practia

A company of
publicis
sapient

Insight Anual 2026

PRIORIDADES, TENDENCIAS Y DESAFÍOS TI

Carta del director

Estimados CIOs, CEOs y líderes empresariales:

Es un privilegio presentarles **la edición 2026 de nuestro Insight Anual,** una iniciativa que busca orientar a quienes marcan la agenda tecnológica en la región.

Este año damos un paso más: dejamos atrás el diagnóstico y avanzamos hacia la acción. Porque la tecnología ya no solo acompaña a la estrategia, sino que se convierte en su motor central.

La Inteligencia Artificial como eje cultural, la irrupción de agentes autónomos, la necesidad de construir confianza digital, la reinvención de la infraestructura tecnológica, la evolución de los modelos de seguridad, el gobierno inteligente de los datos y la resiliencia de las operaciones son hoy fuerzas que están transformando la manera de concebir y dirigir las organizaciones.

En este escenario, nuestra responsabilidad es ofrecer una lectura crítica y anticipatoria que ayude a capitalizar estas tendencias con mirada estratégica y enfoque latinoamericano.

Para ello, hemos reunido la experiencia de especialistas y líderes de Practia con el objetivo de identificar los movimientos clave y analizar sus implicancias en la gestión y en la dirección de negocio.

Este informe fue diseñado como una herramienta que no solo interpreta los retos inmediatos, sino que también abre espacio para reflexionar sobre las decisiones que definirán el futuro cercano.

Nuestra intención es aportar perspectivas que faciliten la adopción de tecnologías disruptivas, fortalezcan la capacidad de adaptación y potencien la innovación en cada ámbito de la empresa.

En un entorno de constante disrupción, **el verdadero desafío no reside en incorporar soluciones tecnológicas aisladas, sino en convertirlas en resultados visibles: mayor resiliencia, organizaciones más ágiles y un crecimiento sostenible en el tiempo.** Ese es el propósito de este Insight y también la esencia de nuestro rol como socio tecnológico de confianza en América Latina.

Agradecemos a todos quienes confían en nuestro trabajo y esperamos que las siguientes páginas les ofrezcan tanto inspiración como herramientas prácticas para liderar con éxito la próxima etapa de la transformación digital.

Atentamente,
Sabrina Vázquez Soler
COO LATAM, Practia —
a Publicis Sapient company

Contenido

01 Panorama 2026 LATAM: Un renacer tecnológico

Cada gran cambio tecnológico dio origen a un nuevo tipo de empresa.

La mecanización impulsó la fábrica moderna. La informática masiva creó la corporación digital. Internet redefinió los modelos de escala.

Hoy, nos encontramos ante el surgimiento de un nuevo arquetipo organizacional sostenido en el ***modelo Frontier Firm.***

Este término fue **acuñado por Microsoft,** nuestro Partner, en el contexto de su investigación sobre el futuro del trabajo con IA, presentado formalmente en el **Work Trend Index 2024.** En ese informe, **la empresa** introduce el concepto de *Frontier Firm* para describir a las organizaciones que están **liderando la adopción avanzada de Inteligencia Artificial,** especialmente a través de **IA generativa, agentes de IA y modelos de trabajo híbridos humano-IA.**

El 2026 encuentra al mundo atravesando una transición profunda: La **tecnología** deja de ser un habilitador periférico para convertirse en **el núcleo operativo** de las economías, los Estados y las organizaciones, nucleado por **la Inteligencia Artificial** como principal motor de productividad y transformación, integrada en el core de negocio.

No se trata simplemente de compañías que "usan" Inteligencia Artificial, sino de **organizaciones diseñadas** desde su médula para **operar con inteligencia integrada** como **sistema nervioso** de sus procesos y decisiones clave: Automatizando procesos, amplificando capacidades humanas y redefiniendo la forma en que se crea valor.

Los avances en IA, automatización y cómputo distribuido están remodelando los ciclos económicos y acortando los horizontes de planificación. **La competitividad** ya no se define únicamente por tamaño, capital o eficiencia marginal, sino por la velocidad con la que las compañías incorporan capacidades digitales y logran traducirlas en productividad real y sostenida.

En este contexto **emerge la "Frontier Firm" como respuesta** a un mundo donde la complejidad es permanente, la velocidad es estratégica y la confianza se consolida como un activo económico crítico.

En este nuevo tipo de organización el valor no lo genera la IA por sí sola, sino su integración concreta dentro de los procesos de negocio y de las actividades productivas. Es allí —y solo allí— donde la tecnología se convierte en capacidad organizacional.

Hasta que la Inteligencia Artificial no se incorpora de forma sistemática y ubicua en los procesos, el impacto permanece latente. Es por esto qué la productividad no aumenta automáticamente con la adopción tecnológica, y por qué modelos como la automatización avanzada de procesos se vuelven centrales.

Algunos Framework de Inteligencia Artificial como Slingshot, o el abordaje de IA End to End de Bodhi, son una mirada de cómo esta tecnología está impactando a las empresas en todo el mundo, desde la experiencia global de Publicis Sapient.

Consideramos que el valor estará dado por la suma de dos factores: gente y producto (people & product) y nos invita a reflexionar respecto de los alcances que la Inteligencia Artificial puede llegar a tener mucho más allá de su mera aplicación como tecnología, sino que con un enfoque muchísimo más integral", comenta ***Daniel Yankelevich, Evangelist en Practia.***

Este nuevo tipo de organización se define menos por su industria y más por su arquitectura interna. Por eso hablamos de empresas IA-centric: Porque reorganizan su manera de pensar, operar y competir alrededor de la Inteligencia Artificial integrada como forma de funcionamiento.

Las estimaciones de McKinsey refuerzan esta tendencia: La Inteligencia Artificial podría aportar hasta USD 4,4 billones en valor anual y aumentar entre 0,1% y 0,6% la productividad laboral global por año, redefiniendo las bases mismas del crecimiento económico.

La IA podría aportar hasta

4,4 billones

en valor anual

*Según señala **Miguel Bilello, Special Business Advisor de Practia,** la encuesta de CIOs del Cono Sur realizada por Practia —con la voz de 289 empresas— revela que la Inteligencia Artificial aún no ha alcanzado la madurez de otras tecnologías, pero avanza con la fuerza de lo inevitable: La mitad de las organizaciones ensaya, prueba, tantea el terreno; y un tercio ya ha cruzado el umbral donde la tecnología deja de ser promesa para convertirse en impacto real sobre el negocio. No es casual, entonces, que la Inteligencia Artificial se encuentre hoy en la cúspide de la agenda del CIO, junto a la transformación, la innovación y la eficiencia operativa. Pero hay algo más profundo: la IA no solo comparte ese lugar de privilegio, sino que se ha convertido en la herramienta esencial para hacer posible esa transformación y esa búsqueda persistente de eficiencia que define al contexto actual.*

En este escenario cobra forma el **modelo centauro:** Una lógica de trabajo donde humanos y sistemas inteligentes colaboran de manera continua.

Las decisiones dejan de ser exclusivamente humanas o totalmente automatizadas para convertirse en el resultado de una interacción deliberada entre criterio, contexto y capacidad computacional.

Este formato entiende que el máximo rendimiento está en la **combinación:** El valor ya no surge de elegir entre personas o máquinas, sino de **diseñar conscientemente cómo trabajan juntas.**

De esta integración nace la **“empresa aumentada”**, una organización expandida en capacidades: Equipos aumentados que trabajan junto a agentes inteligentes, plataformas que aprenden del uso, procesos que se ajustan en tiempo real y estructuras que se reconfiguran frente al cambio.
La productividad deja de depender solo del esfuerzo humano y pasa a apoyarse en sistemas que anticipan, recomiendan y ejecutan con precisión creciente.

Este mismo principio redefine el **talento:** Emerge la noción de **“workforce aumentada”**, donde el rol profesional deja de ser estático para volverse evolutivo. Aprender nuevas capacidades ya no es un evento, sino un flujo continuo.

Las organizaciones más avanzadas no buscan perfiles “perfectos”, sino personas capaces de aprender, colaborar con la tecnología y adaptarse a entornos donde las herramientas cambian constantemente.

Todo esto configura **un nuevo modelo operativo.** Este tipo de organizaciones no se gestionan desde la rigidez ni desde la improvisación, sino **desde la capacidad de diseñar sistemas vivos:** Estructuras que combinan velocidad con control, autonomía con gobernanza, innovación con responsabilidad. Son empresas que no reaccionan al cambio, sino que lo incorporan como parte natural de su funcionamiento.

***Ernesto Kiszkurno, Director del mercado vertical regional de General Business en Practia,** comenta que: “Hoy no estamos ante una simple mejora de herramientas, sino frente a un verdadero proceso de selección natural corporativa. Siguiendo la premisa de Darwin, no sobrevive la empresa más grande ni la más fuerte, sino la que mejor evoluciona. En nuestra región, las organizaciones que integren la Inteligencia Artificial en el corazón de su operación no solo serán más eficientes: habrán dado el salto hacia modelos más resilientes, adaptativos y preparados para liderar el futuro.”*

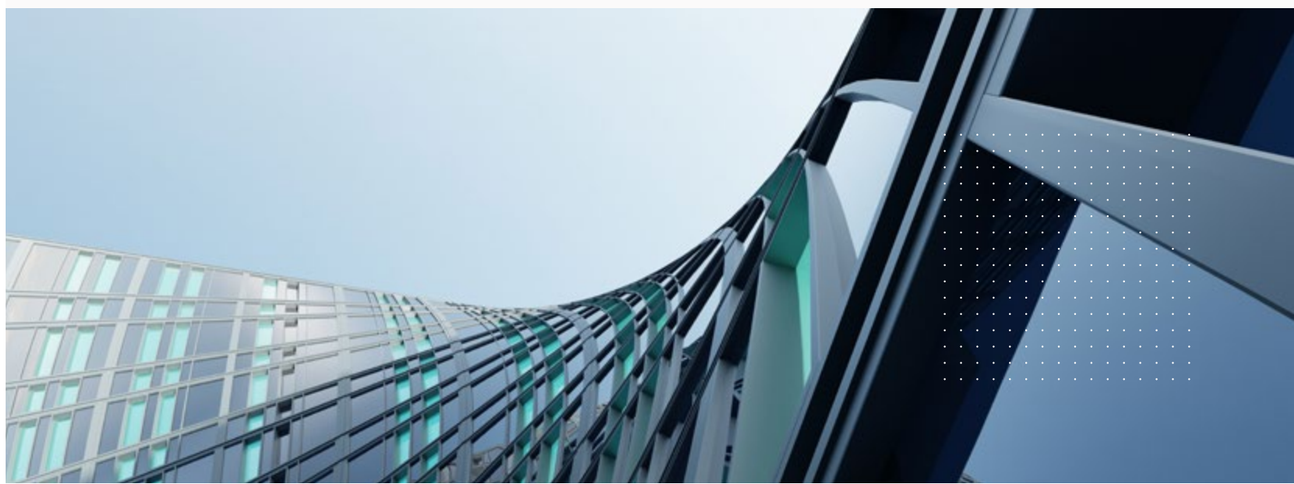
Una premisa se vuelve central: El 2026 no es solo un año de adopción tecnológica. **Es un punto de inflexión donde las empresas redefinen sus capacidades fundamentales para competir, crear valor y sostenerse en un mundo más digital, más regulado y exigente.**

Este Insight parte de esa premisa y explora cómo se articula este nuevo tipo de organización —**inteligente, resiliente y aumentada**— y qué decisiones estratégicas deben tomar hoy los líderes para construirla.

Porque el desafío ya no es entender hacia dónde va la tecnología, sino comprender qué tipo de empresa exige este nuevo tiempo.

Finalmente, este arquetipo emerge como uno de los **que mejor describe el nuevo límite** competitivo del presente **y se define por operar con un enfoque IA Centric.**

Las organizaciones que no comiencen a diseñarse en esa dirección corren el riesgo de quedar rezagadas, no por falta de innovación, sino por exceso de inercia.



02 IA Centric: Una empresa aumentada con aceleración de negocio

Durante la última década, la transformación digital avanzó en tres etapas sucesivas que redefinieron la relación entre tecnología, negocio y personas. Cada una respondió a una necesidad concreta y preparó el terreno que habilitó la emergencia del paradigma actual.

