



# OWASP AIBOM

## Guía de Fundamentos

SEPTIEMBRE 2026



## Índice

|                                                                   |           |
|-------------------------------------------------------------------|-----------|
| <b>Resumen Ejecutivo.....</b>                                     | <b>7</b>  |
| <b>1. Comprender la AI Bill of Materials.....</b>                 | <b>8</b>  |
| <b>1.1 El AIBOM como artefacto de gobernanza .....</b>            | <b>9</b>  |
| <b>2. Qué es un AIBOM .....</b>                                   | <b>10</b> |
| <b>3. Por qué son importantes los AIBOM .....</b>                 | <b>13</b> |
| Factores de seguridad .....                                       | 13        |
| Factores regulatorios .....                                       | 14        |
| Factores de gobernanza .....                                      | 14        |
| Continuidad del negocio .....                                     | 15        |
| Amenazas de la cadena de suministro .....                         | 15        |
| <b>4. Componentes principales de un AIBOM .....</b>               | <b>16</b> |
| Componentes principales de un AIBOM.....                          | 16        |
| El encabezado .....                                               | 18        |
| La lista de componentes .....                                     | 18        |
| Los flujos de datos.....                                          | 18        |
| Zonas y límites de confianza .....                                | 20        |
| Comportamientos .....                                             | 20        |
| Qué permite hacer un AIBOM .....                                  | 20        |
| <b>5. Estructura del AIBOM.....</b>                               | <b>21</b> |
| Qué declara todo AIBOM.....                                       | 21        |
| Ejemplo desarrollado de un sistema de inferencia alojado .....    | 22        |
| Ejemplo desarrollado de una canalización de fine-tuning.....      | 25        |
| Qué no afirma el AIBOM .....                                      | 28        |
| Cómo se representa un AIBOM para quienes desean profundizar ..... | 28        |
| <b>6. AIBOM para sistemas de agentic AI.....</b>                  | <b>30</b> |
| Dependencias entre múltiples agentes.....                         | 30        |
| Herramientas asociadas .....                                      | 31        |
| Conectores de terceros.....                                       | 32        |
| Seguimiento del ecosistema MCP/A2A.....                           | 33        |
| <b>7. Hoja de ruta de adopción empresarial .....</b>              | <b>34</b> |
| Fase 1. Concienciación y situación de partida.....                | 36        |
| Fase 2. Proyecto piloto.....                                      | 37        |
| Fase 3. Integración en la gobernanza .....                        | 38        |
| Fase 4. Operación continua .....                                  | 39        |

# Introducción del líder del proyecto AIBOM

Durante mi etapa como copresidente de la iniciativa SBOM de CISA, dentro del DHS, la lección que más me marcó no tuvo que ver con los formatos de archivo, sino con lo que ocurre después de publicar el formato. Logramos que la industria del software generara SBOM a gran escala y luego vimos cómo la adopción se estancaba justo en ese punto, porque generarlos nunca fue la parte difícil. Lo difícil era construir la capa operativa a su alrededor y determinar quién utiliza el artefacto, qué decisión fundamenta, qué ocurre cuando queda desactualizado y quién responde cuando ni siquiera existe. AIBOM 101 se escribió teniendo presente esa lección. No es una referencia de esquemas. Es la capa operativa para los sistemas de IA que nunca llegamos a construir por completo para el software.

Una AI Bill of Materials (AIBOM) solo justifica su existencia si cambia lo que un equipo de seguridad, un auditor o una persona responsable de revisar adquisiciones puede hacer en la práctica. Por eso, este documento dedica tanta atención al alcance, las declaraciones sobre el grado de completitud y las evidencias como a los componentes y los flujos de datos. Un registro en el que nadie puede confiar y que nadie tiene la obligación de utilizar es un subproducto de ingeniería presentado como un instrumento de gobernanza, no una infraestructura. Nuestro objetivo con esta introducción es ofrecer a los responsables de seguridad empresarial algo que puedan poner en práctica de inmediato, es decir, una manera de preguntar qué IA tienen, de qué depende y si alguien puede responder por esas dependencias, con un lenguaje válido tanto en una reunión del consejo de administración como en una canalización de compilación.

Lo escribimos para que se lea, no solo para consultarlo. Los ejemplos desarrollados, un sistema de inferencia alojado y una canalización de fine-tuning, recorren el razonamiento que debe realizar quien elabora un AIBOM dónde se sitúa el límite del sistema, qué se considera evidencia y qué puede implicar una declaración sobre el grado de completitud. La hoja de ruta de adopción empresarial hace lo mismo en el plano organizativo parte de un inventario de sistemas de IA identificados, pasa por una prueba piloto y la integración en la gobernanza, y llega a una operación continua en la que los AIBOM se regeneran automáticamente ante eventos definidos. Cada fase tiene un criterio de salida comprobable, de forma deliberada, porque una hoja de ruta sin una manera de saber si se ha completado una fase es solo una aspiración.

También lo diseñamos para evolucionar. La agentic AI no es un caso excepcional del futuro; ya está transformando el significado de «dependencia», porque las llamadas a herramientas, las delegaciones a subagentes y las conexiones MCP de un sistema pueden decidirse durante la ejecución en lugar de quedar fijadas durante el diseño. En vez de tratarlo como una excepción que habría que incorporar después, diseñamos el AIBOM como un grafo desde el principio. Este se amplía de forma natural hacia lo que llamamos AgBOM identidades de agentes, permisos de herramientas y patrones de interacción entre múltiples agentes registrados con el mismo rigor que los modelos y los conjuntos de datos. La arquitectura está pensada para adaptarse a la evolución del campo, sin exigir una reescritura cada vez que aparece un patrón nuevo.

Nada de esto ocurre de forma aislada. Este documento es el resultado de las líneas de trabajo del proyecto OWASP AIBOM Requisitos, Buenas Prácticas, Integridad y Calidad, Inteligencia de Amenazas, Políticas, Contenido, Alianzas, Participación, Patrocinio y AgBOM, gestionadas como un sistema interconectado y no como esfuerzos separados. Cada línea de trabajo nos ha impulsado a mantener la precisión de la guía respecto de lo que un AIBOM puede y no puede afirmar. Hemos intentado expresar ese límite con claridad en todo el documento un AIBOM registra lo que contiene un sistema, no si es seguro o cumple los requisitos aplicables. Ese juicio corresponde al lector, con su propio marco de riesgos, y seguirá siendo así a medida que el proyecto madure. El proyecto, el trabajo sobre su esquema y las publicaciones en curso se encuentran en [owaspai bom.org](https://owaspai bom.org), y damos la bienvenida a quienes deseen contribuir en cualquiera de las líneas de trabajo mencionadas.

Si los SBOM enseñaron algo a la industria del software, es que un buen formato sin una disciplina operativa que lo acompañe termina siendo un artefacto olvidado. Nuestro objetivo es que eso nunca ocurra con el AIBOM. Espero que este documento les ofrezca un punto de partida para lograrlo en sus propias organizaciones.

Aruneesh Salhotra

Líder del proyecto OWASP AIBOM

[www.owaspai bom.org](http://www.owaspai bom.org)

## Alcance y público destinatario

Este documento es una introducción a la AI Bill of Materials (AIBOM) qué es, qué debe contener, cómo se elabora y valida, y cómo la adopta una organización. Está dirigido principalmente a quienes elaboran y utilizan AIBOM profesionales de ingeniería de IA y aprendizaje automático (ML), equipos de MLOps y plataformas, arquitectos de seguridad y especialistas en seguridad de productos y riesgos de la cadena de suministro. Está escrito para que una persona con poca o ninguna experiencia previa en AIBOM pueda leerlo de principio a fin; conocer las prácticas de SBOM para software resulta útil, pero no es un requisito.

También buscamos informar a los responsables de seguridad de la información (CISO), responsables de gobernanza de IA y altos directivos que responden por los riesgos de la cadena de suministro de IA. Les resultarán útiles la explicación de la importancia del AIBOM, los factores de seguridad, regulación y gobernanza que impulsan su adopción, la hoja de ruta por fases y los indicadores de madurez. Además, el documento aborda el contexto regulatorio y de gobernanza más amplio de los sistemas de IA, y puede ser útil para los equipos de cumplimiento, asuntos jurídicos, adquisiciones o riesgos de terceros que establecen requisitos de divulgación de AIBOM para proveedores.

Este documento describe la estructura del AIBOM en términos conceptuales y muestra cómo se corresponde con un formato BOM establecido y legible por máquinas. No es una referencia del esquema a nivel de campos; la especificación del formato sigue siendo la referencia autorizada para los detalles de codificación. Los lectores deben consultar su versión vigente en lugar de tratar los ejemplos de esta guía como un esquema. No proporciona una taxonomía de amenazas para sistemas de IA, una metodología de gestión de riesgos de IA ni instrucciones de implementación específicas de proveedores o herramientas. Esos contenidos se mantienen en recursos complementarios de OWASP y en las normas de referencia, citados a lo largo del documento.

## Copyright and License

© OWASP Foundation. This document is released under Creative Commons CC BY-SA 4.0. OWASP and the OWASP logo are trademarks of the OWASP Foundation. Contributors are credited in the Acknowledgements; contribution does not imply endorsement by any contributor's employer. Refer full License Text under <https://creativecommons.org/licenses/by-sa/4.0/legalcode>

# Resumen ejecutivo

La mayoría de las organizaciones no puede afirmar con certeza qué modelo se ejecuta en producción, rastrear los datos y los proveedores de origen que lo sustentan ni demostrar si una vulnerabilidad recién divulgada afecta a un sistema del que dependen. Los sistemas modernos de IA se ensamblan a partir de modelos de terceros, datos internos y bajo licencia, marcos de trabajo de código abierto, canalizaciones de recuperación de información, agentes, herramientas y servicios gestionados por proveedores. Muchos de ellos cambian sin que se publique una nueva versión local. El inventario tradicional de software no se diseñó para registrar estos artefactos que no son código y estos servicios externos; sin embargo, en ellos se determina gran parte del comportamiento de un sistema de IA y de su riesgo.

Un AI Bill of Materials (AIBOM) cubre esta carencia ofrece un registro estructurado y legible por máquinas de lo que contiene realmente un sistema de IA y de cómo circula la información por él. Por diseño, registra hechos en lugar de emitir una puntuación o un dictamen de cumplimiento. Esto le permite servir como una base común y verificable para decisiones de seguridad, gobernanza, adquisiciones y auditoría.

Para los responsables de seguridad, en particular, esto proporciona información práctica para actuar sobre decisiones que ya les corresponden. Un AIBOM transforma las dependencias opacas de los sistemas de IA en dependencias trazables y con responsables identificables; reduce la respuesta ante vulnerabilidades de semanas a horas, proporciona a los equipos de adquisiciones y riesgos de terceros un estándar concreto de divulgación que exigir a los proveedores y ofrece una base única y defendible de evidencias para las revisiones de gobernanza y los informes al consejo de administración. La adopción más eficaz no consiste en crear otro programa paralelo, sino en convertir el AIBOM en una entrada obligatoria de los controles ya existentes puntos de control de publicación, evaluaciones de proveedores, revisiones de riesgos de modelos y respuesta a incidentes. Así, un mismo registro sirve para seguridad, cumplimiento y auditoría sin elaborarse tres veces.

Este documento ofrece un punto de partida práctico para elaborar un AIBOM. Explica qué es y por qué se está convirtiendo en un requisito operativo en lugar de una práctica opcional; muestra su estructura y elaboración mediante ejemplos desarrollados; amplía el modelo para atender las exigencias adicionales de los sistemas de agentic AI; y establece una hoja de ruta por fases para su adopción en toda una empresa.

# 1. Comprender la AI Bill of Materials

Los sistemas de IA dependen de algo más que código. Un sistema en producción utiliza pesos de modelos, conjuntos de datos de entrenamiento y de fine-tuning (fine-tuning), adaptadores y puntos de control, instrucciones de entrada (prompts) y plantillas, corpus de recuperación de información, servicios de protección y moderación, marcos de orquestación y API gestionadas por proveedores. En conjunto, estos elementos forman la cadena de suministro de IA, que se diferencia de una cadena de suministro de software en un aspecto decisivo sus dependencias de mayor impacto con frecuencia ni siquiera son paquetes de software. Son artefactos que no son código y servicios operados externamente cuyo comportamiento puede cambiar sin que se publique una nueva versión local.

Estas dependencias no se concentran en una sola etapa. Se acumulan a lo largo del ciclo de vida. Durante el diseño, los equipos eligen proveedores de modelos y fuentes de datos. Durante el desarrollo, incorporan datos de fine-tuning, prompts y recursos de evaluación. Durante el despliegue, añaden infraestructura, controles de seguridad e integraciones. En producción, los sistemas dependen de corpus de recuperación que cambian continuamente, servicios de moderación que influyen de manera sustancial en las salidas y actualizaciones del proveedor que llegan según un calendario ajeno. Por tanto, una dependencia crítica puede incorporarse en cualquier etapa, y buena parte de ella queda fuera de la visibilidad directa de la organización que despliega el sistema.

Pensemos en un asistente empresarial construido sobre la API de un modelo fundacional alojado por un proveedor. Desde la perspectiva del equipo de la aplicación, nada ha cambiado los prompts, la configuración de recuperación y la infraestructura siguen igual. Sin embargo, los proveedores publican registros de cambios de sus API y mantienen políticas de ciclo de vida que distinguen modelos activos, obsoletos y retirados; además, un alias versionado puede pasar a apuntar a una instantánea más reciente. El modelo evaluado y aprobado puede dejar de ser el que determina el comportamiento en producción. Cuando cambia la calidad de las respuestas o se produce un incidente, el equipo no puede responder las tres primeras preguntas que se le plantean qué cambió, cuándo y si el cambio se originó en una dependencia previa de la cadena. La información necesaria nunca se registró.

La misma carencia aparece incluso sin un proveedor de alojamiento. Las canalizaciones de fine-tuning que no rastrean el linaje no pueden demostrar qué modelo base y qué datos produjeron un artefacto desplegado. Las fuentes de recuperación cambian sin control de versiones. Las capas de seguridad y moderación se tratan como detalles de implementación a pesar de su efecto en las salidas. El patrón es constante las organizaciones heredan capacidades sin heredar el conocimiento necesario para comprenderlas. Saben qué aplicación desplegaron, pero no pueden demostrar qué modelo de origen, conjunto de datos o capa de control determinó realmente su comportamiento.

