2026

ARGORIX™

FROM TECHNICAL CAPABILITIES TO AI-DRIVEN GOVERNANCE WORKFLOWS

WWW.ARGORIX.COM

ARGORIX

¿SABÍAS QUÉ?

IA COMO CAPACIDAD CRITICA

Uso de la IA mundialmente:
Aproximadamente el 76% de las organizaciones están usando IA

Tecnologías:
71% de las organizaciones usan IA generativas del estilo ChatGpt, Gemini, copilot.

Madurez y gobierno:
Sólo el 1% de las organizaciones tiene gobernado, controlado, inventariado sus IAs.

DESAFÍO ACTUAL: CUMPLIMIENTO Y RIESGOS

Costos de una fuga de información: Según IBM Risk report 2025, el costo de una brecha de datos puede llegar a los 4.4. MUSD.

El shadow AI (IA desconocida): Eleva los riesgos de seguridad, los costos de explotación y una niebla de incertidumbre en cómo gobernar y que gobernar

Compliance: Muchos países LATAM ya comenzaron con la adopción de la ley de protección de datos, las IAs son una fuente explotable que se debe proteger.

SOLUCIÓN ¿CÓMO TE AYUDAMOS?

Para resolver esto, hemos creado un GobiernoIA un ecosistema de soluciones que no vende software, sino Madurez Digital.

Nuestra soluciones se basan en una premisa simple: No existe Gobierno de IA sin una base sólida en gestión del riesgo.

Por eso, nuestro camino tiene cuatro estaciones obligatorias que transforman el riesgo en ventaja competitiva, **consultoria, Agentic AI , Formación y Automatización del gobierno de IA.**

IDENTIFICA — **PROTEGE** — **GOBIERNA**

WWW.ARGORIX.COM

CAMINO A LA GOBERNANZA DE IA

Una hoja de ruta diseñada para gestionar el riesgo según tú nivel de madurez

1. Crear Inventario de la IA
2. Definir responsables
3. Establecer controles básicos
4. Medir y monitorear su uso

ARGORIX

WWW.ARGORIX.COM

ARGORIX

¿Que hacemos?

CONSULTORIA EN IA

Evaluación de Impacto (EIPD-IA), Políticas e implementación de gobernanza en IA.

CAPACITACIÓN Y CERTIFICACIONES

1. Integrar la Seguridad en los Flujos de Trabajo de Desarrollo y Operaciones (DevSecOps).
2. Manténgase a la vanguardia dominando la seguridad en tecnologías de punta.
3. Protección de aplicaciones de software contra vulnerabilidades y amenazas

Único partner autorizado en chile & Latam

Practical DevSecOps

AI AGENTIC ENGINEERING

Desarrollamos e integramos sistemas de IA bajo el paradigma de "Secure-by-Design

SAAS GOVERNANCE AI

El motor tecnológico que permite el monitoreo dinámico y la visibilidad total del riesgo

Frameworks Automatizados de forma inteligente

ARGORIX

Impacto Directo P&L Corporativo

El Gobierno de IA no es compliance, **es eficiencia operativa** de última generación.

Sin gobernanza, la innovación se queda trabada y expuesta a riesgos.

Con gobernanza, habilitamos un ciclo de captura de valor acelerado que nos permite **monetizar casos de uso antes que nadie.**

Esto hace que nuestro portafolio sea f**inancieramente más potente y operativamente más ágil,** consolidando una Arquitectura de Confianza que permite a la empresa escalar IA sin fricciones.

Aceleración del Time-to-Revenue

Si un modelo de personalización que genera US$1M mensuales es posible acelerarlo gacias a una gobernanza ágil, habilitando la salida a producción y la captura de valor.

Aumento del rate de éxito del portfolio

Si el costo de desarrollar un PoC es de US$200k y el 70% falla antes de producir revenue, mejorar ese ratio de éxito mediante gobernanza recupera millones en capital de trabajo.

Optimización de OPEX

Reducción directa en el gasto operativo (Opex) de entre un 15% y 30% mediante la centralización de licencias y la eliminación de redundancias de desarrollo entre distintos departamentos

Protección ante riesgo de Multas

Evita multas que pueden llegar al 4% de la facturación anual y protege el Brand Equity. Es mucho más barato invertir en gobernanza que pagar el costo de una brecha de seguridad o una demanda colectiva por sesgo algorítmico

ARGORIX

PROPÓSITO:

"Ser el estándar regional de confianza que permita a las organizaciones adoptar la Inteligencia Artificial y explotar su valor de forma segura transformando la gobernanza y cumplimiento normativo en una ventaja competitiva".

