



Powered by Gnsys Insights



Lo que cambió en 2025 y lo que viene para 2026

Editorial

El 2025 marcó un punto de ruptura en la forma en que las organizaciones asignan su presupuesto tecnológico. El crecimiento global del gasto en TI, estimado **entre el 10% y el 14%**, no respondió a una expansión generalizada de todos los rubros, sino a una concentración clara en infraestructura habilitadora de datos: Servidores de alto desempeño, capacidades de cómputo acelerado, almacenamiento escalable y redes de baja latencia absorbieron una parte sustantiva de la inversión, desplazando otras prioridades tradicionales.

En este contexto, 2026 se perfila como el año en que muchas organizaciones deberán “poner orden” en su ecosistema tecnológico. Consolidar plataformas, tomar decisiones más selectivas sobre nube e infraestructura local, estandarizar monitoreo y avanzar en automatización serán pasos necesarios para transformar el impulso de 2025 en una base sólida, controlada y escalable. Más que crecer por inercia, el reto será gobernar el crecimiento con criterio técnico y visión estratégica.

EN ESTE NÚMERO

EL CAMINO DE LA I.A. EN MÉXICO ¿BURBUJA O CONSOLIDACIÓN?

VMWARE / BROADCOM — LAS NUEVAS REGLAS DEL JUEGO

LA CIBERSEGURIDAD: EL SEGURO DIGITAL QUE TODA EMPRESA NECESITA



El camino de la I.A. en México. ¿Burbuja o consolidación?

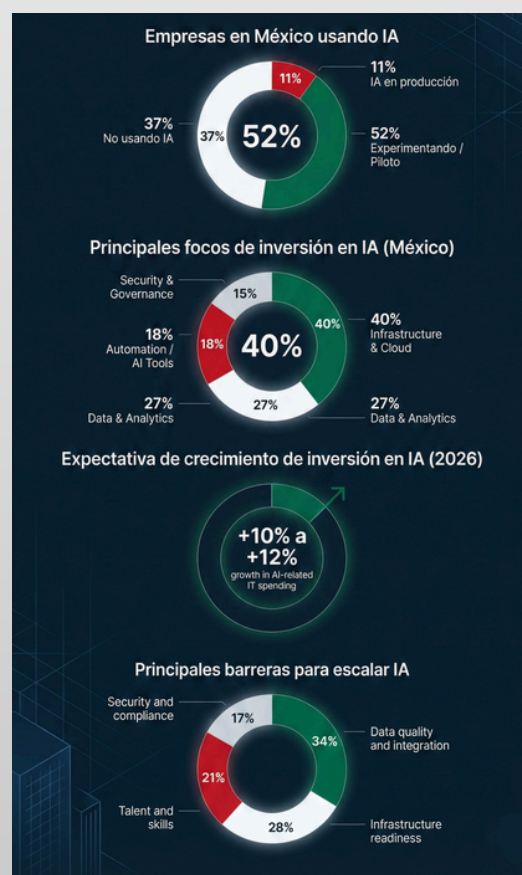
Roberto Sánchez

Hay muchas perspectivas posibles para hablar de lo que hoy llamamos 'inteligencia artificial'. Desde una perspectiva general, vemos su desarrollo dominar la conversación sobre tecnología, y a su vez comenzamos a pensar sobre qué efectos *reales* veremos en el plano empresarial. Podemos entrever también que no es solo una pirueta más de *Silicon Valley* ofreciendo novedosas maneras de 'hacer las mismas cosas'; pues detrás del desarrollo hay una inercia global que se alza entre estrategias corporativas a gran escala, la carrera por chips, la generación masiva de datos, y hasta gobiernos (como lo es el de Estados Unidos y China) aportando su influencia y recursos como estados para consolidar liderazgo.

La conversación es interminable, y además está en boca de todos de alguna manera u otra. Pero aquí no hablaremos sobre credibilidad o escepticismo en lo que 'verdaderamente' es la IA, o lo que "sí hace o no hace"; aquí buscaremos distinguir que implicaciones tiene para el mundo empresarial en México y sus consumidores.

No porque el lado macroeconómico o de cultura tecnológica no nos sea relevante, o que no estemos ya anclados a su desarrollo e impacto casi involuntariamente; sino porque faltan diálogos que nos ayuden a pensar sobre los efectos próximos en nuestra cultura organizacional.

La economía mexicana es particularmente compleja: conviven empresas familiares tradicionales con corporativos multinacionales, economía informal con sectores altamente industrializados, y una herencia cultural que valora las relaciones personales tanto como la eficiencia operativa. Esta diversidad dificulta cualquier análisis tecnocrático simplista.



