelos precompilados listos para usar y modelos personalizados que se entrenan con datos propios, accesibles desde el AI hub de Power Apps y Power Automate; solicitudes reutilizables en agentes, flujos y aplicaciones con supervisión humana; Copilot en Power Apps para crear aplicaciones con lenguaje natural, y Microsoft Copilot en aplicaciones basadas en modelos.

## 3. Deploy AI-powered business solutions

20–25%

### Analyze, monitor, and tune AI-powered business solutions

- La supervisión de agentes combina la página Monitor de Copilot Studio para cada agente, Application Insights para telemetría propia consultable con Kusto, el área Monitor del Centro de administración de Power Platform para el estado agregado del inquilino y Microsoft Purview y Sentinel para auditoría y alertas. Agent 365 ofrece observabilidad nativa para agentes declarativos.
- El análisis del backlog y de la opinión de los usuarios se basa en un ciclo iterativo: reacciones, comentarios, CSAT y temas alimentan historias de usuario que se priorizan y refinan con regularidad, buscando tendencias de varias semanas. Ver comentarios y transcripciones requiere el rol Bot Transcript Viewer. En finanzas y operaciones, la opinión mejorada se habilita por niveles: inquilino, organización y entorno.
- Copilot Studio aplica IA en la página Monitor con un resumen de conclusiones y la valoración de calidad de una muestra de respuestas (integridad, relevancia y fundamentación). El Copilot Agent Kit suma Conversation Analyzer para analizar transcripciones con solicitudes propias, Agent Review Tool para detectar antipatrones, Prompt Advisor para mejorar solicitudes y Agent Debugger para diagnosticar respuestas.
- La página Monitor de Copilot Studio mide resultados de sesión (resuelto, escalado, abandonado, sin interacción), reacciones, CSAT, uso de herramientas y conocimiento, y el rendimiento de agentes secundarios y conectados; los agentes autónomos se miden por resultados de ejecución y uso de desencadenadores. Los usuarios activos requieren autenticación. En Contact Center, el panel Agent insights muestra KPI como la tasa autónoma, desglosa los escalados según su motivo; Knowledge source use y la calidad de las respuestas generadas señalan qué fuentes fallan. En Application Insights se excluyen las pruebas con designMode, y en Microsoft Foundry el seguimiento y el panel de supervisión revelan latencia, tokens y evaluaciones.
- En Copilot Studio, la página Monitor clasifica cada sesión como resuelta, escalada, abandonada o sin interacción, y

### Manage the testing of AI-powered business solutions

- Las pruebas de agentes combinan el chat de prueba con conjuntos de evaluación repetibles: General quality valora relevancia, fundamentación, integridad y abstención sin respuestas esperadas, y los métodos de comparación sí las necesitan. La guía propone un conjunto básico, una línea base con varias ejecuciones y conjuntos de robustez, arquitectura y casos límite que se vuelven a ejecutar tras cada cambio.
- Validar un modelo personalizado exige criterios definidos antes de probarlo. En AI Builder, la calificación de predicción depende de la tasa histórica y una D cercana al 100 % indica sobreajuste; la clasificación usa precisión, exhaustividad y F1. En Microsoft Foundry se comparan puntos de control con datos reservados y con el modelo base, sin fiarse solo de la pérdida de entrenamiento.
- Validar las instrucciones de un agente implica comprobar que se apoyan en herramientas y fuentes realmente configuradas, que especifican tono, detalle y formato, y que usan viñetas para tareas paralelas y pasos solo para secuencias. Las instrucciones no se trasladan a documentos de conocimiento, y fallos como el uso precipitado de herramientas se corrigen con reglas explícitas y pasos de autoevaluación.
- Las pruebas de extremo a extremo conectan todos los procesos del alcance y sus integraciones entre aplicaciones de Dynamics 365, en un entorno integrado con datos migrados y la última versión de la solución, a lo largo de varios ciclos manuales o automatizados. Cada caso define criterios de entrada, pasos y criterios de salida, incluye escenarios negativos y comprueba que el contexto se conserva en los traspasos.
- Copilot Studio puede generar casos de prueba con IA a partir de la descripción del agente, sus fuentes de conocimiento o sus temas, o reutilizar el chat de prueba; generar desde el conocimiento no revela lagunas, así que se añaden preguntas reales de usuarios. Las sugerencias de la IA se revisan, los datos de prueba deben ser sintéticos y se vigila que los casos generados no expongan datos confidenciales.