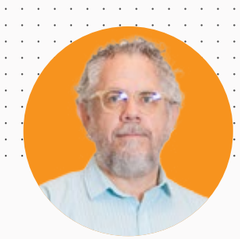
La primera fue la etapa **User Centric,** que marcó la era de la experiencia: Las organizaciones aprendieron a diseñar productos, servicios y plataformas digitales en torno a las necesidades humanas, priorizando la usabilidad, la personalización y la cercanía con el cliente.
La tecnología comenzó a ordenarse alrededor del usuario.

Luego emergió el enfoque **Data Centric,** en la que el foco dejó de ser exclusivamente la experiencia a la información: Los datos se consolidaron como activo estratégico y la prioridad se trasladó a su integración y calidad y gobernanza. La analítica avanzada y el machine learning permitieron tomar decisiones basadas en evidencia, anticipar comportamientos y optimizar resultados a escala.

Hoy, muchas organizaciones comienzan a transitar una tercera fase: la de las **Empresas IA Centric.** El verdadero cambio no es incorporar IA, sino aceptar que el juego competitivo está mutando.

Las reglas que definían eficiencia, escala y ventaja relativa ya no son las mismas.
La Inteligencia Artificial obliga a trabajar de otra manera al redefinir cómo se diseñan los procesos, cómo se toman decisiones y cómo se ejecuta el trabajo.

Las organizaciones no se sienten naturalmente atraídas por la idea de "ser IA Centric", lo que capta su atención es algo más concreto e incómodo: **la posibilidad de seguir jugando al juego conocido mientras otros comienzan a operar bajo una lógica distinta.**



*Tal como comenta **Juan V. Echagüe, Director de Investigación y Desarrollo en Practia,** "De alguna manera la decisión de adoptar Inteligencia Artificial ya la tomaron nuestros clientes, como ya ocurrió antes con la web y los teléfonos celulares. Lo que tenemos que decidir en las empresas es cómo hacerlo de manera ética y segura, generando valor. Y cómo llegar a tiempo.".*

En este nuevo escenario, la Inteligencia Artificial deja de ser una herramienta de apoyo o un componente experimental para convertirse en el **núcleo operativo y cognitivo de la organización.** La IA no solo asiste decisiones, sino que participa activamente en cómo se decide, cómo se opera y cómo se crea valor.

Una empresa IA Centric integra Inteligencia Artificial en **cada capa relevante de su funcionamiento.**

Convergen allí la IA generativa, los agentes autónomos y el software con inteligencia nativa para habilitar **capacidades organizacionales aumentadas:** Los modelos aprenden a partir de datos confiables, automatizan procesos complejos, detectan patrones invisibles al análisis humano y colaboran con las personas para mejorar la asignación de recursos, reducir fricción operativa y acelerar la toma de decisiones. Cuando estos sistemas están bien diseñados, gobernados y supervisados, la organización adquiere la capacidad de adaptarse a contextos cambiantes con niveles de velocidad y precisión antes inalcanzables.

Las proyecciones confirman este punto de inflexión. Gartner anticipa que para 2026 más del 80% de los productos y servicios digitales incorporará algún nivel de Inteligencia Artificial nativa, y que una porción creciente de los modelos operativos evolucionará hacia estructuras impulsadas por IA.

En paralelo, estudios de MIT Sloan muestran que las organizaciones con enfoques IA-first logran ciclos de decisión entre dos y cuatro veces más rápidos, impulsados por automatización cognitiva, reducción de fricción operativa y orquestación inteligente de procesos.

Estos indicadores sugieren un punto de inflexión: En un número creciente de organizaciones, **el valor estratégico** comienza a surgir de operar en torno a GenIA.

En la metodología de Practia, la priorización de casos de uso de IA no se basa únicamente en el atractivo tecnológico, sino en un marco estructurado que conecta directamente la estrategia de negocio con la ejecución.

Cada iniciativa es evaluada de forma integral considerando su impacto esperado en indicadores clave de valor como eficiencia operativa, crecimiento de ingresos, experiencia del cliente o mitigación de riesgos, junto con su viabilidad técnica, que incluye madurez de la arquitectura, capacidades de los equipos y complejidad de integración", Comenta ***Gilberto Strafacci, Gerente en Practia Brasil.***

De manera complementaria, se analiza el perfil de riesgos regulatorios, éticos y de seguridad, así como la dependencia y calidad de los datos requeridos para asegurar sostenibilidad en el tiempo.

Esta visión multidimensional permite construir un portafolio balanceado entre quick wins y apuestas estratégicas de mayor impacto, garantizando foco, retorno y una adopción responsable de la IA dentro de la organización.

¿Qué tan profundo impacta este nuevo paradigma?:

La Inteligencia Artificial integrada emerge entonces como un activo estratégico que **permite construir organizaciones más inteligentes, resilientes y adaptativas.**

Para las corporaciones, migrar hacia un modelo IA Centric no es solo una decisión tecnológica, sino **una estrategia clave de competitividad y sostenibilidad.**

McKinsey advierte que las compañías que no integren IA en el núcleo de sus operaciones podrían experimentar una caída significativa en su productividad relativa hacia el final de la década. En contraste, **aquellas que adopten modelos IA-orquestados capturarán una proporción sustancialmente mayor del valor económico de su sector.**

practia | A company of publicis sapient

Mauricio Sansano, Director del mercado vertical regional de energía en Practia, *argumenta: "En la industria de energía, ser IA Centric ya no es una opción de eficiencia, es una condición de continuidad operativa y competitividad en el mercado. La Inteligencia Artificial empieza a definir cómo se despacha energía, cómo se predicen fallas en activos críticos, cómo se balancea la red y cómo se toman decisiones bajo estrés regulatorio y climático. Por ejemplo, las utilities que integren IA en su core operativo —no como pilotos aislados— serán las únicas capaces de sostener confiabilidad, costos controlados y transición energética simultáneamente.*

En el campo del petróleo y gas, hoy ya es imposible concebir operaciones en tiempo real de perforación, sin la asistencia de agentes especializados que optimicen el ROP, maximicen las condiciones de seguridad, y alerten de manera temprana ante posibles atascamientos del trépano."

Este paradigma impulsa, además, **una transformación cultural profunda.**

Las organizaciones IA Centric promueven formas de trabajo más ágiles, experimentales y colaborativas, donde la alfabetización digital, el pensamiento crítico y la capacidad de interactuar con sistemas inteligentes se vuelven competencias esenciales.

Surgen así los **equipos aumentados, en los que personas y algoritmos trabajan de manera complementaria:** emerge un nuevo modelo híbrido en el que la Inteligencia Artificial asume tareas repetitivas, analíticas o de alto volumen, mientras los humanos aportan criterio, contexto, creatividad y juicio ético.

Un zoom regional: ¿Latinoamérica está surfeando esta ola?:

En América Latina, la mayoría de las organizaciones aún opera bajo enfoques Data Centric o modelos de IA asistida. El índice de adopción de IA de IBM reveló que la **mayor barrera** para la adopción de IA en las empresas latinoamericanas **son las habilidades, los conocimientos o la especialización.**

El camino hacia organizaciones plenamente IA Centric recién comienza. La inversión regional en investigación y desarrollo sigue siendo reducida en comparación con los promedios globales y se concentra en pocos países. Sin embargo, esta realidad convive con una aceleración clara del interés por reposicionar la Inteligencia Artificial como eje operativo del negocio.

Según datos oficiales de IBM, el **67 % de las grandes compañías** latinoamericanas ya implementan o planean implementar soluciones de IA, y muchas de ellas la posicionan como una de las prioridades esenciales.

Para la región, adoptar un enfoque IA Centric implica una reconfiguración integral: Reestructurar procesos para que sean más automatizados y predictivos, tomar decisiones informadas por modelos de aprendizaje automático en tiempo real, construir plataformas con inteligencia integrada que aprenden del uso y construir equipos preparados para trabajar en colaboración continua con sistemas inteligentes.

03 Emergencia de los agentes: Autonomía y Resiliencia Operacional

A medida que la Inteligencia Artificial se integra de forma profunda en los procesos, el desafío deja de ser qué automatizar y pasa a ser **cuánto control, autonomía y capacidad** de acción **delegar a los sistemas.** En entornos cada vez más complejos y dinámicos, donde la velocidad y la anticipación se vuelven críticas, escalar eficiencia solo con intervención humana resulta inviable.

En este contexto, **la evolución tecnológica** deja de ser incremental y se vuelve estructural: la inteligencia ya no solo asiste, sino que actúa. La integración de IA en los procesos habilita sistemas capaces de observar, decidir y ejecutar con distintos niveles de autonomía, redefiniendo la forma en que las organizaciones operan, se adaptan y construyen resiliencia operacional.

En este nuevo estadio, la **IA Generativa** se consolida como el motor más visible de la productividad y la creatividad empresarial aumentada, al acelerar el desarrollo de productos, la personalización y la toma de decisiones a partir de su capacidad para aprender patrones, sintetizar conocimiento y generar contenido de alto valor.

Según Bain, más del **60%** de las empresas ya priorizan incorporar GenIA dentro de sus estrategias de transformación del 2026.

Inteligencia 2.0

Durante años, la Inteligencia Artificial se entendió como un conjunto de modelos que analizaban datos y generaban respuestas. Hoy, ese paradigma evoluciona hacia una nueva etapa: La de los **agentes inteligentes.**

Estas **entidades de software** tienen la capacidad de **observar, razonar, aprender y actuar** de forma autónoma para alcanzar objetivos concretos, y **representan un cambio estructural:** Comienzan a intervenir en el entorno digital y operativo de una organización, habilitando que hasta el 15% de las decisiones laborales diarias se tomen de forma autónoma.

Su funcionamiento se basa en tres componentes: **Percepción, decisión y acción.**

A través de **algoritmos de aprendizaje profundo y procesamiento del lenguaje natural** (NLP), pueden interpretar contextos complejos, acceder a bases de conocimiento, y tomar decisiones informadas en tiempo real.

Según estimaciones de Gartner, para 2028 **el 33% de las aplicaciones empresariales incluirán capacidades agentivas,** frente a menos del 1% en 2024.

¿Qué podríamos esperar de un Agente Inteligente?

Un agente de IA puede comprender instrucciones en lenguaje natural, planificar una secuencia de acciones y ejecutarlas **conectándose** con aplicaciones, APIs o sistemas empresariales. **Los tipos de agentes varían según su nivel de autonomía y propósito:**

Reflejos: Reaccionan con base en reglas simples (por ejemplo, filtros de spam o sistemas de climatización automatizados).

Basados en objetivos: Persiguen metas específicas, como la optimización de rutas en logística o transporte.

De aprendizaje: Mejoran su rendimiento con la experiencia, como los motores de recomendación de streaming.

De utilidad: Equilibran variables para lograr eficiencia, como los termostatos inteligentes o sistemas de energía adaptativos.

Jerárquicos o multiagente: Cooperan entre sí, compartiendo subtareas y decisiones dentro de un sistema complejo, como flotas de drones o ecosistemas de bots de soporte.

Estos agentes no operan aislados, se comunican entre sí dentro de un **sistema multiagente,** donde cada uno ejecuta una parte del flujo y todos aprenden de la experiencia colectiva.

El resultado es un modelo distribuido de inteligencia que combina **precisión, velocidad y adaptabilidad.**

A nivel empresarial, los agentes **amplifican la productividad** y la resiliencia operativa.

Todo converge en Agentic Automation:

La **Agentic Automation** representa la evolución de la automatización robótica (RPA) y la Inteligencia Artificial tradicional: Mientras que la RPA ejecuta reglas predefinidas, la automatización agentiva **comprende objetivos, planifica rutas y decide cómo lograrlos.**

La diferencia clave radica en que no necesitan programación explícita, y poseen la capacidad de aprender y adaptarse.

Para el sector de E&C, la automatización agentiva marca el paso de la operación reactiva a la operación anticipatoria y óptima. Agentes inteligentes pueden monitorear redes, prever sobrecargas, coordinar mantenimiento predictivo y actuar en tiempo real ante eventos climáticos o fallas sistémicas. Pueden incluso cambiar planes operativos y adaptarlos a eventos inesperados, como conflictividad laboral, o fallas de equipamiento. La resiliencia energética del futuro no se logrará con más personas en salas de control, sino con inteligencia distribuida gobernada y una base muy sólida de información que nutra y optimice los modelos", refuerza ***Mauricio S.***

En RPA, los bots ejecutan tareas repetitivas según un flujo rígido. En Agentic Automation, los agentes pueden interpretar, reacomodarse y decidir qué pasos seguir, basándose en el contexto y el aprendizaje continuo. Esto permite escalar la automatización a entornos cambiantes, donde las reglas pueden variar o los procesos no están totalmente definidos.

