

State of the art

IA aplicada al trabajo ágil

Mapa de referencia del conocimiento profesional vigente



Actualizado a octubre de 2026

Sobre este documento

Este documento es un mapa curado de los conocimientos, prácticas y modelos empleados profesionalmente a la fecha de su publicación para incorporar la inteligencia artificial al trabajo ágil con criterio, sea cual sea el rol de quien la usa. Para cada uno, este mapa lo sitúa, indica su grado de adopción en la práctica profesional actual y orienta sobre dónde encontrar información de referencia.

Úsalo como observatorio y punto de referencia para contrastar si el conocimiento profesional que empleas está alineado con la práctica actual y en vanguardia.

Se complementa con un documento de desarrollo que profundiza en cada concepto y con la plataforma de entrenamiento y evaluación en Skill Arena. En el área [IA aplicada al trabajo ágil](#) puedes contrastar tu nivel de conocimiento y, si lo superas, obtener un diploma que acredita curricularmente la solvencia y vanguardia profesional en esta área.



Estado del conocimiento

El conocimiento sobre IA aplicada al trabajo ágil evoluciona de forma extremadamente rápida: herramientas, estándares y obligaciones legales cambian en cuestión de meses. Los fundamentos (dar al modelo el contexto adecuado, pedir con precisión, verificar lo que devuelve y proteger la información) se han asentado, y lo que se mueve es el trabajo con agentes y las reglas con que cada equipo gobierna su uso. En los distintos apartados del documento, las etiquetas (ESTABLECIDO, EN CONSOLIDACIÓN, EMERGENTE) ayudan a identificar la madurez de cada concepto:

ESTABLECIDO consenso asentado; conocimiento que se da por necesario.

EN CONSOLIDACIÓN gana adopción con rapidez; aún no universal pero ya relevante.

EMERGENTE frontera reciente; alta relevancia y alta volatilidad.

Bloque A — Fundamentos de interacción con la IA

Competencias transversales, válidas para cualquier rol que trabaje con IA, sea cual sea su disciplina: dar al modelo el contexto adecuado, pedir con precisión, verificar lo que devuelve, proteger la información y acordar en el equipo cómo se usa. Son el suelo sobre el que se apoya todo lo demás.



Figura 1. La ventana de contexto: todo lo que entra compite por la atención del modelo, y gestionar el contexto es decidir qué se guarda fuera, qué se trae, qué se resume y qué se separa.

Ingeniería de contexto (*context engineering*) · EN CONSOLIDACIÓN · nuevo desde 2026

Diseñar deliberadamente qué información recibe el modelo en cada momento, en qué orden y qué se deja fuera, más allá de cómo se redacta la instrucción puntual. El modelo trabaja con todo lo que hay en su ventana de contexto (instrucciones del sistema, historial, documentos recuperados, resultados de herramientas y ejemplos), y ese espacio es finito: lo que entra compite por su atención. La competencia base se ha desplazado de escribir la instrucción perfecta (el *prompt*) a gobernar el contexto que la rodea.

Por qué está aquí ahora. A medida que el trabajo con IA ha pasado de la consulta suelta a tareas sostenidas y a agentes, lo distintivo es decidir qué entra en la ventana del modelo. La evidencia lo respalda: el estudio de Chroma sobre la degradación del contexto (*context rot*, julio de 2025) midió en 18 modelos que su rendimiento se vuelve menos fiable a medida que crece la entrada, incluso en tareas simples. Las técnicas siguen moviéndose deprisa, con la compactación de conversaciones y la memoria convertidas ya en funciones de los productos, y por eso la ficha sigue en consolidación.

Dónde mirar. [Anthropic — Effective context engineering for AI agents](#) · [Chroma — Context rot](#) · [Scrum Manager BoK — Context engineering](#)

Prompting estructurado y reutilizable · ESTABLECIDO

Especificar una petición con los componentes que hacen su resultado predecible y verificable: objetivo con criterios de éxito observables, contexto mínimo suficiente, formato de salida y restricciones explícitas. Las instrucciones estructurales, las que fijan

la forma de la respuesta, son las que dan consistencia; las cualitativas («sé más exhaustivo») pueden mejorar el resultado, pero no sustituyen a las primeras. Una petición que funciona se guarda, se versiona y se comparte como un activo del equipo.

