¿SU EMPRESA DEPENDE DE INSTALACIONES QUE SON OBJETIVOS DE GUERRA?

¿Lo Sabe su Aseguradora?



LA SEÑAL DE ALARMA YA NO ES HIPOTETICA: El Precedente Real y la Escalada Documentada

> **HECHO VERIFICADO (junio 2026):** **Irán atacó físicamente tres centros de datos de Amazon Web Services en los Emiratos Árabes Unidos y Baréin, y un centro de Oracle en Dubái. Irán declaró formalmente a 18 grandes empresas tecnológicas, entre ellas AWS, Microsoft, Meta, Google y Oracle, como «objetivos militares legítimos». Fuente: Modern War Institute, West Point, 9 de junio de 2026.**

Cuando comencé a escribir este artículo, hace ya varias semanas, la mayor parte de los directivos occidentales habría clasificado el escenario de un ataque militar a centros de datos como una especulación académica. Hoy ya no es especulación. Es un hecho consumado. Y lo que ocurrió en el Golfo Pérsico en junio de 2026 no es un incidente aislado: ***es la primera manifestación pública de una doctrina militar emergente que convierte la infraestructura digital en objetivo de guerra.***
*Me atrevo a afirmar, con más de cuarenta años de experiencia en el asesoramiento de riesgos empresariales, que este evento es el mayor "****smoke signal****" que he visto en mi carrera profesional.* ***Las empresas del mundo occidental, sus directivos, sus gerentes de riesgos y sus aseguradoras no pueden permitirse ignorar lo que está sucediendo.***

La Escalada China: Datos, No Conjeturas

El presupuesto de defensa de China para 2026 asciende a **278.000 millones de dólares**, un incremento del **7%**. En los documentos oficiales del Partido Comunista Chino, **la fórmula diplomática de "oponerse a la independencia de Taiwán" ha sido sustituida por "aplastar la independencia"**. Un cambio de palabra que, en el lenguaje diplomático, equivale a una declaración de intenciones.

El "Council on Foreign Relations" documenta que el equilibrio militar en el Estrecho de Taiwán se ha "deteriorado significativamente a favor de China". El Stimson Center y Foreign Affairs (2026) advierten de una "tormenta perfecta" que **eleva la probabilidad de conflicto armado al 25-35% en la próxima década.**

El CSIS publicó en mayo de 2026 que, en ejercicios de simulación, EE. UU. agotaba sus reservas de misiles de largo alcance en la primera
semana de conflicto. La producción de esos misiles requiere 3-4 años. "Brookings Institution" advierte: **un conflicto sobre Taiwán sería devastador, con potencial de escalada nuclear y un coste económico global de decenas de billones de dólares.**

Guerra en el Espacio: La dimensión Olvidada

China realizó 93 lanzamientos espaciales en 2025, acumulando 1.353 satélites. En el desfile militar de septiembre de 2025 desfiló el sistema HQ-29, arma antisatélite de nueva generación. La US Space Force ha documentado satélites robots chinos capaces de capturar y destruir satélites estadounidenses, y armas de microondas para inutilizar Starlink, de Elon Musk.

Los Centros de Datos Submarinos: China se Blinda

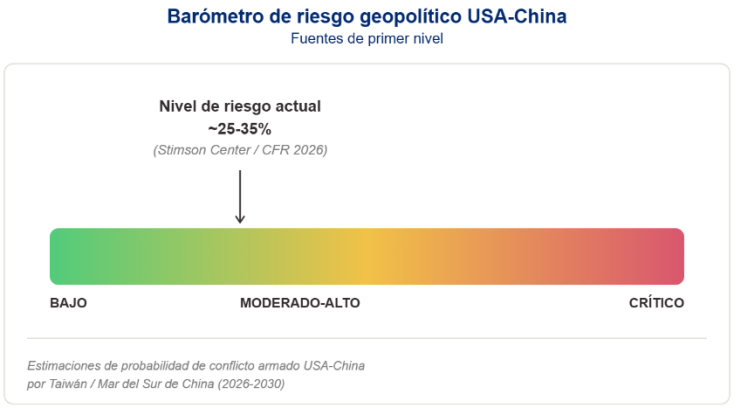
En 2023, China inauguró el primer centro de datos comercial sumergido frente a Hainan. En 2025, el proyecto de Shanghái, alimentado por energía eólica offshore, entró en funcionamiento. Esta arquitectura subacuática es invulnerable a ataques convencionales y ya es política de Estado. **Mientras China protege su infraestructura bajo el mar, la mayoría de los centros de datos occidentales permanecen en superficie, expuestos.**
El "West Point MWI" señala que los nuevos centros de datos de IA en el sur de Taiwán podrían ser objetivo estratégico para China: no para destruirlos, sino para capturarlos intactos. La infraestructura de IA ya no es solo un activo económico: **es un activo militar.**

