ESCENARIOS DE RIESGO 2026 Y MÁS ALLÁ

Perspectivas Estratégicas para Brasil y América Latina

t-Risk
Método de Avaliação de Riscos

Resumen

Este estudio presenta un análisis integral y prospectivo de los riesgos que moldearán el entorno estratégico de Brasil y América Latina en 2026 y más allá. Construido a partir de la evaluación de 32 informes regionales e internacionales, ejercicios de prospectiva *(foresight)*, análisis de fuentes de riesgo conforme a la ISO 31000 y directrices de la ISO 31050 sobre riesgos emergentes, el documento ofrece una visión integrada sobre las transformaciones que presionan a gobiernos, empresas e instituciones en toda la región.

El informe combina tendencias globales y dinámicas regionales para identificar seis fuentes estructurales de riesgo: 1. geopolítica y comercio; 2. tecnología e inteligencia artificial; 3. crimen organizado y finanzas ilícitas; 4. clima y recursos naturales; 5. infraestructura crítica y operaciones industriales; 6. instituciones y confianza social; y cómo estas interactúan para generar entornos de ruptura, oportunidad o estancamiento. A partir de estas fuerzas, se desarrollaron cuatro escenarios posibles para el futuro próximo, cada uno representando combinaciones distintas de madurez tecnológica y coordinación institucional.

Se analizaron en profundidad sectores clave de la economía latinoamericana, incluyendo industria, energía, agronegocios, finanzas, tecnología, minería, salud, servicios urbanos y sector público. También se desarrolló un radar regional de señales anticipatorias, integrando riesgos climáticos, digitales, criminales y económicos, para apoyar procesos continuos de monitoreo y decisión estratégica.

En un entorno marcado por la interdependencia, la volatilidad y las presiones simultáneas, este estudio ofrece no solo una lectura crítica del presente, sino un conjunto de caminos posibles para fortalecer la resiliencia regional. El objetivo es apoyar a los tomadores de decisiones públicos y privados en la construcción de estrategias más adaptativas, inteligentes y alineadas con las transformaciones profundas que definirán la próxima década.

Abstract

This study presents a comprehensive and forward-looking analysis of the risks that will shape the strategic environment of Brazil and Latin America in 2026 and beyond. Built upon the evaluation of 32 regional and international reports, foresight exercises, the analysis of risk sources aligned with ISO 31000, and the ISO 31050 guidelines on emerging risks, the document offers an integrated perspective on the transformations placing pressure on governments, companies, and institutions across the region.

The report brings together global trends and regional dynamics to identify six structural sources of risk – 1. geopolitics and trade; 2. technology and artificial intelligence; 3. organized crime and illicit finance; 4. climate and natural resources; 5. critical infrastructure and industrial operations; 6. institutions and social trust – and examines how they interact to generate environments of disruption, opportunity, or stagnation. Based on these forces, four possible scenarios for the near future were developed, each representing distinct combinations of technological maturity and institutional coordination.

Key sectors of the Latin American economy were analyzed in depth, including industry, energy, agribusiness, finance, technology, mining, healthcare, urban services, and the public sector. A regional early-warning radar was also developed, integrating climatic, digital, criminal, and economic risks to support continuous monitoring and strategic decision-making.

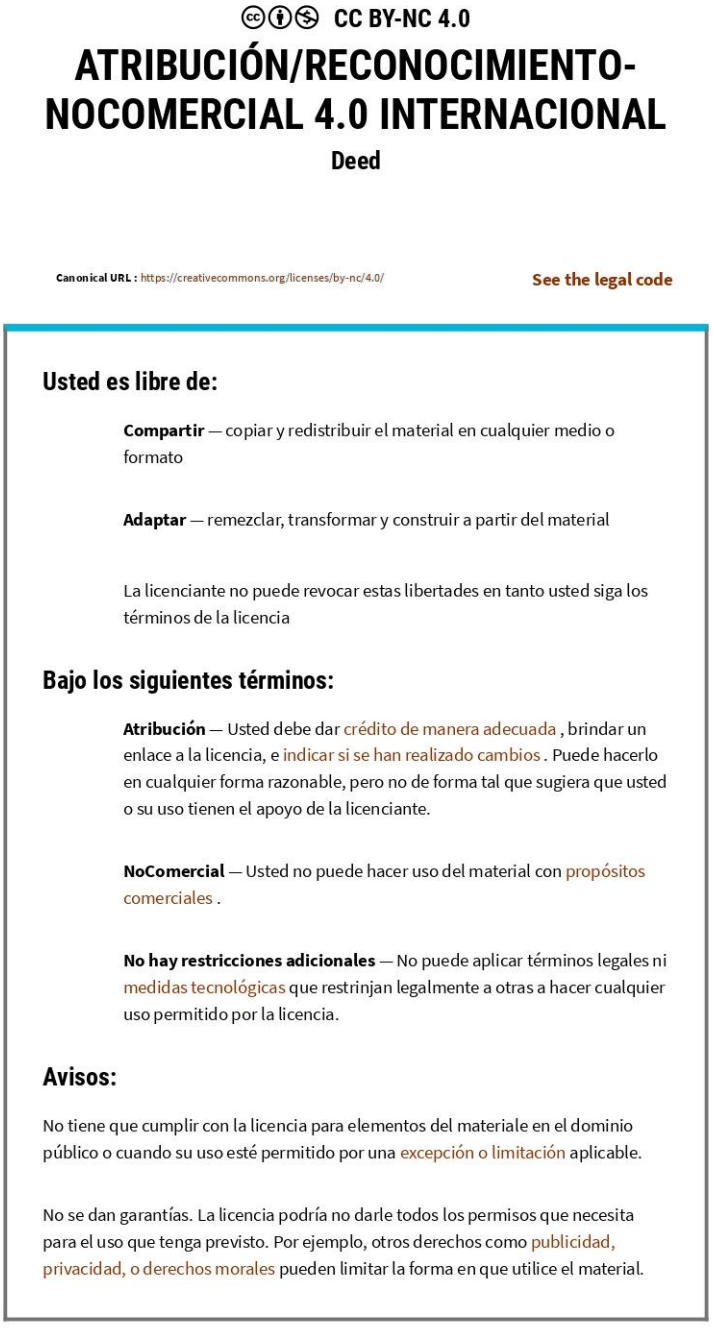
In an environment marked by interdependence, volatility, and simultaneous pressures, this study provides not only a critical reading of the present but also a set of possible pathways to strengthen regional resilience. Its goal is to support public- and private-sector decision-makers in building more adaptive, intelligence-driven strategies aligned with the profound transformations that will define the next decade.

Palabras-Clave

Riesgos emergentes; Escenarios prospectivos; Resiliencia organizacional; Seguridad convergente e integrada; Gobernanza institucional; Inteligencia artificial y tecnología; Delincuencia organizada transnacional; Infraestructuras críticas; Clima y fenómenos extremos; Indicadores de alerta temprana *(Early Warning Indicators).*

Licencia de Distribución

Haga clic en la imagen a continuación para acceder.



CC BY-NC 4.0

ATRIBUCIÓN/RECONOCIMIENTO-NOCOMERCIAL 4.0 INTERNACIONAL

Deed

Canonical URL : https://creativecommons.org/licenses/by-nc/4.0/ **See the legal code**

Usted es libre de:

Compartir — copiar y redistribuir el material en cualquier medio o formato

Adaptar — remezclar, transformar y construir a partir del material

La licenciante no puede revocar estas libertades en tanto usted siga los términos de la licencia

Bajo los siguientes términos:

Atribución — Usted debe dar crédito de manera adecuada , brindar un enlace a la licencia, e indicar si se han realizado cambios . Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo de la licenciante.

NoComercial — Usted no puede hacer uso del material con propósitos comerciales .

No hay restricciones adicionales — No puede aplicar términos legales ni medidas tecnológicas que restrinjan legalmente a otras a hacer cualquier uso permitido por la licencia.

Avisos:

No tiene que cumplir con la licencia para elementos del materiale en el dominio público o cuando su uso esté permitido por una excepción o limitación aplicable.

No se dan garantías. La licencia podría no darle todos los permisos que necesita para el uso que tenga previsto. Por ejemplo, otros derechos como publicidad, privacidad, o derechos morales pueden limitar la forma en que utilice el material.

Índice

Prefacio del CEO

Tácito Augusto Silva Leite
Plataforma t-Risk

Hay momentos en que la historia se acelera. En los que las transformaciones tecnológicas, climáticas, sociales y geopolíticas dejan de ser movimientos aislados y pasan a formar un único pulso, capaz de redefinir el rumbo de naciones, organizaciones e individuos. Atravesamos exactamente ese tipo de momento.

En el estudio t-Risk de 2025, buscamos comprender esta nueva dinámica y mostrar cómo los riesgos — cuando se leen con profundidad — revelan no solo amenazas, sino caminos posibles. Un año después, avanzamos hacia un escenario aún más desafiante, en el cual la incertidumbre no es la excepción: es el propio entorno estratégico. Y es precisamente por eso que mirar solo al presente ya no basta. Es necesario ver lo que puede emerger.

El informe de 2026 nace de ese espíritu. Reconoce que América Latina carga vulnerabilidades históricas, pero también posee capacidades extraordinarias: energía limpia, diversidad productiva, talento humano y una resiliencia que atraviesa décadas. El desafío, ahora, es transformar estas fuerzas en ventaja estratégica en un mundo donde los riesgos se combinan y se multiplican.

Al identificar seis fuentes estructurales de riesgo y construir cuatro escenarios plausibles para 2026, este estudio no pretende anticipar el futuro, sino ampliar nuestra capacidad de dialogar con él. La interdisciplinariedad — uniendo tecnología, clima, economía, seguridad y gobernanza — sirve como punto de apoyo para comprender cómo estas fuerzas se entrelazan y moldean elecciones fundamentales para gobiernos, empresas e instituciones.

Más que respuestas prefabricadas, este informe ofrece perspectivas. Más que previsiones, ofrece dirección. Invita a cada liderazgo a desarrollar el coraje de actuar en un mundo incierto, a cultivar la curiosidad de cuestionar modelos establecidos y a construir, con responsabilidad y visión, las bases de un futuro más seguro y sostenible para nuestra región.

Creo profundamente que el riesgo, cuando se comprende bien, es una forma de inteligencia. Es la capacidad de percibir lo que aún no ha sucedido, de preparar el terreno para lo que puede venir, y de construir resiliencia no como defensa, sino como ventaja competitiva. Este estudio es una contribución a esa jornada.

Que inspire conversaciones profundas, decisiones responsables y colaboración genuina entre sectores y fronteras. América Latina tiene, ante sí, desafíos inmensos, pero también una rara oportunidad de reinventar su lugar en el mundo. Y eso comienza con la calidad de las elecciones que hacemos hoy.

Mensaje del CTO

Carlos Eduardo Espesani Gonser
Plataforma t-Risk

La migración del crimen y de los fraudes al entorno digital se ha vuelto evidente. Lo que antes exigía presencia física — asaltos, intercepciones, sabotajes directos — hoy ocurre silenciosamente por medio de intrusiones, manipulación de identidades, ataques automatizados y explotación de fallas en sistemas críticos. Este movimiento no es aislado: se conecta a un escenario más amplio en el que tecnología, gobernanza institucional, operaciones industriales y estructuras financieras pasaron a funcionar de forma interdependiente, ampliando el impacto de cualquier falla. Es exactamente ese punto de convergencia el que el informe pone de relieve al mapear riesgos sistémicos y escenarios posibles para los próximos años.

Desde el punto de vista tecnológico, la línea entre seguridad cibernética, protección de datos, continuidad de negocios e integridad operativa prácticamente ha desaparecido. La Inteligencia Artificial aceleró este cambio. Ella potencializa los ataques, pero también es uno de los pocos recursos capaces de procesar señales débiles, correlacionar eventos y ofrecer respuestas en un entorno en el que la velocidad y el volumen importan más que nunca. La madurez en IA — tanto en el uso como en la gobernanza — se ha convertido en un diferencial estratégico real, separando a las organizaciones preparadas de aquellas expuestas.

El informe muestra que los riesgos digitales ya no pueden ser tratados como un dominio aislado dentro de las empresas. La superficie de ataque ahora incluye cadenas logísticas, infraestructuras industriales, flujos financieros y mecanismos de toma de decisiones. Los ataques digitales generan impactos físicos; las fragilidades institucionales amplían las vulnerabilidades tecnológicas; y la falta de integración entre áreas reduce la capacidad de respuesta. Este es el punto central: el riesgo tecnológico es riesgo organizacional.

Bajo la óptica de la tecnología, la contribución del estudio radica en ofrecer un marco que ayuda a los líderes a entender cómo estos elementos se conectan, cómo ha evolucionado la criminalidad y cómo la gobernanza de IA, la resiliencia de infraestructuras críticas y la coordinación institucional determinan el grado de exposición. No se trata de previsiones abstractas, sino de comprender un escenario operativo en el que interrupciones, ataques y fraudes dejaron de ser excepciones y se convirtieron en parte del cotidiano corporativo.

Para los próximos años, la ventaja estará con quien adopte modelos integrados de seguridad, inteligencia de riesgo y automatización. Quien no lo haga tiende a operar a oscuras — y en un entorno adversarial como el descrito en este estudio, eso no es una opción.

Mensaje de la CLO

Taís Fernandes Duarte
Plataforma t-Risk

El análisis prospectivo de las seis fuentes estructurales de riesgo, especialmente aquella relacionada con la erosión institucional y la confianza social, revela que Brasil ingresa al ciclo 2026–2030 bajo una fuerte presión para fortalecer sus sistemas de gobernanza. La convergencia entre desinformación, hiperpolarización, fragilidad estatal y expansión del crimen organizado desafía el propio centro de gravedad del Estado de Derecho. En este contexto, instrumentos como la Ley de Software, el Marco Civil de Internet, la LGPD, la Ley Anticorrupción, SOX, FCPA, ISO 37001, ISO 19600, ISO 31000, ISO 31050 y el futuro Marco Legal de la IA no pueden ser interpretados solo como actualizaciones técnicas, sino como parte de un pilar institucional indispensable para la resiliencia nacional. El problema brasileño no reside en la ausencia de normas, sino en la falta de alineación entre instituciones, prácticas corporativas, infraestructura regulatoria y las dinámicas reales de los riesgos contemporáneos, que ya no son lineales ni compartimentables.

El estudio demuestra que Brasil enfrentará en los próximos años tensiones digitales amplificadas, desorden informativo, instrumentalización de la inteligencia artificial por grupos criminales, fragilidad de la autoridad pública, aumento de la judicialización y baja coordinación estatal frente a riesgos multisectoriales.

Paralelamente, Brasil posee uno de los marcos normativos más avanzados de América Latina en protección de datos y gobernanza digital, pero aún fragmentado. El Marco Civil de Internet no responde adecuadamente a los riesgos de la manipulación algorítmica y del colapso informativo; la LGPD se concentra en el dato personal, y no en los riesgos sistémicos; la Ley de Software permanece desactualizada frente a modelos fundacionales e IA generativa. El país también adhirió a estándares robustos de integridad, como la Ley Anticorrupción, SOX, FCPA, ISO 37001 e ISO 19600, pero la expansión del crimen organizado y de las redes ilícitas transnacionales exige ahora un nuevo nivel de diligencia algorítmica y responsabilidad ampliada por fallas digitales previsibles.

El Proyecto de Ley (PL) 2.338/2023, que debe instituir el Marco Legal de la IA, es un avance al definir principios y categorías de riesgo, pero permanece insuficiente para enfrentar la dimensión sistémica de los riesgos tecnológicos que emergen en el estudio. Para que cumpla su función estratégica, la IA debe ser reconocida como infraestructura crítica, debiendo integrar coordinación regulatoria obligatoria entre la ANPD, el SIA, el Banco Central, agencias reguladoras y organismos de seguridad. Las Evaluaciones Preliminares de Riesgo y las Evaluaciones de Impacto Algorítmico deben transformarse en monitoreo continuo, y no en meros informes estáticos. Además, el marco regulatorio debe incorporar directrices de la COP30, de la LGPD, del derecho de la competencia y de las normas climáticas, reconociendo que la IA es simultáneamente vector de mitigación y ampliación de los riesgos climáticos y sociales.

Al confrontar la realidad jurídica brasileña con la de América Latina, se hace evidente que compartimos un mismo patrón: marcos formales avanzados conviven con instituciones frágiles, selectividad en la aplicación de las normas, volatilidad regulatoria y déficits de efectividad. Brasil posee una densidad normativa superior, pero sufre con la erosión de la confianza, la judicialización excesiva y la percepción social de impunidad selectiva, lo que compromete la legitimidad del sistema jurídico como instrumento de estabilidad y desarrollo. La próxima década pondrá a prueba la capacidad del país —y de la región— de transformar el Derecho en infraestructura de resiliencia. Esto exige abandonar la visión de que la sofisticación normativa es suficiente y construir una convergencia jurídica orientada al riesgo, capaz de apoyar decisiones públicas y privadas frente a las profundas transformaciones climáticas, tecnológicas e institucionales que moldearán el futuro. Si Brasil y América Latina son capaces de alinear el Derecho a la dinámica real de los riesgos emergentes, el sistema jurídico dejará de ser solo un reflejo de las crisis para convertirse en un vector activo de estabilidad y confianza.

Sobre la Plataforma t-Risk

La **Plataforma t-Risk** es una solución SaaS disponible desde 2015, diseñada para transformar la **gestión de riesgos en las organizaciones**. Combina innovación tecnológica con las mejores prácticas normativas globales, especialmente las directrices de las **normas ISO 31000, ISO 31050 y 31010.** Totalmente alineada con los estándares internacionales, t-Risk ofrece un **enfoque analítico y práctico**, ayudando a las empresas en todas las etapas de la gestión de riesgos corporativos: **identificación, análisis, evaluación, priorización y tratamiento**. Disponible en portugués, español e inglés, la plataforma **aumenta hasta en un 80% la productividad del proceso de gestión de riesgos**, entregando eficiencia y precisión.

Con funcionalidades avanzadas, t-Risk integra **inteligencia artificial** y ofrece módulos robustos, como **GRC** (Gestión de Riesgos Corporativos), **APR** (Análisis Preliminar de Riesgos), **MBC** *(Módulo de Background Check)*, **MAM** (Módulo de Evaluación de Madurez en Gestión de Riesgos) y **OEA** (Operador Económico Autorizado), **AVSEC** (Gestión de Riesgos en la Aviación Civil), además de un **Panel de Indicadores** (**BI**) y una **App Móvil**. El **módulo 5W2H** permite un seguimiento detallado de proyectos, tareas y controles, con correos electrónicos automáticos, garantizando que los riesgos permanezcan dentro del apetito de riesgo de la organización.

Además de **fortalecer el cumplimiento *(compliance)*** y optimizar procesos, t-Risk capacita a sus clientes para transformar desafíos en oportunidades, ofreciendo ***insights*** **valiosos para decisiones estratégicas**. Ya sea para fortalecer la resiliencia organizacional o impulsar el crecimiento sostenible, t-Risk es **una aliada indispensable para enfrentar un escenario de riesgos** cada vez más dinámico y complejo.

Descubra cómo t-Risk puede revolucionar la gestión de riesgos en su organización. Explore el poder de nuestras soluciones y **fortalezca su estrategia de gestión de riesgos con una herramienta que va más allá de la tecnología**: una verdadera socia en su jornada de transformación.

Resumen Ejecutivo – Contexto General

El año 2026 marca un punto de inflexión para la gestión de riesgos corporativos en América Latina. La combinación entre volatilidad geopolítica, aceleración tecnológica, presiones climáticas extremas y la sofisticación del crimen organizado transnacional inaugura un entorno de riesgos convergentes, en el cual lo físico, lo digital y lo institucional operan en interdependencia creciente.

Desarrollado a partir del análisis comparativo de **32 informes internacionales, regionales y corporativos**, este estudio ofrece una lectura integrada de las fuerzas que moldearán el entorno de riesgos en 2026. El enfoque metodológico sigue las directrices de las normas **ISO 31000, ISO 31050 e ISO 31010**, incorporando prácticas de *foresight, horizon scanning* y construcción de escenarios cualitativos para apoyar decisiones estratégicas en entornos de alta complejidad.

El objetivo central es proporcionar un marco robusto para que organizaciones públicas y privadas anticipen tendencias, identifiquen vulnerabilidades y oportunidades, y fortalezcan su resiliencia institucional en un período marcado por rápidas transformaciones estructurales.

Síntesis Metodológica

El estudio combina tres pilares metodológicos complementarios:

1. **Análisis convergente de 32 fuentes de referencia,** incluyendo organismos multilaterales, centros de inteligencia, consultoras estratégicas e instituciones corporativas.
2. **Estructuración de seis Fuentes de Riesgo Críticas,** que sintetizan patrones recurrentes observados en las evidencias recolectadas.
3. **Construcción de una matriz de escenarios 2×2,** resultando en cuatro futuros plausibles para 2026, cada uno asociado a planes sectoriales, indicadores de alerta temprana (EWI) e implicaciones estratégicas.

Este enfoque garantiza coherencia entre las dimensiones estratégica, técnica y operativa de la gestión de riesgos, ampliando su utilidad para ejecutivos, consejos, líderes de seguridad, *compliance*, ESG y continuidad de negocios.

Principales Conclusiones

O El conjunto de los análisis revela un **cambio estructural en la naturaleza de los riesgos corporativos.**

El crimen organizado se ha convertido en un sistema híbrido, digital y económicamente infiltrado. Antes concentrado en actividades territoriales y violentas, evolucionó hacia una **configuración híbrida, digitalizada y económicamente infiltrada**, conforme se evidencia en el *Global Organized Crime Index 2025 – Crime at a Crossroads*. América Latina aparece entre las regiones de mayor vulnerabilidad, tanto por la **fragilidad institucional como por la integración de lo ilícito en las cadenas logísticas y financieras formales.**

La convergencia de delitos financieros, ataques cibernéticos y corrupción sistémica redefine la exposición de empresas y gobiernos. El clima se ha convertido en un multiplicador de crisis; el aumento de eventos climáticos extremos — sequías, inundaciones y colapsos energéticos — amplía las interdependencias entre riesgos ambientales, reputacionales y de continuidad operativa.

Estas dinámicas se entrelazan con la **fragmentación regulatoria de la Inteligencia Artificial**, cuyos marcos nacionales avanzan de modo desigual, creando brechas para abusos tecnológicos, manipulación de información y riesgos éticos.

Los Cuatro Escenarios para 2026

Escenario	Descripción-síntesis	Implicaciones clave
Alianza PragTécnica	Cooperación regional pragmática y adopción coordinada de estándares de gobernanza digital e IA.	Estabilidad institucional, interoperabilidad de datos y reducción de incidentes OT.
Redes Sombrías	Fragmentación política, captura del Estado y proliferación de redes criminales transnacionales y digitales.	Colapso de la confianza, aumento de pérdidas financieras y riesgos físicos a ejecutivos e infraestructuras.
Clima de Choques	La integración económica avanza, pero la madurez tecnológica permanece baja, exponiendo sistemas a fallas simultáneas.	Interrupciones críticas, elevación de costos (BI) y presión sobre cadenas de suministro.
Datos con Trabas, Fronteras Abiertas	Gobernanza privada de IA y seguridad de élite compensan la inestabilidad política.	Sectores líderes mantienen operación resiliente; fragmentación regional moderada.

Estos escenarios no compiten entre sí: coexisten en grados distintos en cada país o sector, formando un **mapa dinámico de probabilidades** que orienta la priorización de medidas estratégicas.

Principales Tendencias e Impactos Regionales

1. **Geopolítica y comercio:** Reconfiguración de alianzas y cadenas de suministro, con América Latina reposicionándose como exportadora de energía y datos.
2. **Tecnología e IA:** Expansión de *deepfakes*, fraudes automatizados y uso criminal de IA; al mismo tiempo, aceleración de aplicaciones productivas y del uso de la identidad digital como nuevo perímetro de seguridad.
3. **Crimen Organizado y FinCrime:** Infiltración creciente de organizaciones ilícitas en sectores logísticos, agrícolas y financieros; uso de criptomonedas y *marketplaces* para lavado de dinero.
4. **Clima y Recursos Naturales:** Aumento de eventos extremos afectando la estabilidad de energía y agua, exigiendo gobernanza regional y seguros paramétricos.
5. **Infraestructura Crítica (OT):** Vulnerabilidades en sistemas industriales y costos indirectos predominando en las pérdidas; controles ICS–5 ganan relevancia; vulnerabilidad de servicios basados en satélites e infraestructura espacial.
6. **Instituciones y Confianza:** Declive de los índices de percepción de seguridad y crecimiento de la desinformación, reduciendo la cohesión social y el atractivo de inversiones.

Implicaciones Estratégicas

Los resultados indican que el modelo tradicional de gestión de riesgos, basado en control, conformidad y reacción, se ha vuelto limitado ante la complejidad actual. La nueva frontera exige **resiliencia dinámica, integración entre seguridad física y cibernética y uso ético de la inteligencia artificial** como vector de anticipación. Empresas líderes en la región ya inician la convergencia de sus centros de monitoreo (GSOC) y la adopción de políticas de *zero-trust physical*, ampliando la visibilidad sobre activos críticos y personas.

La gobernanza del futuro requiere **decisión en tiempo real, colaboración regional y transparencia algorítmica.** Las organizaciones que comprendan el riesgo como una forma de inteligencia — y no como un obstáculo — estarán más aptas para capturar oportunidades, preservar valor y sostener el crecimiento.

Cuadro resumen de los principales ejes estructurantes de la gestión de riesgos para 2026:

Eje	Descripción	Resultado Esperado
Estratégico	Integración regional, cooperación público-privada y gobernanza digital.	Estabilidad y competitividad regional.
Tecnológico	IA explicable, protección de datos, resiliencia cibernética y operativa (OT).	Reducción de vulnerabilidades y fraudes.
Ambiental	Gobernanza climática e infraestructura adaptativa.	Continuidad operativa y reducción de pérdidas por interrupción de negocios (BI).
Criminal-Institucional	Combate a la infiltración ilícita y fortalecimiento de marcos legales.	Recuperación de la confianza institucional.
Cultural-Organizacional	Cultura de riesgo y aprendizaje continuo.	Liderazgo adaptativo y respuesta anticipatoria.

Mensaje Final del Resumen Ejecutivo

El entorno de 2026 será moldeado no solo por las tendencias tecnológicas, climáticas y geopolíticas, sino por la capacidad de organizaciones públicas y privadas de transformar la incertidumbre en estrategia y el riesgo en ventaja competitiva.

Este informe ofrece una base estructurada para la anticipación, adaptación y toma de decisiones — elementos esenciales para cualquier institución que quiera prosperar en un escenario marcado por la interdependencia, la velocidad y la complejidad.

En última instancia, los escenarios aquí descritos dependen de la calidad de las decisiones tomadas por personas concretas — gestores, líderes públicos y ciudadanos — cuya formación de valores, visión de mundo y capacidad ética de uso del poder constituyen el primer nivel de gobernanza de riesgos.

01

INTRODUCCIÓN

1.1. Objetivo

El escenario global que se dibuja para 2026 está marcado por una combinación inédita de fuerzas disruptivas, incertidumbres estructurales y transformaciones tecnológicas que remodelan el entorno de negocios, de seguridad y de gobernanza a escala mundial.

América Latina, inserta en este contexto, vive el entrelazamiento de fenómenos políticos, económicos y sociales que influyen directamente en la estabilidad institucional, la competitividad empresarial y la capacidad de respuesta de las organizaciones frente a riesgos cada vez más interdependientes.

El aumento de la complejidad sistémica es impulsado por tres vectores principales: **1. el avance acelerado de la Inteligencia Artificial y de la automatización; 2. la intensificación de las crisis climáticas y de los eventos de interrupción de negocios; 3. y la expansión del crimen organizado en sus dimensiones financiera, digital y corporativa.** Estos vectores producen un nuevo tipo de riesgo, simultáneamente transversal y persistente, que trasciende las fronteras tradicionales entre lo físico, lo cibernético y lo regulatorio, exigiendo un modelo de gestión integrado y orientado por inteligencia.

En este contexto, el presente estudio tiene como objetivo principal ofrecer una visión integral de **los escenarios de riesgo y de las estrategias de adaptación para 2026 en Brasil y América Latina**, con base en un conjunto de treinta y dos informes, estudios, bases de datos internacionales y regionales. El trabajo busca apoyar a empresas, gobiernos e instituciones en el fortalecimiento de sus estructuras de gobernanza, en la anticipación de amenazas y en la construcción de modelos de resiliencia compatibles con las exigencias de un entorno volátil e interconectado.

El enfoque metodológico adoptado en este informe combina técnicas de *foresight, horizon scanning* y análisis de escenarios cualitativos para estructurar la lectura de riesgos emergentes e incertidumbres profundas en América Latina. Los detalles del proceso se encuentran descritos en el ítem a continuación (Metodología y Fuentes) y en el Apéndice A.

A partir de esta estructura metodológica, el estudio identifica las principales **fuentes de riesgo** y los **ejes de tensión** que influirán en la trayectoria económica, ambiental, tecnológica y social de América Latina en 2026 y más allá. El análisis integra dimensiones de gobernanza corporativa, seguridad física y cibernética, continuidad de negocios, sostenibilidad, *compliance* y responsabilidad social, permitiendo visualizar cómo diferentes variables se combinan y producen impactos directos sobre el

desempeño y la reputación organizacional.

Más que anticipar amenazas, este informe busca apoyar el desarrollo de una **cultura de inteligencia de riesgo** basada en el aprendizaje continuo, la adaptación estratégica y la cooperación multisectorial. El propósito central es transformar el riesgo en un **instrumento de gobernanza**, capaz de orientar decisiones, alinear estrategias y promover la resiliencia organizacional en todos los niveles de la gestión.

1.2. Metodología y Fuentes

La metodología adoptada en este estudio se basa en un enfoque integrado de análisis de riesgos, combinando técnicas de *foresight*, prospectiva estratégica y evaluación comparativa de fuentes de riesgo en múltiples dominios. El objetivo central es ofrecer una visión estructurada sobre las fuerzas que moldean el entorno de incertidumbre en América Latina en 2026 y más allá, permitiendo a las organizaciones comprender y anticipar eventos que puedan afectar su continuidad, reputación y valor.

El proceso metodológico fue estructurado en cinco etapas principales. La primera etapa consistió en la **recolección y sistematización de información** proveniente de treinta y dos informes internacionales, regionales y corporativos publicados entre 2024 y 2025. Estos documentos fueron seleccionados con base en criterios de credibilidad institucional, alcance temático, rigor analítico y relevancia para el contexto latinoamericano. Entre las entidades y autores incluidos están el Foro Económico Mundial, las Naciones Unidas, la OCDE, el Banco Mundial, Microsoft, la *Global Initiative Against Transnational Organized Crime (GI-TOC), ComplyAdvantage,* el Instituto Internacional de Auditores Internos (IIA), la CEIUC, el ERI y la propia Plataforma t-Risk.

A La segunda etapa involucró la **normalización y clasificación de la información**, con la creación de fichas-fuente para cada documento analizado. Cada ficha registró datos como título, año de publicación, alcance geográfico, metodología empleada, principales hallazgos, fuentes de riesgo identificadas, incertidumbres estructurales, indicadores de alerta y grado de robustez de las evidencias. Esta estandarización garantizó la comparabilidad entre estudios de naturaleza distinta, como informes económicos, análisis de seguridad cibernética, previsiones climáticas y estudios de criminalidad transnacional.

La tercera etapa correspondió al **análisis de convergencia,** en la cual las fuentes de riesgo fueron agrupadas y reinterpretadas según una taxonomía única desarrollada por el equipo de investigación de la Plataforma t-Risk. Esta taxonomía integra seis dimensiones centrales:

(i) Geopolítica y comercio;
(ii) Tecnología e inteligencia artificial;
(iii) Criminalidad organizada y finanzas ilícitas;
(iv) Clima y recursos naturales;
(v) Infraestructura crítica y operaciones industriales;
(vi) Instituciones y confianza social.

Cada una de estas dimensiones fue evaluada en cuanto a su frecuencia de ocurrencia en las fuentes originales, el grado de interdependencia con las demás y el potencial de impacto sistémico.

En la cuarta etapa, se aplicó el análisis de escenarios, que relaciona las fuentes de riesgo y las incertidumbres identificadas para construir proyecciones plausibles del futuro. El procedimiento incluyó el mapeo de las variables más influyentes, la definición de ejes de tensión contrastantes y el modelado de cuatro escenarios que expresan combinaciones posibles de estas fuerzas: *Alianza PragTécnica, Redes Sombrías, Clima de Choques y Datos con Trabas, Fronteras Abiertas.* La técnica de modelado siguió los principios de plausimilitud, coherencia interna y utilidad estratégica, asegurando que los escenarios puedan ser utilizados como instrumentos de planificación y toma de decisiones.

La quinta y última etapa consistió en la **validación cruzada y síntesis ejecutiva**. Las narrativas, gráficos e indicadores fueron revisados por expertos, garantizando el alineamiento metodológico a las normas ISO 31000, ISO 31050 e ISO 31010. Además, los análisis fueron procesados por t-Risk Vision Pro, la inteligencia artificial de la Plataforma t-Risk, lo que permitió correlacionar variables, detectar brechas de información y generar visualizaciones dinámicas de riesgo.

La metodología, por lo tanto, combina rigor técnico y aplicabilidad práctica. Asegura que los resultados presentados en los capítulos siguientes no sean solo proyecciones hipotéticas, sino productos de un proceso comparativo, validado y sistemático, que traduce la complejidad global en *insights* operativos para organizaciones públicas y privadas.