Aquí es donde el inventario convencional de software llega a su límite. Un SBOM registra los componentes de software y sus versiones declaradas; esto sigue siendo necesario, pero no resulta suficiente. Determinar qué hará un sistema de IA exige conocer los modelos preentrenados, los datos utilizados para entrenarlos y evaluarlos, los resultados de evaluación que justificaron el despliegue y los servicios gestionados por proveedores que intervienen en el recorrido de las solicitudes. Ninguno de estos elementos es un componente de software en el sentido del SBOM. El inventario de software indica qué código está presente. La visibilidad de la cadena de suministro de IA también debe indicar qué artefactos distintos del código y qué servicios de etapas anteriores de la cadena influyeron de manera sustancial en el comportamiento, con suficiente información de provenance para reconstruir el estado del sistema en un momento determinado.

Los sistemas de agentic AI intensifican este problema. Cuando un agente selecciona herramientas, llama a servicios externos o delega en otros agentes durante la ejecución, el conjunto de dependencias deja de estar

fijado durante el diseño y surgen diferencias entre tres perspectivas lo que declara la configuración, lo que los permisos permiten alcanzar y lo que las trazas de ejecución muestran que se utilizó realmente.

## 1.1 El AIBOM como artefacto de gobernanza

Un AIBOM no es principalmente una comodidad de ingeniería. Es un artefacto de gobernanza un registro elaborado por una parte que asume responsabilidad, en un formato que otra parte puede leer más adelante y utilizar para actuar. La distinción importa porque quien lo lee no suele ser quien lo escribió y normalmente llega bajo presión un ingeniero de seguridad que delimita un incidente a las dos de la mañana, una persona que revisa la información divulgada por un proveedor durante una adquisición o un auditor que pregunta qué conjuntos de datos entrenaron un modelo que tomó una decisión cuestionada dieciocho meses antes. Cuatro propiedades hacen que un registro sea útil en esos momentos.

- Autoría con responsabilidad identificable: cada afirmación de un AIBOM la formula alguien. Los metadatos del documento registran quién lo elaboró, revisó y aprobó, cuándo y mediante qué método. Estos metadatos permiten distinguir un registro generado a partir de telemetría de compilación de otro redactado manualmente durante la revisión de una adquisición. Dos documentos pueden contener afirmaciones idénticas y justificar niveles de confianza muy diferentes.
- Alcance declarado y declaración sobre el grado de completitud explícita: un AIBOM indica qué abarca y qué confianza tiene quien lo elabora en que cubre ese alcance. Esto permite interpretar las omisiones. Sin una declaración sobre el grado de completitud, la ausencia de un conjunto de datos no demuestra nada; con ella, esa ausencia se convierte en una afirmación de quien elabora el documento en la que se puede confiar y que, si es incorrecta, se puede cuestionar. El capítulo 4 desarrolla estas descripciones del propio AIBOM.
- Afirmaciones vinculadas a evidencias: los hashes, las firmas, las model cards, los registros de conjuntos de datos y los resultados de evaluación se vinculan a afirmaciones individuales. Así, una afirmación se convierte en algo que quien utiliza el AIBOM puede comprobar de forma independiente. Un AIBOM no tiene que aportar evidencia de cada afirmación; cuando no existe, esa ausencia es información que el lector utiliza para decidir cuánto peso puede atribuirle.
- Un ciclo de vida controlado: un artefacto de gobernanza se versiona, revisa, aprueba, actualiza ante cambios sustanciales y conserva, incluso después de retirar el sistema que describe. Un AIBOM elaborado una sola vez y nunca actualizado describe un sistema que ya no existe; leerlo es peor que no tenerlo, porque genera una falsa confianza. El capítulo 7 establece las responsabilidades y los eventos de actualización que esto implica.

Estas propiedades permiten utilizar un AIBOM como evidencia en decisiones ya existentes evaluación de proveedores y requisitos contractuales de divulgación, controles de publicación, análisis del impacto de vulnerabilidades, delimitación de incidentes, revisión de riesgos de modelos y respuesta a requerimientos regulatorios o de auditoría.

**Qué no es un AIBOM** no es una puntuación, una calificación ni un grado de madurez; registra lo que contiene un sistema, no su calidad ni su nivel de seguridad. No afirma el cumplimiento de requisitos ni sustituye la evaluación, el modelado de amenazas o la evaluación de riesgos aporta información para esas actividades, y su valor depende de que se lleven a cabo. Tampoco constituye por sí mismo un control no bloquea nada hasta que una organización implementa un punto de control, una revisión o una consulta que utiliza su contenido. Un AIBOM que nadie utiliza es un subproducto de ingeniería presentado como un instrumento de gobernanza.

## 2. Qué es un AIBOM

Una AI Bill of Materials (AIBOM), también denominada SBOM para IA, es una descripción estructurada y legible por máquinas de un sistema de IA. Consta de cuatro partes: un encabezado que declara qué abarca el documento y cuál es su grado de completitud declarado; un inventario de los componentes y servicios del sistema, como modelos, conjuntos de datos, agentes y herramientas, guardrails y elementos del runtime; los flujos de datos dirigidos entre ellos; y las evidencias de origen, derechos, integridad y evaluación vinculadas a esas declaraciones.

El objetivo de un AIBOM es mejorar la transparencia y la confianza en toda la cadena de suministro de IA. Un AIBOM aporta visibilidad, lo que permite a las organizaciones inspeccionar y analizar cada componente de su ecosistema de IA. Refuerza las prácticas y los procesos de gestión de riesgos existentes y en desarrollo. Ayuda a identificar vulnerabilidades, evaluar riesgos de seguridad relacionados con la IA y rastrear la provenance de los modelos desde el desarrollo hasta el despliegue. Un AIBOM respalda los esfuerzos de la organización para cumplir los requisitos regulatorios y de gestión de riesgos aplicables.

### Objetivos principales

Un AIBOM proporciona un registro completo de los artefactos de IA y de los componentes del ciclo de vida de un sistema de IA durante su diseño, desarrollo y despliegue. Este registro puede servir como evidencia principal para auditorías de IA.

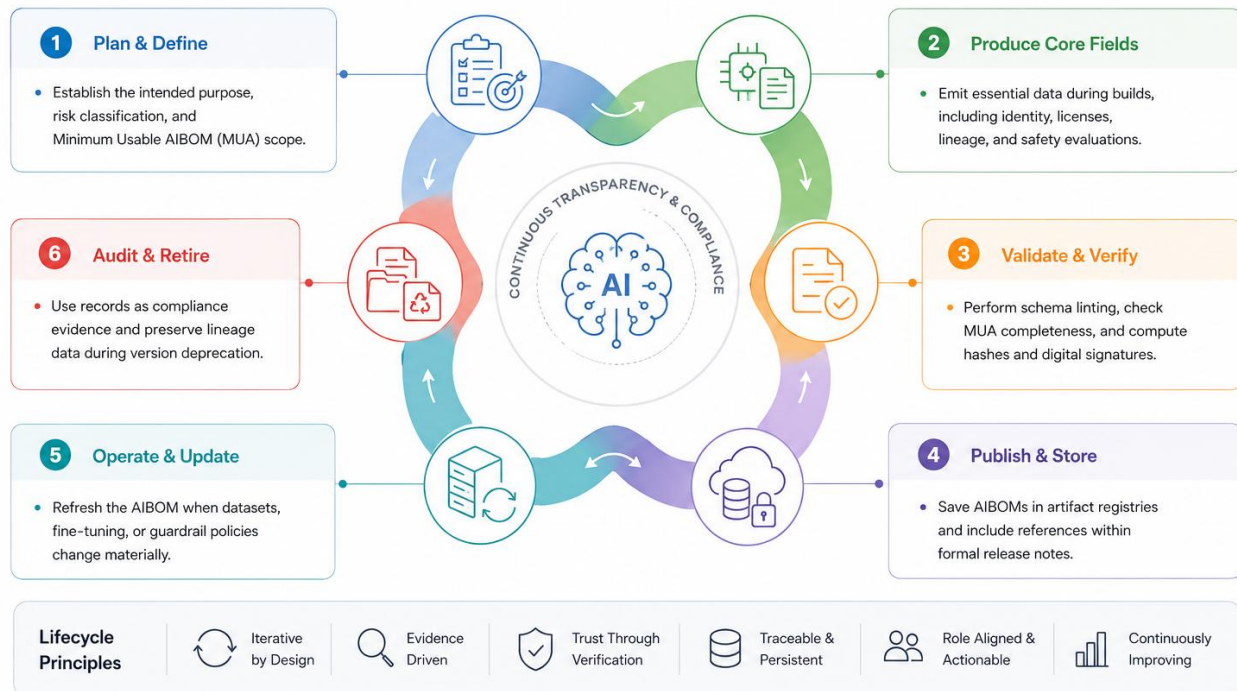
Los artefactos del AIBOM son componentes y activos del sistema de IA que incluyen licencias y obligaciones de uso de modelos y conjuntos de datos, provenance verificable y evidencias de evaluación. Algunos ejemplos son

- Modelos: resúmenes criptográficos (digests) del modelo base, licencias declaradas y determinadas tras su análisis, canales de distribución, firmas, modelos ajustados, adaptadores LoRA/PEFT y puntos de control.
- Conjuntos de datos: identificador y versión, hash, licencias, URL de origen, instantáneas, métodos de recopilación e información sobre datos sensibles y anonimización.
- Agentes y herramientas: orquestadores, API, extensiones y servidores MCP.
- Prompts y guardrails: plantillas, paquetes de políticas y notas de seguridad.
- Runtime: contenedores, dependencias y marcas de tiempo.
- Provenance de la compilación: resúmenes criptográficos de las imágenes compiladas, ubicaciones de las fuentes de entrada, argumentos de compilación y duración de la compilación.

Un objetivo central del AIBOM es sistematizar un proceso iterativo de documentación de los artefactos de los componentes de sistemas de IA durante el diseño, el desarrollo y el despliegue.

# The AIBOM Lifecycle: A Continuous Loop for AI Transparency

A continuous cycle of six iterative stages managing an AI Bill of Materials for compliance, safety, and traceability.



Source: OWASP AIBOM Project – AIBOM 101 v1

**Figura 1. Ciclo de vida del AIBOM**

El ciclo de vida del AIBOM es un ciclo continuo para la transparencia de la IA. Seis etapas iterativas para gestionar una AI Bill of Materials con fines de cumplimiento, seguridad y trazabilidad. Centro de la figura IA; transparencia y cumplimiento continuos.

| Elemento de la figura             | Traducción y contenido                                                                                                                                        |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Planificar y definir           | Establecer el propósito previsto, la clasificación del riesgo y el alcance del AIBOM mínimo utilizable (MUA).                                                 |
| 2. Generar los campos principales | Generar los datos esenciales durante las compilaciones, incluidos identidad, licencias, linaje y evaluaciones de seguridad.                                   |
| 3. Validar y verificar            | Comprobar la conformidad con el esquema, verificar que el MUA contenga todos los campos obligatorios y calcular hashes y firmas digitales.                    |
| 4. Publicar y almacenar           | Guardar los AIBOM en registros de artefactos e incluir referencias en las notas formales de la versión.                                                       |
| 5. Operar y actualizar            | Actualizar el AIBOM cuando cambien de forma sustancial los conjuntos de datos, el fine-tuning o las políticas de guardrails.                                  |
| 6. Auditar y retirar              | Utilizar los registros como evidencia de cumplimiento y preservar los datos de linaje al declarar obsoletas las versiones.                                    |
| Principios del ciclo de vida      | Iterativo por diseño; basado en evidencias; confianza mediante verificación; trazable y persistente; alineado con las funciones y aplicable; mejora continua. |

## Fases de elaboración de un AIBOM

- Planificar: definir el propósito previsto, el alcance, la clase de riesgo y el AIBOM mínimo utilizable (Minimum Usable AIBOM, MUA).
- Elaborar: generar los campos principales durante el entrenamiento y las compilaciones, incluidos, entre otros, identidad, licencias, provenance, linaje, evaluación y seguridad.
- Validar: comprobar los archivos con respecto al esquema, confirmar la completitud del MUA, calcular hashes y firmas, y verificar las licencias.
- Publicar: almacenar junto con el artefacto, en un registro o repositorio de artefactos, y mantener una referencia en las notas de la versión.
- Operar: actualizar ante cambios sustanciales, como cambios en conjuntos de datos, fine-tuning, licencias y políticas de guardrails nuevas o actualizadas.
- Auditar y retirar: utilizar el AIBOM como evidencia principal y preservar el linaje cuando las versiones se declaran obsoletas.

### 3. Por qué son importantes los AIBOM

Los sistemas modernos de IA rara vez se construyen de principio a fin por un solo equipo. Una arquitectura típica de producción obtiene un modelo base de un proveedor, lo adapta mediante fine-tuning con una combinación de datos internos y bajo licencia, integra componentes de código abierto y se conecta a datos en tiempo real mediante canalizaciones de recuperación. Cada capa tiene sus propios riesgos, licencias e interrogantes sobre la provenance.

Sin un inventario formal, las organizaciones a menudo no pueden responder preguntas fundamentales ¿qué versión del modelo está desplegada en producción?, ¿con qué datos se entrenó?, ¿alguno de sus componentes está afectado por una vulnerabilidad recién divulgada?, ¿la licencia es compatible con el uso comercial? Un AIBOM responde a estas preguntas al servir como una fuente de referencia consultable sobre lo que contiene realmente un sistema de IA.

El resto del documento examina los cinco factores principales que están convirtiendo el AIBOM de una idea útil en un requisito operativo.

#### Factores de seguridad

Los sistemas de IA introducen nuevas superficies de ataque que las herramientas tradicionales de seguridad de aplicaciones no se diseñaron para cubrir. Un AIBOM es la base de cualquier programa de seguridad de IA creíble porque indica a quienes lo defienden qué están protegiendo.