PARTNERS

arxia

JHED AI ARTIFICIAL INTELLIGENCE

CCHIA CÁMARA CHILENA DE INTELIGENCIA ARTIFICIAL

Practical DevSecOps

ARGORIX

¿Qué es GovernanceAI?

Nuestra solución

Infraestructura tech que convierte la IA en un activo de negocio, **seguro, rentable y escalable.**

01

Arquitectura Confiable

- Evita alucinaciones de IA
- Eliminación del shadow AI
- Evita fraudes por mal uso de datos sensibles
- Cumplimiento Nativo
- Soberanía de datos
- Gobernanza ética

02

Acelerador del Revenue

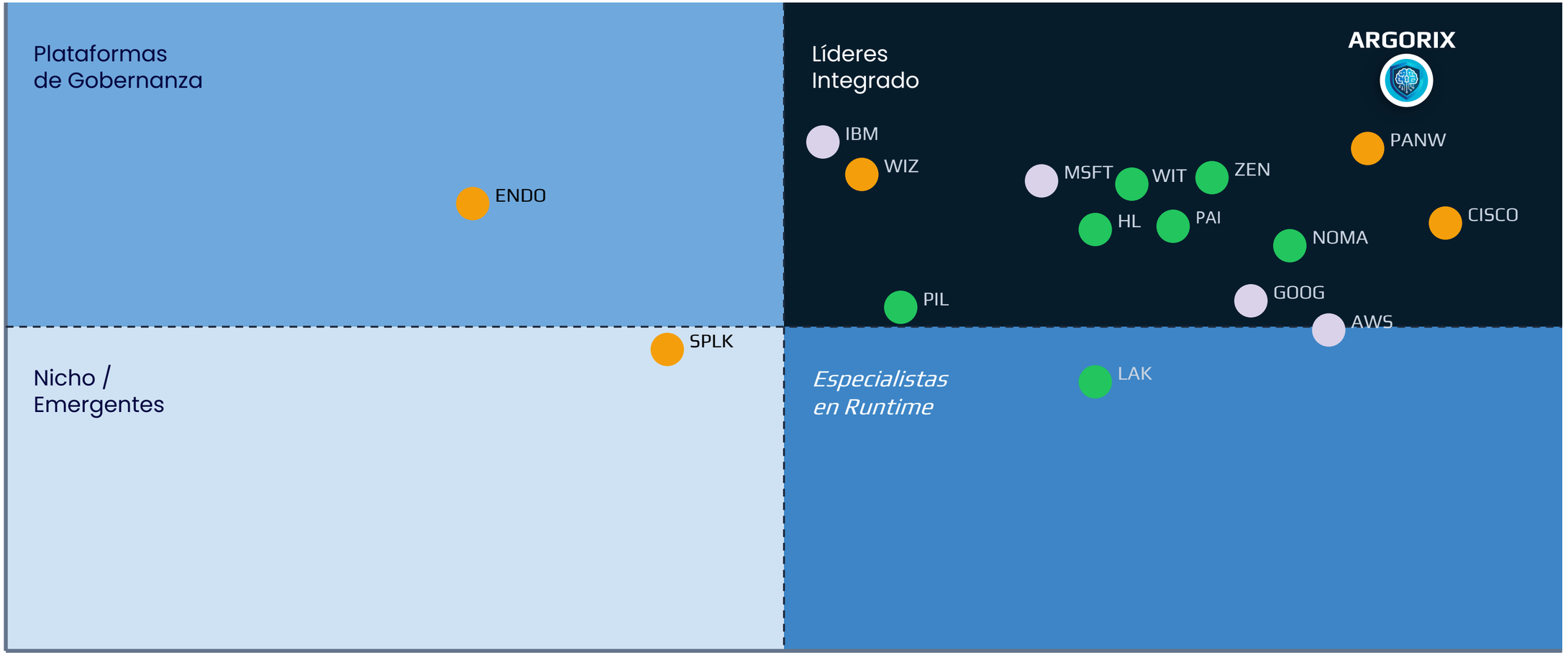
- Aceleración del time to value
- Acelerador del éxito de iniciativas de IA.
- Desbloqueo de casos de uso de alto potencial
- Optimizador de Opex

Con **GovernanceA**I, pasamos de tener '***proyectos de IA***' *a tener un 'negocio gestionado apalancado en IA'.*

La Arquitectura de Confianza protege su marca, el **Acelerador de Revenue** nos hace llegar primero al mercado y el Tablero Financiero asegura que cada dólar invertido en tokens sea rentable.