1.3. Panorama Global 2026 y Más Allá

El panorama global proyectado para 2026 y los años subsiguientes se caracteriza por una creciente inestabilidad estructural, definida por la superposición de crisis y la interdependencia entre sistemas antes considerados autónomos. La economía mundial, la seguridad digital, el clima, las cadenas de suministro y la gobernanza

institucional pasaron a formar un ecosistema de riesgos entrelazados, en el cual las perturbaciones locales pueden asumir rápidamente dimensiones transnacionales.

América Latina emerge como una región de relevancia estratégica dentro de este contexto, no solo por sus recursos naturales y energéticos, sino también por su vulnerabilidad política y por su inserción desigual en las cadenas globales de valor.

Las tendencias más relevantes indican que el sistema internacional permanece en proceso de transición entre un orden global fragmentado y una nueva estructura multipolar. Este cambio de poder geopolítico está marcado por disputas tecnológicas, coerción económica y reconfiguración de las alianzas regionales. La seguridad internacional pasa a estar cada vez más condicionada por el dominio de la Inteligencia Artificial y por el control de infraestructuras críticas, datos y cadenas energéticas. En la práctica, el ciberespacio se ha convertido en el nuevo campo de disputa entre Estados, empresas y actores no estatales, con impactos directos sobre la economía real y sobre la seguridad corporativa.

El avance de la Inteligencia Artificial se transformó en un vector de ruptura tanto económica como ética. Las aplicaciones de aprendizaje automático y automatización amplían la productividad, pero también introducen nuevos riesgos relacionados con la manipulación de información, el fraude digital y la pérdida de control sobre sistemas críticos. Al mismo tiempo, la regulación internacional de la IA avanza de forma desigual. Mientras algunas regiones adoptan marcos legales robustos, otras permanecen en etapas iniciales de gobernanza, creando asimetrías normativas y riesgos de uso indebido. Este contexto favorece la proliferación de *deepfakes*, fraudes de identidad y ataques automatizados que desafían la capacidad de defensa tradicional de las organizaciones.

El componente climático, a su vez, se convierte en un multiplicador de riesgos y un factor determinante para la estabilidad regional. El aumento de la temperatura global, la irregularidad de los regímenes de lluvias y la intensificación de eventos extremos comprometen la seguridad alimentaria, la generación de energía y la disponibilidad de recursos hídricos. El impacto directo de estos fenómenos en América Latina es particularmente elevado debido a la dependencia de la matriz hidroeléctrica, la vulnerabilidad de sectores agrícolas y la urbanización acelerada. Las proyecciones indican que eventos climáticos severos y crisis de abastecimiento tenderán a ocurrir con mayor frecuencia e intensidad en 2026 y más allá, presionando a gobiernos y empresas a adoptar políticas de adaptación y planes de continuidad más amplios.

Paralelamente, **el crimen organizado transnacional** asume una nueva configuración. El informe *Global Organized Crime Index 2025* apunta hacia la consolidación de una

economía ilícita altamente diversificada, en la cual los delitos financieros, cibernéticos y ambientales superan, en crecimiento y rentabilidad, a los delitos violentos convencionales. Esta transformación redefine el concepto de seguridad y revela la erosión de las fronteras entre lo legal y lo ilegal. Las organizaciones criminales pasan a operar en redes globales e híbridas, utilizando empresas legítimas, plataformas digitales y sistemas financieros paralelos como vectores de expansión. La penetración de estas redes en sectores formales de la economía aumenta el riesgo de captura regulatoria, corrupción y distorsión de mercados.

La difusión del crimen organizado de naturaleza corporativa y digital tiene implicaciones directas para el entorno de negocios en América Latina. El debilitamiento institucional y la cooperación limitada entre países dificultan el combate efectivo a fraudes y al lavado de dinero. La convergencia entre grupos criminales, actores privados y flujos de capital ilegales amplía el riesgo de exposición reputacional y de sanciones regulatorias para empresas que no adopten mecanismos rigurosos de *compliance y due diligence*. Esta tendencia está fuertemente asociada al escenario denominado **"Redes Sombrías"**, en el cual la ausencia de coordinación entre políticas públicas, regulación tecnológica e integridad corporativa intensifica las vulnerabilidades sistémicas.

Desde el punto de vista económico, 2026 deberá consolidar un ciclo de crecimiento moderado y desigual, marcado por tensiones comerciales y por políticas fiscales restrictivas. La digitalización y la automatización seguirán como motores de productividad, pero con impactos sociales significativos, especialmente en el mercado laboral y en la distribución del ingreso. América Latina continuará dependiente de la exportación de *commodities* y enfrentará desafíos de competitividad industrial. La reanudación de inversiones dependerá de la capacidad de estabilidad política, de gobernanza ambiental y de seguridad jurídica. Los países que logren combinar políticas climáticas consistentes, integración regional e innovación tecnológica tendrán ventajas competitivas sostenibles en la próxima década.

En síntesis, el panorama global de 2026 y más allá está definido por un conjunto de **tensiones simultáneas**: avance tecnológico versus riesgo digital, globalización económica versus fragmentación política, crecimiento productivo versus inestabilidad climática, y gobernanza ética versus crimen organizado. Estas tensiones moldearán las principales **fuentes de riesgo** y determinarán el grado de resiliencia de cada país y sector. La comprensión de estas interdependencias es esencial para que organizaciones públicas y privadas logren anticipar eventos críticos, fortalecer su gobernanza y transformar la gestión de riesgos en una herramienta estratégica de decisión.

1.4. Fuentes de Riesgo Críticas e Incertidumbres Estructurales

La comprensión de las fuentes de riesgo que moldean el entorno de negocios, seguridad y gobernanza en América Latina en 2026 y más allá es fundamental para orientar estrategias de adaptación y priorización de inversiones. Las fuentes de riesgo representan los elementos o circunstancias que, aisladamente o combinados, pueden originar amenazas, vulnerabilidades u oportunidades, conforme definido por la norma ISO 31000.

Identificarlas y comprender sus interacciones permite desarrollar una visión sistémica de la exposición y de la capacidad de respuesta de las organizaciones ante un escenario de creciente complejidad y convergencia entre riesgos físicos, digitales y sociales.

En este estudio, distinguimos dos categorías principales: **(i) fuentes de riesgo críticas**, que representan conjuntos estructurales de amenazas, vulnerabilidades y oportunidades; y **(ii) incertidumbres estructurales**, que corresponden a variables profundas, de alta influencia y difícil previsibilidad, utilizadas como base para la construcción de los escenarios prospectivos. El estudio consolidó **seis fuentes de riesgo críticas**, derivadas del análisis de treinta y dos informes internacionales y regionales. Estas fuentes están interconectadas y forman el núcleo de las dinámicas que sustentan los cuatro escenarios presentados posteriormente. Ellas expresan tanto las fuerzas motrices globales como las fragilidades internas que determinan la trayectoria de los países latinoamericanos.

Tabla 1 – Fuentes de Riesgo Críticas 2026 y Más Allá

Fuente de Riesgo	Descripción Analítica	Impactos Principales	Tendencia Regional (2026 y más allá)
1. Geopolítica y Comercio Internacional	Reconfiguración de alianzas y cadenas de suministro en un contexto de multipolaridad y coerción económica. Disputas tecnológicas y sanciones comerciales afectan directamente flujos logísticos y cadenas críticas.	Inestabilidad de mercados; restricciones comerciales; vulnerabilidad energética; presiones sobre exportaciones agrícolas y minerales.	Aumento de la dependencia de acuerdos bilaterales y vulnerabilidad a choques externos.

2. Tecnología, Datos e Inteligencia Artificial	Aceleración de la digitalización y de la automatización sin estándares regulatorios uniformes. Expansión del uso indebido de la IA para fraudes, manipulación de datos y ataques cibernéticos automatizados.	Crecimiento de delitos digitales; violación de datos sensibles; impactos éticos y reputacionales; asimetría regulatoria.	Expansión de la IA generativa; aumento de ataques basados en machine learning y deepfakes.
3. Crimen Organizado, Finanzas Ilícitas y Corrupción Sistémica	Consolidación de redes híbridas que operan simultáneamente en economías formales e ilícitas. El *Global Organized Crime Index 2025* señala a América Latina como epicentro de actividades criminales diversificadas, incluyendo tráfico, fraudes financieros y delitos ambientales.	Captura del Estado; distorsión de mercados; riesgos reputacionales y de sanciones; erosión institucional.	Expansión de organizaciones ilícitas digitales; mayor infiltración en sectores logísticos, agrícolas y financieros.
4. Clima, Recursos Naturales y Sostenibilidad	Intensificación de eventos climáticos extremos, escasez hídrica y aumento de la temperatura media. La crisis climática se convierte en un multiplicador de riesgos, afectando la seguridad alimentaria, energética y territorial.	Interrupción de negocios; pérdida de productividad; daños a la infraestructura; inseguridad alimentaria; aumento de litigios ambientales.	Mayor frecuencia de desastres naturales y presión por gobernanza climática corporativa.
5. Infraestructuras Críticas y Operaciones Industriales (OT)	Vulnerabilidad creciente de sistemas industriales conectados a internet y dependencia de cadenas tecnológicas globales. Fallas en sistemas de control y mantenimiento pueden causar interrupciones a gran escala. Creciente dependencia de infraestructuras basadas	Paradas productivas; daños materiales; impactos financieros y ambientales; riesgo para la integridad de trabajadores y comunidades.	Ampliación de ataques a sistemas industriales; aumento de la adopción de controles ICS-5 (Industrial Control Systems nivel 5) e integración OT-IT.

	en el espacio (satélite para comunicaciones, navegación, sincronización financiera, monitoreo climático, etc.), que pasan a ser vectores críticos de riesgo ante posibles ataques cibernéticos y disputas geopolíticas en el entorno espacial.		
6. Instituciones, Gobernanza y Confianza Social	Erosión de la credibilidad institucional y polarización política. Desinformación y radicalización debilitan la capacidad de respuesta estatal y la cooperación regional.	Inestabilidad política; crisis de gobernanza; reducción del atractivo de inversiones; aumento de riesgos sociales y reputacionales.	Persistencia de polarización y desafíos a la legitimidad institucional en varios países latinoamericanos. Esta fragilidad institucional tiene raíces también en dinámicas micro, como erosión de confianza en las relaciones interpersonales, polarización en las comunidades y desgaste de valores compartidos, que se proyectan desde la familia y las redes locales hacia el sistema político, económico y regulatorio.

La migración desordenada intensifica estas fragilidades institucionales al presionar servicios públicos, alterar dinámicas de seguridad y crear oportunidades para que redes ilícitas operen en rutas de desplazamiento humano. Los flujos migratorios no estructurados amplían tensiones sociales, desafían capacidades municipales y nacionales de acogida y exponen vulnerabilidades urbanas y fronterizas. Este fenómeno funciona como vector transversal de inestabilidad, ampliando la complejidad de las respuestas estatales y corporativas y reforzando patrones de asimetría institucional característicos de entornos de riesgo sistémico.

Estas seis fuentes de riesgo no actúan aisladamente, sino que forman **una red de interdependencias** que amplifica sus efectos. El impacto combinado de fallas tecnológicas, eventos climáticos y criminalidad transnacional, por ejemplo, crea situaciones de ruptura que exigen nuevas formas de coordinación entre el sector público y el sector privado. Lo mismo ocurre con la fragilidad institucional, que tiende a

agravar las demás dimensiones de riesgo, reduciendo la capacidad de respuesta colectiva y la confianza en las instituciones.

El análisis de estas fuentes fue complementado por la identificación de tres **incertidumbres estructurales**, que representan las variables de mayor imprevisibilidad e impacto sobre el futuro regional. Ellas funcionan como ejes de tensión que determinan la dirección de los escenarios prospectivos.

Tabla 2 – Incertidumbres estructurales 2026 y Más Allá

Eje de Incertidumbre	Descripción	Relevancia Estratégica
Integración Regional versus Fragmentación Político-Criminal	Mide la capacidad de los países latinoamericanos de cooperar en políticas de seguridad, comercio y tecnología. El avance de la integración regional fortalece la estabilidad y la respuesta colectiva, mientras que la fragmentación favorece al crimen organizado y la inseguridad.	Define el nivel de coordinación institucional y la eficacia de las políticas públicas regionales.
Gobernanza de Inteligencia Artificial versus Caos Digital	Representa el equilibrio entre la innovación tecnológica y la regulación ética. La ausencia de gobernanza sobre algoritmos y datos puede llevar al colapso de la confianza digital y a la expansión de delitos cibernéticos automatizados.	Determina la capacidad de las economías para sostener el crecimiento tecnológico con seguridad y transparencia.
Disciplina Macroeconómica versus Estrés Multichoque	Evalúa la solidez de las políticas fiscales y monetarias ante crisis simultáneas, como eventos climáticos, ciberataques e inestabilidad social. El estrés multichoque afecta directamente el financiamiento de la resiliencia y la capacidad de inversión en infraestructura crítica.	Influye en la sostenibilidad económica y la competitividad regional a largo plazo.

Aunque se han identificado tres incertidumbres estructurales como críticas para el horizonte 2026 y más allá, la construcción de la Matriz de Escenarios exigió una elección metodológica en cuanto a las variables que mejor capturan las diferencias cualitativas entre futuros alternativos. Así, se optó por **utilizar las dos primeras incertidumbres estructurales** — *Integración Regional versus Fragmentación Político-Criminal y Gobernanza de Inteligencia Artificial versus Caos Digital* — como **ejes estructurantes de la matriz 2x2**, por presentar mayor capacidad de generar configuraciones contrastantes de gobernanza, cooperación, competencia y estabilidad institucional. Ambas poseen características centrales en marcos de prospectiva: son simultáneamente inciertas, altamente influyentes y mutuamente independientes para

fines analíticos.

La tercera incertidumbre estructural — *Disciplina Macroeconómica versus Estrés Multichoque* — fue, a su vez, tratada como un **vector transversal**, operando como campo de presión sistémico que permea todos los escenarios, en lugar de constituir un eje separador. Esta decisión refleja su naturaleza distinta: a diferencia de las dos primeras, que definen direcciones estratégicas, la tercera describe un *grado de intensidad* de choques (climáticos, tecnológicos, sociales y fiscales) capaces de amplificar o reducir la resiliencia de las trayectorias futuras. No se trata, por tanto, de un binario que diferencia escenarios, sino de un **gradiente estructural** que afecta la profundidad, la velocidad y el impacto de los eventos descritos en los cuatro cuadrantes.

Al posicionar esta tercera variable como **fuerza transversal**, reconocemos su relevancia sistémica sin comprometer la claridad visual e interpretativa de la matriz. La dimensión "multichoque" funciona como una capa de complejidad adicional que interactúa con cada uno de los escenarios, acentuando riesgos y oportunidades de maneras distintas. De esta forma, la matriz mantiene su función de representar contrastes estratégicos fundamentales, mientras que el informe preserva la coherencia analítica al incorporar la dinámica macroeconómica como elemento indispensable para la comprensión del entorno prospectivo de 2026 y los años subsiguientes.

1.5. Matriz de Escenarios 2026 y Más Allá

La matriz de escenarios presentada en este capítulo sintetiza las combinaciones más plausibles derivadas de las **incertidumbres estructurales seleccionadas como ejes** para diferenciar futuros alternativos. Aunque el análisis anterior identificó tres incertidumbres de alta influencia para el horizonte 2026 y más allá, la construcción de la matriz 2x2 se basa específicamente en **dos de ellas**: aquellas con mayor poder de crear trayectorias contrastantes y mutuamente excluyentes. La tercera incertidumbre estructural, relativa a la disciplina macroeconómica frente al estrés multichoque, es tratada en el estudio como **fuerza transversal sistémica**, permeando todos los escenarios y modulando su intensidad, pero sin operar como eje separador.

Así, la matriz se organiza a partir de dos ejes críticos que definen las direcciones más relevantes de las transformaciones observadas en América Latina. El primero captura la oscilación entre integración y fragmentación institucional; el segundo refleja el equilibrio entre gobernanza tecnológica y caos digital. La interacción entre estos vectores genera cuatro futuros posibles para el entorno de riesgo, seguridad y gobernanza corporativa.

El eje horizontal representa el grado de cooperación entre países latinoamericanos, variando desde procesos de integración económica, política y tecnológica hasta una fragmentación marcada por la expansión del crimen organizado y por el deterioro institucional. El eje vertical corresponde al nivel de gobernanza de la Inteligencia Artificial, de los datos y de las infraestructuras digitales, oscilando entre modelos maduros, éticos y transparentes y escenarios caracterizados por descontrol, manipulación y asimetrías regulatorias. La combinación de estos dos ejes define la estructura 2x2 que organiza cuatro narrativas de futuro, cada una con implicaciones específicas para sectores productivos, instituciones públicas y organizaciones privadas.

Tabla 3 – Matriz de Escenarios 2026 y Más Allá

Eje Vertical	Gobernanza Avanzada de Inteligencia Artificial, Datos e Infraestructuras Digitales	Caos Digital, Uso Indebido de Tecnología y Asimetría Regulatoria
Eje Horizontal		
Integración Regional y Cooperación Económica	**Escenario 1 – Alianza PragTécnica** Entorno de cooperación pragmática entre países; avances regulatorios; interoperabilidad de datos y mecanismos compartidos de seguridad digital; reducción de fraudes e interrupciones de negocios; fortalecimiento de instituciones.	**Escenario 3 – Clima de Choques** La integración económica avanza, pero con fragilidad tecnológica; eventos climáticos extremos y fallas digitales ocurren simultáneamente; alta presión sobre cadenas productivas e infraestructuras críticas; necesidad de respuestas coordinadas.
Fragmentación Político-Criminal y Baja Cooperación Regional	**Escenario 4 – Datos con Trabas, Fronteras Abiertas** Gobernanza avanzada de IA y seguridad liderada por sectores privados; resiliencia concentrada en empresas de gran tamaño; gobiernos inestables; operaciones corporativas sustentadas por tecnología de punta y controles ICS-5.	**Escenario 2 – Redes Sombrías** Fragmentación institucional; captura del Estado por redes criminales; expansión de economías ilícitas; *deepfakes*, fraudes y ataques cibernéticos automatizados; erosión de la confianza; riesgos físicos elevados.

Lectura Estratégica de la Matriz

La matriz indica que el futuro de la región será determinado principalmente por la capacidad de articular tres elementos: **cooperación institucional, gobernanza tecnológica y resiliencia macroeconómica ante entornos de estrés multichoque**. Estos

elementos moldean patrones de riesgo que se manifiestan de forma distinta en cada cuadrante e influyen no solo en la arquitectura institucional, sino también en la estabilidad fiscal, la capacidad de respuesta del Estado y la continuidad de las operaciones privadas. Aunque los escenarios se presentan de forma aislada, en la práctica, países y sectores pueden experimentar características superpuestas, especialmente cuando los choques climáticos, tecnológicos o económicos presionan la disciplina macroeconómica y **amplifican transiciones graduales entre cuadrantes a lo largo del tiempo.**

Lectura Estratégica Ampliada del Escenario 1 – Alianza PragTécnica

El Escenario 1, denominado Alianza PragTécnica, expresa la posibilidad de un entorno regional en el cual la cooperación institucional y la gobernanza tecnológica avanzan de forma pragmática, gradual y consistente. Este escenario no presupone una integración política plena o un salto institucional repentino, sino la adopción incremental de acuerdos, normas y mecanismos operativos que reducen fricciones entre países latinoamericanos y fortalecen la capacidad conjunta de respuesta a riesgos convergentes **en un contexto global aún marcado por choques simultáneos que presionan economías y sectores productivos**.

Desde el punto de vista regulatorio, este escenario se caracteriza por la armonización progresiva de leyes y estándares relacionados con la protección de datos, gobernanza de Inteligencia Artificial, auditoría algorítmica, ciberseguridad e identidad digital. Incluso sin una convergencia legislativa completa, los marcos se vuelven compatibles entre sí, permitiendo la interoperabilidad entre sistemas públicos y privados. La interoperabilidad, en este contexto, abarca desde datos de identidad digital y certificados electrónicos hasta protocolos de investigación financiera, inteligencia de amenazas y trazabilidad de cadenas logísticas críticas; **un factor particularmente relevante cuando la región busca mantener la disciplina macroeconómica y reducir vulnerabilidades a choques externos e internos.**

En el campo de la seguridad, el Escenario 1 asume la consolidación de iniciativas conjuntas entre gobiernos y empresas, sobre todo en los sectores de energía, transporte, telecomunicaciones, industria y finanzas. Esta coordinación posibilita el intercambio de información sobre amenazas, la estandarización de prácticas de respuesta a incidentes y la creación de ejercicios integrados de simulación. La cooperación tecnológica permite que capacidades avanzadas, como detección automatizada de ataques, autenticación biométrica regional y respuesta coordinada a fraudes a gran escala, sean distribuidas de forma más equilibrada entre los países; **reduciendo la exposición sistémica de la región a multichoques que pueden interrumpir cadenas de valor y acelerar presiones económicas.**

La gobernanza de riesgos, en este entorno, se vuelve más previsible y transparente. Los sistemas de monitoreo integrados permiten la detección temprana de eventos críticos, reduciendo el tiempo de respuesta y aumentando la capacidad de mitigación. La confianza institucional crece porque los países demuestran capacidad de actuar colectivamente ante riesgos transnacionales, como delitos cibernéticos, eventos climáticos extremos e interrupciones de cadenas logísticas. Este proceso también fortalece la resiliencia de infraestructuras críticas, que pasan a operar con estándares mínimos regionales de ciberseguridad y continuidad operativa**; un componente esencial para sostener la estabilidad económica en escenarios de estrés multichoque.**

En el plano económico, la Alianza PragTécnica favorece flujos comerciales más estables, reduce incertidumbres regulatorias y atrae inversiones. Sectores con fuerte dependencia de la previsibilidad, como energía renovable, logística integrada, agronegocios y economía digital, son particularmente beneficiados. La reducción de barreras técnicas y el aumento de la confianza regulatoria facilitan el desarrollo de corredores logísticos de bajo riesgo, mecanismos de compensación energética y redes de innovación basadas en Inteligencia Artificial confiable y auditable; **creando un entorno que refuerza la disciplina fiscal, mejora la percepción de riesgo soberano y reduce la vulnerabilidad a choques exógenos.**

Por último, este escenario amplía el espacio para políticas públicas que concilian innovación y seguridad. La Inteligencia Artificial es adoptada con gobernanza ética, mecanismos de explicabilidad y auditoría automatizada, reduciendo la probabilidad de uso indebido por agentes ilícitos y aumentando la confiabilidad de los sistemas automatizados de decisión. Las organizaciones ganan previsibilidad y pueden planificar de forma más robusta, dado que las fuentes de riesgo son monitoreadas por sistemas interconectados que producen alertas tempranas y orientan respuestas coordinadas; **lo que contribuye directamente a amortiguar impactos económicos de eventos multichoque.**

La Alianza PragTécnica, por lo tanto, representa un futuro en el cual América Latina no elimina sus fragilidades históricas, pero desarrolla instrumentos colectivos y tecnologías maduras capaces de reducir el impacto de riesgos transfronterizos. La cooperación regional, combinada con la gobernanza tecnológica avanzada, crea un entorno capaz de limitar la expansión de delitos digitales, mitigar potenciales consecuencias de los posibles eventos climáticos severos y fortalecer la seguridad física y cibernética de sectores **estratégicos, mientras fortalece la resiliencia macroeconómica y reduce la exposición regional a estreses multichoques**. Se trata del escenario en el que las organizaciones encuentran las mejores condiciones para desarrollar resiliencia dinámica, atraer inversiones y consolidar modelos de gobernanza orientados por la inteligencia de riesgos.

Lectura Estratégica Ampliada del Escenario 2 – Redes Sombrías

El Escenario 2, denominado Redes Sombrías, representa la configuración más adversa entre los futuros plausibles para América Latina en 2026 y más allá. Surge cuando la fragmentación político-criminal y la ausencia de gobernanza tecnológica convergen de manera simultánea, creando un entorno marcado por la erosión de las instituciones, el fortalecimiento de redes ilícitas transnacionales y la pérdida progresiva de la confianza pública; **en un contexto de estrés multichoque que debilita aún más la disciplina**

macroeconómica y amplía asimetrías entre países y sectores. En este escenario, el crimen organizado deja de actuar solo en los márgenes del sistema económico y pasa a ocupar posiciones estratégicas en cadenas logísticas, financieras y regulatorias, ampliando su capacidad de influenciar mercados y distorsionar decisiones públicas y privadas.

Desde el punto de vista institucional, el escenario se caracteriza por inestabilidad política, ciclos cortos de gobiernos, presiones populistas y baja capacidad regulatoria. La captura de estructuras estatales por grupos ilícitos, descrita por el *Global Organized Crime Index 2025*, se intensifica y fragmenta la actuación gubernamental, dificultando políticas de seguridad a largo plazo y haciendo inviables las acciones coordinadas entre países. La cooperación internacional es mínima, y los organismos de fiscalización, control e inteligencia se vuelven vulnerables tanto a la corrupción como a la intimidación. Como consecuencia directa, las decisiones regulatorias se vuelven imprevisibles y sujetas a influencias externas, creando un entorno de negocios volátil y propicio a riesgos jurídicos y reputacionales; **cuadro agravado por la incapacidad de sostener políticas macroeconómicas estables en medio de choques sucesivos**.

En el dominio digital, la ausencia de gobernanza de Inteligencia Artificial y la proliferación de tecnologías baratas y accesibles potencializan fraudes, ataques cibernéticos y manipulación automatizada de información. *Deepfakes*, esquemas de ingeniería social de alta sofisticación y clones de identidad digital se convierten en prácticas comunes, alimentadas por modelos de inteligencia artificial no regulados. Los ataques de compromiso de correo empresarial, fraudes financieros y secuestros de datos se multiplican a escala industrial, con agentes criminales utilizando técnicas avanzadas de automatización, aprendizaje automático y explotación simultánea de múltiples vulnerabilidades. La frontera entre ataques cibernéticos y amenazas físicas se disuelve, ya que grupos ilícitos utilizan información digital para extorsión, invasión de propiedades y direccionamiento de delitos violentos; **acelerando daños económicos y elevando costos de recomposición en un entorno ya presionado por múltiples choques.**

El entorno operativo se vuelve altamente imprevisible. Las cadenas logísticas sufren interrupciones recurrentes provocadas por robo de carga, bloqueos organizados, manipulación de rutas e interferencias en sistemas de transporte. Puertos, ferrocarriles y centros de distribución se convierten en objetivos estratégicos de grupos ilícitos que buscan controlar flujos comerciales, tributos informales y rutas de exportación. Empresas de sectores como agronegocios, minería, retail, energía y transporte enfrentan riesgos elevados de interferencia criminal, inflación de costos, pérdida de productividad y exposición a la violencia organizada. El riesgo físico contra ejecutivos y equipos clave crece de forma significativa, exigiendo protocolos de protección ampliados y **presionando aún más los costos operativos en economías ya fragilizadas por la pérdida de disciplina fiscal y por la inestabilidad de precios causada por multichoques.**

En el plano económico y financiero, el escenario está marcado por un aumento expresivo de la economía ilícita, por el lavado de dinero a gran escala y por la infiltración de capital criminal en empresas legítimas. Los delitos financieros sofisticados, inclusive aquellos basados en Inteligencia Artificial, se vuelven más lucrativos que las actividades ilícitas tradicionales. La utilización de criptomonedas, marketplaces digitales y redes de frontera para operaciones de ocultación de activos pasa a integrar la estrategia básica de las organizaciones criminales. Para empresas formales, el riesgo de exposición involuntaria a la economía ilícita aumenta sustancialmente, ampliando la posibilidad de sanciones, investigaciones transnacionales y daños severos a la reputación; **al mismo tiempo que la volatilidad cambiaria, la retracción del crédito y la pérdida de confianza en los mecanismos estatales de estabilización profundizan el estrés macroeconómico.**

La confianza pública sufre un declive acelerado. La desinformación coordinada, las campañas de manipulación política, la polarización digital y los ataques contra instituciones de prensa y justicia provocan el deterioro del entorno democrático. La ausencia de mecanismos eficaces de gobernanza tecnológica permite que agentes criminales, actores extremistas e intereses privados difusos manipulen la percepción social, generando inestabilidad y reduciendo la capacidad de respuesta estatal. El debilitamiento de la cohesión social aumenta la probabilidad de protestas violentas, acciones de milicias digitales, linchamientos reputacionales y ataques a empresas asociadas a temas sensibles; **lo que profundiza aún más la inestabilidad económica al generar fuga de inversiones, retracción de consumo e interrupción de servicios esenciales.**

En este escenario, las organizaciones enfrentan desafíos significativos para operar con seguridad y previsibilidad. Los modelos tradicionales de gestión de riesgos se vuelven insuficientes, pues no logran lidiar con amenazas híbridas que combinan elementos

digitales, financieros, físicos y reputacionales**, incluyendo el uso de drones autónomos y algoritmos de IA para apoyar intrusiones físicas, sabotaje y contrabando en infraestructuras críticas y cadenas logísticas.** La ausencia de coordinación estatal y la retracción de mecanismos de protección pública hacen que las empresas necesiten internalizar capacidades típicas de seguridad nacional, como inteligencia contra amenazas, verificación reforzada de integridad, protección ejecutiva y redundancia logística; **en un entorno económico donde la inestabilidad estructural y la presión multichoque elevan costos, reducen márgenes y hacen que las inversiones a largo plazo sean más arriesgadas.**

El Escenario 2, por lo tanto, representa un entorno en el que la racionalidad económica y la gobernanza pública pierden espacio frente a lógicas informales, ilícitas y opacas, transformando el riesgo en un elemento omnipresente y altamente volátil. La expansión de las redes sombrías reduce el margen de acción de las organizaciones, aumenta costos operativos y genera ciclos prolongados de inseguridad en **economías que ya no logran mantener disciplina fiscal o estabilizar choques sucesivos**, afectando directamente la competitividad, la atracción de inversiones y la sostenibilidad de las cadenas productivas.

Lectura Estratégica Ampliada del Escenario 3 – Clima de Choques

El Escenario 3, denominado Clima de Choques, refleja un entorno en el que la cooperación económica entre los países latinoamericanos avanza, pero permanece limitada por la fragilidad tecnológica, la baja madurez en ciberseguridad y la creciente presión ejercida por los eventos climáticos extremos; **presionando continuamente la disciplina macroeconómica y ampliando la exposición regional a estreses sucesivos**. Se trata de un escenario híbrido en el que las economías logran mantener niveles moderados de integración comercial y acuerdos de infraestructura, pero sin la capacidad institucional y tecnológica necesaria para proteger sus cadenas críticas de las perturbaciones ambientales y digitales que se intensifican en 2026 y más allá.

El principal factor que define este escenario es el clima como multiplicador de riesgos. La región enfrenta sequías prolongadas, olas de calor extremo, tormentas severas e inundaciones que se vuelven más frecuentes e intensas, acelerando el deterioro de suelos, aumentando la volatilidad agrícola y causando perturbaciones significativas en la generación y distribución de energía. La matriz energética basada en hidroelectricidad sufre impactos directos, especialmente en países con embalses cada vez más presionados por la variabilidad hídrica. Al mismo tiempo, los sistemas urbanos densamente poblados enfrentan desafíos relacionados con deslizamientos, falta de agua, islas de calor y fragilidad de drenaje**; choques que afectan directamente precios, productividad y capacidad fiscal de los Estados**.