- Respuesta ante vulnerabilidades. Cuando se divulga una vulnerabilidad en un modelo, marco de trabajo o formato de serialización de uso extendido, como los ataques recurrentes mediante pickle que afectan a repositorios públicos de modelos, un AIBOM permite a los equipos de seguridad identificar la exposición en horas en lugar de semanas.
- Envenenamiento de modelos y datos. Los actores maliciosos pueden comprometer modelos de origen o conjuntos de datos de entrenamiento. Un AIBOM registra provenance, hashes e información de firma para que las manipulaciones puedan detectarse antes del despliegue.
- Detección de puertas traseras y troyanos. Conocer el linaje de cada artefacto de modelo, incluido quién lo entrenó y con qué datos, es esencial para evaluar el riesgo de comportamientos ocultos activados por entradas específicas.
- Filtración de secretos y prompts. Inventariar prompts, instrucciones del sistema y credenciales integradas ayuda a evitar exposiciones accidentales cuando los modelos se comparten o se someten a fine-tuning posteriores.
- Respuesta a incidentes. Cuando un sistema de IA produce una salida dañina o anómala, un AIBOM permite reconstruir exactamente qué se ejecutaba, con qué datos y con qué configuración en el momento del incidente.

## Factores regulatorios

El panorama regulatorio de la IA ha pasado de principios voluntarios a obligaciones exigibles en un periodo notablemente corto. Los AIBOM están surgiendo como un mecanismo práctico para demostrar el cumplimiento de varios marcos a la vez.

- Regulación específica de IA. Las regulaciones emergentes sobre IA exigen cada vez más que los sistemas de alto riesgo mantengan documentación técnica sobre datos de entrenamiento, arquitectura del modelo, métricas de rendimiento y limitaciones conocidas. Un AIBOM permite aplicar estos requisitos mediante un formato estándar.
- Marcos de gestión de riesgos de IA. Sus funciones principales exigen explícitamente inventarios documentados de componentes, datos y dependencias de IA como condición previa para evaluar riesgos.
- Contratación pública y directrices de organismos. Los organismos del sector público exigen cada vez más documentación de los sistemas de IA cuando los adquieren o despliegan, siguiendo el patrón de los requisitos de SBOM introducidos para el software tradicional.
- Normas sectoriales. Los reguladores financieros, las autoridades sanitarias y las autoridades de protección de datos están convergiendo en expectativas similares de divulgación para las decisiones basadas en IA.
- Transferencias transfronterizas. Cuando se aplican normas de residencia o soberanía de datos, un AIBOM proporciona la pista de auditoría necesaria para demostrar que los datos de entrenamiento y los componentes del modelo cumplen los requisitos jurisdiccionales.

## Factores de gobernanza

Históricamente, la gobernanza interna ha avanzado más lentamente que la adopción de IA. Muchas organizaciones descubren, a menudo durante una auditoría o un incidente, que nadie puede afirmar de manera concluyente qué modelos están en producción, quién es responsable de ellos o cómo se validaron. Los AIBOM proporcionan a las funciones de gobernanza un artefacto concreto en el que fundamentar políticas, revisiones y aprobaciones.

- Gestión del ciclo de vida del modelo. Un AIBOM rastrea cada versión, fine-tuning y despliegue de un modelo y sustituye el conocimiento informal por registros auditables.
- Revisión de sesgos, equidad y ética. No se puede evaluar si un modelo es adecuado para la contratación de personal, la concesión de préstamos o la atención sanitaria sin conocer los datos con los que se entrenó. El AIBOM aporta información para esas evaluaciones.
- Cumplimiento de licencias y propiedad intelectual. Los modelos y conjuntos de datos tienen licencias diversas algunas permisivas, otras restrictivas y otras con dudas sin resolver sobre los derechos de autor de los datos de entrenamiento. Identificar estas obligaciones a tiempo evita correcciones costosas después.
- Riesgos de terceros y proveedores. Cuando las capacidades de IA se obtienen de proveedores, un AIBOM forma parte cada vez más de la diligencia debida, junto con informes SOC 2 y cuestionarios de seguridad.
- Visibilidad para el consejo de administración. Los datos agregados de los AIBOM permiten a los directivos y al consejo ver el conjunto de la IA de la organización en una sola vista, en lugar de consultar artefactos dispersos de cada proyecto.

## Continuidad del negocio

Los sistemas de IA suelen volverse críticos sin que resulte evidente. Un motor de recomendaciones, un modelo de detección de fraude o un procesador de documentos puede pasar de una prueba piloto a una infraestructura esencial en cuestión de meses. Cuando algo falla, el costo de no tener un AIBOM se mide en tiempo de inactividad, pérdida de ingresos y daño reputacional.

- **Reproducibilidad.** Si un modelo de producción se pierde, se corrompe o necesita volver a entrenarse, un AIBOM registra las entradas, los parámetros y las dependencias necesarios para reconstruirlo de forma predecible.
- **Fallo del proveedor u obsolescencia.** Cuando un proveedor de modelos cierra un servicio, cambia sus precios o declara obsoleto un modelo, un AIBOM indica qué sistemas se ven afectados y qué alternativas son compatibles.
- **Deriva y degradación.** Rastrear las versiones de modelos y datos a lo largo del tiempo permite relacionar las caídas de calidad con cambios concretos, en lugar de hacer suposiciones.
- **Requerimientos regulatorios de conservación y auditorías.** Cuando los reguladores o tribunales exigen evidencia de lo que hacía un sistema en una fecha determinada, un AIBOM proporciona el registro histórico.
- **Planificación de la recuperación ante desastres.** Los objetivos de tiempo de recuperación y punto de recuperación de los sistemas de IA solo tienen sentido si los componentes necesarios para restaurarlos están inventariados y disponibles.

## Amenazas de la cadena de suministro

La cadena de suministro de IA es más amplia, profunda y menos madura que la cadena de suministro tradicional de software. Los componentes se obtienen de plataformas públicas de modelos, repositorios de conjuntos de datos y API de inferencia con distintos niveles de buenas prácticas de seguridad. Los AIBOM aportan suficiente visibilidad de la cadena como para defenderla.

- **Repositorios públicos de modelos comprometidos.** Las plataformas públicas han alojado repetidamente modelos con código malicioso en sus formatos de serialización. Un AIBOM con hashes verificados permite detectar esta clase de ataque.
- **Typosquatting (suplantación mediante nombres similares) y suplantación de identidad.** Los atacantes publican modelos o paquetes con nombres similares a los legítimos para provocar su descarga accidental. El seguimiento de la provenance en un AIBOM es la defensa principal.
- **Contaminación de conjuntos de datos.** Los datos de entrenamiento o fine-tuning procedentes de la web pública pueden contener material envenenado introducido de forma deliberada. Catalogar las fuentes de los conjuntos de datos y los pasos de procesamiento es el punto de partida para detectarlo.
- **Dependencias transitivas.** Cada modelo incorpora dependencias previas de la cadena, como tokenizadores, pesos base y bibliotecas de apoyo. Los AIBOM hacen explícitas estas relaciones transitivas.
- **Riesgos internos y de desarrolladores.** Las canalizaciones internas de fine-tuning y etiquetado de datos pueden introducir riesgos mediante contribuciones no verificadas. Los controles basados en AIBOM aplican a los artefactos internos el mismo rigor que a los externos.

## 4. Componentes principales de un AIBOM

### Componentes principales de un AIBOM

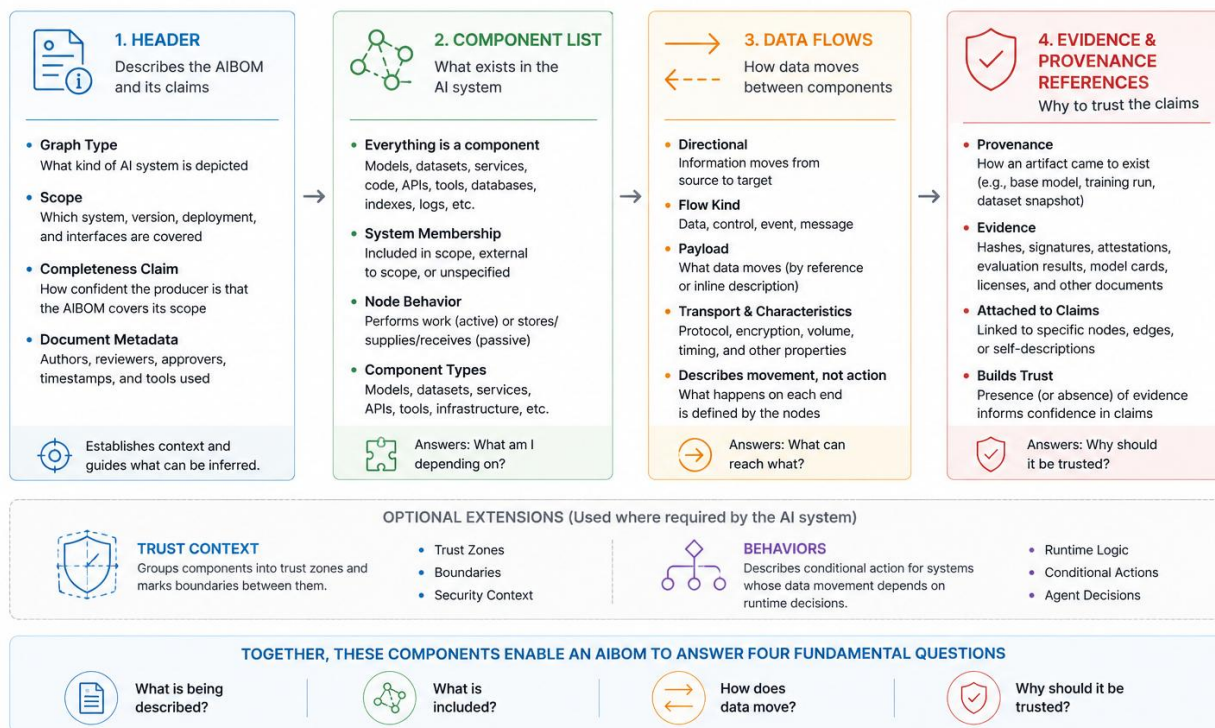
Los capítulos anteriores explicaron qué es un AIBOM y por qué importa. Este capítulo presenta sus partes y la función de cada una, para que el lector sepa qué debe incluir y por qué.

En términos estructurales, un AIBOM tiene cuatro partes un encabezado, una lista de componentes, flujos de datos dirigidos y referencias de evidencias y provenance. Todo AIBOM contiene las cuatro. Dos tipos de contenido opcional completan la descripción cuando el sistema los requiere el contexto de confianza, que agrupa componentes en zonas y marca sus límites, y los comportamientos, que describen acciones condicionales en sistemas cuyos movimientos de datos dependen de decisiones tomadas durante la ejecución. Este capítulo recorre cada parte, la relaciona con su propósito y concluye con lo que permite hacer un AIBOM terminado.

### Core Components of an AIBOM

An AIBOM describes AI systems, how data moves, and why claims can be trusted.

Owasp  
AIBOM



Source: OWASP AIBOM Project – AIBOM 101 v1

Figura 2. Componentes principales de un AIBOM

Un AIBOM describe sistemas de IA, cómo se mueven los datos y por qué se puede confiar en sus afirmaciones. La figura presenta cuatro partes principales y dos extensiones opcionales.

| Elemento de la figura                     | Traducción y contenido                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Encabezado                             | Describe el AIBOM y sus afirmaciones. Tipo de grafo: qué clase de sistema de IA se representa. Alcance: sistema, versión, despliegue e interfaces cubiertos. Declaración sobre el grado de completitud: confianza de quien lo elabora en que cubre su alcance. Metadatos: autores, revisores, aprobadores, marcas de tiempo y herramientas utilizadas. Establece el contexto y orienta las inferencias.                                                                                                  |
| 2. Lista de componentes                   | Indica qué existe en el sistema de IA. Todo es un componente: modelos, conjuntos de datos, servicios, código, API, herramientas, bases de datos, índices, registros, etc. Pertenencia al sistema: incluido en el alcance, externo o sin especificar. Comportamiento del nodo: realiza trabajo (activo) o almacena, suministra o recibe información (pasivo). Tipos de componentes: modelos, conjuntos de datos, servicios, API, herramientas, infraestructura, etc. Responde: ¿de qué estoy dependiendo? |
| 3. Flujos de datos                        | Indican cómo se mueven los datos entre componentes. Son dirigidos: del origen al destino. Clases: datos, control, evento o mensaje. Carga útil: qué datos circulan, por referencia o descripción incluida en el flujo. Transporte y características: protocolo, cifrado, volumen, momento y otras propiedades. Describen movimiento, no acción; los nodos definen lo que ocurre en cada extremo. Responden: ¿qué puede llegar a qué?                                                                     |
| 4. Referencias de evidencias y provenance | Explican por qué confiar en las afirmaciones. Provenance: cómo se originó el artefacto, por ejemplo, modelo base, ejecución de entrenamiento o instantánea de datos. Evidencias: hashes, firmas, atestaciones, resultados de evaluación, model cards, licencias y otros documentos. Se vinculan a afirmaciones de nodos, aristas o descripciones del propio AIBOM específicos. La presencia o ausencia de evidencias informa la confianza. Responden: ¿por qué debería confiarse en ello?                |
| Extensión opcional: contexto de confianza | Agrupa componentes en zonas de confianza y marca sus límites. Incluye zonas de confianza, límites y contexto de seguridad. Se utiliza cuando el sistema de IA lo requiere.                                                                                                                                                                                                                                                                                                                               |
| Extensión opcional: comportamientos       | Describe acciones condicionales en sistemas cuyos movimientos de datos dependen de decisiones durante la ejecución. Incluye lógica de ejecución, acciones condicionales y decisiones de agentes.                                                                                                                                                                                                                                                                                                         |
| Cuatro preguntas fundamentales            | ¿Qué se describe? ¿Qué se incluye? ¿Cómo se mueven los datos? ¿Por qué debería confiarse en ello?                                                                                                                                                                                                                                                                                                                                                                                                        |

## El encabezado

El encabezado del AIBOM describe qué tipo de sistema de IA se está modelando y qué se puede afirmar sobre su alcance y completitud. Esta información aporta contexto para leer el resto del documento. El AIBOM de una organización puede ser una representación completa de un único sistema desplegado, generada automáticamente a partir de telemetría de compilación. El de otra puede ser un bosquejo parcial de un sistema futuro, redactado manualmente durante la revisión de una adquisición. Sin una forma de distinguirlos, el lector no puede extraer las inferencias correctas de ninguno de los dos.