ESTIMACIONES BASADAS EN REPORTES RECIENTES DE IBM, IDC Y MCKINSEY SOBRE ADOPCIÓN DE INTELIGENCIA ARTIFICIAL EN AMÉRICA LATINA

A su vez, la proximidad con el mercado estadounidense ha resonado con la tradición productiva y mercantil mexicana, contribuyendo a moldear el desarrollo de infraestructura y cultura corporativa en México. Típicamente, las tendencias tecnológicas estadounidenses llegan a México con un retraso de 18 a 36 meses, adaptándose a las condiciones locales.

Pero una preocupación es latente: ¿estamos ante una burbuja impulsada por expectativas desmedidas o frente a un proceso real de consolidación tecnológica? La respuesta solo puede ser especulativa, pues hay intereses más allá de lo económico detrás del desarrollo, si nos enfocamos por lo pronto al lenguaje financiero, veremos que la inversión privada en IA creció 26% en 2025. Empresas como Amazon, Alphabet, Microsoft y Meta han comprometido más de \$360 mil millones en gasto de capital este año, reflejando la magnitud de la apuesta. Al mismo tiempo, 9 de cada 10 organizaciones en EE.UU. planean incrementar su inversión en IA en 2026, mientras que crece la dependencia con la nube y el 88% ya emplea IA en al menos una función empresarial.”

— Fuentes: Stanford HAI 2025 AI Index; IMPLAN analysis; McKinsey & Company; Gartner Survey



La adopción en México no ha seguido el mismo ritmo o la misma lógica que economías más industrializadas, un reporte de *El Economista* indica que el mercado mexicano de IA generó unos US\$16 924.8 millones en ingresos en 2025 contrastando con los 294 mil millones del mercado estadounidense. En gran parte nuestro primer contacto ha sido improvisado antes que estructural: experimentación con modelos generativos se montan sobre datos fragmentados, infraestructuras heredadas y una limitada madurez en gobierno tecnológico.

Las organizaciones que han buscado avanzar más allá del experimento han entendido que la IA no es un componente aislado, sino una capa que despliega condiciones previas. La calidad de datos, capacidad de cómputo, seguridad, conectividad y una arquitectura clara dejaron de ser secundarios y ahora son potencialmente un cuello de botella, produciendo a su vez una depuración de empresas sin los “*minimum requirements*” para disponer de tecnologías emergentes. Lo que vemos así en México, se traduce a que la cuestión relevante no es “qué tan avanzada es la IA” sino “qué podemos hacer con ella”, y las organizaciones que se adentran en la conversación son aquellas que han encontrado casos de uso concretos, medibles y alineados a su realidad operativa.

MENSAJE DEL DIRECTOR EJECUTIVO

Nos permitimos comentar nuestra visión de tres temas impactante e indispensables en la operación diaria de los centros de computo como lo son: La Inteligencia Artificial , La Virtualización de los procesos y la Ciberseguridad, cada uno de ellos con su valor y relevancia estamos seguros que estarán de acuerdo con nosotros en que son indispensables para ofrecer un servicio confiable a nuestros usuarios y una

rentabilidad atractiva para los negocios. Agradecemos a nuestros clientes y prospectos nos den sus observaciones, continuaremos compartiendo temas en los que podemos colaborar con ustedes , y nos ponemos a sus ordenes para profundizar y comentar personalmente con mas detalle al respecto.

Atte. Santiago Gutierrez

Entrando a 2026, la industria mexicana continuará viendo la tendencia subir a nivel mundial -y lo hará aún con cierta cautela-, cuestionando riesgo-beneficio de manera pragmática; posiblemente integrando de manera gradual procesos muy específicos como atención al cliente, análisis de datos, automatización operativa, mantenimiento predictivo y soporte a toma de decisiones. En México no se espera una revolución contundente, sino una adopción diferida, condicionada por infraestructura, talento y visibilidad estratégica. En este contexto, el riesgo para algunas empresas está

en adoptar la IA con lentitud y sin cimientos; las organizaciones que confundan narrativa con inmadurez tecnológica podrían correr riesgo de aislarse en la carrera tecnológica, entre fricciones operativas, costos más apretados y brechas de seguridad impredecibles. Pero podemos pensarlo también de otra manera: el lenguaje como habilidad virtual, la posibilidad de darle voz a los procesos operativos de las organizaciones; en donde la coherencia interna de las mismas sea capaz de expresar sus límites y posibilidades.

