

BPC

BEST PRACTICES
CONSULTING

GUÍA EJECUTIVA

MICROSOFT · IA · DATOS · AUTOMATIZACIÓN

Antes de implementar un agente de IA

10 decisiones que tu empresa debe tomar

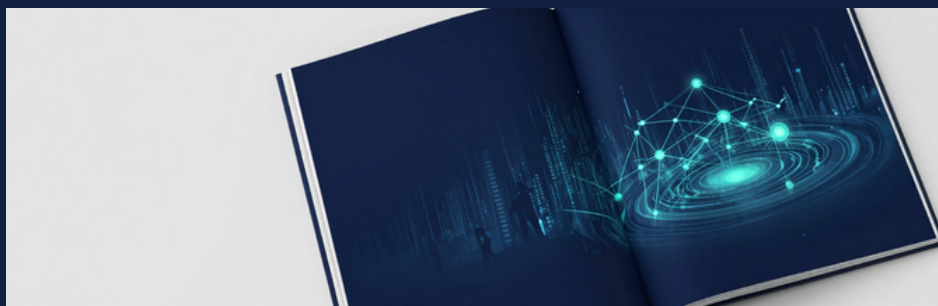
Una guía práctica para identificar un caso de uso, definir límites y avanzar con seguridad, visibilidad y control.

IDEA CENTRAL

La autonomía no comienza cuando un agente puede hacer más. Comienza cuando la empresa define qué puede hacer, con qué información y bajo qué supervisión.

BEST PRACTICES CONSULTING

PartnerMicrosoft · Consultoría tecnológica · IA aplicada a procesos reales



La IA ya no solo responde. También actúa.

Durante la primera etapa de adopción, la inteligencia artificial funcionó principalmente como un asistente: una persona hacía una consulta, recibía una respuesta y decidía qué hacer con ella.

Los agentes amplían esa capacidad. Pueden recibir un objetivo, consultar información y preparar o ejecutar acciones dentro de los límites definidos por la organización.

LA DIFERENCIA EN UNA FRASE

Un asistente ayuda a una persona a realizar una tarea. Un agente puede coordinar pasos para acercarse a un resultado.

¿Qué cambia para la empresa?

Más capacidad El agente puede conectar información, instrucciones y acciones.	Más responsabilidad La empresa debe definir permisos, fuentes y límites.
Más velocidad Los procesos pueden avanzar con menos trabajo manual.	Más necesidad de control Cada acción debe ser visible, trazable y revisable.

Esta guía no pretende sustituir una evaluación técnica, legal o de seguridad. Su propósito es ayudar a los equipos directivos y operativos a formular las preguntas correctas antes de escalar.

No empieces por la tecnología. Empieza por la fricción.

Un agente genera valor cuando resuelve una situación frecuente, usa información disponible y produce un resultado que puede medirse. Si el proceso no está claro, automatizarlo solo acelera la confusión.

Señales de un buen primer caso de uso

- La tarea ocurre con frecuencia y consume tiempo de equipo.
- Existe una fuente de información identificable y responsable.
- El resultado esperado puede explicarse en una frase.
- Las excepciones pueden escalarse a una persona.
- El impacto puede medirse antes y después.

Ejemplos por función

Ventas Preparar el contexto de una oportunidad, resumir interacciones y proponer el siguiente paso para revisión.	Servicio Orientar solicitudes con base en conocimiento autorizado y escalar excepciones.
Operaciones Recopilar datos, identificar faltantes y preparar una solicitud para aprobación.	Finanzas Detectar variaciones y organizar evidencia para que una persona valide la decisión.
Recursos Humanos Responder preguntas frecuentes desde políticas vigentes y dirigir casos sensibles al área responsable.	Tecnología Clasificar requerimientos, reunir contexto y preparar una ruta de atención.

FILTRO RÁPIDO

Si el caso depende de datos desordenados, permisos indefinidos o decisiones que nadie asume, todavía no está listo para convertirse en agente.

Las 10 decisiones antes de implementar un agente

Reúne a negocio, TI, seguridad, datos y al responsable del proceso. Responde cada pregunta con evidencia, no con supuestos.

1. Problema · ¿Qué fricción concreta resolverá para quién?

Describe la situación actual, su frecuencia y su consecuencia. Evita objetivos vagos como "usar IA".