**Por ello, todo AIBOM comienza con tres descripciones de sí mismo:** (1) el tipo de grafo indica qué clase de sistema representa, como un modelo individual, un sistema en ejecución, una extensión del sistema como un servidor MCP o una canalización de entrenamiento; (2) el alcance indica qué pretende abarcar: qué sistema, versión, despliegue e interfaces; (3) la declaración sobre el grado de completitud indica qué confianza tiene quien lo elabora en que cubre lo declarado en su alcance, desde «completo para el alcance declarado», pasando por una cobertura parcial, hasta «no sabemos qué más hay aquí». Junto con estas descripciones, los metadatos estándar registran quién elaboró, revisó y aprobó el AIBOM, cuándo y con qué herramientas. Esos metadatos permiten distinguir un registro generado automáticamente de un bosquejo manual.

La declaración sobre el grado de completitud orienta las conclusiones que el lector puede extraer de la ausencia de información. Si un AIBOM no incluye un conjunto de datos determinado ni declara estar completo, esa ausencia no demuestra nada. Es posible que el conjunto de datos se utilice, pero simplemente no figure en el documento. Sin embargo, si el AIBOM declara estar completo para el alcance definido, la ausencia adquiere significado constituye una afirmación de quien lo elabora de que ningún conjunto de datos de ese tipo interviene dentro de dicho alcance.

Esta asimetría entre las inferencias basadas en la presencia y en la ausencia de información explica por qué la descripción del propio grafo debe preceder a su contenido. Sin alcance ni completitud, dos lectores pueden examinar el mismo AIBOM y llegar a conclusiones opuestas sobre lo que expresa. Las demás secciones de este capítulo presuponen que cada AIBOM incluye las tres descripciones, aunque el texto no las repita.

## La lista de componentes

Un sistema de IA está formado por diversos componentes interrelacionados. Son los «materiales» de la AI Bill of Materials. En un AIBOM, todo elemento del sistema es un componente, incluidos los servicios un módulo de código independiente, un microservicio, un conjunto de datos y un punto de conexión de API alojado por un proveedor son componentes. Se distinguen por su tipo, no mediante listas separadas. La lista de componentes responde a la primera pregunta de toda persona que revisa un sistema ¿de qué estoy dependiendo?

**Más allá de su identidad, dos aspectos describen un nodo, a saber, su pertenencia al sistema y su comportamiento.** La pertenencia indica si el nodo se considera parte integrante del sistema de IA descrito, externo a él o sin especificar. Es una declaración relativa al alcance y se registra de forma estructural el alcance declarado del AIBOM enumera qué componentes se incluyen en el sistema descrito y cuáles se excluyen. No equivale a propiedad ni a control. Un modelo alojado por un tercero puede ser parte integrante del sistema de IA descrito, y una base de datos operada internamente puede quedar fuera de su límite si no forma parte del alcance declarado. Un componente incluido en dicho alcance es un elemento constitutivo del sistema descrito.

Por su parte, el comportamiento del nodo indica qué función desempeña en el grafo. Algunos nodos realizan trabajo. Un procesador de prompts transforma texto. Un modelo genera salidas. Un agente decide a qué llamar después. Un guardrail filtra contenido. Un servicio de recuperación ordena candidatos por relevancia. Otros nodos principalmente almacenan, suministran o reciben información, como conjuntos de datos, índices, registros y almacenes de datos. Un nodo que no procesa directamente la información puede anotarse, a efectos

informativos, como componente «pasivo», o esa condición puede inferirse del patrón de flujos de datos que lo conectan.

Los modelos alojados se encuentran entre los componentes de tipo servicio más importantes en muchos AIBOM, aunque existen muchos otros. Un componente de servicio puede permitir que un modelo o una aplicación de IA acceda a datos, herramientas o sistemas mediante una API de red. El AIBOM registra estos componentes para que el lector pueda ver qué partes del sistema intercambian datos y dónde se cruzan sus límites.

## Los flujos de datos

Los flujos de datos de un AIBOM conectan sus componentes. Si los componentes son la «lista de piezas», los flujos de datos son el «diagrama de construcción» o «diagrama de conexiones» que muestra cómo encajan. Los flujos de datos siempre tienen dirección porque muestran el movimiento de información de un componente a otro. Cuando la información circula en ambas direcciones entre dos componentes, como una solicitud y su respuesta, cada movimiento relevante constituye un flujo propio.

Si la lista de componentes responde de qué estoy dependiendo, los flujos responden a la pregunta que distingue a los sistemas de IA: ¿qué puede llegar a qué? Un mismo modelo tiene un perfil de riesgo completamente distinto según si los datos de clientes pueden llegar a él sin filtrar y adónde se dirige su salida. Una lista de piezas no puede expresar esa diferencia. En los sistemas de IA, el riesgo reside en las conexiones.

Cada flujo puede incluir información sobre lo que circula por él. Declara su clase flujo de datos, flujo de control, evento o mensaje. También puede describir la carga útil que transporta, mediante referencias a objetos de datos descritos en otra parte del AIBOM o mediante un descriptor incluido en el propio flujo cuando su carga útil difiere de cualquier otra descrita. Un flujo también puede registrar cómo ocurre el movimiento si está cifrado, mediante qué protocolo, con qué volumen y en qué momentos.

Lo que un flujo no contiene es una descripción de lo que el componente receptor hace con los datos. Un modelo que genera una salida, un servicio de recuperación que ordena candidatos, un guardrail que filtra contenido o una base de datos que almacena lo recibido representan comportamientos de nodos. Se describen en el nodo, mediante su tipo de componente y sus metadatos, no como anotaciones del flujo. El flujo registra que los datos se movieron de un lugar a otro; los nodos explican qué ocurre en cada extremo.

## Referencias de evidencias y provenance

El encabezado, los componentes y servicios, y las aristas de flujo de datos indican qué contiene el sistema y cómo circula la información por él. Las referencias de evidencias y provenance indican por qué el lector debería creer esas afirmaciones y dónde puede comprobarlas. No constituyen un grafo separado; se vinculan a nodos, aristas y descripciones del propio AIBOM específicos.

Dos tipos de vínculos son especialmente importantes. La provenance registra cómo se originó un artefacto de qué modelo base deriva un modelo ajustado, qué ejecución de entrenamiento lo produjo o qué instantánea de un conjunto de datos alimentó un índice de recuperación. La evidencia registra el respaldo de una afirmación un hash criptográfico que permite comprobar la integridad de un componente, una firma o attestation una declaración formal que vincula un artefacto con la compilación que lo produjo, un resultado de evaluación o un documento externo, como una model card o un archivo de licencia.

Como estas referencias se vinculan a afirmaciones individuales, interactúan directamente con la declaración sobre el grado de completitud del encabezado. Un componente declarado sin ninguna referencia de evidencia es una mera afirmación; el mismo componente acompañado de un hash, una firma y un enlace a su model card constituye una afirmación que quien utiliza el AIBOM puede verificar de forma independiente. Un AIBOM no tiene

que adjuntar evidencia a cada afirmación, pero la presencia o ausencia de evidencias es información que el lector utiliza para decidir cuánto peso puede atribuir a un nodo o una arista.

Los elementos que se registran en estas cuatro partes metadatos de modelos, provenance de conjuntos de datos, entorno de entrenamiento, dependencias y bibliotecas, API y cadenas de herramientas, configuración del entorno de ejecución (runtime) y descriptores de agentes y subagentes para sistemas de agentic AI no constituyen otra lista que haya que mantener. Cada uno es un nodo, una propiedad de un nodo, una arista o una referencia de evidencia vinculada a alguno de ellos.

## **Zonas y límites de confianza**

No todos los componentes están en el mismo lugar ni bajo el mismo control. Un AIBOM puede agruparlos en zonas con distintos niveles de confianza, como la infraestructura del propio equipo, la red empresarial más amplia, la nube de un proveedor o internet público. El punto en el que un flujo pasa de una zona a otra constituye un límite, y es en esos límites donde se concentra la atención de la revisión. Allí los datos cambian de manos, se aplican controles como autenticación y cifrado, y termina la visibilidad de quien elabora el documento.

Las zonas hacen explícita una diferencia que un grafo sin ellas oculta. Un flujo entre dos componentes internos y otro que lleva la misma carga útil a una API de terceros parecen aristas similares, pero representan hechos muy distintos. Sin zonas declaradas, distinguirlos depende del conocimiento previo del lector sobre qué nombres son internos. Con ellas, el propio AIBOM indica qué movimientos permanecen dentro y cuáles salen, y por qué controles debe pasar cada salida.

## **Comportamientos**

Los flujos indican qué puede llegar a qué. Los comportamientos indican cuándo y bajo qué condiciones. En una canalización lineal, los flujos suelen bastar porque los mismos movimientos ocurren para cada solicitud. Los sistemas de agentic AI son diferentes. A menudo, lo relevante de un agente es que decide durante la ejecución si debe actuar llamar a una herramienta, consultar una base de datos o transferir la tarea a otro agente. Un flujo por sí solo puede exagerar lo que ocurre, dando a entender que la herramienta se invoca siempre, o describirlo de forma insuficiente, dejando la conexión sin registrar. Una descripción de comportamiento recoge la parte condicional qué activa una acción, qué puede hacer el componente en respuesta y qué sucede a continuación. La mayoría de los AIBOM no necesitará descripciones de comportamiento; los sistemas cuyo riesgo depende de decisiones tomadas durante la ejecución sí las necesitarán. El capítulo sobre sistemas de agentic AI retoma este tema.

## **Qué permite hacer un AIBOM**

Todo lo descrito en este capítulo son hechos estructurados, y cada elemento componente, flujo, zona y límite tiene un identificador estable. Esto distingue un AIBOM de un diagrama de arquitectura otros artefactos pueden señalar un elemento concreto e inequívoco dentro de él.

El resto de los mecanismos de gobernanza se apoya en esa capacidad de referencia. Los modelos de amenazas, registros de riesgos, correspondencias de controles y declaraciones de vulnerabilidades no vuelven a describir el sistema; hacen referencia al grafo del AIBOM. Una amenaza puede indicar que una ruta de ataque cruza un límite específico. Un control puede indicar qué flujo protege. Un análisis de vulnerabilidades puede señalar que una debilidad no es alcanzable porque los controles de una zona bloquean la ruta. El grafo se construye una vez y los análisis se vinculan a él; siguen vinculados y siendo comprobables a medida que el sistema evoluciona.

El propio AIBOM se mantiene dentro de ese límite. Registra qué es el sistema, no si resulta aceptable. El cumplimiento, la aceptación del riesgo y la suficiencia de los controles son juicios que el lector formula con su propio marco de políticas a partir de los hechos que aporta el AIBOM.

## 5. Estructura del AIBOM

El capítulo Componentes principales de un AIBOM presentó sus cuatro partes encabezados, componentes y servicios, aristas de flujo de datos y referencias de evidencias y provenance como un modelo abstracto. Este capítulo concreta ese modelo. Desarrolla ejemplos de un sistema de inferencia alojado, una canalización de fine-tuning y una ejecución de principio a fin que genera un AIBOM para un modelo publicado; expone con claridad qué afirma y qué no afirma un AIBOM; e introduce los niveles y las capas de codificación que necesita quien va a generarlo.

Las tres descripciones del propio AIBOM en el encabezado tipo de grafo, método de generación, alcance y completitud se dan por supuestas y no se vuelven a desarrollar aquí; véase El encabezado en Componentes principales de un AIBOM. Ningún otro elemento del AIBOM puede interpretarse sin ellas, por lo que cada ejemplo se presenta como si su encabezado ya estuviera definido, aunque el texto no lo repita.

### Qué declara todo AIBOM

Antes de leer un AIBOM, es necesario saber de qué tipo de AIBOM se trata.

Las mismas palabras pueden describir artefactos muy diferentes. El AIBOM de una organización puede ser una representación completa de un único sistema desplegado, generada automáticamente a partir de telemetría de compilación. El de otra puede ser un bosquejo parcial de un sistema futuro, redactado manualmente durante la revisión de una adquisición. Sin una manera de distinguirlos, el lector no puede extraer inferencias correctas de ninguno de los dos.

Por ello, todo AIBOM comienza con tres descripciones de sí mismo

**El tipo de grafo indica si el AIBOM representa un modelo individual, un conjunto de datos individual, un sistema en ejecución, una canalización de entrenamiento u otro artefacto bien definido.** Indica al lector qué tipos de nodos y flujos debe esperar.

**El alcance indica qué sistema, versión, despliegue e interfaces pretende abarcar el AIBOM.** El alcance importa porque todas las demás afirmaciones del AIBOM son relativas a él.

La declaración sobre el grado de completitud indica qué confianza tiene quien elabora el AIBOM en que cubre lo establecido en su alcance. La completitud va desde «completo para el alcance declarado», pasando por una cobertura parcial, hasta «no sabemos qué más hay aquí».

Junto con estas descripciones, los metadatos del AIBOM registran quién lo elaboró, revisó y aprobó, cuándo, con qué herramientas y durante qué periodo de validez. Esos metadatos permiten distinguir un AIBOM redactado manualmente durante la revisión de una adquisición de uno generado a partir de la configuración de compilación o de telemetría de ejecución. En ellos se identifica a la persona o parte responsable de las afirmaciones del documento.

La declaración sobre el grado de completitud cumple una función mayor de lo que parece. Determina qué puede concluir el lector de la ausencia de información. Si un AIBOM no incluye un conjunto de datos concreto ni declara estar completo, esa ausencia no demuestra nada, ya que el conjunto de datos podría estar en uso y simplemente no figurar en el documento. Si el AIBOM declara estar completo para el alcance definido, la ausencia adquiere

significado constituye una afirmación de quien lo elabora de que ningún conjunto de datos de ese tipo interviene dentro de dicho alcance.

Esta asimetría entre las inferencias basadas en la presencia y en la ausencia de información explica por qué la descripción del propio grafo debe preceder a su contenido. Sin alcance ni completitud, dos lectores pueden examinar el mismo AIBOM y llegar a conclusiones opuestas sobre lo que expresa.