VMWARE / BROADCOM : LAS NUEVAS REGLAS DEL JUEGO

Una conversación honesta sobre VMware Cloud Foundation

Jorge Elizondo

Déjame plantearlo así. Si llevas años en TI —como muchos de nosotros— seguramente recuerdas cuándo virtualizar servidores con vSphere dejó de ser una “apuesta” y se volvió una obviedad. No porque fuera moda, sino porque funcionaba: menos fierros, menos consumo eléctrico, menos espacio en el data center y, sobre todo, menos costo operativo.

Hoy estamos en un momento muy parecido, solo que el reto ya no es solo virtualizar servidores. Ahora el reto es cómo operar infraestructura en un mundo híbrido, donde la nube pública promete agilidad, pero también introduce complejidad, costos variables y nuevas preocupaciones de seguridad y soberanía de datos.

Y ahí es donde, con la experiencia acumulada, vale la pena hablar sin hype de VMware Cloud Foundation (VCF).



El problema real que nadie dice en voz alta

Muchos equipos de TI se subieron a la nube pública buscando velocidad. Lo lograron... hasta que llegaron las facturas. Diversos análisis de la industria —incluyendo reportes de Gartner e IDC— coinciden en algo incómodo: no todas las cargas de trabajo son buenas candidatas para la nube pública permanente, especialmente aquellas estables, críticas o reguladas.

IDC, en su estudio Business Value of VMware Cloud Foundation, entrevistó a organizaciones reales y encontró algo interesante: muchas de ellas no estaban “regresando” del cloud, sino re-equilibrando. Buscaban una plataforma que les diera la experiencia de nube, pero con el control financiero y operativo del data center.

Los números que valen la pena mirar

Aquí es donde conviene dejar opiniones y ver datos. IDC —una firma independiente— documentó que las organizaciones que adoptaron VCF obtuvieron, en promedio:

- 564 % de retorno de inversión en tres años
- Recuperación de la inversión en solo 10 meses
- 34 % de reducción en costos de infraestructura
- 42 % de reducción en costos operativos totales

No son cifras menores. Y lo más relevante no es el ROI en sí, sino de dónde viene: menos tiempo en tareas manuales, menos herramientas desconectadas, menos incidentes no planeados.

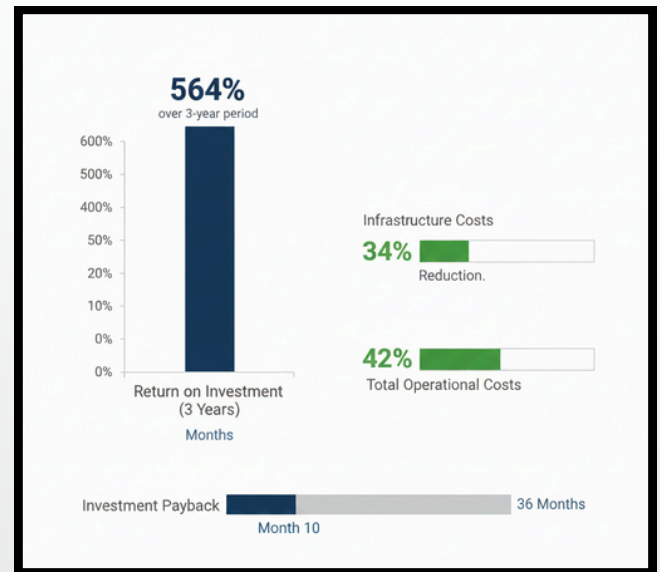
El valor que no siempre aparece en el presupuesto

Uno de los datos que más me llama la atención del estudio es este:

los equipos de infraestructura fueron 53 % más eficientes, y los de seguridad 52 % más eficientes.

Traducido a la vida real:

menos noches apagando incendios, menos configuraciones repetitivas, menos dependencia de “ese ingeniero que sí sabe cómo funciona”. VCF automatiza desde el despliegue hasta el ciclo de vida completo de la infraestructura, y eso libera tiempo humano, que hoy es uno de los recursos más escasos en TI.



Además, el aprovisionamiento de nuevas máquinas virtuales fue 61 % más rápido. Eso no es solo comodidad técnica; es velocidad de negocio

Resiliencia: cuando las cosas fallan (porque siempre fallan)

IDC también documentó algo clave: 98 % menos tiempo de inactividad no planificada.

Este dato suele pasar desapercibido, pero es crítico. En sectores como salud, manufactura o servicios financieros, la resiliencia no es un “nice to have”; es supervivencia.

Varias organizaciones entrevistadas mencionaron que incidentes que antes habrían sido críticos ahora son eventos casi invisibles para el negocio. Esa tranquilidad operativa tiene un valor enorme, aunque no siempre aparezca como una línea directa en el Excel.