Según McKinsey, la adopción de agentes inteligentes en los procesos operativos permite liberar capacidad organizacional de entre 25% y 40% en workflows críticos, mejorar la productividad y reducir errores en tareas repetitivas, gracias a su capacidad de aprendizaje adaptativo, integración con múltiples sistemas y operación autónoma en tiempo real.

APA: La visión de Practia

La IA agentic marca un punto de inflexión en la automatización empresarial al habilitar la gestión de procesos de mayor escala y complejidad, donde la clave ya no está solo en ejecutar tareas, sino en planificar, coordinar y orquestar acciones entre sistemas, robots y personas bajo esquemas robustos de gobernanza y seguridad.

En Practia, esta evolución no se aborda desde una mirada teórica, sino que se traduce en un modelo propio que estructura y operacionaliza estos principios en contextos reales: el enfoque de **Agentic Process Automation (APA).**

*"**APA"** no es solo una metodología técnica, sino un **marco estratégico** para diseñar, implementar y escalar agentes inteligentes en entornos corporativos reales, con foco en el valor tangible y la gobernanza" argumenta* ***Gilberto Strafacci.***

El modelo combina tres principios centrales:

Distribución dinámica del trabajo: Humanos y agentes colaboran de manera simbiótica, asignando tareas según capacidad, contexto y valor agregado.

Orquestación inteligente: Múltiples agentes se coordinan entre sistemas empresariales para ejecutar procesos de principio a fin, garantizando consistencia y trazabilidad.

Aprendizaje continuo: Los sistemas registran resultados, retroalimentan sus modelos y optimizan su desempeño con cada ciclo operativo.

A diferencia de otras aproximaciones, APA incorpora gobernanza desde el diseño, asegurando trazabilidad, seguridad y ética en el uso de IA. Esto permite a las empresas **experimentar, medir y escalar sin perder control** sobre la toma de decisiones ni comprometer la transparencia.

Nuestro enfoque se estructura en cuatro etapas:

Exploración: Identificación de procesos con potencial agentivo.

Pilotos controlados: Validación de casos de uso con resultados medibles.

Optimización: Integración con sistemas core y ajuste de parámetros de decisión.

Escalamiento: Adopción transversal en toda la organización.

Más allá de la eficiencia, su valor está en **impulsar organizaciones que piensan y actúan con inteligencia distribuida:** La automatización agentiva marca el inicio de una nueva era en la relación entre humanos y máquinas.

A medida que las organizaciones delegan parte de la toma de decisiones y la ejecución a sistemas autónomos, el centro de gravedad del negocio cambia: Los flujos se vuelven dinámicos, las operaciones más adaptativas y los equipos humanos pueden enfocarse en análisis, creatividad y diseño de soluciones con alto impacto.

Sin embargo, **la autonomía sin gobernanza es una amenaza.** El paso natural que debe acompañar la adopción de agentes es avanzar hacia marcos de AI TRiSM que aseguren integridad, transparencia y alineación ética.

04 AI TRiSM: Protocolo de Confianza para el Dominio Tecnológico

A medida que la Inteligencia Artificial se convierte en el nuevo motor operativo de las organizaciones, también emerge un frente crítico: **La confianza.**

La expansión acelerada de los modelos autónomos incrementa la complejidad y amplían la superficie de riesgo. Sesgos invisibles, decisiones opacas, fallas en los datos, vulnerabilidades algorítmicas y fugas de información ya no son problemas hipotéticos, son incidentes reales que **impactan en la reputación, la continuidad y la sostenibilidad** de las empresas.

La escasa madurez en la gestión de datos y la ausencia de esquemas sólidos de gobernanza se han convertido en uno de los principales factores de riesgo para los proyectos de Inteligencia Artificial en entornos productivos. En muchas organizaciones, los modelos operan con niveles insuficientes de supervisión y trazabilidad, lo que genera problemas operativos y limita su efectividad. De no fortalecerse estos mecanismos de control, una proporción significativa de las iniciativas de IA difícilmente materializará el valor esperado.

La aparición de dispositivos con IA que no solo procesan información, sino que además interactúan con el mundo físico y toman datos directamente de él, es uno de los fenómenos que más va a acelerar los cambios. El solo hecho de que un agente con IA pueda usar una tarjeta de crédito, moverse en sistemas reales, leer y escribir archivos ya tiene un impacto enorme y consecuencias difíciles de dimensionar. Imaginar eso mismo con robots es un ejercicio que da miedo pero a la vez esperanzas" afirma ***Daniel Y.***

En este contexto, **comprender cómo confiar en la Inteligencia Artificial de forma segura, ética y sostenible,** se ha convertido en el nuevo frente de batalla para los líderes tecnológicos.

La respuesta estructural: AI TRiSM como marco de confianza

AI TRiSM —Artificial Intelligence Trust, Risk and Security Management— se consolida como el estándar para **gestionar la confiabilidad, seguridad, explicabilidad y responsabilidad en sistemas de IA.**

No es un conjunto de controles, sino una arquitectura integral de gobernanza que rige la forma en que operan las empresas líderes que aplican IA.

Como señaló Mark Horvath, vicepresidente de Gartner: "Los CIOs no pueden permitir que la IA controle su organización; Se necesitan nuevas formas de gestión de la confianza, el riesgo y la seguridad que los controles convencionales no ofrecen".

El modelo AI TRiSM articula cuatro capacidades críticas:

01 **Confianza y explicabilidad (Trust):** Garantizar decisiones comprensibles, auditables y justas mediante XAI y detección de sesgos. Los frameworks de explicabilidad sólidos otorgan a las organizaciones un incremento en la confianza de clientes y stakeholders.

02 **Gestión de riesgos (Risk):** Identificar y mitigar riesgos operativos, regulatorios y reputacionales derivados del uso de IA. Cada incidente causado por IA no gobernada puede costar millones, dependiendo de la industria.

03 **Seguridad (Security):** Proteger modelos y datos mediante cifrado, controles de acceso, auditorías y marcos Zero Trust AI. La ciberseguridad algorítmica es hoy un componente tan crítico como la seguridad de red o infraestructura.

04 **Gobernanza continua:** Establecer cuerpos interdisciplinarios que definan políticas, roles, métricas y estándares de ciclo de vida. Se estima que, para 2026, las organizaciones con gobernanza activa de IA aumentarán la adopción real de sus sistemas por parte de usuarios internos.

El mercado global de gobernanza de IA alcanzó los USD 12 mil millones en 2024 y se triplicará hacia 2034, impulsado por legislaciones como la AI Act de la Unión Europea, la AI Accountability Act en Estados Unidos y nuevas regulaciones emergentes en Asia y Oceanía. No se trata solo de cumplimiento, sino de sostenibilidad del negocio.

*Según comenta **Gilberto:** "En el enfoque de Practia, la gobernanza de IA se traduce en mecanismos operativos concretos que garantizan control, transparencia y generación sostenida de valor. Modelos y agentes se gestionan mediante revisiones periódicas técnicas y de negocio, con métricas claras sobre desempeño, deriva de datos, riesgos, seguridad y cumplimiento. Cada solución atraviesa validaciones formales antes de llegar a producción y cuenta con responsables explícitos —negocio, tecnología y governance—, asegurando que la IA se gestione con disciplina, trazabilidad y alineación estratégica."*

La dimensión organizacional: Estructuras, roles y cultura

La adopción de AI TRiSM implica rediseñar la organización: Los modelos de IA responsable requieren nuevas estructuras colaborativas entre Tecnología, Legal, Riesgo, Ética y Negocio, creando responsabilidad compartida sobre los resultados algorítmicos.

Lo que antes era un proyecto de TI, ahora es una **práctica transversal que exige cultura ética,** criterio experto y rendición de cuentas. Por ello, surgen nuevos roles específicos como **AI Product Owners, AI Stewards, Model Risk Officers y Data Custodians,** encargados de supervisar modelos, controlar sesgos, asegurar trazabilidad y garantizar alineación regulatoria.

AI TRiSM debe convertirse en una **práctica continua de gestión del riesgo y la confianza** en todo el ciclo de vida de los modelos.

Adoptar este marco implica **pasar de una IA que funciona a una IA en la que se puede confiar:** Una inteligencia auditable, predecible y controlada.

Aumento de riesgo: ¿Cuál es el nuevo desafío?

La transición hacia agentes inteligentes —presentada en el capítulo anterior— intensifica aún más la necesidad de marcos robustos como AI TRiSM.

Los agentes autónomos incrementan la superficie de riesgo operacional al interactuar directamente con sistemas internos, datos sensibles y flujos de negocio sin los mismos controles inherentes del trabajo humano. Sin AI TRiSM, la autonomía se convierte en opacidad; con AI TRiSM, se convierte en ventaja estratégica.

Con el modelo de centauro como marco, estas garantías habilitan autonomía sin comprometer el negocio: La agentic automation requiere monitoreo humano continuo, trazabilidad algorítmica, explicabilidad en decisiones autónomas, límites de seguridad parametrizados, auditoría de objetivos y comportamientos del agente.

La gobernanza como oportunidad en Latinoamérica

América Latina enfrenta un escenario dual: Alta expectativa tecnológica y baja madurez de gobernanza.

Según IBM, el 37% de las compañías de la región ya implementan IA y el 45% está en exploración; sin embargo, solo un porcentaje menor cuenta con políticas formales de gobernanza, trazabilidad o ética algorítmica.

Latinoamérica tiene un desafío aún mayor. El "bono demográfico" – entendido como población joven – se acabó. Los recursos naturales por sí solos no van a permitir reducir la brecha de crecimiento con el resto del mundo.

Pero también cuenta con una ventaja: la aparición de estas nuevas tecnologías permite realizar un **"leapfrog"**: un salto de tecnologías viejas a las más nuevas evitando transiciones intermedias, lo que permite recuperar parte de la brecha.

La oportunidad es clara: Al no tener un legado complejo, la región puede adoptar marcos modernos desde el inicio. Países como Brasil, Chile, México y Colombia ya avanzan en audiencias regulatorias, auditoría algorítmica y principios de responsabilidad en servicios públicos, dejando ver un nuevo estándar en construcción.

*"Construir confianza no frena la innovación, la acelera al otorgarle legitimidad y sostenibilidad en el tiempo. El mayor desafío no es sólo tecnológico, es también un desafío estratégico y de gestión: Muchas organizaciones no fallan por falta de herramientas, sino por carecer de una hoja de ruta clara, un marco de gobernanza sólido y una visión integral que conecte los objetivos de negocio con los principios de confianza, riesgo y seguridad." argumenta **Carlos Lacchini, Líder de la Practica de IA&Data Science en Practia.***

La visión de Practia: Construir confianza como capacidad interna

Para materializar esta visión, desde Practia acompañamos a las compañías en la definición de su estrategia de IA responsable, el diseño de modelos de gobernanza, y la gestión de la adopción y el cambio organizacional.

El proceso debe abordarse en **cinco etapas secuenciales:**

Diagnóstico de madurez: Mapear todos los modelos de IA existentes, evaluar su trazabilidad y riesgos.

Gobernanza integral: Definir roles, procesos y un AI Governance Board con mandato claro, responsabilidades distribuidas y criterios de toma de decisión.

Explicabilidad y documentación: Implementar XAI y establecer estándares de transparencia.

Seguridad técnica y operativa: Adoptar prácticas de Zero Trust AI, cifrado, detección de anomalías y defensa ante ataques adversariales.

Cultura ética y educación: Formar equipos en ética digital, sesgos y responsabilidad algorítmica.

La verdadera ventaja competitiva no proviene sólo de sumar modelos, sino de sumarlos habiendo construido las **capacidades internas** que permiten gobernar, escalar y sostener la IA en el tiempo.

“

***Mauricio S.**, a partir de su amplia trayectoria en el sector, agrega: “La industria energética opera infraestructuras críticas donde el error algorítmico no es tolerable. En este contexto, AI TRiSM deja de ser un marco de compliance para convertirse en un habilitador del negocio. Sin explicabilidad, trazabilidad y control sobre modelos y agentes, la IA no escala en esta industria. La confianza no acelera después de la adopción: es la condición previa.”*

Una vez que la Inteligencia Artificial opera bajo marcos seguros, explicables y gobernados, el siguiente desafío es sostenerla de forma eficiente y sostenible.