Las demás secciones de este capítulo presuponen que cada AIBOM contiene estas tres descripciones, aunque el texto no las repita.

## **Ejemplo desarrollado de un sistema de inferencia alojado**

Pensemos en un asistente empresarial de atención al cliente. Un cliente escribe una pregunta en una interfaz web. La aplicación prepara un prompt, recupera documentación interna pertinente, comprueba que la entrada no contenga contenido inseguro, envía el prompt a un modelo de lenguaje de gran tamaño alojado por un proveedor, procesa la respuesta y la devuelve al cliente.

El AIBOM de este sistema contiene los siguientes nodos

Un servicio de atención al usuario recibe la consulta del cliente. Es un componente de tipo servicio operado por el equipo del asistente.

Un procesador de prompts prepara el prompt final. Aplica plantillas, oculta información personal, gestiona el contexto de la sesión y decide qué recuperar. El equipo es responsable de este componente.

Un servicio de recuperación almacena representaciones vectoriales (embeddings) de la documentación interna de soporte y devuelve los fragmentos pertinentes. El equipo lo opera en infraestructura interna. El corpus subyacente, una instantánea de la base de conocimientos interna de soporte correspondiente a una fecha concreta, se referencia como un componente de conjunto de datos.

Un servicio de moderación comprueba si la entrada del cliente contiene material con el que el asistente debería negarse a interactuar. En este ejemplo, el equipo está suscrito a una API de moderación de terceros.

Un modelo de lenguaje alojado genera la respuesta del asistente. El equipo accede a él mediante la API del proveedor. Es el nodo más interesante del grafo y se retoma más adelante.

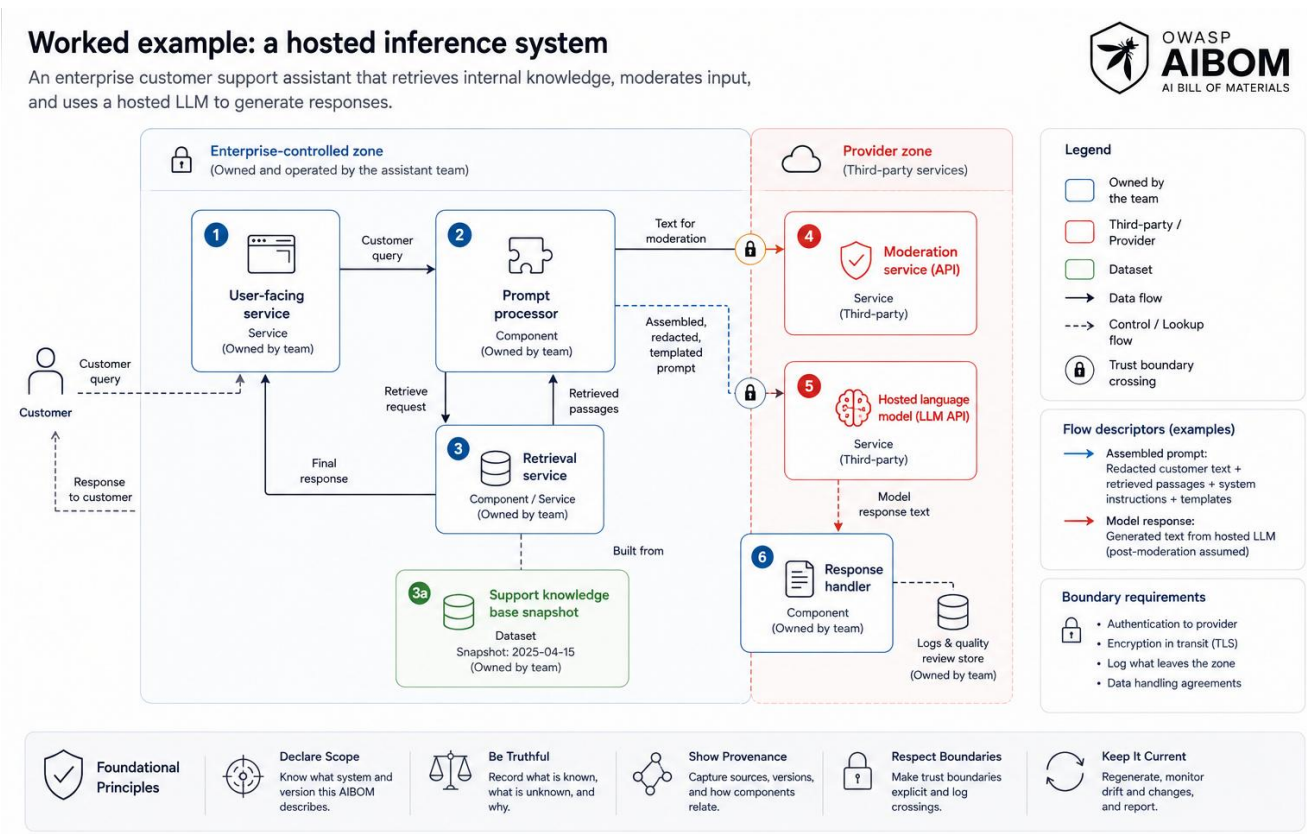
Un gestor de respuestas procesa la salida del modelo al darle formato, registrar el intercambio para una revisión de calidad y devolver el texto final al servicio de atención al usuario.

El AIBOM conecta estos nodos mediante flujos de datos dirigidos. La consulta del cliente pasa del servicio de atención al usuario al procesador de prompts. El procesador envía texto al servicio de moderación, recupera fragmentos del servicio de recuperación y envía el prompt preparado al modelo de lenguaje alojado. El modelo devuelve texto al gestor de respuestas. Este devuelve texto al servicio de atención al usuario, que a su vez lo entrega al cliente.

Cada flujo contiene información sobre lo que circuló por él. El prompt enviado al modelo alojado no es la consulta original del cliente, ya que se ha enriquecido con información recuperada, se ha ocultado información personal y se han aplicado plantillas. El flujo que lo transporta puede incluir una descripción de la carga útil que circuló por ese flujo concreto, en lugar de depender de una descripción genérica de la salida del procesador de prompts. Los descriptores por flujo son importantes cuando la carga útil de una etapa difiere sustancialmente de la de otra.

El ejemplo también incorpora contexto de confianza. El servicio de atención al usuario, el procesador de prompts, el servicio de recuperación y el gestor de respuestas están en una zona controlada por el equipo. La API de moderación y el modelo de lenguaje alojado están en zonas de proveedores. Los dos flujos que salen de la zona del equipo la comprobación de moderación y el prompt preparado cruzan límites declarados. Cada límite registra

los requisitos para atravesarlo, entre ellos la autenticación ante el proveedor, el cifrado en tránsito y el registro de lo que salió. El flujo del prompt merece el mayor escrutinio, y el propio grafo explica por qué lleva texto del cliente con información personal ocultada y documentación interna recuperada a través de un límite hacia una infraestructura que el equipo no puede observar.



Source: OWASP AIBOM Project – AIBOM 101 v1

Figura 3. Ejemplo de un sistema de inferencia alojado

Un asistente empresarial de atención al cliente recupera conocimiento interno, modera las entradas y utiliza un modelo de lenguaje de gran tamaño (LLM) alojado para generar respuestas. Las siguientes correspondencias permiten leer los rótulos del diagrama original.

| Elemento de la figura               | Traducción y contenido                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Zonas y actores                     | Cliente. Zona controlada por la empresa: propiedad y operación del equipo del asistente. Zona del proveedor: servicios de terceros.                                                                                                                                                                                                                                                                 |
| 1. User-facing service              | Servicio de atención al usuario. Servicio propiedad del equipo.                                                                                                                                                                                                                                                                                                                                     |
| 2. Prompt processor                 | Procesador de prompts. Componente propiedad del equipo.                                                                                                                                                                                                                                                                                                                                             |
| 3. Retrieval service                | Servicio de recuperación. Componente o servicio propiedad del equipo.                                                                                                                                                                                                                                                                                                                               |
| 3a. Support knowledge base snapshot | Instantánea de la base de conocimientos de soporte. Conjunto de datos. Instantánea: 2025-04-15. Propiedad del equipo.                                                                                                                                                                                                                                                                               |
| 4. Moderation service (API)         | Servicio de moderación (API). Servicio de terceros.                                                                                                                                                                                                                                                                                                                                                 |
| 5. Hosted language model (LLM API)  | Modelo de lenguaje alojado (API de LLM). Servicio de terceros.                                                                                                                                                                                                                                                                                                                                      |
| 6. Response handler                 | Gestor de respuestas. Componente propiedad del equipo.                                                                                                                                                                                                                                                                                                                                              |
| Logs & quality review store         | Almacén de registros y revisión de calidad. Propiedad del equipo.                                                                                                                                                                                                                                                                                                                                   |
| Rótulos de las conexiones           | Consulta del cliente; respuesta al cliente; solicitud de recuperación; fragmentos recuperados; texto para moderación; prompt preparado, con información ocultada y plantillas aplicadas; texto de respuesta del modelo; respuesta final; construido a partir de.                                                                                                                                    |
| Leyenda                             | Azul: propiedad del equipo. Rojo: tercero o proveedor. Verde: conjunto de datos. Flecha continua: flujo de datos. Flecha discontinua: flujo de control o consulta. Candado: cruce de un límite de confianza.                                                                                                                                                                                        |
| Descriptores de flujo               | Prompt preparado: texto del cliente con información ocultada + fragmentos recuperados + instrucciones del sistema + plantillas. Respuesta del modelo: texto generado por el LLM alojado; se presupone moderación posterior.                                                                                                                                                                         |
| Requisitos en los límites           | Autenticación ante el proveedor; cifrado en tránsito (TLS); registro de lo que sale de la zona; acuerdos sobre el tratamiento de datos.                                                                                                                                                                                                                                                             |
| Principios fundamentales            | Declarar el alcance: conocer qué sistema y versión describe el AIBOM. Reflejar la realidad registrar lo conocido, lo desconocido y sus motivos. Mostrar la provenance registrar fuentes, versiones y relaciones entre componentes. Respetar los límites explicitar los límites de confianza y registrar sus cruces. Mantener actualizado regenerar, supervisar la deriva y los cambios, e informar. |

Dos decisiones estructurales de este ejemplo merecen atención.

El modelo de lenguaje alojado se representa como un componente de tipo servicio cuyo límite es el punto de conexión del proveedor. Esto se debe a que el movimiento de datos termina en ese punto de conexión, no dentro de la infraestructura del proveedor. El equipo no tiene visibilidad de la topología con la que el proveedor presta el servicio; un AIBOM que fingiera lo contrario afirmarían hechos que el equipo no puede demostrar. El componente

de punto de conexión representa lo que el equipo ve realmente, es decir, una dirección, un método de autenticación y un contrato.

Sin embargo, el modelo no está ausente del AIBOM. El componente de punto de conexión contiene una referencia a un componente de modelo de aprendizaje automático, que incluye la identidad, versión, licencia, uso previsto, características de entrenamiento y otros metadatos de la model card. El lector puede identificar qué modelo ofrece el punto de conexión siguiendo una sola referencia. Si el proveedor cambia posteriormente el alias para apuntar a una instantánea más reciente del modelo, el componente de punto de conexión permanece igual. Cambia la referencia al componente de modelo. La siguiente revisión del AIBOM registra la diferencia de versión.

La segunda decisión consiste en indicar si cada nodo forma parte del sistema o queda fuera. El servicio de atención al usuario, el procesador de prompts, el servicio de recuperación y el gestor de respuestas forman parte del sistema descrito porque el equipo los opera y el alcance declarado los incluye. La API de moderación de terceros admite más discusión. Si el equipo considera que la moderación forma parte de lo que permite operar el asistente con seguridad, el servicio es constitutivo. Si lo considera una dependencia externa a la que el asistente llama, es externo. Ambas decisiones pueden ser correctas; el AIBOM hace explícita la elección para que quien lo revise conozca la representación que tiene en mente quien lo elaboró.

El modelo de lenguaje alojado también depende de una decisión de quien elabora el AIBOM. Si el alcance es «el asistente como capacidad desplegada», el punto de conexión del modelo se considera constitutivo porque el modelo forma parte del asistente. Si el alcance es «la integración que construimos alrededor de un modelo externo», se considera externo. El AIBOM formaliza esta distinción mediante el propio alcance declarado, que enumera los componentes incluidos y excluidos del sistema descrito. Para una lectura introductoria basta con comprender que la pertenencia de un nodo es una decisión relativa al alcance, no una propiedad intrínseca del nodo.

## Ejemplo desarrollado de una canalización de fine-tuning

**Consideremos ahora otro sistema en el que un equipo realiza un fine-tuning** de un modelo base con pesos abiertos usando datos internos para producir un modelo adaptado a un dominio que utilizará el asistente anterior.

El equipo parte de un modelo base publicado y obtenido de una plataforma pública de modelos. Dispone de un conjunto de datos de entrenamiento formado por transcripciones internas de atención al cliente, con información personal ocultada. También tiene un conjunto de datos de evaluación etiquetado manualmente por especialistas del dominio, que se utiliza para medir la calidad antes de publicar el modelo ajustado para su uso posterior. El equipo ejecuta el entrenamiento en un entorno de cómputo gestionado, produce un modelo ajustado, lo evalúa y lo publica en un registro interno de modelos.

## Worked example: a fine-tuning pipeline

Fine-tuning an open-weight base model on internal data to produce a domain-tuned model for use in a customer support assistant.

