CENÁRIOS DE RISCO 2026 E ALÉM

Perspectivas Estratégicas para o Brasil e América Latina

t-Risk
Método de Avaliação de Riscos

Resumo

Este estudo apresenta uma análise abrangente e prospectiva dos riscos que moldarão o ambiente estratégico do Brasil e da América Latina em 2026 e além. Construído a partir da avaliação de 32 relatórios regionais e internacionais, exercícios de *foresight*, análise de fontes de risco conforme a ISO 31000 e diretrizes da ISO 31050 sobre riscos emergentes, o documento oferece uma visão integrada sobre as transformações que pressionam governos, empresas e instituições em toda a região.

O relatório combina tendências globais e dinâmicas regionais para identificar seis fontes estruturais de risco – 1. geopolítica e comércio; 2. tecnologia e inteligência artificial; 3. criminalidade organizada e finanças ilícitas; 4. clima e recursos naturais; 5. infraestrutura crítica e operações industriais; 6. instituições e confiança social – e como elas interagem para gerar ambientes de ruptura, oportunidade ou estagnação. A partir dessas forças, foram desenvolvidos quatro cenários possíveis para o futuro próximo, cada um representando combinações distintas de maturidade tecnológica e coordenação institucional.

Setores-chave da economia latino-americana foram analisados em profundidade, incluindo indústria, energia, agronegócio, finanças, tecnologia, mineração, saúde, serviços urbanos e setor público. Também foi desenvolvido um radar regional de sinais antecipatórios, integrando riscos climáticos, digitais, criminais e econômicos, para apoiar processos contínuos de monitoramento e decisão estratégica.

Em um ambiente marcado por interdependência, volatilidade e pressões simultâneas, este estudo oferece não apenas uma leitura crítica do presente, mas um conjunto de caminhos possíveis para fortalecer a resiliência regional. O objetivo é apoiar decisores públicos e privados na construção de estratégias mais adaptativas, inteligentes e alinhadas com as transformações profundas que definirão a 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.

Palavras-Chave

Riscos Emergentes; Cenários Prospectivos; Resiliência Organizacional; Segurança Convergente e Integrada; Governança Institucional; Inteligência Artificial e Tecnologia; Crime Organizado Transnacional; Infraestruturas Críticas; Clima e Eventos Extremos; Sinais Antecipatórios *(Early Warning Indicators).*

Licença de Distribuição

Clique na imagem abaixo para acessar.

Creative Commons License Deed

Atribuição-NãoComercial 4.0 Internacional (CC BY-NC 4.0)

This is a human-readable summary of (and not a substitute for) the license.

Você tem o direito de:

Compartilhar — copiar e redistribuir o material em qualquer suporte ou formato

Adaptar — remixar, transformar, e criar a partir do material

O licenciante não pode revogar estes direitos desde que você respeite os termos da licença.

De acordo com os termos seguintes:

Atribuição — Você deve dar o crédito apropriado, prover um link para a licença e indicar se mudanças foram feitas. Você deve fazê-lo em qualquer circunstância razoável, mas de nenhuma maneira que sugira que o licenciante apoia você ou o seu uso.

NãoComercial — Você não pode usar o material para fins comerciais.

Sem restrições adicionais — Você não pode aplicar termos jurídicos ou medidas de caráter tecnológico que restrinjam legalmente outros de fazerem algo que a licença permita.

Sumário

Prefácio do CEO *9*

Mensagem do CTO *10*

Mensagem da CLO *11*

Sobre a Plataforma t-Risk *13*

Resumo Executivo – Contexto Geral *14*

Capítulo 1 – Introdução *18*

1.1. Objetivo *19*

1.2. Metodologia e Fontes *20*

1.3. Panorama Global 2026 e Além *21*

1.4. Fontes de Risco Críticas e Incertezas Estruturais *23*

1.5. Matriz de Cenários 2026 e Além *28*

Capítulo 2 – Cenários Detalhados *42*

2.1. Introdução *43*

2.2. Cenário 1 – Aliança PragTécnica *43*

2.2.1. Contexto e Fundamentos 43

2.2.2. Cadeia Causal Ampliada 44

2.2.3. Fontes de Risco Predominantes no Cenário 44

2.2.4. Implicações Setoriais Diretas 45

2.2.5. Impactos na Segurança Corporativa (Física, Cibernética e Reputacional) 45

2.2.6. Impactos na Governança e na Continuidade de Negócios 46

2.2.7. Indicadores Específicos de Alerta Precoce (EWI) 46

2.2.8. Sinais de Transição do Cenário 47

2.2.9. Oportunidades Estratégicas 47

2.3. Cenário 2 – Redes Sombrias *47*

2.3.1. Contexto e Fundamentos 47

2.3.2. Cadeia Causal Ampliada 48

2.3.3. Fontes de Risco Predominantes no Cenário 48

2.3.4. Implicações Setoriais Diretas 49

2.3.5. Impactos na Segurança Corporativa (Física, Cibernética e Reputacional) 49

2.3.6. Impactos na Governança e na Continuidade de Negócios 50

2.3.7. Indicadores Específicos de Alerta Precoce (EWI) 50

2.3.8. Sinais de Transição do Cenário 51

2.3.9. Oportunidades Estratégicas 51

2.4. Cenário 3 – Clima de Choques *52*

2.4.1. Contexto e Fundamentos 52

2.4.2. Cadeia Causal Ampliada 52

2.4.3. Fontes de Risco Predominantes no Cenário 53
2.4.4. Implicações Setoriais Diretas 53
2.4.5. Impactos na Segurança Corporativa (Física, Cibernética e Reputacional) 54
2.4.6. Impactos na Governança e na Continuidade de Negócios 54
2.4.7. Indicadores Específicos de Alerta Precoce (EWI) 55
2.4.8. Sinais de Transição do Cenário 55
2.4.9. Oportunidades Estratégicas 55
2.5. Cenário 4 – Dados com Travas, Fronteiras Abertas 56
2.5.1. Contexto e Fundamentos 56
2.5.2. Cadeia Causal Ampliada 56
2.5.3. Fontes de Risco Predominantes no Cenário 57
2.5.4. Implicações Setoriais Diretas 57
2.5.5. Impactos na Segurança Corporativa (Física, Cibernética e Reputacional) 58
2.5.6. Impactos na Governança e na Continuidade de Negócios 58
2.5.7. Indicadores Específicos de Alerta Precoce (EWI) 59
2.5.8. Sinais de Transição do Cenário 59
2.5.9. Oportunidades Estratégicas 60

Capítulo 3 – Implicações Estratégicas por Setor 61
3.1. Introdução 62
3.2. Setor Industrial e Manufatura 63
3.2.1. Riscos Predominantes 63
3.2.2. Impactos Climáticos, Tecnológicos e Operacionais 64
3.2.3. Implicações Específicas para Brasil e América Latina 64
3.2.4. Comparação com Estados Unidos, União Europeia e Ásia 65
3.2.5. Oportunidades Estratégicas 66
3.3. Energia, Infraestruturas Críticas e Utilities 67
3.3.1. Vulnerabilidades Estruturais 67
3.3.2. Pressões Climáticas e Digitais 68
3.3.3. Desafios para Brasil e América Latina 68
3.3.4. Comparação Global 69
3.3.5. Oportunidades 69
3.4. Agronegócio e Alimentos 70
3.4.1. Riscos Climáticos e Logísticos 70
3.4.2. Pressões Tecnológicas e de Mercado 71
3.4.3. Implicações Regionais 72
3.4.4. Comparação com Principais Mercados Globais 72
3.4.5. Oportunidades Estratégicas 73
3.5. Logística, Portos, Rodovias e Infraestruturas Urbanas 74
3.5.1. Fontes de Risco e Pressões Operacionais 74

3.5.2. Implicações Regionais 75
3.5.3. Comparativo Global 75
3.5.4. Oportunidades Estratégicas 76
3.6. Serviços Financeiros e Meios de Pagamento 77
3.6.1. Pressões Tecnológicas, Crimes Financeiros e Riscos Ilícitos 77
3.6.2. Impactos na América Latina e Brasil 78
3.6.3. Comparação Global 78
3.6.4. Oportunidades Estratégicas 79
3.7. Tecnologia, Dados e Plataformas Digitais 80
3.7.1. Riscos Digitais e Governança Algorítmica 80
3.7.2. Implicações para América Latina e Brasil 81
3.7.3. Comparação com Ecossistemas Globais 81
3.7.4. Oportunidades Estratégicas 82
3.8. Mineração, Petróleo e Gás 83
3.8.1. Vulnerabilidades e Pressões Ambientais 83
3.8.2. Implicações Regionais para América Latina e Brasil 84
3.8.3. Comparação Global 85
3.8.4. Oportunidades Estratégicas 85
3.9. Setor Público, Justiça e Regulação 87
3.9.1. Fragilidades Institucionais 87
3.9.2. Pressões Digitais e Criminais 87
3.9.3. Desafios para Brasil e América Latina 88
3.9.4. Comparação Global 88
3.9.5. Oportunidades Estratégicas 89
3.10. Quadro-Síntese Final Multissetorial 90

Capítulo 4 – Segurança Corporativa e Infraestruturas Críticas 94
4.1. Introdução 95
4.2. Pressões do Ambiente de Risco Híbrido 95
4.3. Vulnerabilidades Específicas de Infraestruturas Críticas 96
4.4. Panorama Latino-Americano: Crime Organizado, Convergência Digital e Fragilidade Estatal 96
4.5. Resposta Corporativa: Segurança Convergente e Resiliência Operacional 97
4.6. Pressões e Oportunidades no Contexto Brasileiro 99

Capítulo 5 – Indicadores e Radar de Sinais Antecipatórios 101
5.1. Introdução 102
5.2. Indicadores Climáticos e Ambientais 102
5.3. Indicadores Digitais e Tecnológicos 104
5.4. Indicadores Sociopolíticos e Criminais 106

5.5. Indicadores Econômicos e de Cadeias Críticas 107
5.6. Radar Integrado de Sinais Antecipatórios 109
5.7. Integração com as Diretrizes da ISO 31050 para Riscos Emergentes 110
5.8. O Ciclo de Inteligência para Identificação de Sinais Precoces..... 111
5.9. Consolidação Final do Radar Antecipatório 112

Capítulo 6 – Recomendações Executivas e Caminhos Futuros 113
6.1. Introdução..... 114
6.2. Reforçar a Governança Estratégica de Riscos em Nível de Conselho..... 114
6.3. Construir Resiliência em Infraestruturas Críticas e Cadeias Sensíveis 115
6.4. Aumentar a Maturidade Digital e a Governança de Inteligência Artificial..... 115
6.5. Adaptar-se ao Clima como Principal Multiplicador de Risco 116
6.6. Enfrentar Redes Ilícitas e Fortalecer a Segurança Multidimensional 116
6.7. Harmonizar Regulação e Aprimorar Capacidade Estatal 117
6.8. Desenvolver Ecossistemas de Cooperação e Inteligência Coletiva..... 117
6.9. Integrar Foresight, Cenários e Sinais Antecipatórios Como Processo Continuado 118
6.10. Caminhos Futuros: A Construção de um Horizonte de Resiliência para a América Latina 118

Conclusão 121
Apêndice A – Metodologia Utilizada 125
Apêndice B – Lista de Fontes Consultadas 128
Apêndice C – Glossário de Siglas 131
Apêndice D – Créditos e Agradecimentos 135
Equipe de Pesquisa e Análise 135
Revisão Técnica, Metodológica e Contribuições..... 135
Editoração e Desenho Gráfico..... 136
Agradecimento Especial 137
Nota Final 137

Prefácio do CEO

Tácito Augusto Silva Leite
Plataforma t-Risk

Há momentos em que a história acelera. Em que transformações tecnológicas, climáticas, sociais e geopolíticas deixam de ser movimentos isolados e passam a formar um único pulso, capaz de redefinir o rumo de nações, organizações e indivíduos. Atravessamos exatamente esse tipo de momento.

No estudo t-Risk de 2025, buscamos compreender essa nova dinâmica e mostrar como riscos — quando lidos com profundidade — revelam não apenas ameaças, mas caminhos possíveis. Um ano depois, avançamos para um cenário ainda mais desafiante, no qual incerteza não é exceção: é o próprio ambiente estratégico. E é justamente por isso que olhar apenas para o presente já não basta. É preciso enxergar o que pode emergir.

O relatório de 2026 nasce desse espírito. Ele reconhece que a América Latina carrega vulnerabilidades históricas, mas também possui capacidades extraordinárias — energia limpa, diversidade produtiva, talento humano e uma resiliência que atravessa décadas. O desafio, agora, é transformar essas forças em vantagem estratégica em um mundo onde riscos se combinam e se multiplicam.

*Ao identificar **seis fontes estruturais de risco** e construir **quatro cenários plausíveis para 2026**, este estudo não pretende antecipar o futuro, mas ampliar nossa capacidade de dialogar com ele. A interdisciplinaridade — unindo tecnologia, clima, economia, segurança e governança — serve como ponto de apoio para compreender como essas forças se entrelaçam e moldam escolhas fundamentais para governos, empresas e instituições.*

Mais do que respostas prontas, este relatório oferece perspectivas. Mais do que previsões, oferece direção. Ele convida cada liderança a desenvolver a coragem de agir em um mundo incerto, a cultivar a curiosidade de questionar modelos estabelecidos e a construir, com responsabilidade e visão, as bases de um futuro mais seguro e sustentável para a nossa região.

Acredito profundamente que risco, quando bem compreendido, é uma forma de inteligência. É a capacidade de perceber o que ainda não aconteceu, de preparar o terreno para o que pode vir, e de construir resiliência não como defesa, mas como vantagem competitiva. Este estudo é uma contribuição para essa jornada.

Que ele inspire conversas profundas, decisões responsáveis e colaboração genuína entre setores e fronteiras. A América Latina tem, diante de si, desafios imensos — mas também uma rara oportunidade de reinventar o seu lugar no mundo. E isso começa com a qualidade das escolhas que fazemos hoje.

Mensagem do CTO

Carlos Eduardo Espesani Gonser
Plataforma t-Risk

A migração do crime e das fraudes para o ambiente digital tornou-se evidente. O que antes exigia presença física — assaltos, interceptações, sabotagens diretas — hoje ocorre silenciosamente por meio de invasões, manipulação de identidades, ataques automatizados e exploração de falhas em sistemas críticos. Esse movimento não é isolado: ele se conecta a um cenário mais amplo em que tecnologia, governança institucional, operações industriais e estruturas financeiras passaram a funcionar de forma interdependente, ampliando o impacto de qualquer falha. É exatamente esse ponto de convergência que o relatório evidencia ao mapear riscos sistêmicos e cenários possíveis para os próximos anos.

Do ponto de vista tecnológico, a linha entre segurança cibernética, proteção de dados, continuidade de negócios e integridade operacional praticamente desapareceu. A Inteligência Artificial acelerou essa mudança. Ela potencializa ataques, mas também é um dos poucos recursos capazes de processar sinais fracos, correlacionar eventos e oferecer respostas em um ambiente em que velocidade e volume importam mais do que nunca. A maturidade em IA — tanto no uso quanto na governança — tornou-se um diferencial estratégico real, separando organizações preparadas daquelas expostas.

O relatório mostra que riscos digitais não podem mais ser tratados como um domínio isolado dentro das empresas. A superfície de ataque agora inclui cadeias logísticas, infraestruturas industriais, fluxos financeiros e mecanismos de tomada de decisão. Ataques digitais geram impactos físicos; fragilidades institucionais ampliam vulnerabilidades tecnológicas; e a falta de integração entre áreas reduz a capacidade de resposta. Esse é o ponto central: risco tecnológico é risco organizacional.

Sob a ótica de tecnologia, a contribuição do estudo está em oferecer um enquadramento que ajuda líderes a entender como esses elementos se conectam, como a criminalidade evoluiu e como a governança de IA, a resiliência de infraestruturas críticas e a coordenação institucional determinam o grau de exposição. Não se trata de previsões abstratas, mas de compreender um cenário operacional em que interrupções, ataques e fraudes deixaram de ser exceções e se tornaram parte do cotidiano corporativo.

Para os próximos anos, a vantagem estará com quem adotar modelos integrados de segurança, inteligência de risco e automação. Quem não fizer isso tende a operar no escuro — e em um ambiente adversarial como o descrito neste estudo, isso não é uma opção.

Mensagem da CLO

Taís Fernandes Duarte
Plataforma t-Risk

A análise prospectiva das seis fontes estruturais de risco, especialmente aquela relacionada à erosão institucional e à confiança social, revela que o Brasil ingressa no ciclo 2026–2030 sob forte pressão para fortalecer seus sistemas de governança. A convergência entre desinformação, hiperpolarização, fragilidade estatal e expansão do crime organizado desafia o próprio centro de gravidade do Estado de Direito. Nesse contexto, instrumentos como a Lei de Software, o Marco Civil da Internet, a LGPD, a Lei Anticorrupção, SOX, FCPA, ISO 37001, ISO 19600, ISO 31000, ISO 31050 e o futuro Marco Legal da IA não podem ser interpretados apenas como atualizações técnicas, mas como parte de um pilar institucional indispensável para a resiliência nacional. O problema brasileiro não reside na ausência de normas, mas no desalinhamento entre instituições, práticas corporativas, infraestrutura regulatória e as dinâmicas reais dos riscos contemporâneos, que já não são lineares nem compartimentáveis.

O estudo demonstra que o Brasil enfrentará nos próximos anos tensões digitais amplificadas, desordem informacional, instrumentalização da inteligência artificial por grupos criminosos, fragilidade da autoridade pública, aumento da judicialização e baixa coordenação estatal diante de riscos multissetoriais.

Paralelamente, o Brasil possui um dos arcabouços normativos mais avançados da América Latina em proteção de dados e governança digital, mas ainda fragmentado. O Marco Civil da Internet não responde adequadamente aos riscos da manipulação algorítmica e do colapso informacional; a LGPD concentra-se no dado pessoal, e não nos riscos sistêmicos; a Lei de Software permanece desatualizada diante de modelos fundacionais e IA generativa. O país também aderiu a padrões robustos de integridade, como a Lei Anticorrupção, SOX, FCPA, ISO 37001 e ISO 19600, mas, a expansão do crime organizado e das redes ilícitas transnacionais exige agora um novo nível de diligência algorítmica e responsabilidade ampliada por falhas digitais previsíveis.

O PL 2.338/2023, que deve instituir o Marco Legal da IA, é um avanço ao definir princípios e categorias de risco, mas, permanece insuficiente para enfrentar a dimensão sistêmica dos riscos tecnológicos que emergem no estudo. Para que cumpra sua função estratégica, a IA deve ser reconhecida como infraestrutura crítica, devendo integrar coordenação regulatória obrigatória entre ANPD, SIA, Banco Central, agências reguladoras e órgãos de segurança. As Avaliações Preliminares de Risco e as Avaliações de Impacto Algorítmico devem se transformar em monitoramento contínuo, e não em meros relatórios estáticos. Além disso, o marco regulatório deve incorporar diretrizes da COP30, da LGPD, do direito da concorrência e das normas climáticas, reconhecendo que a IA é simultaneamente vetor de mitigação e ampliação dos riscos climáticos e sociais.

Ao confrontar a realidade jurídica brasileira com a da América Latina, torna-se evidente que compartilhamos um mesmo padrão: arcabouços formais avançados convivem com instituições frágeis, seletividade na aplicação das normas, volatilidade regulatória e déficits de efetividade. O Brasil possui densidade normativa superior, mas sofre com erosão de confiança, judicialização excessiva e percepção social de impunidade seletiva, o que compromete a legitimidade do sistema jurídico como instrumento de estabilidade e desenvolvimento. A próxima década testará a capacidade do país — e da região — de transformar o Direito em infraestrutura de resiliência. Isso exige abandonar a visão de que a sofisticação normativa é suficiente e construir convergência jurídica orientada a risco, capaz de apoiar decisões públicas e privadas frente às profundas transformações climáticas, tecnológicas e institucionais que moldarão o futuro. Se Brasil e América Latina forem capazes de alinhar o Direito à dinâmica real dos riscos emergentes, o sistema jurídico deixará de ser apenas um reflexo das crises para tornar-se um vetor ativo de estabilidade e confiança.

Sobre a Plataforma t-Risk

A **Plataforma t-Risk** é uma solução SaaS disponível desde 2015, projetada para transformar a **gestão de riscos nas organizações**. Ela combina inovação tecnológica com as melhores práticas normativas globais, especialmente as diretrizes das **normas ISO 31000, ISO 31050 e 31010**. Totalmente alinhada aos padrões internacionais, a t-Risk oferece uma **abordagem analítica e prática**, auxiliando as empresas em todas as etapas da gestão de riscos corporativos: **identificação, análise, avaliação, priorização e tratamento**. Disponível em português, espanhol e inglês, a plataforma **aumenta em até 80% a produtividade do processo de gestão de riscos**, entregando eficiência e precisão.

Com funcionalidades avançadas, a t-Risk integra **inteligência artificial** e oferece módulos robustos, como **GRC** (Gestão de Riscos Corporativo), **APR** (Análise Preliminar de Riscos), **MBC** (Módulo de Background Check), **MAM** (Módulo de Avaliação de Maturidade em Gestão de Riscos) e **OEA** (Operador Econômico Autorizado), AVSEC (Gestão de Riscos na Aviação Civil), além de um **Painel de Indicadores** (BI) e um **APP Mobile**. O **módulo 5W2H** permite um acompanhamento detalhado de projetos, tarefas e controles, com e-mails automáticos, garantindo que os riscos permaneçam dentro do apetite de risco da organização.

Além de **fortalecer o *compliance* e otimizar processos**, a t-Risk capacita seus clientes a transformarem desafios em oportunidades, oferecendo **insights valiosos para decisões estratégicas**. Seja para fortalecer a resiliência organizacional ou impulsionar o crescimento sustentável, a t-Risk é **uma aliada indispensável para enfrentar um cenário de riscos** cada vez mais dinâmico e complexo.

Descubra como a t-Risk pode revolucionar a gestão de riscos na sua organização. Explore o poder de nossas soluções e **fortaleça sua estratégia de gestão de riscos com uma ferramenta que vai além da tecnologia**: uma verdadeira parceira na sua jornada de transformação.

Resumo Executivo – Contexto Geral

O ano de 2026 marca um ponto de inflexão para a gestão de riscos corporativos na América Latina. A combinação entre volatilidade geopolítica, aceleração tecnológica, pressões climáticas extremas e a sofisticação do crime organizado transnacional inaugura um ambiente de riscos convergentes, no qual o físico, o digital e o institucional operam em interdependência crescente.

Desenvolvido a partir da análise comparativa de **32 relatórios internacionais, regionais e corporativos**, este estudo oferece uma leitura integrada das forças que moldarão o ambiente de riscos em 2026. A abordagem metodológica segue as diretrizes das normas **ISO 31000, ISO 31050 e ISO 31010**, incorporando práticas de *foresight*, *horizon scanning* e construção de cenários qualitativos para apoiar decisões estratégicas em ambientes de alta complexidade.

O objetivo central é fornecer um quadro robusto para que organizações públicas e privadas antecipem tendências, identifiquem vulnerabilidades, oportunidades e fortaleçam sua resiliência institucional em um período marcado por rápidas transformações estruturais.

Síntese Metodológica

O estudo combina três pilares metodológicos complementares:

1. **Análise convergente de 32 fontes de referência**, incluindo organismos multilaterais, centros de inteligência, consultorias estratégicas e instituições corporativas.
2. **Estruturação de seis Fontes de Risco Críticas**, que sintetizam padrões recorrentes observados nas evidências coletadas.
3. **Construção de uma matriz de cenários 2×2**, resultando em quatro futuros plausíveis para 2026, cada um associado a planos setoriais, indicadores de alerta precoce (EWI) e implicações estratégicas.

Essa abordagem garante coerência entre as dimensões estratégica, técnica e operacional da gestão de riscos, ampliando sua utilidade para executivos, conselhos, lideranças de segurança, *compliance*, ESG e continuidade de negócios.

Principais Conclusões

O conjunto das análises revela uma **mudança estrutural na natureza dos riscos corporativos**.

O crime organizado tornou-se um sistema híbrido, digital e economicamente infiltrado, antes concentrado em atividades territoriais e violentas, evoluiu para uma **configuração híbrida, digitalizada e economicamente infiltrada**, conforme evidenciado no *Global Organized Crime Index 2025 – Crime at a Crossroads*. A América Latina aparece entre as regiões de maior vulnerabilidade, tanto pela **fragilidade institucional** quanto pela **integração do ilícito nas cadeias logísticas e financeiras formais**.

A convergência de crimes financeiros, ataques cibernéticos e corrupção sistêmica redefine a exposição de empresas e governos. O clima tornou-se um multiplicador de crises, o aumento de eventos climáticos extremos – secas, enchentes e colapsos energéticos – amplia as interdependências entre riscos ambientais, reputacionais e de continuidade operacional.

Essas dinâmicas se entrelaçam com a **fragmentação regulatória da Inteligência Artificial**, cujos marcos nacionais avançam de modo desigual, criando brechas para abusos tecnológicos, manipulação de informação e riscos éticos.

Os Quatro Cenários para 2026

Cenário	Descrição-síntese	Implicações-chave
Aliança PragTécnica	Cooperação regional pragmática e adoção coordenada de padrões de governança digital e IA.	Estabilidade institucional, interoperabilidade de dados e redução de incidentes OT.
Redes Sombrias	Fragmentação política, captura do Estado e proliferação de redes criminosas transnacionais e digitais.	Colapso da confiança, aumento de perdas financeiras e riscos físicos a executivos e infraestruturas.
Clima de Choques	Integração econômica avança, mas a maturidade tecnológica permanece baixa, expondo sistemas a falhas simultâneas.	Interrupções críticas, elevação de custos (BI) e pressão sobre cadeias de suprimentos.
Dados com Travas, Fronteiras Abertas	Governança privada de IA e segurança de elite compensam a instabilidade política.	Setores líderes mantêm operação resiliente; fragmentação regional moderada.

Esses cenários não competem entre si: coexistem em graus distintos em cada país ou setor, formando um **mapa dinâmico de probabilidades** que orienta a priorização de medidas estratégicas.

Principais Tendências e Impactos Regionais

1. **Geopolítica e comércio:** reconfiguração de alianças e cadeias de suprimento, com a América Latina reposicionando-se como exportadora de energia e dados.
2. **Tecnologia e IA:** expansão de *deepfakes*, fraudes automatizadas e uso criminoso de IA; ao mesmo tempo, aceleração de aplicações produtivas e do uso da identidade digital como novo perímetro de segurança.
3. **Crime Organizado e FinCrime:** infiltração crescente de organizações ilícitas em setores logísticos, agrícolas e financeiros; uso de criptomoedas e marketplaces para lavagem de dinheiro.
4. **Clima e Recursos Naturais:** aumento de eventos extremos afetando a estabilidade de energia e água, exigindo governança regional e seguros paramétricos.
5. **Infraestrutura Crítica (OT):** vulnerabilidades em sistemas industriais e custos indiretos predominando nas perdas; controles ICS–5 ganham relevância; vulnerabilidade de serviços baseados em satélites e infraestrutura espacial.
6. **Instituições e Confiança:** declínio dos índices de percepção de segurança e crescimento da desinformação, reduzindo a coesão social e a atratividade de investimentos.

Implicações Estratégicas

Os resultados indicam que o modelo tradicional de gestão de riscos, baseado em controle, conformidade e reação, tornou-se limitado diante da complexidade atual. A nova fronteira exige **resiliência dinâmica, integração entre segurança física e cibernética e uso ético da inteligência artificial** como vetor de antecipação. Empresas líderes na região já iniciam a convergência de seus centros de monitoramento (GSOC) e a adoção de políticas de *zero-trust physical*, ampliando a visibilidade sobre ativos críticos e pessoas.

A governança do futuro requer **decisão em tempo real, colaboração regional e transparência algorítmica**. As organizações que compreenderem o risco como uma forma de inteligência – e não como um obstáculo – estarão mais aptas a capturar oportunidades, preservar valor e sustentar crescimento.

Quadro resumo dos principais eixos estruturantes da gestão de riscos para 2026:

Eixo	Descrição	Resultado Esperado
Estratégico	Integração regional, cooperação público-privada e governança digital.	Estabilidade e competitividade regional.
Tecnológico	IA explicável, proteção de dados, resiliência cibernética e operacional (OT).	Redução de vulnerabilidades e fraudes.
Ambiental	Governança climática e infraestrutura adaptativa.	Continuidade operacional e redução de perdas por interrupção de negócios (BI).
Criminal-Institucional	Combate à infiltração ilícita e fortalecimento de marcos legais.	Recuperação da confiança institucional.
Cultural-Organizacional	Cultura de risco e aprendizagem contínua.	Liderança adaptativa e resposta antecipatória.

Mensagem Final do Resumo Executivo

O ambiente de 2026 será moldado não apenas pelas tendências tecnológicas, climáticas e geopolíticas, mas pela capacidade de organizações públicas e privadas transformarem incerteza em estratégia e risco em vantagem competitiva.

Este relatório oferece uma base estruturada para antecipação, adaptação e tomada de decisão — elementos essenciais para qualquer instituição que queira prosperar em um cenário marcado por interdependência, velocidade e complexidade.

Em última instância, os cenários aqui descritos dependem da qualidade das decisões tomadas por pessoas concretas — gestores, líderes públicos e cidadãos — cuja formação de valores, visão de mundo e capacidade ética de uso do poder constituem o primeiro nível de governança de riscos.

01

INTRODUÇÃO

1.1. Objetivo

O cenário global que se desenha para 2026 é marcado por uma combinação inédita de forças disruptivas, incertezas estruturais e transformações tecnológicas que remodelam o ambiente de negócios, de segurança e de governança em escala mundial.

A América Latina, inserida nesse contexto, vivencia o entrelaçamento de fenômenos políticos, econômicos e sociais que influenciam diretamente a estabilidade institucional, a competitividade empresarial e a capacidade de resposta das organizações frente a riscos cada vez mais interdependentes.

O aumento da complexidade sistêmica é impulsionado por três vetores principais: 1. **o avanço acelerado da Inteligência Artificial e da automação; 2. a intensificação das crises climáticas e dos eventos de interrupção de negócios; 3. e a expansão do crime organizado em suas dimensões financeira, digital e corporativa.** Esses vetores produzem um novo tipo de risco, simultaneamente transversal e persistente, que transcende as fronteiras tradicionais entre o físico, o cibernético e o regulatório, exigindo um modelo de gestão integrado e orientado por inteligência.