Esto abre el paso al capítulo siguiente, donde la infraestructura híbrida, el edge computing y la sostenibilidad digital se convierten en **la base para desplegar IA confiable a escala.**

05 Green IT: Infraestructura de negocio alineada a la IA

En 2026, la **infraestructura tecnológica** ingresa en una nueva etapa, impulsada por la convergencia de la **nube híbrida, el edge computing y la sostenibilidad digital.**

Esta combinación redefine su rol dentro de las organizaciones: **La infraestructura** deja de ser un componente de soporte operativo, para transformarse en un **activo estratégico,** directamente **alineado con objetivos financieros, regulatorios, ambientales y de gestión del riesgo.**

El crecimiento exponencial de la Inteligencia Artificial —en particular de los modelos generativos y de los sistemas agentivos— está tensionando las bases tradicionales de la infraestructura: Estudios recientes advierten que los centros de datos podrían llegar a duplicar el consumo de la electricidad mundial para 2030 si no se introducen cambios estructurales.

La escala de cómputo requerida por la IA obliga a repensar no solo la capacidad instalada, sino también cómo, dónde y con qué eficiencia se procesa la inteligencia.
En este contexto, **la infraestructura** deja de ser una decisión puramente tecnológica para convertirse en una **decisión económica, regulatoria y reputacional.**

Cada workload de IA, cada modelo entrenado y cada inferencia ejecutada tiene un **costo energético, financiero y ambiental.** El desafío estratégico ya no es únicamente cuánta potencia se necesita, sino **cómo escalar inteligencia con un costo marginal controlado,** *sin comprometer sostenibilidad, cumplimiento ni rentabilidad.*

Una empresa aumentada sin infraestructura sostenible se vuelve económicamente inviable.

Green IT emerge no solo como una iniciativa ambiental aislada, sino como un **habilitador directo del crecimiento basado en IA.** La eficiencia ambiental se convierte así en un componente estructural del diseño de infraestructura, al mismo nivel que la disponibilidad, la seguridad o la escalabilidad.

¿Cómo se consolida este paradigma en el mundo?

Este viraje responde a una prioridad que ya se está consolidando a nivel global: Según Gartner, para 2027 el 75% de las organizaciones habrá implementado programas formales de sostenibilidad en sus centros de datos. En esa misma línea, proyecta que para 2026 el 50% de las compañías gestionará activamente el consumo energético de sus entornos de nube híbrida mediante herramientas de sostenibilidad.

Estos datos marcan una tendencia clara hacia la optimización energética, la observabilidad ambiental y la trazabilidad del impacto digital.

"Green IT no es solo una iniciativa ambiental para sectores como la Minería o el Oil&Gas: es una paradoja estratégica. La industria que provee energía y recursos naturales debe, al mismo tiempo, optimizar el consumo energético de la inteligencia que la gobierna. Diseñar infraestructuras eficientes, híbridas y conscientes del costo energético de la IA será tan estratégico como producir energía limpia", afirma ***Mauricio S.***

Los gigantes tecnológicos

El paradigma de infraestructura se desplaza entonces de "más potencia a cualquier coste" hacia un equilibrio entre potencia, eficiencia y sostenibilidad. A nivel global, los grandes proveedores de tecnología refuerzan esta transformación demostrando que la eficiencia no está reñida con la innovación:

Microsoft reporta haber reducido más del 80% su consumo de agua en centros de datos y alcanzar hasta un 93% de ahorro energético en entornos cloud frente a infraestructuras tradicionales:

"A medida que Microsoft sigue creciendo e innovando, nuestro compromiso con la sostenibilidad ambiental continúa siendo un valor esencial. Este año, reflexionamos sobre nuestros avances hacia los ambiciosos objetivos marcados para 2030: Ser una compañía negativa en carbono y en agua y cero residuos, al tiempo que protegemos los ecosistemas. Al entrar en la segunda mitad de la década, Microsoft mantiene firme su compromiso con los objetivos de sostenibilidad ambiental establecidos para 2030" – Microsoft, Informe de Sostenibilidad Ambiental 2025.

IBM, por su parte, informa que el 75% de la electricidad utilizada en sus centros de datos proviene de fuentes renovables y una mejora del 20% en eficiencia energética desde 2019.

Estos casos confirman que adoptar Green IT no solo reduce el impacto ambiental, sino que **mejora la competitividad operativa.**

Tres prácticas marcan el rumbo de esta transición:

Green IT apunta a reducir la huella energética del stack tecnológico mediante optimización de enfriamiento, adopción de energías renovables y arquitecturas eficientes.

FinOps incorpora disciplina financiera al consumo de nube, alineando costo, uso y valor, y transformando la nube en una inversión gestionada, no en un gasto impredecible.

Finalmente, el **modelo edge y cloud híbrido** distribuye el procesamiento para reducir latencia, tráfico de red y consumo energético, al tiempo que responde a requisitos de soberanía de datos y resiliencia operativa.

¿Cómo se optimiza el negocio?

Para el negocio, esta evolución implica múltiples beneficios. El impacto es directo y medible: Habilita mayor resiliencia ante fallos, cumplimiento regulatorio, mejora en la experiencia del cliente y reducción del costo total de propiedad.

La adopción de escritorios virtuales (DaaS), por ejemplo, permite trasladar puestos de trabajo al cloud, reduciendo consumo energético in situ, habilitando esquemas de trabajo remoto y fortaleciendo la sostenibilidad organizacional.

Más allá del ahorro, las infraestructuras sostenibles comienzan a incidir de manera directa en la competitividad: Fondos de inversión, entidades financieras y grandes clientes corporativos incorporan métricas ESG y eficiencia digital como criterios de decisión.

Las organizaciones que demuestran control sobre su huella tecnológica acceden a mejores condiciones de financiamiento, reducen riesgos regulatorios futuros y fortalecen su posicionamiento de marca.

Expansión en LATAM

En el entramado Latinoamericano, la infraestructura digital atraviesa una etapa de fuerte expansión: IDC proyecta que la tasa de crecimiento anual del gasto en servicios de nube pública de la región superará el 29% para 2027.

Aunque América Latina enfrenta desafíos estructurales —como la brecha de inversión en centros de datos eficientes, la necesidad de soberanía de los datos y marcos regulatorios ambientales en constante evolución—, estas tensiones conviven con una clara tendencia hacia una adopción creciente, aunque aún incipiente, de la sostenibilidad digital.

Cada vez más organizaciones comienzan a incorporar criterios de eficiencia energética y reducción de huella de carbono, integrándolos de forma progresiva en sus estrategias de TI.

El impacto disruptivo de la Inteligencia Artificial dejó una lección inequívoca: La potencia sin control, sin optimización de costos y sin conciencia ambiental deja de ser una ventaja para convertirse en un riesgo competitivo.

De cara a 2026, la infraestructura del negocio se redefine a partir de la convergencia entre nube híbrida, edge computing y sostenibilidad digital. Repensar este entramado no es solo una decisión tecnológica: es reinventar el negocio, estableciendo una condición que habilita la competitividad, escalabilidad y sostenibilidad en el ecosistema digital de la próxima generación.

La siguiente frontera será dotar a esta infraestructura de **inteligencia operacional.** En ese punto, prácticas como Platform Engineering y DevSecOps emergen como catalizadores clave, redefiniendo la forma en que las organizaciones diseñan, entregan y sostienen soluciones digitales a escala.

06 Aceleración del delivery: Platform Engineering y DevSecOps

En la actualidad, la velocidad que exige el mercado digital junto con la creciente complejidad de las arquitecturas híbridas, la presión regulatoria y la necesidad de garantizar seguridad y calidad desde el diseño, impulsa a las organizaciones hacia un nuevo modelo operativo: **el Platform Engineering.**

Este enfoque habilita la creación de un **ecosistema integral** que redefine la forma en que se concibe, entrega y escala la tecnología, desplazando el foco desde proyectos aislados hacia **capacidades estructurales que sostienen la innovación continua.**

En este contexto, **acelerar el delivery** deja de ser una preocupación exclusiva del área de TI para convertirse en una **capacidad estratégica de ejecución del negocio.**

La **velocidad** con la que una organización transforma visión en productos digitales, y productos en valor tangible, se vuelve un **diferencial competitivo** directo en mercados cada vez más dinámicos e impredecibles.

El delivery eficiente ya no depende solo del talento individual, sino de plataformas que eliminen fricción, reduzcan la complejidad y habiliten escala.

¿Cuál es el verdadero valor agregado?

A diferencia del DevOps tradicional —que integró desarrollo y operaciones para acelerar la entrega— el Platform Engineering da un paso evolutivo: Crea entornos estandarizados, gobernados y reutilizables, donde la complejidad técnica queda encapsulada.

En este contexto, la plataforma se concibe como un producto interno: Diseñado intencionalmente para reducir fricción cognitiva y operativa, y para ofrecer capacidades de autoservicio seguras, consistentes y auditables, que permiten a los equipos desarrollar y desplegar soluciones con mayor autonomía sin comprometer gobernanza, calidad ni seguridad.

Según Gartner, **para 2026 más del 80% de las grandes organizaciones** habrá establecido equipos dedicados de Platform Engineering; y un amplio porcentaje de ellas ya experimenta con plataformas internas de autoservicio.

El núcleo operativo de la innovación digital moderna

Este movimiento consolida una transición hacia modelos de ingeniería centrados en la experiencia del desarrollador (DevEx), hoy reconocida como un punto de dolor crítico para alcanzar objetivos estratégicos del negocio y sostener la innovación a escala.

Un estudio de McKinsey muestra que los desarrolladores que operan en entornos con automatización avanzada y herramientas asistidas por IA completan tareas en casi la mitad del tiempo.

El impacto trasciende la eficiencia técnica: Las organizaciones ganan autonomía sin perder control, las áreas de TI reducen carga operativa reactiva y el negocio accede a un delivery más predecible, seguro y alineado con prioridades estratégicas.

En términos concretos, esto significa mayor capacidad para innovar, ciclos de entrega más cortos y una respuesta más resiliente frente a cambios del mercado o disrupciones externas.

Este nuevo modelo **se potencia cuando se integra con prácticas maduras de DataOps y DevSecOps,** que consolidan la calidad, la seguridad y la gobernanza desde la base. **DataOps** garantiza la trazabilidad, confiabilidad y gobernanza del dato —elementos indispensables en organizaciones impulsadas por IA— mientras que **DevSecOps** incorpora la seguridad como principio de diseño, no como control posterior.

En este punto, **DevSecOps** deja de ser solo una práctica técnica y se convierte en un **mecanismo de gobernanza continua** que integra controles automáticos, auditorías, gestión de identidades y validaciones de cumplimiento en los pipelines de desarrollo, incrementando velocidad sin comprometer seguridad.

La seguridad se vuelve ***"secure by default"***, embebida en cada despliegue.

Microsoft demuestra que la adopción de estas prácticas contribuye a mejorar la seguridad y confiabilidad de los entornos productivos, automatizando la detección de vulnerabilidades y la gestión de controles y la trazabilidad en los despliegues. Esto refuerza la idea de que **la automatización también actúa como defensa.**

Las plataformas modernas ya no se evalúan únicamente por su capacidad de desplegar más rápido, sino por hacerlo de **manera segura, trazable y gobernable,** al consolidarse dentro de **un flujo continuo donde cada despliegue es más confiable y menos riesgoso.**

"En Practia creemos que el verdadero valor de esta transformación reside en traducir este enfoque en valor estratégico. Tener una plataforma bien diseñada que no solo permite acelerar la entrega, sino que reduce la deuda técnica, fortalece la seguridad, mejora la colaboración entre áreas y habilita decisiones más informadas. El resultado es una organización capaz de responder al cambio con rapidez, pero también con confianza y control. Sostiene ***Gonzalo Pasquini, Development Practice Manager en Practia.***

Hacia la madurez del delivery automatizado en LATAM

En América Latina, las prácticas modernas de ingeniería y automatización ya forman parte del presente operativo de un número creciente de organizaciones.

En la región, las tasas de adopción de prácticas asociadas a DevOps —base fundacional de toda estrategia de Platform Engineering— se incrementan progresivamente en sectores como tecnología, servicios financieros, comercio y manufactura, con una proyección de crecimiento sostenido en los próximos años.

Este avance se sostiene sobre una base estructural que ya está en marcha: Más del 80% de las empresas latinoamericanas utiliza la nube de forma habitual, y cerca del 42% se encuentra implementando soluciones cloud a escala organizacional, según un estudio elaborado por NTT DATA y MIT Technology Review.

Estas capacidades no solo habilitan flexibilidad de infraestructura, sino que constituyen prerrequisitos técnicos y operativos para entornos de entrega continua, pipelines automatizados y plataformas internas de autoservicio, pilares del Platform Engineering moderno.