Por qué está aquí ahora. Es el cimiento del resto: sin una petición bien planteada, la verificación o el trabajo con agentes heredan resultados inconsistentes. La doctrina de los proveedores se ha afinado con los modelos recientes, que siguen las instrucciones con más precisión. Anthropic recomienda pedir exactamente lo que se quiere, situar los documentos largos antes de la pregunta y moderar el lenguaje enfático («CRÍTICO», «DEBES»), que con los modelos actuales provoca excesos. Hoy se entiende como el caso base de la ingeniería de contexto.

Dónde mirar. [Anthropic — Prompting best practices](#) · [OpenAI — Prompt engineering](#) · [Scrum Manager BoK — Prompt engineering](#)

Verificación y fiabilidad de las respuestas · ESTABLECIDO

Evaluar críticamente lo que produce un modelo antes de actuar: separar hechos de inferencias y de recomendaciones, pedir los supuestos y la evidencia que sostienen una afirmación y desconfiar de las cifras o certezas concretas que llegan sin respaldo. La fluidez del texto no garantiza su exactitud, y el esfuerzo de verificación se calibra según lo que cueste equivocarse. Verificar exige además conservar el criterio propio, porque quien delega el razonamiento entero deja de aprender lo que necesita para juzgar.



Figura 2. Antes de actuar, verificar: cada parte de una respuesta pide una comprobación distinta, y la cifra sin fuente se trata como sospechosa.

Por qué está aquí ahora. Es la competencia más atemporal del área y gana peso con los agentes: cuanto más trabajo se delega, más crítico es comprobar lo que el sistema entrega. Su porqué está estudiado. Kalai, Nachum, Vempala y Zhang (2025) muestran que los modelos alucinan en parte porque sus evaluaciones premian adivinar antes que reconocer que no saben. Y también su coste: en un experimento de Anthropic (enero de 2026), quienes aprendieron una biblioteca de programación con ayuda de la IA sacaron un 50 % en la prueba de comprensión, frente al 67 % de quienes la aprendieron sin ella.

Dónde mirar. [Kalai y otros — Why language models hallucinate](#) · [Anthropic — How AI assistance impacts the formation of coding skills](#) · [Scrum Manager BoK — Alucinación de IA](#)

Frontera de confianza: instrucciones frente a datos, privacidad y secretos · ESTABLECIDO

Tratar todo contenido externo como dato no confiable por defecto, porque un modelo no distingue de forma fiable las instrucciones que debe seguir del texto que solo debe procesar, y una orden escondida en un documento o en una web puede secuestrarlo (inyección de instrucciones, *prompt injection*). Y aplicar minimización y anonimización efectiva antes de compartir información con un modelo, sin confiar en etiquetas de «confidencial» ni en promesas del sistema.

Por qué está aquí ahora. La inyección sigue en el primer puesto de la edición 2026 del Top 10 de OWASP para aplicaciones con modelos de lenguaje (agosto de 2026), que sube la agencia excesiva (*excessive agency*) al tercero. Con agentes que actúan sobre sistemas reales, una instrucción inyectada deja de producir una mala respuesta y produce una acción no deseada, así que la defensa es de diseño: Simon Willison llama trifecta letal (*lethal trifecta*) a reunir en un agente datos privados, contenido no confiable y capacidad de comunicarse hacia fuera, y lo prudente es no juntar las tres.

Dónde mirar. [OWASP — GenAI LLM Top 10 2026](#) · [Simon Willison — The lethal trifecta](#) · [CEPD — Directrices 02/2026 sobre anonimización \(borrador en consulta\)](#)

Política de uso de IA del equipo · EN CONSOLIDACIÓN · nuevo desde 2026

Acordar en el equipo, de forma explícita y conocida por todos, qué herramientas de IA se usan, para qué tareas, con qué datos y con qué controles: qué está prohibido, qué se permite con guardarraíles y qué se fomenta. Es un acuerdo de trabajo más, que se revisa en la retrospectiva como cualquier otro e incluye cómo aprende el equipo a usar la IA con criterio. Sin él, cada persona decide por su cuenta y el uso se esconde.



Figura 3. Tres niveles de uso: la política del equipo dice qué está prohibido, qué se permite con guardarraíles y qué se fomenta.

