ENKIDU

— MIOVSKI GROUP —

ARQUITECTURA CONCEPTUAL

# Aegis Assure

Un marco alineado con las normas para evaluar y acreditar la gobernanza y la ética de los datos a lo largo del ciclo de vida de los sistemas de IA, aprendizaje automático y redes neuronales — entregado como servicio de Miovski Group, fundado en la disciplina de confianza de Origi.

Español · Edición resumida

Basada en la versión 0.1 · 4 de julio de 2026

Preparado por MIOVSKI GROUP

Clasificación · Confidencial · Borrador para distribución a clientes

La edición completa en inglés prevalece

# Acerca de esta edición

Este documento es una edición resumida, en español, de « Aegis Assure — AI Data Ethics Assessment », versión 0.1 (4 de julio de 2026), preparada por Miovski Group. Cada sección del original está representada de forma abreviada. En caso de divergencia, la edición completa en inglés prevalece. Clasificación: confidencial — borrador para distribución a clientes.

# Resumen

Toda organización que despliega IA afronta hoy la misma exigencia de reguladores, consejos, auditores y clientes: no « ¿funciona el modelo? » sino « ¿puede probar que los datos que lo sustentan se gobernaron de forma responsable? ». La pregunta es difícil porque la evidencia está dispersa por un ciclo de vida de los datos que pocas organizaciones han cartografiado — adquisición, ingesta, integración, clasificación, almacenamiento, mantenimiento, operación, compartición, archivo y retiro — y porque las normas que definen una buena respuesta han cambiado bruscamente en los últimos dieciocho meses.

Aegis Assure es el servicio de Miovski Group para responder con rigor. Es un marco de evaluación y acreditación alineado con las normas, de sesenta y tres criterios que abarcan todo el ciclo de vida de los datos, las obligaciones distintas de los datos de entrenamiento y de inferencia, y la gobernanza organizacional que se sitúa por encima de ambos. Cada criterio empareja un requisito de evidencia definido para los practicantes con una guía estructurada para evaluadores independientes, puntuado en una escala Rojo-Ámbar-Verde y ponderado por criticidad — de modo que el resultado no es una opinión sino un expediente de acreditación defendible y reproducible.

Esta edición reformatea y revalida el marco subyacente. Corrige el fundamento regulatorio al panorama de mediados de 2026 — materialmente cambiado desde la primera redacción: la AIDA canadiense murió en el orden del día, la Ley de IA de la UE pasó del texto a un calendario de cumplimiento por fases, y Estados Unidos invirtió dos veces su postura federal. Y sitúa el marco donde pertenece dentro de la pila Enkidu: la capa de aseguramiento de la gobernanza y la ética que complementa a Origi — misma estructura de caso de aseguramiento, misma separación de funciones, misma convicción de que una afirmación vale solo la cadena de evidencia que la respalda.

La confianza en un sistema de IA no es un eslogan que proclamar; es una posición que argumentar y evidenciar. Aegis Assure es cómo se construye esa posición, criterio a criterio.

# 1. Visión del servicio y posicionamiento

Aegis Assure es un servicio de evaluación y acreditación: una organización encarga a Miovski Group evaluar la gobernanza y la ética de los datos de uno o más sistemas de IA contra un cuerpo definido de criterios, y producir un resultado de acreditación en el que las partes interesadas — reguladores, consejos, autoridades de contratación, aseguradoras, clientes — puedan confiar. El marco es el instrumento; el servicio es la entrega de hallazgos confiables a través de él. Se aplica a toda organización que diseña, desarrolla, despliega u opera sistemas de IA — con especial fuerza en las aplicaciones de alto riesgo y alto impacto.

Por qué ahora: convergen tres presiones. La regulación se ha endurecido — las obligaciones de alto riesgo y de modelos de propósito general de la Ley de IA de la UE siguen ya un calendario concreto. El listón probatorio ha subido — « nos tomamos la ética en serio » ya no es una respuesta aceptable; se exige evidencia documentada, por criterio, evaluada de forma independiente. Y las propias normas se han movido — gran parte de la documentación de gobernanza existente está desactualizada.