Nesse contexto, o presente estudo tem como objetivo principal oferecer uma visão abrangente dos **cenários de risco e das estratégias de adaptação para 2026 no Brasil e na América Latina**, com base em um conjunto de trinta e dois relatórios, estudos, bases de dados internacionais e regionais. O trabalho busca apoiar empresas, governos e instituições no fortalecimento de suas estruturas de governança, na antecipação de ameaças e na construção de modelos de resiliência compatíveis com as exigências de um ambiente volátil e interconectado.

A abordagem metodológica adotada neste relatório combina técnicas de *foresight*, *horizon scanning* e análise de cenários qualitativos para estruturar a leitura de riscos emergentes e incertezas profundas na América Latina. Os detalhes do processo encontram-se descritos no item abaixo (Metodologia e Fontes) e no Apêndice A.

A partir dessa estrutura metodológica, o estudo identifica as principais **fontes de risco** e os **eixos de tensão** que influenciarão a trajetória econômica, ambiental, tecnológica e social da América Latina em 2026 e além. A análise integra dimensões de governança corporativa, segurança física e cibernética, continuidade de negócios, sustentabilidade, *compliance* e responsabilidade social, permitindo visualizar como diferentes variáveis se combinam e produzem impactos diretos sobre o desempenho e a reputação organizacional.

Mais do que antecipar ameaças, este relatório busca apoiar o desenvolvimento de uma **cultura de inteligência de risco** baseada em aprendizagem contínua, adaptação estratégica e cooperação multissetorial. O propósito central é transformar o risco em um **instrumento de governança**, capaz de orientar decisões, alinhar estratégias e promover resiliência organizacional em todos os níveis da gestão.

1.2. Metodologia e Fontes

A metodologia adotada neste estudo baseia-se em uma abordagem integrada de análise de riscos, combinando técnicas de *foresight*, prospectiva estratégica e avaliação comparativa de fontes de risco em múltiplos domínios. O objetivo central é oferecer uma visão estruturada sobre as forças que moldam o ambiente de incerteza na América Latina em 2026 e além, permitindo às organizações compreenderem e antecipar eventos que possam afetar sua continuidade, reputação e valor.

O processo metodológico foi estruturado em cinco etapas principais. A primeira etapa consistiu na **coleta e sistematização de informações** provenientes de trinta e dois relatórios internacionais, regionais e corporativos publicados entre 2024 e 2025. Esses documentos foram selecionados com base em critérios de credibilidade institucional, abrangência temática, rigor analítico e relevância para o contexto latino-americano. Entre as entidades e autores incluídos estão o Fórum Econômico Mundial, as Nações Unidas, a OCDE, o Banco Mundial, a Microsoft, a *Global Initiative Against Transnational Organized Crime* (GI-TOC), a *ComplyAdvantage*, o Instituto Internacional de Auditores Internos (IIA), a CEIUC, o ERI e a própria Plataforma t-Risk.

A segunda etapa envolveu a **normalização e classificação das informações**, com a criação de cartões-fonte para cada documento analisado. Cada cartão registrou dados como título, ano de publicação, escopo geográfico, metodologia empregada, principais achados, fontes de risco identificadas, incertezas estruturais, indicadores de alerta e grau de robustez das evidências. Essa padronização garantiu a comparabilidade entre estudos de natureza distinta, como relatórios econômicos, análises de segurança cibernética, previsões climáticas e estudos de criminalidade transnacional.

A terceira etapa correspondeu à **análise de convergência**, na qual as fontes de risco foram agrupadas e reinterpretadas segundo uma taxonomia única desenvolvida pela equipe de pesquisa da Plataforma t-Risk. Essa taxonomia integra seis dimensões centrais:

(i) Geopolítica e comércio;
(ii) Tecnologia e inteligência artificial;

(iii) Criminalidade organizada e finanças ilícitas;
(iv) Clima e recursos naturais;
(v) Infraestrutura crítica e operações industriais;
(vi) Instituições e confiança social.

Cada uma dessas dimensões foi avaliada quanto à sua frequência de ocorrência nas fontes originais, ao grau de interdependência com as demais e ao potencial de impacto sistêmico.

Na quarta etapa, foi aplicada a **análise de cenários**, que relaciona as fontes de risco e as incertezas identificadas para construir projeções plausíveis do futuro. O procedimento incluiu o mapeamento das variáveis mais influentes, a definição de eixos de tensão contrastantes e a modelagem de quatro cenários que expressam combinações possíveis dessas forças: *Aliança PragTécnica, Redes Sombrias, Clima de Choques e Dados com Travas, Fronteiras Abertas.* A técnica de modelagem seguiu os princípios de plausibilidade, coerência interna e utilidade estratégica, assegurando que os cenários possam ser utilizados como instrumentos de planejamento e tomada de decisão.

A quinta e última etapa consistiu na **validação cruzada e síntese executiva**. As narrativas, gráficos e indicadores foram revisados por especialistas, garantindo alinhamento metodológico às normas ISO 31000, ISO 31050 e ISO 31010. Além disso, as análises foram processadas pela t-Risk Vision Pro, inteligência artificial da Plataforma t-Risk, o que permitiu correlacionar variáveis, detectar lacunas de informação e gerar visualizações dinâmicas de risco.

A metodologia, portanto, combina rigor técnico e aplicabilidade prática. Ela assegura que os resultados apresentados nos capítulos seguintes não sejam apenas projeções hipotéticas, mas sim produtos de um processo comparativo, validado e sistemático, que traduz a complexidade global em *insights* operacionais para organizações públicas e privadas.

1.3. Panorama Global 2026 e Além

O panorama global projetado para 2026 e os anos subsequentes caracteriza-se por uma crescente instabilidade estrutural, definida pela sobreposição de crises e pela interdependência entre sistemas antes considerados autônomos. A economia mundial, a segurança digital, o clima, as cadeias de suprimento e a governança institucional passaram a formar um ecossistema de riscos entrelaçados, no qual perturbações locais podem rapidamente assumir dimensões transnacionais. A América Latina emerge como uma região de relevância estratégica dentro desse contexto, não apenas por seus

recursos naturais e energéticos, mas também por sua vulnerabilidade política e por sua inserção desigual nas cadeias globais de valor.

As tendências mais relevantes indicam que o sistema internacional permanece em processo de transição entre uma ordem global fragmentada e uma nova estrutura multipolar. Essa mudança de poder geopolítico é marcada por disputas tecnológicas, coerção econômica e reconfiguração das alianças regionais. A segurança internacional passa a ser cada vez mais condicionada pelo domínio da Inteligência Artificial e pelo controle de infraestruturas críticas, dados e cadeias energéticas. Na prática, o ciberespaço tornou-se o novo campo de disputa entre Estados, empresas e atores não estatais, com impactos diretos sobre a economia real e sobre a segurança corporativa.

O avanço da Inteligência Artificial transformou-se em um vetor de ruptura tanto econômica quanto ética. As aplicações de aprendizado de máquina e automação ampliam a produtividade, mas também introduzem novos riscos relacionados à manipulação de informações, à fraude digital e à perda de controle sobre sistemas críticos. Ao mesmo tempo, a regulação internacional da IA avança de forma desigual. Enquanto algumas regiões adotam marcos legais robustos, outras permanecem em estágios iniciais de governança, criando assimetrias normativas e riscos de uso indevido. Esse contexto favorece a proliferação de *deepfakes*, fraudes de identidade e ataques automatizados que desafiam a capacidade de defesa tradicional das organizações.

O componente climático, por sua vez, torna-se um multiplicador de riscos e um fator determinante para a estabilidade regional. O aumento da temperatura global, a irregularidade dos regimes de chuvas e a intensificação de eventos extremos comprometem a segurança alimentar, a geração de energia e a disponibilidade de recursos hídricos. O impacto direto desses fenômenos na América Latina é particularmente elevado devido à dependência da matriz hidrelétrica, à vulnerabilidade de setores agrícolas e à urbanização acelerada. As projeções indicam que eventos climáticos severos e crises de abastecimento tenderão a ocorrer com maior frequência e intensidade em 2026 e além, pressionando governos e empresas a adotarem políticas de adaptação e planos de continuidade mais abrangentes.

Paralelamente, o **crime organizado transnacional** assume uma nova configuração. O relatório *Global Organized Crime Index 2025* aponta para a consolidação de uma economia ilícita altamente diversificada, na qual os crimes financeiros, cibernéticos e ambientais superam, em crescimento e rentabilidade, os crimes violentos convencionais. Essa transformação redefine o conceito de segurança e revela a erosão das fronteiras entre o legal e o ilegal. As organizações criminosas passam a operar em redes globais e híbridas, utilizando empresas legítimas, plataformas digitais e sistemas financeiros paralelos como vetores de expansão. A penetração dessas redes em setores

formais da economia aumenta o risco de captura regulatória, corrupção e distorção de mercados.

A difusão do crime organizado de natureza corporativa e digital tem implicações diretas para o ambiente de negócios na América Latina. O enfraquecimento institucional e a cooperação limitada entre países dificultam o combate efetivo a fraudes e à lavagem de dinheiro. A convergência entre grupos criminosos, atores privados e fluxos de capital ilegais amplia o risco de exposição reputacional e de sanções regulatórias para empresas que não adotem mecanismos rigorosos de *compliance* e *due diligence*. Essa tendência está fortemente associada ao cenário denominado **"Redes Sombrias"**, no qual a ausência de coordenação entre políticas públicas, regulação tecnológica e integridade corporativa intensifica as vulnerabilidades sistêmicas.

Do ponto de vista econômico, 2026 deverá consolidar um ciclo de crescimento moderado e desigual, marcado por tensões comerciais e por políticas fiscais restritivas. A digitalização e a automação seguirão como motores de produtividade, porém com impactos sociais significativos, especialmente no mercado de trabalho e na distribuição de renda. A América Latina continuará dependente da exportação de commodities e enfrentará desafios de competitividade industrial. A retomada de investimentos dependerá da capacidade de estabilidade política, de governança ambiental e de segurança jurídica. Países que conseguirem combinar políticas climáticas consistentes, integração regional e inovação tecnológica terão vantagens competitivas sustentáveis na próxima década.

Em síntese, o panorama global de 2026 e além é definido por um conjunto de **tensões simultâneas**: avanço tecnológico versus risco digital, globalização econômica versus fragmentação política, crescimento produtivo versus instabilidade climática, e governança ética versus crime organizado. Essas tensões moldarão as principais **fontes de risco** e determinarão o grau de resiliência de cada país e setor. A compreensão dessas interdependências é essencial para que organizações públicas e privadas consigam antecipar eventos críticos, fortalecer sua governança e transformar a gestão de riscos em uma ferramenta estratégica de decisão.

1.4. Fontes de Risco Críticas e Incertezas Estruturais

A compreensão das **fontes de risco** que moldam o ambiente de negócios, segurança e governança na América Latina em 2026 e além é fundamental para orientar estratégias de adaptação e priorização de investimentos. As fontes de risco representam os elementos ou circunstâncias que, isoladamente ou combinados, podem originar ameaças, vulnerabilidades ou oportunidades, conforme definido pela norma ISO 31000.

Identificá-las e compreender suas interações permite desenvolver uma visão sistêmica da exposição e da capacidade de resposta das organizações diante de um cenário de crescente complexidade e convergência entre riscos físicos, digitais e sociais.

Neste estudo, distinguimos duas categorias principais: **(i) fontes de risco críticas**, que representam conjuntos estruturais de ameaças, vulnerabilidades e oportunidades; e **(ii) incertezas estruturais**, que correspondem a variáveis profundas, de alta influência e difícil previsibilidade, utilizadas como base para a construção dos cenários prospectivos. O estudo consolidou seis **fontes de risco críticas**, derivadas da análise de trinta e dois relatórios internacionais e regionais. Essas fontes estão interconectadas e formam o núcleo das dinâmicas que sustentam os quatro cenários apresentados posteriormente. Elas expressam tanto as forças motrizes globais quanto as fragilidades internas que determinam a trajetória dos países latino-americanos.

Tabela 1 – Fontes de Risco Críticas 2026 e Além

Fonte de Risco	Descrição Analítica	Impactos Principais	Tendência Regional (2026 e além)
1. Geopolítica e Comércio Internacional	Reconfiguração de alianças e cadeias de suprimentos em um contexto de multipolaridade e coerção econômica. Disputas tecnológicas e sanções comerciais afetam diretamente fluxos logísticos e cadeias críticas.	Instabilidade de mercados; restrições comerciais; vulnerabilidade energética; pressões sobre exportações agrícolas e minerais.	Aumento da dependência de acordos bilaterais e vulnerabilidade a choques externos.
2. Tecnologia, Dados e Inteligência Artificial	Aceleração da digitalização e da automação sem padrões regulatórios uniformes. Expansão do uso indevido da IA para fraudes, manipulação de dados e ataques cibernéticos automatizados.	Crescimento de crimes digitais; violação de dados sensíveis; impactos éticos e reputacionais; assimetria regulatória.	Expansão da IA generativa; aumento de ataques baseados em machine learning e *deepfakes*.
3. Crime Organizado, Finanças Ilícitas e Corrupção Sistêmica	Consolidação de redes híbridas que operam simultaneamente em economias formais e ilícitas. O *Global*	Captura do Estado; distorção de mercados; riscos reputacionais e de	Expansão de organizações ilícitas digitais; maior infiltração em setores logísticos, agrícolas e financeiros.

Fonte de Risco	Descrição Analítica	Impactos Principais	Tendência Regional (2026 e além)
	Organized Crime Index 2025 aponta a América Latina como epicentro de atividades criminosas diversificadas, incluindo tráfico, fraudes financeiras e crimes ambientais.	sanções; erosão institucional.	
4. Clima, Recursos Naturais e Sustentabilidade	Intensificação de eventos climáticos extremos, escassez hídrica e aumento da temperatura média. A crise climática se torna um multiplicador de riscos, afetando a segurança alimentar, energética e territorial.	Interrupção de negócios; perda de produtividade; danos à infraestrutura; insegurança alimentar; aumento de litígios ambientais.	Maior frequência de desastres naturais e pressão por governança climática corporativa.
5. Infraestruturas Críticas e Operações Industriais (OT)	Vulnerabilidade crescente de sistemas industriais conectados à internet e dependência de cadeias tecnológicas globais. Falhas em sistemas de controle e manutenção podem causar interrupções de larga escala. Crescente dependência de infraestruturas baseadas no espaço (satélite para comunicações, navegação, sincronização financeira, monitoramento climático etc.), que passam a ser vetores críticos de risco diante de possíveis ataques cibernéticos e disputas geopolíticas no ambiente espacial.	Paradas produtivas; danos materiais; impactos financeiros e ambientais; risco à integridade de trabalhadores e comunidades.	Ampliação de ataques a sistemas industriais; aumento da adoção de controles ICS-5 (Industrial Control Systems nível 5) e integração OT-IT.
6. Instituições, Governança e Confiança Social	Erosão da credibilidade institucional e polarização política. Desinformação e	Instabilidade política; crises de governança; redução	Persistência de polarização e desafios à legitimidade institucional

Fonte de Risco	Descrição Analítica	Impactos Principais	Tendência Regional (2026 e além)
	radicalização enfraquecem a capacidade de resposta estatal e a cooperação regional.	da atratividade de investimentos; aumento de riscos sociais e reputacionais.	em vários países latino-americanos. Essa fragilidade institucional tem raízes também em dinâmicas micro, como erosão de confiança nas relações interpessoais, polarização nas comunidades e desgaste de valores compartilhados, que se projetam da família e das redes locais para o sistema político, econômico e regulatório.

A migração desordenada intensifica essas fragilidades institucionais ao pressionar serviços públicos, alterar dinâmicas de segurança e criar oportunidades para redes ilícitas operarem em rotas de deslocamento humano. Os fluxos migratórios não estruturados ampliam tensões sociais, desafiam capacidades municipais e nacionais de acolhimento e expõem vulnerabilidades urbanas e fronteiriças. Esse fenômeno funciona como vetor transversal de instabilidade, ampliando a complexidade das respostas estatais e corporativas e reforçando padrões de assimetria institucional característicos de ambientes de risco sistêmico.

Essas seis fontes de risco não atuam isoladamente, mas formam uma **rede de interdependências** que amplifica seus efeitos. O impacto combinado de falhas tecnológicas, eventos climáticos e criminalidade transnacional, por exemplo, cria situações de ruptura que exigem novas formas de coordenação entre o setor público e o setor privado. O mesmo ocorre com a fragilidade institucional, que tende a agravar as demais dimensões de risco, reduzindo a capacidade de resposta coletiva e a confiança nas instituições.

A análise dessas fontes foi complementada pela identificação de três **incertezas estruturais**, que representam as variáveis de maior imprevisibilidade e impacto sobre o futuro regional. Elas funcionam como eixos de tensão que determinam a direção dos cenários prospectivos.

Tabela 2 – Incertezas estruturais 2026 e Além

Eixo de Incerteza	Descrição	Relevância Estratégica
Integração Regional versus Fragmentação Político-Criminal	Mede a capacidade dos países latino-americanos de cooperar em políticas de segurança, comércio e tecnologia. O avanço da integração regional fortalece a estabilidade e a resposta coletiva, enquanto a fragmentação favorece o crime organizado e a insegurança.	Define o nível de coordenação institucional e a eficácia das políticas públicas regionais.
Governança de Inteligência Artificial versus Caos Digital	Representa o equilíbrio entre a inovação tecnológica e a regulação ética. A ausência de governança sobre algoritmos e dados pode levar ao colapso da confiança digital e à expansão de crimes cibernéticos automatizados.	Determina a capacidade das economias em sustentar crescimento tecnológico com segurança e transparência.
Disciplina Macroeconômica versus Estresse Multichoque	Avalia a solidez das políticas fiscais e monetárias diante de crises simultâneas, como eventos climáticos, ciberataques e instabilidade social. O estresse multichoque afeta diretamente o financiamento da resiliência e a capacidade de investimento em infraestrutura crítica.	Influencia a sustentabilidade econômica e a competitividade regional de longo prazo.

Embora três incertezas estruturais tenham sido identificadas como críticas para o horizonte 2026 e além, a construção da Matriz de Cenários exigiu uma escolha metodológica quanto às variáveis que melhor capturam as diferenças qualitativas entre futuros alternativos. Assim, optou-se por utilizar **as duas primeiras incertezas estruturais** — *Integração Regional versus Fragmentação Político-Criminal* e *Governança de Inteligência Artificial versus Caos Digital* — como **eixos estruturantes da matriz 2x2**, por apresentarem maior capacidade de gerar configurações contrastantes de governança, cooperação, competição e estabilidade institucional. Ambas possuem características centrais em *frameworks* de prospectiva: são simultaneamente incertas, altamente influentes e mutuamente independentes para fins analíticos.

A terceira incerteza estrutural — *Disciplina Macroeconômica versus Estresse Multichoque* — foi, por sua vez, tratada como um **vetor transversal**, operando como campo de pressão sistêmico que permeia todos os cenários, em vez de constituir um eixo separador. Essa decisão reflete sua natureza distinta: ao contrário das duas primeiras, que definem direções estratégicas, a terceira descreve um *grau de intensidade* de choques (climáticos, tecnológicos, sociais e fiscais) capazes de amplificar

ou reduzir a resiliência das trajetórias futuras. Não se trata, portanto, de um binário que diferencia cenários, mas de um **gradiente estrutural** que afeta a profundidade, a velocidade e o impacto dos eventos descritos nos quatro quadrantes.

Ao posicionar essa terceira variável como **força transversal**, reconhecemos sua relevância sistêmica sem comprometer a clareza visual e interpretativa da matriz. A dimensão "multichoque" funciona como camada de complexidade adicional que interage com cada um dos cenários, acentuando riscos e oportunidades de maneiras distintas. Dessa forma, a matriz mantém sua função de representar contrastes estratégicos fundamentais, enquanto o relatório preserva a coerência analítica ao incorporar a dinâmica macroeconômica como elemento indispensável para compreensão do ambiente prospectivo de 2026 e anos subsequentes.

1.5. Matriz de Cenários 2026 e Além

A matriz de cenários apresentada neste capítulo sintetiza as combinações mais plausíveis derivadas das **incertezas estruturais selecionadas como eixos** para diferenciar futuros alternativos. Embora a análise anterior tenha identificado três incertezas de alta influência para o horizonte 2026 e além, a construção da matriz 2x2 se baseia especificamente em **duas delas** — aquelas com maior poder de criar trajetórias contrastantes e mutuamente exclusivas. A terceira incerteza estrutural, relativa à disciplina macroeconômica frente ao estresse multichoque, é tratada no estudo como **força transversal sistêmica**, permeando todos os cenários e modulando sua intensidade, mas sem operar como eixo separador.

Assim, a matriz organiza-se a partir de dois eixos críticos que definem as direções mais relevantes das transformações observadas na América Latina. O primeiro captura a oscilação entre integração e fragmentação institucional; o segundo reflete o equilíbrio entre governança tecnológica e caos digital. A interação entre esses vetores gera quatro futuros possíveis para o ambiente de risco, segurança e governança corporativa.

O eixo horizontal representa o grau de cooperação entre países latino-americanos, variando desde processos de integração econômica, política e tecnológica até uma fragmentação marcada pela expansão do crime organizado e pela deterioração institucional. O eixo vertical corresponde ao nível de governança da Inteligência Artificial, dos dados e das infraestruturas digitais, oscilando entre modelos maduros, éticos e transparentes e cenários caracterizados por descontrole, manipulação e assimetrias regulatórias. A combinação desses dois eixos define a estrutura 2x2 que organiza quatro narrativas de futuro, cada uma com implicações específicas para setores produtivos, instituições públicas e organizações privadas.

Tabela 3 – Matriz de Cenários 2026 e Além

Eixo Vertical	Governança Avançada de Inteligência Artificial, Dados e Infraestruturas Digitais	Caos Digital, Uso Indevido de Tecnologia e Assimetria Regulatória
Eixo Horizontal		
Integração Regional e Cooperação Econômica	**Cenário 1 – Aliança PragTécnica** Ambiente de cooperação pragmática entre países; avanços regulatórios; interoperabilidade de dados e mecanismos compartilhados de segurança digital; redução de fraudes e interrupções de negócios; fortalecimento de instituições.	**Cenário 3 – Clima de Choques** Integração econômica avança, mas com fragilidade tecnológica; eventos climáticos extremos e falhas digitais ocorrem simultaneamente; alta pressão sobre cadeias produtivas e infraestruturas críticas; necessidade de respostas coordenadas.
Fragmentação Político-Criminal e Baixa Cooperação Regional	**Cenário 4 – Dados com Travas, Fronteiras Abertas** Governança avançada de IA e segurança liderada por setores privados; resiliência concentrada em empresas de grande porte; governos instáveis; operações corporativas sustentadas por tecnologia de ponta e controles ICS-5.	**Cenário 2 – Redes Sombrias** Fragmentação institucional; captura do Estado por redes criminosas; expansão de economias ilícitas; *deepfakes*, fraudes e ataques cibernéticos automatizados; erosão da confiança; riscos físicos elevados.

Leitura Estratégica da Matriz

A matriz indica que o futuro da região será determinado principalmente pela capacidade de articular três elementos: **cooperação institucional, governança tecnológica e resiliência macroeconômica diante de ambientes de estresse multichoque**. Esses elementos moldam padrões de risco que se manifestam de forma distinta em cada quadrante e influenciam não apenas a arquitetura institucional, mas também a estabilidade fiscal, a capacidade de resposta do Estado e a continuidade das operações privadas. Embora os cenários sejam apresentados de forma isolada, na prática, países e setores podem vivenciar características sobrepostas, especialmente quando choques climáticos, tecnológicos ou econômicos pressionam a disciplina macroeconômica e **amplificam transições graduais entre quadrantes ao longo do tempo**.

Leitura Estratégica Ampliada do Cenário 1 – Aliança PragTécnica

O Cenário 1, denominado Aliança PragTécnica, expressa a possibilidade de um ambiente regional no qual a cooperação institucional e a governança tecnológica avançam de forma pragmática, gradual e consistente. Esse cenário não pressupõe uma integração política plena ou um salto institucional repentino, mas sim a adoção incremental de acordos, normas e mecanismos operacionais que reduzem atritos entre países latino-americanos e fortalecem a capacidade conjunta de resposta a riscos convergentes **em um contexto global ainda marcado por choques simultâneos que pressionam economias e setores produtivos**.

Do ponto de vista regulatório, esse cenário é caracterizado pela harmonização progressiva de leis e padrões relacionados à proteção de dados, governança de Inteligência Artificial, auditoria algorítmica, cibersegurança e identidade digital. Mesmo sem uma convergência legislativa completa, os marcos se tornam compatíveis entre si, permitindo interoperabilidade entre sistemas públicos e privados. A interoperabilidade, nesse contexto, abrange desde dados de identidade digital e certificados eletrônicos até protocolos de investigação financeira, inteligência de ameaças e rastreabilidade de cadeias logísticas críticas; **um fator particularmente relevante quando a região busca manter disciplina macroeconômica e reduzir vulnerabilidades a choques externos e internos**.

No campo da segurança, o Cenário 1 assume a consolidação de iniciativas conjuntas entre governos e empresas, sobretudo nos setores de energia, transporte, telecomunicações, indústria e finanças. Essa coordenação possibilita o compartilhamento de informações sobre ameaças, a padronização de práticas de resposta a incidentes e a criação de exercícios integrados de simulação. A cooperação tecnológica permite que capacidades avançadas, como detecção automatizada de ataques, autenticação biométrica regional e resposta coordenada a fraudes em larga escala, sejam distribuídas de forma mais equilibrada entre os países; **reduzindo a exposição sistêmica da região a multichoques que podem interromper cadeias de valor e acelerar pressões econômicas**.

A governança de riscos, nesse ambiente, torna-se mais previsível e transparente. Sistemas de monitoramento integrados permitem a detecção precoce de eventos críticos, reduzindo o tempo de resposta e aumentando a capacidade de mitigação. A confiança institucional cresce porque os países demonstram capacidade de agir coletivamente diante de riscos transnacionais, como crimes cibernéticos, eventos climáticos extremos e interrupções de cadeias logísticas. Esse processo também fortalece a resiliência de infraestruturas críticas, que passam a operar com padrões

mínimos regionais de cibersegurança e continuidade operacional; **um componente essencial para sustentar estabilidade econômica em cenários de estresse multichoque**. No plano econômico, a Aliança PragTécnica favorece fluxos comerciais mais estáveis, reduz incertezas regulatórias e atrai investimentos. Setores com forte dependência de previsibilidade, como energia renovável, logística integrada, agronegócio e economia digital, são particularmente beneficiados. A redução de barreiras técnicas e o aumento da confiança regulatória facilitam o desenvolvimento de corredores logísticos de baixo risco, mecanismos de compensação energética e redes de inovação baseadas em Inteligência Artificial confiável e auditável; **criando um ambiente que reforça a disciplina fiscal, melhora a percepção de risco soberano e reduz a vulnerabilidade a choques exógenos**.

Por fim, esse cenário amplia o espaço para políticas públicas que conciliam inovação e segurança. A Inteligência Artificial é adotada com governança ética, mecanismos de explicabilidade e auditoria automatizada, reduzindo a probabilidade de uso indevido por agentes ilícitos e aumentando a confiabilidade dos sistemas automatizados de decisão. As organizações ganham previsibilidade e podem planejar de forma mais robusta, uma vez que as fontes de risco são monitoradas por sistemas interligados que produzem alertas antecipados e orientam respostas coordenadas; **o que contribui diretamente para amortecer impactos econômicos de eventos multichoque**.

A Aliança PragTécnica, portanto, representa um futuro no qual a América Latina não elimina suas fragilidades históricas, mas desenvolve instrumentos coletivos e tecnologias maduras capazes de reduzir o impacto de riscos transfronteiriços. A cooperação regional, combinada à governança tecnológica avançada, cria um ambiente capaz de limitar a expansão de crimes digitais, mitigar potenciais consequências dos possíveis eventos climáticos severos e fortalecer a segurança física e cibernética de setores estratégicos **enquanto fortalece a resiliência macroeconômica e reduz a exposição regional a estresses multichoques**. Trata-se do cenário em que as organizações encontram as melhores condições para desenvolver resiliência dinâmica, atrair investimentos e consolidar modelos de governança orientados pela inteligência de riscos.

Leitura Estratégica Ampliada do Cenário 2 – Redes Sombrias

O Cenário 2, denominado Redes Sombrias, representa a configuração mais adversa entre os futuros plausíveis para a América Latina em 2026 e além. Ele surge quando a fragmentação político-criminal e a ausência de governança tecnológica convergem de maneira simultânea, criando um ambiente marcado pela erosão das instituições, pelo fortalecimento de redes ilícitas transnacionais e pela perda progressiva da confiança pública; **em um contexto de estresse multichoque que fragiliza ainda mais a disciplina**

macroeconômica e amplia assimetrias entre países e setores. Nesse cenário, o crime organizado deixa de atuar apenas nas margens do sistema econômico e passa a ocupar posições estratégicas em cadeias logísticas, financeiras e regulatórias, ampliando sua capacidade de influenciar mercados e distorcer decisões públicas e privadas.

Do ponto de vista institucional, o cenário é caracterizado por instabilidade política, ciclos curtos de governos, pressões populistas e baixa capacidade regulatória. A captura de estruturas estatais por grupos ilícitos, descrita pelo Global Organized Crime Index 2025, intensifica-se e fragmenta a atuação governamental, dificultando políticas de segurança de longo prazo e inviabilizando ações coordenadas entre países. A cooperação internacional é mínima, e organismos de fiscalização, controle e inteligência tornam-se vulneráveis tanto à corrupção quanto à intimidação. Como consequência direta, decisões regulatórias tornam-se imprevisíveis e sujeitas a influências externas, criando um ambiente de negócios volátil e propício a riscos jurídicos e reputacionais; **quadro agravado pela incapacidade de sustentar políticas macroeconômicas estáveis em meio a choques sucessivos**.

No domínio digital, a ausência de governança de Inteligência Artificial e a proliferação de tecnologias baratas e acessíveis potencializam fraudes, ataques cibernéticos e manipulação automatizada de informações. *Deepfakes*, esquemas de engenharia social de alta sofisticação e clones de identidade digital tornam-se práticas comuns, alimentadas por modelos de inteligência artificial não regulados. Os ataques de comprometimento de e-mail empresarial, fraudes financeiras e sequestros de dados se multiplicam em escala industrial, com agentes criminosos utilizando técnicas avançadas de automação, aprendizado de máquina e exploração simultânea de múltiplas vulnerabilidades. A fronteira entre ataques cibernéticos e ameaças físicas se dissolve, uma vez que grupos ilícitos utilizam informações digitais para extorsão, invasão de propriedades e direcionamento de crimes violentos; **acelerando danos econômicos e elevando custos de recomposição em um ambiente já pressionado por múltiplos choques**.