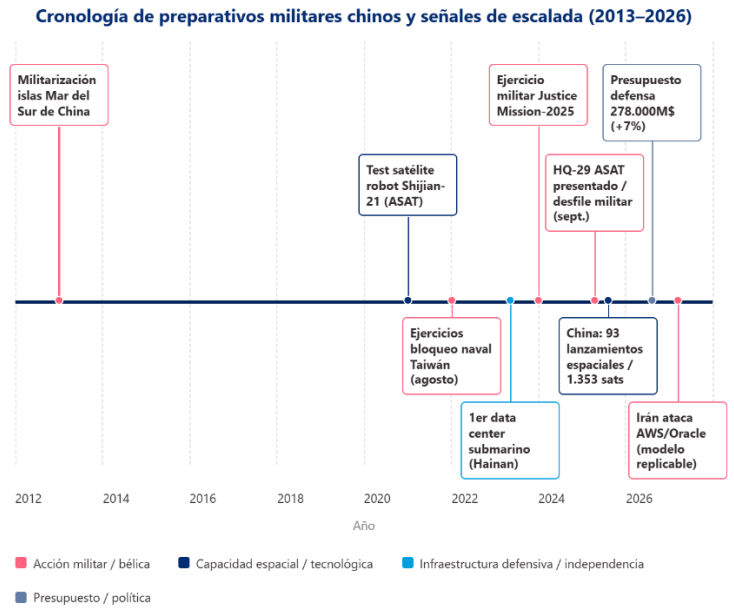
El Mar de China Meridional: militarización Activa

"Defense News" informó en enero de 2026 que China parece decidida a militarizar un nuevo arrecife en el Mar de China Meridional. Los ejercicios navales "Justice Mission 2025" simularon el bloqueo naval completo del Estrecho de Taiwán. Quien controle esas aguas controla los cables submarinos de fibra óptica que transportan más del 95% del tráfico global de internet.

No estamos ante hipótesis académicas. **Estamos ante una escalada militar documentada cuyo objetivo estratégico es la infraestructura digital mundial,** exactamente la misma sobre la que descansa la operación diaria de cualquier empresa occidental. **Los directivos y**

gerentes de riesgo que no actúen en los próximos 18-24 meses estarán incurriendo en una negligencia estratégica grave.





Fuentes: ISW (Marzo 2026) | CFR Global Conflict Tracker | CSIS (mayo 2026) | US Space Force Fact Sheet (Abril 2026) | Modern War Institute West Point (Junio 2026) | Stimson Center / Foreign Affairs 2026

ANATOMIA DE LA NUBE: DONDE VIVE EL CEREBRO DIGITAL

Cuando cualquier directivo de empresa pulsa "enviar" en un correo electrónico, accede a su CRM o ejecuta una videoconferencia, activa una cadena de eventos físicos que pocos imaginan. Ese acto aparentemente inmaterial desencadena el consumo de electricidad equivalente al de un electrodoméstico funcionando durante minutos, el bombeo de varios litros de agua de refrigeración en instalaciones industriales y la activación de miles de servidores físicos que ocupan hectáreas de suelo industrial.