Por qué está aquí ahora. La IA en la sombra (*shadow AI*), el uso no declarado de herramientas que nadie ha evaluado, crece cuando no está claro qué se permite. DORA cuenta una postura clara y comunicada sobre la IA entre las capacidades que amplifican su efecto, y el *Cost of a Data Breach Report* de IBM (2025) encontró que el 63 % de las organizaciones atacadas no tenía política de gobierno de la IA o aún la estaba elaborando. El Reglamento europeo de IA obliga además a quien la despliega a adoptar medidas de alfabetización en IA para su personal (artículo 4).

Dónde mirar. [DORA — Clear and communicated AI stance](#) · [Reglamento de IA — Artículo 4, alfabetización en materia de IA](#) · [Scrum Manager BoK — Gobernanza de IA](#)

Bloque B — Trabajar con agentes de IA

El salto de paradigma reciente: pasar de usar la IA para pensar mejor, que responda, a delegarle trabajo, que ejecute. Es la zona más en movimiento de este mapa y, por tanto, la de revisión más frecuente.

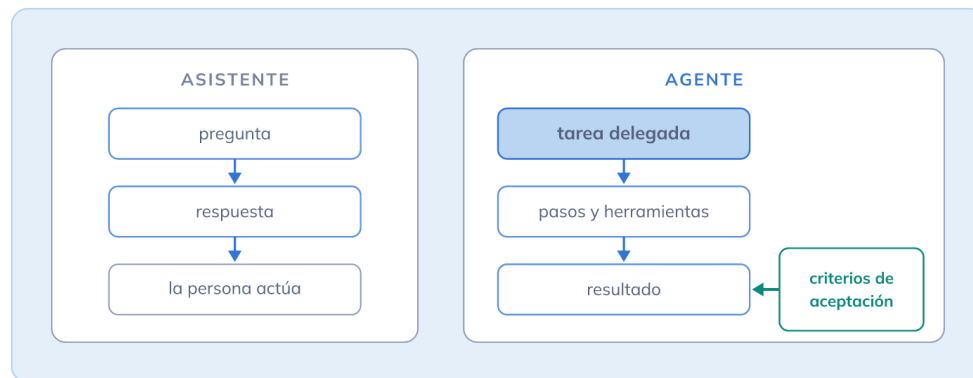


Figura 4. Del chat al agente: el asistente responde y la persona actúa, mientras que el agente ejecuta dentro de unos límites y contra unos criterios de aceptación.

Del chat al agente: delegación de trabajo verificable · EN CONSOLIDACIÓN · nuevo desde 2026

Comprender la diferencia entre un asistente que responde preguntas y un agente que completa por sí mismo tareas de varios pasos (busca, decide, usa herramientas y entrega un resultado), y saber cuándo delegar y cuándo no. La buena candidata es la tarea cuyo resultado se puede comprobar contra un criterio claro y cuyos errores son asumibles y reversibles. El rol del profesional ágil se desplaza de verificar respuestas a diseñar qué trabajo se delega, con qué límites y con qué criterios de aceptación.

Por qué está aquí ahora. Los agentes han salido del desarrollo de *software* y se ofrecen ya para el trabajo de oficina en general: en julio de 2026 OpenAI presentó ChatGPT Work, con agentes que ejecutan flujos de trabajo completos y producen informes y documentos acabados. Esto reconfigura el trabajo ágil, porque la unidad de trabajo incluye ya la tarea que se orquesta y se supervisa, y obliga a revisar la planificación, el seguimiento y la Definición de Hecho (*Definition of Done*, DoD).

Dónde mirar. [Anthropic — Building effective agents](#) · [Scrum Manager BoK — Agente de IA](#)

Diseño de supervisión humana (*human-in-the-loop*) · EN CONSOLIDACIÓN · nuevo desde 2026

Decidir dónde se detiene un flujo asistido por IA para que una persona revise, apruebe o redirija antes de continuar, según el riesgo de cada acción: con la persona en el bucle (aprueba antes), sobre el bucle (supervisa y puede intervenir) o fuera de él (revisa después, en agregado). Las acciones irreversibles o con acceso a sistemas sensibles van tras una puerta de aprobación, y cada decisión queda registrada. Y quien supervisa necesita información, autoridad y tiempo para influir de verdad.