- Tangram — ¿Dónde ocurre el trabajo, y bajo qué condiciones de frontera? — Interno: cómo construimos.
- Origi — ¿Puede ocurrir esta acción, y podemos probar lo que ocurrió? — Interno: cómo construimos.
- Helios Grid — ¿Está el tejido sano, actualizado y recuperable? — Interno: cómo construimos.
- Aegis Defence — ¿Sobrevivirán cada clave y cada firma a un adversario cuántico? — Interno: cómo construimos.
- Aegis Assure — ¿Es responsable y defendible la gobernanza de datos de IA de esta organización? — Hacia fuera: un servicio que entregamos.

El nombre es deliberado: Aegis Defence protege los datos en movimiento criptográficamente; Aegis Assure protege a la organización probando que sus datos se gobernaron éticamente. Dos escudos — uno técnico, otro probatorio. Origi y Aegis Assure son la misma filosofía a dos escalas: Origi es un arnés de confianza en ejecución que verifica cada acción de un sistema en marcha; Aegis Assure es un marco de aseguramiento del ciclo de vida que verifica cada etapa de la gobernanza de datos, periódicamente y en la acreditación. Una organización ya asegurada bajo Aegis Assure está bien preparada para adoptar Origi; una organización que ejecuta Origi genera como subproducto gran parte de la evidencia que Aegis Assure exige. Están diseñados para componerse.

## 2. Fundamento regulatorio

El marco está deliberadamente alineado con regímenes reconocidos para que sus resultados sean defendibles ante terceros — y esa alineación sigue un panorama que ha cambiado materialmente. Unión Europea: la Ley de IA (Reglamento (UE) 2024/1689) entró en vigor el 1 de agosto de 2024 y se aplica por fases — prohibiciones y alfabetización desde el 2 de febrero de 2025; gobernanza y obligaciones GPAI desde el 2 de agosto de 2025; aplicación general, incluidas la mayoría de las obligaciones de alto riesgo, el 2 de agosto de 2026; sistemas de alto riesgo integrados el 2 de agosto de 2027.

Canadá: la referencia anterior a la AIDA como « marco propuesto » ya no es exacta — el proyecto C-27 murió con la prórroga de enero de 2025, y Canadá no tiene hoy ley federal específica de IA. Estados Unidos: la EO 14110 fue derogada en enero de 2025 y sustituida por la EO 14179, que reorienta la política federal del riesgo y los derechos hacia la innovación y la competitividad. Bajo los estatutos cambiantes permanecen las normas estables que forman la columna técnica del marco: NIST AI RMF 1.0 y su perfil de IA generativa, ISO/IEC 42001 y 23894, el RGPD y sus homólogos — confirmadas contra las publicaciones oficiales antes de un uso formal.

## 3. Estructura del marco

El marco organiza sesenta y tres criterios únicos en tres partes, según una sola intuición: las obligaciones de gobernanza difieren por etapa del ciclo de vida, según si el dato entrena u opera el modelo, y según si el control es técnico u organizacional.

- Sección A — Ciclo de vida de los datos — diez etapas, de la adquisición al retiro, evaluadas para datos de entrenamiento y de inferencia — 41 criterios.
- Sección B — Operación de los datos — dividida entre operaciones de entrenamiento y de inferencia, con los mismos cinco códigos aplicados de forma distinta a cada fase — 10 criterios.
- Sección C — Gobernanza y ética — criterios organizacionales transversales, no específicos de ningún proyecto — 12 criterios.

La disciplina estructural central: los datos de entrenamiento y de inferencia portan obligaciones distintas incluso bajo el mismo código — el entrenamiento plantea procedencia, alcance del consentimiento, sesgos históricos y derechos de autor de las fuentes; la inferencia plantea validación en tiempo real y entradas adversarias y fuera de distribución. Cada criterio se expresa en la forma de dos roles que da rigor al marco: un requisito de evidencia que el practicante debe satisfacer, y una guía de evaluación aplicada para juzgarla — la misma separación « evidencia y luego juicio » que Origi impone en ejecución.