Desde la perspectiva del valor económico, los resultados comienzan a ser visibles: Un análisis de McKinsey sobre transformación digital en América Latina indican que **las iniciativas que combinan crecimiento del negocio con eficiencia tecnológica concentran hasta el 49% del impacto económico total de la transformación,** particularmente en organizaciones que logran integrar automatización, estandarización y gobierno de forma coherente.

Esto confirma que el delivery moderno no es solo una mejora técnica, sino un **vector directo de generación de valor.**

La región aún enfrenta desafíos estructurales relevantes: Fragmentación de procesos, escasez de talento especializado y niveles dispares de madurez en prácticas de ingeniería. Aun así, Latinoamérica se perfila como un mercado prometedor para DevOps y las empresas de la región continúan invirtiendo en plataformas internas o automatización DevOps, con Brasil y México a la cabeza. En paralelo, países como Chile, Colombia y Argentina avanzan con fuerza en la adopción de pipelines de integración y despliegue continuo.

La brecha que marca el futuro corporativo

Aquí emerge un punto de inflexión estratégico: **La próxima distinción estratégica** se dará entre las organizaciones capaces de **industrializar el delivery digital** y aquellas que permanezcan atrapadas en modelos de ejecución artesanal, dependientes del esfuerzo manual, el conocimiento tácito y controles reactivos.

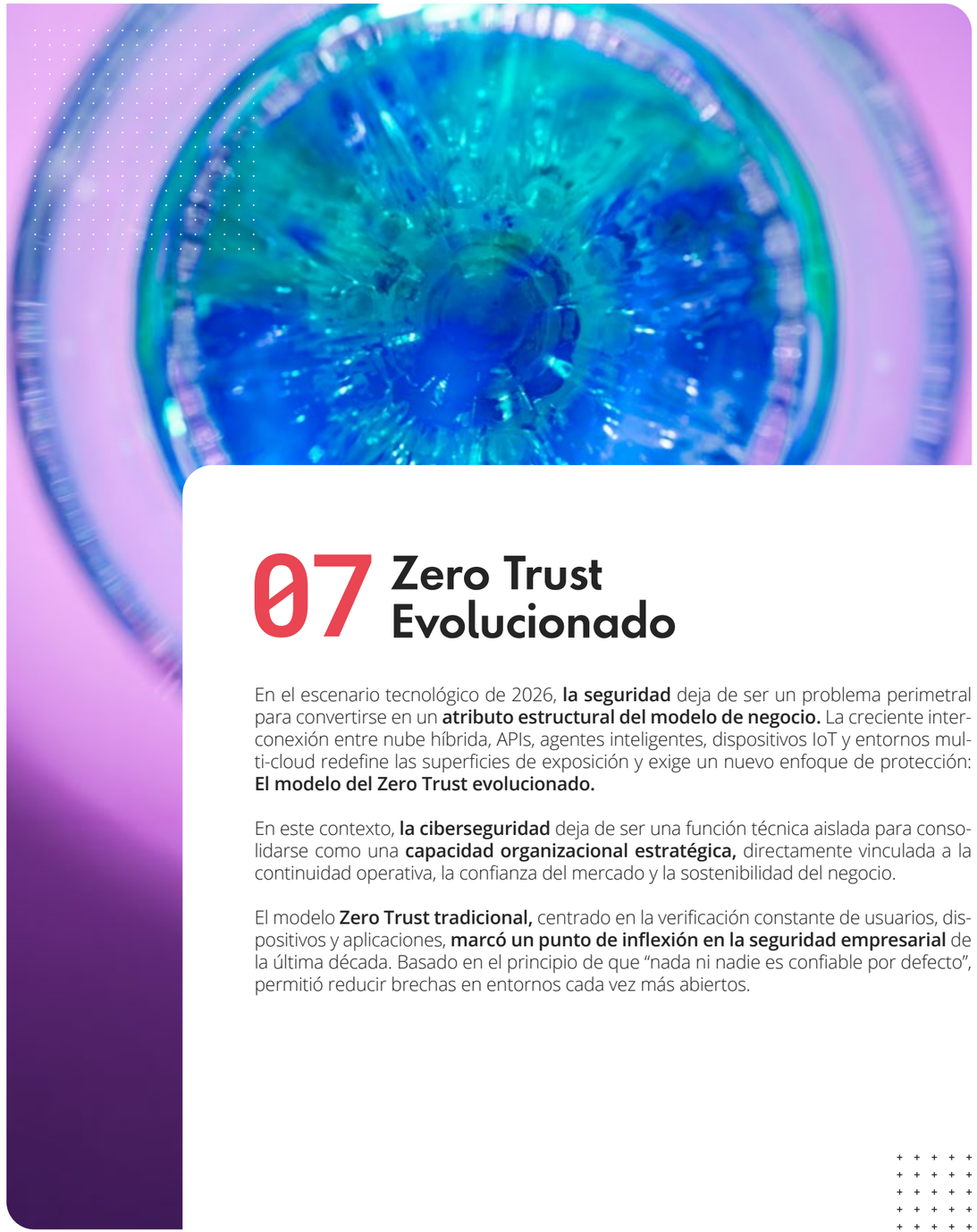
El camino hacia la próxima generación de infraestructura y delivery no pasa por sumar tecnologías de manera aislada, sino por **construir plataformas inteligentes** que integren personas, procesos y tecnología bajo una visión común de **productividad, seguridad y resiliencia operativa.**

Ese salto marca la transición hacia organizaciones preparadas para competir en la economía digital de 2026, donde **la velocidad sin control deja de ser una ventaja, y la gobernanza sin agilidad se vuelve inviable.**

Este nuevo modelo de delivery acelerado y estandarizado eleva, inevitablemente, el nivel de exposición y de riesgo: A mayor autonomía, automatización y velocidad, **mayor es la necesidad de repensar la seguridad como un principio sistémico,** no como una capa posterior.

Es en este punto donde el Platform Engineering y el DevSecOps abren paso a la siguiente evolución: **Un modelo de seguridad distribuido, continuo y contextual,** capaz de acompañar plataformas, agentes y flujos automatizados sin frenar la innovación.

Ese es el umbral que conduce al **Zero Trust evolucionado,** donde la seguridad deja de ser un perímetro o un control puntual para convertirse en un **tejido cognitivo que atraviesa toda la organización**, habilitando confianza, escala y resiliencia en entornos digitales cada vez más autónomos.



07 Zero Trust Evolucionado

En el escenario tecnológico de 2026, **la seguridad** deja de ser un problema perimetral para convertirse en un **atributo estructural del modelo de negocio.** La creciente interconexión entre nube híbrida, APIs, agentes inteligentes, dispositivos IoT y entornos multi-cloud redefine las superficies de exposición y exige un nuevo enfoque de protección: **El modelo del Zero Trust evolucionado.**

En este contexto, **la ciberseguridad** deja de ser una función técnica aislada para consolidarse como una **capacidad organizacional estratégica,** directamente vinculada a la continuidad operativa, la confianza del mercado y la sostenibilidad del negocio.

El modelo **Zero Trust tradicional,** centrado en la verificación constante de usuarios, dispositivos y aplicaciones, **marcó un punto de inflexión en la seguridad empresarial** de la última década. Basado en el principio de que "nada ni nadie es confiable por defecto", permitió reducir brechas en entornos cada vez más abiertos.

Sin embargo, **la escala actual de amenazas y la complejidad de los sistemas digitales demandan una evolución:** Hoy no alcanza con controlar accesos, es necesario **anticipar comportamientos, correlacionar señales y responder de forma autónoma y continua.**

La incorporación de Inteligencia Artificial defensiva redefine por completo la operación del Zero Trust. **La seguridad pasa de ser reactiva a predictiva:** Los modelos analizan patrones de comportamiento, detectan anomalías antes de que se conviertan en incidentes, correlacionan señales provenientes de identidad, red, endpoints y datos, y orquestan respuestas automáticas en tiempo real.

La integración de capacidades de IA en estas arquitecturas está emergiendo como una tendencia que potencia la automatización de la detección y respuesta ante amenazas, reforzando un enfoque de seguridad adaptativa y autoajustable.

Este nuevo enfoque se basa en garantizar confianza dinámica en cada interacción digital, y se sustenta en tres capas convergentes:

La primera es la **identidad como nuevo perímetro,** donde cada acceso se valida de forma continua y contextual, considerando variables como ubicación, comportamiento, nivel de riesgo y tipo de dispositivo.

La segunda es la **automatización defensiva,** que utiliza IA y analítica de comportamiento para anticipar ataques, reducir falsos positivos y ejecutar respuestas autónomas.

La tercera es la **orquestación inteligente,** que unifica seguridad, cumplimiento y operaciones mediante plataformas que aprenden de los incidentes y ajustan las políticas de protección de forma continua.

De acuerdo con la proyección de IDC, el gasto mundial en ciberseguridad seguirá creciendo de doble dígito durante los próximos años, con tecnologías de seguridad como Zero Trust, gestión de identidad avanzada, automatización y analítica basada en IA.

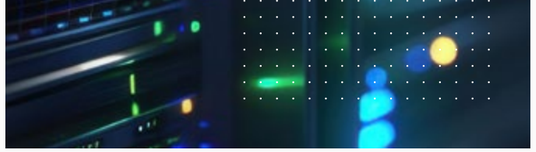
Zero Trust en la era IA Centric y agentiva

La adopción de modelos IA Centric y de automatización agentiva amplifica exponencialmente la superficie de riesgo: Agentes que ejecutan acciones, modelos que toman decisiones y sistemas que interactúan entre sí sin intervención humana directa **redefinen la noción tradicional de control.**

En este nuevo escenario, escalar inteligencia sin escalar confianza equivale a escalar el riesgo junto con la innovación.

El Zero Trust evolucionado se convierte así en el **marco habilitante que permite desplegar autonomía sin perder control,** garantizando que cada identidad, cada flujo de datos y *cada decisión algorítmica opere bajo principios de verificación continua, trazabilidad y responsabilidad.*

No se trata de frenar la automatización, sino de **crear las condiciones** para que la Inteligencia Artificial y los agentes autónomos puedan operar de forma segura, auditable y sostenible.



El desafío cultural: Seguridad como parte del ADN corporativo

Adoptar Zero Trust evolucionado implica mucho más que implementar tecnología: Representa un **cambio cultural profundo.** Su base es **la incorporación de la seguridad desde el diseño** (security by design), integrándola en todo el ciclo de vida de productos y servicios, desde el desarrollo hasta la experiencia del cliente.

Este enfoque promueve una **cultura de corresponsabilidad digital,** donde la protección deja de ser exclusiva del área de TI para convertirse en un componente compartido del modelo operativo.

Aquí convergen prácticas como **DevSecOps,** que integra controles de seguridad automatizados en los pipelines de desarrollo, y **Platform Engineering,** que ofrece entornos preconfigurados, seguros y gobernados para acelerar el delivery sin sacrificar protección.

Según Gartner, las organizaciones que integran seguridad en cada fase del ciclo de desarrollo reducen significativamente las vulnerabilidades explotables antes del despliegue, evidenciando que velocidad, calidad y seguridad ya no son objetivos en tensión, sino variables interdependientes.

Al incorporar automatización defensiva e Inteligencia Artificial, **este modelo incrementa la capacidad de adaptación y garantiza la continuidad operativa** incluso frente a ataques complejos. En sectores críticos como banca, salud o energía, donde el downtime implica pérdidas millonarias por hora, esta capacidad se convierte en una ventaja decisiva.

Según un reporte de IBM, las organizaciones con estrategias Zero Trust maduras, combinadas con capacidades de IA y automatización en sus operaciones de seguridad, lograron reducir en promedio aproximadamente a 1,76 millones el costo de cada brecha de seguridad.

Pero el impacto no es solo financiero: En un contexto donde la confianza es un activo estratégico, el Digital Defense Report de Microsoft señala que, ante un entorno de amenazas crecientes, las organizaciones que comunican de forma transparente sus prácticas de ciberseguridad fortalecen la reputación de marca, la resiliencia operativa y la fidelidad del cliente.

Desde el plano operativo, el Zero Trust evolucionado también impulsa productividad.

Las organizaciones que adopten Zero Trust basado en IA aumentarán ampliamente la productividad de sus equipos de TI al reducir tareas manuales de monitoreo y respuesta. Al mismo tiempo, su arquitectura facilita el cumplimiento regulatorio, ofreciendo trazabilidad, auditoría continua y registro automático frente a normativas de privacidad, seguridad e Inteligencia Artificial.

