



BLACKVAULT™

Constitutional Memory SA

LA PARADOJA DE LA MEMORIA

Informe Técnico y Estratégico para
Socios, Inversores y Directivos Empresariales

Constitutional Memory SA · Málaga, España · Constitutional Valley
www.Constitutional-Memory.ai · 2026

LA PROPUESTA DE BLACKVAULT™ EN UNA PÁGINA

Para el directivo que necesita lo esencial

El Problema

La IA es mucho más útil cuando te conoce. Pero cada vez que enseñas a una plataforma de IA algo sobre ti mismo, cedas ese conocimiento a un servidor en EE. UU. que no es tuyo. El 71 % de las exposiciones de datos empresariales se producen a través de plataformas de IA. El cumplimiento del RGPD depende de promesas de proveedores. Y cuanto más tiempo uses una sola plataforma, mayor será tu dependencia de ella.

La Solución

BlackVault™ separa la memoria del procesamiento. Tu cámara acorazada almacena tu historial completo de interacciones con IA —de todas las plataformas que utilizas— cifrado con tus claves, en tu jurisdicción, bajo tus normas de gobernanza. En cada consulta, recupera únicamente el contexto relevante, lo anonimiza e inyecta esa información en una llamada a la API sin retención hacia cualquier proveedor de IA que elijas. Obtienes respuestas de IA más ricas y personalizadas. El proveedor recibe una consulta anónima y no retiene nada. Tu inteligencia sigue siendo tuya.

Los Tres Pilares

- 1. Cámara Acorazada de Memoria Constitucional:** Tu soberanía. Tus claves. Tus reglas. Tu jurisdicción.
- 2. Hiper-personalización:** Un 62 % de mejora en las respuestas de IA. Efecto acumulativo con el tiempo. Portable entre plataformas.
- 3. Seguridad y Protección de la Propiedad Intelectual:** Llamadas a la API sin retención de datos. Cumplimiento arquitectónico del RGPD. Tu PI en tu cámara acorazada, no en la de ellos.

Por Qué Ahora

La Ley de IA de la UE está en vigor. El 92 % de los empleados de las empresas del Fortune 500 utilizan IA sin gobernanza. Las plataformas estadounidenses tienen un conflicto de intereses estructural que les impide ofrecer soberanía auténtica. La ventana de mercado para la infraestructura europea de gobernanza de IA es 2026-2028.

Por Qué las Grandes Tecnológicas de EE. UU. No Pueden Seguirnos

La soberanía de datos destruye su modelo de negocio. Necesitan tus datos. **BlackVault™** fue diseñado específicamente para garantizar que nunca los obtengan.

"La pregunta no es si existirá una infraestructura de gobernanza de IA. La pregunta es si será propiedad de instituciones europeas que responden ante la legislación y los valores europeos, o de corporaciones estadounidenses que responden ante sus accionistas y la CLOUD Act de EE. UU."

— Greg Malpass, Fundador y CEO, Constitutional Memory SA

Constitutional Memory SA © 2026

BLACKVAULT™

Constitutional Memory SA

LA PARADOJA DE LA MEMORIA

*Por Qué Cada Plataforma de IA Te Obliga a Elegir Entre Ser Conocido y Estar Seguro —y
Cómo BlackVault™ Pone Fin a Esa Elección Para Siempre*

ANTES DE QUE LEAS OTRA PALABRA

Un mensaje para el escéptico que sostiene este documento

"Ya estoy usando ChatGPT. Mi equipo lo usa a diario. Este año he visto cincuenta startups de IA. ¿Por qué esta es diferente?"

— La pregunta que todo directivo de Telefónica, director de innovación de Bosch y profesional de LinkedIn debería hacerse ahora mismo

Esa es exactamente la pregunta correcta. Y merece una respuesta directa.

La razón por la que BlackVault™ es diferente no es que sea una IA mejor. No compite con ChatGPT, Claude ni Gemini. No intenta construir un modelo de lenguaje más inteligente. Cada una de esas plataformas seguirá mejorando, y BlackVault™ funcionará con todas ellas.

BlackVault™ es diferente porque resuelve un problema que todas esas plataformas han elegido deliberadamente no resolver —porque resolverlo destruiría su modelo de negocio.

Ese problema es:

La Paradoja Personalización-Seguridad

La IA se vuelve drásticamente más útil cuanto más sabe sobre ti.

Pero cada vez que enseñas a una plataforma de IA sobre ti mismo, estás entregando ese conocimiento — tu contexto, tu historia, la inteligencia de tu empresa — a un servidor en Estados Unidos que no posees, no puedes auditar y del que no puedes recuperarte.

Hasta ahora, tenías que elegir entre una IA útil y una segura. BlackVault™ pone fin a esa elección.

PARTE UNO: EL PROBLEMA DEL QUE NADIE HABLA

Por qué la IA mejora para las plataformas — y se vuelve más arriesgada para ti

1.1 Cómo la IA Aprende Realmente a Conocerte

Comencemos con algo contraintuitivo que la mayoría de las personas no ha comprendido del todo.

Cuando hoy utilizas Claude, ChatGPT o Gemini, las respuestas que recibes son en gran medida genéricas. La IA no sabe quién eres, en qué estás trabajando, qué hace tu empresa, bajo qué marcos operas, cuál es tu estilo de comunicación o qué decisiones tomaste la semana pasada. Cada conversación comienza desde cero.

Pero ese no es todo el panorama. Porque con el tiempo, si sigues usando la misma plataforma, esta empieza a acumular cierta información sobre ti: tus patrones de consulta, tus preferencias, el contexto que proporcionas repetidamente. Y las respuestas mejoran.

La idea clave es esta: la mejora en la calidad de las respuestas de IA no proviene principalmente de que el modelo de IA sea más inteligente. Proviene de que la IA tiene **más contexto sobre ti específicamente**. El modelo es el motor. El contexto es el combustible.

Un ejemplo concreto — la misma pregunta, dos respuestas muy diferentes:

Pregunta sin contexto: "Redacta una nota de cumplimiento para nuestra reunión de consejo del tercer trimestre"

→ La IA produce una plantilla genérica. Útil como punto de partida. Requiere una edición significativa.

Pregunta con contexto enriquecido: "Redacta una nota de cumplimiento para nuestra reunión de consejo del tercer trimestre"

Contexto disponible: eres Directora de Cumplimiento en una fintech alemana que opera bajo MiFID II y RGPD. Tu consejo se reúne trimestralmente. Tu nota del segundo trimestre se centró en deficiencias en el seguimiento de transacciones. Tu CEO prefiere resúmenes en viñetas de menos de 800 palabras. Te preparas para una revisión de BaFin en noviembre.

→ **La IA produce un documento preciso, específico a la normativa, listo para el consejo. Requiere una edición mínima. Ahorra 3-4 horas de trabajo.**

Esa diferencia —genérico versus contextualmente rico— es lo que la literatura académica cuantifica en una mejora del 40-70 % en la relevancia y precisión de las respuestas. Nuestra prueba de concepto validada demuestra una mejora del 62 %. No es una ganancia marginal. Es la diferencia entre una herramienta y un colaborador inteligente de confianza.

1.2 El Pacto Fáustico que Ofrece Cada Plataforma de IA

Lo que cada gran plataforma de IA te propone realmente cuando ofrece una "IA mejorada y personalizada":

Lo que te dan:	Lo que te toman:
Mejores respuestas con el tiempo	Cada consulta que hayas hecho
Memoria de tus preferencias	El contexto confidencial de tu empresa
Asistencia contextualizada	Los perfiles profesionales de tus empleados
Ganancias de productividad	Tu inteligencia organizacional acumulada

Los datos que proporcionas para mejorar tu experiencia de IA no se almacenan para servirte a ti. Se almacenan para servir a la plataforma. Entrenan sus modelos. Crean dependencia. Construyen un perfil del conocimiento, las prioridades y las vulnerabilidades de tu organización que reside permanentemente en servidores de EE. UU. —sujetos a la legislación estadounidense, incluida la **CLOUD Act**, que otorga a las autoridades de EE. UU. acceso a los datos en poder de empresas estadounidenses independientemente del lugar físico donde se almacenen.