2. Resultado · ¿Qué entregable o cambio debe producir?

Define cómo se verá un buen resultado y qué debe quedar fuera.

3. Información · ¿Qué datos y documentos necesita?

Identifica fuentes autorizadas, vigencia, calidad y persona responsable.

4. Sistemas · ¿Con qué aplicaciones debe interactuar?

Separa lo que solo consulta de lo que puede modificar.

5. Permisos · ¿Cuál es el acceso mínimo necesario?

Diseña el caso con menor privilegio y revisa de pe nde ncias .

6. Acciones · ¿Qué puede preparar, ejecutar o rechazar?

Clasifica acciones por impacto, reversibilidad y sensibilidad.

7. Supervisión · ¿En qué momento debe intervenir una persona?

Define aprobaciones, escalamiento y criterios de detención.

8. Observabilidad · ¿Cómo sabremos qué hizo y por qué?

Asegura registros, seguimiento de excepciones y evidencia.

9. Responsabilidad · ¿Quién será dueño funcional y técnico?

Asigna responsables para contenido, permisos, operación y mejora.

10. Medición · ¿Qué indicador demostrará valor y seguridad?

Mide resultado, tiempo, calidad, adopción, excepciones y riesgo.

04 · NIVEL DE AUTONOMÍA

No todas las tareas deben delegarse igual

La autonomía debe corresponder al impacto de la acción. Una tarea reversible y de bajo riesgo puede automatizarse más que una decisión financiera, legal, reputacional o que afecte directamente a un cliente.

Nivel	Qué puede hacer	Ejemplos
VERDE · Preparar	Consultar, ordenar, resumir o preparar un borrador sin cambiar el sistema de registro.	Resumen de contexto, clasificación, borrador, lista de faltantes.
AMARILLO · Proponer	Preparar una acción o modificación que requiere validación previa.	Actualizar un registro, crear una solicitud, redactar una comunicación externa.
ROJO · Autorizar	Decisiones sensibles, irreversibles o con impacto material. Deben conservar control humano explícito.	Aprobaciones, pagos, bajas, decisiones legales o de cumplimiento.

Regla práctica: si una acción no puede revertirse fácilmente o puede afectar derechos, dinero, cumplimiento, reputación o seguridad, debe diseñarse con autorización humana y controles adicionales.

Tres preguntas para asignar el nivel

- ¿Qué ocurre si el agente se equivoca?
- ¿La acción puede revertirse sin daño?
- ¿Quién debe aprobar una excepción?

Checklist de preparación

Marca una opción por afirmación. Usa el resultado para identificar conversaciones pendientes, no como una certificación.

Afirmación	Sí	Parcial	No
Tenemos un problema de negocio claramente definido.	☐	☐	☐
Conocemos el resultado que debe producir el agente.	☐	☐	☐
Las fuentes de información están identificadas y tienen responsable.	☐	☐	☐
Los datos necesarios son confiables, vigentes y accesibles.	☐	☐	☐
Los permisos mínimos están documentados.	☐	☐	☐
Las acciones permitidas y restringidas están definidas.	☐	☐	☐
Sabemos cuándo debe intervenir una persona.	☐	☐	☐
Podemos registrar y revisar la actividad del agente.	☐	☐	☐
Existe un dueño funcional y un dueño técnico.	☐	☐	☐
Definimos indicadores de valor, calidad, adopción y riesgo.	☐	☐	☐

Cómo interpretar el resultado

8–10 respuestas “Sí” Hay una base sólida para diseñar un piloto controlado. Valida la arquitectura y los riesgos específicos.	5–7 respuestas “Sí” El caso tiene potencial, pero conviene resolver brechas antes de aumentar autonomía.
0–4 respuestas “Sí” Empieza por clarificar el proceso, ordenar datos, permisos y responsabilidades.	

Criterio orientativo desarrollado por BPC. El resultado no sustituye evaluaciones especializadas de seguridad, privacidad, legal, cumplimiento o arquitectura.

06 · HERRAMIENTA DE TRABAJO

Canvas para definir tu primer agente

Completa esta página con el equipo responsable del proceso. Si una respuesta no está disponible, conviértela en una acción previa al piloto.