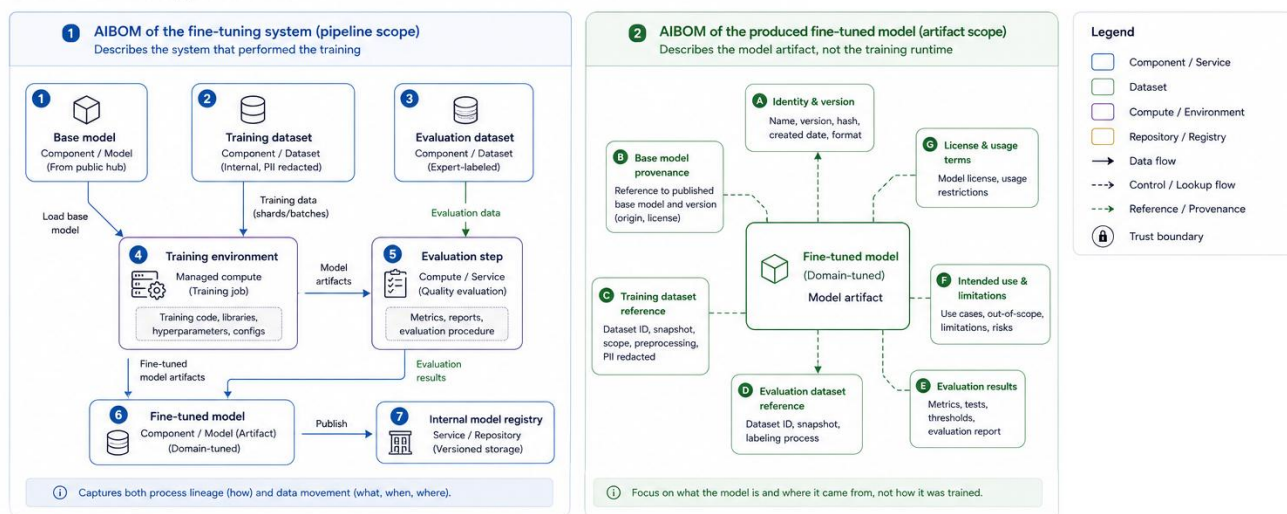


**Figura 4. Ejemplo de una canalización de fine-tuning**

Fine-tuning de un modelo base con pesos abiertos utilizando datos internos para producir un modelo adaptado a un dominio, destinado a un asistente de atención al cliente. La figura distingue el AIBOM del sistema del AIBOM del artefacto resultante.

| Elemento de la figura                     | Traducción y contenido                                                                                                                                                                                                                                                          |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Panel 1. AIBOM del sistema de fine-tuning | Alcance de la canalización. Describe el sistema que realizó el entrenamiento.                                                                                                                                                                                                   |
| 1. Modelo base                            | Componente o modelo obtenido de una plataforma pública.                                                                                                                                                                                                                         |
| 2. Conjunto de datos de entrenamiento     | Componente o conjunto de datos interno, con información de identificación personal (PII) oculta.                                                                                                                                                                                |
| 3. Conjunto de datos de evaluación        | Componente o conjunto de datos etiquetado por especialistas.                                                                                                                                                                                                                    |
| 4. Entorno de entrenamiento               | Cómputo gestionado para la tarea de entrenamiento. Código de entrenamiento, bibliotecas, hiperparámetros y configuraciones.                                                                                                                                                     |
| 5. Etapa de evaluación                    | Cómputo o servicio para evaluar la calidad. Métricas, informes y procedimiento de evaluación.                                                                                                                                                                                   |
| 6. Modelo ajustado                        | Componente o modelo (artefacto) adaptado al dominio.                                                                                                                                                                                                                            |
| 7. Registro interno de modelos            | Servicio o repositorio con almacenamiento versionado.                                                                                                                                                                                                                           |
| Rótulos de los flujos del panel 1         | Cargar modelo base; datos de entrenamiento (fragmentos o lotes); datos de evaluación; artefactos del modelo; artefactos del modelo ajustado; resultados de evaluación; publicar. El panel registra el linaje del proceso (cómo) y el movimiento de datos (qué, cuándo y dónde). |

| Elemento de la figura                               | Traducción y contenido                                                                                                                                                                                                              |
|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Panel 2. AIBOM del modelo ajustado resultante       | Alcance del artefacto. Describe el artefacto de modelo, no el runtime del entrenamiento. Centro modelo ajustado, adaptado al dominio; artefacto de modelo.                                                                          |
| A. Identidad y versión                              | Nombre, versión, hash, fecha de creación y formato.                                                                                                                                                                                 |
| B. Provenance del modelo base                       | Referencia al modelo base publicado y su versión origen y licencia.                                                                                                                                                                 |
| C. Referencia al conjunto de datos de entrenamiento | Identificador, instantánea, alcance, preprocesamiento y PII ocultada.                                                                                                                                                               |
| D. Referencia al conjunto de datos de evaluación    | Identificador, instantánea y proceso de etiquetado.                                                                                                                                                                                 |
| E. Resultados de evaluación                         | Métricas, pruebas, umbrales e informe de evaluación.                                                                                                                                                                                |
| F. Uso previsto y limitaciones                      | Casos de uso, usos fuera de alcance, limitaciones y riesgos.                                                                                                                                                                        |
| G. Licencia y condiciones de uso                    | Licencia del modelo y restricciones de uso.                                                                                                                                                                                         |
| Mensaje del panel 2                                 | Centrarse en qué es el modelo y de dónde procede, no en cómo se entrenó.                                                                                                                                                            |
| Leyenda                                             | Azul: componente o servicio. Verde: conjunto de datos. Violeta: cómputo o entorno. Naranja: repositorio o registro. Flecha continua: flujo de datos. Flecha discontinua: flujo de control o consulta. Candado: límite de confianza. |

Este sistema produce dos AIBOM diferenciables, y la distinción es importante.

**El primero es un AIBOM del propio sistema de fine-tuning, es decir, la canalización que realizó el entrenamiento.** Su grafo incluye el componente de modelo base, el conjunto de datos de entrenamiento, el conjunto de datos de evaluación, el entorno de entrenamiento, la etapa de evaluación y el modelo ajustado resultante. Los flujos describen cómo llegaron los datos a la etapa de entrenamiento, cómo se cargó el modelo base, cómo llegaron los datos de evaluación a su etapa correspondiente y cómo se publicó el modelo resultante en el registro.

El segundo es un AIBOM del propio modelo ajustado resultante, tratado como artefacto. Su alcance es el modelo, no la canalización. Incluye su identidad, su provenance hasta el modelo base, referencias a los conjuntos de datos de entrenamiento y evaluación, resultados de evaluación, uso previsto y licencia. No describe el entorno de ejecución (runtime) del fine-tuning porque, cuando un sistema posterior carga el modelo, ese entorno ya no está presente.

Ambos AIBOM hacen referencia a los mismos conjuntos de datos y al mismo modelo base. No son duplicados; describen alcances distintos. Quien realiza una revisión de riesgos del modelo lee el AIBOM del artefacto. Quien audita el entorno de entrenamiento lee el AIBOM del sistema. Una organización que quiera demostrar la provenance de principio a fin mantiene ambos y los vincula.

El ejemplo de fine-tuning también pone de manifiesto la diferencia entre linaje del proceso y movimiento de datos. El linaje del proceso registra cómo se originó un artefacto, incluido qué modelo base se utilizó, qué código de entrenamiento se ejecutó, qué hiperparámetros rigieron la tarea y qué procedimiento de evaluación produjo las métricas comunicadas. El movimiento de datos registra qué datos fueron a qué lugar, entre qué nodos y cuándo. Las canalizaciones de entrenamiento necesitan ambos. La provenance del modelo ajustado hasta el

modelo base es linaje del proceso. El movimiento, durante la ejecución, de fragmentos de datos de entrenamiento desde un almacén hasta los recursos de cómputo es movimiento de datos. El AIBOM incluye ambos en sus lugares respectivos. Para una lectura introductoria, lo esencial es que un AIBOM no tiene que elegir entre estas dos perspectivas, pues un AIBOM de un sistema de entrenamiento que utilice solo una describirá de forma incompleta lo ocurrido.

## Qué no afirma el AIBOM

Un AIBOM completo contiene hechos estructurados e información de provenance. No es un dictamen.

No declara que un sistema cumpla una regulación concreta. No declara que el riesgo del sistema sea aceptable. No declara que los controles presentes sean suficientes para ese riesgo. No declara quién es legalmente responsable de ningún aspecto del sistema. No es una puntuación de confianza, un nivel de aseguramiento ni una calificación de calidad.

Esta es una decisión deliberada de diseño del AIBOM, no un descuido. Un regulador, auditor, comité interno de revisión o equipo de adquisiciones aplica sus propias políticas, umbrales y marcos de riesgos a los hechos del AIBOM. Esos juicios se formulan después. Si el AIBOM ya incorporara un conjunto concreto de esos juicios, solo sería útil dentro de ese régimen. Al mantenerse en el plano de los hechos y la provenance, sirve como base común sobre la que pueden trabajar distintos regímenes.

Esa base común no es opcional. El AIBOM permite que esos juicios puedan contrastarse y refutarse. Sin él, una evaluación de riesgos es una afirmación no auditada. Con él, cada afirmación de la evaluación puede rastrearse hasta un nodo, un flujo, una referencia de evidencia o un límite de completitud declarado.

## Cómo se representa un AIBOM para quienes desean profundizar

El contenido conceptual de este capítulo cubre lo que necesita quien no va a implementar el formato. Para quienes sí van a generar un AIBOM, conviene conocer un aspecto adicional.

Los aspectos tratados en este capítulo pueden expresarse de forma nativa en CycloneDX 2.0 . El grafo reside en un blueprint, donde los componentes son los nodos; los flujos, los movimientos de datos dirigidos; y las zonas y los límites contienen el contexto de confianza. Las descripciones del propio AIBOM se corresponden con los tipos de modelo y el alcance declarados del blueprint, mientras que la declaración sobre el grado de completitud se expresa mediante las declaraciones de composición del documento. Las evidencias se vinculan mediante declaraciones que hacen referencia a cualquier nodo o flujo por su identificador. No existe un formato de archivo AIBOM separado, un esquema de extensión específico de IA ni una codificación de compatibilidad entre las que elegir, pues un AIBOM es un documento estructurado que utiliza estas estructuras estándar para describir un sistema de IA.

Los identificadores sirven para algo más que la organización interna. Cada componente, flujo, zona, límite y afirmación del documento tiene una referencia estable. El estándar define sus modelos de amenazas, riesgos y controles como elementos al mismo nivel que el blueprint que apuntan al mismo grafo, de modo que una amenaza referencia el límite que cruza su ruta de ataque; un control, el flujo que protege; y un análisis de vulnerabilidades, los componentes afectados. Ninguno vuelve a describir el sistema. Esta es la razón estructural por la que el AIBOM puede mantenerse libre de dictámenes y, a la vez, ser la base hasta la que puede rastrearse cada dictamen. Si se elimina el AIBOM, los análisis posteriores se quedan sin elementos a los que hacer referencia.

Quien elabora el documento puede elegir cuánto detalle incluir. Un AIBOM mínimo componentes, flujos y las tres descripciones del propio AIBOM es plenamente conforme y puede constituir una afirmación completa de quien lo elabora. Uno con abundantes evidencias añade declaraciones, composiciones y registros de formulación para representar evidencias legibles por máquinas y linaje de procesos. El nivel de detalle no es un nivel de

aseguramiento. Un AIBOM mínimo completo y bien respaldado por evidencias es más útil que uno detallado pero incompleto. La confianza en un AIBOM procede de su completitud, provenance, calidad de las evidencias y trayectoria de quien lo elabora, no de las estructuras que utiliza.

---

<sup>1</sup> <https://cyclonedx.org/news/cyclonedx-v2.0-coming-soon/>

## 6. AIBOM para sistemas de agentic AI

Los sistemas de agentic AI introducen un nuevo nivel de complejidad en las cadenas de suministro de IA. A diferencia de los sistemas tradicionales, que funcionan como canalizaciones relativamente estáticas, los sistemas de agentic AI son dinámicos, combinables y, a menudo, autónomos. Interactúan con herramientas externas, invocan otros agentes, adaptan su comportamiento durante la ejecución y dependen de ecosistemas cambiantes de servicios y protocolos.

Un enfoque tradicional de AIBOM se centra en documentar de forma estática modelos, conjuntos de datos y dependencias. En cambio, un AIBOM para sistemas de agentic AI debe contemplar las dependencias dinámicas, las interacciones durante la ejecución y la lógica de orquestación que, en conjunto, definen su comportamiento en producción. Esta sección explica cómo se amplían las prácticas de AIBOM a las arquitecturas de agentic AI, con énfasis en las relaciones entre múltiples agentes, los ecosistemas de herramientas y la conectividad externa.

### Dependencias entre múltiples agentes

Los sistemas de agentic AI suelen estar formados por varios agentes que cooperan y pueden tener funciones distintas, como planificación, ejecución, recuperación, validación u orquestación. Estos agentes pueden:

- Estar contruidos sobre modelos distintos; por ejemplo, un planificador basado en GPT, un agente de recuperación y un ejecutor de herramientas.
- Pertenecer a distintos equipos o proveedores.
- Comunicarse mediante protocolos estructurados o intercambios informales de mensajes.

En este contexto, un AIBOM debe registrar explícitamente:

- Identidades y funciones de los agentes: planificador, ejecutor, crítico, recuperador, supervisor de políticas, enrutador, etc.
- Dependencias de modelos subyacentes de cada agente: modelo base, fine-tuning y adaptadores.
- Patrones de interacción: jerárquicos, entre pares, basados en eventos o de nodo central y nodos periféricos.
- Orquestación del flujo de control: quién invoca a quién, bajo qué condiciones y con qué rutas de escalamiento.

Esto es fundamental porque el riesgo ya no se limita a un único modelo o servicio. Una vulnerabilidad o un fallo en un agente puede propagarse por todo el sistema. Por ejemplo:

- Un agente de recuperación comprometido puede envenenar el razonamiento y las recomendaciones posteriores.
- Un planificador que genera alucinaciones puede activar usos inseguros de herramientas o flujos de trabajo de alto riesgo.
- Un guardrail agent mal configurado puede no bloquear salidas dañinas o que incumplan los requisitos aplicables.

Por ello, el AIBOM debería representar los sistemas de agentic AI como grafos de componentes interdependientes, en lugar de canalizaciones lineales. El BOM se convierte en un grafo de agentes, modelos y aristas de orquestación que permite analizar el impacto de un cambio en un nodo o una arista.

## Herramientas asociadas

Los sistemas de agentic AI obtienen gran parte de su capacidad del uso de herramientas. Estas pueden incluir:

- API de búsqueda, clima, finanzas, recursos humanos, gestión de tickets, etc.
- Entornos de ejecución de código y ejecutores de funciones.
- Bases de datos y almacenes vectoriales. Memoria y estado.
- Servicios empresariales internos y microservicios.
- Sistemas de archivos o repositorios de documentos.