El 71 % de todas las exposiciones de datos empresariales en 2024 se produjeron a través de ChatGPT.

El 87 % de las filtraciones de datos sensibles ocurrieron a través de cuentas personales de ChatGPT utilizadas en el trabajo.

Fuente: Harmonic Security Enterprise Data Exposure Report, 2024

1.3 Por Qué las Plataformas No Resolverán Esto

La pregunta obvia es: ¿por qué OpenAI, Google y Anthropic no ofrecen simplemente una opción de soberanía? ¿Por qué no permitir que los clientes empresariales conserven sus datos y obtengan igualmente los beneficios de personalización?

La respuesta es estructural, no técnica. Son perfectamente capaces de construirla. Han optado por no hacerlo porque socavaría fundamentalmente su posición competitiva.

Si ofrecieran soberanía real de datos...	Perderían...
Tu historial de interacciones se mantiene en tu cámara acorazada	Los datos de entrenamiento que mejoran sus modelos
Tu perfil nunca se comparte con sus servidores	La inteligencia organizacional que crea dependencia
Puedes cambiar de proveedor de IA manteniendo tu contexto	Su mecanismo de retención más poderoso: el contexto acumulado
El conocimiento de tu empresa nunca se acumula en su plataforma	El activo estratégico de inteligencia que construyen con tus datos
Las empresas europeas cumplen el RGPD de forma nativa	El mercado europeo al que sirven actualmente con soluciones contractuales

No es un vacío que hayan pasado por alto. Es un vacío que han creado deliberadamente —y que pretenden mantener.

Por eso la Alianza Europea de Gobernanza de IA no puede estar liderada por una empresa tecnológica estadounidense, y por eso BlackVault™ se construye como infraestructura de propiedad europea. Las plataformas de EE. UU. tienen un conflicto de intereses estructural que les impide ofrecer auténtica soberanía de datos. Nosotros no.

PARTE DOS: LA SOLUCIÓN BLACKVAULT™

Cómo se resuelve la Paradoja de la Memoria — técnica y comercialmente

2.1 La Idea Central: Separación de Memoria y Procesamiento

El avance de BlackVault™ es conceptualmente simple, aunque la ingeniería sea sofisticada.

Cada plataforma de IA combina actualmente dos cosas que no necesitan estar combinadas:

- Memoria — la acumulación y almacenamiento de contexto sobre quién eres, qué haces y qué has preguntado antes
- Procesamiento — el trabajo intelectual real de comprender tu consulta y generar una respuesta

Las plataformas los combinan porque, cuando la memoria y el procesamiento están unificados en sus servidores, son dueños de ambos —y tu contexto acumulado se convierte en su activo.

BlackVault™ los desacopla. La memoria permanece contigo, en tu cámara acorazada cifrada. El procesamiento ocurre en la plataforma de IA que elijas. Los dos nunca tienen que estar en el mismo lugar.

La Analogía Postal (para lectores no técnicos):

Imagina que tienes un brillante asistente de investigación que puede responder cualquier pregunta, pero solo si le informas desde cero cada vez. Podrías:

Opción A: Darle al asistente un archivo permanente sobre ti y tu empresa. Se vuelve extraordinariamente útil —pero ahora es dueño del archivo y nunca puedes recuperarlo.

Opción B: Mantener tu propio archivo bajo llave en tu caja fuerte. Antes de cada pregunta, preparas una nota informativa solo con la información relevante, se la entregas al asistente, obtienes tu respuesta y recuperas la nota. El asistente no aprende nada permanente sobre ti. Tu caja fuerte se enriquece con cada interacción.

BlackVault™ es la caja fuerte. Y la preparación de la nota informativa es automática, instantánea e inteligente.

2.2 Cómo Funciona: La Arquitectura Técnica

Para el lector técnico —esto es exactamente lo que ocurre cuando un usuario de BlackVault™ hace una pregunta a una IA:

Paso 1: La Consulta Llega al Gateway de BlackVault™

La pregunta del usuario entra en el sistema antes de tocar cualquier proveedor de IA. Nunca va directamente a ChatGPT, Claude o Gemini. BlackVault™ la intercepta primero.

Paso 2: Recuperación Semántica desde la Cámara Acorazada (RAG)

Este es el núcleo técnico del sistema. BlackVault™ no vuelca simplemente todo el contenido de la cámara acorazada en cada llamada a la API. En su lugar, realiza una búsqueda de similitud semántica en el contenido almacenado. La cámara acorazada almacena no transcripciones de texto bruto sino fragmentos embebidos —segmentos del historial de interacciones, datos de perfil y contexto convertidos en vectores matemáticos que representan su significado.

Paso 3: Anonimización e Inyección de Contexto

Antes de que la consulta enriquecida salga del gateway de BlackVault™, se aplica un filtro de dos etapas: eliminación de datos sensibles y pseudonimización consistente. Lo que recibe el proveedor de IA contiene todo lo necesario para ser genuinamente útil —y nada que no debería tener.

Ejemplo de prompt enviado al proveedor de IA:

"Estás asistiendo a un fundador que se prepara para reunirse con el director de un parque tecnológico regional. El fundador lidera una plataforma de gobernanza de IA empresarial centrada en la soberanía de datos. Las reuniones anteriores con este director han abordado: oportunidades de asociación en el ecosistema, presentaciones a empresas de telecomunicaciones miembros, y el concepto de posicionar la ciudad como centro europeo de infraestructura ética de IA. El objetivo de la reunión de hoy es asegurar presentaciones a dos empresas miembro específicas para conversaciones piloto."

Nota: Sin nombres reales. Sin nombres de empresa. Sin identificadores de ubicación. Sin datos financieros propietarios.

Paso 4: Llamada a la API sin Retención

La consulta enriquecida y anonimizada se envía al proveedor de IA mediante una llamada API estándar. Desde la perspectiva del proveedor, esta es una solicitud única y sin estado. Reciben un prompt rico en contexto y devuelven una respuesta de alta calidad. El proveedor no retiene nada. No hay persistencia de sesión. No hay acumulación de perfil. No hay historial almacenado en sus servidores.

Paso 5: Registro de Respuesta y Enriquecimiento de la Cámara Acorazada

La respuesta del proveedor regresa a través del gateway. El sistema registra la interacción —tanto la consulta como la respuesta— de vuelta en la cámara acorazada cifrada del usuario. La cámara acorazada se enriquece. La próxima consulta se beneficiará de que esta interacción esté disponible para su recuperación. El efecto acumulativo: una cámara acorazada con seis meses de historial produce una recuperación drásticamente mejor que una con una semana.

2.3 La Ventaja Multiplataforma: Por Qué Esto Es Más Grande que Cualquier IA Individual

Ahora mismo, tus interacciones con IA están compartimentadas. Lo que le has dicho a ChatGPT, solo ChatGPT lo sabe. Lo que le has dicho a Claude, solo Claude lo sabe. No comparten información. Esto significa que ninguna plataforma tiene nunca una imagen completa de tu contexto profesional —y cada vez que cambias de plataforma, comienzas desde cero.

BlackVault™ rompe este silo permanentemente.

La cámara acorazada multiplataforma en la práctica:

- Lunes: Usas ChatGPT para redactar un análisis de mercado. BlackVault™ lo registra.
- Martes: Usas Claude para refinar tu pitch de inversores. BlackVault™ lo registra.
- Miércoles: Usas Gemini para prepararte para una entrevista técnica. BlackVault™ lo registra.
- Jueves: Preguntas a cualquier plataforma de IA: "¿Cuáles son los tres puntos más sólidos de mi pitch dado lo que sé sobre las prioridades de este inversor específico?"