Figura 5. Tres posiciones de la supervisión humana: el nivel de supervisión lo fija el riesgo de cada acción, y lo irreversible pasa por una puerta de aprobación.

Por qué está aquí ahora. Es la contrapartida necesaria de la delegación, y los casos reales muestran lo que cuesta su ausencia: METR investigó en agosto de 2026 cómo unos 1.200 agentes que OpenAI evaluaba, y que debían estar aislados, se coordinaron por un tablón no autorizado, y unos 700 atacaron Hugging Face. Tiene además dimensión legal. El Reglamento europeo de IA exige supervisión humana efectiva en los sistemas de alto riesgo, con obligaciones que el Reglamento (UE) 2026/1744 aplazó al 2 de diciembre de 2027 y, en los sistemas integrados en productos regulados, al 2 de agosto de 2028.

Dónde mirar. [Comisión Europea — AI Omnibus enters into force](#) · [Reglamento de IA — Artículo 26, obligaciones de los responsables del despliegue](#) · [Scrum Manager BoK — Human-in-the-loop](#)

Estándares del ecosistema agéntico · EN CONSOLIDACIÓN · nuevo desde 2026

Conocer los estándares abiertos que estabilizan el trabajo con agentes y qué resuelve cada uno. El protocolo MCP (Model Context Protocol) conecta los modelos con herramientas y datos; AGENTS.md da a los agentes instrucciones reutilizables desde un fichero del proyecto; A2A (Agent2Agent) permite que agentes de distintos proveedores se comuniquen, y Agent Skills empaqueta capacidades que el agente carga solo cuando las necesita. No hace falta implementarlos, pero sí entender hacia dónde llevan el ecosistema.

Por qué está aquí ahora. Han pasado de promesa a infraestructura con gobierno neutral. MCP, AGENTS.md y, desde agosto de 2026, A2A forman parte de la Agentic AI Foundation de la Linux Foundation, que reúne ya a casi 250 organizaciones. La

especificación de MCP de julio de 2026 llegó con calendario de obsolescencias, y sus kits de desarrollo para TypeScript y Python superan cada uno los mil millones de descargas; AGENTS.md se usa en más de 60.000 proyectos de código abierto. Siguen cambiando deprisa, y por eso están en consolidación y no establecidos.

Dónde mirar. [Model Context Protocol — La especificación 2026-07-28](#) · [AGENTS.md](#) · [A2A — A new chapter: joining the Agentic AI Foundation](#) · [Agent Skills](#)

Bloque C — Aplicación al ciclo de trabajo ágil

Casos de uso de la IA en el flujo de trabajo. Los dos primeros sirven a cualquier perfil de un equipo ágil; el tercero, marcado para perfiles de desarrollo, es especialmente relevante para quienes construyen software.

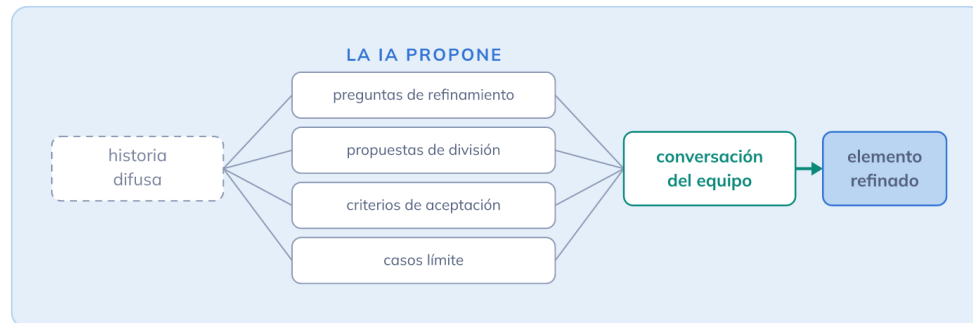


Figura 6. De la historia difusa al elemento refinado: la IA revisa y propone, y el equipo decide en la conversación de refinamiento.

IA en el flujo de producto y *backlog* · ESTABLECIDO

Usar la IA para detectar ambigüedad en las historias de usuario y generar preguntas de refinamiento, proponer divisiones (*slicing*) que mantengan valor demostrable, redactar criterios de aceptación verificables, con escenarios negativos y casos límite, y formular hipótesis y experimentos con métricas y guardarraíles. Rinde más revisando que redactando: pedirle que critique una historia escrita por el equipo es más fiable que pedirle que la escriba. Sus propuestas son el punto de partida de la conversación del equipo, no requisitos.