**Estas herramientas no son simples integraciones, sino extensiones activas de las capacidades del agente, a menudo invocadas de forma autónoma y con alta frecuencia.**

Un AIBOM para sistemas de agentic AI debe documentar, como mínimo:

- Identidad y función de la herramienta: qué hace y sobre qué dominio actúa.
- Mecanismos de invocación: llamadas a funciones, API HTTP, complementos y herramientas nativas del marco de trabajo.
- Alcance del acceso y permisos: solo lectura, lectura y escritura o administración; alcance de los datos y recursos.
- Métodos de autenticación y gestión de secretos: claves de API, OAuth, identidad de cargas de trabajo y almacenes de secretos.
- Límites de frecuencia, cuotas y restricciones operativas, tanto por agente como globales.
- Versión o hash de la definición de la herramienta: el esquema y la descripción exactos cuyo uso se aprobó para el agente.

Desde la perspectiva de seguridad y gobernanza, las herramientas amplían considerablemente la superficie de ataque:

- Los ataques de inyección de prompts pueden manipular el uso de herramientas y provocar acciones dañinas.
- Las herramientas con permisos excesivos pueden exponer datos sensibles o permitir movimientos laterales.
- Las API externas pueden introducir riesgos de exfiltración de datos, integridad o disponibilidad.
- La definición y el comportamiento de una herramienta pueden cambiar después de la revisión, por lo que la aprobación debe vincularse a una versión específica de su definición, no solo a su nombre.

Registrar las dependencias de herramientas en el AIBOM permite:

- Auditorías detalladas de acceso: qué agentes pueden invocar qué herramientas y con qué permisos.
- Evaluación de riesgos por herramienta: criticidad, alcance del impacto y controles compensatorios.
- Una respuesta a incidentes más rápida cuando una herramienta o un conector resulta comprometido: quién lo utiliza, dónde y cómo.

## Conectores de terceros

Los sistemas modernos basados en agentes suelen depender de conectores de terceros para integrarse con plataformas externas, como:

- Aplicaciones SaaS: plataformas de colaboración, CRM, suites de productividad y herramientas de gestión de servicios de TI (ITSM), como Slack, Salesforce, Google Workspace y ServiceNow.
- Proveedores de datos: fuentes de información financiera, bases de datos jurídicas y API sanitarias.
- Servicios en la nube y plataformas de IA: almacenamiento, analítica y API de modelos.

Estos conectores introducen dependencias de la cadena de suministro que van más allá de las bibliotecas de software y los modelos tradicionales, entre ellas:

- API y acuerdos de nivel de servicio (SLA) controlados por proveedores.
- Canalizaciones y transformaciones de procesamiento de datos opacas.
- Sistemas externos de gestión de identidades y accesos y motores de políticas.

Por tanto, el AIBOM debería registrar:

Desde la perspectiva de seguridad y gobernanza, los conectores conllevan riesgos que quedan, en gran medida, fuera del control directo de la organización:

- Los alcances OAuth concedidos al configurar un conector pueden ser mucho más amplios de lo que exige el caso de uso, lo que otorga a los agentes acceso permanente a espacios de trabajo o conjuntos de registros completos.
- Los proveedores pueden cambiar el comportamiento de las API, el tratamiento de los datos o los subencargados del tratamiento sin notificarlo a quienes mantienen AIBOM en etapas posteriores de la cadena.
- Los datos pueden cruzar límites de residencia o soberanía a través de subencargados del tratamiento que nunca se divulgaron.
- Datos del proveedor y del servicio del conector: identidad del proveedor, producto, región y modelo de despliegue.
- Datos intercambiados: clasificación de entradas y salidas, categorías de datos y niveles de sensibilidad.
- Modelos de autenticación y autorización: flujos OAuth, claves de API, cuentas de servicio y acceso delegado.
- Consideraciones de residencia de datos, soberanía y cumplimiento.
- Restricciones contractuales, de licencia y de uso que puedan afectar a la operación o al tratamiento de datos.

Un reto importante es que la visibilidad de los sistemas de terceros suele ser limitada. Las organizaciones deberían:

- Exigir a los proveedores divulgaciones similares a un AIBOM o atestaciones de seguridad cuando sea posible.
- Documentar explícitamente los límites de confianza asumidos y los riesgos residuales.
- Rastrear las carencias conocidas de transparencia, incluidos subencargados del tratamiento desconocidos o etapas de procesamiento opacas.

Esto garantiza que, incluso cuando no se dispone de toda la información de provenance o de los detalles internos, el riesgo se reconozca, registre y gestione explícitamente dentro del marco AIBOM.

## Seguimiento del ecosistema MCP/A2A

Los protocolos emergentes, como Model Context Protocol (MCP) y los marcos de comunicación Agent to Agent (A2A), están definiendo rápidamente cómo interoperan los sistemas de agentic AI. Estos ecosistemas permiten:

- Descubrimiento e invocación estandarizados de herramientas entre plataformas.
- Comunicación entre agentes a través de límites organizativos o de entornos de cliente (tenants).
- Composición dinámica de capacidades durante la ejecución sin desplegar código.

Aunque son potentes, también introducen dependencias muy dinámicas y potencialmente efímeras, difíciles de rastrear con los métodos BOM tradicionales.

Para seguir siendo pertinente, el AIBOM debe evolucionar e incluir:

- Uso de protocolos, como MCP, A2A u otras normas de interoperabilidad entre agentes.
- Puntos de conexión registrados y proveedores de servicios que participan en estos ecosistemas.
- Mecanismos de descubrimiento dinámico de capacidades: registros, catálogos y mercados de herramientas.
- Dependencias a nivel de sesión o contexto, además de la configuración estática.
- MCP: identidad del servidor, transporte, fijación de versiones, hashes de definiciones de herramientas y alcances concedidos.
- A2A: Agent Cards, que publican la identidad, las capacidades y los requisitos de autenticación de un agente y sirven directamente como entrada para un AIBOM.

Por ejemplo:

- Un agente puede descubrir e invocar una herramienta durante la ejecución mediante MCP, sin configuración estática previa.
- Dos agentes de distintos proveedores pueden colaborar mediante canales A2A e intercambiar tareas y resultados.
- Las capacidades y políticas disponibles pueden cambiar sin volver a desplegar la aplicación.

Para abordarlo, las implementaciones de AIBOM deberían:

- Incorporar telemetría, registros y trazas de ejecución como fuentes de referencia para las dependencias reales.
- Rastrear los registros de capacidades, puntos de conexión de descubrimiento y mercados de herramientas como componentes de pleno derecho.
- Mantener registros con referencias temporales de las interacciones y dependencias: quién se comunicó con quién, cuándo y mediante qué protocolo.

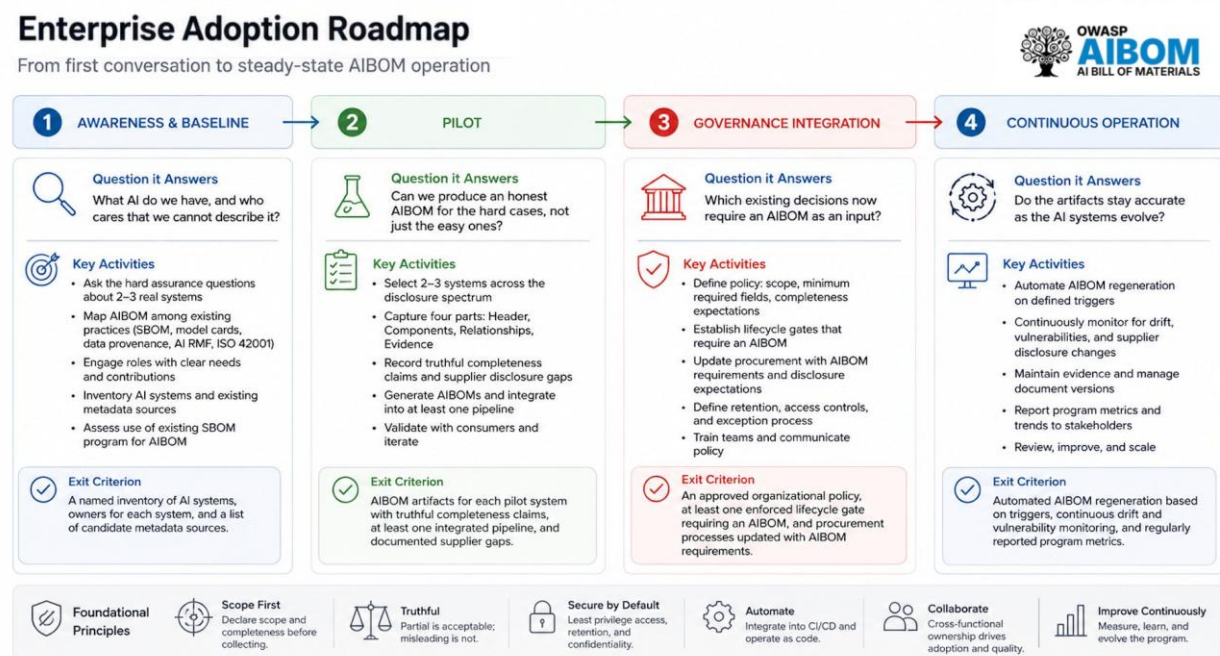
Esto transforma el AIBOM de un artefacto puramente estático en una representación viva del comportamiento del sistema a lo largo del tiempo, que combina configuración de diseño con observaciones de ejecución.

<sup>1</sup> MCP: <https://modelcontextprotocol.io/specification/2026-07-28>

<sup>1</sup> A2A: <https://a2a-protocol.org/latest/>

## 7. Hoja de ruta de adopción empresarial

Elaborar un AIBOM individual es una tarea de ingeniería, y el ciclo de vida del artefacto descrito antes planificar, elaborar, validar, publicar, operar, auditar y retirar define la forma de realizarla. Hacerlo para cada sistema de IA de una empresa, de manera repetible y con resultados que realmente se utilicen en las decisiones, es un programa de cambio organizativo. Este capítulo establece el recorrido desde la primera conversación hasta una operación estable.



Source: OWASP AIBOM Foundations Guide v1.0

Figura 5. Hoja de ruta de adopción empresarial

Desde la primera conversación hasta una operación estable de AIBOM. El original conserva el número de capítulo 9; el texto revisado utiliza el capítulo 7. Las flechas recorren las fases 1, 2, 3 y 4.

| Elemento de la figura                    | Traducción y contenido                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Concienciación y situación de partida | Pregunta: ¿qué IA tenemos y a quién le preocupa que no podamos describirla? Actividades: plantear preguntas difíciles de aseguramiento sobre dos o tres sistemas reales; situar el AIBOM entre las prácticas existentes (SBOM, model cards, provenance de datos, AI RMF e ISO 42001); involucrar a cada función con necesidades y contribuciones claras; inventariar sistemas de IA y fuentes de metadatos existentes; evaluar el uso del programa SBOM para AIBOM. Salida: inventario de sistemas de IA identificados, responsables de cada sistema y lista de posibles fuentes de metadatos.                     |
| 2. Proyecto piloto                       | Pregunta: ¿podemos elaborar un AIBOM que refleje la realidad de los casos difíciles, no solo de los sencillos? Actividades: elegir dos o tres sistemas con distintos niveles de divulgación; registrar encabezado, componentes, relaciones y evidencias; declarar verazmente el grado de completitud y las carencias de divulgación de proveedores; generar AIBOM e integrarlos en al menos una canalización; validar con quienes los utilizan e iterar. Salida: artefactos AIBOM para cada sistema piloto con declaraciones veraces, al menos una canalización integrada y carencias de proveedores documentadas. |
| 3. Integración en la gobernanza          | Pregunta: ¿qué decisiones existentes requieren ahora un AIBOM como entrada? Actividades: definir políticas de alcance, campos mínimos y expectativas de completitud; establecer puntos de control del ciclo de vida que exijan un AIBOM; actualizar adquisiciones con requisitos de AIBOM y expectativas de divulgación; definir conservación, controles de acceso y proceso de excepciones; capacitar a los equipos y comunicar la política. Salida: política organizativa aprobada, al menos un punto de control obligatorio que exija un AIBOM y procesos de adquisición actualizados.                          |
| 4. Operación continua                    | Pregunta: ¿los artefactos siguen siendo precisos a medida que evolucionan los sistemas de IA? Actividades: automatizar la regeneración ante eventos definidos; supervisar continuamente deriva, vulnerabilidades y cambios de divulgación de proveedores; mantener evidencias y gestionar versiones; comunicar métricas y tendencias a las partes interesadas; revisar, mejorar y ampliar. Salida: regeneración automática ante eventos, supervisión continua de deriva y vulnerabilidades e informes periódicos de métricas.                                                                                      |
| Principios fundamentales                 | Primero el alcance: declarar alcance y completitud antes de recopilar. Veracidad: una cobertura parcial es aceptable; inducir a error no lo es. Seguridad por defecto: mínimo privilegio, conservación y confidencialidad. Automatizar: integrar el AIBOM en CI/CD y gestionarlo como código. Colaborar: la responsabilidad compartida entre funciones impulsa adopción y calidad. Mejorar continuamente: medir, aprender y hacer evolucionar el programa.                                                                                                                                                         |

Las cuatro fases siguientes se ordenan según sus dependencias. Cada una responde a una pregunta y termina con una condición comprobable.

| Fase                                  | Pregunta que responde                                                                                          | Criterio de salida                                                                                                                                                                                        |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Concienciación y situación de partida | ¿Qué IA tenemos y a quién le preocupa que no podamos describirla?                                              | Un inventario de sistemas de IA identificados, una persona responsable de cada sistema y una lista de posibles fuentes de metadatos.                                                                      |
| Proyecto piloto                       | ¿Podemos elaborar un AIBOM que refleje fielmente la realidad de los casos difíciles, no solo de los sencillos? | Artefactos AIBOM generados para cada sistema piloto, con declaraciones veraces sobre el grado de completitud, al menos una canalización integrada y carencias de divulgación de proveedores documentadas. |
| Integración en la gobernanza          | ¿Qué decisiones existentes requieren ahora un AIBOM como entrada?                                              | Una política organizativa aprobada, al menos un punto de control obligatorio del ciclo de vida que exija un AIBOM y procesos de adquisición actualizados con requisitos de AIBOM.                         |
| Operación continua                    | ¿Los artefactos siguen siendo precisos a medida que evolucionan los sistemas de IA?                            | Regeneración automática de AIBOM ante eventos definidos, supervisión continua de deriva y vulnerabilidades, y comunicación periódica de métricas del programa.                                            |

## Fase 1. Concienciación y situación de partida

No es necesario reconstruir aquí la justificación para comenzar los factores de seguridad, regulación y gobernanza expuestos antes constituyen el argumento. Esta fase añade concreción. Las preguntas de aseguramiento que la organización no puede responder hoy qué versión del modelo está en producción, con qué se entrenó o ajustó, quién es el proveedor de origen y qué permite su licencia deberían plantearse abiertamente sobre dos o tres sistemas reales. La incapacidad de responderlas es el argumento más eficaz para obtener apoyo, y resulta más convincente que cualquier referencia a un marco.