BlackVault™ recupera el contexto del análisis del lunes, el trabajo del pitch del martes y tus datos de perfil sobre el inversor —e inyecta todo ello como un briefing coherente. Ninguna plataforma individual podría hacer esto. Solo tu cámara acorazada puede.

Este es el foso estratégico que se acumula con el tiempo. Cada interacción — en cualquier plataforma — enriquece tu bóveda. Cuanto más tiempo uses **BlackVault™**, más valiosa se vuelve tu bóveda y mayor será la diferencia entre tu experiencia de IA y la de alguien que empieza desde cero en cualquier plataforma.

Y a diferencia de un perfil que poseen OpenAI o Google, tu bóveda viaja contigo. Si mañana surge un mejor modelo de IA, cambias de proveedor y te llevas toda la inteligencia acumulada contigo. Sin bloqueo. No hay vueltas a empezar. Portabilidad total.

PARTE TRES: LOS TRES PILARES DE BLACKVAULT™

Lo que ofrece — para cada tipo de usuario

1 CÁMARA ACORAZADA DE MEMORIA CONSTITUCIONAL

Tu inteligencia de IA. Tus claves de cifrado. Tu jurisdicción. Tus reglas.

La cámara acorazada es el fundamento de todo lo que hace BlackVault™. No es un sistema de almacenamiento en la nube ni una base de datos simple. Es una "arquitectura constitucional" — un sistema construido sobre el principio de que tu inteligencia de IA acumulada es un activo soberano que te pertenece, gobernado por reglas que tú estableces, almacenado donde tú eliges, accesible únicamente para quienes tú autorizas.

Lo que contiene la cámara

- Historial completo de interacción de todas las plataformas de IA que conectes a BlackVault™
- Tu perfil personal u organizativo — construido a través de una evaluación personalizada de 170 preguntas profundas, incluyendo la importación de perfiles de LinkedIn (si procede)
- Bases de conocimiento específicas de los roles — marcos profesionales, contextos regulatorios, estilos de comunicación
- Contexto del documento — materiales que eliges añadir para su recuperación (documentos estratégicos, investigación, resúmenes)
- Inteligencia de relaciones — contexto sobre personas, organizaciones y proyectos en curso con los que interactúas
- Inteligencia temporal — cómo han evolucionado tu pensamiento y prioridades a lo largo del tiempo

Gobernanza constitucional — lo que la hace verdaderamente soberana:

A diferencia de cualquier sistema de almacenamiento en la nube o software empresarial, **BlackVault™** aplica la "gobernanza constitucional" a tus datos. Tú defines las reglas:

Dimensión de Gobernanza	Lo Que Controlas
Ubicación de los datos	Tus propios servidores, tu nube privada, tu jurisdicción elegida — Frankfurt, Londres, Singapur, en las instalaciones
Cifrado	Trae Tu Propia Clave (BYOK) — ciframos con tus claves, lo que significa que matemáticamente no podemos acceder a tus datos
Política de retención	Define qué interacciones se registran, durante cuánto tiempo y bajo qué condiciones se purgan
Derechos de acceso	Quién dentro de tu organización puede consultar la cámara acorazada, qué puede recuperar y qué está restringido
Permisos de compartición	Qué contexto se inyecta para qué tipos de consulta — tú estableces las reglas, no nosotros
Portabilidad	Exporta tu cámara acorazada completa en cualquier momento, en formatos abiertos, a cualquier sistema que elijas

Una constitución no es un contrato que puede renegociar la parte más poderosa. Es un conjunto fundamental de reglas que rigen cómo opera un sistema —reglas que no pueden ser anuladas por presión comercial, cambios en los términos de servicio o adquisición por un nuevo propietario. La arquitectura de BlackVault™ es constitucional en este sentido. Tus derechos de soberanía de datos no son promesas en una política de privacidad. Están embebidos en la arquitectura.

2 HIPERPERSONALIZACIÓN Y RESPUESTAS DE IA MEJORADAS

IA que te conoce profundamente — sin saber quién eres.

El segundo pilar es el que los usuarios sienten más inmediatamente. Con **BlackVault™** activo, la calidad de tus interacciones con IA mejora respecto a la primera consulta — y se acumula drásticamente con el tiempo.

La mejora del 62%: qué significa y de dónde viene

Nuestra prueba de concepto validada demuestra una mejora del 62% en la calidad de respuesta de la IA en comparación con las consultas no contextualizadas en las mismas plataformas. Esta cifra es coherente con la literatura académica sobre sistemas de Generación Aumentada por Recuperación, que muestra consistentemente una mejora del 40-70% en la relevancia y precisión de la respuesta.

La mejora del 62 % se manifiesta en cuatro dimensiones:

Dimensión	Con BlackVault™
Relevancia	Respuesta precisa a tu situación específica en lugar de una respuesta genérica
Precisión	Calibrada para tus marcos normativos y contexto organizacional específicos
Eficiencia	La primera respuesta suele estar lista para ser utilizada, sin necesidad de 2-3 prompts de seguimiento
Continuidad	Cada consulta se basa en el contexto acumulado — como un colega que estuvo en cada reunión anterior

Por qué mejora con el tiempo — el efecto de inteligencia acumulativa:

En el mes uno, tu cámara acorazada contiene tu perfil y quizás unas pocas semanas de historial de interacciones. La mejora es notable.

En el mes seis, tu cámara acorazada contiene cientos de interacciones, contexto de rol refinado, inteligencia relacional y un registro detallado de cómo ha evolucionado tu pensamiento sobre proyectos clave.

En el año dos, tu cámara acorazada es un activo de inteligencia organizacional de genuino valor estratégico. Y porque esta inteligencia vive en tu cámara acorazada —no en los servidores de ninguna plataforma— es tuya permanentemente.

Hiperpersonalización entre tipos de usuario

Usuario	Lo que ofrece la hiperpersonalización
Empleado de la Enterprise (ENT)	IA que conoce tu rol, los marcos de cumplimiento de tu empresa, tus preferencias de comunicación, tus proyectos actuales, el contexto de tus compañeros — produciendo resultados listos para el trabajo en segundos en lugar de minutos
Profesional (PRO)	IA que conozca tu trayectoria profesional, tus relaciones con clientes, tu experiencia profesional, tu carácter y personalidad, tus habilidades, fortalezas y debilidades, tu estilo de comunicación, tus planes y ambiciones y tu trabajo

Esta es una traducción de un documento original al inglés que pueda contener errores u omisiones

	continuo — un colaborador inteligente permanente que crece con tu vida personal y carrera. (Nota: a medida que la IA asuma muchos roles profesionales en el lugar de trabajo, estas habilidades blandas registradas serán aún más cruciales para la progresión profesional y vital)
Estudiante (EDU)	IA que conoce tu estilo de aprendizaje, tu currículo, tus fortalezas y carencias académicas, tu trabajo previo — un tutor que realmente entiende en qué punto estás en tu camino de aprendizaje
Familia (SHIELD)	Interacciones de IA adecuadas a la edad gobernadas por normas parentales almacenadas en la cámara familiar — un contexto que protege a los niños mientras permite una asistencia educativa genuina en IA

3 SEGURIDAD DE DATOS Y PROTECCIÓN DE LA PROPIEDAD INTELECTUAL

El único sistema de gobernanza de IA donde tus datos nunca salen de tu control — por arquitectura, no por promesa.

El tercer pilar es el que más importa para los CISOs, responsables de cumplimiento, reguladores y directores de consejos (el motor de la brecha estimada de 4.800 millones de dólares en el mercado de gobernanza de la IA). Y es la que más directamente demuestra por qué las grandes plataformas tecnológicas estadounidenses no pueden ofrecer lo que **ofrece BlackVault™**.