¿Esto significa renunciar a la nube pública?

No. Y aquí es importante ser claros. VCF no va en contra de la nube pública; va en contra de usarla sin control.

La realidad que muchos estamos viendo es esta:

- cargas dinámicas o estacionales → nube pública
- cargas estables, reguladas o críticas → nube privada moderna

VCF permite operar ambos mundos con consistencia, usando las mismas herramientas, políticas de seguridad y modelos operativos. Y eso reduce fricción, errores y costos ocultos, como el famoso cloud sprawl.

Soberanía y seguridad: temas que ya no son opcionales

Otro punto que cada año pesa más en las decisiones de arquitectura es la soberanía de los datos. Regulaciones, auditorías y riesgos legales obligan a muchas organizaciones a saber exactamente dónde viven sus datos y quién los controla.

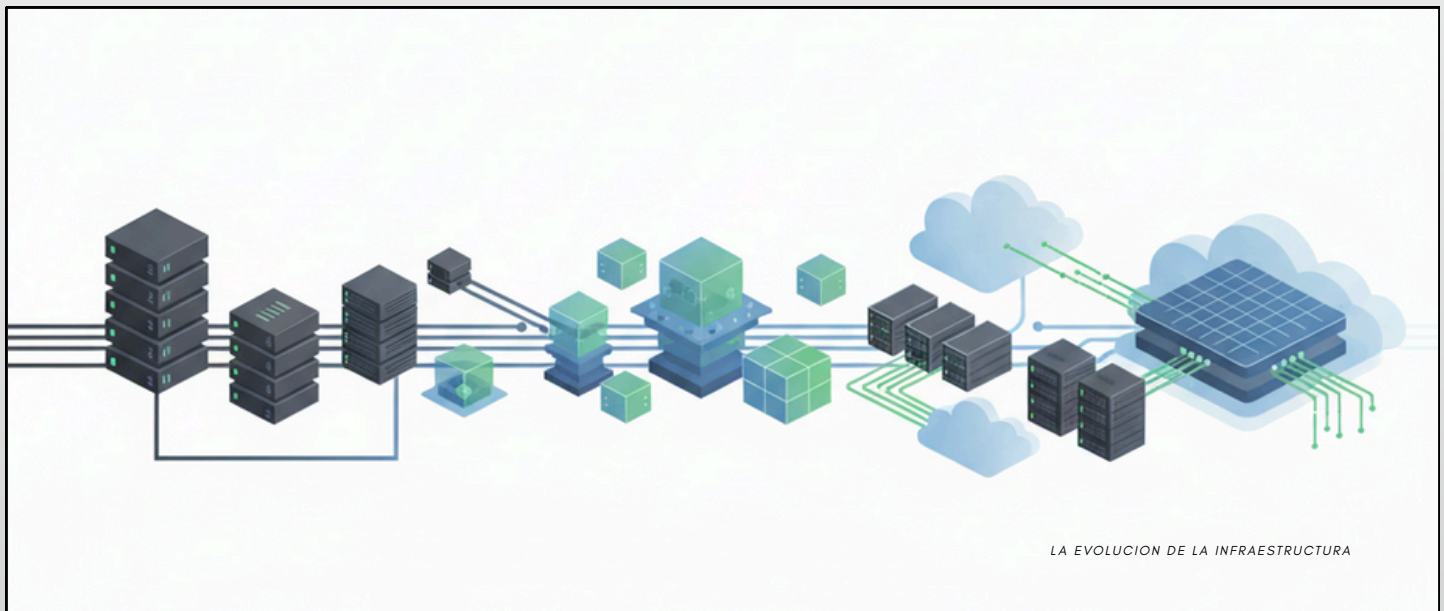
Al integrar seguridad desde la infraestructura —no como un parche posterior— VCF reduce la dependencia de múltiples herramientas aisladas.

Menos piezas, menos huecos, menos deuda técnica. Y eso, otra vez, se traduce en operación más simple y segura.

La analogía inevitable con vSphere

Si algo me resulta familiar de todo esto es la sensación de déjà vu. Hace años, vSphere no se vendía como “revolución”; se adoptó porque hacía la vida más fácil y más barata. Redujo la huella física de servidores, simplificó operaciones y bajó el costo total de la infraestructura.

VCF sigue exactamente esa misma lógica, pero aplicada al mundo híbrido actual. No reinventa la infraestructura; la ordena, la automatiza y la hace predecible.