1. Problema que queremos resolver	2. Personas o áreas beneficiadas
3. Resultado esperado	4. Frecuencia y volumen actual
5. Fuentes de información autorizadas	6. Sistemas que consultará o modificará
7. Acciones permitidas	8. Acciones restringidas
9. Momentos de revisión humana	10. Responsables e indicador de éxito

Una ruta de 30 días para aprender sin perder control

La duración real dependerá del caso y de la arquitectura. Esta secuencia propone un ritmo de trabajo para un piloto acotado, con información de prueba o debidamente autorizada.

SEMANA 1	Definir	Acordar problema, usuarios, resultado, fuentes, dueño funcional y métrica base.
SEMANA 2	Diseñar	Definir instrucciones, conocimiento, permisos, acciones, excepciones y revisión humana.
SEMANA 3	Probar	Ejecutar casos normales, datos faltantes, conflicto de fuentes, fuera de alcance y datos sensibles.
SEMANA 4	Decidir	Comparar resultados, revisar incidentes y decidir: ajustar, ampliar, mantener limitado o detener.

Pruebas mínimas antes de publicar

- Respuesta conocida: usa la fuente correcta.
- Dato faltante: pregunta antes de concluir.
- Fuentes en conflicto: advierte y escala.
- Solicitud fuera de alcance: rechaza y orienta.
- Dato sensible: aplica el límite definido.
- Intento de ejecutar una acción restringida: se detiene y solicita aprobación.

PUERTA DE SALIDA

Un piloto también puede concluir que el caso aún no debe escalar. Detectarlo temprano es un resultado útil.

Mide valor y control al mismo tiempo

Un agente no debe considerarse exitoso solo por responder rápido. La medición debe combinar impacto operativo, calidad, adopción y riesgo.

Valor Tiempo ahorrado, volumen procesado, reducción de retrabajo, tiempo de ciclo.	Calidad Exactitud validada, completitud, consistencia, uso de fuentes autorizadas.
Adopción Usuarios activos, tareas completadas, satisfacción y repetición de uso.	Control Excepciones, escalaciones, accesos indebidos, acciones detenidas e incidentes.
Economía Coste por interacción, consumo, soporte y retorno frente al proceso actual.	Aprendizaje Errores recurrentes, nuevas reglas, fuentes por mejorar y casos fuera de alcance.

Ficha de resultado del piloto

Indicador principal	
Línea base	
Resultado del piloto	
Excepciones observadas	Escalar / Ajustar / Mantener limitado / Detener
Decisión	
Próxima revisión	

La autonomía comienza con límites claros

Los agentes de IA pueden reducir trabajo repetitivo, conectar información y acelerar procesos. Pero su valor no depende únicamente de lo que sean capaces de hacer.

Depende de la calidad de los datos que utilizan, de los permisos que reciben, de la visibilidad sobre sus acciones y de la claridad con la que la empresa define responsabilidades.

PRINCIPIO BPC

Una Empresa Autónoma no es la que delega todas sus decisiones. Es la que sabe qué delegar, bajo qué condiciones y con qué responsabilidad.

Tu siguiente conversación

Selecciona una tarea frecuente, identifica una fuente confiable y reúne a las personas responsables del proceso, los datos y la seguridad. Completa el canvas de esta guía y define qué tendría que ocurrir para considerar exitoso un piloto.

Best Practices Consulting acompaña a las organizaciones desde la identificación del caso de uso hasta el diseño, implementación, adopción y mejora continua de soluciones Microsoft.

SIGUIENTE PASO

Solicita un diagnóstico de proceso candidato para priorizar un caso de uso y definir una ruta de implementación.

www.bestpractices.com.mx | informes@bestpractices.com.mx | +52 442 312 4000

10 · REFERENCIAS

Fuentes y criterios utilizados

Esta guía combina referencias públicas de Microsoft con criterios editoriales y marcos de trabajo de Best Practices Consulting. Las recomendaciones deben adaptarse al contexto, regulación, arquitectura y nivel de riesgo de cada organización.

Microsoft Source Latinoamérica · “Seguridad y agentes de IA: el desafío empresarial”.

[Consultar fuente](#)

Aviso

Documento informativo. No constituye asesoría legal, de ciberseguridad, privacidad o cumplimiento. Las decisiones técnicas y de gobierno deben validarse con las áreas responsables y con especialistas según el caso.

© 2026 Best Practices Consulting. Material preparado para fines educativos y comerciales.