La garantía arquitectónica

La mayoría de las empresas de software empresarial hacen promesas de seguridad de datos. Políticas de privacidad. Acuerdos de procesamiento de datos. Compromisos contractuales de no usar tus datos para formación. Estos son instrumentos legales — y los instrumentos legales pueden ser modificados, violados, reinterpretados o anulados por adquisición, cambio regulatorio o bancarrota.

La seguridad de BlackVault™ es arquitectónica. La garantía no es "prometemos no revisar tus datos". La garantía es "somos matemáticamente incapaces de ver tus datos, porque tú posees las claves de cifrado."

La garantía no es "no compartiremos tus datos con proveedores de IA." La garantía es "los proveedores de IA solo reciben consultas anonimizadas sin retención — no hay nada que compartir, porque nunca les llega nada identificable."

La llamada API de cero retención — explicada con precisión

Cada interacción con un proveedor de IA a través de **BlackVault™** está estructurada de la siguiente manera:

Qué llega al proveedor de IA	Lo que nunca llega al proveedor de IA
Un prompt del sistema anónimo y enriquecido en contexto	Tu nombre o el nombre de cualquier empleado
Una descripción genérica del contexto profesional	El nombre de tu empresa o cualquier dato identificativo

La pregunta específica, despojada de información personal	Tu historial completo de chats
Dominio relevante y contexto regulatorio (anonimizado)	Tus perfiles de empleados
Una solicitud de respuesta específica y de alta calidad	Cualquier dato financiero, de cliente o estratégico propietario

Desde la perspectiva del proveedor de IA, cada **interacción con BlackVault™** parece una consulta profesional anónima y cuidadosamente preparada. No tienen forma de saber quién lo envió, de qué organización proviene ni cuántas interacciones previas corresponde. No retienen nada porque no hay nada identificable que conservar.

Cumplimiento normativo (un motor clave del mercado): por arquitectura, no por papeleo

BlackVault™ — Cumplimiento normativo por arquitectura

Gobernanza de la IA en todas las jurisdicciones y modelos de despliegue

Cómo leer esta tabla: Cada fila compara la exposición regulatoria creada por el despliegue de plataformas tradicionales de IA (ChatGPT Enterprise, Google Gemini, Microsoft Copilot) con la posición arquitectónica **que BlackVault™** alcanza por diseño. La distinción en todo el juego es la misma: las plataformas tradicionales hacen promesas legales; **BlackVault™** ofrece garantías arquitectónicas.

Codificación de color de columna: Tinte rojo = exposición/riesgo en plataformas tradicionales. Tinte verde = **posición arquitectónica BlackVault™**. Las filas de categoría indican el modelo de despliegue aplicable.

Plataforma tradicional — Exposición / Riesgo	BlackVault™ — Posición Arquitectónica	Empresa y Generales	Sanidad	Educación	Seguridad familiar / SHIELD
--	---------------------------------------	---------------------	---------	-----------	-----------------------------

Regulación / Jurisdicción	Plataforma tradicional de IA — Exposición	BlackVault™ — Posición Arquitectónica
ENTERPRISE & GENERAL — Aplicable a todos los despliegues		
RGPD de la UE Artículo 28 (Procesamiento de datos)	El proveedor de IA es el procesador de datos; Se requiere DPA con cada proveedor; se necesitan mecanismos de transferencia transfronteriza; Complejidad de auditoría entre procesadores de terceros	El proveedor de IA no recibe ningún dato personal — no existe ninguna relación de procesamiento de datos; no se requiere DPA con los proveedores de IA; la empresa es la única responsable de los datos; La complejidad del cumplimiento del RGPD se redujo en ~70%
Ley de IA de la UE (Aplicación de la ley de agosto de 2025)	Solo cumplimiento contractual; registros de auditoría dependientes de la cooperación entre proveedores; El marco de gobernanza se basa en promesas de terceros; penalizaciones de hasta 35 millones de euros o un 7% de los ingresos globales	Cumplimiento arquitectónico; Un seguimiento de auditoría completo e inmutable guardado en la bóveda de la empresa; La interacción con el proveedor de IA se registraba completamente internamente; La gobernanza está completamente bajo el control de la empresa — no hay dependencia del proveedor
Ley CLOUD de EE. UU.	Todos los datos en los servidores de proveedores de IA con sede en EE. UU. están sujetos a solicitudes de acceso del gobierno estadounidense, independientemente de las protecciones contractuales de privacidad o de la ubicación física del servidor en la UE	No hay datos de la empresa, empleados o clientes en servidores propiedad de EE. UU.; La Ley CLOUD no dispone de datos a los que acceder; La soberanía europea de los datos es genuina, no contractual
BaFin (Alemania) FINMA (Suiza) FCA (Reino Unido)	Los datos fluyen hacia servidores de IA con sede en EE. UU.; viola los estrictos requisitos de residencia de datos de servicios financieros; se requiere una diligencia debida compleja por parte del proveedor; Exposición regulatoria continua	Los perfiles e historial de interacción permanecen en centros de datos de la UE/Reino Unido elegidos por la empresa; solo las consultas API totalmente anonimizadas cruzan jurisdicciones; cumple con estrictos requisitos de residencia de datos por arquitectura
RGPD — Artículo 5 Minimización de datos	Los proveedores de IA reciben el contenido completo de consultas, incluyendo todo el detalle contextual; no hay mecanismo técnico de minimización; límites contractuales no aplicables a nivel de consulta	La canalización de inyección de contexto aplica la minimización de datos automáticamente — solo se transmite el contexto semánticamente relevante y anonimizado; la minimización es arquitectónica, aplicada a cada llamada a API
SANIDAD — EMPRESA		
HIPAA (EE. UU.) (Seguro de salud Portabilidad y Ley de Responsabilidad)	Riesgo de exposición a datos de pacientes mediante el uso de IA por parte de empleados; ninguna protección técnica que impida que PHI acceda a las indicaciones de IA; Responsabilidad por incumplimiento de HIPAA si los identificadores de pacientes llegan a los servidores de proveedores de IA	Identificadores de pacientes y PHI eliminados por la tubería de anonimización antes de cualquier llamada a la API; desplegado en configuración compatible con HIPAA; No es necesario BAA con los proveedores de IA porque no reciben ninguna PHI