Posicionamiento Argorix

Por qué ARGORIX se diferencia en este mercado



WWW.ARGORIX.COM

2026

ARGORIX™

SaaS Product

ARGORIX

WWW.ARGORIX.COM

ARGORIX

ARQUITECTURA MODULAR

Anexo: Detalle Modular

SHADOW AI DISCOVER

Descubre y mapea el uso real de IA dentro de la organización

ARGORIX

1. INPUT

¿Qué entra?

- Tráfico web y de red
- Logs de acceso a herramientas de IA
- Aplicaciones SaaS
- Endpoints y dispositivos
- Encuestas y reportes de usuarios
- Políticas y catálogos de herramientas aprobadas

2. PROCESO

¿Qué hace?

- Detecta herramientas y modelos de IA en uso
- Analiza patrones de acceso y frecuencia
- Clasifica el nivel de riesgo y criticidad
- Identifica usuarios, equipos y áreas que utilizan IA
- Genera inventario y mapa de uso de IA (Shadow AI)

3. OUTPUT

¿Qué entrega?

- Inventario de herramientas de IA detectadas
- Mapa de adopción por área, usuario y herramienta
- Nivel de riesgo por herramienta y uso
- Alertas de uso no aprobado o riesgoso
- Reportes y dashboards listos para análisis

4. OUTCOME

¿Qué logra?

- Visibilidad completa del uso real de IA
- Identificación temprana de riesgos y brechas
- Priorización de acciones de gobernanza
- Base sólida para políticas, controles y capacitación
- Reducción del riesgo operacional y reputacional

5. IMPACTO / VALOR AGREGADO

¿Cuál es el impacto?

- Gobernanza informada y basada en datos
- Uso seguro, responsable y alineado a políticas
- Mayor productividad con menor riesgo
- Cumplimiento normativo y protección de datos
- Confianza y adopción sustentable de la IA

Shadow AI Discover es el primer paso para gobernar la IA: **sin visibilidad, no hay control.**

GOVERNANCE SHIELD DLP

Protege datos sensibles frente al uso inseguro de IA y automatizaciones

ARGORIX

1. INPUT

¿Qué entra?

- Políticas de datos y de seguridad
- Clasificación de información
- Flujos de datos y repositorios
- Accesos y uso de herramientas de IA
- Contenido generado por usuarios
- Registros de actividad y eventos

2. PROCESO

¿Qué hace?

- Detecta datos sensibles en uso y tránsito
- Clasifica y etiqueta información automáticamente
- Aplica políticas DLP en interacciones con IA
- Bloquea, enmascara o alerta ante riesgos
- Monitorea fuga, exfiltración y uso indebido de datos
- Registra y audita todos los eventos

3. OUTPUT

¿Qué entrega?

- Alertas de fuga o uso indebido de datos
- Registro detallado de eventos DLP
- Clasificación y etiquetado de información
- Reportes de exposición y tendencias
- Dashboard de cumplimiento y riesgos
- Logs auditables para forense y cumplimiento

4. OUTCOME

¿Qué logra?

- Prevención efectiva de fuga de información
- Cumplimiento de políticas y regulaciones
- Control del uso de datos en IA y automatizaciones
- Reducción de incidentes y exposición
- Trazabilidad y auditoría completa

5. IMPACTO / VALOR AGREGADO

¿Cuál es el impacto?

- Protección efectiva de datos sensibles
- Cumplimiento regulatorio y reducción de riesgo legal
- Confianza organizacional y de usuarios
- Mejora en la postura de seguridad
- Uso responsable y seguro de la IA

Governance Shield DLP asegura que los **datos correctos** estén protegidos, en el **lugar correcto**, para el **uso correcto.**

AGENT COMPLIANCE BUILDER

Diseña, valida y documenta proyectos de IA alineados con normas y políticas

ARGORIX

1. INPUT

¿Qué entra?

- Requerimientos del proyecto de IA
- Casos de uso y objetivos
- Normativas, estándares y marcos regulatorios
- Políticas internas y lineamientos
- Modelos, agentes y datasets propuestos
- Arquitectura y flujos del sistema

2. PROCESO

¿Qué hace?

- Evalúa cumplimiento normativo y de políticas
- Identifica y analiza riesgos del modelo y del uso
- Define controles y salvaguardas requeridos
- Valida diseño, datos y gobernanza
- Genera documentación y evidencia automáticamente
- Guía mejoras para cumplimiento y ética

3. OUTPUT

¿Qué entrega?

- Documento de cumplimiento del proyecto
- Matriz de riesgos y controles
- Checklist normativo aplicable
- Blueprint de arquitectura y flujos
- Evidencia y reportes auditables
- Recomendaciones de mitigación y mejoras

4. OUTCOME

¿Qué logra?