O ambiente operacional torna-se altamente imprevisível. Cadeias logísticas sofrem interrupções recorrentes provocadas por roubo de carga, bloqueios organizados, manipulação de rotas e interferências em sistemas de transporte. Portos, ferrovias e centros de distribuição tornam-se alvos estratégicos de grupos ilícitos que buscam controlar fluxos comerciais, tributos informais e rotas de exportação. Empresas de setores como agronegócio, mineração, varejo, energia e transporte enfrentam riscos elevados de interferência criminosa, inflação de custos, perda de produtividade e exposição à violência organizada. O risco físico contra executivos e equipes-chave cresce de forma significativa, exigindo protocolos de proteção ampliados **e pressionando ainda**

mais custos operacionais em economias já fragilizadas pela perda de disciplina fiscal e pela instabilidade de preços causada por multichoques.

No plano econômico e financeiro, o cenário é marcado por um aumento expressivo da economia ilícita, pela lavagem de dinheiro em larga escala e pela infiltração de capital criminoso em empresas legítimas. Crimes financeiros sofisticados, inclusive aqueles baseados em Inteligência Artificial, tornam-se mais lucrativos do que atividades ilícitas tradicionais. A utilização de criptomoedas, marketplaces digitais e redes de fronteira para operações de ocultação de ativos passa a integrar a estratégia básica das organizações criminosas. Para empresas formais, o risco de exposição involuntária à economia ilícita aumenta substancialmente, ampliando a possibilidade de sanções, investigações transnacionais e danos severos à reputação; **ao mesmo tempo em que volatilidade cambial, retração de crédito e perda de confiança nos mecanismos estatais de estabilização aprofundam o estresse macroeconômico**.

A confiança pública sofre declínio acelerado. Desinformação coordenada, campanhas de manipulação política, polarização digital e ataques contra instituições de imprensa e justiça provocam deterioração do ambiente democrático. A ausência de mecanismos eficazes de governança tecnológica permite que agentes criminosos, atores extremistas e interesses privados difusos manipulem a percepção social, gerando instabilidade e reduzindo a capacidade de resposta estatal. O enfraquecimento da coesão social aumenta a probabilidade de protestos violentos, ações de milícias digitais, linchamentos reputacionais e ataques a empresas associadas a temas sensíveis; **o que aprofunda ainda mais a instabilidade econômica ao gerar fuga de investimentos, retração de consumo e interrupção de serviços essenciais**.

Nesse cenário, as organizações enfrentam desafios significativos para operar com segurança e previsibilidade. Modelos tradicionais de gestão de riscos tornam-se insuficientes, pois não conseguem lidar com ameaças híbridas que combinam elementos digitais, financeiros, físicos e reputacionais, **incluindo o uso de drones autônomos e algoritmos de IA para apoiar intrusões físicas, sabotagem e contrabando em infraestruturas críticas e cadeias logísticas.** A ausência de coordenação estatal e a retração de mecanismos de proteção pública fazem com que empresas precisem internalizar capacidades típicas de segurança nacional, como inteligência contra ameaças, verificação reforçada de integridade, proteção executiva e redundância logística; **em um ambiente econômico onde a instabilidade estrutural e a pressão multichoque elevam custos, reduzem margens e tornam investimentos de longo prazo mais arriscados**.

O Cenário 2, portanto, representa um ambiente em que a racionalidade econômica e a governança pública perdem espaço para lógicas informais, ilícitas e opacas,

transformando o risco em um elemento onipresente e altamente volátil. A expansão das redes sombrias reduz a margem de ação das organizações, aumenta custos operacionais e gera ciclos prolongados de insegurança **em economias que já não conseguem manter disciplina fiscal ou estabilizar choques sucessivos**, afetando diretamente a competitividade, a atração de investimentos e a sustentabilidade das cadeias produtivas.

Leitura Estratégica Ampliada do Cenário 3 – Clima de Choques

O Cenário 3, denominado Clima de Choques, reflete um ambiente em que a cooperação econômica entre os países latino-americanos avança, mas permanece limitada pela fragilidade tecnológica, pela baixa maturidade em cibersegurança e pela crescente pressão exercida pelos eventos climáticos extremos; **pressionando continuamente a disciplina macroeconômica e ampliando a exposição regional a estresses sucessivos**. Trata-se de um cenário híbrido em que as economias conseguem manter níveis moderados de integração comercial e acordos de infraestrutura, porém sem a capacidade institucional e tecnológica necessária para proteger suas cadeias críticas das perturbações ambientais e digitais que se intensificam em 2026 e além.

O principal fator que define esse cenário é o clima como multiplicador de riscos. A região enfrenta secas prolongadas, ondas de calor extremo, tempestades severas e inundações que se tornam mais frequentes e intensas, acelerando a deterioração de solos, aumentando a volatilidade agrícola e causando perturbações significativas na geração e na distribuição de energia. A matriz energética baseada em hidreletricidade sofre impactos diretos, especialmente em países com reservatórios cada vez mais pressionados por variabilidade hídrica. Ao mesmo tempo, sistemas urbanos densamente povoados enfrentam desafios relacionados a deslizamentos, falta de água, ilhas de calor e fragilidade de drenagem; **choques que afetam diretamente preços, produtividade e capacidade fiscal dos Estados**.

Esses fenômenos climáticos produzem ciclos recorrentes de interrupção de negócios, com impactos desproporcionais sobre setores como energia, agronegócio, mineração, manufatura e logística. A sinergia entre eventos ambientais e falhas digitais amplia ainda mais os efeitos de cada incidente. Sistemas industriais conectados tornam-se vulneráveis a flutuações elétricas, superaquecimento de componentes, falhas em sensores e perda temporária de conectividade. A interação entre fragilidade climática e fragilidade tecnológica gera interrupções em cadeias produtivas que já operam sob margens estreitas, criando atrasos logísticos, escassez de insumos e perdas financeiras cumulativas **que se propagam como estresse macroeconômico estrutural**.

A logística regional sofre impactos significativos. Rodovias são interrompidas por alagamentos, quedas de barreiras e incêndios florestais. Ferrovias e portos enfrentam paralisações decorrentes de eventos climáticos severos, aumentando custos de transporte e pressionando preços internos. Redes elétricas e de telecomunicações também se tornam vulneráveis, especialmente em áreas com infraestrutura antiga ou mal distribuída. A dependência das cadeias exportadoras de alimentos, minérios e energia torna-se mais evidente, ampliando tensões entre demanda global e limitações físicas locais **e gerando volatilidade macroeconômica adicional em economias já sensíveis a choques externos**.

No campo institucional, apesar de existir cooperação econômica, os governos latino-americanos enfrentam dificuldades para coordenar respostas climáticas em grande escala. A ausência de políticas robustas de adaptação e resiliência produz um ambiente em que a atuação estatal é frequentemente reativa, fragmentada e insuficiente para amortecer o impacto dos choques ambientais. A região apresenta padrões irregulares de fiscalização, licenciamento ambiental, proteção de ecossistemas e prevenção de desastres, dificultando o planejamento integrado. Esses déficits institucionais agravam vulnerabilidades setoriais e intensificam o desgaste da infraestrutura física e social; **além de pressionarem gastos emergenciais, reduzirem a capacidade de investimento público e diminuírem a margem fiscal para políticas anticíclicas**.

A insegurança hídrica torna-se um dos marcadores mais sensíveis do cenário. Em vários países, reservatórios, aquíferos e sistemas de abastecimento público passam a operar em níveis críticos, afetando diretamente indústrias de alto consumo de água, como agricultura irrigada, metalurgia, bebidas, papel e celulose e mineração. A competição por recursos hídricos intensifica conflitos territoriais, pressiona políticas de concessão e impõe custos adicionais a empresas, que precisam investir em reuso de água, fontes alternativas e planos de contingência; **custos que pressionam margens, preços e indicadores macroeconômicos-chave**.

Do ponto de vista tecnológico, a baixa maturidade digital e a insuficiência de controles avançados de segurança aumentam o risco de incidentes cibernéticos que ocorrem paralelamente a choques climáticos. Em situações de estresse ambiental, a probabilidade de falhas humanas e operacionais também cresce, ampliando vulnerabilidades em sistemas de supervisão, monitoramento e controle. Organizações enfrentam dificuldades para manter operações contínuas, sobretudo quando dependem de equipamentos sensíveis à temperatura, conectividade estável e integridade das redes elétricas; **fatores que amplificam custos de produção e impactam estabilidade macroeconômica regional**.

Nesse cenário, a necessidade de resiliência climática torna-se urgente. Empresas e governos são forçados a investir em redundância estrutural, diversificação de fontes energéticas, modernização de infraestruturas e sistemas preditivos baseados em análise de dados e Inteligência Artificial. Modelos de previsão ambiental, sensores, satélites e redes inteligentes tornam-se essenciais para detectar tendências adversas e antecipar respostas. Ao mesmo tempo, cresce a demanda por seguros paramétricos e mecanismos de financiamento climático, especialmente em setores vulneráveis; **instrumentos que, embora reduzam impactos, também pressionam orçamentos públicos e privados, exigindo disciplina financeira mais rigorosa**.

O Cenário 3 também acarreta consequências sociais. A vulnerabilidade climática agrava desigualdades, produz deslocamentos populacionais, pressiona sistemas urbanos e eleva tensões sociais em áreas afetadas por escassez de recursos. Esses impactos aumentam a necessidade de políticas de adaptação, protocolos de emergência e programas de apoio às comunidades mais expostas; **todos dependentes de recursos fiscais que se tornam mais disputados em um ambiente macroeconômico de múltiplos choques**.

O Clima de Choques, portanto, descreve um futuro em que o ambiente econômico mantém relativa estabilidade, mas a capacidade de operar de maneira segura e previsível é profundamente comprometida pela convergência entre eventos ambientais severos e fragilidade tecnológica. A região precisa reforçar sua governança climática, ampliar investimentos em adaptação e fortalecer a resiliência de infraestruturas críticas **para evitar que ciclos de multichoque se convertam em instabilidade fiscal permanente, perda de competitividade e retrocessos estruturais**.

Leitura Estratégica Ampliada do Cenário 4 – Dados com Travas, Fronteiras Abertas

O Cenário 4, denominado Dados com Travas, Fronteiras Abertas, descreve um ambiente no qual o setor privado alcança níveis elevados de maturidade tecnológica e governança digital, enquanto a instabilidade institucional persiste e limita a eficácia das políticas públicas; **um contexto em que choques sucessivos e restrições fiscais dificultam a manutenção de disciplina macroeconômica e aprofundam assimetrias estruturais**. É um futuro marcado pela disparidade entre uma economia corporativa cada vez mais avançada, sofisticada e resiliente, e estruturas estatais fragmentadas, incapazes de acompanhar o ritmo de inovação e de impor padrões uniformes de segurança, regulação ou justiça. Como resultado, a região vive uma assimetria profunda: empresas líderes conseguem operar com relativa estabilidade, mas o conjunto da economia permanece vulnerável a riscos sistêmicos.

Nesse cenário, a governança da Inteligência Artificial passa a ser conduzida prioritariamente por grandes conglomerados, plataformas tecnológicas e empresas de infraestrutura crítica. Elas desenvolvem mecanismos próprios de auditoria algorítmica, explicabilidade e proteção de dados, estabelecendo padrões que se tornam referência para o mercado e que, muitas vezes, ocupam o espaço deixado por marcos regulatórios incompletos ou desatualizados. A ausência de um ambiente regulatório uniforme leva empresas de grande porte a atuarem como "legisladores de fato", definindo diretrizes privadas de conformidade que influenciam fornecedores, parceiros logísticos e cadeias industriais; **fenômeno acentuado pela incapacidade estatal de adaptar-se rapidamente em meio a choques econômicos, climáticos e tecnológicos**.

A maturidade digital das organizações nesse cenário é elevada. Empresas líderes adotam sistemas robustos de autenticação biométrica, segmentação avançada de redes, criptografia de ponta e modelos de Inteligência Artificial defensiva capazes de detectar comportamentos anômalos e antecipar ataques cibernéticos. A implementação de controles ICS-5 torna-se diferencial competitivo em setores industriais, de energia, saneamento, alimentos e logística, permitindo níveis superiores de disponibilidade operacional, redundância e integridade dos processos críticos. Ao mesmo tempo, soluções de monitoramento integrado, como Centros de Operações de Segurança ciberfísica (GSOC convergentes), elevam a capacidade de resposta a incidentes **e funcionam como amortecedores privados em um ambiente de multichoque que pressiona sistemas públicos fragilizados**.

Apesar desse avanço privado, o ambiente institucional é marcado por instabilidade política, fragmentação de políticas públicas e baixa capacidade de execução estatal. Governos enfrentam restrições fiscais e operacionais, dificultando a atualização de marcos legais, a criação de mecanismos eficazes de fiscalização e a modernização de infraestruturas públicas. Em vários países, sistemas judiciais sobrecarregados, disputas políticas e mudanças abruptas de orientação normativa produzem incertezas regulatórias e insegurança jurídica. A ausência de políticas robustas de integração regional também limita o avanço de acordos que poderiam reduzir custos transfronteiriços, ampliar infraestrutura logística e uniformizar padrões de proteção de dados; **e a soma de instabilidade institucional com choques simultâneos aprofunda a volatilidade macroeconômica**.

Nesse ambiente, o risco se torna altamente assimétrico. Organizações com capacidade tecnológica e recursos suficientes conseguem mitigar ameaças, preservar sua reputação e manter a continuidade de suas operações. Já empresas de médio e pequeno porte, bem como cadeias produtivas menos capitalizadas, permanecem expostas a ataques cibernéticos, fraudes, interrupções de energia e instabilidades logísticas. A desigualdade tecnológica amplia o fosso entre empresas resilientes e vulneráveis, criando um

ecossistema de proteção desigual e incompatível com a resiliência sistêmica necessária para evitar colapsos regionais; **especialmente em ambientes macroeconômicos sujeitos a choques sucessivos e volatilidade fiscal**.

O setor privado assume, nesse cenário, um papel ampliado na proteção de infraestruturas críticas. Empresas passam a investir em redundâncias locais, microgeração energética, redes privadas de telecomunicações e modelos avançados de supervisão e controle, reduzindo sua dependência de serviços públicos. Essa tendência reforça a criação de "ilhas de resiliência", nas quais ambientes controlados por empresas alcançam padrões elevados de confiabilidade, enquanto áreas adjacentes continuam sujeitas a falhas sistêmicas, interrupções e criminalidade; **um mosaico de alta resiliência localizada e vulnerabilidade estrutural que se agrava com a incapacidade estatal de estabilizar choques econômicos**.

No campo econômico, o ambiente de negócios se torna competitivo, porém desigual. A inovação prospera em ecossistemas corporativos integrados a cadeias globais de valor, enquanto segmentos dependentes de políticas públicas permanecem estagnados. Serviços financeiros, tecnologia, energia limpa, manufatura avançada e logística de alto valor tornam-se catalisadores de crescimento. Em contrapartida, setores com forte dependência de infraestrutura pública ou de marcos regulatórios estáveis enfrentam desafios estruturais para alcançar produtividade e atrair investimentos; **especialmente em ambientes macroeconomicamente pressionados, com ciclos recorrentes de instabilidade e restrições fiscais crônicas**.

A segurança pública permanece fragilizada. A falta de integração entre agências estatais e a ausência de políticas regionais coerentes ampliam a atuação de redes ilícitas, especialmente em áreas rurais, fronteiriças e portuárias. A criminalidade organizada explora brechas no aparato estatal enquanto evita ambientes empresariais fortificados. Isso produz um fenômeno dual: alta resiliência dentro dos ambientes controlados por grandes empresas e alta vulnerabilidade fora deles; **um espelhamento da assimetria macroeconômica que caracteriza o cenário**.

O cenário também possui implicações sociais significativas. A desigualdade no acesso à tecnologia e à segurança gera fricções entre setores da economia, amplia tensões trabalhistas e reforça a percepção de que a proteção e a estabilidade são bens privados, disponíveis apenas para organizações com altos níveis de investimento. A polarização digital e a fragilidade institucional dificultam a construção de políticas públicas inclusivas, limitando o alcance de soluções de longo prazo **e agravando tensões sociais típicas de ambientes submetidos a estresse multichoque**.

O Cenário 4, portanto, descreve um futuro no qual a resiliência corporativa avança mais rápido do que a resiliência estatal, criando um modelo de proteção fragmentado e insuficiente para amortecer riscos sistêmicos. Embora as organizações líderes consigam preservar competitividade por meio de tecnologias avançadas, a falta de integração institucional e a instabilidade regulatória impedem que os benefícios da inovação se disseminem de maneira uniforme pela região. Trata-se de um cenário ambíguo: próspero para quem está na fronteira tecnológica e vulnerável para quem depende de políticas públicas e infraestrutura estatal. A capacidade das organizações de operar de forma segura nesse ambiente dependerá de investimentos contínuos em tecnologia, resiliência e governança interna, bem como de estratégias para mitigar a ausência de padrões regulatórios e a volatilidade das instituições públicas; **características agravadas por choques econômicos recorrentes e pela dificuldade estrutural de manter disciplina macroeconômica**.

Implicações Gerais da Matriz

A leitura integrada da Matriz de Cenários 2026 e além revela cinco implicações estratégicas de caráter transversal, que influenciam o ambiente político, econômico, tecnológico e institucional de toda a região. Elas sintetizam os elementos comuns que emergem da interação entre as fontes de risco críticas e as incertezas estruturais, incluindo a pressão crescente exercida por choques simultâneos sobre a disciplina macroeconômica. Essa leitura integrada oferece diretrizes fundamentais para orientar decisões de governos, empresas e organismos multilaterais.

Em todas essas dimensões, a integridade ética — tanto na esfera pública quanto na privada — funciona como uma “infraestrutura invisível” da confiança. Quando valores de honestidade, responsabilidade e transparência se deterioram, aumentam os custos de transação, ampliam-se as oportunidades para captura institucional e reduz-se a eficácia dos próprios mecanismos de gestão de riscos. Essa base ético-moral constitui o alicerce que sustenta a cooperação institucional, a governança tecnológica e a capacidade de resiliência organizacional.

A primeira implicação diz respeito à necessidade de elevar de forma consistente o padrão de governança tecnológica, especialmente no que se refere ao uso ético, seguro e transparente da Inteligência Artificial. A ausência de marcos regulatórios coerentes e de mecanismos de auditoria algorítmica amplia vulnerabilidades e permite que tecnologias avançadas sejam utilizadas para fraudes, manipulação de dados e invasão de identidades digitais. A governança tecnológica torna-se, portanto, eixo central para preservar a integridade dos dados, garantir previsibilidade regulatória e reforçar a confiança digital, que é hoje um dos pilares do funcionamento das economias digitais e das infraestruturas críticas; especialmente em ambientes sujeitos a estresse

multichoque, nos quais danos digitais podem rapidamente amplificar impactos econômicos e sociais.

A segunda implicação refere-se à cooperação institucional como elemento decisivo para reduzir vulnerabilidades e enfrentar riscos transnacionais. Crimes financeiros, redes ilícitas, eventos climáticos extremos, ataques cibernéticos e interrupções logísticas não respeitam fronteiras administrativas. Países que operam isoladamente tendem a enfrentar ciclos mais longos de instabilidade, maior custo econômico e dificuldades para manter disciplina fiscal diante de choques sucessivos. Já ambientes que adotam acordos regionais de interoperabilidade, padrões compartilhados de segurança e mecanismos conjuntos de resposta a incidentes conseguem proteger melhor suas cadeias produtivas e fortalecer a capacidade de coordenação institucional. Nesse sentido, a cooperação não é apenas desejável, mas essencial para impedir a expansão de dinâmicas típicas do Cenário 2, marcado por redes ilícitas e fragmentação político-criminal.

A terceira implicação decorre da constatação de que o clima se tornou um multiplicador de riscos estruturais. Os eventos climáticos extremos afetam a produtividade agrícola, pressionam a matriz energética, comprometem a infraestrutura urbana e desestabilizam cadeias logísticas críticas. Eles também amplificam efeitos colaterais, como conflitos territoriais, insegurança hídrica e migração forçada. Essa combinação eleva custos sistêmicos, reduz margens econômicas e pressiona orçamentos públicos, dificultando respostas anticíclicas e erodindo a disciplina macroeconômica. Diante desse cenário, qualquer abordagem de risco baseada apenas em mitigação torna-se insuficiente. A região precisa avançar em políticas de adaptação climática, proteção ambiental e continuidade de negócios, integrando previsões ambientais, dados operacionais e tecnologias de análise preditiva baseadas em Inteligência Artificial. Sem essa capacidade de adaptação, a região ficará presa ao ciclo de vulnerabilidades característico do Cenário 3, no qual o clima interage com fragilidades tecnológicas e econômicas para gerar rupturas contínuas.

A quarta implicação destaca o papel estratégico de uma segurança convergente que ultrapassa os limites tradicionais da segurança corporativa. A separação entre o físico e o cibernético — e entre o público e o privado — deixou de ser adequada para lidar com ameaças híbridas em ambientes ciberfísicos. Redes ilícitas utilizam informações digitais para ataques físicos; grupos criminosos infiltram cadeias logísticas e exploram plataformas digitais para extorsão; eventos climáticos expõem vulnerabilidades tanto em sistemas industriais quanto em infraestruturas públicas. Nesse contexto, a proteção exige uma atuação integrada que articule Estado, empresas e sociedade, combinando segurança física, segurança cibernética, proteção de dados, inteligência contra ameaças e mecanismos de governança reputacional. Modelos como Centros de Operações de Segurança convergentes — que integram monitoramento público e privado — e

controles industriais robustos (incluindo ICS-5) tornam-se essenciais para garantir resiliência ciberfísica, continuidade de serviços essenciais e integridade dos processos críticos, especialmente quando eventos multichoque ampliam simultaneamente riscos digitais, físicos e institucionais.

Por fim, a quinta implicação decorre do fato de que a resiliência organizacional depende da capacidade de navegar dinamicamente entre cenários. A região não evolui de forma linear, e organizações podem vivenciar simultaneamente elementos de diferentes quadrantes. O ambiente futuro exigirá decisões estratégicas ajustáveis, modelos de operação flexíveis e mecanismos de monitoramento contínuo baseados em indicadores de alerta precoce.

Organizações resilientes serão aquelas capazes de ajustar estratégias rapidamente, utilizar Inteligência Artificial explicável para analisar contextos complexos e integrar informações diversas para antecipar rupturas; inclusive rupturas geradas por choques fiscais, climáticos, tecnológicos ou institucionais. O desafio central está em transformar incerteza em capacidade adaptativa e em desenvolver estruturas internas que respondam com velocidade, coerência e inteligência às mudanças do ambiente externo. Em conjunto, essas cinco implicações compõem a base da capacidade regional de enfrentar riscos híbridos, construir estruturas de proteção sistêmica e fortalecer a resiliência econômica, institucional e corporativa. Elas orientam as transições entre os cenários descritos e preparam o terreno para a análise detalhada das narrativas, cadeias causais e impactos estratégicos apresentados nos capítulos seguintes, incluindo a dinâmica transversal dos estresses multichoque e seus efeitos sobre a estabilidade macroeconômica.

02

CENÁRIOS DETALHADOS

2.1. Introdução

O Capítulo 2 apresenta a análise aprofundada dos quatro cenários estruturados na Matriz de Cenários 2026 e além. Diferentemente do capítulo anterior, que forneceu uma leitura estratégica e comparativa das lógicas macro que orientam cada quadrante, esta etapa avança para um nível operacional e decisório. O objetivo é detalhar como cada cenário se manifesta na prática, quais são suas cadeias causais, que riscos específicos emergem em cada ambiente e como empresas, governos e organizações podem compreender e responder de forma mais eficaz às suas dinâmicas.

Nesta etapa não há redundância com o item 1.5. Aqui, aprofundamos as variáveis determinantes por meio da análise das fontes de risco predominantes, das implicações setoriais diretas, dos impactos sobre a segurança corporativa e da avaliação dos fatores que influenciam a continuidade de negócios. Avançamos também sobre a estrutura interna de cada cenário, detalhando tensões, vulnerabilidades e oportunidades que não aparecem nas interpretações estratégicas do capítulo anterior. Essa abordagem permite que o leitor compreenda como cada cenário se materializa no cotidiano das operações, da governança e da infraestrutura crítica.

A análise segue uma estrutura uniforme para os quatro cenários. Para cada um deles, são apresentados: o contexto e seus fundamentos; a cadeia causal ampliada que explica como diferentes fontes de risco interagem; os impactos sobre setores produtivos e cadeias críticas; os efeitos específicos na segurança física, cibernética e reputacional; as implicações para a governança, a continuidade e a integridade organizacional; além dos indicadores de alerta precoce que permitem monitorar sinais de transição entre cenários. Finalmente, são identificadas oportunidades estratégicas que podem emergir mesmo em contextos adversos ou instáveis.

Com essa abordagem, o Capítulo 2 oferece um mapa detalhado das trajetórias possíveis de risco, permitindo que organizações desenvolvam estratégias adaptativas e fortaleçam sua resiliência em um ambiente marcado por incertezas crescentes e interdependência entre riscos físicos, digitais, climáticos e institucionais.

2.2. Cenário 1 – Aliança PragTécnica

2.2.1. Contexto e Fundamentos

O Cenário 1, Aliança PragTécnica, surge da combinação de dois elementos estruturais: maior integração regional e avanços consistentes na governança tecnológica. Ele descreve um ambiente no qual países latino-americanos conseguem coordenar políticas

de segurança, comércio, infraestrutura e tecnologia, criando padrões comuns que reduzem a fragmentação regulatória e fortalecem a capacidade coletiva de enfrentar riscos transnacionais. As organizações operam em um contexto de previsibilidade moderada, com mecanismos eficientes de interoperabilidade e marcos normativos que evoluem de forma gradual, porém contínua.

Este cenário não representa uma integração plena; trata-se de um processo pragmático, baseado em acordos operacionais, protocolos técnicos e iniciativas de cooperação multissetorial mediadas por organismos regionais, setores empresariais e parcerias público-privadas. A estabilidade institucional, relativa, mas crescente, permite investimentos em inovação, infraestrutura e proteção de dados, criando condições mais robustas para o desenvolvimento sustentável e para a competitividade regional.

2.2.2. Cadeia Causal Ampliada

A dinâmica do Cenário 1 se estrutura a partir de uma cadeia causal composta por cinco elementos principais. Primeiro, ocorre a harmonização gradual de regulações de proteção de dados, cibersegurança e Inteligência Artificial, reduzindo a assimetria jurídica entre países.

Segundo essa harmonização favorece a interoperabilidade entre sistemas públicos e privados, ampliando a capacidade de monitoramento de ameaças e compartilhamento seguro de informações.

Terceiro, a interoperabilidade fortalece mecanismos de prevenção e resposta a incidentes, tanto no espaço digital quanto nas operações físicas.

Quarto, a eficiência desses mecanismos aumenta a confiança institucional e reduz incentivos para atividades ilícitas, diminuindo a exposição a fraudes, crimes financeiros e ataques coordenados.

Quinto, essa maior previsibilidade estimula investimentos em inovação, infraestrutura e modernização de cadeias produtivas, criando um ciclo positivo entre regulação, tecnologia e resiliência.

2.2.3. Fontes de Risco Predominantes no Cenário

Mesmo em um ambiente mais favorável, três fontes de risco permanecem predominantes e exigem atenção constante.

Primeiro, riscos tecnológicos relacionados à Inteligência Artificial e à automação, que exigem governança contínua para evitar vieses, falhas e ataques sofisticados.

Segundo riscos geopolíticos e de comércio internacional, uma vez que a América Latina ainda depende de mercados externos e está sujeita a volatilidades que podem afetar cadeias de suprimentos estratégicas.

Terceiro, riscos climáticos, que continuam pressionando infraestrutura, agricultura, energia e abastecimento hídrico, mesmo com esforços de adaptação.

Essas fontes de risco não desaparecem; o diferencial deste cenário está na capacidade de mitigação ampliada, sustentada por coordenação regional e investimentos estruturais.

2.2.4. Implicações Setoriais Diretas

O impacto do Cenário 1 varia conforme o setor. Na indústria e na agricultura, a adoção de tecnologias avançadas e padrões comuns de cibersegurança reduz interrupções e aumenta produtividade.

No setor financeiro, a integração regulatória fortalece a proteção contra crimes digitais e lavagem de dinheiro, ampliando a confiança de investidores.

No setor de energia, a cooperação regional facilita a modernização de redes elétricas, a expansão de fontes renováveis e a implementação de sistemas de monitoramento preditivo baseados em Inteligência Artificial.

Na logística, corredores integrados reduzem custos e aumentam previsibilidade. Em saúde, educação e serviços públicos, a interoperabilidade permite maior eficiência e qualidade.

Com isso, setores mais intensivos em tecnologia e operações críticas tornam-se mais competitivos e resilientes.

2.2.5. Impactos na Segurança Corporativa (Física, Cibernética e Reputacional)

A segurança corporativa no Cenário 1 adquire caráter preventivo, integrado e preditivo. A cooperação regional e a governança avançada de dados reduzem a superfície de ataque e fortalecem mecanismos de autenticação, detecção e resposta.

A integração entre segurança física e cibernética se torna padrão, com Centros de Operações Convergentes operando tanto para riscos digitais quanto para riscos físicos, ambientais e reputacionais.

Do ponto de vista operacional, práticas de segurança baseadas em sensores, análise comportamental, monitoramento contínuo e machine learning reduzem eventos adversos.

O risco reputacional também diminui, uma vez que os níveis de confiança institucional e corporativa aumentam.

Além disso, a maior transparência regulatória facilita auditorias, certificações e *due diligence*, protegendo empresas contra riscos legais e de conformidade.

2.2.6. Impactos na Governança e na Continuidade de Negócios

A governança corporativa se fortalece por meio de padrões regionais compartilhados, especialmente na proteção de dados, na gestão de riscos digitais e na integração de planos de continuidade entre países.

Empresas passam a adotar políticas de redundância e adaptação climática alinhadas a recomendações multilaterais, tornando-se mais preparadas para eventos de alta complexidade.

A Inteligência Artificial explicável e auditável se torna parte da governança interna, reforçando a confiança entre stakeholders.

A continuidade de negócios passa a considerar cenários transfronteiriços, ampliando a capacidade de resposta a interrupções climáticas, logísticas ou tecnológicas. Planos integrados de contingência e cadeias de suprimentos mais diversificadas mitigam riscos de rupturas inesperadas.

2.2.7. Indicadores Específicos de Alerta Precoce (EWI)

O monitoramento de sinais antecipatórios é essencial para detectar possíveis desvios que podem deslocar o ambiente para cenários mais adversos. Entre os principais indicadores estão:

- Redução de políticas regionais de interoperabilidade;

- Quedas no índice de confiança institucional;
- Crescimento de incidentes cibernéticos que ultrapassam fronteiras;
- Aumento de disputas regulatórias entre países;
- Retrocessos em marcos de governança de dados e IA;
- Falhas energéticas ou hídricas recorrentes;
- Redução de investimentos em inovação e infraestrutura crítica.