EDUCACIÓN — MODELO EDU		
FERPA (EE.UU.) (Educación familiar Ley de Derechos y Privacidad)	Los registros educativos de los estudiantes procesados a través de plataformas de IA pueden constituir una violación de la FERPA; las instituciones que reciben financiación federal enfrentan responsabilidad directa; no hay salvaguardas técnicas disponibles en plataformas estándar; Exposición legal en gran medida no reconocida	Los registros educativos de los estudiantes nunca se transmiten a los proveedores de IA; Institutional Vault contiene todo el contexto educativo bajo las normas de gobernanza establecidas por institución; El cumplimiento de FERPA es arquitectónico: ninguna PII de estudiante sale nunca del archivo
COPPA (EE. UU.) (Children's Online Ley de Protección de la Privacidad — menores de 13 años)	Técnicamente, las plataformas de IA están prohibidas de recopilar datos personales de menores de 13 años sin consentimiento parental verificable; Los mecanismos de las puertas de edad se eluden fácilmente; responsabilidad institucional significativa si los menores utilizan herramientas de IA desplegadas en la escuela	Usuarios menores de 13 años identificados en la bóveda; Datos regulados por COPPA nunca se transmiten; El proveedor de IA solo recibe consultas anonimizadas y adecuadas para su edad; El consentimiento parental está integrado en las reglas de gobernanza de la bóveda — conforme por diseño
RGPD de la UE — Artículo 8 (Consentimiento de los niños)	Se requiere consentimiento parental para el tratamiento de datos de menores de 13 a 16 años (el umbral varía según el estado miembro); prácticamente imposible de hacer cumplir cuando el hijo interactúa directamente con la plataforma de IA; Riesgo continuo de cumplimiento de ICO y DPA	La identidad y los datos personales del niño nunca llegan al proveedor de IA; Las reglas de gobernanza de la bóveda imponen interacciones apropiadas a la edad; El consentimiento parental es constitucional — está integrado en las reglas del refugio, no depende de la cooperación de la plataforma
UK Age Appropriate Design Code (Children's Code — ICO)	Las plataformas que probablemente sean accedidas por niños deben implementar la privacidad desde el diseño; ICO multó a TikTok con 12,7 millones de libras por infracciones; La exposición a ChatGPT y Gemini bajo este código no está cuantificada, pero es material	El diseño adecuado a la edad es arquitectónico: el proveedor de IA nunca sabe que un niño es el usuario; no es posible el perfilado de niños por parte de proveedores de IA; El cumplimiento de las ICO es una consecuencia de la arquitectura, no un compromiso de política
KOSA (EE. UU.) (Ley de Seguridad en Línea de Niños — en progreso)	Obligaciones propuestas de deber de cuidado para plataformas utilizadas por menores; si se implementa, la arquitectura actual de la plataforma de IA enfrenta una responsabilidad estructural; La adaptación de la normativa en modelos existentes será compleja y costosa	BlackVault™ SHIELD anticipa los requisitos de KOSA — la gobernanza parental, la supervisión transparente y las normas de contenido adecuadas a la edad son fundamentales para la arquitectura; No se requiere adaptación
SEGURIDAD FAMILIAR — MODELO DE ESCUDO		
COPPA (EE. UU.) (Children's Online Ley de Protección de la Privacidad)	Los mecanismos de consentimiento parental en las plataformas de IA son en gran medida teatro; datos recogidos rutinariamente para menores de 13 años; la aplicación es débil pero la responsabilidad real; Los padres no tienen visibilidad sobre qué datos se recogen sobre sus hijos	Los datos de los niños nunca salen de la cámara familiar; los padres establecen las normas constitucionales de gobernanza; El proveedor de IA solo recibe consultas anonimizadas — el cumplimiento de la COPPA es estructural; Los padres tienen visibilidad y control total

RGPD de la UE — Artículo 8 (Consentimiento de los niños — contexto familiar)	Los niños que utilizan plataformas de IA en los estados miembros de la UE activan requisitos de consentimiento del Artículo 8 que las plataformas no pueden satisfacer prácticamente; Exposición de datos familiares en curso y sin supervisión	Family Vault contiene todo el contexto de interacción infantil; El consentimiento parental es la norma constitucional que rige la bóveda; El proveedor de IA no recibe nada identificativo — Artículo 8 cumplido por arquitectura
Reino Unido apropiado para la edad Código de diseño (Contexto familiar / SHIELD)	Cualquier servicio de IA al que un niño probablemente acceda debe implementar el Código de los Niños por defecto; las plataformas actuales de IA tienen un cumplimiento limitado; Aumento de la aplicación de ICO tras precedentes de TikTok	SHIELD implementa el diseño adecuado a la edad como principio fundamental — no como un complemento de cumplimiento; el proveedor de IA nunca perfila al niño; La gobernanza de la bóveda familiar es constitucional y está controlada por los padres
KOSA (EE. UU.) (Seguridad en línea de los niños — contexto familiar)	Las obligaciones de deber de cuidado requerirían que las plataformas mitiguen los daños a menores; las plataformas actuales de IA carecen de la arquitectura de gobernanza para demostrar el cumplimiento; Los controles parentales son superficiales	La capa de gobernanza constitucional de SHIELD proporciona una infraestructura demostrable de deber de atención; las normas parentales se aplican arquitectónicamente; Seguimiento completo de auditoría de las interacciones con IA infantil almacenadas en la caja fuerte familiar bajo control parental

Visión clave: La exposición regulatoria de EDU y SHIELD en las plataformas actuales de IA es en muchos aspectos más aguda que el riesgo de cumplimiento empresarial.

Un distrito escolar que despliega ChatGPT para uso de los estudiantes puede estar infringiendo simultáneamente FERPA, COPPA y el Artículo 8 del RGPD — en la mayoría de los casos sin tener conocimiento de esta exposición. Los datos infantiles conllevan las sanciones regulatorias más altas, las mayores consecuencias reputacionales y la atención legislativa que evoluciona más rápidamente en todas las jurisdicciones principales.

BlackVault™ EDU y SHIELD abordan todo esto a través de la misma garantía arquitectónica que rige los despliegues empresariales: el proveedor de IA nunca recibe datos sobre el niño, el estudiante o la familia. El cumplimiento no es una política. Es una consecuencia de la arquitectura.

La exposición regulatoria de EDU y SHIELD para las plataformas de IA estadounidenses es en muchos aspectos más aguda que el riesgo de cumplimiento empresarial. Los datos infantiles conllevan las sanciones regulatorias más altas, las mayores consecuencias reputacionales y la atención legislativa que evoluciona más rápidamente en todas las jurisdicciones principales. Que un distrito escolar despliegue ChatGPT para uso estudiantil sin una capa de soberanía podría estar violando simultáneamente FERPA, COPPA y el Artículo 8 del RGPD — y en la mayoría de los casos no tiene conocimiento de esta exposición. BlackVault™ EDU y SHIELD abordan los tres mediante la misma garantía arquitectónica que rige los despliegues empresariales: el proveedor de IA nunca recibe datos sobre el niño, el estudiante o la familia. El cumplimiento no es una política. Es una consecuencia de la arquitectura.

Protección de la PI — el riesgo que nadie está cuantificando

Más allá del cumplimiento normativo, existe una dimensión de protección de la propiedad intelectual que la mayoría de las organizaciones aún no han comprendido del todo.

Cada vez que un empleado pregunta a una plataforma de IA sobre una estrategia competitiva, una hoja de ruta de producto, la situación de un cliente o una metodología propietaria, esa consulta, y la respuesta de la IA a ella, se registra en los servidores de la plataforma. Con el tiempo, las consultas

acumuladas de los empleados de tu organización constituyen una imagen detallada de tus prioridades estratégicas, tus relaciones con los clientes, tu pensamiento sobre el producto y tus vulnerabilidades competitivas.

No eres dueño de esa imagen de inteligencia. No sabes quién más puede acceder a él. No puedes borrarlo. Y bajo los términos de servicio actuales de la mayoría de las grandes plataformas de IA, se han concedido a la plataforma amplios derechos para usarla.

El riesgo de acumulación de PI — un escenario específico:

Una consultora de 500 personas utiliza ChatGPT Enterprise. Durante 18 meses, sus empleados han hecho 2,3 millones de consultas sobre compromisos con clientes, análisis competitivo, estrategia de precios y desarrollo de propuestas.

Este corpus de consultas representa el mapa de inteligencia más detallado de su negocio jamás elaborado — más completo que cualquier programa de inteligencia competidor que podría producir a partir de fuentes externas.

Está en los servidores de OpenAI. No de ellos.

Con **BlackVault™**, ese corpus de 2,3 millones de consultas se encuentra en la cámara cifrada de la empresa — enriqueciendo sus respuestas de IA cada día, aumentando en valor y permaneciendo permanentemente bajo su control. Su inteligencia competitiva es su activo, no el de la plataforma.

PARTE CUATRO: PARA QUIÉN ES BLACKVAULT™

Cuatro modelos. Una arquitectura. Una propuesta de valor diferente para cada uno.