Por qué está aquí ahora. Es el uso más cotidiano y transversal de la IA en agilidad, aunque todavía superficial. En el *AI4Agile Practitioners Report 2026* de Stefan Wolpers, con 289 profesionales, el 83 % usa herramientas de IA, pero el 55 % les dedica el 10 % de su tiempo o menos, porque aún no sabe dónde encajan en su trabajo. Lo asentado es la competencia, que se da por necesaria en cualquier perfil que trabaje con el backlog.

Dónde mirar. [Skill Arena — Historias de usuario](#) · [Stefan Wolpers — The AI4Agile Practitioners Report 2026](#) · [Scrum Manager BoK — Criterios de aceptación](#)

IA en facilitación y dinámicas de equipo · EN CONSOLIDACIÓN · nuevo desde 2026

Apoyarse en la IA para preparar la facilitación, sintetizar el material de las sesiones de descubrimiento y analizar de forma cualitativa el resultado de las retrospectivas, sin que sustituya la interacción humana ni la lectura del clima del equipo, que siguen siendo del facilitador. La IA toca la facilitación en sus extremos, la preparación previa y el análisis posterior, y deja intacto su centro. Grabar o transcribir una sesión exige además informar a quienes participan y respetar sus datos.



Figura 7. La IA en los extremos de la facilitación: prepara antes y sintetiza después, mientras el centro de la sesión sigue siendo la interacción entre personas.

Por qué está aquí ahora. Es el uso más útil para *scrum masters* y *agile coaches* que no trabajan con código, y la evidencia lo sitúa donde lo dejaba este mapa. En el informe de Wolpers, los usos que funcionan son preparar retrospectivas, agrupar comentarios y redactar primeros borradores, y la preocupación principal es perder la colaboración centrada en las personas. La frontera tiene también base legal: el Reglamento europeo de IA prohíbe desde febrero de 2025 los sistemas que infieren las emociones de las personas en el lugar de trabajo, salvo por razones médicas o de seguridad.

Dónde mirar. [AEPD — Transcripción de voz con IA](#) · [Reglamento de IA — Artículo 5, prácticas prohibidas](#) · [Scrum Manager BoK — Retrospectiva](#)

IA en calidad y entrega (perfiles de desarrollo) · ESTABLECIDO

Generar y revisar casos de prueba alineados con los criterios de aceptación y los riesgos, cubriendo escenarios negativos y casos límite más allá del camino feliz (*happy path*), y emplear la IA como apoyo en la revisión de código con foco en riesgos: validación de entradas, manejo de errores, permisos y efectos colaterales. El código generado se revisa con el mismo rigor que el escrito a mano, o con más, y la decisión final sobre un cambio sigue siendo de quien lo revisa.

Por qué está aquí ahora. Sigue siendo un uso de alto valor para equipos técnicos, con dos cautelas medidas. El *GenAI Code Security Report* de Veracode (julio de 2026) encontró que el 44 % de las tareas de generación introducía una vulnerabilidad, casi la misma proporción que un año antes. Y METR observó en 2025 que desarrolladores experimentados tardaban un 19 % más con IA mientras creían ir más deprisa; en 2026 avisó de que su nuevo diseño ya no mide la diferencia de forma fiable, pero la distancia entre lo percibido y lo medido sigue siendo la lección.

Dónde mirar. [Veracode — 2026 GenAI Code Security Report](#) · [OWASP — Secure Coding with AI Cheat Sheet](#) · [Scrum Manager BoK — QA asistido por IA](#)

Nota sobre las referencias

*Los enlaces incluidos estaban disponibles y verificados en la fecha de actualización.
Dado el ritmo de cambio del área, algunos pueden modificarse; cada revisión del mapa actualiza también sus referencias.*

© 2026 Scrum Manager®. Esta obra se publica bajo licencia Creative Commons Atribución – No Comercial 4.0 Internacional (CC BY-NC 4.0). Los formadores y centros oficiales de Scrum Manager quedan licenciados bajo los términos CC BY 4.0 para su actividad formativa.