# 4. Sección A — Los criterios del ciclo de vida

Diez etapas portan cuarenta y un criterios. Cada una declara su alcance, su fase aplicable y las preocupaciones que sus criterios evalúan — los códigos se conservan para la trazabilidad hacia el libro de evaluación.

- Adquisición (AC-01…05) — base legal de la recogida (RGPD art. 6 / PIPEDA / CCPA), procedencia y cadena de custodia, sesgo de recolección, minimización, propiedad intelectual.
- Ingesta (IN-01…04) — validación de calidad, estandarización de formatos, seguridad en la ingesta (cifrado en tránsito, autenticación, registro), calidad del etiquetado.
- Integración (IT-01…04) — trazado del linaje de extremo a extremo, calidad entre fuentes, evaluación de amplificación de sesgos, gobernanza de la integración.
- Clasificación (CL-01…04) — sensibilidad (IPS, categorías especiales del art. 9 RGPD), clasificación regulatoria, etiquetado entrenamiento/inferencia, alineación de accesos.
- Almacenamiento (ST-01…05) — controles de seguridad en reposo (AES-256, gestión de claves, RBAC/ABAC), retención, respaldo y recuperación, registros de auditoría, resiliencia.
- Mantenimiento (MA-01…05) — vigencia de los datos, limpieza y corrección, reequilibrado y aumento, evolución de esquemas, integridad continua.
- Compartición y difusión (SH-01…05, solo inferencia) — gobernanza de la compartición, protección de la privacidad (anonimización, privacidad diferencial), gestión de encargados, limitación de uso.
- Archivo (AR-01…04) — política y procedimientos, seguridad y privacidad a largo plazo, documentación y metadatos, accesibilidad duradera (migración de formatos).
- Retiro (DR-01…05) — borrado seguro (borrado criptográfico, multiubicación), derecho de supresión, retirada de modelos, documentación de disposición.

## 5. Sección B — Los criterios de operación

Cinco criterios (OP-01…05) se evalúan dos veces — una para la fase de entrenamiento, otra para la inferencia — porque la misma preocupación se comporta distinto en cada una: vigilancia de calidad y deriva, vigilancia del desempeño, supervisión humana, sesgo y equidad, validación en tiempo real. Los criterios OP del lado de inferencia son el punto de encuentro más directo entre Aegis Assure y Origi: OP-03 (supervisión humana), OP-04 (equidad) y OP-05 (detección adversaria y fuera de distribución) describen, en términos de evaluación, exactamente los controles que el arnés de confianza de Origi ejecuta como aplicación en inferencia. Una organización que ejecuta Origi produce la evidencia de estos criterios como salida operativa.

# 6. Sección C — Gobernanza y ética

Doce criterios organizacionales se aplican a todo sistema y uso de datos — evalúan la madurez institucional, no un proyecto aislado.

- Gobernanza organizacional (GV-01…03) — estructura de gobernanza de la IA (comité de ética, supervisión del consejo), gestión de riesgos alineada con el NIST AI RMF, gestión del cumplimiento.
- Documentación y transparencia (DC-01…03) — documentación técnica (fichas de modelos y de conjuntos de datos), explicabilidad e interpretabilidad (XAI), evaluaciones de impacto algorítmico.
- Principios éticos y rendición de cuentas (ET-01…04) — equidad y no discriminación, transparencia y rendición de cuentas (recurso y contestación), impacto en derechos humanos, bienestar social.
- Formación y concienciación (TR-01…02) — formación y competencia del personal, cultura organizacional (mecanismos de denuncia, ejemplo del liderazgo).