Mi recomendación honesta es esta:

si tu organización ya confió en VMware para consolidar, virtualizar y estabilizar su infraestructura durante años, VCF no es un salto al vacío, es una evolución natural. No se trata de perseguir tendencias, sino de recuperar control, optimizar costos y darle a TI la agilidad que el negocio exige, sin perder seguridad ni gobernanza. Y si algo nos ha enseñado la experiencia en TI es que las plataformas que realmente valen la pena no son las más ruidosas, sino las que funcionan bien durante muchos años.



La ciberseguridad: el seguro digital que toda empresa necesita

Adrian Guel

En un entorno empresarial cada vez más digital, la tecnología se ha convertido en el motor principal de la operación diaria. Sin embargo, junto con las oportunidades también han crecido los riesgos. Ataques informáticos, robo de información y fraudes digitales ya no son escenarios lejanos, sino amenazas reales para empresas de todos los tamaños.

En este contexto, la ciberseguridad debe entenderse como lo que realmente es: el seguro digital del negocio, tan indispensable como un seguro de autos.

Invertir para no usarla: una buena decisión

Cuando una empresa contrata un seguro vehicular, no lo hace pensando en usarlo de inmediato. Al contrario, espera nunca necesitarlo. Aun así, nadie duda de su importancia, porque el día que ocurre un accidente, el seguro evita pérdidas económicas severas y permite una recuperación más rápida. La ciberseguridad funciona bajo el mismo principio. Contar con soluciones de protección, monitoreo, respaldo de información y controles de acceso no significa que la empresa espere sufrir un ataque, sino que está preparada para enfrentarlo si llega a ocurrir.

Invertir en ciberseguridad y no tener que utilizarla es, en realidad, el mejor escenario posible.

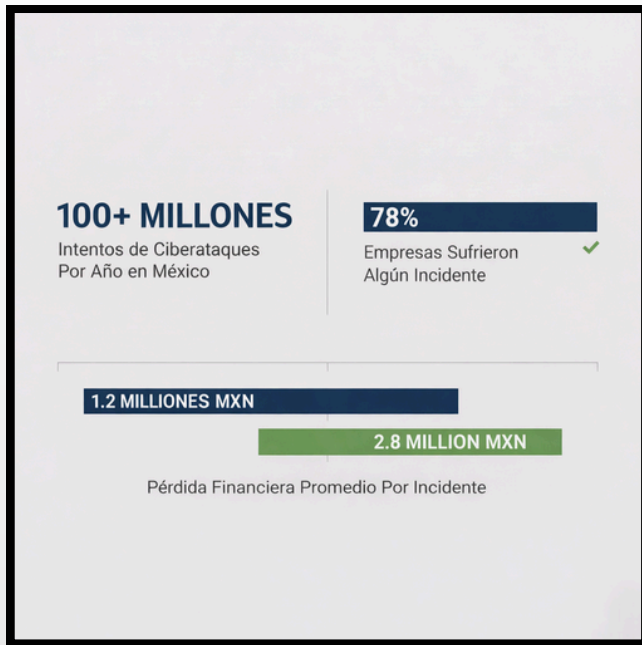
El riesgo de operar sin protección

Muchas organizaciones postergan la inversión en ciberseguridad porque “nunca ha pasado nada”. Sin embargo, cuando ocurre un incidente, las consecuencias suelen ser graves:

- Interrupción de operaciones críticas
- Pérdida o secuestro de información
- Afectación a la reputación de la empresa
- Sanciones por incumplimiento normativo
- Pérdida de confianza de clientes y socios

En términos simples, es como sufrir un accidente automovilístico sin seguro: el impacto financiero llega de golpe y puede comprometer seriamente la estabilidad del negocio.





Conclusión

La ciberseguridad es ese respaldo silencioso que idealmente nunca se nota, pero que resulta indispensable cuando ocurre un incidente.

Invertir en ella es una decisión responsable y estratégica: es mejor contar con protección y no necesitarla, que enfrentar un ataque sin estar preparado.

En un mundo digital en constante evolución, proteger la información y los sistemas es proteger el futuro del negocio.

Prevenir siempre será más rentable que reaccionar

Una estrategia de ciberseguridad bien implementada permite a las empresas:

- Reducir la probabilidad de ataques exitosos
- Minimizar el impacto de incidentes de seguridad
- Recuperar operaciones en menor tiempo
- Proteger la información y la continuidad del negocio

Hoy en día, la pregunta ya no es si una empresa será objetivo de un ataque, sino qué tan preparada está para responder.

La ciberseguridad como parte del negocio

Las organizaciones más competitivas entienden que la ciberseguridad no es un gasto tecnológico, sino una inversión en continuidad, confianza y reputación. Así como nadie pondría en circulación un vehículo sin seguro, ninguna empresa debería operar sin una estrategia sólida de protección digital.