- Proyectos de IA diseñados con cumplimiento desde el inicio
- Reducción de riesgos regulatorios y éticos
- Aprobación y auditoría más rápida
- Trazabilidad y transparencia de decisiones
- Estándares consistentes para todos los proyectos

5. IMPACTO / VALOR AGREGADO

¿Cuál es el impacto?

- Cumplimiento asegurado desde el diseño
- Menor riesgo legal, financiero y reputacional
- Escalabilidad segura de soluciones de IA
- Confianza de auditores, clientes y usuarios
- Aceleración de la innovación responsable

Agent Compliance Builder asegura que cada proyecto de IA **cumpla normativas, políticas y estándares** desde el diseño.

AI RED TEAM & LIVE

Evalúa la resistencia de tus modelos y agentes frente a ataques y comportamientos inseguros

ARGORIX

1. INPUT

¿Qué entra?

- Modelos de IA y LLMs
- APIs, endpoints y flujos de integración
- Prompts y workflows existentes
- Datos y contexto de negocio (no sensibles)
- Escenarios de amenaza y vectores de ataque
- Políticas y reglas de seguridad

2. PROCESO

¿Qué hace?

- Diseña y ejecuta pruebas adversarias automatizadas y manuales
- Simula ataques reales: prompt injection, jailbreaking, data leakage, toxicidad, etc.
- Evalúa comportamiento de agentes y herramientas
- Mide resistencia, sesgos y exposición de datos
- Clasifica y prioriza vulnerabilidades
- Valida mitigaciones y re-test en vivo

3. OUTPUT

¿Qué entrega?

- Reporte de vulnerabilidades detectadas
- Evidencias de ataques exitosos (prompts, outputs)
- Nivel de riesgo por vulnerabilidad y modelo
- Matriz de impacto y probabilidad
- Recomendaciones técnicas y de mitigación
- Dashboard de métricas y tendencias

4. OUTCOME

¿Qué logra?

- Identificación de debilidades antes de ser explotadas
- Modelos y agentes más robustos y seguros
- Reducción del riesgo operacional y reputacional
- Mejora continua basada en pruebas reales
- Confianza en el despliegue y uso seguro de IA

5. IMPACTO / VALOR AGREGADO

¿Cuál es el impacto?

- IA resiliente frente a ataques reales y emergentes
- Menor probabilidad de incidentes y brechas
- Protección de datos, usuarios y marca
- Cumplimiento normativo y estándares de seguridad
- Ventaja competitiva en confianza y adopción

AI Red Team & Live prueba lo que los atacantes harían, para que tu IA sea **segura en el mundo real.**

GUARDRAILS & AGENTS

Válida y restringe el comportamiento de agentes y modelos en tiempo real

ARGORIX

1. INPUT

¿Qué entra?

- Prompts e interacciones de usuarios
- Respuestas generadas por el modelo
- Modelos y agentes en uso
- Políticas, reglas y restricciones
- Contexto y datos de la sesión
- Historial de interacciones y eventos

2. PROCESO

¿Qué hace?

- Valida prompts e intenciones antes de procesar
- Detecta contenidos, ataques y comportamientos riesgosos
- Aplica guardrails y políticas en tiempo real
- Bloquea o modifica respuestas no permitidas
- Enruta a revisión humana cuando corresponde
- Aprende y mejora reglas continuamente

3. OUTPUT

¿Qué entrega?

- Respuestas seguras y alineadas a políticas
- Eventos bloqueados y alertas en tiempo real
- Logs auditables de decisiones y acciones
- Métricas de cumplimiento y uso seguro
- Reportes y dashboards de comportamiento
- Trazabilidad completa por sesión e interacción

4. OUTCOME

¿Qué logra?

- Prevención de abusos, jailbreaks y filtraciones
- Comportamiento confiable y consistente del modelo
- Reducción de incidentes y exposición
- Cumplimiento operativo en tiempo real
- Mejor experiencia de usuario y confianza en la IA

5. IMPACTO / VALOR AGREGADO

¿Cuál es el impacto?

- IA segura y controlada en producción
- Protección de datos, usuarios y marca
- Cumplimiento normativo y políticas corporativas
- Reducción de riesgos legales y reputacionales
- Adopción sostenible y escalable de la IA
- Confianza y ventaja competitiva

Guardrails & Agents mantiene tus modelos y agentes dentro de los límites definidos, en cada interacción, en tiempo real.

WWW.ARGORIX.COM

ARGORIX

Listo para el desafio?

SALES@ARGORIX.COM

*La **IA** ya está ocurriendo.*
*La gobernanza **aún no...***

Sé el primero en liderar la gestión de IA de forma segura!!

ARGORIX