En este sentido, **Zero Trust evolucionado redefine el rol del liderazgo tecnológico:** Ya no se trata de reaccionar ante incidentes, sino de **diseñar organizaciones donde la seguridad es inherente a la forma en que se innova, se entrega valor y se escala el negocio.**

Zero Trust comienza a posicionarse como un **diferenciador competitivo.** Las organizaciones que avanzan hacia modelos integrales no solo reducen riesgos, sino que tienden a acelerar la digitalización de procesos críticos, fortalecer el cumplimiento y construir confianza en mercados cada vez más exigentes.

En la economía digital de 2026, la confianza ya no es una consecuencia: Es una condición de diseño. El Zero Trust evolucionado protege activos, habilita innovación segura, automatización responsable y toma de decisiones confiable en entornos de alta complejidad.

Una vez establecida esta base de confianza dinámica, el desafío siguiente es extender estos principios al activo más crítico de la organización: **El dato.**

08 Gobierno de datos y privacidad: La base de la confianza y el cumplimiento

En el escenario tecnológico actual, **la gobernanza de datos se consolida como un pilar estratégico fundamental** en la economía digital. Los datos se han convertido en el cimiento sobre el que se construye la confianza, la competitividad y la sostenibilidad empresarial. Su gestión adecuada es una decisión crítica que impacta la estrategia global de las organizaciones.

Daniel Y. reflexiona: "Si los datos son un activo que sabemos que tiene valor, y muchas organizaciones los monetizan ¿por qué no los cuidamos como cualquier otro activo? Nadie dejaría petróleo o herramientas tiradas por ahí sin saber dónde están y sin ningún cuidado. Si los datos son un activo, debiésemos actuar acordemente"

La gobernanza es hoy fundamental

El volumen global de datos continúa creciendo exponencialmente, y según IDC, se estima que el Global Datasphere superará los 200 zettabytes para 2026. Este auge se ve impulsado por la expansión de la Inteligencia Artificial generativa, el edge computing y la digitalización industrial.

En este contexto, los modelos tradicionales de gestión centralizada de datos se están quedando obsoletos. **La respuesta estructural está en marcos modernos como Data Fabric y Data Mesh,** que permiten **integrar, gobernar y escalar los datos de manera descentralizada, manteniendo coherencia,** control y garantizando la calidad de la información.

Data Fabric actúa como una capa inteligente que conecta fuentes dispares (on-premise, nube, edge o SaaS) **para ofrecer una visión unificada y gobernada de los datos.** La adopción de este modelo habilita una reducción de los costes operativos de integración y gestión de datos, además de acelerar la entrega de insights de negocio.

Data Mesh propone un modelo federado en el que cada dominio de negocio asume la responsabilidad sobre sus propios datos como "productos", garantizando calidad, trazabilidad y valor contextual. **Este enfoque distribuye la gobernanza, impulsa la autonomía y convierte al dato en un bien compartido,** no en un recurso fragmentado.

El impacto táctico

El desafío de implementar una estrategia de gobernanza de datos no es únicamente técnico, sino estratégico. implementan un marco de gobernanza de datos maduro habilita a las organizaciones a **incrementar su eficiencia operativa, reducir errores analíticos y obtener hasta el doble de retorno** sobre sus inversiones en IA y analítica avanzada. Estos modelos de gobernanza no solo mejoran la productividad, sino que generan valor tangible para la organización.

Por otro lado, el **entorno regulatorio global** está imponiendo nuevas exigencias que las empresas deben abordar con urgencia. En Europa, regulaciones como el **AI Act** y el **Data Governance** Act están estableciendo estrictas obligaciones de transparencia, trazabilidad y documentación.

En América Latina, más de diez países (entre ellos Argentina, Brasil, Chile, México y Colombia) están avanzando hacia marcos de protección de datos inspirados en el RGPD europeo.

Esta convergencia normativa subraya la importancia de la gobernanza de datos como una dimensión estratégica para la competitividad.

Cuatro ejes estratégicos

La gobernanza de datos efectiva se apoya en cuatro pilares clave:

Trazabilidad y calidad: Asegurar que cada dato tenga un origen verificable y cumpla con estándares de integridad y precisión.

Privacidad por diseño: Incorporar la protección de datos desde el inicio de todo desarrollo digital (privacy by design), lo que no solo cumple con la normativa, sino que genera confianza tanto dentro como fuera de la organización.

Seguridad y cumplimiento continuo: Integrar auditorías automáticas, cifrado y control de acceso adaptativo, alineando la gestión de los datos con los principios de Zero Trust, minimizando riesgos y fortaleciendo la resiliencia de los sistemas.

Ética y transparencia: Establecer políticas que garanticen el uso legítimo de los datos en modelos de IA, evitando sesgos y reforzando la confianza social en las tecnologías emergentes.

El motor que impulsa la institucionalización

El valor estratégico de una buena gobernanza de datos se observa cuando **esta opera como motor de transformación cultural y organizacional,** y no solo como un marco normativo o tecnológico.

Según **McKinsey,** las organizaciones que institucionalizan una **cultura sólida de datos y analítica** —integrando los datos en la toma de decisiones y adoptando un enfoque estratégico sobre analítica avanzada— tienen una probabilidad significativamente mayor de que sus iniciativas de data y analytics contribuyan con al menos un 20% de su EBIT (resultado operativo), en comparación con compañías con menor madurez en datos.

Este cambio cultural fortalece la confianza interna en la información, mejora su disponibilidad y **potencia la colaboración entre áreas,** promoviendo procesos más coherentes y decisiones basadas en datos de mayor calidad.

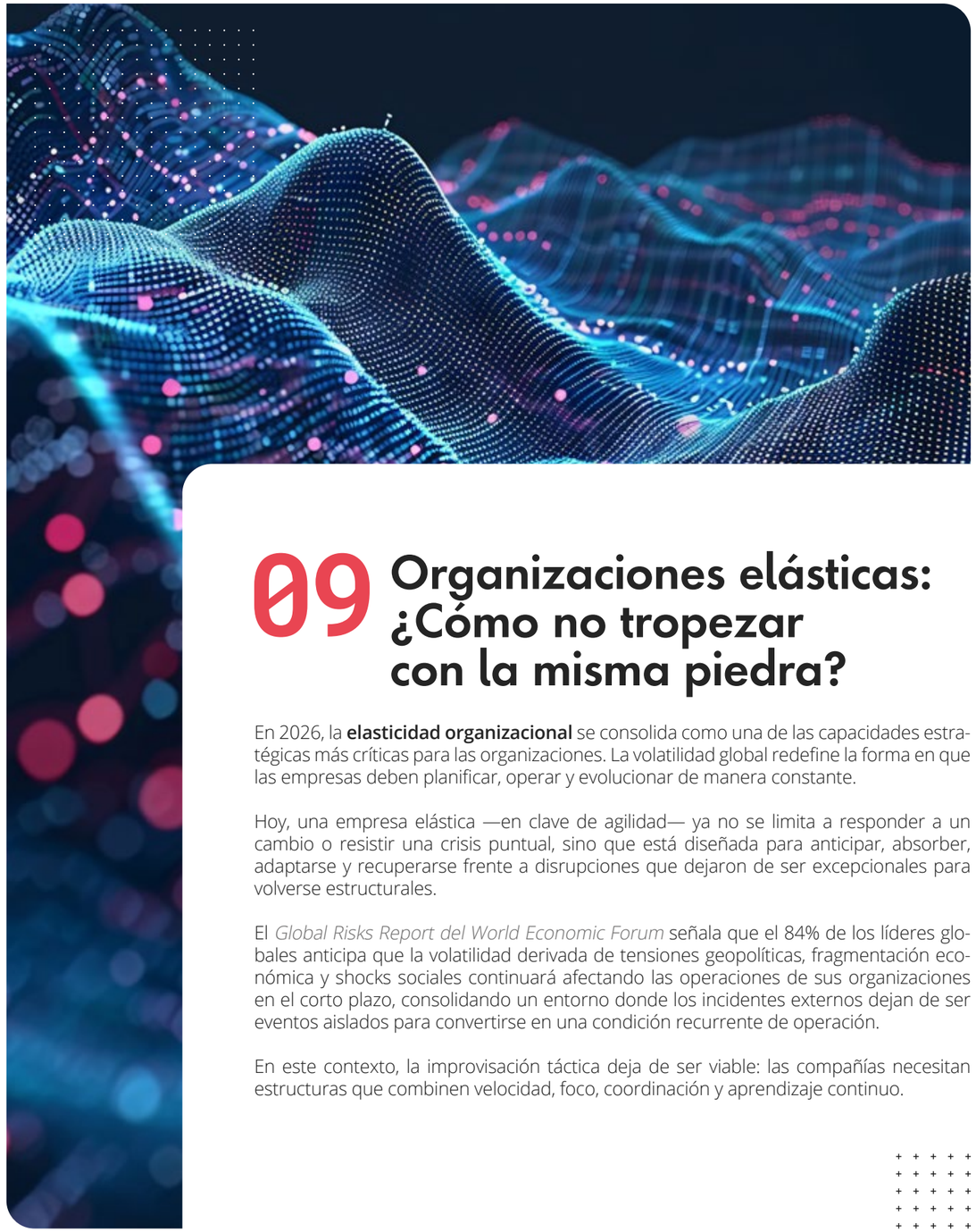
Leandro Tirante, Head of Data en Practia, sentencia: "Nosotros no gestionamos datos para cumplir normas, los gobernamos para sobrevivir y escalar. Sin una base de confianza sólida, la Inteligencia Artificial y la digitalización son solo promesas vacías"

En un entorno cada vez más competitivo, la gobernanza de datos opera como una **palanca estratégica fundamental:** la forma en que una organización gestiona, protege y utiliza sus datos puede marcar la diferencia entre el éxito y el fracaso, no solo en términos operativos, sino también en la **sostenibilidad a largo plazo y en la construcción de confianza** con clientes, inversionistas y otros stakeholders.

Practia acompaña a las organizaciones en la creación de una estrategia integral de gobierno de datos que conecte la tecnología con los objetivos del negocio y el cumplimiento normativo. Su enfoque aborda desde la definición de políticas de **data** y trazabilidad, hasta la integración de modelos como **Data Fabric y Data Mesh,** asegurando que los datos sean gestionados con precisión, ética y responsabilidad.

La convergencia entre **gobernanza de datos, privacidad y resiliencia** marca un punto de inflexión en la evolución del ecosistema digital. Para las organizaciones, la clave no está solo en proteger su infraestructura, sino en **garantizar la integridad, la trazabilidad y el uso ético de los datos,** que sustentan las decisiones empresariales más relevantes.

La forma en que las empresas gestionan sus datos se convierte en la base para **sostener la innovación, asegurar el cumplimiento regulatorio y promover un crecimiento sostenible** en la economía digital del futuro.



09 Organizaciones elásticas: ¿Cómo no tropezar con la misma piedra?

En 2026, la **elasticidad organizacional** se consolida como una de las capacidades estratégicas más críticas para las organizaciones. La volatilidad global redefine la forma en que las empresas deben planificar, operar y evolucionar de manera constante.

Hoy, una empresa elástica —en clave de agilidad— ya no se limita a responder a un cambio o resistir una crisis puntual, sino que está diseñada para anticipar, absorber, adaptarse y recuperarse frente a disrupciones que dejaron de ser excepcionales para volverse estructurales.

El *Global Risks Report del World Economic Forum* señala que el 84% de los líderes globales anticipa que la volatilidad derivada de tensiones geopolíticas, fragmentación económica y shocks sociales continuará afectando las operaciones de sus organizaciones en el corto plazo, consolidando un entorno donde los incidentes externos dejan de ser eventos aislados para convertirse en una condición recurrente de operación.

En este contexto, la improvisación táctica deja de ser viable: las compañías necesitan estructuras que combinen velocidad, foco, coordinación y aprendizaje continuo.

Arquitectura organizacional

La capacidad adaptativa contemporánea no se construye únicamente desde la infraestructura tecnológica, sino desde la capacidad de la organización para responder y reacomodarse de forma continua.

En entornos donde la incertidumbre dejó de ser excepcional para volverse estructural, sostener velocidad y alineamiento estratégico depende menos de la incorporación de nuevas herramientas y más del diseño de organizaciones capaces de ajustar sus prioridades, redistribuir esfuerzos y aprender mientras operan.