Estos fenómenos climáticos producen ciclos recurrentes de interrupción de negocios, con impactos desproporcionados sobre sectores como energía, agronegocios, minería, manufactura y logística. La sinergia entre eventos ambientales y fallas digitales amplía aún más los efectos de cada incidente. Los sistemas industriales conectados se vuelven vulnerables a fluctuaciones eléctricas, sobrecalentamiento de componentes, fallas en sensores y pérdida temporal de conectividad. La interacción entre fragilidad climática y fragilidad tecnológica genera interrupciones en cadenas productivas que ya operan bajo márgenes estrechos, creando retrasos logísticos, escasez de insumos y pérdidas financieras acumulativas **que se propagan como estrés macroeconómico estructural.**

La logística regional sufre impactos significativos. Carreteras son interrumpidas por inundaciones, derrumbes e incendios forestales. Ferrocarriles y puertos enfrentan paralizaciones derivadas de eventos climáticos severos, aumentando costos de transporte y presionando precios internos. Redes eléctricas y de telecomunicaciones también se vuelven vulnerables, especialmente en áreas con infraestructura antigua o mal distribuida. La dependencia de las cadenas exportadoras de alimentos, minerales y energía se hace más evidente, ampliando tensiones entre demanda global y limitaciones físicas locales **y generando volatilidad macroeconómica adicional en economías ya sensibles a choques externos.**

En el campo institucional, a pesar de existir cooperación económica, los gobiernos latinoamericanos enfrentan dificultades para coordinar respuestas climáticas a gran escala. La ausencia de políticas robustas de adaptación y resiliencia produce un entorno en el que la actuación estatal es frecuentemente reactiva, fragmentada e insuficiente para amortiguar el impacto de los choques ambientales. La región presenta estándares irregulares de fiscalización, licenciamiento ambiental, protección de ecosistemas y prevención de desastres, dificultando la planificación integrada. Estos déficits institucionales agravan vulnerabilidades sectoriales e intensifican el desgaste de la infraestructura física y social; **además de presionar gastos de emergencia, reducir la capacidad de inversión pública y disminuir el margen fiscal para políticas anticíclicas.**

La inseguridad hídrica se convierte en uno de los marcadores más sensibles del escenario. En varios países, embalses, acuíferos y sistemas de abastecimiento público pasan a operar en niveles críticos, afectando directamente a industrias de alto consumo de agua, como agricultura de regadío, metalurgia, bebidas, papel y celulosa y minería. La competencia por recursos hídricos intensifica conflictos territoriales, presiona políticas de concesión e impone costos adicionales a empresas, que necesitan invertir en reúso de agua, fuentes alternativas y planes de contingencia; **costos que presionan márgenes, precios e indicadores macroeconómicos clave.**

Desde el punto de vista tecnológico, la baja madurez digital y la insuficiencia de controles avanzados de seguridad aumentan el riesgo de incidentes cibernéticos que ocurren paralelamente a choques climáticos. En situaciones de estrés ambiental, la probabilidad de fallas humanas y operativas también crece, ampliando vulnerabilidades en sistemas de supervisión, monitoreo y control. Las organizaciones enfrentan dificultades para mantener operaciones continuas, sobre todo cuando dependen de equipos sensibles a la temperatura, conectividad estable e integridad de las redes eléctricas; **factores que amplifican costos de producción e impactan la estabilidad macroeconómica regional.**

En este escenario, la necesidad de resiliencia climática se vuelve urgente. Empresas y gobiernos se ven forzados a invertir en redundancia estructural, diversificación de fuentes energéticas, modernización de infraestructuras y sistemas predictivos basados en análisis de datos e Inteligencia Artificial. Modelos de previsión ambiental, sensores, satélites y redes inteligentes se vuelven esenciales para detectar tendencias adversas y anticipar respuestas. Al mismo tiempo, crece la demanda de seguros paramétricos y mecanismos de financiamiento climático, especialmente en sectores vulnerables; **instrumentos que, aunque reducen impactos, también presionan presupuestos públicos y privados, exigiendo una disciplina financiera más rigurosa.**

El Escenario 3 también acarrea consecuencias sociales. La vulnerabilidad climática agrava desigualdades, produce desplazamientos poblacionales, presiona sistemas urbanos y eleva tensiones sociales en áreas afectadas por escasez de recursos. Estos impactos aumentan la necesidad de políticas de adaptación, protocolos de emergencia y programas de apoyo a las comunidades más expuestas; **todos dependientes de recursos fiscales que se vuelven más disputados en un entorno macroeconómico de múltiples choques.**

El Clima de Choques, por lo tanto, describe un futuro en el que el entorno económico mantiene relativa estabilidad, pero la capacidad de operar de manera segura y previsible está profundamente comprometida por la convergencia entre eventos ambientales severos y fragilidad tecnológica. La región necesita reforzar su gobernanza climática, ampliar inversiones en adaptación y fortalecer la resiliencia de infraestructuras críticas **para evitar que ciclos de multichoque se conviertan en inestabilidad fiscal permanente, pérdida de competitividad y retrocesos estructurales**.

Lectura Estratégica Ampliada del Escenario 4 – Datos con Trabas, Fronteras Abiertas

El Escenario 4, denominado Datos con Trabas, Fronteras Abiertas, describe un entorno en el cual el sector privado alcanza niveles elevados de madurez tecnológica y

gobernanza digital, mientras que la inestabilidad institucional persiste y limita la eficacia de las políticas públicas; **un contexto en el que choques sucesivos y restricciones fiscales dificultan el mantenimiento de la disciplina macroeconómica y profundizan asimetrías estructurales**. Es un futuro marcado por la disparidad entre una economía corporativa cada vez más avanzada, sofisticada y resiliente, y estructuras estatales fragmentadas, incapaces de seguir el ritmo de innovación y de imponer estándares uniformes de seguridad, regulación o justicia. Como resultado, la región vive una asimetría profunda: empresas líderes logran operar con relativa estabilidad, pero el conjunto de la economía permanece vulnerable a riesgos sistémicos.

En este escenario, la gobernanza de la Inteligencia Artificial pasa a ser conducida prioritariamente por grandes conglomerados, plataformas tecnológicas y empresas de infraestructura crítica. Ellas desarrollan mecanismos propios de auditoría algorítmica, explicabilidad y protección de datos, estableciendo estándares que se convierten en referencia para el mercado y que, muchas veces, ocupan el espacio dejado por marcos regulatorios incompletos o desactualizados. La ausencia de un entorno regulatorio uniforme lleva a empresas de gran tamaño a actuar como "legisladores de facto", definiendo directrices privadas de conformidad que influencian proveedores, socios logísticos y cadenas industriales**; fenómeno acentuado por la incapacidad estatal de adaptarse rápidamente en medio de choques económicos, climáticos y tecnológicos.**

La madurez digital de las organizaciones en este escenario es elevada. Empresas líderes adoptan sistemas robustos de autenticación biométrica, segmentación avanzada de redes, criptografía de punta y modelos de Inteligencia Artificial defensivas capaces de detectar comportamientos anómalos y anticipar ataques cibernéticos. La implementación de controles ICS-5 se convierte en diferencial competitivo en sectores industriales, de energía, saneamiento, alimentos y logística, permitiendo niveles superiores de disponibilidad operativa, redundancia e integridad de los procesos críticos. Al mismo tiempo, soluciones de monitoreo integrado, como Centros de Operaciones de Seguridad ciberfísica (GSOC convergentes), elevan la capacidad de respuesta a incidentes **y funcionan como amortiguadores privados en un entorno de multichoque que presiona sistemas públicos fragilizados.**

A pesar de este avance privado, el entorno institucional está marcado por inestabilidad política, fragmentación de políticas públicas y baja capacidad de ejecución estatal. Los gobiernos enfrentan restricciones fiscales y operativas, dificultando la actualización de marcos legales, la creación de mecanismos eficaces de fiscalización y la modernización de infraestructuras públicas. En varios países, sistemas judiciales sobrecargados, disputas políticas y cambios abruptos de orientación normativa producen incertidumbres regulatorias e inseguridad jurídica. La ausencia de políticas robustas de

integración regional también limita el avance de acuerdos que podrían reducir costos transfronterizos, ampliar infraestructura logística y uniformizar estándares de protección de datos; **y la suma de inestabilidad institucional con choques simultáneos profundiza la volatilidad macroeconómica.**

En este entorno, el riesgo se vuelve altamente asimétrico. Organizaciones con capacidad tecnológica y recursos suficientes logran mitigar amenazas, preservar su reputación y mantener la continuidad de sus operaciones. En cambio, empresas de mediano y pequeño tamaño, así como cadenas productivas menos capitalizadas, permanecen expuestas a ataques cibernéticos, fraudes, interrupciones de energía e inestabilidades logísticas. La desigualdad tecnológica amplía la brecha entre empresas resilientes y vulnerables, creando un

ecosistema de protección desigual e incompatible con la resiliencia sistémica necesaria para evitar colapsos regionales; **especialmente en entornos macroeconómicos sujetos a choques sucesivos y volatilidad fiscal.**

El sector privado asume, en este escenario, un papel ampliado en la protección de infraestructuras críticas. Las empresas pasan a invertir en redundancias locales, microgeneración energética, redes privadas de telecomunicaciones y modelos avanzados de supervisión y control, reduciendo su dependencia de servicios públicos. Esta tendencia refuerza la creación de “islas de resiliencia”, en las cuales entornos controlados por empresas alcanzan estándares elevados de confiabilidad, mientras que áreas adyacentes continúan sujetas a fallas sistémicas, interrupciones y criminalidad; **un mosaico de alta resiliencia localizada y vulnerabilidad estructural que se agrava con la incapacidad estatal de estabilizar choques económicos.**

En el campo económico, el entorno de negocios se vuelve competitivo, pero desigual. La innovación prospera en ecosistemas corporativos integrados a cadenas globales de valor, mientras que segmentos dependientes de políticas públicas permanecen estancados. Servicios financieros, tecnología, energía limpia, manufactura avanzada y logística de alto valor se convierten en catalizadores de crecimiento. En contrapartida, sectores con fuerte dependencia de infraestructura pública o de marcos regulatorios estables enfrentan desafíos estructurales para alcanzar productividad y atraer inversiones; **especialmente en entornos macroeconómicamente presionados, con ciclos recurrentes de inestabilidad y restricciones fiscales crónicas.**

La seguridad pública permanece fragilizada. La falta de integración entre agencias estatales y la ausencia de políticas regionales coherentes amplían la actuación de redes ilícitas, especialmente en áreas rurales, fronterizas y portuarias. La criminalidad organizada explota brechas en el aparato estatal mientras evita entornos

empresariales fortificados. Esto produce un fenómeno dual: alta resiliencia dentro de los entornos controlados por grandes empresas y alta vulnerabilidad fuera de ellos; **un reflejo de la asimetría macroeconómica que caracteriza el escenario.**

El escenario también posee implicaciones sociales significativas. La desigualdad en el acceso a la tecnología y a la seguridad genera fricciones entre sectores de la economía, amplía tensiones laborales y refuerza la percepción de que la protección y la estabilidad son bienes privados, disponibles solo para organizaciones con altos niveles de inversión. La polarización digital y la fragilidad institucional dificultan la construcción de políticas públicas inclusivas, limitando el alcance de soluciones a largo plazo **y agravando tensiones sociales típicas de entornos sometidos a estrés multichoque**.

El Escenario 4, por lo tanto, describe un futuro en el cual la resiliencia corporativa avanza más rápido que la resiliencia estatal, creando un modelo de protección fragmentado e insuficiente para amortiguar riesgos sistémicos. Aunque las organizaciones líderes logran preservar la competitividad por medio de tecnologías avanzadas, la falta de integración institucional y la inestabilidad regulatoria impiden que los beneficios de la innovación se diseminen de manera uniforme por la región. Se trata de un escenario ambiguo: próspero para quien está en la frontera tecnológica y vulnerable para quien depende de políticas públicas e infraestructura estatal. La capacidad de las organizaciones de operar de forma segura en este entorno dependerá de inversiones continuas en tecnología, resiliencia y gobernanza interna, así como de estrategias para mitigar la ausencia de estándares regulatorios y la volatilidad de las instituciones públicas; **características agravadas por choques económicos recurrentes y por la dificultad estructural de mantener disciplina macroeconómica**.

Implicaciones Generales de la Matriz

A La lectura integrada de la Matriz de Escenarios 2026 y más allá revela cinco implicaciones estratégicas de carácter transversal, que influyen en el entorno político, económico, tecnológico e institucional de toda la región. Ellas sintetizan los elementos comunes que emergen de la interacción entre las fuentes de riesgo críticas y las incertidumbres estructurales, incluyendo la presión creciente ejercida por choques simultáneos sobre la disciplina macroeconómica. Esta lectura integrada ofrece directrices fundamentales para orientar decisiones de gobiernos, empresas y organismos multilaterales.

En todas estas dimensiones, la integridad ética — tanto en la esfera pública como en la privada — funciona como una “infraestructura invisible” de la confianza. Cuando los valores de honestidad, responsabilidad y transparencia se deterioran, aumentan los

costos de transacción, se amplían las oportunidades para la captura institucional y se reduce la eficacia de los propios mecanismos de gestión de riesgos. Esta base ético-moral constituye el cimiento que sostiene la cooperación institucional, la gobernanza tecnológica y la capacidad de resiliencia organizacional.

La primera implicación se refiere a la necesidad de elevar de forma consistente el estándar de gobernanza tecnológica, especialmente en lo que se refiere al uso ético, seguro y transparente de la Inteligencia Artificial. La ausencia de marcos regulatorios coherentes y de mecanismos de auditoría algorítmica amplía vulnerabilidades y permite que tecnologías avanzadas sean utilizadas para fraudes, manipulación de datos e invasión de identidades digitales. La gobernanza tecnológica se convierte, por lo tanto, en eje central para preservar la integridad de los datos, garantizar previsibilidad regulatoria y reforzar la confianza digital, que es hoy uno de los pilares del funcionamiento de las economías digitales y de las infraestructuras críticas;

especialmente en entornos sujetos a estrés multichoque, en los cuales los daños digitales pueden amplificar rápidamente impactos económicos y sociales.

La segunda implicación se refiere a la cooperación institucional como elemento decisivo para reducir vulnerabilidades y enfrentar riesgos transnacionales. Delitos financieros, redes ilícitas, eventos climáticos extremos, ataques cibernéticos e interrupciones logísticas no respetan fronteras administrativas. Los países que operan aisladamente tienden a enfrentar ciclos más largos de inestabilidad, mayor costo económico y dificultades para mantener disciplina fiscal ante choques sucesivos. En cambio, entornos que adoptan acuerdos regionales de interoperabilidad, estándares compartidos de seguridad y mecanismos conjuntos de respuesta a incidentes logran proteger mejor sus cadenas productivas y fortalecer la capacidad de coordinación institucional. En este sentido, la cooperación no es solo deseable, sino esencial para impedir la expansión de dinámicas típicas del Escenario 2, marcado por redes ilícitas y fragmentación político-criminal.

La tercera implicación deriva de la constatación de que el clima se ha convertido en un multiplicador de riesgos estructurales. Los eventos climáticos extremos afectan la productividad agrícola, presionan la matriz energética, comprometen la infraestructura urbana y desestabilizan cadenas logísticas críticas. También amplifican efectos colaterales, como conflictos territoriales, inseguridad hídrica y migración forzada. Esta combinación eleva costos sistémicos, reduce márgenes económicos y presiona presupuestos públicos, dificultando respuestas anticíclicas y erosionando la disciplina macroeconómica. Ante este escenario, cualquier enfoque de riesgo basado solo en mitigación se vuelve insuficiente. La región necesita avanzar en políticas de adaptación climática, protección ambiental y continuidad de negocios, integrando previsiones

ambientales, datos operativos y tecnologías de análisis predictivo basadas en Inteligencia Artificial. Sin esta capacidad de adaptación, la región quedará atrapada en el ciclo de vulnerabilidades característico del Escenario 3, en el cual el clima interactúa con fragilidades tecnológicas y económicas para generar rupturas continuas.

La cuarta implicación destaca el papel estratégico de una seguridad convergente que sobrepasa los límites tradicionales de la seguridad corporativa. La separación entre lo físico y lo cibernético — y entre lo público y lo privado — ha dejado de ser adecuada para lidiar con amenazas híbridas en entornos ciberfísicos. Redes ilícitas utilizan información digital para ataques físicos; grupos criminales infiltran cadenas logísticas y explotan plataformas digitales para extorsión; eventos climáticos exponen vulnerabilidades tanto en sistemas industriales como en infraestructuras públicas. En este contexto, la protección exige una actuación integrada que articule Estado, empresas y sociedad, combinando seguridad física, seguridad cibernética, protección de datos, inteligencia contra amenazas y mecanismos de gobernanza reputacional. Modelos como Centros de Operaciones de Seguridad convergentes — que integran monitoreo público y privado — y controles industriales robustos (incluyendo ICS-5) se vuelven esenciales para garantizar resiliencia ciberfísica, continuidad de servicios esenciales e integridad de los procesos críticos, especialmente cuando eventos multichoque amplían simultáneamente riesgos digitales, físicos e institucionales.

Por último, la quinta implicación deriva del hecho de que la resiliencia organizacional depende de la capacidad de navegar dinámicamente entre escenarios. La región no evoluciona de forma lineal, y las organizaciones pueden experimentar simultáneamente elementos de diferentes cuadrantes. El entorno futuro exigirá decisiones estratégicas ajustables, modelos de operación flexibles y mecanismos de monitoreo continúo basados en indicadores de alerta temprana.

Las organizaciones resilientes serán aquellas capaces de ajustar estrategias rápidamente, utilizar Inteligencia Artificial explicable para analizar contextos complejos e integrar información diversa para anticipar rupturas; inclusive rupturas generadas por choques fiscales, climáticos, tecnológicos o institucionales. El desafío central está en transformar la incertidumbre en capacidad adaptativa y en desarrollar estructuras internas que respondan con velocidad, coherencia e inteligencia a los cambios del entorno externo. En conjunto, estas cinco implicaciones componen la base de la capacidad regional de enfrentar riesgos híbridos, construir estructuras de protección sistémica y fortalecer la resiliencia económica, institucional y corporativa. Ellas orientan las transiciones entre los escenarios descritos y preparan el terreno para el análisis detallado de las narrativas, cadenas causales e impactos estratégicos presentados en los capítulos siguientes, incluyendo la dinámica transversal de los estreses multichoque y sus efectos sobre la estabilidad macroeconómica.

02

ESCENARIOS DETALLADOS

2.1. Introducción

O El Capítulo 2 presenta el análisis profundo de los cuatro escenarios estructurados en la Matriz de Escenarios 2026 y más allá. A diferencia del capítulo anterior, que proporcionó una lectura estratégica y comparativa de las lógicas macro que orientan cada cuadrante, esta etapa avanza hacia un nivel operativo y decisorio. El objetivo es detallar cómo cada escenario se manifiesta en la práctica, cuáles son sus cadenas causales, qué riesgos específicos emergen en cada entorno y cómo empresas, gobiernos y organizaciones pueden comprender y responder de forma más eficaz a sus dinámicas.

En esta etapa no hay redundancia con el ítem 1.5. Aquí, profundizamos las variables determinantes por medio del análisis de las fuentes de riesgo predominantes, de las implicaciones sectoriales directas, de los impactos sobre la seguridad corporativa y de la evaluación de los factores que influyen en la continuidad de negocios. Avanzamos también sobre la estructura interna de cada escenario, detallando tensiones, vulnerabilidades y oportunidades que no aparecen en las interpretaciones estratégicas del capítulo anterior. Este enfoque permite que el lector comprenda cómo cada escenario se materializa en lo cotidiano de las operaciones, de la gobernanza y de la infraestructura crítica.

El análisis sigue una estructura uniforme para los cuatro escenarios. Para cada uno de ellos, se presentan: el contexto y sus fundamentos; la cadena causal ampliada que explica cómo interactúan diferentes fuentes de riesgo; los impactos sobre sectores productivos y cadenas críticas; los efectos específicos en la seguridad física, cibernética y reputacional; las implicaciones para la gobernanza, la continuidad y la integridad organizacional; además de los indicadores de alerta temprana que permiten monitorear señales de transición entre escenarios. Finalmente, se identifican oportunidades estratégicas que pueden emerger incluso en contextos adversos o inestables.

Con este enfoque, el Capítulo 2 ofrece un mapa detallado de las trayectorias posibles de riesgo, permitiendo que las organizaciones desarrollen estrategias adaptativas y fortalezcan su resiliencia en un entorno marcado por incertidumbres crecientes e interdependencia entre riesgos físicos, digitales, climáticos e institucionales.

2.2. Escenario 1 – Alianza PragTécnica

2.2.1. Contexto y Fundamentos

El Escenario 1, Alianza PragTécnica, surge de la combinación de dos elementos estructurales: mayor integración regional y avances consistentes en la gobernanza tecnológica. Describe un entorno en el cual los países latinoamericanos logran coordinar políticas de seguridad, comercio, infraestructura y tecnología, creando estándares comunes que reducen la fragmentación regulatoria y fortalecen la capacidad colectiva de enfrentar riesgos transnacionales. Las organizaciones operan en un contexto de previsibilidad moderada, con mecanismos eficientes de interoperabilidad y marcos normativos que evolucionan de forma gradual, pero continua.

Este escenario no representa una integración plena; se trata de un proceso pragmático, basado en acuerdos operativos, protocolos técnicos e iniciativas de cooperación multisectorial mediadas por organismos regionales, sectores empresariales y alianzas público-privadas. La estabilidad institucional, relativa pero creciente, permite inversiones en innovación, infraestructura y protección de datos, creando condiciones más robustas para el desarrollo sostenible y para la competitividad regional.

2.2.2. Cadena Causal Ampliada

La dinámica del Escenario 1 se estructura a partir de una cadena causal compuesta por cinco elementos principales.

Primero, ocurre la armonización gradual de regulaciones de protección de datos, ciberseguridad e Inteligencia Artificial, reduciendo la asimetría jurídica entre países.

Segundo, esta armonización favorece la interoperabilidad entre sistemas públicos y privados, ampliando la capacidad de monitoreo de amenazas y el intercambio seguro de información.

Tercero, la interoperabilidad fortalece mecanismos de prevención y respuesta a incidentes, tanto en el espacio digital como en las operaciones físicas.

Cuarto, la eficiencia de estos mecanismos aumenta la confianza institucional y reduce incentivos para actividades ilícitas, disminuyendo la exposición a fraudes, delitos financieros y ataques coordinados.

Quinto, esta mayor previsibilidad estimula inversiones en innovación, infraestructura y modernización de cadenas productivas, creando un ciclo positivo entre regulación, tecnología y resiliencia.

2.2.3. Fuentes de Riesgo Predominantes en el Escenario

Incluso en un entorno más favorable, tres fuentes de riesgo permanecen predominantes y exigen atención constante.

Primero, riesgos tecnológicos relacionados con la Inteligencia Artificial y la automatización, que exigen gobernanza continua para evitar sesgos, fallas y ataques sofisticados.

Segundo, riesgos geopolíticos y de comercio internacional, dado que América Latina aún depende de mercados externos y está sujeta a volatilidades que pueden afectar cadenas de suministro estratégicas.

Tercero, riesgos climáticos, que continúan presionando infraestructura, agricultura, energía y abastecimiento hídrico, incluso con esfuerzos de adaptación.

Estas fuentes de riesgo no desaparecen; el diferencial de este escenario está en la capacidad de mitigación ampliada, sostenida por coordinación regional e inversiones estructurales.

2.2.4. Implicaciones Sectoriales Directas

El impacto del Escenario 1 varía según el sector. En la industria y en la agricultura, la adopción de tecnologías avanzadas y estándares comunes de ciberseguridad reduce interrupciones y aumenta la productividad.

En el sector financiero, la integración regulatoria fortalece la protección contra delitos digitales y lavado de dinero, ampliando la confianza de los inversores.

En el sector de energía, la cooperación regional facilita la modernización de redes eléctricas, la expansión de fuentes renovables y la implementación de sistemas de monitoreo predictivo basados en Inteligencia Artificial.

En la logística, corredores integrados reducen costos y aumentan la previsibilidad. En salud, educación y servicios públicos, la interoperabilidad permite mayor eficiencia y

calidad.

Con esto, sectores más intensivos en tecnología y operaciones críticas se vuelven más competitivos y resilientes.

2.2.5. Impactos en la Seguridad Corporativa (Física, Cibernética y Reputacional)

La seguridad corporativa en el Escenario 1 adquiere carácter preventivo, integrado y predictivo. La cooperación regional y la gobernanza avanzada de datos reducen la superficie de ataque y fortalecen mecanismos de autenticación, detección y respuesta.

La integración entre seguridad física y cibernética se convierte en estándar, con Centros de Operaciones Convergentes operando tanto para riesgos digitales como para riesgos físicos, ambientales y reputacionales.

Desde el punto de vista operativo, prácticas de seguridad basadas en sensores, análisis conductual, monitoreo continuo y machine learning reducen eventos adversos.

El riesgo reputacional también disminuye, ya que los niveles de confianza institucional y corporativa aumentan.

Además, la mayor transparencia regulatoria facilita auditorías, *certificaciones y due diligence*, protegiendo a las empresas contra riesgos legales y de conformidad.

2.2.6. Impactos en la Gobernanza y en la Continuidad de Negocios

La gobernanza corporativa se fortalece por medio de estándares regionales compartidos, especialmente en la protección de datos, en la gestión de riesgos digitales y en la integración de planes de continuidad entre países.

Las empresas pasan a adoptar políticas de redundancia y adaptación climática alineadas a recomendaciones multilaterales, volviéndose más preparadas para eventos de alta complejidad.

La Inteligencia Artificial explicable y auditable se convierte en parte de la gobernanza interna, reforzando la confianza entre *stakeholders*.

La continuidad de negocios pasa a considerar escenarios transfronterizos, ampliando la capacidad de respuesta a interrupciones climáticas, logísticas o tecnológicas. Planes

integrados de contingencia y cadenas de suministro más diversificadas mitigan riesgos de rupturas inesperadas.

2.2.7. Indicadores Específicos de Alerta Temprana (EWI)

El monitoreo de señales anticipatorias es esencial para detectar posibles desvíos que pueden desplazar el entorno hacia escenarios más adversos. Entre los principales indicadores están:

- Reducción de políticas regionales de interoperabilidad;
- Caídas en el índice de confianza institucional;
- Crecimiento de incidentes cibernéticos que traspasan fronteras;
- Aumento de disputas regulatorias entre países;
- Retrocesos en marcos de gobernanza de dados e IA;
- Fallas energéticas o hídricas recurrentes;
- Reducción de inversiones en innovación e infraestructura crítica.

El deterioro de estos indicadores puede señalar una transición hacia el Escenario 3 o hacia el Escenario 4.

2.2.8. Señales de Transición del Escenario

La Alianza PragTécnica puede debilitarse si existe polarización política, presión fiscal prolongada, retrocesos institucionales o inestabilidad regulatoria. En caso de que estos elementos se intensifiquen, la región puede migrar hacia el Escenario 4 (si el sector privado sostiene la madurez tecnológica) o hacia el Escenario 3 (si el clima y la infraestructura se convierten en las mayores fuentes de ruptura).

2.2.9. Oportunidades Estratégicas

Aun siendo el escenario más favorable, la Alianza PragTécnica contiene oportunidades importantes para ampliar la resiliencia y la competitividad.

Entre ellas están: expansión de mercados digitales integrados; desarrollo de estándares regionales de ciberseguridad y protección de datos; fortalecimiento de redes logísticas inteligentes; avance en energía limpia e infraestructura verde; construcción de plataformas regionales de interoperabilidad; y utilización de Inteligencia Artificial para gobernanza, *compliance* y análisis predictivo.

Las empresas que inviertan en innovación, cooperación institucional y estándares elevados de gobernanza estarán mejor posicionadas para capturar valor y anticipar rupturas.

2.3. Escenario 2 – Redes Sombrías

2.3.1. Contexto y Fundamentos

El Escenario 2, Redes Sombrías, emerge de la combinación entre fragmentación político-institucional y ausencia de gobernanza tecnológica. Describe un entorno en el cual las instituciones públicas pierden capacidad de coerción, regulación y fiscalización, y en el cual redes ilícitas transnacionales expanden su actuación hacia sectores formales de la economía. La erosión de la confianza institucional abre espacio para que grupos criminales, actores privados oportunistas y movimientos clandestinos influencien cadenas económicas, decisiones públicas y flujos financieros.

La ausencia de coordinación regional y la incapacidad de actualizar marcos legales hacen a los Estados más lentos que los agentes ilícitos, que operan con estructuras flexibles, redes digitales descentralizadas y modelos financieros opacos. Este desequilibrio crea un entorno de riesgo permanente, en el cual la imprevisibilidad, la violencia y la manipulación digital se convierten en elementos estructurantes de las relaciones económicas y sociales.

2.3.2. Cadena Causal Ampliada

La evolución del Escenario 2 puede explicarse por la interacción de cinco fenómenos encadenados.

Primero, la fragilidad institucional reduce la capacidad de monitorear delitos financieros, tráfico de datos, corrupción y lavado de dinero, abriendo espacio para la infiltración en sectores críticos.

Segundo, la gobernanza digital inexistente permite que grupos ilícitos usen Inteligencia Artificial para fraudes, *deepfakes*, extorsión y ataques automatizados.
Tercero, la expansión de estas redes compromete cadenas de suministro, creando dependencias invisibles entre sectores formales e informales.

Cuarto, esta inestabilidad afecta la seguridad física, elevando riesgos de violencia, sabotaje y extorsión.

Quinto, el deterioro simultáneo del entorno físico y digital reduce la confianza pública, promueve inestabilidad económica y desestimula inversiones, creando un círculo vicioso difícil de revertir.

2.3.3. Fuentes de Riesgo Predominantes en el Escenario

Tres grandes fuentes de riesgo asumen protagonismo en el Escenario 2. La primera es el crimen organizado transnacional, que opera en múltiples dominios: digital, financiero, logístico, ambiental y político.

La segunda es la desinformación y la manipulación digital basada en Inteligencia Artificial, que se convierten en herramientas estructurales de influencia y extorsión.

La tercera es la fragilidad institucional, que limita la capacidad de respuesta de los Estados y facilita la captura de organismos públicos, empresas estatales, regulaciones estratégicas y procesos de licenciamiento.

Estas fuentes se refuerzan mutuamente, creando un entorno donde amenazas digitales, físicas y reputacionales se manifiestan de forma híbrida y continua.

2.3.4. Implicaciones Sectoriales Directas

En el sector financiero, el aumento de fraudes, lavado de dinero y ocultamiento de activos hace que el riesgo sistémico sea elevado. Operaciones bancarias, medios de pago y ecosistemas de criptoactivos son objetivos frecuentes de redes ilícitas.

En la logística, grupos criminales controlan rutas, intimidan operadores e infiltran cadenas de transporte, elevando costos e inseguridad.

En los agronegocios, parte de la producción es desviada o cooptada por redes criminales que buscan controlar *commodities*, créditos de carbono y rutas de exportación. En el sector energético, robos, sabotaje y manipulación de infraestructura aumentan las interrupciones.

En la minería, la minería ilegal y las presiones territoriales promueven conflictos socioambientales intensos.

Todos los sectores enfrentan riesgos crecientes de coacción, fraude y manipulación digital.

2.3.5. Impactos en la Seguridad Corporativa (Física, Cibernética y Reputacional)

La seguridad corporativa, entendida como función estratégica que integra sus dimensiones física, cibernética, reputacional, entre otras, se convierte en uno de los pilares más críticos para operar en este escenario. La seguridad física enfrenta amenazas directas como secuestros, extorsión, sabotaje y violencia organizada, especialmente contra ejecutivos y equipos de campo. La seguridad cibernética es presionada por ataques automatizados, clones de identidad, *deepfakes* ejecutivos y extorsiones basadas en filtración de datos.

La seguridad reputacional se vuelve volátil debido a campañas coordinadas de desinformación, manipulación política y ataques contra marcas asociados a temas sensibles.

Los modelos tradicionales de seguridad se vuelven insuficientes. Las organizaciones pasan a adoptar estructuras integradas de inteligencia, protección ejecutiva reforzada, análisis conductuales continuos y operaciones coordinadas entre seguridad física, digital y jurídica.

2.3.6. Impactos en la Gobernanza y en la Continuidad de Negocios

La gobernanza corporativa es presionada por la complejidad de riesgos ilegales y por la posibilidad de implicación involuntaria con flujos ilícitos.

Las *due diligences* se vuelven más complejas, las auditorías más frecuentes y las exigencias regulatorias más rigurosas, especialmente de organismos internacionales.

Las empresas enfrentan riesgos jurídicos ampliados si son expuestas a cadenas contaminadas por ilícitos, corrupción o delitos ambientales.

La continuidad de negocios sufre con interrupciones derivadas de sabotaje, extorsión digital, bloqueios logísticos y fluctuaciones políticas intensas.

Las organizaciones necesitan desarrollar planes de contingencia basados en riesgos híbridos, crear redundancias operativas e internalizar capacidades típicas de agencias de inteligencia.

2.3.7. Indicadores Específicos de Alerta Temprana (EWI)

Entre las señales anticipatorias más relevantes están:

- Aumento atípico de delitos financieros transnacionales;
- Expansión de *deepfakes* utilizados para extorsión y manipulación corporativa;
- Instabilidad regulatoria persistente y retrocesos en gobernanza digital;
- Aumento de bloqueos portuarios, interrupciones logísticas y controles informales;
- Crecimiento de la violencia contra ejecutivos y trabajadores esenciales;
- Investigaciones internacionales involucrando cadenas productivas;
- Infiltración creciente de grupos ilícitos em sectores formales.

La intensificación de estas señales indica deterioro acelerado y posible transición hacia estados aún más caóticos.

2.3.8. Señales de Transición del Escenario

El Escenario 2 tiende a agravarse cuando hay colapso de instituciones de justicia, retracción de inversiones internacionales, expansión de delitos ambientales, proliferación de desinformación y aumento de violencia organizada.

Si algunas capacidades institucionales son parcialmente recuperadas o si hay avance aislado de gobernanza digital, el escenario puede migrar hacia el Escenario 4.

En contrapartida, en caso de que eventos climáticos extremos se vuelvan predominantes, puede ocurrir transición hacia el Escenario 3.

2.3.9. Oportunidades Estratégicas

Incluso en un entorno adverso, algunas oportunidades emergen. Sectores ligados a seguridad física, ciberseguridad, análisis de datos, investigación corporativa, protección ejecutiva y soluciones antifraude se fortalecen.

Empresas con gobernanza sólida, excelencia en *compliance* y fuerte cultura de integridad se vuelven más valiosas.

Cadenas productivas capaces de ofrecer trazabilidad, certificaciones robustas y estándares internacionales de ESG ganan ventaja competitiva, especialmente en mercados exigentes.

Organizaciones que inviertan en inteligencia contra amenazas, auditorías tecnológicas, protección integrada y mecanismos avanzados de *due diligence* serán capaces de operar con mayor resiliencia y posicionarse de forma diferenciada incluso en entornos dominados por redes ilícitas.

2.4. Escenario 3 – Clima de Choques

2.4.1. Contexto y Fundamentos

El Escenario 3, Clima de Choques, emerge de la combinación entre cooperación económica moderada y fragilidades estructurales en infraestructura, tecnología y gobernanza climática. La región experimenta avances puntuales en integración comercial y logística, pero falla en crear estándares robustos de resiliencia climática y digital. Con esto, choques ambientales y fallas tecnológicas ocurren de manera cada vez más frecuente y simultánea, produciendo presiones continuas sobre sectores productivos, cadenas de suministro y servicios esenciales.