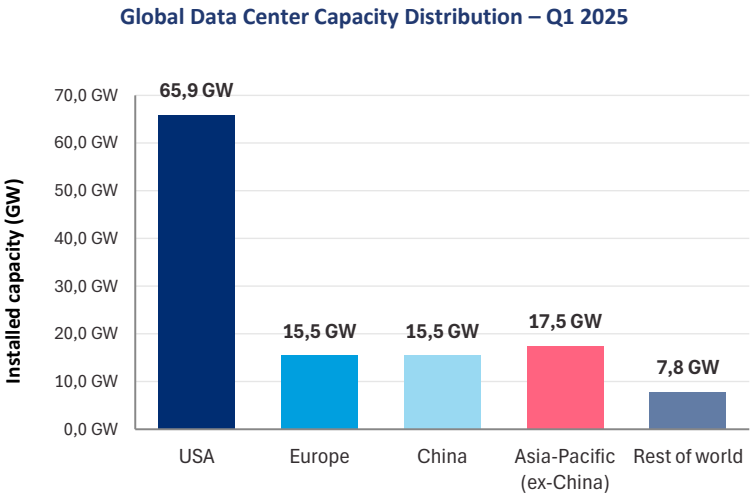
Hablo de los centros de datos de hiperescala: las catedrales industriales del siglo XXI. Y, como cualquier catedral, tienen una ubicación física, consumen recursos y son vulnerables.

El Mapa de la Computación Global, el problema de la energía.

En el primer trimestre de 2025, la capacidad de computación global en hiperescala se distribuía así, según "Synergy Research Group":

- **América del Norte: 39%** de la capacidad global (AWS, Microsoft Azure, Google Cloud, Meta).
- **Europa: 27%**, concentrada en Irlanda, Alemania, Países Bajos y Suecia.
- **Asia-Pacífico: 28%**, con China liderando, seguida de Singapur, Japón y Australia.
- **Resto del mundo: 6%**, con crecimiento acelerado en Oriente Medio y África.

El 60% de toda la capacidad de computación mundial se concentra en apenas 15 áreas metropolitanas. Esta concentración geográfica extrema es en sí misma un riesgo sistémico.



Fuente: Synergy Research Group, Q1 2025

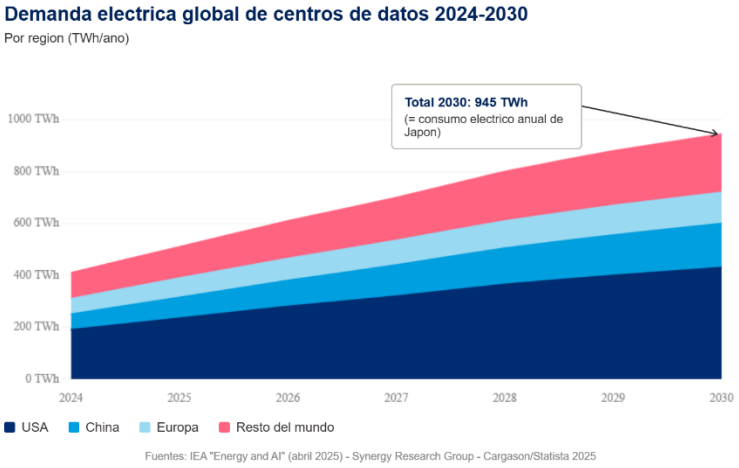
El problema de la energía

En 2024, la demanda global de electricidad de los centros de datos superó los **415 TWh**, según la Agencia Internacional de la Energía.

Goldman Sachs estima que la demanda eléctrica de los centros de datos crecerá un 160% entre 2023 y 2030, impulsada por los modelos de inteligencia artificial. El incremento equivale a la demanda total actual de **Alemania, Francia e Italia combinadas.**

Este crecimiento colisiona con dos realidades: la infraestructura de red eléctrica existente no fue diseñada para absorber este incremento; y la transición energética introduce volatilidades que un gestor de riesgos competente no puede ignorar.

La dependencia energética de la infraestructura digital es ya hoy el primer gran riesgo sistémico de la economía global que carece de cobertura aseguradora adecuada.