A deterioração desses indicadores pode sinalizar uma transição para o Cenário 3 ou para o Cenário 4.

2.2.8. Sinais de Transição do Cenário

A Aliança PragTécnica pode enfraquecer se houver polarização política, pressão fiscal prolongada, retrocessos institucionais ou instabilidade regulatória. Caso esses elementos se intensifiquem, a região pode migrar para o Cenário 4 (se o setor privado sustentar a maturidade tecnológica) ou para o Cenário 3 (se o clima e a infraestrutura se tornarem as maiores fontes de ruptura).

2.2.9. Oportunidades Estratégicas

Mesmo sendo o cenário mais favorável, a Aliança PragTécnica contém oportunidades importantes para ampliar a resiliência e a competitividade.

Entre elas estão: expansão de mercados digitais integrados; desenvolvimento de padrões regionais de cibersegurança e proteção de dados; fortalecimento de redes logísticas inteligentes; avanço em energia limpa e infraestrutura verde; construção de plataformas regionais de interoperabilidade; e utilização de Inteligência Artificial para governança, *compliance* e análise preditiva.

Empresas que investirem em inovação, cooperação institucional e padrões elevados de governança estarão mais bem posicionadas para capturar valor e antecipar rupturas.

2.3. Cenário 2 – Redes Sombrias

2.3.1. Contexto e Fundamentos

O Cenário 2, Redes Sombrias, emerge da combinação entre fragmentação político-institucional e ausência de governança tecnológica. Ele descreve um ambiente no qual

as instituições públicas perdem capacidade de coerção, regulação e fiscalização, e no qual redes ilícitas transnacionais expandem sua atuação para setores formais da economia. A erosão da confiança institucional abre espaço para que grupos criminosos, atores privados oportunistas e movimentos clandestinos influenciem cadeias econômicas, decisões públicas e fluxos financeiros.

A ausência de coordenação regional e a incapacidade de atualizar marcos legais tornam os Estados mais lentos do que os agentes ilícitos, que operam com estruturas flexíveis, redes digitais descentralizadas e modelos financeiros opacos. Esse desequilíbrio cria um ambiente de risco permanente, no qual a imprevisibilidade, a violência e a manipulação digital tornam-se elementos estruturantes das relações econômicas e sociais.

2.3.2. Cadeia Causal Ampliada

A evolução do Cenário 2 pode ser explicada pela interação de cinco fenômenos encadeados.

Primeiro, a fragilidade institucional reduz a capacidade de monitorar crimes financeiros, tráfico de dados, corrupção e lavagem de dinheiro, abrindo espaço para infiltração em setores críticos.

Segundo a governança digital inexistente permite que grupos ilícitos usem Inteligência Artificial para fraudes, *deepfakes*, extorsão e ataques automatizados. Terceiro, a expansão dessas redes compromete cadeias de suprimentos, criando dependências invisíveis entre setores formais e informais.

Quarto, essa instabilidade afeta a segurança física, elevando riscos de violência, sabotagem e extorsão.

Quinto, a deterioração simultânea do ambiente físico e digital reduz a confiança pública, promove instabilidade econômica e desestimula investimentos, criando um ciclo vicioso difícil de reverter.

2.3.3. Fontes de Risco Predominantes no Cenário

Três grandes fontes de risco assumem protagonismo no Cenário 2. A primeira é o crime organizado transnacional, que opera em múltiplos domínios: digital, financeiro, logístico, ambiental e político.

A segunda é a desinformação e a manipulação digital baseada em Inteligência Artificial, que se tornam ferramentas estruturais de influência e extorsão.

A terceira é a fragilidade institucional, que limita a capacidade de resposta dos Estados e facilita a captura de órgãos públicos, empresas estatais, regulações estratégicas e processos de licenciamento.

Essas fontes se reforçam mutuamente, criando um ambiente onde ameaças digitais, físicas e reputacionais se manifestam de forma híbrida e contínua.

2.3.4. Implicações Setoriais Diretas

No setor financeiro, o aumento de fraudes, lavagem de dinheiro e ocultação de ativos torna o risco sistêmico elevado. Operações bancárias, meios de pagamento e ecossistemas de criptoativos são alvos frequentes de redes ilícitas.

Na logística, grupos criminosos controlam rotas, intimidam operadores e infiltram cadeias de transporte, elevando custos e insegurança.

No agronegócio, parte da produção é desviada ou cooptada por redes criminosas que buscam controlar commodities, créditos de carbono e rotas de exportação. No setor energético, furtos, sabotagem e manipulação de infraestrutura aumentam interrupções.

Na mineração, garimpos ilegais e pressões territoriais promovem conflitos socioambientais intensos.

Todos os setores enfrentam riscos crescentes de coação, fraude e manipulação digital.

2.3.5. Impactos na Segurança Corporativa (Física, Cibernética e Reputacional)

A segurança corporativa, entendida como função estratégica que integra suas dimensões física, cibernética, reputacional, entre outras, torna-se um dos pilares mais críticos para operar nesse cenário. A segurança física enfrenta ameaças diretas como sequestros, extorsão, sabotagem e violência organizada, especialmente contra executivos e equipes de campo. A segurança cibernética é pressionada por ataques automatizados, clones de identidade, *deepfakes* executivos e extorsões baseadas em vazamento de dados.

A segurança reputacional torna-se volátil devido a campanhas coordenadas de desinformação, manipulação política e ataques contramarcas associados a temas sensíveis.

Modelos tradicionais de segurança tornam-se insuficientes. Organizações passam a adotar estruturas integradas de inteligência, proteção executiva reforçada, análises comportamentais contínuas e operações coordenadas entre segurança física, digital e jurídica.

2.3.6. Impactos na Governança e na Continuidade de Negócios

A governança corporativa é pressionada pela complexidade de riscos ilegais e pela possibilidade de envolvimento involuntário com fluxos ilícitos.

Due diligences tornam-se mais complexas, auditorias mais frequentes e exigências regulatórias mais rigorosas, especialmente de órgãos internacionais.

Empresas enfrentam riscos jurídicos ampliados se forem expostas a cadeias contaminadas por ilícitos, corrupção ou crimes ambientais.

A continuidade de negócios sofre com interrupções derivadas de sabotagem, extorsão digital, bloqueios logísticos e flutuações políticas intensas.

Organizações precisam desenvolver planos de contingência baseados em riscos híbridos, criar redundâncias operacionais e internalizar capacidades típicas de agências de inteligência.

2.3.7. Indicadores Específicos de Alerta Precoce (EWI)

Entre os sinais antecipatórios mais relevantes estão:

- Aumento atípico de crimes financeiros transnacionais;
- Expansão de *deepfakes* utilizados para extorsão e manipulação corporativa;
- Instabilidade regulatória persistente e retrocessos em governança digital;
- Aumento de bloqueios portuários, interrupções logísticas e controles informais;
- Crescimento de violência contra executivos e trabalhadores essenciais;
- Investigações internacionais envolvendo cadeias produtivas;
- Infiltração crescente de grupos ilícitos em setores formais.

A intensificação desses sinais indica deterioração acelerada e possível transição para estados ainda mais caóticos.

2.3.8. Sinais de Transição do Cenário

O Cenário 2 tende a se agravar quando há colapso de instituições de justiça, retração de investimentos internacionais, expansão de crimes ambientais, proliferação de desinformação e aumento de violência organizada.

Se algumas capacidades institucionais forem parcialmente recuperadas ou se houver avanço isolado de governança digital, o cenário pode migrar para o Cenário 4.

Em contrapartida, caso eventos climáticos extremos se tornem predominantes, pode ocorrer transição para o Cenário 3.

2.3.9. Oportunidades Estratégicas

Mesmo em um ambiente adverso, algumas oportunidades emergem. Setores ligados a segurança física, cibersegurança, análise de dados, investigação corporativa, proteção executiva e soluções antifraude se fortalecem.

Empresas com governança sólida, excelência em *compliance* e forte cultura de integridade tornam-se mais valiosas.

Cadeias produtivas capazes de oferecer rastreabilidade, certificações robustas e padrões internacionais de ESG ganham vantagem competitiva, especialmente em mercados exigentes.

Organizações que investirem em inteligência contra ameaças, auditorias tecnológicas, proteção integrada e mecanismos avançados de *due diligence* serão capazes de operar com maior resiliência e posicionar-se de forma diferenciada mesmo em ambientes dominados por redes ilícitas.

2.4. Cenário 3 – Clima de Choques

2.4.1. Contexto e Fundamentos

O Cenário 3, Clima de Choques, emerge da combinação entre cooperação econômica moderada e fragilidades estruturais em infraestrutura, tecnologia e governança climática. A região experimenta avanços pontuais em integração comercial e logística, mas falha em criar padrões robustos de resiliência climática e digital. Com isso, choques ambientais e falhas tecnológicas ocorrem de maneira cada vez mais frequente e simultânea, produzindo pressões contínuas sobre setores produtivos, cadeias de suprimentos e serviços essenciais.

A instabilidade climática, traduzida em ondas de calor intensas, secas prolongadas, tempestades severas e enchentes recorrentes, interfere diretamente na produtividade agrícola, na segurança energética e na funcionalidade das cidades. Esses eventos interagem com sistemas tecnológicos frágeis, redes elétricas sobrecarregadas e infraestrutura insuficiente, multiplicando impactos e tornando o ambiente operacional imprevisível. Embora haja alguma cooperação regional, ela não se traduz em políticas ambientais estruturadas ou em investimentos suficientes em adaptação e mitigação.

2.4.2. Cadeia Causal Ampliada

A dinâmica do Cenário 3 se desenvolve por meio de cinco elementos interligados. Primeiro, eventos climáticos extremos aumentam em intensidade e frequência, gerando interrupções nos sistemas de energia, água e transporte.

Segundo, as falhas nessas infraestruturas críticas comprometem a continuidade das operações industriais, elevando custos, atrasos logísticos e perdas de produtividade.

Terceiro, a fragilidade tecnológica - especialmente em sistemas de supervisão, sensores e redes industriais conectadas - amplifica o impacto dessas interrupções.

Quarto, setores dependentes de energia, água e logística tornam-se vulneráveis a impactos simultâneos, criando ciclos de instabilidade multissetorial.

Quinto, a falta de políticas públicas consistentes de adaptação climática impede a rápida recuperação, perpetuando vulnerabilidades e forçando empresas a internalizar custos de resiliência.

2.4.3. Fontes de Risco Predominantes no Cenário

Três fontes de risco se destacam. A primeira é a instabilidade climática, que atua como um multiplicador de riscos e afeta diretamente cadeias produtivas, infraestruturas e comunidades.

A segunda é a fragilidade das infraestruturas críticas, especialmente sistemas elétricos, redes de transporte, saneamento e telecomunicações.

A terceira é a vulnerabilidade tecnológica, que inclui sensores expostos a altas temperaturas, ICS sensíveis a flutuações elétricas, falhas em conectividade e limites na capacidade de previsão e resposta.

Essas fontes de risco se combinam, criando ambientes altamente voláteis e sensíveis a choques externos.

2.4.4. Implicações Setoriais Diretas

No setor energético, secas prolongadas e instabilidade hídrica aumentam a dependência de termelétricas, elevando custos e emissões. Interrupções tornam-se recorrentes.

No agronegócio, a irregularidade climática reduz produtividade, altera calendários de plantio e afeta qualidade de solos.

No setor industrial, flutuações de energia e falhas de sensores prejudicam operações contínuas.

Na logística, rodovias, ferrovias e portos são interrompidos com frequência devido a enchentes, incêndios ou intempéries.

Na mineração, enchentes, colapsos estruturais e conflitos socioambientais tornam operações mais complexas.

No setor urbano, crises de água e calor extremo ampliam riscos sanitários e pressões sobre infraestrutura urbana.

Todos os setores enfrentam volatilidade operacional e aumento de custos com resiliência.

2.4.5. Impactos na Segurança Corporativa (Física, Cibernética e Reputacional)

A segurança corporativa nesse cenário é pressionada por eventos ambientais extremos que provocam deslocamentos populacionais, conflitos territoriais e aumento de crimes oportunistas em áreas severamente afetadas.

A segurança física precisa lidar com evacuações, riscos de integridade para equipes de campo e proteção de ativos expostos a incêndios, inundações ou deslizamentos.

A segurança cibernética enfrenta desafios decorrentes de instabilidade elétrica, falhas de conectividade e aumento de ataques que exploram momentos de desorganização operacional.

Ataques à cadeia de suprimentos digital tornam-se mais frequentes, com aproveitamento da vulnerabilidade momentânea das organizações durante eventos climáticos severos.

O risco reputacional aumenta em setores associados a impactos ambientais ou à falha em responder adequadamente a crises, elevando demandas por transparência, responsabilidade socioambiental e comunicação eficaz.

2.4.6. Impactos na Governança e na Continuidade de Negócios

A governança corporativa precisa incorporar métricas avançadas de adaptação climática, impacto socioambiental e gestão de crises.

Planos de continuidade tornam-se mais complexos, exigindo redundâncias energéticas, estratégias de diversificação hídrica e mecanismos de resposta rápida baseados em monitoramento preditivo.

Empresas precisam integrar dados climáticos em tempo real com modelos de análise preditiva, combinando previsão meteorológica avançada com Inteligência Artificial para detectar anomalias e antecipar impactos.

A continuidade de negócios passa a depender de redundâncias estruturais e energéticas, parcerias regionais e diversificação logística.

Empresas que não investem em resiliência climática enfrentam interrupções prolongadas e perda de competitividade.

2.4.7. Indicadores Específicos de Alerta Precoce (EWI)

Sinais antecipatórios essenciais incluem:

- Aumento da frequência e severidade de eventos climáticos extremos;
- Declínio prolongado de níveis de reservatórios e aquíferos;
- Interrupções elétricas recorrentes e sobrecarga de redes;
- Falhas simultâneas em sensores, ICS e redes industriais;
- Aumento de perdas operacionais em cadeias logísticas;
- Crescimento de custos com seguros e indenizações;
- Expansão de conflitos por água ou energia;
- Instabilidade de preços de commodities sensíveis ao clima.

A persistência desses indicadores reforça a transição para ciclos de choque contínuo.

2.4.8. Sinais de Transição do Cenário

O Cenário 3 pode migrar rapidamente para o Cenário 2 se eventos extremos forem explorados por redes ilícitas, ampliando a criminalidade em regiões afetadas.

Pode transitar para o Cenário 4 caso o setor privado avance significativamente em resiliência tecnológica, enquanto o Estado permaneça incapaz de modernizar sua infraestrutura ambiental.

Pode aproximar-se do Cenário 1 caso investimentos robustos em adaptação climática e infraestrutura verde se consolidem regionalmente.

2.4.9. Oportunidades Estratégicas

Mesmo em um ambiente adverso, surgem oportunidades importantes. A inovação em gestão hídrica, infraestrutura verde, energia renovável e agricultura resiliente ganha tração.

Tecnologias de previsão ambiental, análise preditiva e Inteligência Artificial aplicada ao clima tornam-se altamente valorizadas.

Modelos de seguro paramétrico, créditos de resiliência e fundos climáticos se expandem.

Empresas com capacidade de desenvolver cadeias sustentáveis, comunicação de risco transparente e ações robustas de adaptação conquistarão mercados e reputação.

Organizações que priorizarem resiliência ambiental e integração tecnológica estarão mais bem posicionadas para enfrentar o Clima de Choques e mitigar rupturas repetitivas.

2.5. Cenário 4 – Dados com Travas, Fronteiras Abertas

2.5.1. Contexto e Fundamentos

O Cenário 4, denominado Dados com Travas, Fronteiras Abertas, descreve um ambiente caracterizado por maturidade tecnológica elevada no setor privado e instabilidade persistente nas instituições públicas. Trata-se de um futuro no qual a capacidade empresarial de inovar, proteger dados e operar com padrões avançados de segurança supera amplamente a capacidade dos Estados de regulamentar, fiscalizar e prover serviços críticos. A região experimenta um descompasso entre a força das empresas em tecnologia e a fragilidade dos governos em assegurar estabilidade política, jurídica e institucional.

Nesse cenário, a governança de Inteligência Artificial e proteção de dados avança de forma desigual. Grandes organizações se tornam referência em auditoria algorítmica, explicabilidade de modelos e cibersegurança de alto nível, enquanto o Estado se mostra incapaz de acompanhar o ritmo tecnológico ou de padronizar exigências regulatórias. Como resultado, o ambiente apresenta alta assimetria de proteção, na qual ambientes corporativos são significativamente mais seguros do que o entorno institucional e social que os envolve.

2.5.2. Cadeia Causal Ampliada

A dinâmica do Cenário 4 emerge da combinação de cinco fatores principais. Primeiro, o setor privado avança rapidamente em digitalização, Inteligência Artificial, automação e segurança convergente, adotando padrões elevados como ICS 5 e centros integrados de monitoramento.

Segundo a instabilidade institucional impede que governos criem marcos legais consistentes, atualizados e aplicáveis regionalmente, gerando ambientes regulatórios fragmentados.

Terceiro, essa fragmentação estimula empresas a internalizar mecanismos de governança, criando normas privadas que se tornam referência para fornecedores e parceiros.

Quarto, a desigualdade tecnológica aumenta e cadeias produtivas menos capitalizadas permanecem vulneráveis a ataques, fraudes e interrupções.

Quinto, a ausência de políticas públicas robustas amplia tensões sociais e territoriais, criando zonas de volatilidade que convivem com áreas altamente protegidas controladas por organizações privadas.

2.5.3. Fontes de Risco Predominantes no Cenário

Três fontes de risco se destacam. A primeira é a instabilidade institucional, marcada por mudanças abruptas de orientação política, volatilidade regulatória e dificuldade de execução estatal.

A segunda é a desigualdade tecnológica, que cria ecossistemas híbridos com empresas altamente protegidas e ambientes públicos frágeis.

A terceira é o risco cibernético avançado, alimentado por ataques de automação, exploração de vulnerabilidades e uso indevido de Inteligência Artificial por agentes oportunistas.

Essas fontes de risco se combinam e reforçam a assimetria entre setores resilientes e setores expostos.

2.5.4. Implicações Setoriais Diretas

No setor de tecnologia e serviços financeiros, a inovação avança rapidamente graças a ecossistemas corporativos altamente protegidos.

No setor industrial, empresas com maturidade OT avançada conseguem operar com estabilidade, enquanto pequenas e médias indústrias sofrem interrupções frequentes.

Na logística, cadeias integradas por grandes operadores são resilientes, mas regiões dependentes de infraestrutura pública enfrentam falhas recorrentes.

No setor de energia, empresas privadas adotam microgeração, redes inteligentes, redundâncias e sistemas preditivos, enquanto a infraestrutura pública permanece vulnerável a falhas e ataques.

No varejo e serviços urbanos, a desigualdade digital cria ambientes de hiper proteção corporativa e vulnerabilidade comunitária simultânea.

Essa dinâmica amplia a distância entre setores com alta capacidade de investimento e setores que dependem da estabilidade institucional.

2.5.5. Impactos na Segurança Corporativa (Física, Cibernética e Reputacional)

A segurança corporativa assume papel central nesse cenário. A segurança física é reforçada por sistemas de videomonitoramento inteligente, controle avançado de acessos, perímetros reforçados e integração com sistemas digitais de detecção. Empresas se tornam ambientes altamente protegidos, funcionando como ilhas de estabilidade.

A segurança cibernética opera com estruturas sofisticadas de prevenção e resposta, integrando *machine learning*, análise comportamental e controles segmentados de redes críticas.

A segurança reputacional passa a depender da capacidade das organizações de demonstrar governança transparente, padrões éticos de Inteligência Artificial e práticas consistentes de proteção de dados.

Empresas tornam-se agentes de proteção central diante da fragilidade do aparato estatal.

2.5.6. Impactos na Governança e na Continuidade de Negócios

A governança corporativa precisa internalizar funções que, em ambientes mais estáveis, seriam desempenhadas pelo Estado.

Com isso, empresas definem suas próprias normas de conformidade, padrões de auditoria, critérios de proteção de dados, protocolos de cibersegurança e mecanismos de integridade digital.

Planos de continuidade incluem redundâncias energéticas, redes privadas de telecomunicações, centros de resposta distribuídos e sistemas avançados de recuperação.

Organizações precisam antecipar volatilidades regulatórias, mudanças de governo, restrições setoriais e impactos sociais relacionados à desigualdade de infraestrutura pública.

A resiliência é construída internamente e suplementada por parcerias estratégicas entre empresas.

2.5.7. Indicadores Específicos de Alerta Precoce (EWI)

Alguns sinais antecipatórios relevantes incluem:

- Retrocessos em marcos regulatórios de proteção de dados ou Inteligência Artificial;
- Aumento de ataques cibernéticos sofisticados contra empresas de médio porte;
- Crescimento da diferença entre ambientes corporativos protegidos e ambientes públicos vulneráveis;
- Uso crescente de normas privadas como referência regulatória;
- Instabilidade política persistente ou polarização ampliada;
- Interrupções repetidas em infraestruturas públicas essenciais;
- Aumento da dependência empresarial de serviços privados de energia e telecomunicações.

Esses sinais ajudam a antecipar intensificação das assimetrias desse cenário.

2.5.8. Sinais de Transição do Cenário

O Cenário 4 pode evoluir para o Cenário 1 se a cooperação institucional aumentar e marcos regulatórios avançarem.

Também pode se aproximar do Cenário 2 se, redes ilícitas explorarem fragilidades institucionais e ampliarem a captura de setores públicos.

Caso eventos climáticos se tornem mais intensos e frequentes, o cenário pode deslizar parcialmente para o Cenário 3.

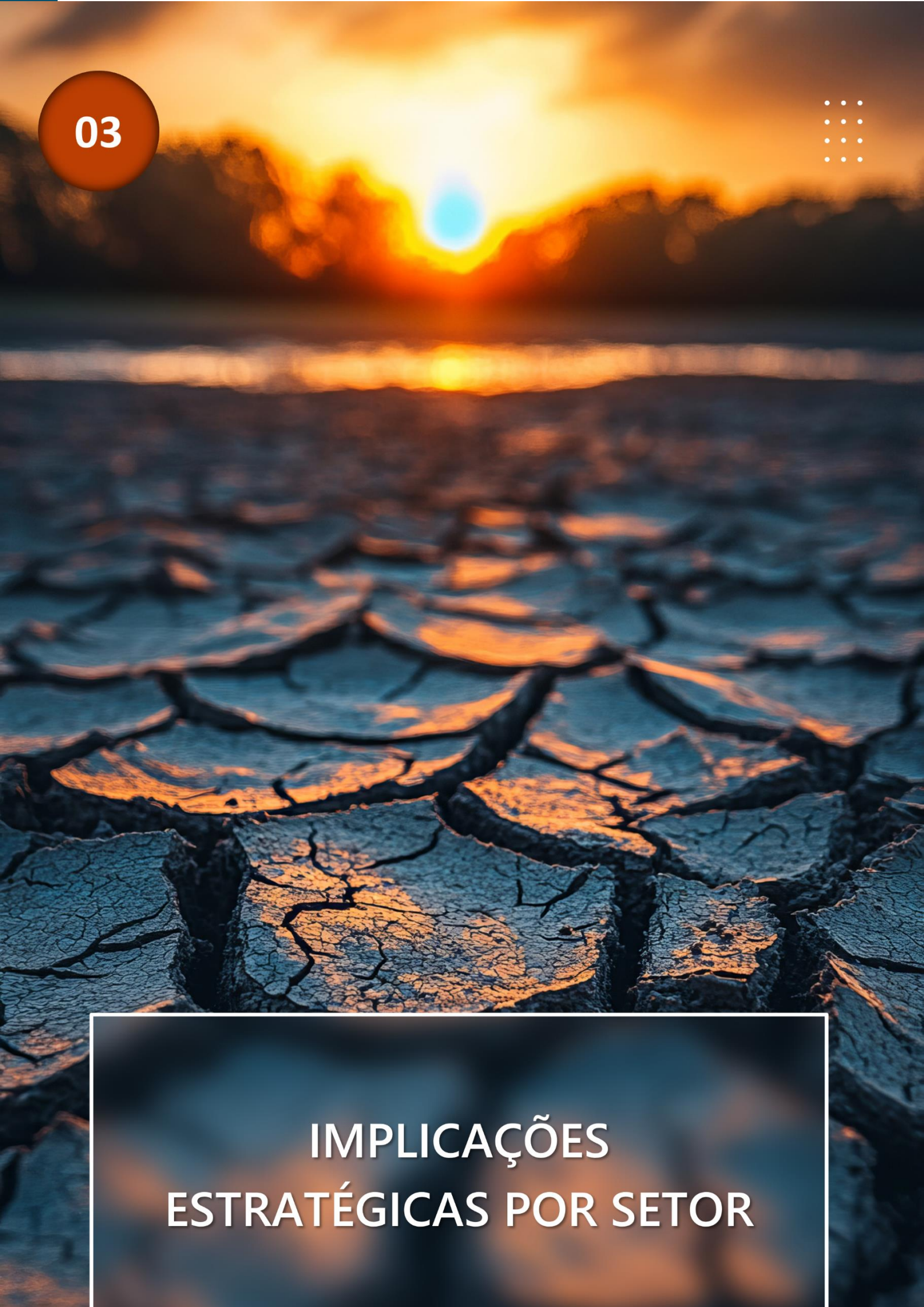
2.5.9. Oportunidades Estratégicas

O cenário apresenta importantes oportunidades empresariais. Tecnologias avançadas de cibersegurança, proteção de dados, automação defensiva, integração OT IT, Inteligência Artificial explicável e auditoria algorítmica se tornam extremamente valorizadas.

Soluções de energia distribuída, infraestrutura privada, redes independentes e centros de monitoramento convergente ampliam competitividade.

Empresas com governança sólida e padrões avançados de resiliência se tornam polos de confiança regional, atraindo investimentos e parcerias.

Mesmo em um ambiente institucional frágil, a inovação tecnológica permite o surgimento de ecossistemas privados altamente resilientes e competitivos.



03

IMPLICAÇÕES ESTRATÉGICAS POR SETOR

3.1. Introdução

A análise setorial que compõe o Capítulo 3 apresenta as implicações práticas dos cenários prospectivos para os principais setores econômicos da América Latina, com especial atenção ao contexto brasileiro. Enquanto os capítulos anteriores identificaram fontes de risco estruturantes, incertezas críticas e cenários abrangentes para 2026 e além, esta etapa tem como objetivo traduzir essas dinâmicas em impactos diretos sobre cadeias produtivas, regulações, infraestruturas, operações corporativas e mercados específicos.

A América Latina, apesar de compartilhar tendências globais como digitalização acelerada, pressão climática crescente e complexificação do ambiente de segurança, apresenta características próprias que amplificam ou redirecionam a forma como riscos se materializam em cada setor. A combinação entre fragilidade institucional, desigualdades estruturais, dependência de *commodities*, heterogeneidade regulatória e exposição a redes ilícitas produz um mosaico de vulnerabilidades e oportunidades que não são uniformes em relação ao cenário global. O Brasil, por sua vez, por sua dimensão econômica, energética e territorial, exerce papel determinante na configuração dessas dinâmicas regionais e na evolução das cadeias produtivas continentais.

A lógica deste capítulo é aprofundar, setor por setor, como as fontes de risco identificadas nos itens 1.3. e 1.4. e como as combinações prospectivas dos cenários do item 1.5. moldam a tomada de decisão no curto e médio prazo. A abordagem privilegia uma leitura operacional e comparativa, destacando não apenas riscos e fragilidades, mas também as oportunidades estratégicas que emergem mesmo em contextos adversos. A análise incorpora elementos de tecnologia, clima, governança, integridade, crime organizado, dinâmica geopolítica, maturidade de Inteligência Artificial, continuidade de negócios e resiliência de infraestruturas, sempre com foco no que é mais relevante para cada setor.

Outro aspecto central deste capítulo é a comparação sistemática com outras regiões do mundo, em especial Estados Unidos, União Europeia e Ásia. Essa comparação permite dimensionar a posição relativa da América Latina frente a ambientes que possuem níveis mais altos ou mais baixos de governança tecnológica, maturidade institucional, resiliência climática e segurança de infraestrutura. Esse contraste é fundamental para compreender onde estão as assimetrias e onde surgem oportunidades de convergência ou de diferenciação competitiva.

Cada subseção do capítulo segue uma estrutura uniforme para facilitar a análise comparada entre setores. Cada setor será examinado segundo cinco dimensões principais: riscos predominantes, impactos climáticos e tecnológicos, implicações

específicas para a América Latina e Brasil, comparação com as principais regiões do mundo e oportunidades estratégicas decorrentes desses movimentos. Em seguida, é apresentada uma tabela de síntese que destaca os pontos centrais da análise e permite uma visualização consolidada das tensões e vetores estratégicos daquele setor.

Com essa abordagem, a Seção 3.0 estabelece o ponto de partida para uma leitura setorial que conecta os cenários prospectivos aos desafios e oportunidades de cada cadeia econômica. A intenção é oferecer um quadro analítico sólido que permita a tomada de decisão baseada em evidências, a antecipação de rupturas e a formulação de estratégias de resiliência alinhadas às transformações estruturais da região.

3.2. Setor Industrial e Manufatura

3.2.1. Riscos Predominantes

O setor industrial e de manufatura enfrenta um conjunto de riscos estruturais que se intensificam em 2026 e além, impulsionados por fatores climáticos, tecnológicos, logísticos e geopolíticos. Entre os riscos mais relevantes estão interrupções na cadeia de suprimentos, flutuações no fornecimento de energia, ataques cibernéticos direcionados a sistemas industriais, competição global assimétrica, alta dependência de insumos críticos e vulnerabilidades decorrentes da integração entre tecnologia operacional e tecnologia da informação.

No contexto latino-americano, esses riscos assumem contornos específicos devido à maior dependência de commodities, à fragilidade de infraestruturas críticas, à menor padronização tecnológica e à maturidade irregular de governança digital entre países. No Brasil, fatores como volatilidade tributária, custos logísticos elevados e exposição climática acentuam desafios que influenciam diretamente a competitividade da indústria.

As tensões geopolíticas globais, a disputa por minerais estratégicos e os gargalos logísticos persistentes aumentam a pressão sobre o setor, exigindo maior capacidade de adaptação e de antecipação de riscos. Ao mesmo tempo, a proliferação de fraudes, sabotagens corporativas e ataques a sistemas industriais exige níveis crescentes de segurança convergente.