La inestabilidad climática, traducida en olas de calor intensas, sequías prolongadas, tormentas severas e inundaciones recurrentes, interfiere directamente en la productividad agrícola, en la seguridad energética y en la funcionalidad de las ciudades. Estos eventos interactúan con sistemas tecnológicos frágiles, redes eléctricas sobrecargadas e infraestructura insuficiente, multiplicando impactos y haciendo que el entorno operativo sea imprevisible. Aunque existe alguna cooperación regional, no se traduce en políticas ambientales estructuradas o en inversiones suficientes en adaptación y mitigación.

2.4.2. Cadena Causal Ampliada

La dinámica del Escenario 3 se desarrolla por medio de cinco elementos interconectados. Primero, los eventos climáticos extremos aumentan en intensidad y frecuencia, generando interrupciones en los sistemas de energía, agua y transporte.

Segundo, las fallas en estas infraestructuras críticas comprometen la continuidad de las operaciones industriales, elevando costos, retrasos logísticos y pérdidas de productividad.

Tercero, la fragilidad tecnológica — especialmente en sistemas de supervisión, sensores y redes industriales conectadas — amplifica el impacto de estas interrupciones.

Cuarto, sectores dependientes de energía, agua y logística se vuelven vulnerables a impactos simultáneos, creando ciclos de inestabilidad multisectorial.

Quinto, la falta de políticas públicas consistentes de adaptación climática impide la rápida recuperación, perpetuando vulnerabilidades y forzando a las empresas a internalizar costos de resiliencia.

2.4.3. Fuentes de Riesgo Predominantes en el Escenario

Tres fuentes de riesgo se destacan. La primera es la inestabilidad climática, que actúa como un multiplicador de riesgos y afecta directamente cadenas productivas, infraestructuras y comunidades.

La segunda es la fragilidad de las infraestructuras críticas, especialmente sistemas eléctricos, redes de transporte, saneamiento y telecomunicaciones.

La tercera es la vulnerabilidad tecnológica, que incluye sensores expuestos a altas temperaturas, ICS sensibles a fluctuaciones eléctricas, fallas en conectividad y límites en la capacidad de previsión y respuesta.

Estas fuentes de riesgo se combinan, creando entornos altamente volátiles y sensibles a choques externos.

2.4.4. Implicaciones Sectoriales Directas

En el sector energético, sequías prolongadas e inestabilidad hídrica aumentan la dependencia de termoeléctricas, elevando costos y emisiones. Las interrupciones se vuelven recurrentes.

En los agronegocios, la irregularidad climática reduce la productividad, altera calendarios de siembra y afecta la calidad de los suelos.

En el sector industrial, fluctuaciones de energía y fallas de sensores perjudican operaciones continuas.

En la logística, carreteras, ferrocarriles y puertos son interrumpidos con frecuencia debido a inundaciones, incendios o inclemencias del tiempo.

En la minería, inundaciones, colapsos estructurales y conflictos socioambientales

hacen que las operaciones sean más complejas.

En el sector urbano, crisis de agua y calor extremo amplían riesgos sanitarios y presiones sobre la infraestructura urbana.

Todos los sectores enfrentan volatilidad operativa y aumento de costos con resiliencia.

2.4.5. Impactos en la Seguridad Corporativa (Física, Cibernética y Reputacional)

La seguridad corporativa en este escenario es presionada por eventos ambientales extremos que provocan desplazamientos poblacionales, conflictos territoriales y aumento de delitos oportunistas en áreas severamente afectadas.

La seguridad física necesita lidiar con evacuaciones, riesgos de integridad para equipos de campo y protección de activos expuestos a incendios, inundaciones o deslizamientos.

La seguridad cibernética enfrenta desafíos derivados de la inestabilidad eléctrica, fallas de conectividad y aumento de ataques que explotan momentos de desorganización operativa.

Ataques a la cadena de suministro digital se vuelven más frecuentes, aprovechando la vulnerabilidad momentánea de las organizaciones durante eventos climáticos severos.

El riesgo reputacional aumenta en sectores asociados a impactos ambientales o a la falla en responder adecuadamente a crisis, elevando demandas por transparencia, responsabilidad socioambiental y comunicación eficaz.

2.4.6. Impactos en la Gobernanza y en la Continuidad de Negocios

La gobernanza corporativa necesita incorporar métricas avanzadas de adaptación climática, impacto socioambiental y gestión de crisis.

Planes de continuidad se vuelven más complejos, exigiendo redundancias energéticas, estrategias de diversificación hídrica y mecanismos de respuesta rápida basados en monitoreo predictivo.

Las empresas necesitan integrar datos climáticos en tiempo real con modelos de análisis predictivo, combinando previsión meteorológica avanzada con Inteligencia

Artificial para detectar anomalías y anticipar impactos.

La continuidad de negocios pasa a depender de redundancias estructurales y energéticas, alianzas regionales y diversificación logística.

Las empresas que no invierten en resiliencia climática enfrentan interrupciones prolongadas y pérdida de competitividad.

2.4.7. Indicadores Específicos de Alerta Temprana (EWI)

Señales anticipatorias esenciales incluyen:

- Aumento de la frecuencia y severidad de eventos climáticos extremos;
- Declive prolongado de niveles de embalses y acuíferos;
- Interrupciones eléctricas recurrentes y sobrecarga de redes;
- Fallas simultáneas en sensores, ICS y redes industriales;
- Aumento de pérdidas operativas en cadenas logísticas;
- Crecimiento de costos con seguros e indemnizaciones;
- Expansión de conflictos por agua o energía;
- Inestabilidad de precios de *commodities* sensibles al clima.

La persistencia de estos indicadores refuerza la transición hacia ciclos de choque continuo.

2.4.8. Señales de Transición del Escenario

El Escenario 3 puede migrar rápidamente hacia el Escenario 2 si eventos extremos son explotados por redes ilícitas, ampliando la criminalidad en regiones afectadas.

Puede transitar hacia el Escenario 4 en caso de que el sector privado avance significativamente en resiliencia tecnológica, mientras el Estado permanezca incapaz de modernizar su infraestructura ambiental.

Puede aproximarse al Escenario 1 en caso de que inversiones robustas en adaptación climática e infraestructura verde se consoliden regionalmente.

2.4.9. Oportunidades Estratégicas

Incluso en un entorno adverso, surgen oportunidades importantes. La innovación en

gestión hídrica, infraestructura verde, energía renovable y agricultura resiliente gana tracción.

Tecnologías de previsión ambiental, análisis predictivo e Inteligencia Artificial aplicada al clima se vuelven altamente valoradas.

Modelos de seguro paramétrico, créditos de resiliencia y fondos climáticos se expanden.

Empresas con capacidad de desarrollar cadenas sostenibles, comunicación de riesgo transparente y acciones robustas de adaptación conquistarán mercados y reputación.

Organizaciones que prioricen la resiliencia ambiental y la integración tecnológica estarán mejor posicionadas para enfrentar el Clima de Choques y mitigar rupturas repetitivas.

2.5. Escenario 4 – Datos con Trabas, Fronteras Abiertas

2.5.1. Contexto y Fundamentos

El Escenario 4, denominado Datos con Trabas, Fronteras Abiertas, describe un entorno caracterizado por madurez tecnológica elevada en el sector privado e inestabilidad persistente en las instituciones públicas. Se trata de un futuro en el cual la capacidad empresarial de innovar, proteger datos y operar con estándares avanzados de seguridad supera ampliamente la capacidad de los Estados de regular, fiscalizar y proveer servicios críticos. La región experimenta un desajuste entre la fuerza de las empresas en tecnología y la fragilidad de los gobiernos para asegurar estabilidad política, jurídica e institucional.

En este escenario, la gobernanza de Inteligencia Artificial y protección de datos avanza de forma desigual. Grandes organizaciones se convierten en referencia en auditoría algorítmica, explicabilidad de modelos y ciberseguridad de alto nivel, mientras el Estado se muestra incapaz de seguir el ritmo tecnológico o de estandarizar exigencias regulatorias. Como resultado, el entorno presenta alta asimetría de protección, en la cual entornos corporativos son significativamente más seguros que el entorno institucional y social que los rodea.

2.5.2. Cadena Causal Ampliada

La dinámica del Escenario 4 emerge de la combinación de cinco factores principales. Primero, el sector privado avanza rápidamente en digitalización, Inteligencia Artificial, automatización y seguridad convergente, adoptando estándares elevados como ICS 5 y centros integrados de monitoreo.

Segundo, la inestabilidad institucional impide que los gobiernos creen marcos legales consistentes, actualizados y aplicables regionalmente, generando entornos regulatorios fragmentados.

Tercero, esta fragmentación estimula a las empresas a internalizar mecanismos de gobernanza, creando normas privadas que se convierten en referencia para proveedores y socios.

Cuarto, la desigualdad tecnológica aumenta y cadenas productivas menos capitalizadas permanecen vulnerables a ataques, fraudes e interrupciones.

Quinto, la ausencia de políticas públicas robustas amplía tensiones sociales y territoriales, creando zonas de volatilidad que conviven con áreas altamente protegidas controladas por organizaciones privadas.

2.5.3. Fuentes de Riesgo Predominantes en el Escenario

Tres fuentes de riesgo se destacan. La primera es la inestabilidad institucional, marcada por cambios abruptos de orientación política, volatilidad regulatoria y dificultad de ejecución estatal.

La segunda es la desigualdad tecnológica, que crea ecosistemas híbridos con empresas altamente protegidas y entornos públicos frágiles.

La tercera es el riesgo cibernético avanzado, alimentado por ataques de automatización, explotación de vulnerabilidades y uso indebido de Inteligencia Artificial por agentes oportunistas.

Estas fuentes de riesgo se combinan y refuerzan la asimetría entre sectores resilientes y sectores expuestos.

2.5.4. Implicaciones Sectoriales Directas

En el sector de tecnología y servicios financieros, la innovación avanza rápidamente gracias a ecosistemas corporativos altamente protegidos.

En el sector industrial, empresas con madurez OT avanzada logran operar con estabilidad, mientras pequeñas y medianas industrias sufren interrupciones frecuentes.

En la logística, cadenas integradas por grandes operadores son resilientes, pero regiones dependientes de infraestructura pública enfrentan fallas recurrentes.

En el sector de energía, empresas privadas adoptan microgeneración, redes inteligentes, redundancias y sistemas predictivos, mientras que la infraestructura pública permanece vulnerable a fallas y ataques.

En el retail y servicios urbanos, la desigualdad digital crea entornos de hiperprotección corporativa y vulnerabilidad comunitaria simultánea.

Esta dinámica amplía la distancia entre sectores con alta capacidad de inversión y sectores que dependen de la estabilidad institucional.

2.5.5. Impactos en la Seguridad Corporativa (Física, Cibernética y Reputacional)

La seguridad corporativa asume un papel central en este escenario. La seguridad física es reforzada por sistemas de videovigilancia inteligente, control avanzado de accesos, perímetros reforzados e integración con sistemas digitales de detección. Las empresas se convierten en entornos altamente protegidos, funcionando como islas de estabilidad.

La seguridad cibernética opera con estructuras sofisticadas de prevención y respuesta, integrando *machine learning*, análisis conductual y controles segmentados de redes críticas.

La seguridad reputacional pasa a depender de la capacidad de las organizaciones de demostrar gobernanza transparente, estándares éticos de Inteligencia Artificial y prácticas consistentes de protección de datos.

Las empresas se convierten en agentes de protección central ante la fragilidad del aparato estatal.

2.5.6. Impactos en la Gobernanza y en la Continuidad de Negocios

La gobernanza corporativa necesita internalizar funciones que, en entornos más estables, serían desempeñadas por el Estado.

Con esto, las empresas definen sus propias normas de conformidad, estándares de auditoría, criterios de protección de datos, protocolos de ciberseguridad y mecanismos de integridad digital.

Planes de continuidad incluyen redundancias energéticas, redes privadas de telecomunicaciones, centros de respuesta distribuidos y sistemas avanzados de recuperación.

Las organizaciones necesitan anticipar volatilidades regulatorias, cambios de gobierno, restricciones sectoriales e impactos sociales relacionados con la desigualdad de infraestructura pública.

La resiliencia se construye internamente y se suplementa mediante alianzas estratégicas entre empresas.

2.5.7. Indicadores Específicos de Alerta Temprana (EWI)

Algunas señales anticipatorias relevantes incluyen:

- Retrocesos en marcos regulatorios de protección de datos o Inteligencia Artificial;
- Aumento de ataques cibernéticos sofisticados contra empresas de mediano tamaño;
- Crecimiento de la diferencia entre entornos corporativos protegidos y entornos públicos vulnerables;
- Uso creciente de normas privadas como referencia regulatoria;
- Instabilidad política persistente o polarización ampliada;
- Interrupciones repetidas en infraestructuras públicas esenciales;
- Aumento de la dependencia empresarial de servicios privados de energía y telecomunicaciones.

Estas señales ayudan a anticipar la intensificación de las asimetrías de este escenario.

2.5.8. Señales de Transición del Escenario

El Escenario 4 puede evolucionar hacia el Escenario 1 si la cooperación institucional aumenta y los marcos regulatorios avanzan.

También puede aproximarse al Escenario 2 si redes ilícitas explotan fragilidades institucionales y amplían la captura de sectores públicos.

En caso de que eventos climáticos se vuelvan más intensos y frecuentes, el escenario puede deslizarse parcialmente hacia el Escenario 3.

2.5.9. Oportunidades Estratégicas

El escenario presenta importantes oportunidades empresariales. Tecnologías avanzadas de ciberseguridad, protección de datos, automatización defensiva, integración OT-IT, Inteligencia Artificial explicable y auditoría algorítmica se vuelven extremadamente valoradas.

Soluciones de energía distribuida, infraestructura privada, redes independientes y centros de monitoreo convergente amplían la competitividad.

Empresas con gobernanza sólida y estándares avanzados de resiliencia se convierten en polos de confianza regional, atrayendo inversiones y alianzas.

Incluso en un entorno institucional frágil, la innovación tecnológica permite el surgimiento de ecosistemas privados altamente resilientes y competitivos.

03

IMPLICACIONES ESTRATÉGICAS POR SECTOR

3.1. Introducción

El análisis sectorial que compone el Capítulo 3 presenta las implicaciones prácticas de los escenarios prospectivos para los principales sectores económicos de América Latina, con especial atención al contexto brasileño. Mientras que los capítulos anteriores identificaron fuentes de riesgo estructurantes, incertidumbres críticas y escenarios generales para 2026 y más allá, esta etapa tiene como objetivo traducir estas dinámicas en impactos directos sobre cadenas productivas, regulaciones, infraestructuras, operaciones corporativas y mercados específicos.

América Latina, a pesar de compartir tendencias globales como la digitalización acelerada, la presión climática creciente y la complejidad del entorno de seguridad, presenta características propias que amplifican o redireccionan la forma en que los riesgos se materializan en cada sector. La combinación entre fragilidad institucional, desigualdades estructurales, dependencia de commodities, heterogeneidad regulatoria y exposición a redes ilícitas produce un mosaico de vulnerabilidades y oportunidades que no son uniformes en relación con el escenario global. Brasil, por su parte, debido a su dimensión económica, energética y territorial, ejerce un papel determinante en la configuración de estas dinámicas regionales y en la evolución de las cadenas productivas continentales.

La lógica de este capítulo es profundizar, sector por sector, en cómo las fuentes de riesgo identificadas en los ítems 1.3 y 1.4 y cómo las combinaciones prospectivas de los escenarios del ítem 1.5 moldean la toma de decisiones a corto y mediano plazo. El enfoque privilegia una lectura operativa y comparativa, destacando no solo riesgos y fragilidades, sino también las oportunidades estratégicas que emergen incluso en contextos adversos. El análisis incorpora elementos de tecnología, clima, gobernanza, integridad, crimen organizado, dinámica geopolítica, madurez de Inteligencia Artificial, continuidad de negocios y resiliencia de infraestructuras, siempre con foco en lo que es más relevante para cada sector.

Otro aspecto central de este capítulo es la comparación sistemática con otras regiones del mundo, en especial Estados Unidos, la Unión Europea y Asia. Esta comparación permite dimensionar la posición relativa de América Latina frente a entornos que poseen niveles más altos o bajos de gobernanza tecnológica, madurez institucional, resiliencia climática y seguridad de infraestructura. Este contraste es fundamental para comprender dónde están las asimetrías y dónde surgen oportunidades de convergencia o de diferenciación competitiva.

Cada subsección del capítulo sigue una estructura uniforme para facilitar el análisis

comparado entre sectores. Cada sector será examinado según cinco dimensiones principales: riesgos predominantes, impactos climáticos y tecnológicos, implicaciones específicas para América Latina y Brasil, comparación con las principales regiones del mundo y oportunidades estratégicas derivadas de estos movimientos. A continuación, se presenta una tabla de síntesis que destaca los puntos centrales del análisis y permite una visualización consolidada de las tensiones y vectores estratégicos de ese sector.

Con este enfoque, la Sección 3.0 establece el punto de partida para una lectura sectorial que conecta los escenarios prospectivos con los desafíos y oportunidades de cada cadena económica. La intención es ofrecer un marco analítico sólido que permita la toma de decisiones basada en evidencia, la anticipación de rupturas y la formulación de estrategias de resiliencia alineadas con las transformaciones estructurales de la región.

3.2. Sector Industrial y Manufactura

3.2.1. Riesgos Predominantes

El sector industrial y de manufactura enfrenta un conjunto de riesgos estructurales que se intensifican en 2026 y más allá, impulsados por factores climáticos, tecnológicos, logísticos y geopolíticos. Entre los riesgos más relevantes están las interrupciones en la cadena de suministro, fluctuaciones en el suministro de energía, ataques cibernéticos dirigidos a sistemas industriales, competencia global asimétrica, alta dependencia de insumos críticos y vulnerabilidades derivadas de la integración entre tecnología operativa (OT) y tecnología de la información (IT).

En el contexto latinoamericano, estos riesgos asumen contornos específicos debido a la mayor dependencia de *commodities*, la fragilidad de infraestructuras críticas, la menor estandarización tecnológica y la madurez irregular de la gobernanza digital entre países. En Brasil, factores como la volatilidad tributaria, los costos logísticos elevados y la exposición climática acentúan desafíos que influyen directamente en la competitividad de la industria.

Las tensiones geopolíticas globales, la disputa por minerales estratégicos y los cuellos de botella logísticos persistentes aumentan la presión sobre el sector, exigiendo mayor capacidad de adaptación y de anticipación de riesgos. Al mismo tiempo, la proliferación de fraudes, sabotajes corporativos y ataques a sistemas industriales exige niveles crecientes de seguridad convergente.

3.2.2. Impactos Climáticos, Tecnológicos y Operativos

Los impactos climáticos se vuelven cada vez más determinantes para el sector industrial. Las olas de calor extremo afectan la productividad de los trabajadores, reducen la vida útil de componentes industriales y provocan fallas en sistemas de refrigeración. Las sequías prolongadas comprometen operaciones que dependen del agua para procesos industriales, como metalurgia, papel y celulosa, bebidas e industrias químicas. Los eventos extremos aumentan el riesgo de interrupción energética, creando inestabilidad en líneas de producción sensibles a variaciones eléctricas.

La dimensión tecnológica presenta impactos igualmente significativos. La aceleración de la digitalización y de la automatización aumenta la eficiencia, pero expone los sistemas industriales a riesgos cibernéticos sofisticados. Ataques a Sistemas de Control Industrial (ICS) pueden provocar paralizaciones críticas, daños a equipos, alteraciones indetectables en parámetros operativos y riesgos de seguridad para los trabajadores. Las vulnerabilidades en sensores, redes industriales y sistemas de telemetría elevan la probabilidad de eventos simultáneos entre fallas digitales y físicas.

Desde el punto de vista operativo, los cuellos de botella logísticos, las oscilaciones en el precio de insumos y la dependencia de cadenas largas aumentan la volatilidad de los costos. La adopción de tecnologías avanzadas de manufactura depende de la estabilidad energética, la madurez digital y la capacidad de inversión, que varían significativamente entre países latinoamericanos. Estos factores definen un escenario de competitividad desigual, en el cual las empresas de mayor tamaño avanzan mientras que las pequeñas y medianas enfrentan dificultades para seguir el ritmo tecnológico.

3.2.3. Implicaciones Específicas para Brasil y América Latina

América Latina presenta un conjunto de vulnerabilidades estructurales que amplifican riesgos para el sector industrial, especialmente en comparación con el escenario global. La región depende fuertemente de una infraestructura logística y energética limitada, con exposición significativa a eventos climáticos extremos y variaciones hídricas. Este contexto afecta directamente la productividad industrial, crea incertidumbres operativas y reduce la previsibilidad de las inversiones.

En Brasil, aunque existe una base industrial diversificada, desafíos como la volatilidad regulatoria, la complejidad tributaria, la infraestructura deficiente y el riesgo climático elevado crean obstáculos adicionales. La dependencia de la matriz hidroeléctrica hace

al país especialmente vulnerable a las sequías, y la creciente urbanización presiona los sistemas de agua, energía y movilidad. La exposición a redes ilícitas, fraudes, conflictos territoriales y presiones ambientales también interfiere en cadenas productivas estratégicas.

La baja estandarización digital entre empresas y sectores dificulta la adopción de tecnologías de manufactura avanzada y amplía la desigualdad de madurez tecnológica entre grandes industrias y pequeñas fábricas. La ausencia de una política industrial regional coordinada reduce sinergias y limita las economías de escala que son esenciales para competir con economías maduras.

Al mismo tiempo, América Latina posee ventajas competitivas, como abundancia de recursos naturales, potencial energético renovable, capacidad logística transcontinental y proximidad geográfica con grandes mercados. Estas oportunidades, sin embargo, exigen inversiones estructurales para ser convertidas en resiliencia y competitividad.

3.2.4. Comparación con Estados Unidos, Unión Europea y Asia

En relación con Estados Unidos, América Latina presenta brechas relevantes en infraestructura logística, automatización industrial, resiliencia energética y seguridad OT-IT. Mientras que el mercado norteamericano opera con madurez elevada en automatización avanzada, redes industriales inteligentes e integración con IA defensiva, los países latinoamericanos aún enfrentan inestabilidades básicas de suministro y conectividad.

En comparación con la Unión Europea, la brecha reside principalmente en la gobernanza climática, en la regulación tecnológica y en la integración regional. Europa avanza rápidamente en normas robustas de protección de datos, auditoría algorítmica, seguridad industrial y estándares ambientales rigurosos. América Latina, por otro lado, ha avanzado de forma desigual en la adopción de estos marcos, creando entornos regulatorios fragmentados e imprevisibles.

En relación con Asia, la competitividad latinoamericana se ve perjudicada por la menor eficiencia logística, la falta de clústeres industriales integrados y la baja madurez tecnológica en pequeñas y medianas industrias. Asia opera con cadenas productivas diversificadas, centros de manufactura distribuidos y capacidad tecnológica elevada. La falta de infraestructura adecuada en América Latina limita la expansión de cadenas productivas globales en la región.

A pesar de estas diferencias, América Latina posee ventajas relevantes en el contexto global: proximidad con fuentes de energía renovable, disponibilidad de materiales estratégicos, espacio para expansión industrial sostenible y oportunidad de desarrollar *clústeres* industriales avanzados con foco en tecnologías verdes, bioeconomía y cadenas productivas digitales.

3.2.5. Oportunidades Estratégicas

Incluso ante desafíos estructurales significativos, el sector industrial de América Latina posee oportunidades estratégicas importantes para reposicionarse con mayor competitividad global. Inversiones en automatización defensiva, Inteligencia Artificial explicable, manufactura avanzada, integración OT-IT y resiliencia climática pueden elevar la calidad y eficiencia de las cadenas productivas regionales.

El fortalecimiento de normas industriales armonizadas entre países latinoamericanos amplía la previsibilidad y facilita la integración regional. La modernización de sistemas energéticos con fuentes renovables y redes inteligentes aumenta la seguridad operativa y reduce costos. La creación de corredores logísticos resilientes, parques industriales sostenibles y ecosistemas de innovación se vuelve esencial para atraer inversiones a largo plazo.

En Brasil, políticas industriales orientadas a la descarbonización, productividad, infraestructura crítica y transición energética pueden posicionar al país como referencia continental. Tecnologías de previsión ambiental, sensores avanzados, sistemas de monitoreo y herramientas de análisis predictivo tienen el potencial de transformar vulnerabilidades climáticas en ventaja competitiva.

Las industrias que adopten estándares elevados de resiliencia, seguridad convergente y gobernanza tecnológica estarán mejor preparadas para enfrentar rupturas y capturar valor en mercados globales que exigen transparencia, integridad y sostenibilidad.

Tabla 4 – Síntesis: Sector Industrial y Manufactura

Dimensión	Brasil y América Latina	Estados Unidos	Unión Europea	Asia
Infraestructura logística	Limitada, con cuellos de botella significativos	Alta integración nacional	Alta estandarización y eficiencia	Elevada capacidad, clústeres consolidados
Madurez OT / IT	Baja a media, con desigualdades sectoriales	Alta, con integración avanzada	Alta, con gobernanza fuerte	Muy alta, especialmente en la manufactura
Exposición climática	Alta, con sequías, inundaciones y olas de calor	Media	Media a alta, pero con mejor adaptación	Alta en algunos países, moderada en otros
Gobernanza tecnológica	Heterogénea y fragmentada	Madura y consolidada	Rígida y armonizada	Variable, pero avanzada en grandes economías
Seguridad industrial	Vulnerable a ataques y fallas estructurales	Alta protección, ICS desarrollados	Estándares fuertes de seguridad	Ciberseguridad y protección digital robusta

3.3. Energía, Infraestructuras Críticas y Utilities

3.3.1. Vulnerabilidades Estructurales

El sector de energía y de infraestructuras críticas concentra algunos de los riesgos más significativos para la estabilidad económica y social de América Latina. La región presenta heterogeneidad en la calidad de las redes eléctricas, fuerte dependencia hídrica, baja redundancia estructural, elevada exposición a eventos climáticos extremos y madurez desigual en la protección de Sistemas de Control Industrial. Este conjunto de características produce un entorno en el cual fallas puntuales pueden provocar interrupciones a gran escala, afectando industrias, hospitales, sistemas de transporte, telecomunicaciones y servicios esenciales.

En Brasil, la dependencia de la matriz hidroeléctrica hace que el sector sea particularmente sensible a ciclos de sequía, a la irregularidad de las lluvias y al agotamiento de embalses. La expansión de fuentes renovables ocurre a un ritmo acelerado, pero aún con limitaciones de integración plena al sistema energético. La fragilidad de infraestructuras antiguas, la falta de inversiones continuas y la dificultad de modernización de redes de transmisión crean riesgos de interrupciones sistémicas.

Además, el sector enfrenta vulnerabilidades estructurales relacionadas con presiones criminales. Sabotajes, vandalismo, robos de cables, interferencias en subestaciones e infiltración de redes ilícitas en contratos públicos amplían riesgos y elevan costos operativos. La convergencia entre crimen organizado, eventos climáticos y fragilidad tecnológica hace de la seguridad de infraestructuras críticas un desafío central.

3.3.2. Presiones Climáticas y Digitales

Los eventos climáticos extremos ejercen un impacto progresivamente más severo sobre el sector de energía. Las sequías prolongadas reducen la capacidad de las hidroeléctricas, exigiendo el accionamiento de emergencia de termoeléctricas y presión sobre las tarifas. Las inundaciones y tormentas dañan torres de transmisión, aíslan comunidades y comprometen la distribución. Las olas de calor provocan picos de consumo que sobrecargan redes que ya operan por encima de los estándares internacionales de eficiencia.

Desde el punto de vista digital, el sector enfrenta riesgos crecientes asociados a ataques cibernéticos y manipulación de sistemas críticos. Los Sistemas de Supervisión y de Control Industrial son objetivos frecuentes de agentes maliciosos que buscan causar interrupciones, secuestrar datos, alterar parámetros de generación y transmisión o comprometer sistemas de telemetría. Las fallas coordinadas pueden afectar simultáneamente sectores interdependientes, como saneamiento, telecomunicaciones y transporte.

La convergencia entre fallas digitales y eventos climáticos intensifica la probabilidad de colapso operativo. Un ataque cibernético durante una crisis hídrica, por ejemplo, puede llevar a la interrupción prolongada de energía, afectando hospitales, redes de refrigeración, servicios de emergencia y operaciones industriales críticas. Este tipo de riesgo híbrido se ha vuelto más frecuente y demanda nuevos enfoques de protección.

3.3.3. Desafíos para Brasil y América Latina

América Latina enfrenta desafíos estructurales que hacen del sector de energía uno de los más vulnerables de la región. La alta dependencia hídrica en países como Brasil, Colombia y Perú amplifica riesgos operativos ante variaciones climáticas. La falta de redes inteligentes, la baja digitalización de campo, la ausencia de redundancias y la deficiente capacidad de almacenamiento reducen la resiliencia del sistema eléctrico.

En Brasil, desafíos adicionales incluyen redes envejecidas, disputas regulatorias, vulnerabilidades en contratos de concesión, exposición a fraudes y logística limitada para la expansión de generación renovable. La dependencia de combustibles fósiles en períodos de crisis hídrica amplía costos y presiona metas de descarbonización.

La desintegración regional en términos regulatorios complica la posibilidad de integración energética plena entre países latinoamericanos. Los proyectos de interconexión avanzan lentamente debido a la inestabilidad política, dificultades fiscales y riesgos de captura regulatoria. Este escenario reduce oportunidades de intercambio energético y amplía vulnerabilidades locales.

3.3.4. Comparación Global

En comparación con Estados Unidos, América Latina presenta redes eléctricas menos redundantes, menor capacidad de almacenamiento de energía y cobertura limitada de redes inteligentes. Estados Unidos posee mayor robustez regulatoria, capacidad de respuesta rápida y mejor integración entre energía, telecomunicaciones y seguridad digital.

En relación con la Unión Europea, la brecha es aún mayor. Europa invirtió fuertemente en gobernanza climática, transición energética y resiliencia de Redes Inteligentes (Smart Grids), con integración regional avanzada y capacidad significativa de interconexión transfronteriza. América Latina, a su vez, opera con estructuras desconectadas y amplia variación de madurez entre países.

Cuando se compara con Asia, América Latina enfrenta dos desafíos principales: menor escala industrial y menor capacidad de inversión pública y privada en infraestructura crítica. Países como China, Corea del Sur y Japón poseen sistemas altamente digitalizados e integrados, con fuerte presencia de Inteligencia Artificial para monitoreo predictivo. América Latina aún opera con alto grado de mantenimiento correctivo y vulnerabilidad climática.

3.3.5. Oportunidades

A pesar de las fragilidades, la región presenta oportunidades estratégicas relevantes. La expansión de energía renovable, especialmente solar, eólica, biomasa e hidrógeno verde posiciona a América Latina como una de las regiones con mayor potencial de transición energética en el mundo. Brasil y Chile se destacan como protagonistas naturales en este movimiento.

El sector posee la oportunidad de avanzar en la implementación de redes inteligentes, sistemas avanzados de monitoreo y control, sensores distribuidos, automatización defensiva y redundancias estructurales. Tecnologías emergentes de almacenamiento, previsión climática basada en Inteligencia Artificial, integración OT-IT y expansión de generación distribuida pueden elevar significativamente la resiliencia del sistema.

La creación de corredores energéticos regionales, además de la modernización de subestaciones, monitoreo de las líneas de transmisión y fortalecimiento de la seguridad física y digital, puede generar ventajas competitivas y permitir la integración estratégica con mercados globales interesados en energía baja en carbono.

Tabla 5 – Síntesis: Energía e Infraestructuras Críticas

Dimensión	Brasil y América Latina	Estados Unidos	Unión Europea	Asia
Matriz energética	Predominancia hídrica y renovable, pero vulnerable	Diversificada y resiliente	Alta integración renovable	Fuerte expansión renovable
Digitalización	Baja a media	Alta	Muy alta	Avanzada
Redundancia eléctrica	Limitada	Alta	Alta	Media a alta
Exposición climática	Muy alta	Media	Media	Variable
Seguridad digital	Vulnerable	Robusta	Estandarizada	Avanzada
Oportunidades	Renovables, redes inteligentes, IA climática	Innovación, hidrógeno	Transición verde	Industrialización y digitalización

3.4. Agronegocios y Alimentos

En América Latina, los agronegocios y la biotecnología constituyen una extensión de la infraestructura crítica nacional. Laboratorios de semillas, centros de genética, estaciones de investigación, biofábricas y ensayos de campo integran cadenas altamente sensibles al espionaje industrial, sabotaje, activismo violento y biocrímenes. Estos activos, por influir en la seguridad alimentaria, la competitividad global y la soberanía tecnológica, amplían la superficie crítica de riesgo y exigen enfoques de seguridad convergente y protocolos específicos de protección.

3.4.1. Riesgos Climáticos y Logísticos

El agronegocio latinoamericano es uno de los sectores más expuestos a las transformaciones estructurales que moldean el entorno global en 2026 y más allá. La región, responsable de parte expresiva del suministro mundial de granos, proteínas,

fibras y alimentos procesados, enfrenta riesgos crecientes relacionados con la variabilidad climática, la escasez de agua, la intensificación de eventos extremos y presiones regulatorias internacionales sobre deforestación, trazabilidad y sostenibilidad.