En este marco, — y tal como lo hacemos en Practia— los modelos ágiles no funcionan como soluciones aisladas ni como prácticas metodológicas aplicables únicamente a nivel de equipo, sino como marcos que permiten desarrollar **elasticidad organizacional:** la capacidad de amoldarse sin perder dirección, de responder sin desarticularse y de evolucionar sin necesidad de rediseñarse ante cada nueva disrupción.

"Este rediseño en la forma en que se prioriza, se decide y se coordina el trabajo, supone distribuir la toma de decisiones hacia donde se encuentra la información más relevante, operar en ciclos más cortos de inspección y adaptación, y empoderar equipos para experimentar, fallar temprano y ajustar antes de escalar", comenta ***Martín Cordiano, Agile Product Manager en Practia.***

En contextos de alta incertidumbre, la planificación deja de ser un ejercicio de predicción y pasa a ser un proceso iterativo. Las organizaciones no pueden diseñar una planificación a largo plazo, pero si sostener una visión estratégica a partir de ejecutar en ciclos breves que les permitan validar hipótesis, aprender rápidamente y reorientar esfuerzos sin fricción estructural.

Desde esta perspectiva, no es solo resistir el cambio, sino funcionar eficazmente mientras el contexto cambia. En escenarios donde tecnologías habilitadoras como la Inteligencia Artificial, la automatización, el data fabric o el edge computing evolucionan mes a mes, la ventaja competitiva ya no estará únicamente en su adopción, sino en la capacidad de las organizaciones —y de las personas que las integran— para reorientar rápidamente su uso, transformar el error temprano en aprendizaje y convertir ese aprendizaje en decisiones accionables.

Gestión del cambio: El motor continúa siendo humano

A pesar de los avances tecnológicos, las transformaciones siguen fallando donde siempre fallaron: *En la dimensión humana.*

La mayoría de los fracasos de transformación digital se debe a **la falta de estrategias de Change Management maduras,** no a limitaciones técnicas. La resiliencia requiere comportamientos colectivos sostenidos en el tiempo: Adaptabilidad, transparencia, coordinación interáreas y capacidad de incorporar nuevas prácticas sin fricción.

En organizaciones donde la IA redefine roles, la automatización elimina tareas repetitivas y los equipos operan en esquemas híbridos y distribuidos, **la gestión del cambio se convierte en la columna vertebral de la continuidad operativa.**

"Actualmente, para una adopción cultural razonable, es tan crítico para las organizaciones preparar a las personas como preparar las herramientas", comenta ***Guillermo Ibañez, responsable de la Práctica de Project Management en Practia.***

Value Management Office (VMO): Gobernar el valor

Como evolución natural del modelo operativo moderno, surge el **Value Management Office (VMO),** una figura cada vez más extendida en organizaciones que buscan capturar valor de manera sostenida.

Martín C, *argumenta que: "A diferencia de las PMO tradicionales, el VMO se enfoca en resultados, impacto y alineación estratégica, no solo en la ejecución de proyectos. Apalancados en ciclos cortos de inspección y adaptación este modelo genera ventajas estratégicas como la captura efectiva de valor permanente y reducir ampliamente las ineficiencias de su portafolio. De esta forma agilizamos el modelo de gestión estratégica, donde la estrategia y la operación están siempre alineadas y los datos nos permites tomar mejores decisiones."*

Inteligencia Operacional

La capacidad adaptativa de las organizaciones elásticas no depende únicamente de procesos o herramientas, sino de cómo las personas interactúan con la información para tomar decisiones en entornos cambiantes.

De acuerdo con el informe *Cost of Complexity* del IBM Institute for Business Value, **la automatización inteligente puede traducirse en una disminución de hasta un 36% en incidentes vinculados a seguridad y una reducción del 28% en costos de TI,** además de un crecimiento de ingresos asociado a estas inversiones.

Sin embargo, estos resultados no provienen solo de la tecnología, sino de su integración efectiva en los flujos de trabajo de los equipos. En este contexto, la adaptación deja de ser únicamente una cuestión estructural y pasa a configurarse como una competencia híbrida: humana, tecnológica y organizacional. La toma de decisiones comienza a apoyarse en información accesible en tiempo real, habilitando dinámicas de trabajo más distribuidas, colaborativas y ajustables frente al cambio.

Construir esta capacidad plantea un nuevo desafío estratégico: ¿cómo preparar a las personas para operar en entornos donde la Inteligencia Artificial y la automatización redefinen roles, habilidades y formas de colaboración?

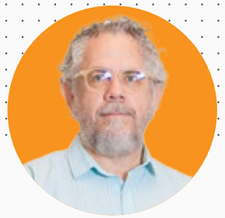
10 Talento digital: Workforce aumentada

En 2026, el concepto de **talento digital** atraviesa una redefinición profunda. Ya no alcanza con disponer de profesionales calificados ni con atraer perfiles escasos al mercado. En el presente, emerge con fuerza el paradigma de la **"Workforce aumentada".**

Se trata de un modelo de upskilling estructurado por rol y perfil, en el que las capacidades humanas se expanden de manera sistemática mediante Inteligencia Artificial, automatización y herramientas cognitivas, integradas al aprendizaje en el trabajo y acompañadas por métricas claras de adopción y productividad.

En este esquema, las organizaciones dejan de gestionar únicamente "recursos humanos" para diseñar **ecosistemas de talento,** donde personas, agentes inteligentes y plataformas tecnológicas colaboran de forma integrada para sostener productividad, innovación y resiliencia.

Este cambio responde a una presión estructural: **La escasez global de habilidades digitales se consolida como uno de los principales riesgos estratégicos para la ejecución del negocio.**



*Tal como comenta **Juan V. Echagüe, Director de Investigación y Desarrollo en Practia,** "De alguna manera la decisión de adoptar Inteligencia Artificial ya la tomaron nuestros clientes, como ya ocurrió antes con la web y los teléfonos celulares. Lo que tenemos que decidir en las empresas es cómo hacerlo de manera ética y segura, generando valor. Y cómo llegar a tiempo.".*

La mayoría de los CIOs a nivel mundial ya identifica la falta de capacidades tecnológicas como el principal freno para llevar adelante sus agendas de transformación, en un contexto donde la demanda de nuevos roles crecerá de forma acelerada durante el resto de la década. La brecha no es coyuntural ni se resuelve únicamente con contratación, es sistémica y acumulativa.

> El verdadero desafío ya no es atraer talento, **sino transformar continuamente las capacidades internas.**

Upskilling y Reskilling: El nuevo estándar

Este escenario obliga a **replantear de raíz los modelos de formación,** desarrollo profesional, liderazgo y colaboración. El **upskilling y el reskilling** dejan de ser iniciativas tácticas o programas aislados de capacitación y se convierten en una **política estructural de supervivencia competitiva.**

Las organizaciones que invierten de manera sostenida en formación digital, academias internas y aprendizaje continuo logran no solo mejorar la productividad y acelerar la adopción tecnológica, sino también **reducir la rotación en roles críticos y fortalecer su capacidad de innovación.**

La evidencia muestra que cuando la formación se sostiene en el tiempo y se integra al modelo operativo, consecuentemente *aumenta la velocidad de lanzamiento de nuevos productos, la calidad de las decisiones y la capacidad de absorber cambios tecnológicos sin fricción.*

La Inteligencia Artificial, lejos de reemplazar al talento, redefine su rol. El impacto se manifiesta en tres dimensiones simultáneas:

- Por un lado, la automatización de tareas burocráticas y operativas reduce la carga manual y el error humano.
- Por otro, la IA amplifica las capacidades humanas, permitiendo decisiones más informadas, mayor velocidad en el desarrollo y análisis más precisos.
- Finalmente, emergen nuevos roles que combinan criterio técnico, pensamiento crítico y comprensión ética: Perfiles que entrenan modelos, diseñan interacciones humano-máquina, gobiernan riesgos algorítmicos y orquestan arquitecturas de automatización avanzada.

La productividad deja de depender exclusivamente del número de personas y pasa a depender de **cómo se combina talento humano con Inteligencia Artificial.**

Workforce en el epicentro

Este cambio tecnológico trae aparejado un cambio cultural inevitable: **La workforce aumentada exige nuevas formas de liderazgo y colaboración.**

Los equipos de alto desempeño en entornos digitales comparten patrones claros: Autonomía alineada a propósito, transparencia en métricas y objetivos, y fluidez en el uso de plataformas e IA como parte del trabajo cotidiano.

El liderazgo se desplaza desde estructuras jerárquicas hacia un rol habilitador, enfocado en crear condiciones para el aprendizaje continuo, la toma de decisiones basada en datos, la seguridad psicológica y la coordinación en ciclos cortos.

"La cultura digital no se impone con discursos, se construye a través de prácticas, rituales y herramientas coherentes con el modelo operativo", comenta ***Guillermo Ibañez, responsable de la Práctica de Project Management en Practia.***

El desafío latinoamericano

En América Latina, este desafío se manifiesta con particular intensidad. La región enfrenta una brecha persistente de profesionales en áreas STEM y tecnología, acompañada por déficit de competencias avanzadas, fuga de talento y baja articulación entre academia, empresas y sector público.

Sin embargo, también cuenta con una ventaja estratégica relevante: Una fuerza laboral joven, adaptable y con creciente acceso a plataformas cloud y formación digital. Esto habilita acelerar procesos de reconversión mediante academias internas, programas intensivos de reskilling y modelos de aprendizaje asistido por IA, **reduciendo la dependencia exclusiva del mercado externo.**

En este contexto, desde Practia, una empresa Publicis Sapient, estamos dando los primeros pasos en un rol activo orientado al desarrollo de talento digital en la región. Abordamos este desafío desde una mirada amplia y en evolución, combinando definición estratégica, formación técnica, acompañamiento cultural y la incorporación progresiva de Inteligencia Artificial aplicada al aprendizaje.

A través de iniciativas internas que estamos poniendo en marcha —como academias alineadas a marcos tecnológicos actuales, programas de reskilling que permiten reconvertir perfiles operativos en roles digitales en ciclos acotados, y primeros modelos de equipos aumentados donde profesionales comienzan a trabajar junto a agentes inteligentes— acompañamos a las organizaciones en la **construcción gradual de capacidades,** evitando depender de acciones aisladas y favoreciendo una adopción sostenida en el tiempo.

Estamos seguros de que, en la economía digital de 2026, el talento del futuro no se busca exclusivamente en el mercado: **Se diseña, se desarrolla y se gobierna. La workforce aumentada** redefine cómo las organizaciones operan, aprenden y crean valor. Y este cambio desemboca inevitablemente en **una evolución del liderazgo.**

Ernesto K., *agrega que: "Desde nuestra organización consideramos que tenemos una oportunidad pensando al talento como una ventaja competitiva que se diseña y gobierna, y no como un recurso escaso que debe comprarse."*

11 Hoy la corona está en manos del CIO

En 2026, el rol del CIO atraviesa la transformación más profunda desde su creación. Lo que históricamente fue una función orientada a garantizar continuidad operativa, disponibilidad tecnológica y control de costos, se ha convertido en **una posición central en la definición del rumbo del negocio.**

El CIO del presente se consolida como el arquitecto del modelo digital, custodio del dato, habilitador de la Inteligencia Artificial y líder cultural de organizaciones que se expanden impulsadas por tecnología. Hoy, la **responsabilidad estratégica está en sus manos.**

En un contexto de creciente incertidumbre y versatilidad, las decisiones tecnológicas marcan el rumbo del negocio e impactan de manera directa en el desempeño financiero, el cumplimiento regulatorio, la reputación y la competitividad de las compañías.
No existe hoy ninguna decisión relevante —desde expansión, eficiencia, innovación o sostenibilidad— **que no tenga una dimensión tecnológica crítica.**

Esta centralidad se explica por una convergencia inédita: Arquitectura cloud, Inteligencia Artificial, ciberseguridad, datos, automatización, plataformas internas y talento aumentado ya no son dominios aislados, sino que forman un **sistema interdependiente** que define la forma en que una organización opera, aprende, se adapta y crea valor.

Gobernar al interior de la complejidad es, en esencia, **la nueva misión del CIO.**

Del modelo operativo al modelo arquitectónico

El CIO de 2026 se ha transformado. Ya no es evaluado únicamente por la estabilidad de la infraestructura o la eficiencia del gasto tecnológico, sino que se espera que diseñe modelos operativos, cree capacidades organizacionales, habilite Inteligencia Artificial responsable, impulse talento aumentado y asegure que el dato se gestione como un activo estratégico.