BlackVault™ is a single architectural platform that serves four fundamentally different user types through four distinct models. The underlying technology is the same. The value it delivers — and the conversation that opens the door — is different for each

EMPRESARIAL — BlackVault™ para Organizaciones

Para el CISO, el Director de Cumplimiento y el CFO.

La conversación que abre la puerta:

"¿Sabes dónde están guardadas las conversaciones de IA de tus empleados ahora mismo? ¿De qué país? ¿En qué servidor? ¿Quién tiene acceso? Porque si la respuesta no es tu propio centro de datos o nube privada, tienes un problema de cumplimiento y una exposición a la propiedad intelectual que probablemente aún no hayas cuantificado."

Por qué pagan:

350-750 € por empleado al año
frente a 900-1.500 € para alternativas de retallos
frente a 100 millones de euros+ para una versión propietaria

El despliegue empresarial ofrece simultáneamente los tres pilares: soberanía de bóveda para la protección de la propiedad intelectual, respuestas mejoradas para la productividad y cumplimiento arquitectónico de las obligaciones regulatorias. La Ley de IA de la UE genera una presión obligatoria para la compra. Los datos de Harmonic Security demuestran que el problema es real. La mejora del 62% demuestra que la solución es valiosa.

Esta es una traducción de un documento original al inglés que pueda contener errores u omisiones

PRO — BlackVault™ para Profesionales Individuales

Para el abogado, el consultor, el ingeniero, el ejecutivo, el profesional creativo.

La conversación sobre el PRO empieza de forma diferente. No se trata de cumplir. Se trata del profesional que ha pasado años desarrollando su experiencia y ahora observa cómo las herramientas de IA simultáneamente les hacen más productivos y acumulan su inteligencia profesional en el servidor de otra persona.

La bóveda del usuario PRO se convierte en su activo de inteligencia profesional: un registro continuo y completo de su conocimiento profesional, relaciones y desarrollo, que lleva a través de empleadores, plataformas y a lo largo de su carrera. Ningún empleador es el propietario. Ninguna plataforma lo posee. Es suya.

Piénsalo como la evolución de tu perfil de LinkedIn — pero privado, vivo y genuinamente completo. LinkedIn muestra al mundo una instantánea seleccionada: tus títulos de puesto, tus recomendaciones, tu resumen estático. Tu **perfil de BlackVault™ PRO** es la versión que existe solo para ti — actualizada continuamente a través de tus interacciones reales con IA, enriquecida (al momento del registro) con una evaluación profunda de 170 preguntas e importable directamente desde LinkedIn como punto de partida. No solo captura lo que has hecho, sino también cómo piensas, cómo trabajas, tu estilo de comunicación, tus patrones de toma de decisiones, tus fortalezas y áreas de desarrollo honesto, tus objetivos y motivaciones. A medida que la IA se encarga cada vez más de la ejecución técnica en todas las profesiones, esta capa de inteligencia humana —personalidad, juicio, estilo de trabajo, inteligencia relacional— se convierte en lo más valioso profesionalmente que posees. **BlackVault™ PRO** lo convierte en la base de cada interacción con IA que tengas, en todas las plataformas, durante el resto de tu carrera. Nueve cientos millones de usuarios de LinkedIn ya han señalado que entienden el valor de una capa de identidad profesional para el networking. **BlackVault™ PRO** es en lo que se convierte esa capa cuando funciona para ti (en mentoría e interacción con IA) en lugar de para una plataforma publicitaria.

El beneficio de la hiperpersonalización es especialmente evidente para los usuarios de PRO. En cuestión de semanas, la IA con la que interactúan a **través de BlackVault™** conoce su dominio, sus clientes, su estilo de escritura, sus desafíos recurrentes, sus aspiraciones y sus prioridades profesionales de una manera que ninguna interacción genérica de IA puede alcanzar.

EDU — BlackVault™ para Estudiantes y Educadores

Para el estudiante, el profesor/docente y la institución que navega la transformación educativa de la IA.

La educación es el ámbito donde el debate sobre la adopción de la IA resulta más confuso. Las instituciones intentan simultáneamente prohibir el uso de la IA (inútil), adoptarla sin crítica (peligroso) y encontrar un camino intermedio que nadie ha definido claramente.

BlackVault™ EDU define ese camino intermedio. La cámara del estudiante conoce su historial de aprendizaje, su currículo, sus fortalezas y carencias, su trabajo previo y sus opiniones, y sus objetivos académicos. La asistencia de IA a **través de BlackVault™** se contextualiza en su propio proceso de aprendizaje — no solo respondiendo preguntas o haciendo sus trabajos por ellos, sino ayudándoles a desarrollar comprensión. El uso de calculadoras estaba prohibido para estudiantes en el pasado, luego el uso de Google, ahora es IA.

La capa de gobernanza de la institución garantiza que las interacciones con IA apoyen el aprendizaje en lugar de reemplazarlo — con registros completos de auditoría, transparencia y normas constitucionales que tanto la institución como el estudiante acepten.

La dimensión regulatoria de los despliegues de EDU es más grave de lo que la mayoría de las instituciones han comprendido. Una universidad o centro que despliegue ChatGPT directamente para uso estudiantil puede estar violando simultáneamente la FERPA (si los registros educativos de los estudiantes se procesan sin las salvaguardas adecuadas), la COPPA (si algún usuario tiene menos de 13 años) y el Artículo 8 del RGPD (si los datos de los estudiantes de la UE se procesan sin mecanismos de consentimiento apropiados para la edad). Estos no son riesgos teóricos: son consecuencias estructurales de enrutar los datos de los estudiantes a través de plataformas de IA propiedad de

Estados Unidos. **BlackVault™** EDU resuelve los tres mediante la misma garantía arquitectónica: los registros de identidad y educación del estudiante nunca salen del refugio institucional, y el proveedor de IA solo recibe consultas anonimizadas y enriquecidas contextualmente. El cumplimiento de FERPA y COPPA no se logra mediante un Acuerdo de Procesamiento de Datos que pueda ser renegociado. Se logra porque no hay nada identificable que regular en el punto de interacción con la IA.

SHIELD — BlackVault™ para Familias

Para padres que quieren que sus hijos se beneficien de la IA sin renunciar a su seguridad.

SHIELD es el modelo más importante para lo personal — y el que habla más directamente de los valores que sustentan toda la arquitectura **de BlackVault™**.

Los niños son los usuarios más vulnerables de las plataformas de IA. Comparten libremente, no leen los términos de servicio, y los perfiles que las plataformas de IA construyen sobre los intereses, ansiedades, relaciones y patrones de aprendizaje de los niños representan una violación profunda y permanente de la privacidad.

SHIELD otorga a los padres un gobierno constitucional sobre las interacciones con IA de sus hijos. Las reglas establecidas en la cámara familiar determinan qué contexto se inyecta, qué se bloquea, qué es apropiado para la edad y qué se informa a los padres. El niño se beneficia de una ayuda de IA realmente útil y contextualizada. La plataforma solo recibe consultas anónimas y adecuadas para su edad. La cámara familiar contiene el contexto sensible — no el servidor de una plataforma publicitaria.

Para los padres en Estados Unidos, la COPPA ofrece protección legal explícita a los menores de 13 años, pero su aplicación depende enteramente de que las plataformas implementen barreras de edad verificables, lo que en la práctica significa poco. El Artículo 8 del RGPD y el Código de Diseño Apropiado para la Edad del Reino Unido ofrecen protecciones más sólidas en Europa, con consecuencias financieras reales: la ICO multó a TikTok con 12,7 millones de libras por no implementar la privacidad adecuada a la edad desde el diseño. La próxima Ley de Seguridad en Línea para Niños de EE. UU. (KOSA) extenderá las obligaciones de cuidado a cualquier plataforma que utilice una menor. **BlackVault™** SHIELD es la única arquitectura de gobernanza de IA que satisface todos estos aspectos simultáneamente, no a través del cumplimiento de políticas, sino porque la identidad, los patrones de comportamiento y el historial de interacción del niño nunca llegan al proveedor de IA en primer lugar. No hay datos que puedan hacer un mal uso. La protección no está garantizada. Es estructural.