Los riesgos climáticos dominan el sector. Sequías prolongadas, inundaciones inesperadas, variaciones bruscas de temperatura e irregularidad de los ciclos de lluvia afectan plantaciones, productividad, calidad del suelo y disponibilidad de agua. Sequías intensas comprometen cultivos sensibles, elevan costos de riego y presionan embalses, mientras tormentas severas provocan erosión, pérdida de cosechas y afectan silos y depósitos. Este escenario se agravará en 2026 y más allá, exigiendo adaptaciones estructurales en toda la cadena productiva.

La dimensión logística también enfrenta presiones significativas. Puertos saturados, carreteras vulnerables a deslizamientos, puentes frágiles, interrupciones ferroviarias y capacidad limitada de almacenamiento crean cuellos de botella operativos que amplían costos y reducen eficiencia. Estos impactos se intensifican durante eventos climáticos severos, cuando las carreteras se vuelven intransitables y los puertos enfrentan paralizaciones. La dependencia de rutas únicas en países como Brasil aumenta la probabilidad de rupturas simultáneas.

3.4.2. Presiones Tecnológicas y de Mercado

La aceleración de la digitalización y de la automatización en los agronegocios transforma profundamente el sector, pero también crea nuevos riesgos y desigualdades de capacidad tecnológica. Las empresas con acceso a tecnologías avanzadas logran operar con mayor previsibilidad, mientras que los pequeños y medianos productores permanecen vulnerables a fallas climáticas, volatilidad de precios y riesgos digitales.

El uso de sensores, telemetría, monitoreo satelital, drones y análisis avanzados basados en Inteligencia Artificial se vuelve esencial para prever el rendimiento,

detectar plagas, estimar la productividad y anticipar riesgos. Sin embargo, la desigualdad tecnológica entre grandes conglomerados y productores menores crea asimetrías competitivas y limita la adopción de prácticas de agricultura de precisión.

La presión internacional por estándares ambientales rígidos también se intensifica. Europa y Asia avanzan en exigencias de trazabilidad, comprobación de origen sostenible, certificaciones ambientales y reducción de emisiones en toda la cadena. Estas exigencias pueden funcionar como barreras no arancelarias para una parte significativa de la producción latinoamericana, especialmente en países donde la deforestación ilegal y la fragilidad de la fiscalización ambiental permanecen como desafíos estructurales.

3.4.3. Implicaciones Regionales

América Latina, por ser una potencia agroalimentaria global, enfrenta implicaciones económicas, ambientales e institucionales de gran magnitud. La región posee ventajas naturales como tierras fértiles, clima tropical, disponibilidad de agua y alta productividad relativa, pero estas ventajas se ven comprometidas por vulnerabilidades relacionadas con el clima, la infraestructura y la gobernanza ambiental.

En Brasil, los agronegocios son responsables de una parte significativa del PIB, de las exportaciones y del empleo rural. Por lo tanto, las interrupciones climáticas, las exigencias regulatorias internacionales o las fallas logísticas tienen impacto directo sobre la economía nacional. La presión por la trazabilidad de la cadena bovina, el control de la deforestación y la comprobación de conformidad ESG ya produce efectos tangibles y debe intensificarse en los próximos años.

A estas presiones externas se suma la inseguridad jurídica, que permanece como un vector crítico de vulnerabilidad para el agronegocio latinoamericano. Cambios abruptos en marcos regulatorios, disputas tributarias, judicialización recurrente y asimetrías normativas entre países reducen la previsibilidad, amplían los costos de conformidad y afectan las decisiones de inversión a largo plazo. Estos factores comprometen la competitividad regional, crean barreras adicionales al acceso a mercados y hacen de la gobernanza jurídica un elemento central de la resiliencia del sector.

El crimen organizado también está cada vez más presente en el sector. Redes ilícitas actúan en áreas rurales, controlando territorios, minería ilegal, rutas de transporte y áreas de almacenamiento. Esto crea riesgos físicos y reputacionales para empresas y productores, además de ampliar la probabilidad de contaminación de la cadena por

actividades ilegales.

La escasez hídrica emergente en regiones productivas de Argentina, Brasil, Paraguay y México aumenta tensiones territoriales y demanda inversiones urgentes en riego sostenible, captación de agua, manejo integrado de cuencas y tecnologías de reutilización.

3.4.4. Comparación con Principales Mercados Globales

América Latina enfrenta distorsiones importantes en comparación con los principales mercados agrícolas globales.

En relación con Estados Unidos, la región presenta menor resiliencia climática, menor integración logística y madurez tecnológica inferior. Estados Unidos posee redes logísticas altamente integradas, sistemas avanzados de riego, gobernanza climática robusta y estabilidad regulatoria amplia.

Comparando con la Unión Europea, la mayor diferencia está en la gobernanza ambiental. Europa posee mecanismos avanzados de certificación, trazabilidad y control de emisiones, lo que le permite ocupar una posición de referencia global en estándares de sostenibilidad. América Latina aún enfrenta dificultades para armonizar prácticas y reducir impactos socioambientales.

En relación con Asia, especialmente China e India, la diferencia es menos tecnológica y más estructural. Asia opera con fuerte integración entre producción, procesamiento y distribución, además de una gran inversión en agricultura de precisión. América Latina posee productividad elevada, pero separada por grandes distancias y dependiente de una infraestructura logística limitada.

A pesar de estas diferencias, América Latina posee una ventaja competitiva significativa en escala productiva, potencial hídrico y capacidad de expansión sostenible, siempre que invierta en modernización logística, reducción de la deforestación y gobernanza ambiental avanzada.

3.4.5. Oportunidades Estratégicas

El sector presenta oportunidades que pueden transformar vulnerabilidades en ventaja competitiva. La expansión de la agricultura de precisión, el uso intensivo de Inteligencia Artificial para la previsión de eventos climáticos y la optimización de la

productividad, y la adopción de sistemas avanzados de monitoreo ambiental son esenciales para elevar la resiliencia y la competitividad.

Inversiones en infraestructura logística, riego sostenible, silos climatizados y redes ferroviarias pueden reducir costos y aumentar la previsibilidad. El desarrollo de cadenas completas de bioeconomía, incluyendo biocombustibles, biomasa y productos bajos en carbono, posiciona a la región como protagonista de la transición energética global.

Brasil puede asumir el liderazgo continental con políticas que integren descarbonización, protección de biomas, trazabilidad digital, innovación en el campo y seguridad jurídica para inversiones privadas. Programas de gobernanza ambiental robusta permiten que los productos latinoamericanos cumplan con las exigencias internacionales y accedan a mercados de alto valor.

Los productores que inviertan en sostenibilidad trazable, agricultura de precisión e integración tecnológica estarán mejor preparados para operar en entornos de riesgo elevado y capturar nuevas oportunidades en mercados globales que valoran el origen, la integridad y la conformidad ambiental.

Tabla 6 – Síntesis: Agronegocios y Alimentos

Dimensión	Brasil y América Latina	Estados Unidos	Unión Europea	Asia
Exposición climática	Muy alta	Media	Media	Variable
Logística	Vulnerable y fragmentada	Altamente integrada	Moderada, pero eficiente	Integrada y creciente
Gobernanza ambiental	Heterogénea e insuficiente	Moderada	Avanzada	Variable
Madurez tecnológica	Media con desigualdades	Alta	Alta	Alta en grandes productores
Vulnerabilidad criminal	Alta en áreas rurales	Baja	Baja	Moderada
Oportunidades	Agricultura de precisión, trazabilidad, bioeconomía, IA climática	Riego avanzado, agro 4.0	Sostenibilidad premium	Escala y automatización

3.5. Logística, Puertos, Carreteras e Infraestructuras Urbanas

3.5.1. Fuentes de Riesgo y Presiones Operativas

La logística latinoamericana enfrenta un conjunto de presiones persistentes que se intensifican en 2026 y más allá, reflejando la combinación entre vulnerabilidades climáticas, fragilidad institucional, deficiencias estructurales y aumento de la actuación de redes ilícitas. La región presenta elevada dependencia de modos viales, infraestructura fragmentada, baja integración multimodal y capacidad limitada de respuesta a choques simultáneos. Eventos climáticos severos, interrupciones eléctricas, bloqueos territoriales e insuficiencia de mantenimiento amplían riesgos operativos y aumentan costos de transporte.

Puertos ubicados en áreas de riesgo climático elevado sufren con inundaciones, elevación del nivel del mar, tormentas e interrupciones intermitentes. La baja profundidad de canales, congestionamientos y limitaciones de dragado también afectan la eficiencia logística. Aeropuertos y ferrocarriles enfrentan desafíos

estructurales como falta de conectividad, baja digitalización y capacidad limitada de integración con sistemas de previsión y monitoreo en tiempo real.

En las áreas urbanas, la expansión desordenada, la insuficiencia de drenaje, la sobrecarga de redes de saneamiento y la fragilidad de sistemas de movilidad crean riesgos adicionales. Inundaciones, deslizamientos, colapsos de laderas e interrupciones en el transporte público comprometen la circulación de personas, mercancías y servicios críticos. Este cuadro se agrava por fallas de planificación urbana y por la ausencia de integración entre políticas de movilidad, vivienda e infraestructura verde.

3.5.2. Implicaciones Regionales

América Latina presenta uno de los costos logísticos relativos más altos del mundo, representando muchas veces entre el 12% y el 18% del PIB, debido a la fragilidad estructural, extensión territorial y baja integración multimodal. La dependencia del modo vial hace a la región extremadamente vulnerable a interrupciones climáticas, incidentes criminales, huelgas y bloqueos. La actuación de redes ilícitas en áreas portuarias, rutas estratégicas y zonas fronterizas crea riesgos físicos y reputacionales para empresas y operadores logísticos.

Brasil enfrenta desafíos particularmente significativos debido a la dimensión continental del territorio y a la concentración de la producción agrícola e industrial

lejos de los principales puertos. La falta de ferrocarriles integrados, la vulnerabilidad de las carreteras a eventos extremos y la insuficiencia de infraestructura portuaria aumentan costos y reducen la competitividad. La dependencia de pocos corredores logísticos afecta directamente la previsibilidad de las exportaciones, especialmente de granos, carnes, minerales y manufacturas.

Infraestructuras urbanas en ciudades como São Paulo, Río de Janeiro, Bogotá, Buenos Aires y Lima enfrentan riesgos crecientes de colapso parcial durante eventos de lluvia extrema, con impactos directos sobre centros financieros, cadenas de suministro y continuidad de servicios esenciales. La ampliación de riesgos urbanos está conectada a la expansión desordenada, al déficit habitacional y a la sobrecarga de sistemas de transporte.

3.5.3. Comparativo Global

En comparación con Estados Unidos, América Latina presenta menor redundancia logística, menor integración multimodal y menor capacidad de respuesta a choques climáticos o ciberataques. Estados Unidos posee ferrocarriles robustos, red de hidrovías eficiente, puertos modernizados y alta capacidad de dragado y monitoreo.

En relación con la Unión Europea, la brecha se concentra en la planificación urbana, la integración transporte-logística y la gobernanza de infraestructura. Europa opera con redes de transporte integradas, políticas sólidas de adaptación climática urbana y fuerte digitalización portuaria. América Latina, por otro lado, permanece con baja interoperabilidad entre modos y alto grado de informalidad en las operaciones.

En comparación con Asia, especialmente China, Japón y Corea del Sur, la región enfrenta desafíos asociados a la baja automatización logística, infraestructura portuaria menos avanzada y limitada inversión pública y privada. Países asiáticos operan con puertos inteligentes, ferrocarriles de alta capacidad, logística integrada con tecnologías emergentes y fuerte uso de Inteligencia Artificial para previsión y optimización.

A pesar de las brechas, América Latina posee potencial estratégico significativo debido a su posición geográfica, abundancia de recursos, proximidad con grandes mercados y oportunidades de expansión logística sostenible. Brasil, con su costa extensa y capacidad productiva, presenta potencial para convertirse en un corredor logístico global si invierte en infraestructura estratégica integrada.

3.5.4. Oportunidades Estratégicas

El sector presenta diversas oportunidades para transformar vulnerabilidades en ventajas competitivas. La digitalización logística con uso de Inteligencia Artificial, sensores distribuidos, *blockchain* para trazabilidad de cargas y sistemas integrados de previsión climática puede elevar significativamente la eficiencia. La expansión de ferrocarriles de alta capacidad, hidrovías interiores, puertos inteligentes y corredores logísticos sostenibles crea nuevos vectores de crecimiento regional.

El desarrollo de infraestructura resiliente, incluyendo drenaje mejorado, urbanismo sostenible, redes eléctricas reforzadas e integración entre movilidad urbana y logística, fortalece la capacidad de respuesta a choques climáticos. Alianzas público-privadas, inversiones en concesiones e integración regulatoria entre países latinoamericanos son fundamentales para elevar la competitividad y reducir costos logísticos.
En Brasil, proyectos estratégicos como Ferrogrão, corredores Norte y Centro-Oeste, modernización de puertos y expansión de hidrovías pueden posicionar al país como polo logístico hemisférico. La adopción de tecnologías de previsión, automatización portuaria y monitoreo integrado permite una ganancia expresiva de eficiencia y reducción de vulnerabilidades.

Tabla 7 – Síntesis: Logística, Puertos, Carreteras e Infraestructuras Urbanas

Dimensión	Brasil y América Latina	Estados Unidos	Unión Europea	Asia
Logística multimodal	Limitada y desigual	Altamente integrada	Integrada y eficiente	Avanzada, automatizada
Vulnerabilidad climática	Alta	Media	Media	Variable
Seguridad en puertos	Alta exposición a ilícitos	Moderada	Alta	Moderada
Digitalización logística	Baja a media	Alta	Muy alta	Avanzada
Infraestructura urbana	Sobrecarga y fragilidad	Resiliente	Planificada	Modernizada
Oportunidades	Corredores logísticos verdes, puertos inteligentes, ferrocarriles	Automatización avanzada	Urbanismo sostenible	Cadenas globales integradas

3.6. Servicios Financieros y Medios de Pago

3.6.1. Presiones Tecnológicas, Delitos Financieros y Riesgos Ilícitos

O El sector de servicios financieros y medios de pago es uno de los más impactados por la transformación digital acelerada, por la expansión de la Inteligencia Artificial y por la evolución de las redes ilícitas transnacionales. Estos factores hacen al sector altamente expuesto a riesgos cibernéticos, fraudes sofisticados, ataques a la infraestructura crítica financiera, manipulación de identidades digitales, lavado de dinero y utilización de sistemas financieros para el movimiento de economías ilícitas.

La innovación en el sector, acelerada por sistemas de pagos instantáneos, *open finance* y múltiples capas de digitalización, eleva no solo la eficiencia de las operaciones, sino también el grado de complejidad de los ataques. Los criminales utilizan herramientas avanzadas de automatización, Inteligencia Artificial generativa e ingeniería social para realizar fraudes a gran escala, simular identidades y explotar vulnerabilidades en APIs, billeteras digitales y sistemas automatizados de análisis de riesgo.

Además de las presiones tecnológicas, el sector enfrenta riesgos estructurales relacionados con la volatilidad macroeconómica, inestabilidad regulatoria, pérdida de confianza digital, presiones internacionales por conformidad y tensiones geopolíticas que afectan el flujo de capitales y el costo de financiamiento. La interacción entre delito financiero, corrupción, contrabando y mercados ilícitos crea un entorno de riesgo híbrido que desafía las estructuras tradicionales de *compliance*.

3.6.2. Impactos en América Latina y Brasil

América Latina es considerada una de las regiones más vulnerables del mundo a estafas digitales, fraudes financieros, explotación de identidades y ataques cibernéticos dirigidos al sector bancario. El crecimiento del uso de pagos digitales, especialmente en poblaciones no totalmente incluidas digitalmente, amplía la superficie de ataque. La ausencia de estandarización regional en regulación financiera y protección de datos intensifica estas vulnerabilidades.

Brasil es simultáneamente referencia global en innovación financiera y uno de los mercados más expuestos a riesgos digitales. El *sistema de pagos instantáneos (Pix)* transformó el sector, pero también abrió espacio para fraudes cada vez más sofisticados que utilizan secuestro digital, ingeniería social, *deepfakes* y manipulación de identidades a gran escala. La madurez de las instituciones financieras brasileñas es elevada, pero la presión sobre sistemas de detección, respuesta y contención aumenta

continuamente.

Además, Brasil enfrenta desafíos relacionados con la infiltración de organizaciones criminales en el sistema financiero por medio de testaferros, empresas fachadas, transacciones de bajo valor repetidas, uso indebido de criptomonedas, fraudes en medios de pago y lavado de dinero conectado a mercados ilícitos como minería ilegal, tráfico de drogas, delitos ambientales y contrabando. Esta convergencia amplía la complejidad de monitoreo y exige modelos avanzados de análisis conductual.

3.6.3. Comparación Global

En comparación con Estados Unidos, América Latina enfrenta mayor exposición a estafas digitales, menor estandarización regulatoria y menor madurez en gobernanza de datos entre empresas de mediano y pequeño tamaño. Estados Unidos posee estructuras robustas de ciberseguridad, regulación más consistente y capacidad de respuesta rápida, aunque también enfrenta un aumento significativo de fraudes con uso de IA.

En relación con la Unión Europea, la brecha se concentra en la protección de datos, trazabilidad de transacciones y estandarización regulatoria. Europa opera con modelos avanzados de gobernanza de IA, arquitectura regulatoria unificada y políticas de mitigación de riesgos financieros digitales más consolidadas. América Latina aún presenta grandes asimetrías entre países e instituciones.

En comparación con Asia, especialmente China, Japón y Singapur, el principal diferencial reside en la escala tecnológica y en la integración entre plataformas financieras, comercio electrónico y ecosistemas digitales. Asia opera con niveles elevados de automatización y sistemas unificados de identidad digital. América Latina posee dinamismo tecnológico, pero con menor integración y capacidad de control unificado.

A pesar de estas brechas, Brasil y México son reconocidos globalmente como laboratorios financieros de innovación, con rápido crecimiento en el uso de pagos digitales, *fintechs*, bancos digitales y ecosistemas de *open finance.*

3.6.4. Oportunidades Estratégicas

El sector presenta oportunidades importantes para transformar vulnerabilidades en sistemas robustos de resiliencia financiera. La expansión de Inteligencia Artificial

explicable para monitoreo de transacciones, análisis conductual avanzado, detección predictiva de fraudes y modelos de riesgo basados en machine learning permite mayor capacidad de respuesta en tiempo real. La evolución de sistemas de biometría, identidad digital soberana y herramientas de auditoría algorítmica refuerza la integridad operativa.

La modernización de los marcos regulatorios regionales, la armonización de estándares de gobernanza y la integración entre sistemas financieros latinoamericanos pueden elevar significativamente la competitividad de la región. Brasil posee la oportunidad estratégica de liderar iniciativas regionales de interoperabilidad financiera, identidades digitales avanzadas, sistemas de pago a escala y regulación de Inteligencia Artificial aplicada a servicios financieros.

Fintechs latinoamericanas, aliadas a soluciones de *compliance* inteligente e infraestructura crítica digital resiliente, pueden convertirse en protagonistas globales en innovación. La creación de mecanismos avanzados de trazabilidad y transparencia, aliada a certificaciones ESG y regulación integrada, atrae inversiones y aumenta la confianza de los mercados internacionales.

Tabla 8 – Síntesis: Servicios Financieros y Medios de Pago

Dimensión	Brasil y América Latina	Estados Unidos	Unión Europea	Asia
Exposición a fraudes	Muy alta	Moderada	Baja	Variable
Madurez digital	Alta, pero desigual	Muy alta	Alta y estandarizada	Muy alta
Gobernanza financiera	Fragmentada	Consolidada	Altamente integrada	Avanzada
Crimen financiero	Elevado y sofisticado	Alto, pero controlado	Bajo	Moderado
Uso de IA en el sector	Creciente, pero desigual	Avanzado	Regulado y maduro	Extensivo
Oportunidades	IA explicable, biometría, open finance, compliance inteligente	Automatización avanzada	Gobernanza y integración	Escala tecnológica

3.7. Tecnología, Datos y Plataformas Digitales

3.7.1. Riesgos Digitales y Gobernanza Algorítmica

El sector de tecnología, datos y plataformas digitales enfrenta presiones complejas derivadas de la rápida evolución de la Inteligencia Artificial, de la expansión de ecosistemas digitales y de la intensificación de riesgos cibernéticos. En 2026 y más allá, la región observa un aumento significativo de ataques sofisticados, manipulación algorítmica, secuestro digital, uso de herramientas automatizadas para fraudes, explotación de vulnerabilidades en APIs y ataques dirigidos a infraestructuras críticas digitales.

La consolidación de la Inteligencia Artificial generativa amplía tanto las capacidades como los riesgos. Los algoritmos pueden ser utilizados para crear identidades falsas, generar contenido malicioso altamente convincente, automatizar ataques y explotar vulnerabilidades con precisión creciente. Al mismo tiempo, las empresas necesitan lidiar con riesgos asociados a la integridad de los modelos de IA, al sesgo algorítmico, a la explicabilidad de los sistemas y a la creciente presión regulatoria internacional por transparencia.

Otro riesgo creciente es la concentración de datos en plataformas privadas que operan con diferentes niveles de gobernanza y seguridad. La falta de estandarización de políticas de privacidad, la ausencia de auditorías externas y la dependencia de infraestructuras digitales de terceros aumentan las vulnerabilidades, especialmente para empresas de mediano tamaño.

3.7.2. Implicaciones para América Latina y Brasil

América Latina vive un contraste estructural: al mismo tiempo que es una de las regiones más dinámicas en la adopción de tecnologías digitales, también es una de las más expuestas a fraudes, estafas en línea y ataques cibernéticos. Países como Brasil, México, Colombia y Argentina presentan crecimiento acelerado de plataformas digitales, pero con madurez desigual en gobernanza de datos, seguridad cibernética y estandarización tecnológica.

Brasil lidera regionalmente en innovación digital, reglamentación de datos, adopción de Inteligencia Artificial y desarrollo de plataformas financieras. Sin embargo, también es objetivo frecuente de ataques cibernéticos sofisticados, manipulación de APIs, explotación de sistemas de pago y uso indebido de datos. La ausencia de integración plena entre sectores y la desigualdad de madurez tecnológica aumentan la

probabilidad de fallas sistémicas.

La volatilidad institucional y la presencia de organizaciones criminales que utilizan plataformas digitales para fraudes, comercio ilícito, extorsión y lavado de dinero crean riesgos adicionales. La intensificación del uso de *deepfakes*, *bots* avanzados y redes automatizadas de desinformación amplía los impactos sobre seguridad, reputación y procesos decisorios.

3.7.3. Comparación con Ecosistemas Globales

En comparación con Estados Unidos, América Latina presenta menor madurez regulatoria en Inteligencia Artificial, menor capacidad de auditoría algorítmica y menor integración entre sectores público y privado. Estados Unidos posee una fuerte estructura de ciberseguridad, un ecosistema de innovación consolidado y capacidad de respuesta rápida a incidentes digitales.

En relación con la Unión Europea, la diferencia principal está en el grado de estandarización regulatoria. Europa opera con modelos robustos de gobernanza algorítmica, auditoría de IA, seguridad digital y protección de datos. Los países latinoamericanos, a pesar de avances importantes, aún enfrentan fragmentación regulatoria y carencia de mecanismos de control efectivo.

Comparando con Asia, especialmente países como China, Corea del Sur, Japón y Singapur, la brecha se concentra en la escala tecnológica y en la integración sistémica. Asia desarrolla plataformas digitales con arquitectura avanzada, identidades digitales unificadas y ecosistemas de IA totalmente integrados. América Latina presenta dinamismo tecnológico, pero dependiente de *players* globales y con menor capacidad de control soberano sobre los datos.

A pesar de estas diferencias, Brasil se destaca como polo regional emergente de regulación de IA e innovación en plataformas digitales, con potencial para influir en estándares continentales.

3.7.4. Oportunidades Estratégicas

El sector de tecnología presenta oportunidades decisivas para elevar la competitividad, la resiliencia y la gobernanza en toda América Latina. La adopción de modelos avanzados de Inteligencia Artificial explicable, auditoría algorítmica y trazabilidad de datos permite mayor seguridad, eficiencia y conformidad con estándares

internacionales.

El desarrollo de centros regionales de innovación, *hubs digitales* y alianzas entre gobiernos y empresas puede ampliar la soberanía tecnológica y reducir la dependencia de plataformas externas. La creación de sistemas de identidad digital fuerte, infraestructura crítica de datos y gobernanza integrada de ciberseguridad representa una oportunidad de reposicionamiento estratégico continental.

La expansión de centros de datos sostenibles, la adopción de energías renovables en la infraestructura digital y la integración entre ciencia de datos, seguridad corporativa y continuidad de negocios fortalecen a la región ante riesgos globales. Las empresas que inviertan en modelos de IA confiables, gobernanza robusta y arquitectura digital resiliente estarán más preparadas para operar en entornos híbridos marcados por presiones tecnológicas y riesgos complejos.

Tabla 9 – Síntesis: Tecnología, Datos y Plataformas Digitales

Dimensión	Brasil y América Latina	Estados Unidos	Unión Europea	Asia
Gobernanza de IA	Avanzando, pero fragmentada	Robusta e influyente	Altamente estandarizada	Avanzada e integrada
Madurez de datos	Media a alta, desigual	Muy alta	Alta y regulada	Muy alta
Exposición a fraudes digitales	Muy alta	Media	Baja	Variable
Infraestructura digital	Creciente, pero asimétrica	Amplia y consolidada	Integrada	Avanzada y escalable
Dependencia de plataformas externas	Elevada	Baja	Elevada	Variable
Oportunidades	Auditoría algorítmica, IA explicable, data centers, identidad digital	Innovación acelerada	Gobernanza fuerte	Escala e integración

3.8. Minería, Petróleo y Gas

3.8.1. Vulnerabilidades y Presiones Ambientales

Los sectores de minería, petróleo y gas enfrentan algunas de las fuentes de riesgo más complejas del escenario contemporáneo. En 2026 y más allá, presiones climáticas, ambientales, sociales y tecnológicas convergen para intensificar riesgos operativos,

regulatorios, geopolíticos y reputacionales. Estos sectores lidian con activos altamente expuestos al clima, dependen de infraestructura crítica sensible a interrupciones y operan bajo creciente escrutinio internacional sobre emisiones, trazabilidad e impactos sociales.

Eventos climáticos extremos, como inundaciones que afectan minas, rupturas de represas, erosión de laderas, tormentas que interrumpen operaciones marítimas y sequías que reducen la disponibilidad hídrica para procesos industriales, elevan los riesgos físicos. Además, la intensificación de movimientos socioambientales amplía los riesgos de paralizaciones, presiones judiciales y exigencias regulatorias más rígidas.

La transición energética global genera un conjunto doble de presiones. Por un lado, los combustibles fósiles sufren presión por la reducción de emisiones. Por otro, crece la demanda de minerales críticos como **cobre, litio, niobio, níquel, grafito y tierras raras,** esenciales para baterías, infraestructura energética limpia y tecnologías digitales. Esta dinámica amplía riesgos de oferta, eleva tensiones territoriales y aumenta la competencia global por áreas mineras.

El creciente interés mundial por las tierras raras —fundamentales para energías renovables, movilidad eléctrica, tecnologías digitales y sistemas de defensa— trae a América Latina, especialmente a Brasil, un conjunto de oportunidades y amenazas. La fuerte concentración internacional de las etapas de refinación y procesamiento de

estos minerales aumentan la posibilidad de interrupciones en las cadenas productivas globales y amplía la exposición de la región a disputas geopolíticas. Sin avanzar en capacidades propias de procesamiento, diversificación de mercados y mecanismos de seguridad estratégica, los países latinoamericanos tienden a permanecer vulnerables a choques de oferta, presiones comerciales y asimetrías tecnológicas.

3.8.2. Implicaciones Regionales para América Latina y Brasil

América Latina desempeña un papel central en la transición global debido a su abundancia de minerales críticos, depósitos de hidrocarburos, reservas energéticas y relevancia en cadenas productivas de alto impacto. Sin embargo, la región también enfrenta inestabilidades políticas, conflictos territoriales, presencia de redes ilícitas y fragilidad regulatoria que amplían los riesgos operativos.

Además, la volatilidad de los precios internacionales del petróleo y las decisiones estratégicas de grandes productores globales —como recortes de oferta, redireccionamiento de producción o sanciones económicas— funcionan como vectores

de choque para América Latina, afectando ingresos públicos, balanzas comerciales, inversiones en exploración y la previsibilidad macroeconómica. Estos movimientos amplifican la exposición de la región a ciclos de bonanza y crisis (*boom-and-bust*) y refuerzan la importancia de estrategias de diversificación energética y de gestión fiscal prudente.

Brasil es uno de los países más estratégicos del mundo en reservas minerales, energía y biocombustibles. La producción de mineral de hierro, niobio, petróleo *offshore*, gas natural y minerales estratégicos coloca al país en el centro de disputas globales por recursos. Sin embargo, el historial de tragedias involucrando represas, deforestación ilegal, explotación depredadora y fallas de fiscalización mantiene al sector bajo vigilancia intensa.

La expansión de grupos criminales en regiones mineras y áreas fronterizas representa un riesgo creciente. La minería ilegal de oro, casiterita y otros minerales está conectada a redes de tráfico, trabajo esclavo, delitos ambientales y lavado de dinero. Esta convergencia entre crimen organizado y actividades extractivas amplía riesgos físicos, reputacionales y regulatorios para empresas legales.

En algunos países de la región, crece también la actuación de economías paralelas asociadas al cobre; incluyendo robo y desvío de cables, manipulación ilícita de stocks industriales e interferencia en rutas logísticas. Estos mecanismos amplían riesgos operativos, financieros y reputacionales para empresas y para infraestructuras intensivas en cobre, afectando redes eléctricas, telecomunicaciones, transporte y sistemas industriales que dependen de este insumo estratégico.

Además, presiones internacionales por certificaciones ambientales, trazabilidad de origen e integración ESG colocan a América Latina bajo mayor escrutinio. Las empresas de la región enfrentan una expectativa creciente por transparencia, uso de tecnologías de monitoreo ambiental y prácticas robustas de gobernanza socioambiental.

3.8.3. Comparación Global

En comparación con Estados Unidos, América Latina presenta mayor exposición a riesgos ambientales graves, mayor incidencia de conflictos socioambientales y menor capacidad de respuesta integrada entre sectores. Estados Unidos opera con gobernanza ambiental más estructurada y mayor capacidad de fiscalización, aunque también enfrenta riesgos climáticos crecientes.

En relación con la Unión Europea, la brecha es principalmente regulatoria y

tecnológica. Europa avanza rápidamente en políticas de descarbonización, economía circular, trazabilidad integrada y monitoreo ambiental continuo. América Latina avanza, pero de forma fragmentada, con estándares muy distintos entre países.
Cuando se compara con Asia, especialmente Australia y China, la región enfrenta menor capacidad de inversión continua en modernización, menor estandarización tecnológica y mayores presiones territoriales. Australia se destaca como referencia en minería sostenible, mientras que China opera con gran escala, fuerte control estatal y rápidas expansiones de infraestructura.

A pesar de estas distancias, América Latina posee ventajas competitivas esenciales: abundancia geológica, potencial para minería sostenible, capacidad de expansión energética renovable y relevancia estratégica en la economía verde global.

Estudios internacionales sobre minerales críticos proyectan un crecimiento acelerado de la demanda global de cobre, litio y tierras raras hasta 2030, impulsado por la expansión de energías renovables, baterías e infraestructura digital, reforzando el peso estratégico de América Latina en estas cadenas.

3.8.4. Oportunidades Estratégicas

El sector presenta oportunidades significativas para el fortalecimiento de la competitividad, la resiliencia y la sostenibilidad. La adopción de tecnologías de monitoreo predictivo, sensores avanzados, sistemas remotos de supervisión y modelos de Inteligencia Artificial para la previsión de fallas puede reducir drásticamente riesgos operativos y ambientales.

La expansión de prácticas de minería sostenible, trazabilidad digital de la cadena y certificación ambiental robusta aumenta la confianza de los mercados internacionales.

Brasil posee potencial estratégico para liderar la producción de minerales críticos de forma sostenible, atrayendo inversiones globales y posicionándose como proveedor confiable en cadenas de energía limpia y tecnología de punta. La limitación de la minería ilegal, el fortalecimiento de la fiscalización y la creación de zonas regulatorias robustas pueden transformar vulnerabilidades en oportunidades.

La transición energética crea nuevos frentes de inversión en hidrógeno verde, captura de carbono, logística de gas natural, biocombustibles avanzados y almacenamiento energético. Las empresas que integren sostenibilidad, seguridad convergente e innovación tecnológica podrán operar con mayor resiliencia y capturar valor en mercados globales de alto crecimiento.

El fortalecimiento de las cadenas industriales asociadas a minerales críticos — incluyendo procesamiento, refinación, manufactura avanzada e integración tecnológica — despunta como una de las oportunidades estratégicas más relevantes para Brasil y América Latina en los próximos años. Avanzar del modelo tradicional basado solo en extracción y exportación hacia un modelo que incorpore beneficio, transformación y agregación de valor puede reposicionar a la región como protagonista de la economía verde global, ampliando competitividad, soberanía tecnológica y capacidad de actuación en mercados globales de alto crecimiento.