3.2.2. Impactos Climáticos, Tecnológicos e Operacionais

Os impactos climáticos tornam-se cada vez mais determinantes para o setor industrial. Ondas de calor extremo afetam a produtividade de trabalhadores, reduzem a vida útil de componentes industriais e provocam falhas em sistemas de refrigeração. Secas prolongadas comprometem operações que dependem de água para processos industriais, como metalurgia, papel e celulose, bebidas e indústrias químicas. Eventos extremos aumentam o risco de interrupção energética, criando instabilidade em linhas de produção sensíveis a variações elétricas.

A dimensão tecnológica apresenta impactos igualmente significativos. A aceleração da digitalização e da automação aumenta a eficiência, mas expõe sistemas industriais a riscos cibernéticos sofisticados. Ataques a Sistemas de Controle Industrial (ICS) podem provocar paralisações críticas, danos a equipamentos, alterações indetectáveis em parâmetros operacionais e riscos de segurança para trabalhadores. Vulnerabilidades em sensores, redes industriais e sistemas de telemetria elevam a probabilidade de eventos simultâneos entre falhas digitais e físicas.

Do ponto de vista operacional, gargalos logísticos, oscilações no preço de insumos e a dependência de cadeias longas aumentam a volatilidade de custos. A adoção de tecnologias avançadas de manufatura depende de estabilidade energética, maturidade digital e capacidade de investimento que variam significativamente entre países latino-americanos. Esses fatores definem um cenário de competitividade desigual, no qual empresas de maior porte avançam enquanto pequenas e médias enfrentam dificuldades para acompanhar o ritmo tecnológico.

3.2.3. Implicações Específicas para Brasil e América Latina

A América Latina apresenta um conjunto de vulnerabilidades estruturais que amplificam riscos para o setor industrial, especialmente em comparação ao cenário global. A região depende fortemente de infraestrutura logística e energética limitada, com exposição significativa a eventos climáticos extremos e variações hídricas. Esse contexto afeta diretamente a produtividade industrial, cria incertezas operacionais e reduz a previsibilidade de investimentos.

No Brasil, embora exista uma base industrial diversificada, desafios como volatilidade regulatória, complexidade tributária, infraestrutura deficiente e risco climático elevado criam obstáculos adicionais. A dependência da matriz hidrelétrica torna o país especialmente vulnerável às secas, e a crescente urbanização pressiona sistemas de

água, energia e mobilidade. A exposição a redes ilícitas, fraudes, conflitos territoriais e pressões ambientais também interfere em cadeias produtivas estratégicas.

A baixa padronização digital entre empresas e setores dificulta a adoção de tecnologias de manufatura avançada e amplia a desigualdade de maturidade tecnológica entre grandes indústrias e pequenas fábricas. A ausência de uma política industrial regional coordenada reduz sinergias e limita ganhos de escala que são essenciais para competir com economias maduras.

Ao mesmo tempo, a América Latina possui vantagens competitivas, como abundância de recursos naturais, potencial energético renovável, capacidade logística transcontinental e proximidade geográfica com grandes mercados. Essas oportunidades, porém, exigem investimentos estruturais para serem convertidas em resiliência e competitividade.

3.2.4. Comparação com Estados Unidos, União Europeia e Ásia

Em relação aos Estados Unidos, a América Latina apresenta defasagens relevantes em infraestrutura logística, automação industrial, resiliência energética e segurança OT IT. Enquanto o mercado norte americano opera com maturidade elevada em automação avançada, redes industriais inteligentes e integração com IA defensiva, países latino-americanos ainda enfrentam instabilidades básicas de fornecimento e conectividade.

Em comparação com a União Europeia, a lacuna reside principalmente na governança climática, na regulação tecnológica e na integração regional. A Europa avança rapidamente em normas robustas de proteção de dados, auditoria algorítmica, segurança industrial e padrões ambientais rigorosos. A América Latina, por outro lado, avançou de forma desigual na adoção desses marcos, criando ambientes regulatórios fragmentados e imprevisíveis.

Em relação à Ásia, a competitividade latino-americana é prejudicada pela menor eficiência logística, pela falta de *clusters* industriais integrados e pela baixa maturidade tecnológica em pequenas e médias indústrias. A Ásia opera com cadeias produtivas diversificadas, centros de manufatura distribuídos e capacidade tecnológica elevada. A falta de infraestrutura adequada na América Latina limita a expansão de cadeias produtivas globais na região.

Apesar dessas diferenças, a América Latina possui vantagens relevantes no contexto global: proximidade com fontes de energia renovável, disponibilidade de materiais estratégicos, espaço para expansão industrial sustentável e oportunidade de

desenvolver *clusters* industriais avançados com foco em tecnologias verdes, bioeconomia e cadeias produtivas digitais.

3.2.5. Oportunidades Estratégicas

Mesmo diante de desafios estruturais significativos, o setor industrial da América Latina possui oportunidades estratégicas importantes para se reposicionar com maior competitividade global. Investimentos em automação defensiva, Inteligência Artificial explicável, manufatura avançada, integração OT IT e resiliência climática podem elevar a qualidade e eficiência das cadeias produtivas regionais.

O fortalecimento de normas industriais harmonizadas entre países latino-americanos amplia previsibilidade e facilita integração regional. A modernização de sistemas energéticos com fontes renováveis e redes inteligentes aumenta a segurança operacional e reduz custos. A criação de corredores logísticos resilientes, parques industriais sustentáveis e ecossistemas de inovação se torna essencial para atrair investimentos de longo prazo.

No Brasil, políticas industriais voltadas para descarbonização, produtividade, infraestrutura crítica e transição energética podem posicionar o país como referência continental. Tecnologias de previsão ambiental, sensores avançados, sistemas de monitoramento e ferramentas de análise preditiva têm potencial para transformar vulnerabilidades climáticas em vantagem competitiva.

Indústrias que adotarem padrões elevados de resiliência, segurança convergente e governança tecnológica estarão mais bem preparadas para enfrentar rupturas e capturar valor em mercados globais que exigem transparência, integridade e sustentabilidade.

Tabela 4 – Síntese: Setor Industrial e Manufatura

Dimensão	Brasil e América Latina	Estados Unidos	União Europeia	Ásia
Infraestrutura logística	Limitada, com gargalos significativos	Alta integração nacional	Alta padronização e eficiência	Elevada capacidade, clusters consolidados
Maturidade OT / IT	Baixa a média, com desigualdades setoriais	Alta, com integração avançada	Alta, com governança forte	Muito alta, especialmente na manufatura

Dimensão	Brasil e América Latina	Estados Unidos	União Europeia	Ásia
Exposição climática	Alta, com secas, enchentes e ondas de calor	Média	Média a alta, porém com melhor adaptação	Alta em alguns países, moderada em outros
Governança tecnológica	Heterogênea e fragmentada	Madura e consolidada	Rígida e harmonizada	Variável, mas avançada em grandes economias
Segurança industrial	Vulnerável a ataques e falhas estruturais	Alta proteção, ICS desenvolvidos	Padrões fortes de segurança	Cibersegurança e proteção digital robusta
Oportunidades	Energia renovável, automação defensiva, clusters verdes	Inovação acelerada	Transição verde, integração regulatória	Cadeias produtivas globais

3.3. Energia, Infraestruturas Críticas e Utilities

3.3.1. Vulnerabilidades Estruturais

O setor de energia e de infraestruturas críticas concentra alguns dos riscos mais significativos para a estabilidade econômica e social da América Latina. A região apresenta heterogeneidade na qualidade das redes elétricas, forte dependência hídrica, baixa redundância estrutural, elevada exposição a eventos climáticos extremos e maturidade desigual em proteção de Sistemas de Controle Industrial. Esse conjunto de características produz um ambiente no qual falhas pontuais podem provocar interrupções de grande escala, afetando indústrias, hospitais, sistemas de transporte, telecomunicações e serviços essenciais.

No Brasil, a dependência da matriz hidrelétrica torna o setor particularmente sensível a ciclos de seca, à irregularidade das chuvas e ao esgotamento de reservatórios. A expansão de fontes renováveis ocorre em ritmo acelerado, mas ainda com limitações de integração plena ao sistema energético. A fragilidade de infraestruturas antigas, a falta de investimentos contínuos e a dificuldade de modernização de redes de transmissão criam riscos de interrupções sistêmicas.

Além disso, o setor enfrenta vulnerabilidades estruturais relacionadas a pressões criminais. Sabotagens, vandalismo, furtos de cabos, interferências em subestações e infiltração de redes ilícitas em contratos públicos ampliam riscos e elevam custos

operacionais. A convergência entre crime organizado, eventos climáticos e fragilidade tecnológica torna a segurança de infraestruturas críticas um desafio central.

3.3.2. Pressões Climáticas e Digitais

Eventos climáticos extremos exercem impacto progressivamente mais severo sobre o setor de energia. Secas prolongadas reduzem a capacidade das hidrelétricas, exigindo acionamento emergencial de termelétricas e pressão sobre tarifas. Enchentes e tempestades danificam torres de transmissão, isolam comunidades e comprometem a distribuição. Ondas de calor provocam picos de consumo que sobrecarregam redes que já operam acima de padrões internacionais de eficiência.

Do ponto de vista digital, o setor enfrenta riscos crescentes associados a ataques cibernéticos e manipulação de sistemas críticos. Sistemas Supervisórios e de Controle Industrial são alvos frequentes de agentes maliciosos que buscam causar interrupções, sequestrar dados, alterar parâmetros de geração e transmissão ou comprometer sistemas de telemetria. Falhas coordenadas podem afetar simultaneamente setores interdependentes, como saneamento, telecomunicações e transporte.

A convergência entre falhas digitais e eventos climáticos intensifica a probabilidade de colapso operacional. Um ataque cibernético durante uma crise hídrica, por exemplo, pode levar à interrupção prolongada de energia, afetando hospitais, redes de refrigeração, serviços emergenciais e operações industriais críticas. Esse tipo de risco híbrido se tornou mais frequente e demanda novas abordagens de proteção.

3.3.3. Desafios para Brasil e América Latina

A América Latina enfrenta desafios estruturais que tornam o setor de energia um dos mais vulneráveis da região. A alta dependência hídrica em países como Brasil, Colômbia e Peru amplifica riscos operacionais diante de variações climáticas. A falta de redes inteligentes, a baixa digitalização de campo, a ausência de redundâncias e a deficiente capacidade de armazenamento reduzem a resiliência do sistema elétrico.

No Brasil, desafios adicionais incluem redes envelhecidas, disputas regulatórias, vulnerabilidades em contratos de concessão, exposição a fraudes e logística limitada para expansão de geração renovável. A dependência de combustíveis fósseis em períodos de crise hídrica amplia custos e pressiona metas de descarbonização.

A desintegração regional em termos regulatórios complica a possibilidade de integração energética plena entre países latino-americanos. Projetos de interconexão avançam lentamente devido à instabilidade política, dificuldades fiscais e riscos de captura regulatória. Esse cenário reduz oportunidades de troca energética e amplia vulnerabilidades locais.

3.3.4. Comparação Global

Em comparação aos Estados Unidos, a América Latina apresenta redes elétricas menos redundantes, menor capacidade de armazenamento de energia e cobertura limitada de redes inteligentes. Os Estados Unidos possuem maior robustez regulatória, capacidade de resposta rápida e melhor integração entre energia, telecomunicações e segurança digital.

Em relação à União Europeia, a defasagem é ainda maior. A Europa investiu fortemente em governança climática, transição energética e resiliência de Redes Inteligentes, com integração regional avançada e capacidade significativa de interconexão transfronteiriça. A América Latina, por sua vez, opera com estruturas desconectadas e ampla variação de maturidade entre países.

Quando comparada à Ásia, a América Latina enfrenta dois desafios principais: menor escala industrial e menor capacidade de investimento público e privado em infraestrutura crítica. Países como China, Coreia do Sul e Japão possuem sistemas altamente digitalizados e integrados, com forte presença de Inteligência Artificial para monitoramento preditivo. A América Latina ainda opera com alto grau de manutenção corretiva e vulnerabilidade climática.

3.3.5. Oportunidades

Apesar das fragilidades, a região apresenta oportunidades estratégicas relevantes. A expansão de energia renovável, especialmente solar, eólica, biomassa e hidrogênio verde, posiciona a América Latina como uma das regiões com maior potencial de transição energética no mundo. O Brasil e o Chile destacam-se como protagonistas naturais nesse movimento.

O setor possui oportunidade de avançar na implementação de redes inteligentes, sistemas avançados de monitoramento e controle, sensores distribuídos, automação defensiva e redundâncias estruturais. Tecnologias emergentes de armazenamento,

previsão climática baseada em Inteligência Artificial, integração OT IT e expansão de geração distribuída podem elevar significativamente a resiliência do sistema.

A criação de corredores energéticos regionais, além da modernização de subestações, monitoramento das linhas de transmissão e fortalecimento da segurança física e digital, pode gerar vantagens competitivas e permitir integração estratégica com mercados globais interessados em energia de baixo carbono.

Tabela 5 – Síntese: Energia e Infraestruturas Críticas

Dimensão	Brasil e América Latina	Estados Unidos	União Europeia	Ásia
Matriz energética	Predominância hídrica e renovável, porém, vulnerável	Diversificada e resiliente	Alta integração renovável	Forte expansão renovável
Digitalização	Baixa a média	Alta	Muito alta	Avançada
Redundância elétrica	Limitada	Alta	Alta	Média a alta
Exposição climática	Muito alta	Média	Média	Variável
Segurança digital	Vulnerável	Robusta	Padronizada	Avançada
Oportunidades	Renováveis, redes inteligentes, IA climática	Inovação, hidrogênio	Transição verde	Industrialização e digitalização

3.4. Agronegócio e Alimentos

Na América Latina, o agronegócio e a biotecnologia constituem uma extensão da infraestrutura crítica nacional. Laboratórios de sementes, centros de genética, estações de pesquisa, biofábricas e ensaios de campo integram cadeias altamente sensíveis a espionagem industrial, sabotagem, ativismo violento e biocrimes. Esses ativos, por influenciarem segurança alimentar, competitividade global e soberania tecnológica, ampliam a superfície crítica de risco e exigem abordagens de segurança convergente e protocolos específicos de proteção.

3.4.1. Riscos Climáticos e Logísticos

O agronegócio latino-americano é um dos setores mais expostos às transformações estruturais que moldam o ambiente global em 2026 e além. A região, responsável por parte expressiva do fornecimento mundial de grãos, proteínas, fibras e alimentos

processados, enfrenta riscos crescentes relacionados à variabilidade climática, à escassez de água, à intensificação de eventos extremos e a pressões regulatórias internacionais sobre desmatamento, rastreabilidade e sustentabilidade.

Os riscos climáticos dominam o setor. Secas prolongadas, enchentes inesperadas, variações bruscas de temperatura e irregularidade dos ciclos de chuva afetam plantios, produtividade, qualidade do solo e disponibilidade de água. Estiagens intensas comprometem culturas sensíveis, elevam custos com irrigação e pressionam reservatórios, enquanto tempestades severas provocam erosão, perdem safras e afetam silos e depósitos. Esse cenário se agravará em 2026 e além, exigindo adaptações estruturantes em toda a cadeia produtiva.

A dimensão logística também enfrenta pressões significativas. Portos saturados, estradas vulneráveis a deslizamentos, pontes frágeis, interrupções ferroviárias e capacidade limitada de armazenamento criam gargalos operacionais que ampliam custos e reduzem eficiência. Esses impactos se intensificam durante eventos climáticos severos, quando estradas se tornam intransitáveis e portos enfrentam paralisações. A dependência de rotas únicas em países como o Brasil aumenta a probabilidade de rupturas simultâneas.

3.4.2. Pressões Tecnológicas e de Mercado

A aceleração da digitalização e da automação no agronegócio transforma profundamente o setor, mas também cria novos riscos e desigualdades de capacidade tecnológica. Empresas com acesso a tecnologias avançadas conseguem operar com maior previsibilidade, enquanto pequenos e médios produtores permanecem vulneráveis a falhas climáticas, volatilidade de preços e riscos digitais.

O uso de sensores, telemetria, monitoramento por satélite, drones e análises avançadas baseadas em Inteligência Artificial torna-se essencial para prever rendimento, detectar pragas, estimar produtividade e antecipar riscos. Contudo, a desigualdade tecnológica entre grandes conglomerados e produtores menores cria assimetrias competitivas e limita a adoção de práticas de agricultura de precisão.

A pressão internacional por padrões ambientais rígidos também se intensifica. Europa e Ásia avançam em exigências de rastreabilidade, comprovação de origem sustentável, certificações ambientais e redução de emissões em toda a cadeia. Essas exigências podem funcionar como barreiras não tarifárias para parte significativa da produção latino-americana, especialmente em países onde o desmatamento ilegal e a fragilidade da fiscalização ambiental permanecem como desafios estruturais.

3.4.3. Implicações Regionais

A América Latina, por ser uma potência agroalimentar global, enfrenta implicações econômicas, ambientais e institucionais de grande magnitude. A região possui vantagens naturais como terras férteis, clima tropical, disponibilidade de água e alta produtividade relativa, mas essas vantagens são comprometidas por vulnerabilidades relacionadas a clima, infraestrutura e governança ambiental.

No Brasil, o agronegócio é responsável por parcela significativa do PIB, das exportações e do emprego rural. Portanto, interrupções climáticas, exigências regulatórias internacionais ou falhas logísticas têm impacto direto sobre a economia nacional. A pressão por rastreabilidade da cadeia bovina, controle de desmatamento e comprovação de conformidade ESG, já produz efeitos tangíveis e deve se intensificar nos próximos anos.

A essas pressões externas soma-se a insegurança jurídica, que permanece um vetor crítico de vulnerabilidade para o agronegócio latino-americano. Mudanças abruptas em marcos regulatórios, disputas tributárias, judicialização recorrente e assimetrias normativas entre países reduzem previsibilidade, ampliam custos de conformidade e afetam decisões de investimento de longo prazo. Esses fatores comprometem a competitividade regional, criam barreiras adicionais ao acesso a mercados e tornam a governança jurídica um elemento central da resiliência do setor.

O crime organizado também está cada vez mais presente no setor. Redes ilícitas atuam em áreas rurais, controlando territórios, garimpos ilegais, rotas de transporte e áreas de armazenamento. Isso cria riscos físicos e reputacionais para empresas e produtores, além de ampliar a probabilidade de contaminação da cadeia por atividades ilegais.

A escassez hídrica emergente em regiões produtivas da Argentina, Brasil, Paraguai e México aumenta tensões territoriais e demanda investimentos urgentes em irrigação sustentável, captação de água, manejo integrado de bacias e tecnologias de reuso.

3.4.4. Comparação com Principais Mercados Globais

A América Latina enfrenta distorções importantes em comparação aos principais mercados agrícolas globais.

Em relação aos Estados Unidos, a região apresenta menor resiliência climática, menor integração logística e maturidade tecnológica inferior. Os Estados Unidos possuem

redes logísticas altamente integradas, sistemas avançados de irrigação, governança climática robusta e estabilidade regulatória ampla.

Comparando com a União Europeia, a maior diferença está na governança ambiental. A Europa possui mecanismos avançados de certificação, rastreabilidade e controle de emissões, o que lhe permite ocupar posição de referência global em padrões de sustentabilidade. A América Latina ainda enfrenta dificuldade para harmonizar práticas e reduzir impactos socioambientais.

Em relação à Ásia, especialmente China e Índia, a diferença é menos tecnológica e mais estrutural. A Ásia opera com forte integração entre produção, processamento e distribuição, além de grande investimento em agricultura de precisão. A América Latina possui produtividade elevada, mas separada por grandes distâncias e dependente de infraestrutura logística limitada.

Apesar dessas diferenças, a América Latina possui vantagem competitiva significativa em escala produtiva, potencial hídrico e capacidade de expansão sustentável, desde que invista em modernização logística, redução de desmatamento e governança ambiental avançada.

3.4.5. Oportunidades Estratégicas

O setor apresenta oportunidades que podem transformar vulnerabilidades em vantagem competitiva. A expansão da agricultura de precisão, o uso intensivo de Inteligência Artificial para previsão de eventos climáticos e otimização de produtividade e a adoção de sistemas avançados de monitoramento ambiental são essenciais para elevar resiliência e competitividade.

Investimentos em infraestrutura logística, irrigação sustentável, silos climatizados e redes ferroviárias podem reduzir custos e aumentar previsibilidade. O desenvolvimento de cadeias completas de bioeconomia, incluindo biocombustíveis, biomassa e produtos de baixo carbono, posiciona a região como protagonista da transição energética global.

O Brasil pode assumir liderança continental com políticas que integrem descarbonização, proteção de biomas, rastreabilidade digital, inovação no campo e segurança jurídica para investimentos privados. Programas de governança ambiental robusta permitem que produtos latino-americanos atendam às exigências internacionais e acessem mercados de alto valor.

Produtores que investirem em sustentabilidade rastreável, agricultura de precisão e integração tecnológica estarão melhor preparados para operar em ambientes de risco elevado e capturar novas oportunidades em mercados globais que valorizam origem, integridade e conformidade ambiental.

Tabela 6 – Síntese: Agronegócio e Alimentos

Dimensão	Brasil e América Latina	Estados Unidos	União Europeia	Ásia
Exposição climática	Muito alta	Média	Média	Variável
Logística	Vulnerável e fragmentada	Altamente integrada	Moderada, porém eficiente	Integrada e crescente
Governança ambiental	Heterogênea e insuficiente	Moderada	Avançada	Variável
Maturidade tecnológica	Média com desigualdades	Alta	Alta	Alta em grandes produtores
Vulnerabilidade criminal	Alta em áreas rurais	Baixa	Baixa	Moderada
Oportunidades	Agricultura de precisão, rastreabilidade, bioeconomia, IA climática	Irrigação avançada, agro 4.0	Sustentabilidade premium	Escala e automação

3.5. Logística, Portos, Rodovias e Infraestruturas Urbanas

3.5.1. Fontes de Risco e Pressões Operacionais

A logística latino-americana enfrenta um conjunto de pressões persistentes que se intensificam em 2026 e além, refletindo a combinação entre vulnerabilidades climáticas, fragilidade institucional, deficiências estruturais e aumento da atuação de redes ilícitas. A região apresenta elevada dependência de modais rodoviários, infraestrutura fragmentada, baixa integração multimodal e capacidade limitada de resposta a choques simultâneos. Eventos climáticos severos, interrupções elétricas, bloqueios territoriais e insuficiência de manutenção ampliam riscos operacionais e aumentam custos de transporte.

Portos localizados em áreas de risco climático elevado sofrem com enchentes, elevação do nível do mar, tempestades e interrupções intermitentes. A baixa profundidade de canais, congestionamentos e limitações de dragagem também afetam a eficiência

logística. Aeroportos e ferrovias enfrentam desafios estruturais como falta de conectividade, baixa digitalização e capacidade limitada de integração com sistemas de previsão e monitoramento em tempo real.

Nas áreas urbanas, a expansão desordenada, a insuficiência de drenagem, a sobrecarga de redes de saneamento e a fragilidade de sistemas de mobilidade criam riscos adicionais. Inundações, deslizamentos, colapsos de encostas e interrupções em transporte público comprometem a circulação de pessoas, mercadorias e serviços críticos. Esse quadro é agravado por falhas de planejamento urbano e pela ausência de integração entre políticas de mobilidade, habitação e infraestrutura verde.

3.5.2. Implicações Regionais

A América Latina apresenta um dos maiores custos logísticos relativos do mundo, muitas vezes representando entre 12% e 18% do PIB, devido à fragilidade estrutural, extensão territorial e baixa integração multimodal. A dependência do modal rodoviário torna a região extremamente vulnerável a interrupções climáticas, incidentes criminais, greves e bloqueios. A atuação de redes ilícitas em áreas portuárias, rotas estratégicas e zonas fronteiriças cria riscos físicos e reputacionais para empresas e operadores logísticos.

O Brasil enfrenta desafios particularmente significativos devido à dimensão continental do território e à concentração de produção agrícola e industrial longe dos principais portos. A falta de ferrovias integradas, a vulnerabilidade de rodovias a eventos extremos e a insuficiência de infraestrutura portuária aumentam custos e reduzem competitividade. A dependência de poucos corredores logísticos afeta diretamente a previsibilidade das exportações, especialmente de grãos, carnes, minérios e manufaturados.

Infraestruturas urbanas em cidades como São Paulo, Rio de Janeiro, Bogotá, Buenos Aires e Lima enfrentam riscos crescentes de colapso parcial durante eventos de chuva extrema, com impactos diretos sobre centros financeiros, cadeias de suprimentos e continuidade de serviços essenciais. A ampliação de riscos urbanos está conectada à expansão desordenada, ao déficit habitacional e à sobrecarga de sistemas de transporte.

3.5.3. Comparativo Global

Em comparação com os Estados Unidos, a América Latina apresenta menor redundância logística, menor integração multimodal e menor capacidade de resposta a choques climáticos ou ciberataques. Os Estados Unidos possuem ferrovias robustas, rede de

hidrovias eficiente, portos modernizados e alta capacidade de dragagem e monitoramento.

Em relação à União Europeia, a lacuna se concentra em planejamento urbano, integração transporte-logística e governança de infraestrutura. A Europa opera com redes de transporte integradas, políticas sólidas de adaptação climática urbana e forte digitalização portuária. A América Latina, por outro lado, permanece com baixa interoperabilidade entre modais e alto grau de informalidade nas operações.

Em comparação com a Ásia, especialmente China, Japão e Coreia do Sul, a região enfrenta desafios associados à baixa automação logística, infraestrutura portuária menos avançada e limitado investimento público e privado. Países asiáticos operam com portos inteligentes, ferrovias de alta capacidade, logística integrada com tecnologias emergentes e forte uso de Inteligência Artificial para previsão e otimização.

Apesar das defasagens, a América Latina possui potencial estratégico significativo devido à sua posição geográfica, abundância de recursos, proximidade com grandes mercados e oportunidades de expansão logística sustentável. O Brasil, com sua costa extensa e capacidade produtiva, apresenta potencial de se tornar corredor logístico global se investir em infraestrutura estratégica integrada.

3.5.4. Oportunidades Estratégicas

O setor apresenta diversas oportunidades para transformar vulnerabilidades em vantagens competitivas. A digitalização logística com uso de Inteligência Artificial, sensores distribuídos, *blockchain* para rastreabilidade de cargas e sistemas integrados de previsão climática pode elevar significativamente a eficiência. A expansão de ferrovias de alta capacidade, hidrovias interioranas, portos inteligentes e corredores logísticos sustentáveis cria novos vetores de crescimento regional.

O desenvolvimento de infraestrutura resiliente, incluindo drenagem aprimorada, urbanismo sustentável, redes elétricas reforçadas e integração entre mobilidade urbana e logística, fortalece a capacidade de resposta a choques climáticos. Parcerias público-privadas, investimentos em concessões e integração regulatória entre países latino-americanos são fundamentais para elevar competitividade e reduzir custos logísticos.

No Brasil, projetos estratégicos como Ferrogrão, corredores Norte e Centro-Oeste, modernização de portos e expansão de hidrovias podem posicionar o país como polo logístico hemisférico. A adoção de tecnologias de previsão, automação portuária e

monitoramento integrado permite ganho expressivo de eficiência e redução de vulnerabilidades.

Tabela 7 – Síntese: Logística, Portos, Rodovias e Infraestruturas Urbanas

Dimensão	Brasil e América Latina	Estados Unidos	União Europeia	Ásia
Logística multimodal	Limitada e desigual	Altamente integrada	Integrada e eficiente	Avançada, automatizada
Vulnerabilidade climática	Alta	Média	Média	Variável
Segurança em portos	Alta exposição a ilícitos	Moderada	Alta	Moderada
Digitalização logística	Baixa a média	Alta	Muito alta	Avançada
Infraestrutura urbana	Sobrecarga e fragilidade	Resiliente	Planejada	Modernizada
Oportunidades	Corredores logísticos verdes, portos inteligentes, ferrovias	Automação avançada	Urbanismo sustentável	Cadeias globais integradas

3.6. Serviços Financeiros e Meios de Pagamento

3.6.1. Pressões Tecnológicas, Crimes Financeiros e Riscos Ilícitos

O setor de serviços financeiros e meios de pagamento é um dos mais impactados pela transformação digital acelerada, pela expansão de Inteligência Artificial e pela evolução das redes ilícitas transnacionais. Esses fatores tornam o setor altamente exposto a riscos cibernéticos, fraudes sofisticadas, ataques à infraestrutura crítica financeira, manipulação de identidades digitais, lavagem de dinheiro e utilização de sistemas financeiros para movimentação de economias ilícitas.

A inovação no setor, acelerada por sistemas de pagamentos instantâneos, *open finance* e múltiplas camadas de digitalização, eleva não somente a eficiência das operações, mas também o grau de complexidade dos ataques. Criminosos utilizam ferramentas avançadas de automação, Inteligência Artificial generativa e engenharia social para realizar fraudes em larga escala, simular identidades e explorar vulnerabilidades em APIs, carteiras digitais e sistemas automatizados de análise de risco.

Além das pressões tecnológicas, o setor enfrenta riscos estruturais relacionados à volatilidade macroeconômica, instabilidade regulatória, perda de confiança digital, pressões internacionais por conformidade e tensões geopolíticas que afetam o fluxo de capitais e custo de financiamento. A interação entre crime financeiro, corrupção, contrabando e mercados ilícitos cria um ambiente de risco híbrido que desafia estruturas tradicionais de *compliance*.

3.6.2. Impactos na América Latina e Brasil

A América Latina é considerada uma das regiões mais vulneráveis do mundo a golpes digitais, fraudes financeiras, exploração de identidades e ataques cibernéticos direcionados ao setor bancário. O crescimento do uso de pagamentos digitais, especialmente em populações não totalmente incluídas digitalmente, amplia a superfície de ataque. A ausência de padronização regional em regulação financeira e proteção de dados intensifica essas vulnerabilidades.

O Brasil é simultaneamente referência global em inovação financeira e um dos mercados mais expostos a riscos digitais. O sistema de pagamentos instantâneos (Pix) transformou o setor, mas também abriu espaço para fraudes cada vez mais sofisticadas que utilizam sequestro digital, engenharia social, *deepfakes* e manipulação de identidades em larga escala. A maturidade das instituições financeiras brasileiras é elevada, mas a pressão sobre sistemas de detecção, resposta e contenção aumenta continuamente.

Além disso, o Brasil enfrenta desafios relacionados à infiltração de organizações criminosas no sistema financeiro por meio de laranjas, empresas de fachada, transações de baixo valor repetidas, uso indevido de criptomoedas, fraudes em meios de pagamento e lavagem de dinheiro conectada a mercados ilícitos como mineração ilegal, tráfico de drogas, crimes ambientais e contrabando. Essa convergência amplia a complexidade de monitoramento e exige modelos avançados de análise comportamental.