### Design the ALM process for AI-powered business solutions

- El ciclo de vida de los datos separa lo que viaja en la solución de lo que no: las variables de entorno parametrizan URL y secretos, Configuration Migration tool mueve datos de configuración relacionales y los datos de entrenamiento de AI Builder no se exportan. En Foundry, las definiciones de agentes y sus referencias de conocimiento se versionan, y los conjuntos de referencia se mantienen al día.
- Los agentes de Copilot Studio se trasladan en soluciones personalizadas desde desarrollo, como administradas en prueba y producción, con variables de entorno para ajustes y secretos y referencias de conexión para credenciales. Los conectores personalizados se importan antes que la solución del agente, y elementos como Application Insights, la autenticación manual o los canales requieren pasos tras la implementación.
- En Microsoft Foundry Agent Service, cada cambio de un agente se guarda como versión inmutable y el código lo referencia por nombre y versión. Las canalizaciones de azd usan entornos separados y credenciales federadas; antes de promover un candidato se fija producción a la versión actual y se valida el candidato. La infraestructura se define como código y los permisos se reasignan al agente publicado.
- Los modelos de AI Builder se distribuyen en soluciones: solo viaja la versión publicada, sin datos de entrenamiento, conviene bloquear las personalizaciones antes de importar y el modelo se añade explícitamente porque no es dependencia de la aplicación. Cloud Adoption Framework pide control de versiones con reversión, reentrenamiento por rendimiento, puertas de calidad y seguimiento de la retirada de modelos.
- Copilot en finanzas y operaciones se basa en un agente de Copilot Studio incluido en una solución de Microsoft y requiere Power Platform Integration. Las ampliaciones combinan elementos de Power Platform, como temas, flujos y entidades virtuales, con código X++ implementado en el entorno de finanzas, cuya seguridad debe asignarse a mano, se desarrollan en entornos gobernados de nivel superior.

### Design responsible AI, security, governance, risk management, and compliance

- La seguridad de un agente empieza por la autenticación: Authenticate with Microsoft para Teams, SharePoint, Power Apps y Microsoft Copilot, o autenticación manual cuando se necesita el token del usuario u otros canales. Los conectores deben usar credenciales del usuario final; el análisis de seguridad avisa ante cambios inseguros. Para casos críticos se suman CMK, Customer Lockbox, firewall de IP y secretos en el canal web.
- La gobernanza de agentes se organiza por zonas según el riesgo: agentes personales aislados en entornos de desarrollador, agentes de departamento con revisión de TI y canalizaciones, y agentes empresariales con los controles más estrictos. Las directivas de datos bloquean canales, conectores o el uso sin autenticación, y las reglas de uso compartido limitan la difusión. Microsoft Agent 365 añade registro, propietarios y riesgos centralizados.
- En Microsoft Foundry, la seguridad del modelo combina Microsoft Entra ID con identidades administradas y RBAC de privilegio mínimo, aislamiento de red con puntos de conexión privados y barreras de protección (guardrails) con niveles de bloqueo por riesgo. Los modelos vendidos por Azure no comparten solicitudes ni datos de entrenamiento con sus proveedores, y los modelos ajustados son exclusivos del cliente.
- La manipulación de solicitudes llega por dos vías: ataques en la solicitud del usuario e instrucciones ocultas en documentos, correos o páginas (inyección de solicitudes entre dominios). Prompt Shields detecta ambos si se separa la entrada del usuario del contenido de terceros y no se envía la solicitud del sistema. Copilot Studio bloquea UPIA y XPIA de forma predeterminada, y las pruebas de red team completan la defensa.
- Revisar una solución frente a la IA responsable implica evaluarla con los seis principios: equidad, fiabilidad y seguridad, privacidad y seguridad, inclusión, transparencia y responsabilidad. Microsoft Foundry organiza el trabajo en Discover, Protect y Govern. En Copilot Studio, las respuestas generativas no verifican la exactitud, así que se limita el ámbito, se modera el contenido y se prueba antes de publicar.