Tabla 10 – Síntesis: Minería, Petróleo y Gas

Dimensión	Brasil y América Latina	Estados Unidos	Unión Europea	Asia
Exposición ambiental	Muy alta	Media	Media	Variable
Gobernanza socioambiental	Fragmentada	Moderada	Elevada	Variable
Presión regulatoria	Creciente, pero desigual	Consistente	Muy alta	Alta en los grandes productores
Riesgos criminales	Elevados en áreas remotas	Bajos	Bajos	Moderados
Transición energética	Oportunidad estratégica	Madura	Avanzada	Dinámica y acelerada
Oportunidades	Minerales críticos, IA predictiva, trazabilidad, energía limpia	Tecnologías avanzadas	Economía verde	Escala productiva

3.9. Sector Público, Justicia y Regulación

3.9.1. Fragilidades Institucionales

El sector público, incluyendo poderes Ejecutivo, Legislativo, Judicial y organismos de control, ocupa una posición central en la configuración de los escenarios de riesgo para 2026 y más allá. En América Latina, fragilidades institucionales recurrentes, como inestabilidad política, baja capacidad de ejecución de políticas públicas, sobrecarga de los sistemas de justicia y asimetrías regulatorias, actúan como amplificadores de riesgos para todos los demás sectores analizados a lo largo de este estudio.

Entre las fragilidades más relevantes están la dificultad de armonizar políticas a largo

plazo, alternancias abruptas de agenda entre gobiernos, limitaciones presupuestarias prolongadas, procesos burocráticos poco digitalizados, ausencia de integración de datos entre organismos y deficiencias en la planificación basada en evidencia. En muchos países, la capacidad de formular políticas robustas de seguridad, gobernanza digital, adaptación climática y combate al crimen organizado se ve afectada por estas restricciones estructurales.

Los sistemas de justicia, aunque representan un pilar de estabilidad, frecuentemente operan con congestión procesal, baja automatización, limitada integración con bases de datos digitales y dificultad para lidiar con delitos complejos que involucran Inteligencia Artificial, criptomonedas, redes transnacionales e infraestructuras críticas. Esto reduce la capacidad de disuasión, amplía la sensación de impunidad e incentiva la expansión de economías ilícitas.

3.9.2. Presiones Digitales y Criminales

La rápida digitalización del Estado en entornos institucionalmente frágiles crea una ecuación desafiante. Por un lado, los gobiernos adoptan servicios digitales, identidades electrónicas, plataformas integradas y sistemas de recaudación automatizados. Por otro, muchas de estas iniciativas se implementan con brechas de seguridad, baja gobernanza de datos y protección insuficiente contra ataques cibernéticos.

Ataques a organismos públicos, tribunales, ministerios, alcaldías, parlamentos y empresas estatales se han vuelto más frecuentes y sofisticados. Estos ataques incluyen secuestro de datos, paralización de servicios, filtración de información sensible, compromiso de sistemas electorales y manipulación de registros. En contextos de polarización política, estos incidentes tienen un impacto amplificado sobre la confianza pública y la estabilidad democrática.

Al mismo tiempo, redes criminales utilizan la propia fragilidad estatal para operar. La combinación entre corrupción, captura regulatoria, infiltración de grupos ilícitos en estructuras públicas y uso de plataformas digitales para fraudes y lavado de dinero crea un escenario crítico. El crimen organizado se beneficia de fallas de coordinación entre organismos, de la falta de interoperabilidad entre bases de datos y de la ausencia de una estrategia integrada de seguridad pública y financiera a escala regional.

3.9.3. Desafíos para Brasil y América Latina

América Latina enfrenta desafíos estructurales comunes, como la baja integración entre sistemas nacionales de justicia, seguridad pública, fiscalización tributaria y control financiero. Muchos países disponen de islas de excelencia institucional, pero carecen de una arquitectura integral de gobernanza de riesgos a nivel de Estado.

Brasil desempeña un papel central en la configuración regional, tanto por su dimensión económica y territorial como por la complejidad de sus sistemas político, jurídico y administrativo. El país ha avanzado en algunos frentes importantes, como sistemas de control financiero, combate al lavado de dinero, automatización de tribunales y regulación de protección de datos. Sin embargo, permanece con desafíos significativos en áreas como seguridad pública, integración de bases entre organismos, combate coordinado al crimen organizado e implementación consistente de políticas a largo plazo.

La sobrecarga de demandas sobre el sector público brasileño, combinada con restricciones fiscales e inestabilidad política recurrente, dificulta la adopción de estrategias estructurantes en temas como gobernanza de Inteligencia Artificial, resiliencia de infraestructuras críticas, protección ambiental integrada y fortalecimiento de capacidades estatales en regiones remotas dominadas por redes ilícitas. Estos factores limitan la capacidad de respuesta del Estado ante riesgos híbridos, que combinan dimensiones físicas, digitales, financieras y climáticas.

3.9.4. Comparación Global

En comparación con Estados Unidos, América Latina presenta menor previsibilidad regulatoria, mayor exposición a la captura política de instituciones, menor integración entre organismos de justicia y seguridad y menor capacidad de respuesta en crisis de alta complejidad. Estados Unidos, a pesar de tensiones políticas internas, mantiene estructuras institucionales más estables y con mayor capacidad de hacer cumplir las leyes y regulaciones *(enforcement).*

En relación con la Unión Europea, la diferencia es aún más pronunciada en la dimensión regulatoria. Europa opera con un marco normativo altamente integrado, fuerte regulación supranacional, estándares mínimos de gobernanza y sistemas de justicia relativamente armónicos. América Latina, por otro lado, está marcada por la fragmentación y variaciones profundas de calidad institucional entre países.

Comparando con Asia, la evaluación es heterogénea. Países como Japón, Corea del Sur

y Singapur presentan instituciones robustas y elevada capacidad tecnológica, mientras que otras economías asiáticas comparten desafíos similares a los contextos latinoamericanos, como sobrecarga de los sistemas de justicia, informalidad, corrupción y fragilidad regulatoria. Aun así, la integración regional asiática en temas estratégicos como infraestructura, comercio e innovación tecnológica tiende a ser más avanzada que en América Latina.

3.9.5. Oportunidades Estratégicas

A pesar de las fragilidades, el sector público, la justicia y la regulación en América Latina poseen oportunidades para el reposicionamiento estratégico. Una de ellas es la adopción de modelos de gobernanza orientados por riesgo, integrando principios de la gestión de riesgos a la formulación de políticas públicas, a la regulación de tecnologías y a la supervisión de infraestructuras críticas. Esto permite priorizar acciones, optimizar recursos escasos y reducir vulnerabilidades sistémicas.

Otra oportunidad consiste en fortalecer la cooperación regional en temas como combate al crimen organizado, delitos financieros, ciberseguridad, protección ambiental y gobernanza de Inteligencia Artificial. La creación de marcos regulatorios alineados, mecanismos de reconocimiento mutuo, sistemas de interoperabilidad de datos y plataformas conjuntas de inteligencia puede elevar significativamente la resiliencia estatal.

Brasil posee condiciones de liderazgo en diversas de estas agendas, especialmente en temas como protección de datos, combate a delitos financieros, regulación tecnológica y desarrollo de políticas integradas de seguridad y justicia. La modernización de tribunales, el uso responsable de IA en el sistema de justicia, la automatización segura de servicios públicos y la ampliación de la transparencia y la rendición de cuentas son caminos para aumentar la confianza pública y fortalecer el Estado de Derecho.

La adopción de estructuras regulatorias claras para IA, datos, ciberseguridad, infraestructuras críticas y medio ambiente, asociada a programas de fortalecimiento institucional y formación de cuadros públicos en gestión de riesgos, puede transformar al sector público en protagonista de la resiliencia regional, en lugar de permanecer como el eslabón más frágil de la cadena.

Tabla 11 – Síntesis: Sector Público, Justicia y Regulación

Dimensión	Brasil y América Latina	Estados Unidos	Unión Europea	Asia
Estabilidad institucional	Variable, frecuentemente inestable	Relativamente estable	Alta	Heterogénea
Capacidad regulatoria	Fragmentada	Alta	Muy alta	Variable
Integración entre organismos	Limitada	Elevada en temas estratégicos	Elevada	Variable
Exposición al crimen organizado	Alta	Media	Baja	Variable
Digitalización del Estado	En expansión, pero desigual	Avanzada	Avanzada y regulada	Avanzada en algunos países
Oportunidades	Gobernanza de riesgos, cooperación regional, regulación de IA, fortalecimiento institucional	Innovación y estabilidad	Liderazgo regulatorio	Integración en bloques regionales

3.10. Cuadro-Síntesis Final Multisectorial

El análisis integrado de los ocho sectores considerados en este estudio evidencia un cuadro en el que riesgos climáticos, digitales, institucionales y criminales no actúan de forma aislada, sino como un sistema de presiones interdependientes. La resiliencia de América Latina en 2026 y más allá no dependerá solo del desempeño individual de cada sector, sino de la capacidad de coordinar políticas, inversiones y gobernanza en una perspectiva multisectorial. Brasil, por su escala económica, por la relevancia en energía, agronegocios, minería y servicios financieros, ocupa una posición central en este arreglo, pudiendo funcionar tanto como factor de estabilización como de amplificación de vulnerabilidades regionales.

La lectura horizontal de los sectores muestra que clima, infraestructura crítica y logística funcionan como multiplicadores de riesgo para todos los demás dominios. Interrupciones energéticas impactan industria, servicios financieros, tecnología y

sector público, al mismo tiempo que agravan tensiones urbanas y debilitan respuestas estatales. Eventos climáticos extremos afectan directamente agronegocios, minería,

ciudades, redes viales y puertos, presionando finanzas públicas, aumentando la morosidad y exigiendo instrumentos más sofisticados de gestión de riesgos y seguros. En paralelo, la digitalización acelerada de todos los sectores, sin gobernanza proporcional, crea una capa adicional de vulnerabilidad que atraviesa cadenas productivas, servicios esenciales e instituciones.

Otra convergencia importante es la presencia transversal del crimen organizado y de las economías ilícitas. En la práctica, no se trata solo de un problema de seguridad pública, sino de un vector estructural de riesgo que impacta logística, agronegocios, minería, servicios financieros, tecnología y la propia capacidad del Estado para hacer valer regulaciones. Rutas ilícitas utilizan infraestructura formal, explotan brechas regulatorias, infiltran servicios financieros y utilizan plataformas digitales para coordinar operaciones. En escenarios más adversos, como Redes Sombrías, esta convergencia amplía el riesgo sistémico y compromete la credibilidad de las instituciones.

Desde el punto de vista tecnológico, todos los sectores analizados avanzan en digitalización, automatización y uso de datos, pero con velocidades y niveles de madurez muy distintos. Sectores como servicios financieros, tecnología y medios de pago presentan alta sofisticación, pero también alta exposición a ataques cibernéticos y fraudes. Industria, energía y logística aún poseen grandes asimetrías internas entre empresas de punta y operadores con baja madurez digital, lo que crea zonas de vulnerabilidad que pueden ser exploradas por agentes maliciosos. El sector público, a su vez, vive la tensión de digitalizar rápidamente sin disponer, en muchos casos, de la misma robustez de seguridad y gobernanza que el sector privado.

Al mismo tiempo, el cuadro multisectorial revela un conjunto consistente de oportunidades convergentes. La expansión de energía renovable, la modernización logística, la agricultura de precisión, la minería sostenible, la digitalización responsable de servicios públicos, la integración financiera y la gobernanza robusta de Inteligencia Artificial pueden posicionar a Brasil y América Latina como protagonistas en una economía global que valora resiliencia, sostenibilidad e integridad. Para ello, será necesario alinear estrategias sectoriales, reducir fragmentaciones regulatorias y fortalecer mecanismos de cooperación regional en seguridad, datos, clima e infraestructura crítica. La tabla a continuación sintetiza, de manera comparativa, las principales características de riesgo y oportunidad de cada sector, destacando cuatro dimensiones transversales: sensibilidad climática, exposición a riesgos digitales y crimen organizado, dependencia de instituciones públicas y potencial de oportunidad estratégica en 2026 y más allá.

Tabla 12 – Síntesis: Multisectorial

Sector	Sensibilidad climática	Exposición a riesgos digitales y crimen organizado	Dependencia de instituciones públicas	Potencial de oportunidad estratégica
Industria y Manufactura	Alta, debido a energía, agua y logística	Media a alta, con aumento de ataques a sistemas industriales	Alta, en infraestructura, regulación e incentivos	Elevado, con automatización defensiva, manufactura avanzada y transición verde
Energía e Infraestructuras Críticas	Muy alta, por dependencia hídrica y de redes físicas expuestas	Muy alta, con ataques a sistemas de control y redes críticas	Muy alta, en regulación, concesiones y planificación	Muy elevado, en renovables, redes inteligentes e integración regional
Agronegocios y Alimentos	Muy alta, por clima, agua y suelos	Media, con creciente digitalización y presencia de ilícitos en áreas rurales	Alta, en infraestructura, regulación ambiental y fiscalización	Elevadísimo, en agricultura de precisión, bioeconomía y trazabilidad sostenible
Logística, Puertos, Carreteras e Infraestructuras Urbanas	Muy alta, por eventos extremos que afectan circulación y almacenamiento	Media, creciente con digitalización de cadenas y puertos	Muy alta, en inversiones, concesiones y planificación urbana	Elevado, en corredores verdes, puertos inteligentes e integración multimodal
Servicios Financieros y Medios de Pago	Indirecta, pero relevante por impactos en morosidad y crédito	Muy alta, con fraudes digitales, IA maliciosa y lavado de dinero	Alta, en regulación, supervisión y políticas monetarias	Muy elevado, en IA explicable, open finance, biometría y compliance inteligente
Tecnología, Datos y Plataformas Digitales	Indirecta, pero crítica para previsión, respuesta y resiliencia	Muy alta, por ser objetivo y vector de riesgos cibernéticos	Media a alta, en políticas de datos, IA y soberanía digital	Elevadísimo, en gobernanza algorítmica, identidad digital, data centers y servicios de valor agregado
Minería, Petróleo y Gas	Muy alta, con riesgos	Alta, con aumento de automatización	Alta, en licenciamiento,	Elevado, en minerales

	ambientales y territoriales intensos	y ataque a infraestructuras	regulación ambiental y seguridad	críticos, energía de transición y trazabilidad
Sector Público, Justicia y Regulación	Alta, por la necesidad de respuesta a crisis y adaptación climática	Alta, en ataques a organismos públicos y manipulación digital	Estructural, pues es el centro de la regulación y de la coordinación	Muy elevado, en gobernanza de riesgos, regulación de IA, cooperación regional y fortalecimiento institucional

El cuadro multisectorial confirma que la resiliencia regional no será alcanzada solo mediante inversiones sectoriales aisladas. Dependerá de la capacidad de articular políticas públicas consistentes, marcos regulatorios claros y estrategias corporativas integradas. Sectores como energía, logística, finanzas y tecnología funcionan como columna vertebral de la economía y, por ello, deben ser tratados como prioridades estratégicas en cualquier agenda de desarrollo para 2026 y más allá. Al mismo tiempo, la modernización del sector público, la profesionalización de la justicia y el fortalecimiento de la regulación en temas como Inteligencia Artificial, protección de datos, combate al lavado de dinero y gobernanza ambiental serán determinantes para transformar vulnerabilidades históricas en ventajas competitivas duraderas.

04

SEGURIDAD CORPORATIVA E INFRAESTRUCTURAS CRÍTICAS

4.1. Introducción

La seguridad corporativa asume un papel central en la resiliencia organizacional y en la estabilidad operativa de sectores estratégicos ante los escenarios prospectivos delineados para 2026 y más allá. El entorno de riesgo contemporáneo en América Latina está marcado por presiones simultáneas que atraviesan dominios físicos, digitales, climáticos, criminales e institucionales. Estas presiones moldean el ecosistema de seguridad de forma integrada y exigen enfoques convergentes capaces de responder a amenazas complejas que evolucionan rápidamente.

Las infraestructuras críticas de la región, incluyendo energía, logística, saneamiento, telecomunicaciones, salud, finanzas, minería, abastecimiento alimentario y movilidad urbana, enfrentan una creciente vulnerabilidad ante ataques cibernéticos, eventos climáticos extremos y la expansión de redes ilícitas transnacionales. La interdependencia entre estos sistemas crea un entorno en el cual fallas en un dominio pueden desencadenar interrupciones en cascada, amplificando impactos y aumentando el costo de los incidentes. El fortalecimiento de la seguridad corporativa se convierte, por lo tanto, en un requisito operativo y estratégico para garantizar la continuidad, estabilidad y confianza de los *stakeholders*.

A continuación, este capítulo presenta una lectura integrada de las presiones sobre la seguridad corporativa, destacando riesgos físicos, digitales y reputacionales, además de analizar la situación específica de América Latina y de Brasil, comparando con estándares globales e identificando oportunidades de evolución.

4.2. Presiones del Entorno de Riesgo Híbrido

La convergencia entre riesgos físicos y digitales transforma profundamente la lógica de la seguridad corporativa. La digitalización de las operaciones aumenta la eficiencia, pero amplía la superficie de ataque, especialmente con la integración entre tecnología de la información, tecnología operativa y dispositivos conectados. Sistemas críticos utilizados en energía, manufactura, puertos, aeropuertos, hospitales y servicios financieros se convierten en objetivos de agentes maliciosos que buscan paralizar operaciones, causar daños físicos u obtener ventaja financiera.

Eventos climáticos extremos también impactan directamente la seguridad, provocando interrupciones eléctricas, daños estructurales, sobrecarga de redes, desplazamientos poblacionales y situaciones que amplían la probabilidad de delitos oportunistas, invasiones y desorganización operativa. En paralelo, la difusión de plataformas

digitales facilitas acciones de grupos ilícitos que utilizan datos, identidades simuladas, herramientas de automatización y redes sociales para ampliar la escala de fraudes, extorsiones y manipulación informativa.

La seguridad corporativa deja de ser un pilar aislado y pasa a actuar como interfaz entre continuidad de negocios, gobernanza digital, gestión de riesgos y protección de infraestructuras críticas. Las organizaciones necesitan desarrollar competencias multidisciplinarias para enfrentar un entorno en el que las amenazas se desplazan entre el mundo físico y el digital con una fluidez cada vez mayor.

4.3. Vulnerabilidades Específicas de Infraestructuras Críticas

Las infraestructuras críticas de América Latina presentan vulnerabilidades que derivan de factores estructurales y coyunturales. Estructuras envejecidas, baja redundancia, falta de mantenimiento continuo, déficit de inversiones y exposición climática elevada aumentan la probabilidad de fallas sistémicas. Al mismo tiempo, la expansión de la conectividad y sensores en sistemas industriales no ha sido acompañada del mismo grado de inversión en seguridad digital, generando brechas en protección de datos, protocolos de respuesta y actualizaciones de sistemas.

La falta de integración entre sectores, la ausencia de estándares mínimos de resiliencia y la fragmentación regulatoria amplían las vulnerabilidades. En muchos países, las infraestructuras críticas son operadas por empresas privadas que dependen de un entorno institucional estable para implementar planes robustos de protección. La inestabilidad política, la burocracia y la falta de coordinación entre los sectores energético, logístico, sanitario y tecnológico reducen la capacidad de respuesta conjunta ante incidentes severos.

Además, redes ilícitas explotan fragilidades estructurales para robar cables, atacar subestaciones, interferir en rutas logísticas, manipular sistemas de transporte e infiltrar cadenas de suministro. La criminalidad, cuando se combina con eventos climáticos extremos o ataques cibernéticos, puede generar situaciones de crisis prolongada y un aumento significativo de los costos operativos.

4.4. Panorama Latinoamericano: Crimen Organizado, Convergencia Digital y Fragilidad Estatal

A América Latina presenta una de las combinaciones más adversas para la seguridad corporativa entre las grandes regiones del mundo. La presencia de organizaciones

criminales con capacidad transnacional, el uso de tecnologías avanzadas para fraudes y

extorsiones, la vulnerabilidad de puertos y fronteras y la inestabilidad institucional crean un entorno que exige enfoques altamente especializados de mitigación.

Puertos estratégicos, como Santos, Colón, Buenaventura, Guayaquil y Buenos Aires, son utilizados por cárteles internacionales para lavado de dinero, contrabando y flujo de cargas ilícitas, muchas veces infiltrando operadores logísticos y facilitando la contaminación de cadenas legales. Las empresas que operan en estos entornos necesitan implementar controles rigurosos, sistemas de trazabilidad y protocolos de inspección que superen las fallas estatales.

En el sector digital, fraudes avanzados, ingeniería social automatizada, manipulación de APIs y uso de Inteligencia Artificial para la creación de falsificaciones amplían la complejidad de la protección de identidades y operaciones electrónicas. Pequeñas y medianas empresas son desproporcionadamente más vulnerables debido a la menor madurez de seguridad y a la dependencia de proveedores externos.

La fragilidad estatal amplía estos riesgos al dificultar la fiscalización de áreas remotas, reducir la capacidad de respuesta ante incidentes severos, limitar la cooperación internacional y dificultar la implementación de políticas robustas de protección de datos e infraestructuras críticas.

4.5. Respuesta Corporativa: Seguridad Convergente y Resiliencia Operativa

A La respuesta corporativa ante el entorno de riesgos híbridos exige la transición de modelos fragmentados hacia una arquitectura de seguridad verdaderamente convergente. En este modelo, la protección de activos físicos, digitales, informacionales y operativos no se trata como funciones aisladas, sino como componentes interdependientes de un mismo sistema estratégico orientado por la resiliencia organizacional. A continuación, se presentan las cuatro dimensiones centrales que estructuran este enfoque.

En este estudio, el término **Seguridad Corporativa** se utiliza para designar la función de gobernanza estratégica que integra y orienta diferentes dominios de protección — física, patrimonial, cibernética, informacional, reputacional, entre otros — conectándolos a la continuidad de negocios, a la protección de activos críticos y a la resiliencia organizacional.

Aunque las tecnologías avanzadas y la Inteligencia Artificial amplían significativamente

la capacidad analítica y la eficiencia operativa, no sustituyen el juicio humano. La madurez profesional, la experiencia acumulada y la colaboración entre equipos permanecen como elementos decisivos para transformar información en acción estratégica y sostener la resiliencia corporativa en entornos volátiles.

La **primera dimensión** corresponde a la arquitectura de protección convergente e inteligente. Integra tecnologías avanzadas, análisis conductuales, sensores distribuidos y sistemas remotos de monitoreo para proteger activos críticos en diferentes capas. Esta arquitectura se basa en la evaluación continua de riesgos, en la protección dinámica de perímetros y en mecanismos de disuasión que incorporan datos climáticos y operativos. La protección deja de ser solo vigilancia física y evoluciona hacia un sistema coordinado capaz de anticipar amenazas, responder rápidamente a cambios en el contexto y apoyar decisiones estratégicas.

La **segunda dimensión** es la defensa digital estructurante, que posiciona a la ciberseguridad como núcleo de la continuidad de negocios. Involucra la protección integral de sistemas críticos, gobernanza de datos, trazabilidad digital, segmentación avanzada de redes y uso de Inteligencia Artificial defensiva para la detección temprana de anomalías. Incluye también gobernanza algorítmica, con mecanismos de explicabilidad, auditoría y supervisión continua de modelos automatizados. Esta dimensión es esencial para reducir la probabilidad de eventos sistémicos en entornos altamente digitalizados.

La **tercera dimensión** corresponde a la gobernanza estratégica de riesgos y continuidad. En ella, la seguridad corporativa se integra al centro de la toma de decisiones, conectando gestión de riesgos, gobernanza de datos, continuidad operativa y estrategia institucional. Se trata de estructurar mecanismos de evaluación de riesgos complejos, establecer métricas e indicadores de resiliencia, incorporar análisis de escenarios al proceso de decisión y fortalecer la relación entre áreas de seguridad, consejo, comité ejecutivo y planificación estratégica. Esta dimensión permite que la organización desarrolle una visión anticipatoria y capacidad de adaptación continua.

En la práctica, esta gobernanza de riesgos y continuidad exige que escenarios de crimen organizado, violencia dirigida contra activos corporativos e interrupciones provocadas por acciones ilícitas sean tratados explícitamente en los planes de continuidad de negocios (BCP), de recuperación ante desastres (DRP) y en los análisis de impacto en el negocio (BIA), junto con desastres naturales, fallas tecnológicas y choques macroeconómicos. Incorporar estos vectores criminales a la agenda de resiliencia evita que la seguridad corporativa permanezca en un plano meramente operativo y la reposiciona como componente estratégico de la protección de valor.

La **cuarta dimensión** se refiere a la capacidad de respuesta integrada, adaptativa y basada en inteligencia. Esta capacidad opera con protocolos unificados para incidentes físicos, digitales, climáticos y reputacionales, garantizando que los equipos de

seguridad, tecnología, operaciones, jurídico y comunicación actúen de forma coordinada. Involucra centros integrados de comando y control, simulaciones periódicas, procesos de recuperación escalables y mecanismos de aprendizaje post-incidente que retroalimentan toda la gobernanza de riesgos. La resiliencia deja de entenderse como un plan aislado y pasa a ser un atributo estratégico que permite a la organización operar incluso bajo condiciones severamente degradadas.

La seguridad corporativa contemporánea debe ser comprendida como un **sistema de gobernanza integrado** que articula riesgos físicos, digitales, climáticos, reputacionales e institucionales con foco en los objetivos de la organización. Su actuación demanda visión estratégica y capacidad de anticipación, y no solo control operativo. A continuación, presentamos un resumen estratégico de las cuatro dimensiones.

Tabla 13 – Dimensiones del sistema de gobernanza integrado de la seguridad corporativa

Dimensión Estratégica	Foco Central	Valor Agregado
Arquitectura de Protección Convergente	Gobernanza integrada de activos físicos y tecnológicos	Reducción de vulnerabilidades híbridas y aumento de protección estructural
Defensa Digital Estructurante	Ciberseguridad como núcleo de la continuidad	Prevención de ataques sistémicos y protección de datos críticos
Gobernanza Estratégica de Riesgos	Seguridad como función estratégica de la organización	Alineación con consejo, estrategia y decisiones de alto impacto
Respuesta Integrada y Adaptativa	Resiliencia organizacional en múltiples capas	Capacidad de operar incluso en entorno degradado

Estas cuatro dimensiones, cuando se implementan de forma integrada, transforman la seguridad corporativa en un pilar estructurante de la resiliencia organizacional. Refuerzan la capacidad de anticipar amenazas, absorber choques, responder de forma eficaz y recuperar operaciones críticas en entornos marcados por incertidumbre, interdependencia y rápidas transformaciones. Este enfoque prepara a empresas e instituciones para enfrentar de manera sólida los desafíos complejos que caracterizan a América Latina en 2026 y más allá.

4.6. Presiones y Oportunidades en el Contexto Brasileño

O Brasil es simultáneamente uno de los países más desafiantes y prometedores en seguridad corporativa. La presencia de grupos criminales sofisticados, la extensión territorial, la importancia de sus puertos y refinerías, la dependencia de hidrovías y carreteras y la creciente digitalización de servicios financieros amplían la complejidad de la protección de activos. Al mismo tiempo, el país lidera la región en innovación tecnológica, adopción de sistemas avanzados de seguridad e integración entre sectores público y privado.

Además de la protección de activos físicos y digitales, el contexto brasileño exige atención permanente a la integridad física de colaboradores y equipos operativos. Riesgos de asaltos y secuestros en desplazamientos, coacciones en regiones bajo influencia de facciones criminales y episodios de violencia en el entorno de plantas industriales, obras y centros logísticos impactan directamente programas de continuidad de negocios, el clima organizacional, el deber de cuidado (duty of care) de las empresas y su exposición a riesgos jurídicos y reputacionales.

Áreas críticas como minería, energía, logística, agronegocios y servicios financieros exigen enfoques específicos basados en monitoreo remoto, auditoría de sistemas, protección de datos sensibles, gestión de incidentes climáticos y respuesta rápida a crisis. La capacidad brasileña de desarrollar centros integrados, algoritmos propios de detección, plataformas de trazabilidad y tecnologías de previsión climática crea oportunidades relevantes para elevar su resiliencia.

El fortalecimiento de programas nacionales de protección de infraestructuras críticas, la armonización regulatoria y la expansión de iniciativas de cooperación interestatal son esenciales para reducir vulnerabilidades, ampliar la previsibilidad y fortalecer el entorno de negocios.

05

INDICADORES Y RADAR DE SEÑALES ANTICIPATORIAS

5.1. Introducción

La construcción de un radar de señales anticipatorias es una etapa esencial para transformar el estudio de escenarios en capacidad real de monitoreo, anticipación y respuesta organizacional. Indicadores bien definidos permiten que empresas, gobiernos y organizaciones evalúen cambios en el entorno externo, detecten rupturas emergentes y ajusten estrategias antes de que los impactos se vuelvan irreversibles. En un contexto de riesgos híbridos, fragmentación institucional y aceleración tecnológica, la capacidad de interpretación temprana se convierte en factor de ventaja competitiva.

El radar de señales anticipatorias presentado en este capítulo está estructurado con base en las cuatro dimensiones centrales que moldean el entorno estratégico analizado a lo largo del informe: clima y ambiente, tecnología y datos, crimen e inestabilidad institucional, economía y cadenas críticas. Cada dimensión posee indicadores específicos que permiten un monitoreo sistemático, reduciendo incertidumbres y ampliando la capacidad de adaptación ante eventos imprevisibles. La combinación de estos indicadores forma una matriz de alerta que puede ser utilizada tanto por sectores privados como por organismos públicos.

América Latina y Brasil exigen un conjunto particular de indicadores debido a vulnerabilidades estructurales y asimetrías regionales. Eventos climáticos extremos, volatilidad regulatoria, expansión del crimen organizado, ataques cibernéticos y fragilidad de infraestructuras críticas ocurren con mayor frecuencia e intensidad en la región, lo que requiere un radar más sensible y completo. A continuación, se detallan las señales anticipatorias organizadas por dominio estratégico.

5.2. Indicadores Climáticos y Ambientales

Los indicadores climáticos constituyen la primera capa del radar, pues funcionan como multiplicadores de riesgo para logística, energía, agricultura, minería, infraestructura urbana y salud. El análisis histórico muestra que los eventos extremos en América Latina producen efectos operativos y económicos más severos debido a la menor redundancia estructural y a la fragilidad de redes energéticas y logísticas.

Indicadores prioritarios incluyen variaciones anómalas en el régimen de lluvias, declive persistente de embalses estratégicos, aumento de la temperatura media en áreas productivas, ocurrencia repetida de olas de calor, inundaciones en corredores logísticos, incendios forestales en zonas críticas, reducción del nivel de ríos utilizados para transporte y presiones hídricas constantes en centros urbanos. La simultaneidad

de estos eventos señala la transición hacia ciclos más intensos y prolongados de inestabilidad.

Otro indicador clave es el aumento en el costo de seguros climáticos y paramétricos, pues el mercado financiero incorpora riesgos incluso antes de su materialización física. La elevación gradual de la prima de seguros señala deterioro de la resiliencia climática y necesidad de una adaptación más intensa.

Tabla 14 – Indicadores Climáticos y Ambientales (Resumen Ejecutivo)

Categoría de Indicador	Descripción de la Señal Anticipatoria	Implicación Estratégica	Relevancia para América Latina y Brasil
Variaciones anómalas de lluvia	Desvíos persistentes en el régimen de lluvias y reducción de la previsibilidad climática	Afecta agricultura, energía hidroeléctrica y abastecimiento urbano	Alta; eventos extremos más frecuentes y severos
Declive de embalses y acuíferos	Reducción continua de volúmenes de agua en áreas estratégicas	Presiona generación de energía, riego y abastecimiento humano	Muy alta; dependencia de la matriz hídrica es significativa
Aumento de la temperatura media	Elevación de temperaturas en áreas productivas y urbanas	Reduce productividad agrícola, aumenta enfermedades y eleva costos operativos	Alta; olas de calor ya afectan grandes centros urbanos
Olas de calor recurrentes	Ocurrencia repetida de picos extremos de temperatura	Afecta salud pública, estabilidad energética y condiciones de trabajo	Muy alta; fuerte impacto en operaciones industriales y urbanas
Inundaciones en corredores logísticos	Inundaciones y deslizamientos interrumpen vías críticas	Eleva costos de transporte, retrasa exportaciones y genera pérdidas productivas	Muy alta; infraestructura vulnerable a eventos extremos
Incendios forestales en zonas sensibles	Expansión de quemas naturales o criminales	Afecta biodiversidad, agronegocios, salud pública y cadenas logísticas	Alta; fronteras agrícolas y regiones remotas son muy expuestas
Reducción del nivel de ríos de transporte	Caída del calado en hidrovías esenciales	Interrumpe flujo agrícola e industrial, eleva costos logísticos	Muy alta; especialmente crítico en Brasil y en la Cuenca Amazónica

Presiones hídricas urbanas	Racionamiento, sobrecarga de redes y déficit de drenaje	Afecta movilidad, salud y seguridad urbana	Alta; ciudades latinoamericanas poseen infraestructura limitada
Aumento de seguros climáticos	Elevación continua de la prima de seguros y paramétricos	Indica deterioro de la resiliencia climática del territorio	Alta; el mercado reacciona antes de la materialización de los eventos

5.3. Indicadores Digitales y Tecnológicos

Los indicadores digitales monitorean la presión creciente sobre sistemas de información, datos, Inteligencia Artificial e infraestructuras críticas. América Latina es una de las regiones con mayor número de ataques cibernéticos per cápita, lo que demanda observación continua de anomalías digitales que pueden anteceder incidentes de gran escala.