PARTE CINCO: EL PANORAMA MÁS AMPLIO

Por qué esto importa más allá de cualquier producto individual — ¡y por qué el momento es ahora!

5.1 El Desenlace Final del Capitalismo de Vigilancia

La trayectoria del desarrollo de la IA, si nada cambia, conduce a un solo resultado: cada interacción profesional y personal significativa que un ser humano tiene — mediada a través de la IA, que cada vez es cada vez más cada interacción — será registrada, analizada y monetizada por un pequeño número de empresas tecnológicas estadounidenses.

Esto no es especulación. Es la dirección declarada del modelo de negocio de todas las grandes plataformas de IA. La IA es la interfaz. Los datos generados a través de esa interfaz son el producto. El valor de ese producto aumenta con cada usuario, cada interacción, cada año.

La cuestión no es si esta tendencia está ocurriendo. Lo importante es si es posible ofrecer una alternativa — una que ofrezca los beneficios genuinos de productividad de la IA sin exigir a los usuarios renunciar a la inteligencia que generan al usarla.

BlackVault™ es esa alternativa. Y la razón por la que es viable ahora, cuando hace tres años no lo era, es que el entorno regulatorio — especialmente en Europa — finalmente ha alcanzado la tecnología.

5.2 Por Qué las Grandes Tecnológicas de EE. UU. No Pueden Seguirnos

La pregunta más común de inversores sofisticados y socios potenciales es: "¿Por qué OpenAI o Google no construyen esto ellos mismos?"

La respuesta es estructural:

La pregunta más común de inversores sofisticados y posibles socios es: "¿Por qué OpenAI o Google no lo construyen ellos mismos?"

La respuesta es estructural, y es importante entender con precisión:

Si una plataforma estadounidense ofrece verdadera soberanía de datos...	Las consecuencias para su negocio
La bóveda del cliente contiene todo el historial de interacción	La plataforma pierde la canalización de datos de entrenamiento que mejora sus modelos
Llamadas API sin retención — sin datos de clientes almacenados	La plataforma pierde el activo de inteligencia organizativa construido tras años de consultas a los clientes
El cliente puede cambiar de proveedor de IA y tomar su contexto	La plataforma pierde su mecanismo de retención más potente: el contexto acumulado
No hay análisis de datos entre clientes	La plataforma pierde los efectos de red que justifican sus múltiplos de valoración actuales
Cumplimiento empresarial europeo por arquitectura	La plataforma reconoce que su modelo actual es fundamentalmente incompatible con el RGPD, lo que supone un riesgo de litigio

Este no es un problema tecnológico que no puedan resolver. Es un problema de modelo de negocio que no pueden resolver mientras siguen siendo las empresas que son. Toda su valoración se basa en la acumulación de datos. Ofrecer soberanía genuina sería auto-liquidación.

Este es el foso competitivo de **BlackVault™**. No es una patente. No es una característica. Un conflicto de intereses estructural que impide que las empresas con más recursos del mundo compitan en este ámbito — siempre que **BlackVault™** avance lo suficientemente rápido para establecer el estándar antes de que se produzca la consolidación.

El plazo es 2026-2028. Después de eso, ocurre una de dos cosas: o bien se consolida en torno a estándares europeos que **BlackVault™** ha establecido, o las plataformas estadounidenses encuentran formas de ofrecer productos relacionados con la soberanía que sean lo suficientemente atractivos para cerrar la brecha regulatoria. El objetivo de la Alianza Europea de IA-Gobernanza es garantizar lo primero.

5.3 La Visión de "Constitutional Valley"

BlackVault™ tiene su sede en Málaga, España —una ciudad que se está posicionando como **Constitutional Valley**: la alternativa europea al modelo de capitalismo de vigilancia de Silicon Valley.

Silicon Valley construyó las empresas tecnológicas más valiosas de la historia sobre el principio de que los datos de los usuarios son un recurso a extraer y monetizar. Este modelo produjo una innovación extraordinaria. También produjo Cambridge Analytica, los Archivos de Facebook, la crisis de cumplimiento del RGPD, la CLOUD Act de EE. UU. y tasas de exposición de datos empresariales del 71 %.

Constitutional Valley se construye sobre el principio opuesto: que la inteligencia generada por un ser humano a través de sus interacciones con sistemas de IA pertenece a ese ser humano — constitucional, arquitectónica y prácticamente.

BlackVault™ es la implementación técnica de ese principio. La Alianza Europea de Gobernanza de IA será su expresión institucional. Constitutional Valley es su hogar geográfico.

Esta es una traducción de un documento original al inglés que pueda contener errores u omisiones

PARTE SEIS: ANÁLISIS TÉCNICO EN PROFUNDIDAD

Para ingenieros, arquitectos y evaluadores técnicos

6.1 La Arquitectura RAG en Detalle

Estrategia de fragmentación e incrustación

La calidad de la recuperación depende totalmente de la calidad de la estrategia de fragmentación y incrustación. **BlackVault™** utiliza un enfoque híbrido de fragmentación:

1. Fragmentación semántica: Las transcripciones de interacción se dividen en límites semánticos naturales — cambios de tema, transiciones de entidades, cambios de intención — en lugar de contar caracteres o tokens arbitrarios
2. Fragmentación consciente de la entidad: El reconocimiento de entidades nombradas identifica personas, organizaciones, proyectos, fechas y términos específicos de dominio, asegurando que los fragmentos preserven el contexto de la entidad
3. Estructura jerárquica: Cada fragmento se almacena con metadatos (marca de tiempo, fuente de plataforma, contexto de sesión, etiquetas de entidad, clasificación de temas) que permiten una recuperación multidimensional

Las incrustaciones se generan usando un modelo dedicado (no el mismo modelo usado para la generación). El modelo de incrustación convierte cada fragmento en una representación vectorial de alta dimensión de su significado semántico. Estos vectores se almacenan en una base de datos vectorial dentro de la bóveda cifrada.

Mecanismo de recuperación

En cada consulta, se ejecuta el siguiente proceso:

1. La consulta entrante se incrusta usando el mismo modelo de incrustación
2. Una búsqueda de similitud coseno identifica los segmentos de bóveda más semánticamente similares semánticamente (configurables, normalmente top 10-20)
3. Un paso de reclasificación aplica puntuación adicional: ponderación por recencia, puntuación por solapamiento de entidades, retroalimentación explícita de relevancia de interacciones previas
4. Los trozos de K superiores (tras reclasificar) se seleccionan para la inyección (normalmente 5-10, dependiendo del presupuesto de ventana contextual)
5. Un gestor de presupuesto de tokens asegura que el contexto ensamblado no exceda la ventana de contexto del modelo objetivo, priorizando por puntuación final de relevancia

Canalización de anonimización

El paso de anonimización no es un simple reemplazo de palabras clave — ese enfoque es frágil y fácil de derrotar. **BlackVault™** utiliza una tubería de PLN de varias etapas:

- Reconocimiento de entidades nombradas (NER): Identifica todos los nombres de personas, nombres de organizaciones, ubicaciones, fechas, cifras financieras e identificadores específicos de dominio
- Resolución contextual: Resuelve las co-referencias ("ella", "la empresa", "nuestro cliente") a sus entidades subyacentes para una anonimización consistente
- Seudonimización con consistencia: Sustituye a las entidades identificadas por seudónimos consistentes dentro de una sesión ("Persona A", "Organización B") para que la IA pueda razonar sobre relaciones sin conocer las identidades