# 7. Metodología de evaluación

La integridad del método descansa en la separación de funciones: los practicantes recogen y documentan la evidencia de cada criterio aplicable; los evaluadores la juzgan de forma independiente y asignan las puntuaciones. Nadie produce y juzga a la vez la evidencia del mismo criterio — el principio de separación de Origi aplicado a la evaluación.

- Gris — aún no evaluado — el estado por defecto.
- Verde — conforme — los controles son eficaces y la evidencia respalda la afirmación.
- Ámbar — parcial / brechas menores — los controles existen pero con deficiencias menores de diseño u operación.
- Rojo — no conforme — los controles faltan, son ineficaces o fallan significativamente.
- Crítico (C) — 40 % — un criterio Crítico bajo el umbral bloquea la acreditación hasta remediarse.
- Alto (H) — 30 % — exige un plan de remediación antes de la acreditación.
- Medio (M) — 20 % — activa una hoja de ruta de mejora.
- Bajo (L) — 10 % — foco de mejora continua.

La regla de bloqueo es lo decisivo: un buen promedio no compra un control Crítico fallido — el reflejo de la postura « fallo cerrado » de Origi. Y la salida de un encargo no es una nota sino un expediente: por criterio, su aplicabilidad, su evidencia, el razonamiento del evaluador, su calificación RAV y su estado de remediación — ensamblados en una acreditación de nivel de sistema con pista de auditoría defendible. En el lenguaje de Origi, ese expediente es el caso de aseguramiento de la gobernanza de datos del sistema.

## 8. Implantación y entrega

Flujo del practicante: alcance -> planificación -> recogida de evidencia (documentación, entrevistas, pruebas) -> documentación -> identificación de brechas -> autorrevisión de calidad -> entrega. Flujo del evaluador: revisión de la evidencia -> verificación (muestreo, pruebas, entrevistas) -> puntuación RAV -> documentación de hallazgos -> calibración entre pares -> informe (el expediente de acreditación) -> seguimiento de la remediación.

La acreditación es una posición que se mantiene, no un certificado que se archiva. La reevaluación se activa por: revisión anual de los sistemas de alto riesgo desplegados; cambio material del sistema (nuevas fuentes, cambio de algoritmo, ampliación de uso); cambio regulatorio; incidentes significativos o descubrimiento de sesgos; paso de piloto a producción. Miovski Group entrega el servicio en tres formas: una evaluación de preparación (exploración rápida de brechas, solo RAV), una acreditación completa (el ciclo íntegro de sesenta y tres criterios que produce el expediente) y un aseguramiento continuo (reevaluación recurrente según los disparadores, integrable con Origi).

# 9. Conclusión

El mercado ha pasado de preguntar si un sistema de IA funciona a exigir prueba de que los datos que lo sustentan se gobernaron responsablemente — y las normas que definen una buena respuesta han cambiado lo bastante como para dejar obsoleta gran parte de la documentación existente, incluidas las referencias regulatorias anteriores de este mismo marco. Esta edición hace las correcciones: la AIDA consta como muerta y no como pendiente, la Ley de IA de la UE como calendario vivo por fases y no como texto lejano, y la postura estadounidense como invertida.

Lo que no cambia: la estructura y el valor del marco — sesenta y tres criterios por todo el ciclo de vida, la disciplina entrenamiento-frente-a-inferencia, la gobernanza organizacional por encima de ambos, y un método de dos roles, « evidencia y luego juicio », que produce un expediente de acreditación defendible en lugar de una opinión. Situado en la pila Enkidu, Aegis Assure es la cara exterior de la misma filosofía de confianza que Origi impone dentro de los productos de Miovski Group — el caso de aseguramiento, la separación de funciones, la primacía de la evidencia — ofrecida como servicio a toda organización que hoy debe probar, y no meramente afirmar, que su IA está bien gobernada.

La confianza en un sistema de IA no es un eslogan que proclamar; es una posición que argumentar y evidenciar. Aegis Assure es cómo se construye esa posición, criterio a criterio.