Entre los principales indicadores están anomalías persistentes en accesos no autorizados, aumento de ataques de fuerza bruta, actividad inusual en *APIs*, desvíos conductuales en sistemas analíticos, fallas simultáneas en proveedores de nube, interrupciones en plataformas de pago, uso creciente de *deepfakes* para fraudes y campañas coordinadas de desinformación.

Indicadores de gobernanza también son relevantes, como retrasos en la implementación de regulaciones de IA, aumento de incidentes involucrando sesgo algorítmico, fallas de transparencia en modelos de decisión automatizada y ausencia de auditoría en sistemas críticos. Estas señales revelan fragilidad institucional y aumento de la probabilidad de eventos sistémicos.

Tabla 15 – Indicadores Digitales y Tecnológicos (Resumen Ejecutivo)

Categoría de Indicador	Descripción de la Señal Anticipatoria	Implicación Estratégica	Relevancia para América Latina y Brasil
Accesos no autorizados e intentos anómalos	Aumento persistente de intentos de intrusión y comportamientos fuera del patrón	Anuncia ataques coordinados y explotación de vulnerabilidades críticas	Muy alta; la región es objetivo prioritario de grupos globales

Ataques de fuerza bruta y explotación de APIs	Intensificación de intentos automatizados de quiebre de credenciales y manipulación de APIs	Indica riesgo de intrusión en sistemas operativos, financieros e industriales	Muy alta; amplia digitalización sin estandarización robusta
Desvíos conductuales en sistemas analíticos	Cambios inesperados en patrones de uso, transacciones o flujos internos	Puede indicar manipulación de modelos, fraudes o presencia de actores maliciosos	Alta; empresas dependen de sistemas analíticos poco protegidos
Fallas simultáneas en proveedores de nube	Interrupciones paralelas o inestabilidad en múltiples entornos cloud	Alto riesgo de falla sistémica e interrupción de operaciones críticas	Alta; fuerte dependencia de pocos proveedores globales
Inestabilidad en plataformas de pago	Caídas recurrentes, latencia anormal o inconsistencias en pagos digitales	Afecta servicios financieros, e-commerce y confianza pública	Muy alta; Brasil y México son polos de pagos digitales
Uso de deepfakes en fraudes y extorsiones	Expansión de falsificaciones hiperrealistas para estafas y manipulación	Eleva riesgos reputacionales y compromete procesos de verificación	Creciente; casos se multiplican a ritmo acelerado
Campañas coordinadas de desinformación	Acción combinada de bots y contenido manipulativo a gran escala	Afecta elecciones, reputación corporativa y estabilidad institucional	Muy alta; alta polarización facilita diseminación
Retrasos en regulación de IA	Falta de directrices claras, reglamentación lenta o fragmentada	Aumenta exposición a riesgos éticos, legales y de conformidad	Alta; maduración regulatoria en etapa inicial
Incidentes de sesgo algorítmico y falta de transparencia	Resultados inconsistentes, discriminación o decisiones automatizadas sin explicación	Compromete gobernanza digital y confianza de stakeholders	Alta; pocos sectores poseen auditoría algorítmica formal

Ausencia de auditoría en sistemas críticos	Falta de monitoreo sistemático en modelos de IA, algoritmos y redes	Eleva posibilidad de eventos sistémicos y fallas no detectadas	Muy alta; auditorías aún son incipientes en la región

5.4. Indicadores Sociopolíticos y Criminales

La convergencia entre inestabilidad institucional, presiones sociales y expansión de redes ilícitas crea un entorno que exige monitoreo constante. Indicadores sociopolíticos permiten anticipar ciclos de tensión que impactan directamente operaciones corporativas, cadenas logísticas e inversiones estratégicas.

Entre las señales prioritarias están el aumento expresivo de homicidios en regiones fronterizas, escalada de enfrentamientos entre facciones, infiltración de grupos ilícitos en corredores logísticos, intensificación de robos de carga, aumento de delitos ambientales vinculados a la minería ilegal, interferencias en puertos, presiones territoriales en regiones de minería y elevación de ataques a organismos públicos.

Indicadores institucionales incluyen retrasos persistentes en procesos regulatorios, volatilidad legislativa, disputas entre poderes, disminución de la confianza en instituciones, judicialización de políticas públicas, fragmentación de las agencias de seguridad, reducción del presupuesto de fiscalización y eventos que señalen crisis de gobernabilidad.

Tabla 16 – Indicadores Sociopolíticos y Criminales (Resumen Ejecutivo)

Categoría de Indicador	Descripción de la Señal Anticipatoria	Implicación Estratégica	Relevancia para América Latina y Brasil
Escalada de homicidios en regiones fronterizas	Aumento rápido y continuo de la violencia en áreas transfronterizas	Indica fortalecimiento de organizaciones criminales y disputas territoriales	Muy alta; fronteras amazónicas y Cono Sur son hotspots críticos
Enfrentamientos entre facciones y grupos armados	Intensificación de conflictos armados urbanos o rurales	Riesgo para cadenas logísticas, movilidad de empleados y activos corporativos	Muy alta; presencia fuerte de facciones y milicias en centros urbanos

Infiltración en corredores logísticos	Actuación criminal en puertos, carreteras, ferrocarriles y zonas aduaneras	Afecta exportaciones, contamina cadenas, facilita contrabando y lavado	Muy alta; puerta de entrada y salida de ilícitos hacia otros continentes
Robos de carga e interferencias en rutas	Aumento persistente en hurtos, saqueos o bloqueos territoriales	Eleva costos operativos y compromete continuidad logística	Alta; Brasil es uno de los líderes globales en robo de cargas
Delitos ambientales ligados a minería ilegal	Minería clandestina, explotación depredadora y ocupaciones irregulares	Riesgos reputacionales, jurídicos y operativos en áreas remotas	Muy alta; fuerte correlación con redes ilícitas transnacionales
Actividades ilícitas en puertos estratégicos	Señales de corrupción, pérdidas inexplicables, interferencia armada o sabotaje	Amenaza el comercio exterior, compliance e integridad de cargas	Muy alta; Santos, Colón, Guayaquil y Buenos Aires son puntos críticos
Presiones territoriales en áreas de minería	Expansión de invasiones, conflictos y presencia de grupos armados	Afecta minería, agronegocios, protección ambiental y seguridad de equipos	Alta; Amazonía, Orinoco y Cerrado presentan alta vulnerabilidad
Ataques a organismos públicos e instituciones	Incursiones criminales contra alcaldías, comisarías, tribunales y fuerzas de seguridad	Afecta legitimidad institucional y capacidad de respuesta estatal	Alta; eventos recientes muestran aumento de este tipo de violencia
Retrasos regulatorios persistentes	Morosidad o paralización de acciones regulatorias esenciales	Crea incertidumbre jurídica y operativa para sectores críticos	Alta; fragmentación regulatoria es marcada en la región
Volatilidad legislativa y disputas entre poderes	Cambios abruptos, conflictos entre poderes y judicialización excesiva	Reduce previsibilidad y aumenta riesgo de inestabilidad política	Muy alta; intensidad de fragmentación institucional es acentuada
Reducción de presupuesto de fiscalización	Recortes continuos en organismos ambientales, regulatorios y de seguridad	Amplía riesgo de ilícitos, degradación ambiental y vulnerabilidad estatal	Alta; común en ciclos de austeridad fiscal en la región

5.5. Indicadores Económicos y de Cadenas Críticas

La resiliencia económica depende de la estabilidad de las cadenas productivas, de la capacidad de financiamiento, de la previsibilidad regulatoria y del flujo eficiente de bienes y servicios. Indicadores económicos deben ser monitoreados en conjunto con riesgos climáticos y digitales, ya que rupturas simultáneas elevan drásticamente la probabilidad de inestabilidad sistémica.

Entre los indicadores esenciales están niveles críticos de stock en cadenas sensibles, interrupciones recurrentes en puertos y carreteras, fluctuaciones abruptas en el precio de combustibles, caída de la capacidad hídrica de usinas, retrasos en el flujo de la producción agrícola, interrupciones en la generación de petróleo debido a tormentas y presiones de crédito sobre consumidores y empresas.

La sensibilidad de los mercados financieros ante eventos climáticos o cibernéticos también funciona como indicador anticipatorio. Aumento abrupto del riesgo-país, elevación del spread bancario, retracción de inversiones y valorización de *commodities* climáticas pueden señalar deterioro anticipado del entorno operativo.

Tabla 17 – Indicadores Económicos y de Cadenas Críticas (Resumen Ejecutivo)

Categoría de Indicador	Descripción de la Señal Anticipatoria	Implicación Estratégica	Relevancia para América Latina y Brasil
Niveles críticos de stock en cadenas sensibles	Reducción acelerada o por debajo del mínimo operativo en sectores como alimentos, combustibles y medicamentos	Indica riesgo inminente de ruptura, desabastecimiento y aumento de precios	Muy alta; cadenas largas e infraestructura frágil amplifican rupturas
Interrupciones recurrentes en puertos y carreteras	Bloqueos, inundaciones, huelgas, accidentes y cuellos de botella estructurales	Afectan exportaciones, producción industrial y logística agrícola	Muy alta; dependencia exagerada del modo vial
Fluctuaciones bruscas en el precio de combustibles	Oscilaciones abruptas en petróleo, diésel, gas y energía	Presiona costos logísticos, afecta transporte y genera inestabilidad macroeconómica	Alta; volatilidad externa impacta economías importadoras

Caída de la capacidad hídrica de usinas	Reducción de generación hidroeléctrica y dependencia de emergencia de fuentes alternativas	Eleva costo de energía y riesgo de racionamientos	Muy alta; Brasil y países andinos dependen intensamente de hidroenergía
Retrasos en el flujo de la producción agrícola	Congestionamientos, falta de almacenes, déficits logísticos y fallas climáticas	Impacta exportaciones, aumenta pérdidas y reduce competitividad	Muy alta; agronegocio es pilar de la economía regional
Interrupciones en la producción de petróleo	Paradas causadas por tormentas, accidentes o fallas operativas	Presiona costos energéticos y compromete ingresos fiscales	Alta; Brasil, México y Venezuela son grandes productores
Presiones de crédito en consumidores y empresas	Aumento de morosidad, reducción de liquidez e intereses elevados	Afecta consumo, inversión y estabilidad financiera	Alta; economías sensibles a choques fiscales y monetarios
Aumento súbito en el riesgo-país	Percepción de riesgo político, fiscal o institucional por inversores	Eleva costo de capital, afecta tipo de cambio y reduce inversión externa	Muy alta; volatilidad institucional es característica regional
Elevación del spread bancario	Aumento de la diferencia entre costo de captación e intereses cobrados	Señala deterioro del entorno económico y mayor aversión al riesgo	Alta; crédito empresarial suele ser más caro en la región
Valorización anómala de commodities climáticas	Alza súbita en azúcar, soja, maíz, café, hidroenergía, seguros climáticos	Indica riesgos climáticos intensos o disfunciones en cadenas productivas	Muy alta; región es gran productora y altamente expuesta al clima

5.6. Radar Integrado de Señales Anticipatorias

La integración de los cuatro dominios presentados permite construir un radar que identifica no solo señales aisladas, sino patrones que anteceden eventos de gran impacto. La convergencia entre indicadores climáticos, digitales, criminales y económicos es el elemento que, en la práctica, genera rupturas significativas.

El radar integrado debe priorizar:

- Eventos climáticos que coincidan con fallas digitales o interrupciones energéticas;
- Actividad criminal creciente en regiones sensibles al flujo de producción;
- Anomalías simultáneas en sistemas de pago, cadenas logísticas e infraestructura crítica;
- Variaciones extremas en el nivel de embalses combinadas con presión en redes eléctricas;
- Indicadores institucionales que revelen pérdida de capacidad estatal.

La lectura combinada de estos elementos permite anticipar cambios en los escenarios delineados en el Capítulo 1 – ítem 1.5 e identificar el inicio de transiciones entre cuadrantes, especialmente cuando señales de fragmentación institucional se combinan con eventos climáticos y vulnerabilidades digitales.

Con esto, el radar de señales anticipatorias se convierte en instrumento fundamental para orientar decisiones estratégicas, revisar planes de continuidad, reforzar la seguridad convergente y alinear inversiones con las tendencias que moldearán a América Latina en 2026 y más allá.

5.7. Integración con las Directrices de la ISO 31050 para Riesgos Emergentes

La ISO 31050 amplía el entendimiento tradicional de la gestión de riesgos al enfatizar la necesidad de estructuras específicas para lidiar con riesgos emergentes caracterizados por novedad, incertidumbre extrema, datos insuficientes, complejidad y ambigüedad. Estos riesgos exigen un enfoque distinto del aplicado a riesgos conocidos, justamente porque no se manifiestan a través de señales clásicas, sino por medio de pequeñas anomalías, cambios contextuales discretos e interacciones que, aisladamente, pueden parecer irrelevantes.

En este sentido, el radar de señales anticipatorias descrito en los ítems anteriores debe ser interpretado a la luz de **tres principios fundamentales de la ISO 31050.**

El **primer principio** es el análisis continuo del contexto en múltiples dimensiones. Cambios climáticos, rupturas tecnológicas, transformaciones socioeconómicas, tensiones políticas y alteraciones regulatorias son parte del entorno en el que los riesgos emergentes se desarrollan. Estos elementos necesitan ser monitoreados simultáneamente, pues sus efectos combinados pueden crear condiciones propicias para la emergencia de nuevos riesgos sistémicos.

El **segundo principio** es la identificación e interpretación de señales débiles. Estas señales incluyen pequeñas fluctuaciones en indicadores climáticos, desvíos discretos en sistemas digitales, presiones territoriales aún incipientes, cambios en el comportamiento de consumidores, anomalías en cadenas logísticas y dificultades aisladas en proveedores críticos. La ISO 31050 destaca que los riesgos emergentes casi nunca se anuncian por eventos abruptos; surgen como patrones difusos que solo pueden ser percibidos con radar sensible, observación disciplinada y ciclos rápidos de interpretación.

El **tercer principio** es la necesidad de anticipación estratégica. La ISO 31050 orienta que los riesgos emergentes deben ser tratados como potenciales transformadores del entorno operativo y no solo como eventos puntuales. Esta perspectiva exige integración con análisis de escenarios, ejercicios de *foresight*, modelado de impactos y evaluación de interdependencias. Los riesgos emergentes son, en esencia, señales de cambios futuros, y su correcta lectura puede transformar incertidumbres en ventaja competitiva.

Al integrar estas directrices, el radar presentado al inicio del capítulo se convierte no solo en una herramienta de monitoreo, sino en un instrumento de resiliencia adaptativa que ayuda a las organizaciones a identificar tendencias, anticipar rupturas y preparar respuestas antes de que los eventos se conviertan en crisis.

5.8. El Ciclo de Inteligencia para Identificación de Señales Tempranas

La detección de riesgos emergentes y señales anticipatorias exige un proceso estructurado de inteligencia que transforme datos dispersos en *insights* estratégicos. Este proceso, reforzado por la ISO 31050, puede organizarse en cuatro etapas continuas.

La **primera etapa** es el encuadre. En ella, la organización define las preguntas críticas que orientan la búsqueda de señales: qué cambios en el entorno pueden alterar significativamente nuestras operaciones, cadenas críticas o estrategias. El encuadre también determina prioridades, dominios de interés, fronteras de análisis y el tipo de

impacto que se desea anticipar.

La **segunda etapa** es la recolección y verificación. Involucra la recolección sistemática de datos internos y externos, incluyendo registros climáticos, incidentes digitales, información de mercado, informes de organismos públicos, movimientos sociales, ruidos regulatorios, actividades inusuales de proveedores y eventos en regiones sensibles. La verificación garantiza calidad y confiabilidad, filtrando ruidos y destacando anomalías relevantes.

La **tercera etapa** es la interpretación. Es aquí donde las señales débiles se vuelven inteligibles. La interpretación involucra análisis crítico, modelado de riesgos, cruce de variables, lectura de patrones, elaboración de hipótesis y uso de herramientas de *foresight* para identificar posibles trayectorias de riesgo. Muchas veces, esta etapa requiere el uso de algoritmos de detección de anomalías, análisis conductuales o juicio especializado de equipos interdisciplinarios.

La **cuarta etapa** es la inteligencia aplicada. Se trata de la transformación del conocimiento producido en recomendaciones prácticas, priorizaciones de inversión, decisiones ejecutivas y ajustes de estrategia. La inteligencia aplicada garantiza que el radar no sea un proceso meramente analítico, sino un mecanismo efectivo de toma de decisiones.

Cuando se opera de forma continua, el ciclo de inteligencia permite que las organizaciones detecten riesgos emergentes en etapas iniciales, reduzcan la incertidumbre, mejoren la preparación y fortalezcan la resiliencia. Funciona como eslabón entre monitoreo y acción y debe ser revisado periódicamente para incorporar nuevas fuentes de datos, tecnologías, tendencias y cambios en el entorno externo.

5.9. Consolidación Final del Radar Anticipatorio

La inclusión de las orientaciones de la ISO 31050 y la adopción del ciclo de inteligencia amplían significativamente la capacidad del radar para identificar riesgos que se desarrollan silenciosamente, muchas veces imperceptibles para los indicadores tradicionales. La combinación entre indicadores estructurales (ítems 5.2 a 5.5), interpretación integrada (ítem 5.6) y mecanismos de anticipación estratégica (ítems 5.7 y 5.8) proporciona una estructura robusta para la detección temprana de rupturas.

Este radar expandido permite que las organizaciones:

- Anticipen ciclos climáticos adversos antes de su manifestación plena;

- Detecten presiones digitales y conductuales que anuncian ataques cibernéticos sofisticados;
- Reconozcan fragilidades institucionales y tensiones sociopolíticas antes de convertirse en crisis;
- Identifiquen riesgos sistémicos en cadenas críticas con tiempo suficiente para preparar redundancias;
- Conviertan señales débiles en decisiones preventivas y movimientos estratégicos

Con esto, el Capítulo 5 concluye mostrando que la verdadera resiliencia no depende solo de respuestas eficientes, sino de la capacidad de **leer el futuro mientras aún se está formando**, principio esencial de la gestión de riesgos emergentes y de la inteligencia estratégica alineada a la ISO 31050.

06

RECOMENDACIONES EJECUTIVAS Y CAMINOS FUTUROS

6.1. Introducción

El entorno estratégico de América Latina en 2026 y en los años subsiguientes será moldeado por combinaciones complejas de riesgos climáticos, digitales, criminales y económicos, intensificados por vulnerabilidades estructurales y fragmentación institucional. A la luz de los análisis prospectivos, de los escenarios construidos, de la lectura sectorial y del radar de señales anticipatorias, se hace evidente que las organizaciones públicas y privadas necesitan adoptar una postura más dinámica, preventiva e integrada. La capacidad de anticipar tendencias, interpretar señales débiles, fortalecer la gobernanza y construir resiliencia pasa a ser elemento central de competitividad y supervivencia.

Este capítulo presenta un conjunto estructurado de recomendaciones ejecutivas que funcionan como transición natural entre los escenarios prospectivos y los caminos estratégicos de fortalecimiento institucional, económico y operativo. Las recomendaciones están organizadas en ejes que dialogan directamente con los cuatro cuadrantes de la matriz de escenarios y con las fragilidades y oportunidades identificadas a lo largo de este estudio.

6.2. Reforzar la Gobernanza Estratégica de Riesgos a Nivel de Consejo

La primera transformación necesaria consiste en reposicionar la gestión de riesgos como disciplina estratégica y no solo operativa. Los Consejos y comités ejecutivos deben incorporar análisis de escenarios, riesgos emergentes, indicadores prospectivos y métricas de resiliencia como elementos permanentes del proceso de decisión.

Para ello, se recomienda:

- Incorporar informes periódicos de riesgos emergentes y análisis de señales anticipatorias;
- Integrar ISO 31000 e ISO 31050 como base estructurante de la gobernanza;
- Crear agendas de riesgo dedicadas en reuniones de Consejo;
- Definir responsabilidades claras entre Consejo, dirección y gestión operativa;
- Incluir análisis de interdependencias, efectos en cascada y riesgos sistémicos.

La madurez de la gobernanza pasa a determinar la capacidad de adaptación a los rápidos cambios del entorno.

6.3. Construir Resiliencia en Infraestructuras Críticas y Cadenas Sensibles

Los análisis de este informe indican que los riesgos climáticos y digitales serán los principales factores de ruptura en cadenas productivas, redes logísticas, puertos, sistemas de energía, telecomunicaciones y abastecimiento urbano. Por eso, se recomienda la adopción de estructuras robustas de resiliencia intersectorial.

Las organizaciones deben:

- Ampliar redundancias estructurales y tecnológicas;
- Fortalecer mecanismos de monitoreo continuo de cadenas críticas;
- Integrar datos climáticos avanzados e inteligencia territorial en la gestión operativa;
- Mejorar planes de contingencia considerando rupturas simultáneas;
- Desarrollar alianzas con gobiernos y otros sectores para la protección compartida de puertos, carreteras y centros logísticos.

Las organizaciones con actuación transnacional necesitan, además, adoptar protocolos regionales de resiliencia, especialmente en operaciones que atraviesan corredores sensibles.

6.4. Aumentar la Madurez Digital y la Gobernanza de Inteligencia Artificial

El avance de la digitalización, aliado a la creciente sofisticación de ataques cibernéticos, exige que empresas y gobiernos adopten modelos maduros de protección de datos, sistemas críticos y estructuras de IA. Este informe muestra que América Latina permanece vulnerable tanto por la falta de estandarización regulatoria como por la adopción acelerada y, muchas veces, descoordinada de nuevas tecnologías. Se recomienda:

- Implementación de políticas formales de gobernanza de IA;
- Creación de mecanismos de auditoría algorítmica y explicabilidad;
- Segmentación avanzada de redes y protección de APIs;
- Uso de inteligencia artificial defensiva integrada a centros de operación de seguridad;
- Adopción de estándares internacionales de protección de infraestructura crítica digital;
- Reducción de dependencia de proveedores únicos de nube;
- Capacitación continua para equipos de seguridad cibernética y desarrollo.

Las organizaciones maduras deben evolucionar hacia modelos de seguridad convergente, en los cuales la inteligencia de riesgo, el análisis de anomalías y la gestión digital se integran al nivel ejecutivo.

6.5. Adaptarse al Clima como Principal Multiplicador de Riesgo

El clima es, conforme a lo demostrado en el Capítulo 5, el elemento de mayor impacto transversal entre sectores. Los eventos extremos aumentan costos logísticos, presionan la energía, reducen la productividad agrícola, debilitan infraestructuras y desencadenan crisis sanitarias y sociales.

Para mitigar estos efectos, se recomienda:

- Fortalecer planes de adaptación climática a nivel corporativo y sectorial;
- Invertir en infraestructura resiliente y sistemas de drenaje;
- Incorporar datos climáticos y modelos predictivos en las operaciones;
- Adoptar seguros paramétricos para riesgos extremos;
- Desarrollar protocolos para el trabajo en condiciones de calor severo;
- Mapear dependencias hídricas y reducir vulnerabilidades críticas.

En el ámbito público, los gobiernos deben acelerar la modernización de infraestructura urbana, protección de cuencas hidrográficas, gestión de represas y refuerzo de redes energéticas.

6.6. Enfrentar Redes Ilícitas y Fortalecer la Seguridad Multidimensional

Los escenarios apuntan a la expansión de redes ilícitas transnacionales, aumento de enfrentamientos, fragmentación institucional e infiltración criminal en cadenas logísticas, especialmente en puertos y fronteras. La seguridad corporativa pasa a depender de respuestas integradas involucrando al sector público, empresas, sociedad civil y cooperación internacional.

Se recomiendan acciones como:

- Adopción de mecanismos de *due diligence* ampliada en proveedores críticos;
- Integración entre seguridad física, digital, ambiental y financiera;
- Uso de sistemas avanzados de trazabilidad de cargas e insumos;
- Fortalecimiento de alianzas con autoridades policiales y aduaneras;

- Creación de protocolos de inteligencia corporativa enfocados en crimen organizado;
- Desarrollo de sistemas de protección para ejecutivos, trabajadores y operaciones en regiones remotas.

Las organizaciones necesitan tratar el riesgo criminal como riesgo estratégico, no solo operativo.

6.7. Armonizar la Regulación y Mejorar la Capacidad Estatal

La fragmentación regulatoria descrita a lo largo de este informe eleva costos, genera incertidumbres y reduce la competitividad. La región demanda movimientos de convergencia regulatoria para protección de datos, Inteligencia Artificial, ciberseguridad, combate al delito financiero, infraestructura crítica y gobernanza ambiental.

Se recomienda:

- Crear foros nacionales y regionales de armonización regulatoria;
- Fortalecer la autonomía y capacidad técnica de agencias reguladoras;
- Ampliar la digitalización segura de servicios públicos;
- Invertir en sistemas integrados de fiscalización ambiental y tributaria;
- Acelerar procesos legislativos que traten riesgos emergentes.

La capacidad estatal **de aplicación efectiva de la ley** *(enforcement)* es fundamental para sostener el crecimiento económico y la estabilidad institucional.

6.8. Desarrollar Ecosistemas de Cooperación e Inteligencia Colectiva

El entorno de riesgos híbridos exige colaboración constante entre sectores. Ninguna organización, pública o privada, puede responder aisladamente a riesgos sistémicos. La integración entre empresas, gobiernos, universidades, centros de investigación y organismos multilaterales fortalece soluciones, crea estándares regionales y aumenta la resiliencia.

Se recomienda:

- Creación de redes de inteligencia compartida entre sectores;
- Iniciativas de interoperabilidad de datos en infraestructuras críticas;

- Alianzas de innovación para el desarrollo de tecnologías de detección de riesgos;
- Cooperación transfronteriza para protección de rutas logísticas y fronteras;
- Participación activa en consorcios y alianzas regionales;
- Estímulo a la investigación aplicada en clima, IA, seguridad e infraestructura.

Estos ecosistemas impulsan la capacidad colectiva de prevención, respuesta y recuperación.

6.9. Integrar Foresight, Escenarios y Señales Anticipatorias Como Proceso Continuo

La ISO 31050 orienta que la gestión de riesgos emergentes debe ser apoyada por métodos continuos de *foresight*, detección de señales débiles e interpretación dinámica del entorno.

El Capítulo 5 demostró que gran parte de las rupturas en 2026 y más allá serán precedidas por microindicios que exigen vigilancia disciplinada.

Por eso, las organizaciones deben:

- Institucionalizar ejercicios de escenarios y prospectiva;
- Crear rutinas de monitoreo de señales débiles y *early warnings*;
- Actualizar periódicamente matrices de impacto cruzado;
- Revisar planes estratégicos a la luz de cambios en el entorno;
- Ajustar criterios de riesgo para soportar incertidumbre profunda;
- Integrar equipos multidisciplinarios de inteligencia y riesgo.

La capacidad de anticipación se convierte en eje central de la resiliencia.

6.10. Caminos Futuros: La Construcción de un Horizonte de Resiliencia para América Latina

América Latina posee alto potencial para transformar vulnerabilidades en oportunidades estratégicas. Los escenarios presentados muestran que, a pesar de la fragmentación institucional, la región reúne ventajas competitivas importantes en energía renovable, biodiversidad, agricultura avanzada, minería de alto valor, innovación digital y economía creativa.

Para aprovechar este potencial, se recomienda:

- Construir políticas públicas integradas de resiliencia;
- Alinear inversiones estratégicas con tendencias globales de innovación;
- Posicionar a la región como referencia en gobernanza de IA y sostenibilidad;
- Fortalecer la cooperación regional para infraestructura y seguridad;
- Ampliar la capacidad científica y tecnológica;
- Atraer alianzas internacionales para el desarrollo sostenible.

Brasil, como mayor economía de la región, tiene un papel decisivo en la articulación de este horizonte estratégico, pudiendo liderar consorcios regionales de resiliencia, estandarización regulatoria, protección de infraestructuras críticas e innovación climática.

Tabla 18 – Cuadro Resumen: Recomendaciones Ejecutivas y Caminos Futuros

Eje Estratégico	Recomendación Central	Objetivo Principal	¿Por qué es crítico para 2026 y más allá?
1. Gobernanza de Riesgos a Nivel de Consejo	Integrar riesgos emergentes, escenarios e ISO 31050 a la toma de decisión	Fortalecer la visión a largo plazo y reducir puntos ciegos estratégicos	Los entornos volátiles exigen decisiones ancladas en anticipación y resiliencia
2. Resiliencia de Infraestructuras Críticas	Proteger puertos, energía, logística, telecom y abastecimiento	Evitar rupturas sistémicas y minimizar efectos en cascada	Riesgos climáticos y digitales aumentan fallas simultáneas en la región
3. Madurez Digital y Gobernanza de IA	Estructurar políticas robustas de datos, IA y ciberseguridad	Reducir ataques, fallas y sesgo digital, preservando la continuidad	América Latina es uno de los principales objetivos globales de ataques cibernéticos
4. Adaptación Climática Integrada	Incorporar modelos climáticos a la operación y a la planificación	Proteger producción, energía, logística y centros urbanos	El clima es el mayor multiplicador de riesgos de la región
5. Combate a Redes Ilícitas y Crimen Transnacional	Integrar seguridad física, digital, territorial y financiera	Preservar cadenas críticas y reducir exposición a ilícitos	El crecimiento de facciones y rutas ilegales afecta múltiples sectores

6. Armonización Regulatoria y Fortalecimiento Estatal	Reducir fragmentación y aumentar capacidad regulatoria	Crear previsibilidad jurídica y capacidad de enforcement	La incertidumbre regulatoria es uno de los mayores riesgos de América Latina
7. Ecosistemas de Cooperación	Crear redes público-privadas y alianzas regionales de resiliencia	Compartir inteligencia y estandarizar prácticas	Ningún actor aislado logra enfrentar riesgos híbridos
8. Integración de Foresight, Señales Débiles y Prospectiva	Transformar el radar anticipatorio en proceso continuo	Mejorar capacidad de detectar cambios antes de que se vuelvan crisis	La ISO 31050 refuerza la prospectiva como base de la gestión de riesgos emergentes
9. Caminos Futuros para América Latina	Posicionar a la región como líder en energía, IA, agricultura y sostenibilidad	Aprovechar ventajas competitivas y atraer inversiones	La región puede evolucionar de vulnerable a protagonista global

07

CONCLUSIÓN Y APÉNDICES

Conclusión

El análisis integrado realizado a lo largo de este estudio revela una América Latina que camina hacia 2026 y más allá inmersa en un entorno de riesgos híbridos, interdependientes y acelerados, en el cual choques climáticos, fragilidades digitales, tensiones sociopolíticas y presiones económicas no solo coexisten, sino que se amplifican mutuamente. El ejercicio de escenarios demostró que el futuro regional será moldeado por fuerzas que escapan a los modelos tradicionales de previsión y exigen enfoques dinámicos, orientados por inteligencia y capaces de lidiar con incertidumbre profunda.

La región enfrenta desafíos estructurales, como fragmentación institucional, desigualdad, vulnerabilidad climática, expansión del crimen transnacional y asimetrías tecnológicas. Estos elementos, cuando se combinan, aumentan la probabilidad de rupturas sistémicas, especialmente en cadenas críticas como energía, logística, alimentación, telecomunicaciones, finanzas e infraestructura urbana. Al mismo tiempo, América Latina presenta oportunidades expresivas en sectores de alta relevancia global, como agricultura sostenible, energía renovable, minería estratégica e innovación digital. La trayectoria hacia 2026 y más allá no será lineal, sino marcada por disputas entre estas fuerzas.

El estudio muestra que la resiliencia organizacional dependerá menos de la capacidad de reaccionar ante crisis y más de la habilidad **de interpretar señales anticipatorias, detectar riesgos emergentes, integrar escenarios al proceso de decisión y actuar con inteligencia adaptativa**. La ISO 31050 refuerza este punto al destacar que los riesgos emergentes surgen inicialmente como señales débiles, discretas, dispersas y ambiguas, que solo pueden ser comprendidas por organizaciones que adoptan procesos continuos de *foresight* e inteligencia de riesgo. En este sentido, el radar anticipatorio presentado en el Capítulo 5 no es solo un instrumento analítico, sino un mecanismo de supervivencia institucional en un entorno de cambios rápidos y muchas veces imprevisibles.

También se evidencia que la gobernanza será el eje decisivo de diferenciación entre organizaciones y países. La capacidad estatal de aplicación efectiva de la ley, la previsibilidad regulatoria, la coordinación institucional y la integridad pública se vuelven determinantes tanto para la seguridad como para el crecimiento económico. Países con gobernanzas frágiles enfrentarán mayor exposición a redes ilícitas, volatilidad financiera, inseguridad digital y conflictos territoriales. Países con gobernanza más sólida tendrán condiciones de liderar agendas de resiliencia, innovación e integración regional.

Las empresas también necesitan reposicionar su visión estratégica. Los modelos

tradicionales de seguridad, continuidad y gestión de riesgos ya no son suficientes ante amenazas que atraviesan simultáneamente entornos físicos, digitales, reputacionales y climáticos. Las organizaciones resilientes serán aquellas que adopten seguridad convergente, gobernanza robusta de IA, protección de infraestructuras críticas, autonomía digital, diversificación de cadenas productivas y mecanismos adaptativos de respuesta.