La concienciación también implica situar correctamente el AIBOM entre las prácticas que la organización ya puede estar aplicando. Un SBOM inventaría componentes de software y sigue siendo necesario; un AIBOM extiende esa disciplina a modelos, conjuntos de datos, prompts, guardrails y servicios que intervienen en el recorrido de las solicitudes. Una model card documenta el uso previsto y el rendimiento de un modelo; el AIBOM incorpora ese contenido como evidencia vinculada a un componente, dentro de un documento versionado con alcance declarado. El trabajo sobre provenance de datos aporta el linaje de los conjuntos de datos que registra el AIBOM. Los marcos establecidos de gestión de riesgos y sistemas de gestión de IA requieren documentación estructurada de las características del sistema sin especificar su formato; el AIBOM es una forma de satisfacer esa necesidad. No sustituye ni duplica ninguna de estas prácticas.

La participación debería definirse por función desde el principio, porque la falta de alineación en este punto produce pruebas piloto fragmentadas que nunca llegan a integrarse en la gobernanza.

| Función                                                            | Qué necesita del AIBOM                                                                                           | Qué aporta                                                                                                                                                   |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Arquitectura de seguridad y equipo de pruebas ofensivas (red team) | Información sobre la superficie de ataque específica de IA vinculada a componentes.                              | Alcance del modelado de amenazas y definición de las preguntas de seguridad que debe responder el AIBOM.                                                     |
| Asesoría jurídica y de propiedad intelectual                       | Condiciones de licencia de modelos y conjuntos de datos, derechos de uso y restricciones aplicables.             | Interpretación de obligaciones jurídicas, requisitos de licencia y cumplimiento en materia de propiedad intelectual.                                         |
| Cumplimiento y auditoría                                           | Evidencias que respalden la transparencia, la trazabilidad y las obligaciones regulatorias de IA.                | Políticas de conservación, controles de gobernanza, requisitos de auditoría y expectativas sobre evidencias.                                                 |
| Ingeniería de plataformas y MLOps                                  | Requisitos de automatización, mecanismos de recopilación de metadatos y puntos de integración en canalizaciones. | Implementación de la generación automática de AIBOM, integración CI/CD y mantenimiento continuo.                                                             |
| Equipos de IA y aprendizaje automático                             | Reconocimiento de que registrar el linaje es una parte integral del desarrollo de sistemas de IA.                | Linaje de los datos de entrenamiento, procedencia del modelo base, historial de fine-tuning, resultados de evaluación y metadatos del desarrollo del modelo. |

El análisis de la situación de partida cierra la fase con tres tareas: inventariar los sistemas de IA en producción o desarrollo activo, incluidos modelos internos, variantes ajustadas, modelos externos accesibles mediante API y funciones de IA en servicios SaaS contratados; identificar los metadatos disponibles en fichas de modelo, registros de entrenamiento y de conjuntos de datos, y manifiestos de dependencias; y evaluar si un programa de SBOM existente puede incorporar el trabajo de AIBOM en vez de crear otro en paralelo.

## Fase 2. Proyecto piloto

Seleccione dos o tres sistemas con distintos niveles de divulgación, porque la dificultad de elaborar un AIBOM depende de la información disponible. Un modelo entrenado y desplegado internamente ofrece acceso completo a los metadatos y constituye un punto de partida manejable. Una variante interna de un modelo base externo exige registrar cadenas de procedencia internas y externas, y representa un escenario empresarial frecuente. Un modelo alojado al que se accede mediante una API permite comprobar la fiabilidad y los límites de la información divulgada por el proveedor. Una función de IA integrada en una aplicación SaaS contratada establece el nivel mínimo de cobertura alcanzable y aporta información especialmente útil para el proceso de adquisiciones.

La recopilación de información es el punto en el que más suelen fallar los proyectos piloto, porque los equipos reúnen datos sin definir qué debe acreditar el documento. Estructure el trabajo en torno a las cuatro partes descritas anteriormente:

**El encabezado. Declare el alcance antes de recopilar información sobre qué sistema, versión, despliegue e interfaces están incluidos o excluidos.** Después, registre una declaración sobre el grado de completitud que refleje fielmente la información que fue posible obtener. Una declaración de completitud parcial para una función SaaS de caja negra constituye un artefacto válido. En cambio, una declaración que afirme una cobertura total del mismo sistema sería inexacta.

Los componentes. Identidad, versión, arquitectura y referencia al modelo base; conjuntos de datos con versión, fuente, método de recopilación, licencia y limitaciones conocidas; herramientas, orquestadores y conectores que

invoca el sistema; instrucciones (prompts) y políticas de barreras de protección (guardrails); entorno de ejecución y sus dependencias, con referencias cruzadas a registros SBOM existentes en lugar de volver a inventariarlos.

Los flujos. Qué datos se mueven entre esos componentes y qué límites atraviesan; información que ninguna lista de campos puede representar y que los equipos de respuesta a incidentes consultan en primer lugar.

Las evidencias. Valores hash de archivos de pesos e instantáneas de conjuntos de datos, firmas, fichas de modelo, resultados de evaluación y registros de los responsables de la elaboración, revisión y aprobación, que permiten revisar el documento y no limitarse a constatar su existencia.

En materia de automatización, la pregunta del proyecto piloto no es qué formato utilizar, ya que eso se resuelve en otra parte del documento, sino de dónde procede cada campo. Extraiga la información de las canalizaciones de compilación y entrenamiento cuando ya esté disponible, conéctelas con el sistema de seguimiento de experimentos de la organización y especifique qué campos deben completarse manualmente y quién es responsable de ellos. Evite comprometer el programa con una plataforma basándose únicamente en los resultados del proyecto piloto.

La elaboración corresponde al equipo más cercano a cada sistema, con revisión y aprobación por parte de una función designada de gobernanza o seguridad. Centralizarla en un equipo sin conocimiento directo del sistema es precisamente el tipo de fallo que este modelo distribuido pretende evitar.

### Fase 3. Integración en la gobernanza

Integrar significa convertir el AIBOM en un insumo obligatorio para las decisiones que la organización ya toma. Crear un proceso paralelo para el AIBOM es la razón por la que la mayoría de los programas se estanca después del proyecto piloto.

| Proceso existente                   | Qué aporta el AIBOM                                                                                                                                               | Dónde se exige                                                                                                                                      |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Gestión de riesgos de modelos       | Un inventario completo de componentes de IA, dependencias y metadatos de apoyo necesarios para evaluar riesgos.                                                   | Entrada obligatoria para cada evaluación y revisión de riesgos del modelo.                                                                          |
| Ciclo de vida de desarrollo de IA   | Alcance declarado del sistema, procedencia, linaje y evidencias de evaluación registrados en cada etapa del ciclo de vida.                                        | Punto de control obligatorio para la aprobación previa al entrenamiento, la revisión previa al despliegue y la evaluación posterior a un incidente. |
| Adquisiciones y riesgos de terceros | Información sobre la procedencia declarada por el proveedor, dependencias de software y modelos, e identificación explícita de datos no divulgados o incompletos. | Requisito mínimo de divulgación durante la evaluación de proveedores y sistemas de IA de alto riesgo.                                               |
| Revisión del diseño de seguridad    | Componentes de IA, flujos de datos, dependencias y límites de confianza necesarios para el modelado de amenazas y la revisión de arquitectura.                    | Entrada estándar para las revisiones de arquitectura y diseño de seguridad de IA.                                                                   |
| Preparación regulatoria y auditoría | Evidencias trazables y con control de versiones vinculadas a las obligaciones regulatorias, de gobernanza y de cumplimiento aplicables.                           | Artefacto de gobernanza conservado y presentado durante inspecciones regulatorias, auditorías y evaluaciones de cumplimiento.                       |

Una política formal permite exigirlo. Debería definir el AIBOM mínimo utilizable por nivel de riesgo, las responsabilidades de elaboración y revisión, los periodos de conservación, los eventos de actualización y el procedimiento de escalamiento cuando un proveedor no divulgue información. El propio artefacto debe tratarse como un documento controlado: debe contar con control de versiones y firma; registrar la identidad de quien lo revisa, así como la fecha y el alcance de la revisión; y estar sujeto a los mismos controles de conservación y acceso que los registros de validación de modelos.

## **Fase 4. Operación continua**

Un AIBOM describe un sistema en un momento concreto. Los sistemas cambian continuamente, y un artefacto que ya no refleja el sistema desplegado es peor que no disponer de ninguno, porque genera una confianza que no puede respaldar.

La regeneración debería activarse ante un nuevo entrenamiento o una actualización de datos; sustitución de adaptadores o cambios en parámetros de fine-tuning; cambios de versión de conjuntos de datos, incluidos los incrementales; cambios introducidos por el proveedor en los modelos de origen o sus alias; actualizaciones de las dependencias del entorno de inferencia o de la canalización de preprocesamiento; cambios en guardrails y paquetes de políticas; vulnerabilidades divulgadas que afecten a componentes rastreados; y cualquier cambio en el uso previsto, el alcance del despliegue o los límites de acceso. Los cambios del proveedor merecen especial atención, porque pueden producirse sin que se publique localmente una nueva versión.

En la operación, esto supone integrar la generación de AIBOM en las canalizaciones de entrenamiento para generar artefactos cuando el proceso finaliza correctamente; incorporar comprobaciones de validación en los puntos de control de despliegue para que los registros incompletos o desactualizados bloqueen el paso a la siguiente etapa; incorporar los registros de componentes a los mismos flujos de correlación de vulnerabilidades que ya utiliza el programa SBOM, en lugar de crear otro silo; y verificar la integridad para detectar modificaciones posteriores a la generación. Las responsabilidades se asignan a las funciones existentes: los equipos de ingeniería de ML y de plataformas realizan las actualizaciones; el equipo de operaciones de seguridad clasifica y prioriza las alertas; el área de gobernanza informa; y el equipo de riesgos de terceros hace seguimiento de la divulgación de los proveedores.

Conviene medir el desempeño del programa mediante un conjunto reducido de indicadores, entre ellos la cobertura, es decir, la proporción de sistemas de IA en producción con un artefacto vigente; la vigencia, medida por el tiempo transcurrido entre un evento de activación y la actualización correspondiente; el grado de completitud respecto del AIBOM mínimo utilizable, desglosado por nivel de riesgo; la respuesta ante vulnerabilidades, medida desde la divulgación hasta la evaluación del impacto; y el cumplimiento de los proveedores, es decir, la proporción de proveedores de IA contratados que cumplen el estándar mínimo de divulgación. Estos indicadores miden el programa, no los sistemas que documenta. Un registro totalmente cumplimentado de un sistema mal gobernado sigue siendo solo un registro totalmente cumplimentado; ninguna de estas métricas evalúa el sistema de IA ni el AIBOM. Preséntelos donde ya se informa del riesgo de IA para que las mismas evidencias sirvan a la preparación regulatoria, la auditoría interna y los informes ejecutivos sin elaborarse tres veces.

# Agradecimientos

## Personas que contribuyeron

| Nombre                                                                         | Organización o afiliación                                      |
|--------------------------------------------------------------------------------|----------------------------------------------------------------|
| Yuvaraj Govindarajulu (responsable de línea de trabajo y colíder del proyecto) | Protectt.ai, India                                             |
| Aruneesh Salhotra (líder del proyecto)                                         | Fundador y director ejecutivo, Stealth Startup, Estados Unidos |
| Martin Espinoza                                                                | Fabletics                                                      |
| Van Lindberg                                                                   | Model Monster, Estados Unidos                                  |
| Tanmay Ambegaokar                                                              | Onix, Estados Unidos                                           |
| Bakul Singhal                                                                  | Steve Madden, Estados Unidos                                   |
| L.Frances. Domingo                                                             |                                                                |
| Anmol Kumar                                                                    | Stealth Startup, Estados Unidos                                |
| Binal Patel                                                                    | SISA, India                                                    |
| Ranjan Goel                                                                    | NuGuard AI, Estados Unidos                                     |
| Sapna Paul                                                                     | Dayforce, Estados Unidos                                       |
| Behnaz Karimi                                                                  | OWASP, Alemania                                                |
| John Cavanaugh                                                                 | ProCap360, Estados Unidos                                      |
| Yash Omer                                                                      | Bajaj Financial Services, India                                |
| Pratibha Aphale                                                                | Goldman Sachs, Estados Unidos                                  |
| Deba Mishra                                                                    | EY, Estados Unidos                                             |
| Karen Bennet                                                                   |                                                                |
| Chetan Velicheti                                                               |                                                                |

## Patrocinadores del proyecto

Agradecemos a los patrocinadores del proyecto, cuyas contribuciones económicas ayudan a impulsar los objetivos del proyecto OWASP AIBOM y a cubrir los costos operativos, además de los recursos aportados por OWASP Foundation.

Los patrocinadores reciben reconocimiento por sus contribuciones en nuestros materiales y sitios web. Todos los materiales del proyecto son desarrollados e impulsados por la comunidad y se publican bajo licencias de código abierto y Creative Commons. Para obtener más información sobre cómo patrocinar y apoyar el proyecto, visite la sección de patrocinio de nuestro sitio web: <https://owaspai bom.org/sponsorship/>.

## Patrocinadores de categoría Gold del proyecto



## Patrocinadores de categoría Silver del proyecto





# Guía de Fundamentos de OWASP AIBOM

SEPTIEMBRE 2026

**Versión 1.0 (ES)**