3.6.3. Comparação Global

Em comparação com os Estados Unidos, a América Latina enfrenta maior exposição a golpes digitais, menor padronização regulatória e menor maturidade em governança de dados entre empresas de médio e pequeno porte. Os Estados Unidos possuem estruturas robustas de cibersegurança, regulação mais consistente e capacidade de resposta rápida, embora também enfrentem aumento significativo de fraudes com uso de IA.

Em relação à União Europeia, a lacuna se concentra em proteção de dados, rastreabilidade de transações e padronização regulatória. A Europa opera com modelos avançados de governança de IA, arquitetura regulatória unificada e políticas de mitigação de riscos financeiros digitais mais consolidadas. A América Latina ainda apresenta grandes assimetrias entre países e instituições.

Em comparação com a Ásia, especialmente China, Japão e Singapura, o principal diferencial reside na escala tecnológica e na integração entre plataformas financeiras, comércio eletrônico e ecossistemas digitais. A Ásia opera com níveis elevados de automação e sistemas unificados de identidade digital. A América Latina possui dinamismo tecnológico, porém com menor integração e menor capacidade de controle unificado.

Apesar dessas lacunas, Brasil e México são reconhecidos globalmente como laboratórios financeiros de inovação, com rápido crescimento no uso de pagamentos digitais, *fintechs*, bancos digitais e ecossistemas de *open finance*.

3.6.4. Oportunidades Estratégicas

O setor apresenta oportunidades importantes para transformar vulnerabilidades em sistemas robustos de resiliência financeira. A expansão de Inteligência Artificial explicável para monitoramento de transações, análise comportamental avançada, detecção preditiva de fraudes e modelos de risco baseados em machine learning permite maior capacidade de resposta em tempo real. A evolução de sistemas de biometria, identidade digital soberana e ferramentas de auditoria algorítmica reforça a integridade operacional.

A modernização dos marcos regulatórios regionais, harmonização de padrões de governança e integração entre sistemas financeiros latino-americanos podem elevar significativamente a competitividade da região. O Brasil possui oportunidade estratégica de liderar iniciativas regionais de interoperabilidade financeira, identidades digitais avançadas, sistemas de pagamento em escala e regulação de Inteligência Artificial aplicada a serviços financeiros.

Fintechs latino-americanas, aliadas a soluções de *compliance* inteligente e infraestrutura crítica digital resiliente, podem se tornar protagonistas globais em inovação. A criação de mecanismos avançados de rastreabilidade e transparência, aliada a certificações ESG e regulação integrada, atrai investimentos e aumenta a confiança dos mercados internacionais.

Tabela 8 – Síntese: Serviços Financeiros e Meios de Pagamento

Dimensão	Brasil e América Latina	Estados Unidos	União Europeia	Ásia
Exposição a fraudes	Muito alta	Moderada	Baixa	Variável
Maturidade digital	Alta, porém desigual	Muito alta	Alta e padronizada	Muito alta
Governança financeira	Fragmentada	Consolidada	Altamente integrada	Avançada
Crime financeiro	Elevado e sofisticado	Alto, mas controlado	Baixo	Moderado
Uso de IA no setor	Crescente, porém desigual	Avançado	Regulamentado e maduro	Extensivo
Oportunidades	IA explicável, biometria, *open finance*, *compliance* inteligente	Automação avançada	Governança e integração	Escala tecnológica

3.7. Tecnologia, Dados e Plataformas Digitais

3.7.1. Riscos Digitais e Governança Algorítmica

O setor de tecnologia, dados e plataformas digitais enfrenta pressões complexas derivadas da rápida evolução da Inteligência Artificial, da expansão de ecossistemas digitais e da intensificação de riscos cibernéticos. Em 2026 e além, a região observa aumento significativo de ataques sofisticados, manipulação algorítmica, sequestro digital, uso de ferramentas automatizadas para fraudes, exploração de vulnerabilidades em APIs e ataques direcionados a infraestruturas críticas digitais.

A consolidação da Inteligência Artificial generativa amplia tanto as capacidades quanto os riscos. Algoritmos podem ser utilizados para criar falsas identidades, gerar conteúdo malicioso altamente convincente, automatizar ataques e explorar vulnerabilidades com precisão crescente. Ao mesmo tempo, empresas precisam lidar com riscos associados à integridade dos modelos de IA, ao viés algorítmico, à explicabilidade dos sistemas e à crescente pressão regulatória internacional por transparência.

Outro risco crescente é a concentração de dados em plataformas privadas que operam com diferentes níveis de governança e segurança. A falta de padronização de políticas de privacidade, ausência de auditorias externas e dependência de infraestruturas

digitais de terceiros aumentam vulnerabilidades, especialmente para empresas de médio porte.

3.7.2. Implicações para América Latina e Brasil

A América Latina vive um contraste estrutural: ao mesmo tempo em que é uma das regiões mais dinâmicas na adoção de tecnologias digitais, também é uma das mais expostas a fraudes, golpes online e ataques cibernéticos. Países como Brasil, México, Colômbia e Argentina apresentam crescimento acelerado de plataformas digitais, mas com maturidade desigual em governança de dados, segurança cibernética e padronização tecnológica.

O Brasil lidera regionalmente em inovação digital, regulamentação de dados, adoção de Inteligência Artificial e desenvolvimento de plataformas financeiras. Contudo, também é alvo frequente de ataques cibernéticos sofisticados, manipulação de APIs, exploração de sistemas de pagamento e uso indevido de dados. A ausência de integração plena entre setores e a desigualdade de maturidade tecnológica aumentam a probabilidade de falhas sistêmicas.

A volatilidade institucional e a presença de organizações criminosas que utilizam plataformas digitais para fraudes, comércio ilícito, extorsão e lavagem de dinheiro criam riscos adicionais. A intensificação do uso de *deepfakes*, *bots* avançados e redes automatizadas de desinformação amplia impactos sobre segurança, reputação e processos decisórios.

3.7.3. Comparação com Ecossistemas Globais

Em comparação com os Estados Unidos, a América Latina apresenta menor maturidade regulatória em Inteligência Artificial, menor capacidade de auditoria algorítmica e menor integração entre setores público e privado. Os Estados Unidos possuem forte estrutura de cibersegurança, ecossistema de inovação consolidado e capacidade de resposta rápida a incidentes digitais.

Em relação à União Europeia, a diferença principal está no grau de padronização regulatória. A Europa opera com modelos robustos de governança algorítmica, auditoria de IA, segurança digital e proteção de dados. Países latino-americanos, apesar de avanços importantes, ainda enfrentam fragmentação regulatória e carência de mecanismos de controle efetivo.

Comparando com a Ásia, especialmente países como China, Coreia do Sul, Japão e Singapura, a lacuna se concentra na escala tecnológica e na integração sistêmica. A Ásia desenvolve plataformas digitais com arquitetura avançada, identidades digitais unificadas e ecossistemas de IA totalmente integrados. A América Latina apresenta dinamismo tecnológico, mas dependente de *players* globais e com menor capacidade de controle soberano sobre dados.

Apesar dessas diferenças, o Brasil se destaca como polo regional emergente de regulação de IA e inovação em plataformas digitais, com potencial para influenciar padrões continentais.

3.7.4. Oportunidades Estratégicas

O setor de tecnologia apresenta oportunidades decisivas para elevar competitividade, resiliência e governança em toda a América Latina. A adoção de modelos avançados de Inteligência Artificial explicável, auditoria algorítmica e rastreabilidade de dados permite maior segurança, eficiência e conformidade com padrões internacionais.

O desenvolvimento de centros regionais de inovação, *hubs* digitais e parcerias entre governos e empresas pode ampliar a soberania tecnológica e reduzir dependência de plataformas externas. A criação de sistemas de identidade digital forte, infraestrutura crítica de dados e governança integrada de cibersegurança representa uma oportunidade de reposicionamento estratégico continental.

A expansão de *data centers* sustentáveis, a adoção de energias renováveis na infraestrutura digital e a integração entre ciência de dados, segurança corporativa e continuidade de negócios fortalecem a região diante de riscos globais. Empresas que investirem em modelos de IA confiáveis, governança robusta e arquitetura digital resiliente estarão mais preparadas para operar em ambientes híbridos marcados por pressões tecnológicas e riscos complexos.

Tabela 9 – Síntese: Tecnologia, Dados e Plataformas Digitais

Dimensão	Brasil e América Latina	Estados Unidos	União Europeia	Ásia
Governança de IA	Avançando, porém fragmentada	Robusta e influente	Altamente padronizada	Avançada e integrada
Maturidade de dados	Média a alta, desigual	Muito alta	Alta e regulada	Muito alta
Exposição a fraudes digitais	Muito alta	Média	Baixa	Variável

Dimensão	Brasil e América Latina	Estados Unidos	União Europeia	Ásia
Infraestrutura digital	Crescente, porém assimétrica	Ampla e consolidada	Integrada	Avançada e escalável
Dependência de plataformas externas	Elevada	Baixa	Elevada	Variável
Oportunidades	Auditoria algorítmica, IA explicável, data centers, identidade digital	Inovação acelerada	Governança forte	Escala e integração

3.8. Mineração, Petróleo e Gás

3.8.1. Vulnerabilidades e Pressões Ambientais

Os setores de mineração, petróleo e gás enfrentam algumas das fontes de risco mais complexas do cenário contemporâneo. Em 2026 e além, pressões climáticas, ambientais, sociais e tecnológicas convergem para intensificar riscos operacionais, regulatórios, geopolíticos e reputacionais. Esses setores lidam com ativos altamente expostos ao clima, dependem de infraestrutura crítica sensível a interrupções e operam sob crescente escrutínio internacional sobre emissões, rastreabilidade e impactos sociais.

Eventos climáticos extremos, como enchentes que afetam minas, rompimentos de barragens, erosão de encostas, tempestades que interrompem operações marítimas e secas que reduzem disponibilidade hídrica para processos industriais, elevam riscos físicos. Além disso, a intensificação de movimentos socioambientais amplia os riscos de paralisações, pressões judiciais e exigências regulatórias mais rígidas.

A transição energética global gera um conjunto duplo de pressões. De um lado, combustíveis fósseis sofrem pressão por redução de emissões. De outro, cresce a demanda por minerais críticos como **cobre, lítio, nióbio, níquel, grafite e terras raras**, essenciais para baterias, infraestrutura energética limpa e tecnologias digitais. Essa dinâmica amplia riscos de oferta, eleva tensões territoriais e aumenta a competição global por áreas mineráveis.

O crescente interesse mundial pelas terras raras — fundamentais para energias renováveis, mobilidade elétrica, tecnologias digitais e sistemas de defesa — traz à América Latina, especialmente ao Brasil, um conjunto de oportunidades e ameaças. A forte concentração internacional das etapas de refino e processamento desses minerais

aumenta a possibilidade de interrupções nas cadeias produtivas globais e amplia a exposição da região a disputas geopolíticas. Sem avançar em capacidades próprias de processamento, diversificação de mercados e mecanismos de segurança estratégica, países latino-americanos tendem a permanecer vulneráveis a choques de oferta, pressões comerciais e assimetrias tecnológicas.

3.8.2. Implicações Regionais para América Latina e Brasil

A América Latina desempenha papel central na transição global devido a sua abundância de minerais críticos, depósitos de hidrocarbonetos, reservas energéticas e relevância em cadeias produtivas de alto impacto. Porém, a região também enfrenta instabilidades políticas, conflitos territoriais, presença de redes ilícitas e fragilidade regulatória que ampliam riscos operacionais.

Além disso, a volatilidade dos preços internacionais do petróleo e as decisões estratégicas de grandes produtores globais — como cortes de oferta, redirecionamento de produção ou sanções econômicas — funcionam como vetores de choque para a América Latina, afetando receitas públicas, balanças comerciais, investimentos em exploração e a previsibilidade macroeconômica. Esses movimentos amplificam a exposição da região a ciclos de bonança e crise *(boom-and-bust)* e reforçam a importância de estratégias de diversificação energética e de gestão fiscal prudente.

O Brasil é um dos países mais estratégicos do mundo em reservas minerais, energia e biocombustíveis. A produção de minério de ferro, nióbio, petróleo offshore, gás natural e minerais estratégicos coloca o país no centro de disputas globais por recursos. Contudo, o histórico de tragédias envolvendo barragens, desmatamento ilegal, exploração predatória e falhas de fiscalização mantém o setor sob vigilância intensa.

A expansão de grupos criminosos em regiões mineradoras e áreas de fronteira representa um risco crescente. Mineração ilegal de ouro, cassiterita e outros minerais está conectada a redes de tráfico, trabalho escravo, crimes ambientais e lavagem de dinheiro. Essa convergência entre crime organizado e atividades extrativas amplia riscos físicos, reputacionais e regulatórios para empresas legais.

Em alguns países da região, cresce também a atuação de economias paralelas associadas ao cobre; incluindo roubo e desvio de cabos, manipulação ilícita de estoques industriais e interferência em rotas logísticas. Esses mecanismos ampliam riscos operacionais, financeiros e reputacionais para empresas e para infraestruturas intensivas em cobre, afetando redes elétricas, telecomunicações, transporte e sistemas industriais que dependem desse insumo estratégico.

Além disso, pressões internacionais por certificações ambientais, rastreabilidade de origem e integração ESG colocam a América Latina sob maior escrutínio. Empresas da região enfrentam expectativa crescente por transparência, uso de tecnologias de monitoramento ambiental e práticas robustas de governança socioambiental.

3.8.3. Comparação Global

Em comparação com os Estados Unidos, a América Latina apresenta maior exposição a riscos ambientais graves, maior incidência de conflitos socioambientais e menor capacidade de resposta integrada entre setores. Os Estados Unidos operam com governança ambiental mais estruturada e maior capacidade de fiscalização, embora também enfrentem riscos climáticos crescentes.

Em relação à União Europeia, a lacuna é principalmente regulatória e tecnológica. A Europa avança rapidamente em políticas de descarbonização, economia circular, rastreabilidade integrada e monitoramento ambiental contínuo. A América Latina avança, porém de forma fragmentada, com padrões muito distintos entre países.

Quando comparada com a Ásia, especialmente Austrália e China, a região enfrenta menor capacidade de investimento contínuo em modernização, menor padronização tecnológica e maiores pressões territoriais. Austrália se destaca como referência em mineração sustentável, enquanto a China opera com grande escala, forte controle estatal e rápidas expansões de infraestrutura.

Apesar dessas distâncias, a América Latina possui vantagens competitivas essenciais: abundância geológica, potencial para mineração sustentável, capacidade de expansão energética renovável e relevância estratégica na economia verde global.

Estudos internacionais sobre minerais críticos projetam crescimento acelerado da demanda global por cobre, lítio e terras raras até 2030, impulsionado pela expansão de energias renováveis, baterias e infraestrutura digital, reforçando o peso estratégico da América Latina nessas cadeias.

3.8.4. Oportunidades Estratégicas

O setor apresenta oportunidades significativas para fortalecimento de competitividade, resiliência e sustentabilidade. A adoção de tecnologias de monitoramento preditivo, sensores avançados, sistemas remotos de supervisão e modelos de Inteligência Artificial para previsão de falhas pode reduzir drasticamente riscos operacionais e ambientais. A

expansão de práticas de mineração sustentável, rastreabilidade digital da cadeia e certificação ambiental robusta aumenta a confiança de mercados internacionais.

O Brasil possui potencial estratégico para liderar a produção de minerais críticos de forma sustentável, atraindo investimentos globais e posicionando-se como fornecedor confiável em cadeias de energia limpa e tecnologia de ponta. A limitação da mineração ilegal, o fortalecimento da fiscalização e a criação de zonas regulatórias robustas podem transformar vulnerabilidades em oportunidades.

A transição energética cria novas frentes de investimento em hidrogênio verde, captura de carbono, logística de gás natural, biocombustíveis avançados e armazenamento energético. Empresas que integrarem sustentabilidade, segurança convergente e inovação tecnológica poderão operar com maior resiliência e capturar valor em mercados globais de alto crescimento.

O fortalecimento das cadeias industriais associadas a minerais críticos — incluindo processamento, refino, manufatura avançada e integração tecnológica — desponta como uma das oportunidades estratégicas mais relevantes para o Brasil e a América Latina nos próximos anos. Avançar do modelo tradicional baseado apenas em extração e exportação para um modelo que incorpore beneficiamento, transformação e agregação de valor pode reposicionar a região como protagonista da economia verde global, ampliando competitividade, soberania tecnológica e capacidade de atuação em mercados globais de alto crescimento.

Tabela 10 – Síntese: Mineração, Petróleo e Gás

Dimensão	Brasil e América Latina	Estados Unidos	União Europeia	Ásia
Exposição ambiental	Muito alta	Média	Média	Variável
Governança socioambiental	Fragmentada	Moderada	Elevada	Variável
Pressão regulatória	Crescente, porém desigual	Consistente	Muito alta	Alta nos grandes produtores
Riscos criminais	Elevados em áreas remotas	Baixos	Baixos	Moderados
Transição energética	Oportunidade estratégica	Madura	Avançada	Dinâmica e acelerada
Oportunidades	Minerais críticos, IA preditiva, rastreabilidade, energia limpa	Tecnologias avançadas	Economia verde	Escala produtiva

3.9. Setor Público, Justiça e Regulação

3.9.1. Fragilidades Institucionais

O setor público, incluindo poderes Executivo, Legislativo, Judiciário e órgãos de controle, ocupa posição central na configuração dos cenários de risco para 2026 e além. Na América Latina, fragilidades institucionais recorrentes, como instabilidade política, baixa capacidade de execução de políticas públicas, sobrecarga dos sistemas de justiça e assimetrias regulatórias, atuam como amplificadores de riscos para todos os demais setores analisados ao longo deste estudo.

Entre as fragilidades mais relevantes estão a dificuldade de harmonizar políticas de longo prazo, alternâncias abruptas de agenda entre governos, limitações orçamentárias prolongadas, processos burocráticos pouco digitalizados, ausência de integração de dados entre órgãos e deficiências em planejamento baseado em evidências. Em muitos países, a capacidade de formular políticas robustas de segurança, governança digital, adaptação climática e combate ao crime organizado é afetada por essas restrições estruturais.

Os sistemas de justiça, embora representem um pilar de estabilidade, frequentemente operam com congestionamento processual, baixa automação, limitada integração com bases de dados digitais e dificuldade de lidar com crimes complexos que envolvem Inteligência Artificial, criptomoedas, redes transnacionais e infraestruturas críticas. Isso reduz a capacidade de dissuasão, amplia a sensação de impunidade e incentiva a expansão de economias ilícitas.

3.9.2. Pressões Digitais e Criminais

A rápida digitalização do Estado em ambientes institucionalmente frágeis cria uma equação desafiadora. Por um lado, governos adotam serviços digitais, identidades eletrônicas, plataformas integradas e sistemas de arrecadação automatizados. Por outro, muitas dessas iniciativas são implementadas com lacunas de segurança, baixa governança de dados e proteção insuficiente contra-ataques cibernéticos.

Ataques a órgãos públicos, tribunais, ministérios, prefeituras, parlamentos e empresas estatais tornaram-se mais frequentes e sofisticados. Esses ataques incluem sequestro de dados, paralisação de serviços, vazamento de informações sensíveis, comprometimento de sistemas eleitorais e manipulação de cadastros. Em contextos de polarização política, esses incidentes têm impacto ampliado sobre a confiança pública e a estabilidade democrática.

Ao mesmo tempo, redes criminosas utilizam a própria fragilidade estatal para operar. A combinação entre corrupção, captura regulatória, infiltração de grupos ilícitos em estruturas públicas e uso de plataformas digitais para fraudes e lavagem de dinheiro cria um cenário crítico. O crime organizado se beneficia de falhas de coordenação entre órgãos, da falta de interoperabilidade entre bases de dados e da ausência de uma estratégia integrada de segurança pública e financeira em escala regional.

3.9.3. Desafios para Brasil e América Latina

A América Latina enfrenta desafios estruturais comuns, como baixa integração entre sistemas nacionais de justiça, segurança pública, fiscalização tributária e controle financeiro. Muitos países dispõem de ilhas de excelência institucional, mas carecem de uma arquitetura abrangente de governança de riscos em nível de Estado.

O Brasil desempenha papel central na configuração regional, tanto pela sua dimensão econômica e territorial quanto pela complexidade de seus sistemas político, jurídico e administrativo. O país avançou em algumas frentes importantes, como sistemas de controle financeiro, combate à lavagem de dinheiro, automação de tribunais e regulação de proteção de dados. No entanto, permanece com desafios significativos em áreas como segurança pública, integração de bases entre órgãos, combate coordenado ao crime organizado e implementação consistente de políticas de longo prazo.

A sobrecarga de demandas sobre o setor público brasileiro, combinada com restrições fiscais e instabilidade política recorrente, torna difícil a adoção de estratégias estruturantes em temas como governança de Inteligência Artificial, resiliência de infraestruturas críticas, proteção ambiental integrada e fortalecimento de capacidades estatais em regiões remotas dominadas por redes ilícitas. Esses fatores limitam a capacidade de resposta do Estado diante de riscos híbridos, que combinam dimensões físicas, digitais, financeiras e climáticas.

3.9.4. Comparação Global

Em comparação com os Estados Unidos, a América Latina apresenta menor previsibilidade regulatória, maior exposição à captura política de instituições, menor integração entre órgãos de justiça e segurança e menor capacidade de resposta em crises de alta complexidade. Os Estados Unidos, apesar de tensões políticas internas, mantêm estruturas institucionais mais estáveis e com maior capacidade de fazer cumprir as leis e regulações *(enforcement).*

Em relação à União Europeia, a diferença é ainda mais pronunciada na dimensão regulatória. A Europa opera com arcabouço normativo altamente integrado, forte regulação supranacional, padrões mínimos de governança e sistemas de justiça relativamente harmônicos. A América Latina, por outro lado, é marcada por fragmentação e variações profundas de qualidade institucional entre países.

Comparando com a Ásia, a avaliação é heterogênea. Países como Japão, Coreia do Sul e Singapura apresentam instituições robustas e elevada capacidade tecnológica, enquanto outras economias asiáticas compartilham desafios semelhantes aos contextos latino-americanos, como sobrecarga dos sistemas de justiça, informalidade, corrupção e fragilidade regulatória. Ainda assim, a integração regional asiática em temas estratégicos como infraestrutura, comércio e inovação tecnológica tende a ser mais avançada do que na América Latina.

3.9.5. Oportunidades Estratégicas

Apesar das fragilidades, o setor público, a justiça e a regulação na América Latina possuem oportunidades para reposicionamento estratégico. Uma delas é a adoção de modelos de governança orientados por risco, integrando princípios da gestão de riscos à formulação de políticas públicas, à regulação de tecnologias e à supervisão de infraestruturas críticas. Isso permite priorizar ações, otimizar recursos escassos e reduzir vulnerabilidades sistêmicas.

Outra oportunidade consiste em fortalecer a cooperação regional em temas como combate ao crime organizado, crimes financeiros, cibersegurança, proteção ambiental e governança de Inteligência Artificial. A criação de marcos regulatórios alinhados, mecanismos de reconhecimento mútuo, sistemas de interoperabilidade de dados e plataformas conjuntas de inteligência pode elevar significativamente a resiliência estatal.

O Brasil possui condições de liderança em diversas dessas agendas, especialmente em temas como proteção de dados, combate a crimes financeiros, regulação tecnológica e desenvolvimento de políticas integradas de segurança e justiça. A modernização de tribunais, o uso responsável de IA no sistema de justiça, a automação segura de serviços públicos e a ampliação de transparência e prestação de contas são caminhos para aumentar a confiança pública e fortalecer o Estado de Direito.

A adoção de estruturas regulatórias claras para IA, dados, cibersegurança, infraestruturas críticas e meio ambiente, associada a programas de fortalecimento institucional e formação de quadros públicos em gestão de riscos, pode transformar o

setor público em protagonista da resiliência regional, em vez de permanecer como elo mais frágil da cadeia.

Tabela 11 – Síntese: Setor Público, Justiça e Regulação

Dimensão	Brasil e América Latina	Estados Unidos	União Europeia	Ásia
Estabilidade institucional	Variável, frequentemente instável	Relativamente estável	Alta	Heterogênea
Capacidade regulatória	Fragmentada	Alta	Muito alta	Variável
Integração entre órgãos	Limitada	Elevada em temas estratégicos	Elevada	Variável
Exposição ao crime organizado	Alta	Média	Baixa	Variável
Digitalização do Estado	Em expansão, porém desigual	Avançada	Avançada e regulada	Avançada em alguns países
Oportunidades	Governança de riscos, cooperação regional, regulação de IA, fortalecimento institucional	Inovação e estabilidade	Liderança regulatória	Integração em blocos regionais

3.10. Quadro-Síntese Final Multissetorial

A análise integrada dos oito setores considerados neste estudo evidencia um quadro em que riscos climáticos, digitais, institucionais e criminais não atuam de forma isolada, mas como um sistema de pressões interdependentes. A resiliência da América Latina em 2026 e além não dependerá apenas do desempenho individual de cada setor, e sim da capacidade de coordenar políticas, investimentos e governança em uma perspectiva multissetorial. O Brasil, pela escala econômica, pela relevância em energia, agronegócio, mineração e serviços financeiros, ocupa posição central nesse arranjo, podendo funcionar tanto como fator de estabilização quanto de amplificação de vulnerabilidades regionais.

A leitura horizontal dos setores mostra que clima, infraestrutura crítica e logística funcionam como multiplicadores de risco para todos os demais domínios. Interrupções energéticas impactam indústria, serviços financeiros, tecnologia e setor público, ao

mesmo tempo em que agravam tensões urbanas e fragilizam respostas estatais. Eventos climáticos extremos afetam diretamente agronegócio, mineração, cidades, redes rodoviárias e portos, pressionando finanças públicas, aumentando a inadimplência e exigindo instrumentos mais sofisticados de gestão de riscos e seguros. Em paralelo, a digitalização acelerada de todos os setores, sem governança proporcional, cria uma camada adicional de vulnerabilidade que atravessa cadeias produtivas, serviços essenciais e instituições.

Outra convergência importante é a presença transversal do crime organizado e das economias ilícitas. Na prática, não se trata apenas de um problema de segurança pública, e sim de um vetor estrutural de risco que impacta logística, agronegócio, mineração, serviços financeiros, tecnologia e a própria capacidade do Estado em fazer valer regulações. Rotas ilícitas utilizam infraestrutura formal, exploram brechas regulatórias, infiltram serviços financeiros e utilizam plataformas digitais para coordenar operações. Em cenários mais adversos, como Redes Sombrias, essa convergência amplia o risco sistêmico e compromete a credibilidade das instituições.

Do ponto de vista tecnológico, todos os setores analisados avançam em digitalização, automação e uso de dados, porém com velocidades e níveis de maturidade muito distintos. Setores como serviços financeiros, tecnologia e meios de pagamento apresentam alta sofisticação, mas também alta exposição a ataques cibernéticos e fraudes. Indústria, energia e logística ainda possuem grandes assimetrias internas entre empresas de ponta e operadores com baixa maturidade digital, o que cria zonas de vulnerabilidade que podem ser exploradas por agentes maliciosos. O setor público, por sua vez, vive a tensão de digitalizar rapidamente sem dispor, em muitos casos, da mesma robustez de segurança e governança que o setor privado.

Ao mesmo tempo, o quadro multissetorial revela um conjunto consistente de oportunidades convergentes. A expansão de energia renovável, a modernização logística, a agricultura de precisão, a mineração sustentável, a digitalização responsável de serviços públicos, a integração financeira e a governança robusta de Inteligência Artificial podem posicionar Brasil e América Latina como protagonistas em uma economia global que valoriza resiliência, sustentabilidade e integridade. Para isso, será necessário alinhar estratégias setoriais, reduzir fragmentações regulatórias e fortalecer mecanismos de cooperação regional em segurança, dados, clima e infraestrutura crítica. A tabela a seguir sintetiza, de maneira comparativa, as principais características de risco e oportunidade de cada setor, destacando quatro dimensões transversais: sensibilidade climática, exposição a riscos digitais e crime organizado, dependência de instituições públicas e potencial de oportunidade estratégica em 2026 e além.

Tabela 12 – Síntese: Multissetorial

Setor	Sensibilidade climática	Exposição a riscos digitais e crime organizado	Dependência de instituições públicas	Potencial de oportunidade estratégica
Indústria e Manufatura	Alta, devido a energia, água e logística	Média a alta, com aumento de ataques a sistemas industriais	Alta, em infraestrutura, regulação e incentivos	Elevado, com automação defensiva, manufatura avançada e transição verde
Energia e Infraestruturas Críticas	Muito alta, pela dependência hídrica e de redes físicas expostas	Muito alta, com ataques a sistemas de controle e redes críticas	Muito alta, em regulação, concessões e planejamento	Muito elevado, em renováveis, redes inteligentes e integração regional
Agronegócio e Alimentos	Muito alta, por clima, água e solos	Média, com crescente digitalização e presença de ilícitos em áreas rurais	Alta, em infraestrutura, regulação ambiental e fiscalização	Elevadíssimo, em agricultura de precisão, bioeconomia e rastreabilidade sustentável
Logística, Portos, Rodovias e Infraestruturas Urbanas	Muito alta, por eventos extremos que afetam circulação e armazenamento	Média, crescente com digitalização de cadeias e portos	Muito alta, em investimentos, concessões e planejamento urbano	Elevado, em corredores verdes, portos inteligentes e integração multimodal
Serviços Financeiros e Meios de Pagamento	Indireta, mas relevante por impactos em inadimplência e crédito	Muito alta, com fraudes digitais, IA maliciosa e lavagem de dinheiro	Alta, em regulação, supervisão e políticas monetárias	Muito elevado, em IA explicável, *open finance*, biometria e *compliance* inteligente
Tecnologia, Dados e Plataformas Digitais	Indireta, porém crítica para previsão, resposta e resiliência	Muito alta, por ser alvo e vetor de riscos cibernéticos	Média a alta, em políticas de dados, IA e soberania digital	Elevadíssimo, em governança algorítmica, identidade digital, data centers e serviços de valor agregado
Mineração, Petróleo e Gás	Muito alta, com riscos ambientais	Alta, com aumento da	Alta, em licenciamento,	Elevado, em minerais críticos,

Setor	Sensibilidade climática	Exposição a riscos digitais e crime organizado	Dependência de instituições públicas	Potencial de oportunidade estratégica
	e territoriais intensos	automação e ataque a infraestruturas	regulação ambiental e segurança	energia de transição e rastreabilidade
Setor Público, Justiça e Regulação	Alta, pela necessidade de resposta a crises e adaptação climática	Alta, em ataques a órgãos públicos e manipulação digital	Estrutural, pois é o centro da regulação e da coordenação	Muito elevado, em governança de riscos, regulação de IA, cooperação regional e fortalecimento institucional

O quadro multissetorial confirma que a resiliência regional não será alcançada apenas por investimentos setoriais isolados. Ela dependerá da capacidade de articular políticas públicas consistentes, marcos regulatórios claros e estratégias corporativas integradas. Setores como energia, logística, finanças e tecnologia funcionam como espinha dorsal da economia e, por isso, devem ser tratados como prioridades estratégicas em qualquer agenda de desenvolvimento para 2026 e além. Ao mesmo tempo, a modernização do setor público, a profissionalização da justiça e o fortalecimento da regulação em temas como Inteligência Artificial, proteção de dados, combate à lavagem de dinheiro e governança ambiental serão determinantes para transformar vulnerabilidades históricas em vantagens competitivas duradouras.