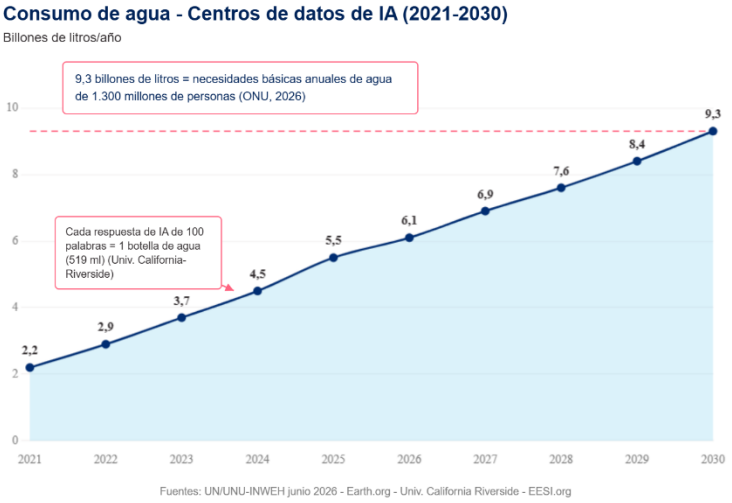
EL TALON DE AQUILES HIDRICO

Los centros de datos modernos utilizan sistemas de refrigeración evaporativa que consumen cantidades industriales de agua. Un estudio de la Universidad de California y UMass (2023) cuantifica que los grandes modelos de lenguaje consumen entre 0,5 y 5 litros de agua por cada conversación de veinte preguntas.

A escala global, el consumo hídrico de la IA superó en 2024 los 700 millones de litros diarios, equivalente al consumo doméstico de una ciudad de dos millones de habitantes. Y **se triplicará antes de 2030, según las proyecciones más conservadoras.**

El problema no es solo cuantitativo: es geográfico. **Los grandes centros de datos se ubican donde hay energía renovable y agua, pero el cambio climático está alterando la disponibilidad hídrica exactamente en esas regiones**. En Virginia, en el centro de Europa y en la costa oeste de EE. UU., **la competencia por el agua entre uso agrícola, residencial e industrial ya es una tensión regulatoria activa.**

El gestor de riesgos que hoy no incluye el estrés hídrico en su mapa de riesgos está omitiendo una variable crítica de continuidad de negocio.



El escenario 2030: lobotomía digital

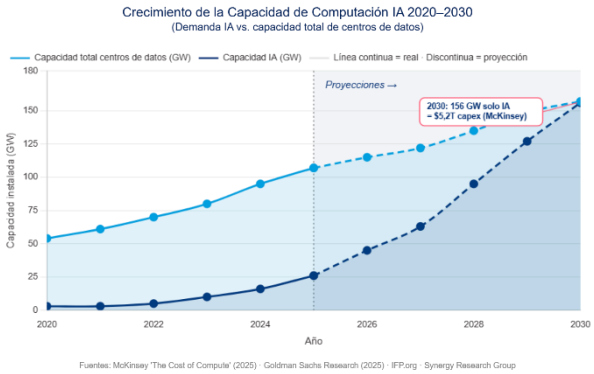
"Epoch AI" documenta que la **capacidad de computación para entrenar modelos de IA se duplica aproximadamente cada seis meses**. Entre 2020 y 2030, el incremento acumulado será de varios órdenes de magnitud. **Estamos en el equivalente digital de la Revolución Industrial.**

La economía digital del mundo occidental depende de una infraestructura física concentrada, energéticamente voraz, hídricamente dependiente y, como acabamos de ver, ya convertida en objetivo militar declarado.

El escenario denominado "lobotomía digital", la incapacitación masiva y simultánea de los centros de datos que sustentan la economía de un país, ya no es ciencia ficción. **Es un riesgo operativo que debe gestionarse con la misma seriedad con la que gestionamos el riesgo de incendio o responsabilidad civil.**

Si el 60% de la capacidad computacional global está en 15 áreas metropolitanas, y la economía occidental depende de esa computación para funcionar en tiempo real, entonces la destrucción o captura de esas instalaciones equivale a una lobotomía económica de la que ningún seguro tradicional puede recuperar a las empresas afectadas.

Ese es el riesgo que hoy no está asegurado. Y ese es el riesgo que la industria aseguradora tiene la obligación profesional y la oportunidad comercial histórica de aprender a cubrir.



LA GRAN BRECHA DE COBERTURA

Cuarenta años en el sector asegurador me han enseñado que los mercados de seguros funcionan bien cuando el riesgo es históricamente conocido, estadísticamente modelizable y contractualmente delimitado. **Los riesgos de la infraestructura digital global no cumplen ninguno de esos tres criterios.**

Lloyd's of London, en sus 'Realistic Disaster Scenarios' de 2023, identificó la interrupción masiva de la nube como uno de los tres escenarios de pérdida sistémica sin precedentes en la historia del seguro, con exposición potencial superior a 15.000 millones de dólares por evento. **Munich Re y Swiss Re coinciden: el mercado actual de ciberseguros cubre fundamentalmente la ciberdelincuencia, pero deja fuera la interrupción física de infraestructura, el daño por conflicto de Estado y la dependencia de terceros proveedores críticos.**

Esta es la brecha estructural que representa la mayor oportunidad comercial para el mercado asegurador en la próxima década.