Su rol se expande hacia **cuatro dimensiones críticas que redefinen su impacto en el negocio.**

En primer lugar, el CIO se consolida como **estratega corporativo:** Participa activamente en la definición de la visión empresarial, en virtud de incrementar el éxito en sus iniciativas digitales y un crecimiento más sostenido de los ingresos asociados a tecnología en las compañías. La tecnología se convierte en insumo de la estrategia desde su concepción.

En segundo lugar, actúa como **arquitecto de plataformas y capacidades:** Su responsabilidad ya no es administrar sistemas, sino orquestar ecosistemas híbridos que integran nube, edge, automatización, Zero Trust, datos y plataformas internas orientadas a desarrolladores y equipos de negocio. Estas plataformas se convierten en el sistema nervioso del negocio digital, habilitando velocidad, gobernanza y escalabilidad simultáneamente.

En tercer lugar, se consolida como **custodio del dato y de la Inteligencia Artificial:** A medida que la IA generativa y los agentes autónomos se integran en procesos críticos, la trazabilidad, la seguridad, la ética y el valor de los modelos se vuelven una responsabilidad indelegable. La gobernanza de la IA deja de ser un tema técnico para convertirse en un imperativo estratégico compartido con las áreas de datos, riesgo y compliance.

Finalmente, asume una dimensión cada vez más relevante como **líder cultural y de talento aumentado:** En organizaciones donde el trabajo se redefine por la automatización y la IA, el CIO impulsa nuevas formas de aprendizaje continuo, colaboración humano-máquina y liderazgo distribuido. El impacto no es menor: Culturas digitales maduras mejoran productividad, retención y capacidad de adaptación.

Mauricio S. *comenta: "El CIO deja de ser un habilitador tecnológico para convertirse en garante de continuidad, confiabilidad y transición. Y surge como integrador entre dos mundos: IT y OT. Sus decisiones impactan directamente en la estabilidad del sistema, el cumplimiento regulatorio y la capacidad de integrar, automatizar y poner en funciones la IA, sin comprometer el suministro, la continuidad operativa y el abastecimiento."*

De esta manera, El CIO ya no ocupa un rol eminentemente técnico, y se transforma en un **guía profundamente humano y empresarial,** capaz de traducir complejidad tecnológica en decisiones comprensibles y accionables para el negocio.

El nuevo mandato: Continuidad y sostenibilidad

Los capítulos anteriores convergen en una conclusión clara: La resiliencia operativa se ha transformado en una variable central del valor económico. Infraestructura híbrida, Zero Trust evolucionado, agilidad a escala, automatización y gobierno del dato no generan ventaja por separado; lo hacen cuando **son integrados bajo una visión coherente.**

Ese rol de integración recae, de manera natural, en el CIO. Las organizaciones donde el liderazgo tecnológico asume la resiliencia y la continuidad como ejes estratégicos, tienden a reducir significativamente las pérdidas asociadas a interrupciones y acelerar de forma sustancial los tiempos de recuperación.

Liderazgo tensionado por la IA

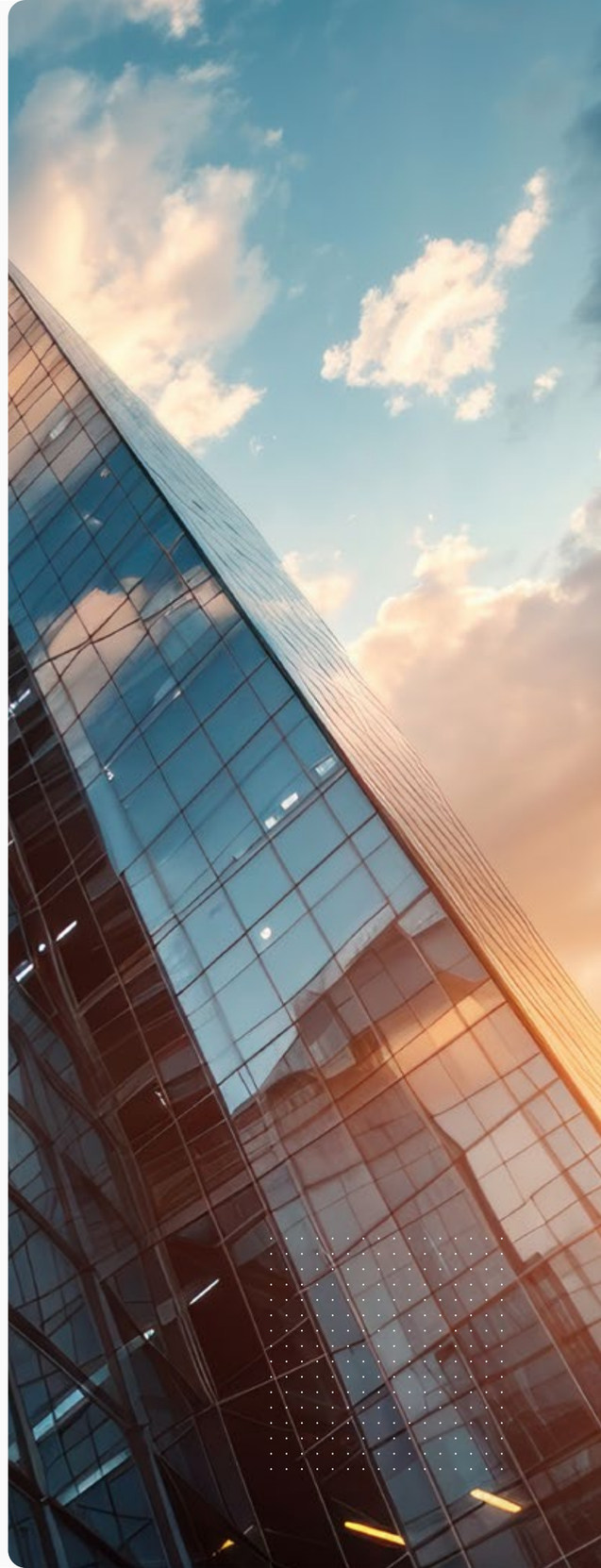
La Inteligencia Artificial amplificó la dualidad entre oportunidad y riesgo, como nunca antes. Su potencial para incrementar productividad, acelerar decisiones y habilitar nuevos modelos de negocio es indiscutible. **Pero esos beneficios solo se materializan cuando la adopción se realiza bajo marcos claros de gobernanza, ética, seguridad y control.**

Aquí el mayor desafío radica en conseguir un equilibrio que habilite innovación sin comprometer confianza; Acelere adopción sin perder trazabilidad; Otorgue autonomía sin exponer riesgos sistémicos; Y despliegue agentes inteligentes sin erosionar la confiabilidad de los procesos. **El dominio de la IA demanda coraje estratégico y sensibilidad organizacional.**

Cuando el CIO lidera activamente marcos como AI TRiSM, las organizaciones reducen incidentes asociados a modelos y logran una adopción más amplia y sostenible de la IA por parte del negocio. **La confianza se convierte en el principal acelerador de valor.**

LATAM: El CIO como puente de transformación

En América Latina, el rol del CIO adquiere una relevancia adicional. Debe gestionar la adopción tecnológica en contextos donde conviven restricciones presupuestarias, brechas de talento, legados históricos y una presión cre-



ciente por digitalizar procesos y modelos de negocio. Sin embargo, la región muestra una aceleración ascendente en inversión en IA, nube, seguridad y modernización de datos, así como en la adopción de modelos de agilidad a escala.

Esto posiciona al CIO regional como **un puente entre ambición y ejecución.**

El líder latinoamericano dirige transformación: Tiene la oportunidad de impulsar una adopción directa de marcos modernos de IA responsable, plataformas internas, Zero Trust y arquitecturas de datos avanzadas, con el objetivo de construir organizaciones más competitivas que no repliquen errores de mercados más maduros.

*Como advierte **Miguel Bilello:** "El CIO ha dejado de ser un custodio de sistemas para convertirse en uno de los ejecutivos más influyentes de la empresa contemporánea, al interior de un mundo en el que ya no existen organizaciones ajenas a la tecnología. Esta se vuelve omnipresente y transforma cada proceso, cada decisión, cada actividad de la vida corporativa"*

En Practia, una empresa Publicis Sapient, sostenemos una convicción clara: El CIO, actuando como socio en el diseño de capacidades, es hoy el rol más influyente del ecosistema digital.

Este estilo de liderazgo —transversal, estratégico, humano y profundamente tecnológico— es el que permite cerrar la primera era de la transformación digital e inaugurar una nueva: **La del negocio aumentado,** donde la inteligencia colectiva entre personas, IA y plataformas se convierte en motor de valor sostenido.

*"La encuesta realizada por Practia a 289 empresas del Cono Sur revela que más del 60% de los CIOs reporta directamente al CEO, no como un mero ejecutor, sino como un socio estratégico en la ardua tarea de la transformación digital. Más aún, el 72% participa activamente en la definición de la estrategia empresarial y en la creación de valor para el cliente, mientras que un contundente 91% se encuentra profundamente involucrado en ese proceso de cambio permanente que llamamos transformación digital", agrega **Miguel.***

Conclusión | 2026: El año en que la tecnología es el ADN del negocio

El 2026 marca el punto de inflexión más profundo desde el inicio de la transformación digital. No es simplemente un cambio tecnológico: **Es un cambio cultural.**

Cada capítulo de este Insight converge en una idea central: **La tecnología dejó de ser un habilitador, para convertirse en el ADN del negocio, pautando cómo las organizaciones existen, operan, se adaptan, crean valor y sostienen confianza.**

La Inteligencia Artificial se coloca como la **capa cognitiva transversal** que amplifica capacidades humanas, automatiza decisiones, rediseña procesos y acelera resultados.

La **infraestructura** evoluciona hacia modelos híbridos, inteligentes y energéticamente responsables.

La **seguridad** deja de ser un perímetro estático para convertirse en un sistema vivo, predictivo y adaptativo.

Los **datos** se consolidan como un activo estratégico que debe ser gobernado con trazabilidad, ética y responsabilidad.

La **resiliencia** deja de ser defensiva para ser un diferencial competitivo de las empresas aumentadas.

En paralelo, **el talento** ya no compite con **la máquina, se complementa** con ella.

La noción de workforce aumentada redefine el trabajo, la productividad y el aprendizaje continuo.

Inspirado en el modelo del **"Centauro",** personas y sistemas inteligentes colaboran para **expandir la capacidad organizacional** a niveles inéditos, dando lugar a un nuevo estándar de desempeño.

Todo esto configura **una nueva arquitectura empresarial** donde la velocidad de decisión, la confianza operativa y la adaptabilidad estructural se convierten en las monedas más valiosas del mercado.

Las tres condiciones de la competitividad moderna

Las organizaciones que comandarán esta década no serán necesariamente las más grandes ni las que adopten más tecnología, sino aquellas que **logren sostener tres condiciones simultáneas:**

- Pensar **IA-centric,** integrando inteligencia en cada capa del negocio, desde la operación hasta la toma de decisiones estratégicas.
- Operar con **resiliencia estructural,** diseñando sistemas capaces de anticipar, absorber y recuperarse del cambio continuo.
- Construir **talento aumentado,** con profesionales capaces de aprender, colaborar y crear valor junto a plataformas y agentes inteligentes.

Este triángulo —Inteligencia Artificial, resiliencia y talento— **redefine la competitividad contemporánea.**

Ya no se trata solo de ejecutar mejor, sino de **aprender más rápido, decidir con mayor precisión y evolucionar de manera sostenida.** En este nuevo escenario, la improvisación táctica deja de ser una opción viable.

Si hubiera que sintetizar este documento en una sola idea, sería la siguiente: **La ventaja de los próximos años no estará en tener más tecnología, sino en desarrollar mejores capacidades para convertirla en valor.**

El futuro pertenece a las organizaciones que vinculen IA con propósito, seguridad con estrategia, datos con ética, talento con aprendizaje continuo y liderazgo con visión.

En LATAM, esta urgencia es aún mayor: La ventana para transformar capacidades en ventaja competitiva es más corta y el margen de error, menor.

El 2026 marca el inicio de la era del Negocio Aumentado, capaz de alcanzar niveles de productividad, creatividad y resiliencia inéditos. El desafío ya no es imaginar lo que viene, es diseñarlo, gobernarlo y construirlo. **Y ese desafío comienza ahora.**

practia

A company of
publicis sapient

Insight Anual 2026

PRIORIDADES, TENDENCIAS Y DESAFÍOS TI