04

SEGURANÇA CORPORATIVA E INFRAESTRUTURAS CRÍTICAS

4.1. Introdução

A segurança corporativa assume papel central na resiliência organizacional e na estabilidade operativa de setores estratégicos diante dos cenários prospectivos delineados para 2026 e além. O ambiente de risco contemporâneo na América Latina é marcado por pressões simultâneas que atravessam domínios físicos, digitais, climáticos, criminais e institucionais. Essas pressões moldam o ecossistema de segurança de forma integrada e exigem abordagens convergentes capazes de responder a ameaças complexas que evoluem rapidamente.

As infraestruturas críticas da região, incluindo energia, logística, saneamento, telecomunicações, saúde, finanças, mineração, abastecimento alimentar e mobilidade urbana, enfrentam crescente vulnerabilidade diante de ataques cibernéticos, eventos climáticos extremos e expansão de redes ilícitas transnacionais. A interdependência entre esses sistemas cria um ambiente no qual falhas em um domínio podem desencadear interrupções em cascata, amplificando impactos e aumentando o custo dos incidentes. O fortalecimento da segurança corporativa torna-se, portanto, um requisito operacional e estratégico para garantir continuidade, estabilidade e confiança dos stakeholders.

A seguir, este capítulo apresenta uma leitura integrada das pressões sobre segurança corporativa, destacando riscos físicos, digitais e reputacionais, além de analisar a situação específica da América Latina e do Brasil, comparando com padrões globais e identificando oportunidades de evolução.

4.2. Pressões do Ambiente de Risco Híbrido

A convergência entre riscos físicos e digitais transforma profundamente a lógica de segurança corporativa. A digitalização das operações aumenta a eficiência, mas amplia a superfície de ataque, especialmente com a integração entre tecnologia da informação, tecnologia operacional e dispositivos conectados. Sistemas críticos utilizados em energia, manufatura, portos, aeroportos, hospitais e serviços financeiros tornam-se alvos de agentes maliciosos que buscam paralisar operações, causar danos físicos ou obter vantagem financeira.

Eventos climáticos extremos também impactam diretamente a segurança, provocando interrupções elétricas, danos estruturais, sobrecarga de redes, deslocamentos populacionais e situações que ampliam a probabilidade de crimes oportunistas, invasões e desorganização operacional. Em paralelo, a difusão de plataformas digitais facilita ações de grupos ilícitos que utilizam dados, identidades simuladas, ferramentas de

automação e redes sociais para ampliar a escala de fraudes, extorsões e manipulação informacional.

A segurança corporativa deixa de ser um pilar isolado e passa a atuar como interface entre continuidade de negócios, governança digital, gestão de riscos e proteção de infraestruturas críticas. As organizações precisam desenvolver competências multidisciplinares para enfrentar um ambiente em que ameaças se deslocam entre o mundo físico e o digital com fluidez cada vez maior.

4.3. Vulnerabilidades Específicas de Infraestruturas Críticas

As infraestruturas críticas da América Latina apresentam vulnerabilidades que decorrem de fatores estruturais e conjunturais. Estruturas envelhecidas, baixa redundância, falta de manutenção contínua, déficit de investimentos e exposição climática elevada aumentam a probabilidade de falhas sistêmicas. Ao mesmo tempo, a expansão de conectividade e sensores em sistemas industriais não tem sido acompanhada do mesmo grau de investimento em segurança digital, gerando lacunas em proteção de dados, protocolos de resposta e atualizações de sistemas.

A falta de integração entre setores, a ausência de padrões mínimos de resiliência e a fragmentação regulatória ampliam as vulnerabilidades. Em muitos países, infraestruturas críticas são operadas por empresas privadas que dependem de um ambiente institucional estável para implementar planos robustos de proteção. A instabilidade política, a burocracia e a falta de coordenação entre setores energético, logístico, sanitário e tecnológico reduzem a capacidade de resposta conjunta a incidentes severos.

Além disso, redes ilícitas exploram fragilidades estruturais para furtar cabos, atacar subestações, interferir em rotas logísticas, manipular sistemas de transporte e infiltrar cadeias de suprimentos. A criminalidade, quando combinada com eventos climáticos extremos ou ataques cibernéticos, pode gerar situações de crise prolongada e aumento significativo de custos operacionais.

4.4. Panorama Latino-Americano: Crime Organizado, Convergência Digital e Fragilidade Estatal

A América Latina apresenta uma das combinações mais adversas para segurança corporativa entre as grandes regiões do mundo. A presença de organizações criminosas com capacidade transnacional, o uso de tecnologias avançadas para fraudes e extorsões,

a vulnerabilidade de portos e fronteiras e a instabilidade institucional criam um ambiente que exige abordagens altamente especializadas de mitigação.

Portos estratégicos, como Santos, Colón, Buenaventura, Guayaquil e Buenos Aires, são utilizados por cartéis internacionais para lavagem de dinheiro, contrabando e fluxo de cargas ilícitas, muitas vezes infiltrando operadores logísticos e facilitando contaminação de cadeias legais. As empresas que operam nesses ambientes precisam implementar controles rigorosos, sistemas de rastreabilidade e protocolos de inspeção que superem falhas estatais.

No setor digital, fraudes avançadas, engenharia social automatizada, manipulação de APIs e uso de Inteligência Artificial para criação de falsificações ampliam a complexidade da proteção de identidades e operações eletrônicas. Pequenas e médias empresas são desproporcionalmente mais vulneráveis devido à menor maturidade de segurança e à dependência de fornecedores externos.

A fragilidade estatal amplia esses riscos ao dificultar a fiscalização de áreas remotas, reduzir capacidade de resposta a incidentes severos, limitar cooperação internacional e dificultar a implementação de políticas robustas de proteção de dados e infraestruturas críticas.

4.5. Resposta Corporativa: Segurança Convergente e Resiliência Operacional

A resposta corporativa diante do ambiente de riscos híbridos exige a transição de modelos fragmentados para uma arquitetura de segurança verdadeiramente convergente. Nesse modelo, a proteção de ativos físicos, digitais, informacionais e operacionais não é tratada como funções isoladas, mas como componentes interdependentes de um mesmo sistema estratégico orientado pela resiliência organizacional. A seguir são apresentadas as quatro dimensões centrais que estruturam essa abordagem.

Neste estudo, o termo **Segurança Corporativa** é utilizado para designar a função de governança estratégica que integra e orienta diferentes domínios de proteção — física, patrimonial, cibernética, informacional, reputacional entre outros — conectando-os à continuidade de negócios, à proteção de ativos críticos e à resiliência organizacional.

Embora tecnologias avançadas e Inteligência Artificial ampliem significativamente a capacidade analítica e a eficiência operacional, elas não substituem o julgamento humano. A maturidade profissional, a experiência acumulada e a colaboração entre

equipes permanecem como elementos decisivos para transformar informação em ação estratégica e sustentar a resiliência corporativa em ambientes voláteis.

A **primeira dimensão** corresponde à arquitetura de proteção convergente e inteligente. Ela integra tecnologias avançadas, análises comportamentais, sensores distribuídos e sistemas remotos de monitoramento para proteger ativos críticos em diferentes camadas. Essa arquitetura baseia-se em avaliação contínua de riscos, em proteção dinâmica de perímetros e em mecanismos de dissuasão que incorporam dados climáticos e operacionais. A proteção deixa de ser apenas vigilância física e evolui para um sistema coordenado capaz de antecipar ameaças, responder rapidamente a mudanças no contexto e apoiar decisões estratégicas.

A **segunda dimensão** é a defesa digital estruturante, que posiciona a cibersegurança como núcleo da continuidade de negócios. Ela envolve proteção integral de sistemas críticos, governança de dados, rastreabilidade digital, segmentação avançada de redes e uso de Inteligência Artificial defensiva para detecção precoce de anomalias. Inclui também governança algorítmica, com mecanismos de explicabilidade, auditoria e supervisão contínua de modelos automatizados. Essa dimensão é essencial para reduzir a probabilidade de eventos sistêmicos em ambientes altamente digitalizados.

A **terceira dimensão** corresponde à governança estratégica de riscos e continuidade. Nela, a segurança corporativa é integrada ao centro da tomada de decisão, conectando gestão de riscos, governança de dados, continuidade operacional e estratégia institucional. Trata-se de estruturar mecanismos de avaliação de riscos complexos, estabelecer métricas e indicadores de resiliência, incorporar análises de cenários ao processo decisório e fortalecer a relação entre áreas de segurança, conselho, comitê executivo e planejamento estratégico. Essa dimensão permite que a organização desenvolva visão antecipatória e capacidade de adaptação contínua.

Na prática, essa governança de riscos e continuidade exige que cenários de crime organizado, violência dirigida contra ativos corporativos e interrupções provocadas por ações ilícitas sejam tratados explicitamente nos planos de continuidade de negócios (BCP), de recuperação de desastres (DRP) e nas análises de impacto nos negócios (BIA), ao lado de desastres naturais, falhas tecnológicas e choques macroeconômicos. Incorporar esses vetores criminais à agenda de resiliência evita que a corporativa permaneça em um plano meramente operacional e a reposiciona como componente estratégico da proteção de valor.

A **quarta dimensão** refere-se à capacidade de resposta integrada, adaptativa e baseada em inteligência. Essa capacidade opera com protocolos unificados para incidentes físicos, digitais, climáticos e reputacionais, garantindo que equipes de segurança,

tecnologia, operações, jurídico e comunicação atuem de forma coordenada. Envolve centros integrados de comando e controle, simulações periódicas, processos de recuperação escaláveis e mecanismos de aprendizagem pós-incidente que retroalimentam toda a governança de riscos. A resiliência deixa de ser entendida como plano isolado e passa a ser um atributo estratégico que permite à organização operar mesmo sob condições severamente degradadas.

A segurança corporativa contemporânea deve ser compreendida como um **sistema de governança integrado** que articula riscos físicos, digitais, climáticos, reputacionais e institucionais com foco nos objetivos da organização. Sua atuação demanda visão estratégica e capacidade de antecipação, e não apenas controle operacional. A seguir, apresentamos um resumo estratégico das quatro dimensões.

Tabela 13 – Dimensões do sistema de governança integrado da segurança corporativa

Dimensão Estratégica	Foco Central	Valor Adicionado
Arquitetura de Proteção Convergente	Governança integrada de ativos físicos e tecnológicos	Redução de vulnerabilidades híbridas e aumento de proteção estrutural
Defesa Digital Estruturante	Cibersegurança como núcleo da continuidade	Prevenção de ataques sistêmicos e proteção de dados críticos
Governança Estratégica de Riscos	Segurança como função estratégica da organização	Alinhamento com conselho, estratégia e decisões de alto impacto
Resposta Integrada e Adaptativa	Resiliência organizacional em múltiplas camadas	Capacidade de operar mesmo em ambiente degradado

Essas quatro dimensões, quando implementadas de forma integrada, transformam a segurança corporativa em pilar estruturante da resiliência organizacional. Elas reforçam a capacidade de antecipar ameaças, absorver choques, responder de forma eficaz e recuperar operações críticas em ambientes marcados por incerteza, interdependência e rápidas transformações. Essa abordagem prepara empresas e instituições para enfrentar de maneira sólida os desafios complexos que caracterizam a América Latina em 2026 e além.

4.6. Pressões e Oportunidades no Contexto Brasileiro

O Brasil é simultaneamente um dos países mais desafiadores e promissores em segurança corporativa. A presença de grupos criminosos sofisticados, a extensão territorial, a importância de seus portos e refinarias, a dependência de hidrovias e rodovias e a crescente digitalização de serviços financeiros ampliam a complexidade da proteção de ativos. Ao mesmo tempo, o país lidera a região em inovação tecnológica,

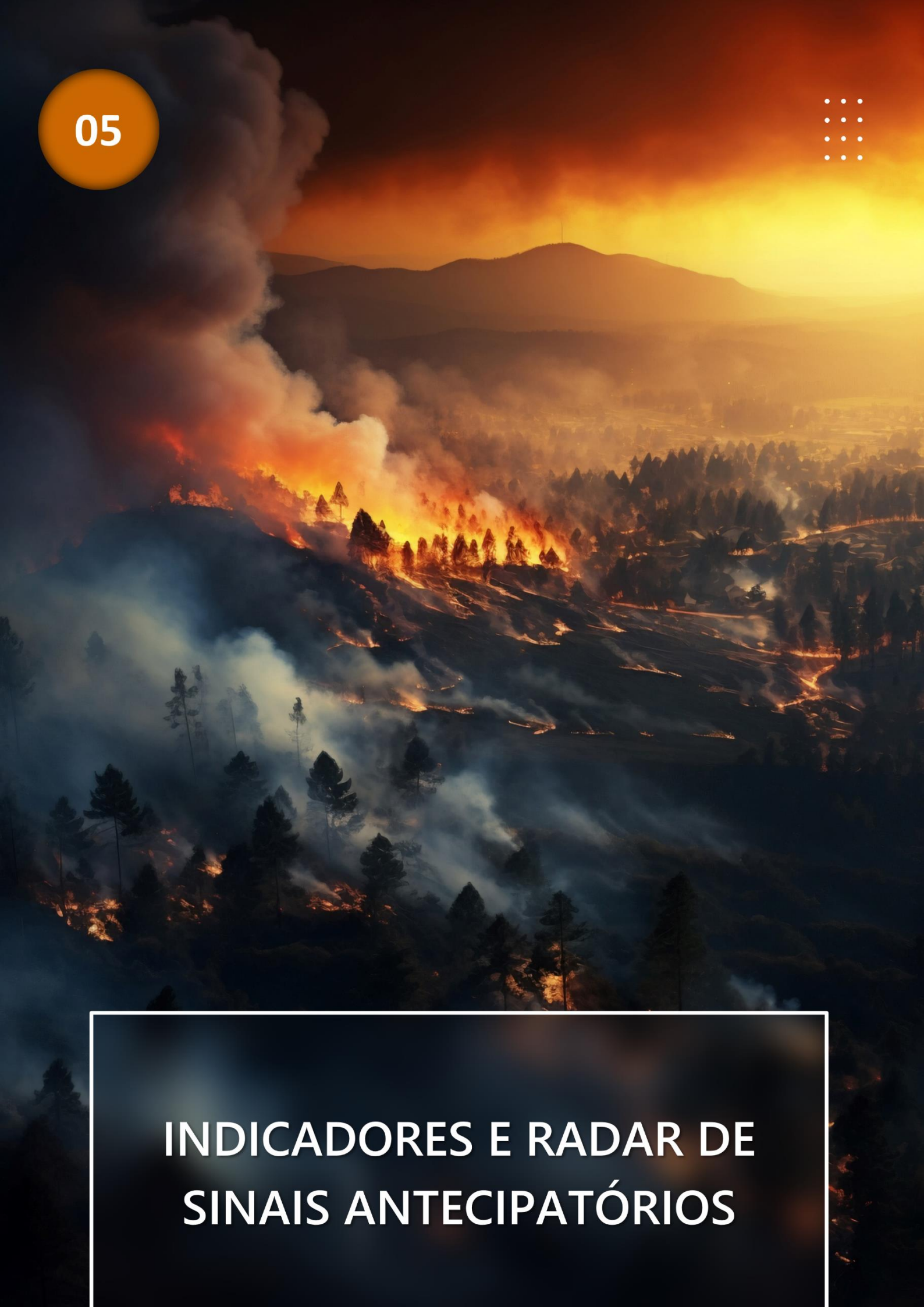
adoção de sistemas avançados de segurança e integração entre setores público e privado.

Além da proteção de ativos físicos e digitais, o contexto brasileiro exige atenção permanente à integridade física de colaboradores e equipes operacionais. Riscos de assaltos e sequestros em deslocamentos, coações em regiões sob influência de facções criminosas e episódios de violência no entorno de plantas industriais, obras e centros logísticos impactam diretamente programas de continuidade de negócios, o clima organizacional, o dever de cuidado das empresas e sua exposição a riscos jurídicos e reputacionais.

Áreas críticas como mineração, energia, logística, agronegócio e serviços financeiros exigem abordagens específicas baseadas em monitoramento remoto, auditoria de sistemas, proteção de dados sensíveis, gestão de incidentes climáticos e resposta rápida a crises. A capacidade brasileira de desenvolver centros integrados, algoritmos próprios de detecção, plataformas de rastreabilidade e tecnologias de previsão climática cria oportunidades relevantes para elevar sua resiliência.

O fortalecimento de programas nacionais de proteção de infraestruturas críticas, a harmonização regulatória e a expansão de iniciativas de cooperação interestadual são essenciais para reduzir vulnerabilidades, ampliar previsibilidade e fortalecer o ambiente de negócios.

05



INDICADORES E RADAR DE SINAIS ANTECIPATÓRIOS

5.1. Introdução

A construção de um radar de sinais antecipatórios é uma etapa essencial para transformar o estudo de cenários em capacidade real de monitoramento, antecipação e resposta organizacional. Indicadores bem definidos permitem que empresas, governos e organizações avaliem mudanças no ambiente externo, detectem rupturas emergentes e ajustem estratégias antes que os impactos se tornem irreversíveis. Em um contexto de riscos híbridos, fragmentação institucional e aceleração tecnológica, a capacidade de interpretação precoce torna-se fator de vantagem competitiva.

O radar de sinais antecipatórios apresentado neste capítulo está estruturado com base nas quatro dimensões centrais que moldam o ambiente estratégico analisado ao longo do relatório: clima e ambiente, tecnologia e dados, crime e instabilidade institucional, economia e cadeias críticas. Cada dimensão possui indicadores específicos que permitem monitoramento sistemático, reduzindo incertezas e ampliando a capacidade de adaptação diante de eventos imprevisíveis. A combinação desses indicadores forma uma matriz de alerta que pode ser utilizada tanto por setores privados quanto por órgãos públicos.

A América Latina e o Brasil exigem conjunto particular de indicadores devido a vulnerabilidades estruturais e assimetrias regionais. Eventos climáticos extremos, volatilidade regulatória, expansão do crime organizado, ataques cibernéticos e fragilidade de infraestruturas críticas ocorrem com maior frequência e intensidade na região, o que requer radar mais sensível e abrangente. A seguir, detalham-se os sinais antecipatórios organizados por domínio estratégico.

5.2. Indicadores Climáticos e Ambientais

Os indicadores climáticos constituem primeira camada do radar, pois funcionam como multiplicadores de risco para logística, energia, agricultura, mineração, infraestrutura urbana e saúde. A análise histórica mostra que eventos extremos na América Latina produzem efeitos operacionais e econômicos mais severos devido à menor redundância estrutural e à fragilidade de redes energéticas e logísticas.

Indicadores prioritários incluem variações anômalas no regime de chuvas, declínio persistente de reservatórios estratégicos, aumento da temperatura média em áreas produtivas, ocorrência repetida de ondas de calor, enchentes em corredores logísticos, incêndios florestais em zonas críticas, redução do nível de rios utilizados para transporte e pressões hídricas constantes em centros urbanos. A simultaneidade desses eventos sinaliza transição para ciclos mais intensos e prolongados de instabilidade.

Outro indicador-chave é o aumento no custo de seguros climáticos e paramétricos, pois o mercado financeiro incorpora riscos antes mesmo de sua materialização física. A elevação gradual do prêmio de seguros sinaliza deterioração da resiliência climática e necessidade de adaptação mais intensa.

Tabela 14 – Indicadores Climáticos e Ambientais (Resumo Executivo)

Categoria de Indicador	Descrição do Sinal Antecipatório	Implicação Estratégica	Relevância para América Latina e Brasil
Variações anômalas de chuva	Desvios persistentes no regime de chuvas e redução da previsibilidade climática	Afeta agricultura, energia hidroelétrica e abastecimento urbano	Alta; eventos extremos mais frequentes e severos
Declínio de reservatórios e aquíferos	Redução contínua de volumes de água em áreas estratégicas	Pressiona geração de energia, irrigação e abastecimento humano	Muito alta; dependência da matriz hídrica é significativa
Aumento da temperatura média	Elevação de temperaturas em áreas produtivas e urbanas	Reduz produtividade agrícola, aumenta doenças e eleva custos operacionais	Alta; ondas de calor já afetam grandes centros urbanos
Ondas de calor recorrentes	Ocorrência repetida de picos extremos de temperatura	Afeta saúde pública, estabilidade energética e condições de trabalho	Muito alta; forte impacto em operações industriais e urbanas
Enchentes em corredores logísticos	Alagamentos e deslizamentos interrompem vias críticas	Eleva custos de transporte, atrasa exportações e gera perdas produtivas	Muito alta; infraestrutura vulnerável a eventos extremos
Incêndios florestais em zonas sensíveis	Expansão de queimadas naturais ou criminosas	Afeta biodiversidade, agronegócio, saúde pública e cadeias logísticas	Alta; fronteiras agrícolas e regiões remotas são muito expostas
Redução do nível de rios de transporte	Queda do calado em hidrovias essenciais	Interrompe escoamento agrícola e industrial, eleva custos logísticos	Muito alta; especialmente crítico no Brasil e na Bacia Amazônica
Pressões hídricas urbanas	Racionamento, sobrecarga de redes e déficit de drenagem	Afeta mobilidade, saúde e segurança urbana	Alta; cidades latino-americanas possuem infraestrutura limitada
Aumento de seguros climáticos	Elevação contínua do prêmio de seguros e paramétricos	Indica deterioração da resiliência climática do território	Alta; mercado reage antes da materialização dos eventos

5.3. Indicadores Digitais e Tecnológicos

Os indicadores digitais monitoram a pressão crescente sobre sistemas de informação, dados, Inteligência Artificial e infraestruturas críticas. A América Latina é uma das regiões com maior número de ataques cibernéticos per capita, o que demanda observação contínua de anomalias digitais que podem anteceder incidentes de grande escala.

Entre os principais indicadores estão anomalias persistentes em acessos não autorizados, aumento de ataques de força bruta, atividade incomum em APIs, desvios comportamentais em sistemas analíticos, falhas simultâneas em provedores de nuvem, interrupções em plataformas de pagamento, uso crescente de *deepfakes* para fraudes e campanhas coordenadas de desinformação.

Indicadores de governança também são relevantes, como atrasos na implementação de regulações de IA, aumento de incidentes envolvendo viés algorítmico, falhas de transparência em modelos de decisão automatizada e ausência de auditoria em sistemas críticos. Esses sinais revelam fragilidade institucional e aumento da probabilidade de eventos sistêmicos.

Tabela 15 – Indicadores Digitais e Tecnológicos (Resumo Executivo)

Categoria de Indicador	Descrição do Sinal Antecipatório	Implicação Estratégica	Relevância para América Latina e Brasil
Acessos não autorizados e tentativas anômalas	Aumento persistente de tentativas de invasão e comportamentos fora do padrão	Anuncia ataques coordenados e exploração de vulnerabilidades críticas	Muito alta; região é alvo prioritário de grupos globais
Ataques de força bruta e exploração de APIs	Intensificação de tentativas automatizadas de quebra de credenciais e manipulação de APIs	Indica risco de intrusão em sistemas operacionais, financeiros e industriais	Muito alta; ampla digitalização sem padronização robusta
Desvios comportamentais em sistemas analíticos	Mudanças inesperadas em padrões de uso, transações ou fluxos internos	Pode indicar manipulação de modelos, fraudes ou presença de atores maliciosos	Alta; empresas dependem de sistemas analíticos pouco protegidos

Categoria de Indicador	Descrição do Sinal Antecipatório	Implicação Estratégica	Relevância para América Latina e Brasil
Falhas simultâneas em provedores de nuvem	Interrupções paralelas ou instabilidade em múltiplos ambientes cloud	Alto risco de falha sistêmica e interrupção de operações críticas	Alta; forte dependência de poucos provedores globais
Instabilidade em plataformas de pagamento	Quedas recorrentes, latência anormal ou inconsistências em pagamentos digitais	Afeta serviços financeiros, e-commerce e confiança pública	Muito alta; Brasil e México são polos de pagamentos digitais
Uso de *deepfakes* em fraudes e extorsões	Expansão de falsificações hiper-realistas para golpes e manipulação	Eleva riscos reputacionais e compromete processos de verificação	Crescente; casos multiplicam-se em ritmo acelerado
Campanhas coordenadas de desinformação	Ação combinada de *bots* e conteúdo manipulativo em larga escala	Afeta eleições, reputação corporativa e estabilidade institucional	Muito alta; alta polarização facilita disseminação
Atrasos em regulação de IA	Falta de diretrizes claras, regulamentação lenta ou fragmentada	Aumenta exposição a riscos éticos, legais e de conformidade	Alta; amadurecimento regulatório em estágio inicial
Incidentes de viés algorítmico e falta de transparência	Resultados inconsistentes, discriminação ou decisões automatizadas sem explicação	Compromete governança digital e confiança de stakeholders	Alta; poucos setores possuem auditoria algorítmica formal
Ausência de auditoria em sistemas críticos	Falta de monitoramento sistemático em modelos de IA, algoritmos e redes	Eleva possibilidade de eventos sistêmicos e falhas não detectadas	Muito alta; auditorias ainda são incipientes na região

5.4. Indicadores Sociopolíticos e Criminais

A convergência entre instabilidade institucional, pressões sociais e expansão de redes ilícitas cria ambiente que exige monitoramento constante. Indicadores sociopolíticos permitem antecipar ciclos de tensão que impactam diretamente operações corporativas, cadeias logísticas e investimentos estratégicos.

Entre os sinais prioritários estão aumento expressivo de homicídios em regiões de fronteira, escalada de confrontos entre facções, infiltração de grupos ilícitos em corredores logísticos, intensificação de roubos de carga, aumento de crimes ambientais vinculados à mineração ilegal, interferências em portos, pressões territoriais em regiões de garimpo e elevação de ataques a órgãos públicos.

Indicadores institucionais incluem atrasos persistentes em processos regulatórios, volatilidade legislativa, disputas entre poderes, diminuição da confiança em instituições, judicialização de políticas públicas, fragmentação das agências de segurança, redução do orçamento de fiscalização e eventos que sinalizem crise de governabilidade.

Tabela 16 – Indicadores Sociopolíticos e Criminais (Resumo Executivo)

Categoria de Indicador	Descrição do Sinal Antecipatório	Implicação Estratégica	Relevância para América Latina e Brasil
Escalada de homicídios em regiões de fronteira	Aumento rápido e contínuo da violência em áreas transfronteiriças	Indica fortalecimento de organizações criminosas e disputas territoriais	Muito alta; fronteiras amazônicas e Cone Sul são *hotspots* críticos
Confrontos entre facções e grupos armados	Intensificação de conflitos armados urbanos ou rurais	Risco para cadeias logísticas, mobilidade de funcionários e ativos corporativos	Muito alta; presença forte de facções e milícias em centros urbanos
Infiltração em corredores logísticos	Atuação criminosa em portos, rodovias, ferrovias e zonas alfandegárias	Afeta exportações, contamina cadeias, facilita contrabando e lavagem	Muito alta; porta de entrada e saída de ilícitos para outros continentes
Roubos de carga e interferências em rotas	Aumento persistente em furtos, saques ou bloqueios territoriais	Eleva custos operacionais e compromete continuidade logística	Alta; Brasil é um dos campeões globais em roubo de cargas
Crimes ambientais ligados à mineração ilegal	Garimpo clandestino, exploração predatória e ocupações irregulares	Riscos reputacionais, jurídicos e operacionais em áreas remotas	Muito alta; forte correlação com redes ilícitas transnacionais

Categoria de Indicador	Descrição do Sinal Antecipatório	Implicação Estratégica	Relevância para América Latina e Brasil
Atividades ilícitas em portos estratégicos	Sinais de corrupção, perdas inexplicadas, interferência armada ou sabotagem	Ameaça o comércio exterior, *compliance* e integridade de cargas	Muito alta; Santos, Colón, Guayaquil e Buenos Aires são pontos críticos
Pressões territoriais em áreas de garimpo	Expansão de invasões, conflitos e presença de grupos armados	Afeta mineração, agronegócio, proteção ambiental e segurança de equipes	Alta; Amazônia, Orinoco e Cerrado apresentam alta vulnerabilidade
Ataques a órgãos públicos e instituições	Investidas criminosas contra prefeituras, delegacias, tribunais e forças de segurança	Afeta legitimidade institucional e capacidade de resposta estatal	Alta; eventos recentes mostram aumento desse tipo de violência
Atrasos regulatórios persistentes	Morosidade ou paralisação de ações regulatórias essenciais	Cria incerteza jurídica e operacional para setores críticos	Alta; fragmentação regulatória é marcante na região
Volatilidade legislativa e disputas entre poderes	Mudanças abruptas, conflitos entre poderes e judicialização excessiva	Reduz previsibilidade e aumenta risco de instabilidade política	Muito alta; intensidade de fragmentação institucional é acentuada
Redução de orçamento de fiscalização	Cortes contínuos em órgãos ambientais, regulatórios e de segurança	Amplia risco de ilícitos, degradação ambiental e vulnerabilidade estatal	Alta; comum em ciclos de austeridade fiscal na região

5.5. Indicadores Econômicos e de Cadeias Críticas

A resiliência econômica depende da estabilidade das cadeias produtivas, da capacidade de financiamento, da previsibilidade regulatória e do fluxo eficiente de bens e serviços. Indicadores econômicos devem ser monitorados em conjunto com riscos climáticos e digitais, uma vez que rupturas simultâneas elevam drasticamente a probabilidade de instabilidade sistêmica.

Entre os indicadores essenciais estão níveis críticos de estoque em cadeias sensíveis, interrupções recorrentes em portos e rodovias, flutuações abruptas no preço de combustíveis, queda da capacidade hídrica de usinas, atrasos no escoamento da produção agrícola, interrupções na geração de petróleo devido a tempestades e pressões de crédito sobre consumidores e empresas.

A sensibilidade de mercados financeiros a eventos climáticos ou cibernéticos também funciona como indicador antecipatório. Aumento abrupto do risco-país, elevação do spread bancário, retração de investimentos e valorização de commodities climáticas podem sinalizar deterioração antecipada do ambiente operacional.