Matriz de brecha de cobertura aseguradora: riesgos de infraestructura digital vs. coberturas disponibles en el mercado actual.

LO QUE EL MERCADO ASEGURADOR NECESITA CONSTRUIR

La buena noticia es que el mercado asegurador ya dispone de las herramientas conceptuales. Las malas noticias son dos: el ritmo de desarrollo de nuevos productos es muy inferior a la velocidad a la que crece la exposición; y el regulador todavía no ha establecido marcos claros de solvencia y capital para estas coberturas.

Coberturas paramétricas para infraestructura crítica

El seguro paramétrico, en el que el pago se activa automáticamente al verificarse un parámetro objetivo sin necesidad de acreditar

pérdida contable, es la arquitectura de cobertura más adecuada para los riesgos de infraestructura digital. Su principal ventaja: velocidad. Cuando una empresa pierde acceso a sus sistemas críticos, necesita liquidez inmediata, no semanas de peritos.

Me atrevo a predecir que los primeros productos paramétricos específicamente diseñados para dependencia de centros de datos estarán en el mercado antes de 2027. El camino técnico ya existe; falta voluntad comercial y claridad regulatoria.

Productos de dependencia tecnológica no maliciosa

La mayoría de las pólizas de seguro excluyen explícitamente las pérdidas derivadas de la interrupción de servicios de terceros cuando no es consecuencia de un acto malicioso. Calor extremo, sequía, fallos eléctricos, errores de configuración masivos: estos escenarios reales quedan fuera de cobertura.

El producto que el mercado necesita cubre: la interrupción no maliciosa de proveedores cloud críticos; el impacto en cuenta de resultados de la indisponibilidad prolongada; y los costes de contingencia y recuperación. Requiere actuaría especializada, datos de SLA y triggers bien definidos. Todo existe. Solo falta ensamblarlo.

seguro paramétrico de conflicto para activos digitales

El producto más innovador y de mayor potencial: cobertura específicamente diseñada para proteger los ingresos de empresas cuya actividad depende de infraestructura digital en zonas de riesgo geopolítico elevado. El precedente iraní de junio de 2026 ha creado, de facto, un nuevo mercado de riesgo que todavía no tiene producto asegurador correspondiente.

CONCLUSION: EL MOMENTO DE ACTUAR ES AHORA

A lo largo de cuarenta años en el asesoramiento en riesgos y seguros, he visto surgir nuevos mercados de cobertura cada vez que una amenaza emergente alcanzaba masa crítica de conciencia. La cobertura medioambiental en los noventa. El ciberseguro en la primera década del siglo. El paramétrico climático en los últimos cinco años.

Estamos en el umbral de ese momento para los riesgos de infraestructura digital. La confluencia de cuatro factores; **crecimiento exponencial de la dependencia computacional, vulnerabilidad hídrica y energética, conversión de los centros de datos en objetivos militares, y vacío de cobertura aseguradora**, crea las condiciones para que el mercado asegurador construya el producto de la próxima década.

✓ ¿Saben los directivos que leen estas líneas de qué instalaciones físicas depende la operación digital de su empresa?
✓ ¿Conocen los SLA de sus proveedores cloud?
✓ ¿Han cuantificado el impacto en su EBITDA de 48 horas sin acceso a sus sistemas críticos?
✓ ¿Han revisado si su póliza actual cubre ese escenario?

Si la respuesta a alguna de estas preguntas es "no" o "no estoy seguro", tienen un trabajo urgente que hacer. Y **los gerentes de riesgos, brokers y aseguradoras tienen la responsabilidad profesional de guiarlos en ese camino.**

No es alarmismo. Es rigor profesional. El riesgo ya está ahí. La cobertura, todavía no.

Casimiro Rey

Director de Empresas y Negocio Internacional
Miembro del Comité de Dirección
Grupo Galilea S.L. (Söderberg & Partners)