El estudio deja claro que el clima será el mayor multiplicador de riesgos en la región. La combinación de olas de calor, eventos extremos, pérdida hídrica, incendios e impactos sobre la agricultura y la energía afectará directamente la competitividad regional. Al mismo tiempo, abre espacio para oportunidades de liderazgo en bioeconomía, energías limpias, agricultura de precisión, infraestructura resiliente y tecnologías verdes. La capacidad de adaptación climática será medida por la rapidez con la que gobiernos y empresas incorporen inteligencia climática a sus decisiones.

En el campo digital, los riesgos evolucionan a una velocidad aún mayor. América Latina permanece entre las regiones más atacadas del mundo, y la adopción acelerada de Inteligencia Artificial — sin mecanismos maduros de gobernanza — amplía no solo vulnerabilidades técnicas, sino riesgos éticos, legales y reputacionales. La madurez digital ya no es un diferencial competitivo, sino una condición mínima para operar. Las organizaciones que no evolucionen hacia modelos de protección integrados, con automatización defensiva, auditoría algorítmica y segmentación avanzada, enfrentarán interrupciones, fraudes y exposición sistémica.

Cuando confrontamos todos estos elementos — clima, tecnología, crimen, gobernanza y economía — percibimos que América Latina no enfrenta solo riesgos aislados, sino un **nuevo régimen de riesgo**, caracterizado por simultaneidad, velocidad, interdependencia y profundidad transformacional. Esta combinación exige que gobiernos, empresas y sociedad adopten una postura más madura, colaborativa y orientada hacia la construcción de capacidades estructurales a largo plazo.

La conclusión más contundente de este estudio es que el **mayor riesgo de América Latina no es climático, ni digital, ni económico; es la falta de integración entre ellos**. El riesgo sistémico surge justamente de la incapacidad colectiva de comprender cómo estas dimensiones se alimentan mutuamente y exigen respuestas coordinadas. La región podrá caminar hacia ciclos recurrentes de crisis, o podrá transformarse en referencia global de resiliencia e innovación, dependiendo de la calidad de las decisiones tomadas hoy.

En síntesis, el futuro de América Latina será definido por tres fuerzas centrales: **la capacidad de anticipar, la capacidad de cooperar y la capacidad de adaptar.** Las

organizaciones que combinen inteligencia de riesgo, gobernanza estratégica, resiliencia operativa y visión a largo plazo podrán no solo sobrevivir, sino liderar la transformación. Aquellas que permanezcan ancladas en modelos reactivos enfrentarán un entorno cada vez más hostil, inestable e imprevisible.

Más que señalar riesgos, este estudio evidencia caminos. La región tiene potencial para evolucionar de un territorio marcado por vulnerabilidades a un polo global de soluciones en seguridad, sostenibilidad, energía, tecnología y agricultura. El futuro aún no está definido. Será moldeado por la capacidad de gobiernos, empresas e instituciones de transformar incertidumbre en estrategia, turbulencia en innovación y riesgos emergentes en ventaja competitiva.

Apéndice A – Metodología Utilizada

La construcción de este estudio siguió un enfoque metodológico anclado en los principios de la ISO 31000 y, sobre todo, de la ISO 31050, que establece directrices específicas para la identificación, análisis y gestión de riesgos emergentes en entornos caracterizados por alta complejidad, incertidumbre estructural e interdependencia sistémica. Todo el proceso analítico adoptó como técnica central el *horizon scanning*, comprendida como una metodología sistemática de exploración de evidencias, tendencias y señales anticipatorias provenientes de múltiples fuentes, con el objetivo de identificar elementos que puedan influir en el entorno de riesgos en el horizonte de mediano plazo.

El *horizon scanning* se aplicó involucrando la recolección, lectura, categorización temática y comparación cruzada de treinta y dos informes nacionales e internacionales publicados entre 2024 y 2025. Este conjunto formó la base documental primaria y fue tratado como corpus de evidencias para la interpretación prospectiva. El proceso se inició con la extracción y organización sistemática de los elementos clave de cada documento, incluyendo riesgos emergentes, tendencias estructurales, indicadores, incertidumbres críticas y cambios en curso. A partir de este material bruto, se crearon fichas-fuente que permitieron realizar una lectura transversal estandarizada de las contribuciones originales, en línea con las recomendaciones de la ISO 31050 para la reducción de sesgos de selección y ampliación de la diversidad informativa.

Tras esta etapa de mapeo exploratorio, se condujo un análisis de triangulación estructural de fuentes, utilizada como técnica complementaria esencial para garantizar robustez y coherencia. La triangulación consistió en confrontar sistemáticamente los hallazgos de los diferentes informes, identificando convergencias recurrentes, divergencias significativas y brechas temáticas. Esta comparación cruzada permitió validar la consistencia interna de los hallazgos, reducir el riesgo de sobreinterpretación de evidencias aisladas y asegurar que las conclusiones derivaran de patrones amplios y no de opiniones o tendencias específicas de una única institución. Este método es ampliamente reconocido en los estudios de riesgos emergentes y encuentra correspondencia directa con el énfasis de la ISO 31050 en la multiperspectividad y en la integración de fuentes heterogéneas.

Durante todo el proceso analítico, se utilizó apoyo de Inteligencia Artificial como herramienta de organización, clusterización preliminar de temas e identificación de patrones semánticos entre las fuentes. Su papel se restringió a la etapa de procesamiento y ordenación de las evidencias, proporcionando una base estructurada sobre la cual el equipo analítico pudo actuar con mayor precisión.

La etapa subsiguiente consistió en la síntesis interpretativa, en la cual se consolidaron **seis fuentes de riesgo críticas** derivadas del análisis cruzado. Esta síntesis siguió los principios de la ISO 31050 al integrar riesgos de naturaleza tecnológica, climática, geopolítica, institucional, criminal e infraestructural, reconociendo que los riesgos emergentes raramente operan aislados y tienden a manifestarse de forma convergente, acumulativa y no lineal. En conformidad con el enfoque sistémico de la norma, se privilegiaron interpretaciones capaces de capturar interdependencias, tensiones y combinaciones de riesgos con potencial de producir efectos amplificados.

A lo largo del estudio, estas seis fuentes de riesgo son tratadas como el núcleo estructural de las dinámicas de riesgo regional, razón por la cual se denominan **fuentes de riesgo críticas.**

A partir de estas **seis fuentes de riesgo críticas**, se desarrollaron cuadros prospectivos que culminaron en la elaboración de la Matriz de Escenarios 2026. La técnica de escenarios, recomendada por la ISO 31050 para lidiar con incertidumbres profundas, se aplicó de forma cualitativa e interpretativa, utilizando los ejes de mayor tensión identificados por el *horizon scanning.* Los escenarios resultantes no tienen carácter predictivo, sino exploratorio, con el objetivo de ampliar la capacidad decisoria, identificar vulnerabilidades sistémicas y anticipar posibles futuros que impacten a organizaciones públicas y privadas en Brasil y América Latina.

Por último, el estudio pasó por un proceso de revisión técnica y validación externa, en el cual versiones parciales y la versión final fueron sometidas a especialistas de diferentes países de América Latina, garantizando diversidad de perspectivas regionales. Esta revisión crítica tuvo como propósito evaluar la coherencia de los hallazgos, la robustez de las inferencias, la claridad conceptual y la adherencia a las prácticas internacionales de análisis prospectivo. Las contribuciones provenientes de esta etapa fueron incorporadas para fortalecer el rigor metodológico y asegurar que el documento final represente una interpretación sólida y defendible del entorno de riesgos proyectado para 2026 y años subsiguientes.

Este proceso metodológico, integralmente fundamentado en *horizon scanning,* triangulación de fuentes y análisis cualitativo en conformidad con la ISO 31050, ofrece una estructura de trabajo transparente y alineada con las mejores prácticas internacionales para estudios de riesgos emergentes de naturaleza sistémica y prospectiva.

Limitaciones del Estudio y Alcance de Uso

Este estudio adopta un enfoque prospectivo, cualitativo y exploratorio, alineado a los

principios de la ISO 31000 y a las directrices específicas de la ISO 31050 para el análisis de riesgos emergentes y escenarios de incertidumbre profunda. Por esta razón, es fundamental aclarar explícitamente sus limitaciones y el alcance adecuado de uso de sus conclusiones. El

objetivo central del estudio no es predecir el futuro, establecer probabilidades matemáticas de eventos ni formular modelos econométricos o proyecciones cuantitativas. Su propósito es ampliar la capacidad decisoria de organizaciones públicas y privadas mediante la identificación de tendencias estructurales, mapeo de riesgos convergentes, análisis sistémico y construcción de escenarios plausibles que sirvan como base para la planificación estratégica, anticipación de amenazas y fortalecimiento de la resiliencia institucional.

La metodología empleada, fundamentada en *horizon scanning*, triangulación de fuentes y análisis interpretativo, privilegia la integración de múltiples perspectivas y la identificación de patrones emergentes en un entorno de incertidumbre, pero no tiene la pretensión de ofrecer previsiones deterministas, cálculos de probabilidad o mediciones estadísticas de impacto. Estos enfoques, aunque valiosos en otros contextos, serían inadecuados para el tipo de fenómeno analizado, caracterizado por interdependencia sistémica, dinámicas no lineales y eventos potencialmente disruptivos que escapan a modelos cuantitativos tradicionales.

Las conclusiones presentadas reflejan una síntesis calificada de las evidencias disponibles en el momento de la elaboración del estudio, considerando los límites naturales de las fuentes utilizadas, así como el hecho de que las tendencias y los riesgos emergentes pueden evolucionar de forma rápida e inesperada. Así, se recomienda que los hallazgos sean utilizados como insumo estratégico complementario, y no como única base para decisiones críticas. El estudio no sustituye análisis sectoriales específicos, evaluaciones cuantitativas internas, diagnósticos regulatorios o estudios técnicos especializados en áreas como macroeconomía, clima, criminalidad o tecnología de la información.

Finalmente, por tratarse de un documento prospectivo, sus recomendaciones deben ser periódicamente revisadas, ajustadas y validadas a la luz de nuevos datos, cambios geopolíticos y transformaciones tecnológicas. La utilidad del estudio reside justamente en su capacidad de orientar decisiones en contextos de incertidumbre, ofrecer referencias claras para el monitoreo continuo y sostener procesos de resiliencia organizacional, y no en proporcionar respuestas definitivas sobre futuros específicos. Dentro de estos límites, el estudio permanece plenamente coherente, metodológicamente sólido y adecuado a su propósito estratégico.

Apéndice B – Lista de Fuentes Consultadas

Este estudio se basa en el análisis profundo de **32 informes nacionales e internacionales publicados entre 2024 y 2025**, seleccionados por su relevancia metodológica y capacidad de iluminar tendencias, fuentes de riesgo y transiciones sistémicas pertinentes al horizonte prospectivo de 2026 y más allá.

La matriz analítica utilizada en este Informe divide el conjunto de amenazas y tendencias en seis Fuentes de Riesgo, conforme definido en el ítem 1.4.

Para las definiciones completas de las Fuentes de Riesgo (1 a 6) y de los Escenarios Estructurantes (1 a 4), consulte los ítems 1.4 y 1.5.

Tabla 19 – Informes y Ejes de Contribución

Nº	Informe/Documento	Organización	Año	Fuentes de Riesgo Contribuyentes	Escenarios Contribuyentes
1	*Global Risk Report 2024*	United Nations	2024	(i), (iv)	Escenario 3
2	*Global Risks Report 2025*	World Economic Forum	2025	(i), (ii)	Todos (matriz base)
3	*Top Risks 2025*	Eurasia Group / IA	2025	(i), (vi)	Escenario 2
4	*Global Trends 2040*	U.S. Intelligence Community	2021	(i), (ii)	Escenario 1
5	*Strategic Outlook 2025*	Think Tank Internacional	2025	(i), (vi)	Escenario 3
6	*Strategic Intelligence Estimate 2025*	Think Tank Militar / Inteligencia	2025	(i), (ii)	Escenario 2
7	*Risk Report 2025*	Corporate & Economic Analysis	2025	(vi), (iv)	Escenario 4
8	*Polycrisis Introduction 2024*	Varios Autores / Policrises	2024	(i), (vi)	Matriz (riesgos convergentes)
9	*Cenário Macroeconômico Global e Brasil 2025*	Institución Económica Brasileña	2025	(i), (vi)	Escenario 3
10	*FUSk - Fundación Sherman Kent – Primer Informe*	FUSK	2024–25	(vi), (iii)	Escenario 2

11	*Risk in Focus: Latin America 2026*	Corporate LATAM	2025	(vi), (iii)	Escenario 2
12	*Riesgo Político América Latina 2025*	CEIUC	2025	(vi), (i)	Escenario 2
13	*Global Riesgo Pronóstico 2025*	Crisis24	2025	(vi), (iii)	Escenario 2
14	*Global Safety Report 2025*	Gallup	2025	(vi), (iii)	Escenario 2
15	*Global Organized Crime Index 2025*	GI-TOC	2025	(iii), (vi)	Escenario 2
16	*2025 Security Benchmark Report*	Corporate Security Benchmark	2025	(v), (iii)	Escenario 4
17	*2025 CSO Survey*	Clarity Factory	2025	(v), (ii)	Escenario 1
18	*The State of Financial Crime 2025*	Consultora Financiera Internacional	2025	(iii), (ii)	Escenario 2
19	*Global Terrorism Index 2025*	IEP	2025	(iii), (i)	Escenario 2
20	*Relatório Global de Auditoria Interna 2025*	IIA	2025	(vi), (ii)	Escenario 1
21	*Internal Audit Global Hot Topics 2025*	IIA	2025	(ii), (iii)	Escenario 4
22	*Propuesta Agers–IAI V5*	Agers / IAI	2025	(iv), (v)	Escenario 3
23	*Communications Security Annual Report 2024*	Communications Security Group	2024	(ii), (v)	Escenario 4
24	*Global Cybersecurity Outlook 2025*	WEF	2025	(ii), (v)	Escenario 4
25	*AI & Cybersecurity Report 2025*	WEF	2025	(ii), (v)	Escenario 1
26	*Microsoft Digital Defense Report 2025*	Microsoft	2025	(ii), (iii)	Escenario 2
27	*AI Security Framework*	IA Security Consortium	2025	(ii), (v)	Escenario 4
28	*Risk Radar 2025*	Healix	2025	(iv), (vi)	Escenario 3

29	*The Future of the Risk Management Profession 2025*	Consultora Especializada	2025	(ii), (vi)	Escenario 1
30	*Estudo t-Risk – Riscos Corporativos 2025*	Plataforma t-Risk	2025	(v), (ii)	Apoyo transversal
31	*Risk in Focus 2026 – Middle East. 2025*	IIA	2025	(ii), (vi)	Escenario 1
32	*White papers e briefs adicionales (IA–Cyber)*	WEF	2025	(ii), (v)	Escenarios 1 y 4

Apéndice C – Glosario de Siglas

El presente glosario reúne las siglas utilizadas a lo largo de este estudio y tiene como objetivo apoyar la lectura técnica, reducir la ambigüedad y reforzar la coherencia conceptual con las normas de gestión de riesgos de la familia ISO 31000 y con la ABNT. Los significados se presentan en portugués, con indicación del término original cuando es relevante, y siempre contextualizados al uso específico en este informe.

Tabla 20 – Glosario de Siglas

Sigla	Término por extenso	Definición aplicada en este estudio
ABNT	*Asociación Brasileña de Normas Técnicas*	Entidad responsable por la normalización técnica en Brasil, incluyendo la adopción nacional de las normas ISO de gestión de riesgos, como ABNT NBR ISO 31000 y ABNT ISO/TS 31050.
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*	Estructura de referencia internacional para gestión de riesgos corporativos y controles internos, utilizada aquí como base para discutir madurez de gobernanza de riesgos, especialmente en servicios financieros y en el sector corporativo en general.
ESG	*Ambiental, Social y Gobernanza (Environmental, Social and Governance)*	Enfoque integrado de evaluación de desempeño de organizaciones en aspectos ambientales, sociales y de gobernanza. En el estudio, ESG aparece como eje de presión regulatoria, de riesgo reputacional y de ventaja competitiva en diversos sectores, como agronegocios, energía y finanzas.
ERM	*Enterprise Risk Management*	Modelo de gestión de riesgos a nivel corporativo, que integra riesgos estratégicos, operativos, financieros, de conformidad y de reputación. El estudio dialoga con el concepto de ERM al proponer una visión integrada de escenarios, sectores y continuidad de negocios.
EE. UU.	*Estados Unidos de América*	Principal referencia de comparación internacional para capacidades de seguridad, innovación tecnológica, mercado financiero y gobernanza de riesgos, especialmente en los capítulos sectoriales.
UE	*Unión Europea (en inglés European Union, EU)*	Bloque regional utilizado como referencia para estándares regulatorios, gobernanza climática, protección de datos, auditoría algorítmica e integración de cadenas productivas.
EWI	*Early Warning Indicator (Indicador de Alerta Temprana)*	Indicadores cuantitativos o cualitativos diseñados para captar señales anticipatorias de cambios de escenario, ruptura o deterioro de riesgo. En el informe EWI están

		organizados en un radar de señales para apoyar el monitoreo estratégico continuo.
GI-TOC	*Global Initiative Against Transnational Organized Crime*	Organización internacional que produce el Global Organized Crime Index. En este estudio, GI-TOC es referencia empírica para análisis de crimen organizado transnacional, mercados ilícitos y sus impactos en América Latina.
GRC	*Governance, Risk and Compliance*	Enfoque integrado de gobernanza, gestión de riesgos y conformidad. Aunque el foco del informe sea macroestratégico, GRC aparece como referencia de estructura organizacional para conectar riesgos, controles, auditoría y seguridad corporativa.
IA	*Inteligencia Artificial*	Conjunto de técnicas computacionales de aprendizaje automático (machine learning), modelos estadísticos y sistemas automatizados de decisión, que amplían la eficiencia y también introducen nuevos riesgos digitales, éticos, regulatorios y de seguridad, en especial en entornos de alta complejidad e interdependencia.
IAG	*Inteligencia Artificial Generativa*	Subconjunto de la Inteligencia Artificial capaz de generar textos, imágenes, voz, código y otros contenidos con base en grandes modelos de lenguaje o modelos multimodales. En el estudio, IAG es tratada como vector tanto de innovación como de riesgo, especialmente en fraudes digitales, desinformación y deepfakes.
ICS	*Industrial Control Systems (Sistemas de Control Industrial)*	Conjunto de sistemas, sensores, actuadores y software que controlan procesos físicos en industrias, energía, saneamento, transporte y otras infraestructuras críticas. Son objetivos prioritarios de ataques cibernéticos que pueden generar impactos físicos relevantes en la operación.
ICS-5	*Seguridad Corporativa Integrada en cinco capas (Integrated Corporate Security)*	Estructura conceptual utilizada en el estudio para organizar la seguridad corporativa en cinco capas integradas: gobernanza y estrategia; protección de personas y activos físicos; seguridad digital y de datos; gestión de proveedores y cadena de valor; inteligencia de riesgos y continuidad de negocios. Funciona como referencia para arquitecturas de seguridad convergente.
IoT	*Internet de las Cosas (Internet of Things)*	Red de dispositivos físicos conectados que recolectan y transmiten datos, muchas veces asociados a sensores en entornos industriales, urbanos, logísticos o de consumo. En el estudio, aparece como vector de aumento de superficie de ataque cibernético y de complejidad operativa.

ISO	*International Organization for Standardization*	Organización internacional que desarrolla normas técnicas, incluyendo la ISO 31000 y la ISO/TS 31050, referencias centrales para el enfoque de gestión de riesgos y riesgos emergentes adoptado en este informe.
ISO 31000	*ISO 31000: Gestión de Riesgos – Directrices*	Norma internacional que establece principios, estructura y proceso para la gestión de riesgos. En el estudio, es el marco general de referencia para el proceso de gestión de riesgos corporativos y para la lógica de fuentes de riesgo, análisis, evaluación y tratamiento.
ISO/TS 31050	*ISO/TS 31050: Gestión de Riesgos Emergentes*	Especificación técnica que ofrece orientaciones complementarias a la ISO 31000 para lidiar con riesgos emergentes, incertidumbre estructural, señales anticipatorias y foresight. Sustenta metodológicamente el uso de escenarios, radar de señales y ejercicios de foresight en este informe.
IT	*Information Technology (Tecnología de la Información)*	Conjunto de infraestructuras, redes, sistemas y aplicaciones digitales orientados al procesamiento, almacenamiento y transmisión de datos. Aparece en contraste e integración con OT en entornos de manufactura, energía, finanzas y servicios digitales.
KYC	*Know Your Customer*	Conjunto de procedimientos y controles para conocer, validar y monitorear clientes. En el contexto de servicios financieros y combate a delitos financieros, es un pilar de prevención de lavado de dinero, financiamiento al terrorismo y fraudes.
KPI	*Key Performance Indicator (Indicador Clave de Desempeño)*	Indicadores utilizados para monitorear desempeño y resultados organizacionales. En el estudio, se mencionan en contraste con indicadores de riesgo y con EWI, que tienen foco predictivo y de alerta.
OCDE	*Organización para la Cooperación y el Desarrollo Económicos*	Organismo internacional que produce estudios y benchmarks sobre economía, comercio, gobernanza e integridad. En el informe, es referencia para análisis de comercio internacional, flujos de bienes, estándares regulatorios e indicadores económicos.
OEA	*Organización de los Estados Americanos*	Organismo regional que reúne países del continente americano. En el estudio, aparece como referencia institucional ligada a la gobernanza democrática, a la estabilidad política y a la cooperación regional.
ONU	*Organización de las Naciones Unidas*	Organización internacional que apoya la cooperación entre Estados en temas como paz y seguridad, derechos humanos, desarrollo y clima. Es fuente de datos e informes utilizados como insumo para el panorama global y para riesgos climáticos, migratorios y humanitarios.

OT	*Operational Technology (Tecnología Operativa)*	Tecnologías asociadas a la operación de procesos físicos, como sistemas de control, sensores industriales y automatización de plantas productivas. Cuando se integran con TI, amplían tanto la eficiencia como el riesgo, especialmente en seguridad cibernética de infraestructuras críticas.
OT / IT	*Integración entre Operational Technology e Information Technology*	Expresión usada para caracterizar entornos en que sistemas industriales y sistemas de información están cada vez más conectados. Esta integración aumenta la eficiencia, pero expande la superficie de ataque cibernético y exige gobernanza de riesgos integrada.
PIB	*Producto Interno Bruto*	Medida del valor total de bienes y servicios producidos en una economía. Utilizada en el estudio para discutir crecimiento económico, capacidad de inversión e impacto de choques de riesgo en diferentes países y regiones.
UE	*Unión Europea*	Bloque de países europeos, utilizado como referencia de comparación en clima, regulación tecnológica, protección de datos, gobernanza de IA, estándares ambientales y modelos de integración económica y regulatoria.
WEF	*World Economic Forum (Foro Económico Mundial)*	Organización internacional que produce el Global Risks Report y otros estudios sobre riesgos globales, tecnología, economía y gobernanza. Es una de las principales fuentes de este informe para el análisis de tendencias sistémicas y riesgos emergentes.

Apéndice D – Créditos y Agradecimientos

La elaboración de este **Estudio de Escenarios de Riesgos y Estrategias para 2026 y Más Allá – Brasil y América Latina** solo fue posible gracias a la contribución técnica, intelectual e institucional de diversos profesionales, organizaciones aliadas y especialistas que dedicaron tiempo, conocimiento y análisis críticos.

Este documento consolida más de un año de observación continua, consultas a fuentes internacionales, análisis comparativos, ejercicios de *foresight* e integración de las metodologías previstas en la ISO 31000 y en la ISO/TS 31050. Su construcción exigió rigor metodológico, interdisciplinariedad y un esfuerzo colaborativo permanente.

La **Plataforma t-Risk** agradece profundamente a todos los que contribuyeron a este estudio, ya sea en la fase de recolección de datos, revisión técnica, lectura crítica o validación de los escenarios prospectivos.

Equipo de Investigación y Análisis

- **Tácito Leite**, CEO t-Risk – LinkedIn: https://www.linkedin.com/in/tacitoleite/;
- **Taís Fernandes Duarte**, Directora Jurídica t-Risk - LinkedIn: https://www.linkedin.com/in/taisfernandesduarte/;
- **Carlos Gonser**, CTO t-Risk – LinkedIn: https://www.linkedin.com/in/carlosgonser/;
- **Pedro Gallo**, Coordinador de Customer Success t-Risk – LinkedIn: https://www.linkedin.com/in/gallopedro/.

Revisión Técnica, Metodológica y Contribuciones

- Alírio Rodrigues Junior – Gerente Regional de Seguridad Corporativa en Bayer
  LinkedIn: https://www.linkedin.com/in/al%C3%ADrio-rodrigues/
- Annibal Sartori, DSE – Socio Consultor en Núcleo Consultoria em Segurança
  LinkedIn: https://www.linkedin.com/in/annibal-sartori/
- Carlos Faria Salaorni – Consultor em Seguridad Empresarial en CF∑A Consultoria em Segurança Empresarial
  LinkedIn: https://www.linkedin.com/in/carlosfariaconsultor/
- Daniel Richards – CEO en LatinRisk Argentina
  LinkedIn: https://www.linkedin.com/in/daniel-richards-99049314/
- Davi Prates – Gerente de Seguridad Corporativa en Siemens
  LinkedIn: https://www.linkedin.com/in/davi-prates-35aa49ab/

- Diego Escobal – Director de Vea Consultoria
  LinkedIn: https://www.linkedin.com/in/diegoescobaldigitalizacion/
- Diego Serpa, CPP – Gerente de Seguridad en Colgate-Palmolive
  LinkedIn: https://www.linkedin.com/in/diego-serpa-cpp%C2%AE-harvardx-mba-17682a68/
- Edison Luiz Gonçalves Fontes, MSc, CISA, CRISC, CISM – Advisor, Consultor y Gestor en Seguridad de la Información en Núcleo Consultoria em Segurança
  LinkedIn: https://www.linkedin.com/in/edisonfontes/
- Hélio Jorge Paixão – Asesor de Información Estratégica en el Tribunal de Contas dos Municípios do Estado da Bahia
  LinkedIn: https://www.linkedin.com/in/h%C3%A9lio-jorge-paix%C3%A3o-4b4671100/
- João Jaouiche – Socio Consultor en Núcleo Consultoria em Segurança
  LinkedIn: https://www.linkedin.com/in/jo%C3%A3o-jaouiche-38bb0a69/
- Marcelo de Sá Dias – Auditor de Conformidad, Posgraduado en Administración de Empresas por la FAAP y en Dirección de Seguridad Empresarial por la Universidad Comillas
  LinkedIn: https://www.linkedin.com/in/marcelo-de-s%C3%A1-6bb0a458/
- Ricardo Franco Coelho – Administrador de Empresas en TrendServ Multiserviços Corporativos
  LinkedIn: https://www.linkedin.com/in/ricardofcoelho/
- Ricardo Oscar Botta, CPP – Head Consultant en LatinRisk Argentina
  LinkedIn: https://www.linkedin.com/in/ricardo-botta/
- Ronivon Alves de Oliveira – Coordinador de Seguridad Empresarial en Lundin Mining y Director del Comité de Seguridad en la Minería en ABSEG
  LinkedIn: https://www.linkedin.com/in/ronivon-oliveira-cpai-2a95aa36/
- Víctor Escobal Morales – Director VEA Consultores de Riesgos
  LinkedIn: https://www.linkedin.com/in/v%C3%ADctor-escobal-morales-807b953/
- Wanderson Gloor – Director Unidad de Negocios São Paulo en Anjos da Guarda
  LinkedIn: https://www.linkedin.com/in/wandersongloor/

Edición y Diseño Gráfico

- Marcela Floriano – Directora de Marketing
  LinkedIn: https://www.linkedin.com/in/marcela-floriano-0343b4309/

Agradecimiento Especial

La **Plataforma t-Risk** reconoce el apoyo de todos aquellos que contribuyeron con *insights*, documentos, datos, críticas constructivas y validaciones metodológicas a lo largo del desarrollo de este informe. La pluralidad de perspectivas y la colaboración entre expertos de diferentes sectores fortalecieron la precisión y la utilidad estratégica de este estudio.

Agradecemos también a las instituciones nacionales e internacionales que ponen a disposición públicamente sus informes de riesgos, permitiendo que análisis como este sean construidos con base en evidencias sólidas y comparables.

Nota Final

Este estudio representa un esfuerzo continuo de inteligencia de riesgos y anticipa un futuro marcado por la complejidad, la incertidumbre y la interdependencia. t-Risk mantiene el compromiso de actualizar periódicamente sus análisis y seguir contribuyendo al fortalecimiento de la capacidad de resiliencia de las organizaciones brasileñas y latinoamericanas.

Softwares t-Risk

Conozca todos los módulos y herramientas de la Plataforma Total Risk.

Módulo de Gestión de Riesgos Corporativos

Gestión de riesgos integrados y estratégicos.

Módulo de Análisis Preliminar de Riesgos

Análisis previo y operativo de los riesgos.

Módulo Operador Económico Autorizado

Gestión de los riesgos logísticos - OEA.

Módulo Background Check

Due Diligence Digital para la gestión de riesgos de terceros.

Módulo de Evaluación de Madurez

Análisis del nivel de madurez organizacional en la gestión de riesgos.

Módulo AVSEC Aeropuertos

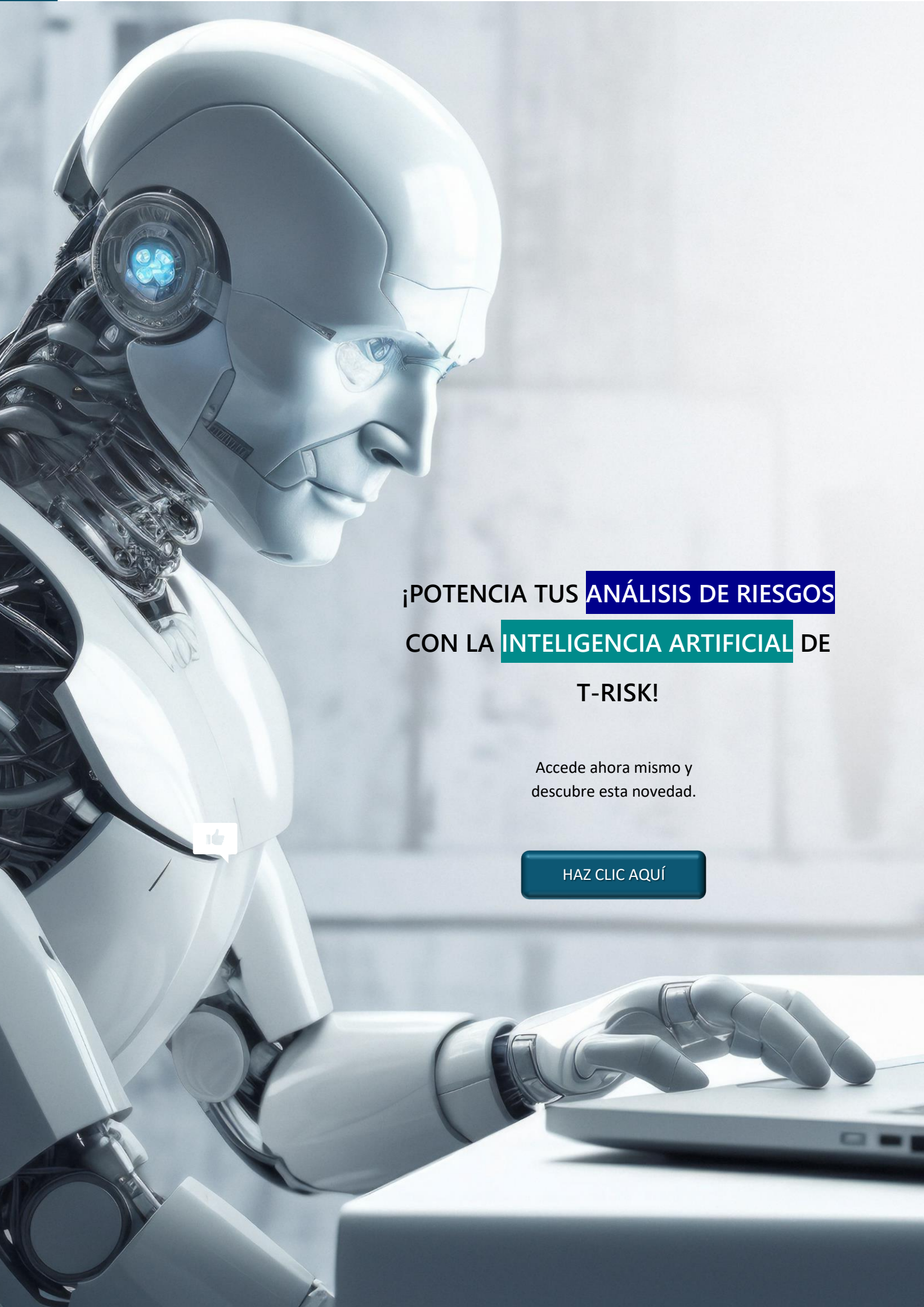
Gestión de riesgos de seguridad de la aviación civil (Security).

Aplicación de Evaluación de Riesgos

APP móvil completo para la identificación de los riesgos.

IA Vision Pro

Inteligencia Artificial creada para potenciar la gestión de riesgos corporativos.


¡POTENCIA TUS ANÁLISIS DE RIESGOS
CON LA INTELIGENCIA ARTIFICIAL DE
T-RISK!
Accede ahora mismo y
descubre esta novedad.
HAZ CLIC AQUÍ

www.totalrisk.com.br/es

• 2026 •