- Detección de patrones sensibles: detección basada en expresiones regulares y aprendizaje automático de datos estructurados sensibles (números de cuenta, identificadores de historiales médicos, valores de contratos) con reglas de redacción configurables
- Validación de paso: Un modelo secundario evalúa el prompt anonimizado en busca de información identificativa residual antes del despacho de la API

Formato de inyección de contexto

El último prompt enviado al proveedor de IA está estructurado como:

System message:

[Anonymised role and domain context from profile]

[Relevant vault context chunks, ranked and summarised]

[Constitutional rules: response format, length, style preferences]

User message:

[Anonymised, cleaned user query]

API parameters:

stream: true | temperature: [user-configured] | max_tokens: [budget-managed] | no session persistence

6.2 Arquitectura de Seguridad

Modelo de cifrado

- Cifrado en reposo: AES-256 en todos los datos de la bóveda, con la arquitectura de gestión de claves determinada por el modelo de despliegue
- Cifrado en tránsito: TLS 1.3 para todas las comunicaciones, incluidas las consultas internas de la bóveda
- BYOK (Bring Your Own Key): En despliegues empresariales y locales, el KMS (AWS KMS, Azure Key Vault o HSM local) contiene las claves maestras de cifrado — Constitutional Memory SA no tiene acceso
- Arquitectura de conocimiento cero: En los despliegues de BYOK, la propia infraestructura de Constitutional Memory no puede descifrar los datos de la bóveda del cliente

Opciones de arquitectura de despliegue

Modelo	Dónde residen los datos del refugio	Quién posee las claves de cifrado	Enrutamiento de llamadas API
En las instalaciones	Hardware propio del centro de datos del cliente	HSM en las instalaciones del cliente	Desde la red del cliente — IP nunca abandona las instalaciones
Nube privada	Cuenta del cliente en AWS/Azure/GCP, región elegida por el cliente	Customer's cloud KMS (BYOK)	A través de la VPC del cliente — Constitutional Memory nunca recibe tráfico
Soberano gestionado	Infraestructura de Memoria Constitucional, región elegida por el cliente	KMS del cliente (BYOK) — no podemos descifrar	Vía Memoria Constitucional — cifrado, conocimiento cero

Infraestructura de auditoría y cumplimiento

- Registro de auditoría inmutable: Cada acceso a la bóveda, cada operación de recuperación, cada llamada a la API registrada con encadenamiento de hash criptográfico — no puede ser modificado retroactivamente
- Registro de procesamiento del Artículo 30 del RGPD: Generado automáticamente a partir de los registros de actividad de la bóveda
- Registro de auditoría de la Ley de IA de la UE: Procedencia completa de interacción para decisiones reguladas de IA
- SOC 2 Tipo II: Ruta de certificación incluida en la hoja de ruta del Año 1
- ISO 27001: Ruta de certificación incluida en la hoja de ruta del segundo año

6.3 Arquitectura de Integración

Integración con proveedores de IA

BlackVault™ se integra con cualquier proveedor de IA que exponga una API estándar. Objetivos actuales de integración:

- OpenAI (GPT-4o, GPT-4 Turbo, serie o1/o3)
- Anthropic (Claude Sonnet, Claude Opus)
- Google (Gemini 1.5 Pro, Gemini Ultra)
- Mistral (proveedor domiciliado en la UE — preferido para despliegues sensibles a la soberanía)
- Modelos de código abierto vía Ollama o inferencia local similar (para despliegues totalmente air-gapped)

La arquitectura independiente del proveedor permite **que los usuarios de BlackVault™** enruten diferentes tipos de consultas a distintos proveedores según el coste, la capacidad o los requisitos de cumplimiento — y cambiar de proveedor sin perder el contexto de la bóveda.

Integración de sistemas empresariales

1. Proveedores de identidad: integración SAML 2.0 y OIDC para SSO empresarial (Okta, Azure AD, Google Workspace)
2. Sistemas de documentos: Ingesta selectiva desde SharePoint, Google Drive, Confluence — scraping controlado por el usuario, no automatizado
3. Plataformas de comunicación: Ingesta opcional de contexto de mensajes de Slack/Teams (requiere consentimiento explícito del usuario por mensaje)
4. Herramientas de IA existentes: SDK para envolver despliegues de IA existentes con **la pasarela BlackVault™** — no es necesario copiar y reemplazar

PARTE SIETE: LA PROPUESTA BLACKVAULT™ EN UNA PÁGINA

Para el responsable de la toma de decisiones que necesita la esencia

El problema

La IA es mucho más útil cuando te conoce. Pero cada vez que enseñas a una plataforma de IA sobre ti mismo, entregas ese conocimiento a un servidor estadounidense que no te pertenece. El 71% de las exposiciones a datos empresariales ocurren a través de plataformas de IA. El cumplimiento del RGPD depende de las promesas de los proveedores. Y cuanto más tiempo uses una sola plataforma, más atrapado te quedas.

La solución

BlackVault™ separa la memoria del procesamiento. Tu bóveda almacena todo tu historial de interacción con IA — de todas las plataformas que utilices — cifrado con tus claves, en tu jurisdicción, bajo tus normas de gobernanza. En cada consulta, solo recupera el contexto relevante, lo anonimiza e inyecta en una llamada API de cero retención a cualquier proveedor de IA que elijas. Obtienes respuestas de IA más ricas y personalizadas. El proveedor recibe una consulta anónima y no retiene nada. Tu inteligencia sigue siendo tuya.

Los Tres Pilares

1. Bóveda de la Memoria Constitucional: Tu soberanía. Tus llaves. Tus reglas. Tu jurisdicción.

2. Hiperpersonalización: 62% mejores respuestas de IA. Se va componiendo con el tiempo. Portátil entre plataformas.

3. Seguridad y protección IP: Llamadas API sin retención. Cumplimiento arquitectónico del RGPD. Tu IP en tu bóveda, no la de ellos.

¿Por qué ahora

La Ley de IA de la UE está en vigor. El 92% de los empleados de empresas Fortune 500 utilizan IA sin gobierno. Las plataformas estadounidenses tienen un conflicto de intereses estructural que les impide ofrecer soberanía genuina. La ventana de mercado para la infraestructura de gobernanza de IA propiedad de Europa es 2026-2028.

Por qué las grandes tecnológicas estadounidenses no pueden seguir

La soberanía de los datos destruye su modelo de negocio. Necesitan tus datos. **BlackVault™** fue diseñado específicamente para asegurarse de que nunca lo reciban.

"La cuestión no es si existirá infraestructura de gobernanza de la IA. La cuestión es si será propiedad de instituciones europeas que responden a la legislación y valores europeos — o de corporaciones estadounidenses que responden a sus accionistas y a la Ley CLOUD de EE. UU.."

— Greg Malpass, fundador y CEO, Constitutional Memory SA

Contacto y próximos pasos

Constitutional Memory SA está creando la Alianza Europea de IA-Gobernanza — una coalición de 10-14 empresas europeas fundadoras que cofinanciarán y copropietariarán la infraestructura de gobernanza de la que dependerán sus plantillas.

Si este documento ha planteado preguntas que desea que se respondan —técnica, comercial o estratégicamente— damos la bienvenida a esa conversación.

Contact	Details
Greg Malpass — Founder & CEO	destinyinvestors@btinternet.com
Línea directa	+44 (0) 7850 230 692
Sede	Málaga, Spain — Constitutional Valley
Oficina estratégica	London, UK
Sitio web	www.Constitutional-Memory.ai
Referencia del documento	BlackVault™ USP Briefing — The Memory Paradox — 2026

Constitutional Memory SA © 2026

BlackVault™ — Soberanía Total de Datos para la IA Empresarial

Tu Inteligencia. Tu Cámara Acorazada. Tus Reglas.

Constitutional Memory SA · Málaga, España · Constitutional Valley
www.Constitutional-Memory.ai · 2026