Tabela 17 – Indicadores Econômicos e de Cadeias Críticas (Resumo Executivo)

Categoria de Indicador	Descrição do Sinal Antecipatório	Implicação Estratégica	Relevância para América Latina e Brasil
Níveis críticos de estoque em cadeias sensíveis	Redução acelerada ou abaixo do mínimo operacional em setores como alimentos, combustíveis e medicamentos	Indica risco iminente de ruptura, desabastecimento e aumento de preços	Muito alta; cadeias longas e infraestrutura frágil amplificam rupturas
Interrupções recorrentes em portos e rodovias	Bloqueios, enchentes, greves, acidentes e gargalos estruturais	Afetam exportações, produção industrial e logística agrícola	Muito alta; dependência exagerada do modal rodoviário
Flutuações bruscas no preço de combustíveis	Oscilações abruptas em petróleo, diesel, gás e energia	Pressiona custos logísticos, afeta transporte e gera instabilidade macroeconômica	Alta; volatilidade externa impacta economias importadoras
Queda da capacidade hídrica de usinas	Redução de geração hidrelétrica e dependência emergencial de fontes alternativas	Eleva custo de energia e risco de racionamentos	Muito alta; Brasil e países andinos dependem intensamente de hidroenergia
Atrasos no escoamento da produção agrícola	Congestionamentos, falta de armazéns, déficits logísticos e falhas climáticas	Impacta exportações, aumenta perdas e reduz competitividade	Muito alta; agronegócio é pilar da economia regional
Interrupções na produção de petróleo	Paradas causadas por tempestades, acidentes ou falhas operacionais	Pressiona custos energéticos e compromete receitas fiscais	Alta; Brasil, México e Venezuela são grandes produtores
Pressões de crédito em consumidores e empresas	Aumento de inadimplência, redução de liquidez e juros elevados	Afeta consumo, investimento e estabilidade financeira	Alta; economias sensíveis a choques fiscais e monetários

Categoria de Indicador	Descrição do Sinal Antecipatório	Implicação Estratégica	Relevância para América Latina e Brasil
Aumento súbito no risco-país	Percepção de risco político, fiscal ou institucional por investidores	Eleva custo de capital, afeta câmbio e reduz investimento externo	Muito alta; volatilidade institucional é característica regional
Elevação do spread bancário	Aumento da diferença entre custo de captação e juros cobrados	Sinaliza deterioração do ambiente econômico e maior aversão ao risco	Alta; crédito empresarial costuma ser mais caro na região
Valorização anômala de commodities climáticas	Alta súbita em açúcar, soja, milho, café, hidroenergia, seguros climáticos	Indica riscos climáticos intensos ou disfunções em cadeias produtivas	Muito alta; região é grande produtora e altamente exposta ao clima

5.6. Radar Integrado de Sinais Antecipatórios

A integração dos quatro domínios apresentados permite construir um radar que identifica não apenas sinais isolados, mas padrões que antecedem eventos de grande impacto. A convergência entre indicadores climáticos, digitais, criminais e econômicos é o elemento que, na prática, gera rupturas significativas.

O radar integrado deve priorizar:

- Eventos climáticos que coincidam com falhas digitais ou interrupções energéticas;
- Atividade criminosa crescente em regiões sensíveis a escoamento de produção;
- Anomalias simultâneas em sistemas de pagamento, cadeias logísticas e infraestrutura crítica;
- Variações extremas no nível de reservatórios combinadas com pressão em redes elétricas;
- Indicadores institucionais que revelem perda de capacidade estatal.

A leitura combinada desses elementos permite antecipar mudanças nos cenários delineados no Capítulo 1 – item 1.5. e identificar o início de transições entre quadrantes, especialmente quando sinais de fragmentação institucional se combinam com eventos climáticos e vulnerabilidades digitais.

Com isso, o radar de sinais antecipatórios torna-se instrumento fundamental para orientar decisões estratégicas, revisar planos de continuidade, reforçar segurança

convergente e alinhar investimentos com as tendências que moldarão a América Latina em 2026 e além.

5.7. Integração com as Diretrizes da ISO 31050 para Riscos Emergentes

A ISO 31050 amplia o entendimento tradicional da gestão de riscos ao enfatizar a necessidade de estruturas específicas para lidar com riscos emergentes caracterizados por novidade, incerteza extrema, dados insuficientes, complexidade e ambiguidade. Esses riscos exigem abordagem distinta daquela aplicada a riscos conhecidos, justamente porque não se manifestam através de sinais clássicos, mas sim por meio de pequenas anomalias, mudanças contextuais discretas e interações que, isoladamente, podem parecer irrelevantes.

Nesse sentido, o radar de sinais antecipatórios descrito nos itens anteriores deve ser interpretado à luz de **três princípios fundamentais da ISO 31050**.

O **primeiro princípio** é a análise contínua do contexto em múltiplas dimensões. Mudanças climáticas, rupturas tecnológicas, transformações socioeconômicas, tensões políticas e alterações regulatórias são parte do ambiente em que riscos emergentes se desenvolvem. Esses elementos precisam ser monitorados simultaneamente, pois seus efeitos combinados podem criar condições propícias à emergência de novos riscos sistêmicos.

O **segundo princípio** é a identificação e interpretação de sinais fracos. Esses sinais incluem pequenas flutuações em indicadores climáticos, desvios discretos em sistemas digitais, pressões territoriais ainda incipientes, mudanças no comportamento de consumidores, anomalias em cadeias logísticas e dificuldades isoladas em fornecedores críticos. A ISO 31050 destaca que riscos emergentes quase nunca se anunciam por eventos abruptos; eles surgem como padrões difusos que só podem ser percebidos com radar sensível, observação disciplinada e ciclos rápidos de interpretação.

O **terceiro princípio** é a necessidade de antecipação estratégica. A ISO 31050 orienta que riscos emergentes devem ser tratados como potenciais transformadores do ambiente operacional e não apenas como eventos pontuais. Essa perspectiva exige integração com análise de cenários, exercícios de *foresight*, modelagem de impactos e avaliação de interdependências. Riscos emergentes são, em essência, sinais de mudanças futuras, e sua correta leitura pode transformar incertezas em vantagem competitiva.

Ao integrar essas diretrizes, o radar apresentado no início do capítulo torna-se não apenas uma ferramenta de monitoramento, mas um instrumento de resiliência adaptativa que ajuda organizações a identificar tendências, antecipar rupturas e preparar respostas antes que eventos se tornem crises.

5.8. O Ciclo de Inteligência para Identificação de Sinais Precoces

A detecção de riscos emergentes e sinais antecipatórios exige processo estruturado de inteligência que transforme dados dispersos em *insights* estratégicos. Esse processo, reforçado pela ISO 31050, pode ser organizado em quatro etapas contínuas.

A **primeira etapa** é o enquadramento. Nela, a organização define as perguntas críticas que orientam a busca por sinais: quais mudanças no ambiente podem alterar significativamente nossas operações, cadeias críticas ou estratégias. O enquadramento também determina prioridades, domínios de interesse, fronteiras de análise e o tipo de impacto que se deseja antecipar.

A **segunda etapa** é a coleta e verificação. Ela envolve a coleta sistemática de dados internos e externos, incluindo registros climáticos, incidentes digitais, informações de mercado, relatórios de órgãos públicos, movimentações sociais, ruídos regulatórios, atividades incomuns de fornecedores e eventos em regiões sensíveis. A verificação garante qualidade e confiabilidade, filtrando ruídos e destacando anomalias relevantes.

A **terceira etapa** é a interpretação. É aqui que sinais fracos se tornam inteligíveis. A interpretação envolve análise crítica, modelagem de riscos, cruzamento de variáveis, leitura de padrões, elaboração de hipóteses e uso de ferramentas de *foresight* para identificar possíveis trajetórias de risco. Muitas vezes, essa etapa requer uso de algoritmos de detecção de anomalias, análises comportamentais ou juízo especializado de equipes interdisciplinares.

A **quarta etapa** é a inteligência aplicada. Trata-se da transformação do conhecimento produzido em recomendações práticas, priorizações de investimento, decisões executivas e ajustes de estratégia. A inteligência aplicada garante que o radar não seja um processo meramente analítico, mas um mecanismo efetivo de tomada de decisão.

Quando operado de forma contínua, o ciclo de inteligência permite que organizações detectem riscos emergentes em estágios iniciais, reduzam incerteza, melhorem preparação e fortaleçam a resiliência. Ele funciona como elo entre monitoramento e ação e deve ser revisado periodicamente para incorporar novas fontes de dados, tecnologias, tendências e mudanças no ambiente externo.

5.9. Consolidação Final do Radar Antecipatório

A inclusão das orientações da ISO 31050 e a adoção do ciclo de inteligência ampliam significativamente a capacidade do radar para identificar riscos que se desenvolvem silenciosamente, muitas vezes imperceptíveis aos indicadores tradicionais. A combinação entre indicadores estruturais (itens 5.2. a 5.5.), interpretação integrada (item 5.6.) e mecanismos de antecipação estratégica (itens 5.7. e 5.8.) fornece uma estrutura robusta para detecção precoce de rupturas.

Esse radar expandido permite que organizações:

- Antecipem ciclos climáticos adversos antes de sua manifestação plena;
- Detectem pressões digitais e comportamentais que anunciam ataques cibernéticos sofisticados;
- Reconheçam fragilidades institucionais e tensões sociopolíticas antes de se tornarem crises;
- Identifiquem riscos sistêmicos em cadeias críticas com tempo suficiente para preparar redundâncias;
- Convertam sinais fracos em decisões preventivas e movimentos estratégicos.

Com isso, o Capítulo 5 se encerra mostrando que a verdadeira resiliência não depende apenas de respostas eficientes, mas da capacidade de **ler o futuro enquanto ele ainda está se formando**, princípio essencial da gestão de riscos emergentes e da inteligência estratégica alinhada à ISO 31050.

06

RECOMENDAÇÕES EXECUTIVAS E CAMINHOS FUTUROS

6.1. Introdução

O ambiente estratégico da América Latina em 2026 e nos anos subsequentes será moldado por combinações complexas de riscos climáticos, digitais, criminais e econômicos, intensificados por vulnerabilidades estruturais e fragmentação institucional. À luz das análises prospectivas, dos cenários construídos, da leitura setorial e do radar de sinais antecipatórios, torna-se evidente que organizações públicas e privadas precisam adotar uma postura mais dinâmica, preventiva e integrada. A capacidade de antecipar tendências, interpretar sinais fracos, fortalecer governança e construir resiliência passa a ser elemento central de competitividade e sobrevivência.

Este capítulo apresenta um conjunto estruturado de recomendações executivas que funcionam como transição natural entre os cenários prospectivos e os caminhos estratégicos de fortalecimento institucional, econômico e operacional. As recomendações estão organizadas em eixos que dialogam diretamente com os quatro quadrantes da matriz de cenários e com as fragilidades e oportunidades identificadas ao longo deste estudo.

6.2. Reforçar a Governança Estratégica de Riscos em Nível de Conselho

A primeira transformação necessária consiste em reposicionar a gestão de riscos como disciplina estratégica e não apenas operacional. Conselhos e comitês executivos devem incorporar análises de cenários, riscos emergentes, indicadores prospectivos e métricas de resiliência como elementos permanentes do processo decisório.

Para isso, recomenda-se:

- Incorporar relatórios periódicos de riscos emergentes e análises de sinais antecipatórios;
- Integrar ISO 31000 e ISO 31050 como base estruturante da governança;
- Criar agendas de risco dedicadas em reuniões de conselho;
- Definir responsabilidades claras entre conselho, diretoria e gestão operacional;
- Incluir análises de interdependências, efeitos em cascata e riscos sistêmicos.

A maturidade da governança passa a determinar a capacidade de adaptação às rápidas mudanças do ambiente.

6.3. Construir Resiliência em Infraestruturas Críticas e Cadeias Sensíveis

As análises deste relatório indicam que riscos climáticos e digitais serão os principais fatores de ruptura em cadeias produtivas, redes logísticas, portos, sistemas de energia, telecomunicações e abastecimento urbano. Por isso, recomenda-se a adoção de estruturas robustas de resiliência intersetorial.

As organizações devem:

- Ampliar redundâncias estruturais e tecnológicas;
- Fortalecer mecanismos de monitoramento contínuo de cadeias críticas;
- Integrar dados climáticos avançados e inteligência territorial na gestão operacional;
- Aprimorar planos de contingência considerando rupturas simultâneas;
- Desenvolver parcerias com governos e outros setores para proteção compartilhada de portos, rodovias e centros logísticos.

Organizações com atuação transnacional precisam ainda adotar protocolos regionais de resiliência, especialmente em operações que atravessam corredores sensíveis.

6.4. Aumentar a Maturidade Digital e a Governança de Inteligência Artificial

O avanço da digitalização, aliado à crescente sofisticação de ataques cibernéticos, exige que empresas e governos adotem modelos maduros de proteção de dados, sistemas críticos e estruturas de IA. Este relatório mostra que a América Latina permanece vulnerável tanto pela falta de padronização regulatória quanto pela adoção acelerada e, muitas vezes, descoordenada de novas tecnologias.

Recomenda-se:

- Implementação de políticas formais de governança de IA;
- Criação de mecanismos de auditoria algorítmica e explicabilidade;
- Segmentação avançada de redes e proteção de APIs;
- Uso de inteligência artificial defensiva integrada a centros de operação de segurança;
- Adoção de padrões internacionais de proteção de infraestrutura crítica digital;
- Redução de dependência de provedores únicos de nuvem;
- Treinamento contínuo para equipes de segurança cibernética e desenvolvimento.

Organizações maduras devem evoluir para modelos de segurança convergente, nos quais inteligência de risco, análise de anomalias e gestão digital são integradas ao nível executivo.

6.5. Adaptar-se ao Clima como Principal Multiplicador de Risco

O clima é, conforme demonstrado no Capítulo 5, o elemento de maior impacto transversal entre setores. Eventos extremos aumentam custos logísticos, pressionam energia, reduzem produtividade agrícola, fragilizam infraestruturas e desencadeiam crises sanitárias e sociais.

Para mitigar esses efeitos, recomenda-se:

- Fortalecer planos de adaptação climática no nível corporativo e setorial;
- Investir em infraestrutura resiliente e sistemas de drenagem;
- Incorporar dados climáticos e modelos preditivos nas operações;
- Adotar seguros paramétricos para riscos extremos;
- Desenvolver protocolos para trabalho em condições de calor severo;
- Mapear dependências hídricas e reduzir vulnerabilidades críticas.

No âmbito público, governos devem acelerar modernização de infraestrutura urbana, proteção de bacias hidrográficas, gestão de barragens e reforço de redes energéticas.

6.6. Enfrentar Redes Ilícitas e Fortalecer a Segurança Multidimensional

Os cenários apontam expansão de redes ilícitas transnacionais, aumento de confrontos, fragmentação institucional e infiltração criminosa em cadeias logísticas, especialmente em portos e fronteiras. A segurança corporativa passa a depender de respostas integradas envolvendo setor público, empresas, sociedade civil e cooperação internacional.

Recomendam-se ações como:

- Adoção de mecanismos de *due diligence* ampliada em fornecedores críticos;
- Integração entre segurança física, digital, ambiental e financeira;
- Uso de sistemas avançados de rastreabilidade de cargas e insumos;
- Fortalecimento de parcerias com autoridades policiais e aduaneiras;
- Criação de protocolos de inteligência corporativa focados em crime organizado;

- Desenvolvimento de sistemas de proteção para executivos, trabalhadores e operações em regiões remotas.

Organizações precisam tratar risco criminal como risco estratégico, não apenas operacional.

6.7. Harmonizar Regulação e Aprimorar Capacidade Estatal

A fragmentação regulatória descrita ao longo deste relatório eleva custos, gera incertezas e reduz competitividade. A região demanda movimentos de convergência regulatória para proteção de dados, Inteligência Artificial, cibersegurança, combate ao crime financeiro, infraestrutura crítica e governança ambiental.

Recomenda-se:

- Criar fóruns nacionais e regionais de harmonização regulatória;
- Fortalecer autonomia e capacidade técnica de agências reguladoras;
- Ampliar digitalização segura de serviços públicos;
- Investir em sistemas integrados de fiscalização ambiental e tributária;
- Acelerar processos legislativos que tratem de riscos emergentes.

A capacidade estatal de **aplicação efetiva da lei** *(enforcement)* é fundamental para sustentar crescimento econômico e estabilidade institucional.

6.8. Desenvolver Ecossistemas de Cooperação e Inteligência Coletiva

O ambiente de riscos híbridos exige colaboração constante entre setores. Nenhuma organização, pública ou privada, pode responder isoladamente a riscos sistêmicos. A integração entre empresas, governos, universidades, centros de pesquisa e organismos multilaterais fortalece soluções, cria padrões regionais e aumenta resiliência.

Recomenda-se:

- Criação de redes de inteligência compartilhada entre setores;
- Iniciativas de interoperabilidade de dados em infraestruturas críticas;
- Parcerias de inovação para desenvolvimento de tecnologias de detecção de riscos;
- Cooperação transfronteiriça para proteção de rotas logísticas e fronteiras;
- Participação ativa em consórcios e alianças regionais;

- Estímulo à pesquisa aplicada em clima, IA, segurança e infraestrutura.

Esses ecossistemas impulsionam capacidade coletiva de prevenção, resposta e recuperação.

6.9. Integrar *Foresight*, Cenários e Sinais Antecipatórios Como Processo Continuado

A ISO 31050 orienta que gestão de riscos emergentes deve ser apoiada por métodos contínuos de *foresight*, detecção de sinais fracos e interpretação dinâmica do ambiente.

O Capítulo 5 demonstrou que grande parte das rupturas em 2026 e além será precedida por micro indícios que exigem vigilância disciplinada.

Por isso, organizações devem:

- Institucionalizar exercícios de cenários e prospectiva;
- Criar rotinas de monitoramento de sinais fracos e *early warnings*;
- Atualizar periodicamente matrizes de impacto cruzado;
- Revisar planos estratégicos à luz de mudanças no ambiente;
- Ajustar critérios de risco para comportar incerteza profunda;
- Integrar equipes multidisciplinares de inteligência e risco.

A capacidade de antecipação torna-se eixo central da resiliência.

6.10. Caminhos Futuros: A Construção de um Horizonte de Resiliência para a América Latina

A América Latina possui alto potencial para transformar vulnerabilidades em oportunidades estratégicas. Os cenários apresentados mostram que, apesar da fragmentação institucional, a região reúne vantagens competitivas importantes em energia renovável, biodiversidade, agricultura avançada, mineração de alto valor, inovação digital e economia criativa.

Para aproveitar esse potencial, recomenda-se:

- Construir políticas públicas integradas de resiliência;
- Alinhar investimentos estratégicos com tendências globais de inovação;
- Posicionar a região como referência em governança de ia e sustentabilidade;
- Fortalecer cooperação regional para infraestrutura e segurança;

- Ampliar capacidade científica e tecnológica;
- Atrair parcerias internacionais para desenvolvimento sustentável.

O Brasil, como maior economia da região, tem papel decisivo na articulação desse horizonte estratégico, podendo liderar consórcios regionais de resiliência, padronização regulatória, proteção de infraestruturas críticas e inovação climática.

Tabela 18 – Quadro Resumo: Recomendações Executivas e Caminhos Futuros

Eixo Estratégico	Recomendação Central	Objetivo Principal	Por que é crítico para 2026 e além?
1. Governança de Riscos no Nível de Conselho	Integrar riscos emergentes, cenários e ISO 31050 à tomada de decisão	Fortalecer visão de longo prazo e reduzir pontos cegos estratégicos	Ambientes voláteis exigem decisões ancoradas em antecipação e resiliência
2. Resiliência de Infraestruturas Críticas	Proteger portos, energia, logística, telecom e abastecimento	Evitar rupturas sistêmicas e minimizar efeitos em cascata	Riscos climáticos e digitais aumentam falhas simultâneas na região
3. Maturidade Digital e Governança de IA	Estruturar políticas robustas de dados, IA e cibersegurança	Reduzir ataques, falhas e viés digital, preservando continuidade	América Latina é um dos principais alvos globais de ataques cibernéticos
4. Adaptação Climática Integrada	Incorporar modelos climáticos à operação e ao planejamento	Proteger produção, energia, logística e centros urbanos	Clima é o maior multiplicador de riscos da região
5. Combate a Redes Ilícitas e Crime Transnacional	Integrar segurança física, digital, territorial e financeira	Preservar cadeias críticas e reduzir exposição a ilícitos	Crescimento de facções e rotas ilegais afeta múltiplos setores
6. Harmonização Regulatória e Fortalecimento Estatal	Reduzir fragmentação e aumentar capacidade regulatória	Criar previsibilidade jurídica e capacidade de *enforcement*	Incerteza regulatória é um dos maiores riscos da América Latina
7. Ecossistemas de Cooperação	Criar redes público-privadas e alianças regionais de resiliência	Compartilhar inteligência e padronizar práticas	Nenhum ator isolado consegue enfrentar riscos híbridos
8. Integração de *Foresight*, Sinais Fracos e Prospectiva	Transformar o radar antecipatório em processo contínuo	Melhorar capacidade de detectar mudanças antes que se tornem crises	ISO 31050 reforça prospectiva como base da gestão de riscos emergentes

Eixo Estratégico	Recomendação Central	Objetivo Principal	Por que é crítico para 2026 e além?
9. Caminhos Futuros para a América Latina	Posicionar a região como líder em energia, IA, agricultura e sustentabilidade	Aproveitar vantagens competitivas e atrair investimentos	A região pode evoluir de vulnerável para protagonista global

07

CONCLUSÃO E APÊNDICES

Conclusão

A análise integrada realizada ao longo deste estudo revela uma América Latina que caminha para 2026 e além imersa em um ambiente de riscos híbridos, interdependentes e acelerados, no qual choques climáticos, fragilidades digitais, tensões sociopolíticas e pressões econômicas não apenas coexistem, mas se amplificam mutuamente. O exercício de cenários demonstrou que o futuro regional será moldado por forças que escapam aos modelos tradicionais de previsão e exigem abordagens dinâmicas, orientadas por inteligência e capazes de lidar com incerteza profunda.

A região enfrenta desafios estruturais, como fragmentação institucional, desigualdade, vulnerabilidade climática, expansão do crime transnacional e assimetrias tecnológicas. Esses elementos, quando combinados, aumentam a probabilidade de rupturas sistêmicas, especialmente em cadeias críticas como energia, logística, alimentação, telecomunicações, finanças e infraestrutura urbana. Ao mesmo tempo, a América Latina apresenta oportunidades expressivas em setores de alta relevância global, como agricultura sustentável, energia renovável, mineração estratégica e inovação digital. A trajetória para 2026 e além não será linear, mas marcada por disputas entre essas forças.

O estudo mostra que a resiliência organizacional dependerá menos da capacidade de reagir a crises e mais da habilidade de **interpretar sinais antecipatórios**, **detectar riscos emergentes**, **integrar cenários ao processo decisório** e **atuar com inteligência adaptativa**. A ISO 31050 reforça esse ponto ao destacar que riscos emergentes surgem inicialmente como sinais fracos, discretos, dispersos e ambíguos, que só podem ser compreendidos por organizações que adotam processos contínuos de *foresight* e inteligência de risco. Nesse sentido, o radar antecipatório apresentado no Capítulo 5 não é apenas um instrumento analítico, mas um mecanismo de sobrevivência institucional em um ambiente de mudanças rápidas e muitas vezes imprevisíveis.

Também se evidencia que a governança será o eixo decisivo de diferenciação entre organizações e países. A capacidade estatal de aplicação efetiva da lei, a previsibilidade regulatória, a coordenação institucional e a integridade pública tornam-se determinantes tanto para a segurança quanto para o crescimento econômico. Países com governanças frágeis enfrentarão maior exposição a redes ilícitas, volatilidade financeira, insegurança digital e conflitos territoriais. Países com governança mais sólida terão condições de liderar agendas de resiliência, inovação e integração regional.

As empresas também precisam reposicionar sua visão estratégica. Modelos tradicionais de segurança, continuidade e gestão de riscos não são mais suficientes diante de ameaças que atravessam simultaneamente ambientes físicos, digitais, reputacionais e

climáticos. Organizações resilientes serão aquelas que adotarem segurança convergente, governança robusta de IA, proteção de infraestruturas críticas, autonomia digital, diversificação de cadeias produtivas e mecanismos adaptativos de resposta.

O estudo deixa claro que o clima será o maior multiplicador de riscos na região. A combinação de ondas de calor, eventos extremos, perda hídrica, incêndios e impactos sobre agricultura e energia afetará diretamente a competitividade regional. Ao mesmo tempo, abre espaço para oportunidades de liderança em bioeconomia, energias limpas, agricultura de precisão, infraestrutura resiliente e tecnologias verdes. A capacidade de adaptação climática será medida pela rapidez com que governos e empresas incorporarem inteligência climática às suas decisões.

No campo digital, os riscos evoluem em velocidade ainda maior. A América Latina permanece entre as regiões mais atacadas do mundo, e a adoção acelerada de Inteligência Artificial – sem mecanismos maduros de governança – amplia não apenas vulnerabilidades técnicas, mas riscos éticos, legais e reputacionais. A maturidade digital já não é diferencial competitivo, mas condição mínima para operação. Organizações que não evoluírem para modelos de proteção integrados, com automação defensiva, auditoria algorítmica e segmentação avançada, enfrentarão interrupções, fraudes e exposição sistêmica.

Quando confrontamos todos esses elementos – clima, tecnologia, crime, governança e economia – percebemos que a América Latina não enfrenta apenas riscos isolados, mas um **novo regime de risco**, caracterizado por simultaneidade, velocidade, interdependência e profundidade transformacional. Essa combinação exige que governos, empresas e sociedade adotem postura mais madura, colaborativa e orientada pela construção de capacidades estruturantes de longo prazo.

A conclusão mais contundente deste estudo é que **o maior risco da América Latina não é climático, nem digital, nem econômico; é a falta de integração entre eles**. O risco sistêmico surge justamente da incapacidade coletiva de compreender como essas dimensões se alimentam mutuamente e exigem respostas coordenadas. A região poderá caminhar para ciclos recorrentes de crise, ou poderá se transformar em referência global de resiliência e inovação, dependendo da qualidade das decisões tomadas hoje.

Em síntese, o futuro da América Latina será definido por três forças centrais: **a capacidade de antecipar, a capacidade de cooperar e a capacidade de adaptar**. Organizações que combinarem inteligência de risco, governança estratégica, resiliência operacional e visão de longo prazo poderão não apenas sobreviver, mas liderar a

transformação. Aquelas que permanecerem ancoradas em modelos reativos enfrentarão um ambiente cada vez mais hostil, instável e imprevisível.

Mais do que apontar riscos, este estudo evidencia caminhos. A região tem potencial para evoluir de um território marcado por vulnerabilidades para um polo global de soluções em segurança, sustentabilidade, energia, tecnologia e agricultura. O futuro ainda não está definido. Ele será moldado pela capacidade de governos, empresas e instituições de transformar incerteza em estratégia, turbulência em inovação e riscos emergentes em vantagem competitiva.

Apêndice A – Metodologia Utilizada

A construção deste estudo seguiu uma abordagem metodológica ancorada nos princípios da ISO 31000 e, sobretudo, da ISO 31050, que estabelece diretrizes específicas para a identificação, análise e gerenciamento de riscos emergentes em ambientes caracterizados por alta complexidade, incerteza estrutural e interdependência sistêmica. Todo o processo analítico adotou como técnica central o *horizon scanning*, compreendida como uma metodologia sistemática de varredura de evidências, tendências e sinais antecipatórios provenientes de múltiplas fontes, com o objetivo de identificar elementos que possam influenciar o ambiente de riscos no horizonte de médio prazo.

O *horizon scanning* foi aplicado envolvendo a coleta, leitura, categorização temática e comparação cruzada de trinta e dois relatórios nacionais e internacionais publicados entre 2024 e 2025. Esse conjunto formou a base documental primária e foi tratado como corpus de evidências para interpretação prospectiva. O processo iniciou-se com a extração e organização sistemática dos elementos-chave de cada documento, incluindo riscos emergentes, tendências estruturais, indicadores, incertezas críticas e mudanças em curso. A partir desse material bruto, foram criados cartões-fonte que permitiram realizar uma leitura transversal padronizada das contribuições originais, em linha com as recomendações da ISO 31050 para redução de viés de seleção e ampliação da diversidade informacional.

Após essa etapa de mapeamento exploratório, foi conduzida uma análise de triangulação estrutural de fontes, utilizada como técnica complementar essencial para garantir robustez e coerência. A triangulação consistiu em confrontar sistematicamente os achados dos diferentes relatórios, identificando convergências recorrentes, divergências significativas e lacunas temáticas. Essa comparação cruzada permitiu validar a consistência interna dos achados, reduzir o risco de superinterpretação de evidências isoladas e assegurar que as conclusões derivassem de padrões amplos e não de opiniões ou tendências específicas de uma única instituição. Esse método é amplamente reconhecido nos estudos de riscos emergentes e encontra correspondência direta com a ênfase da ISO 31050 na multi-perspectividade e na integração de fontes heterogêneas.

Durante todo o processo analítico, foi utilizado apoio de Inteligência Artificial como ferramenta de organização, clusterização preliminar de temas e identificação de padrões semânticos entre as fontes. Seu papel foi restrito à etapa de processamento e ordenação das evidências, fornecendo uma base estruturada sobre a qual a equipe analítica pôde atuar com maior precisão.

A etapa subsequente consistiu na síntese interpretativa, na qual foram consolidadas **seis fontes de risco críticas** derivadas da análise cruzada. Essa síntese seguiu os princípios da ISO 31050 ao integrar riscos de natureza tecnológica, climática, geopolítica, institucional, criminal e infraestrutural, reconhecendo que riscos emergentes raramente operam isolados e tendem a se manifestar de forma convergente, acumulativa e não linear. Em conformidade com a abordagem sistêmica da norma, foram privilegiadas interpretações capazes de capturar interdependências, tensões e combinações de riscos com potencial de produzir efeitos amplificados.

Ao longo do estudo, essas seis fontes de risco são tratadas como o núcleo estrutural das dinâmicas de risco regional, razão pela qual são denominadas **fontes de risco críticas**.

A partir dessas **seis fontes de risco críticas**, foram desenvolvidos quadros prospectivos que culminaram na elaboração da Matriz de Cenários 2026. A técnica de cenários, recomendada pela ISO 31050 para lidar com incertezas profundas, foi aplicada de forma qualitativa e interpretativa, utilizando os eixos de maior tensão identificados pelo *horizon scanning*. Os cenários resultantes não têm caráter preditivo, mas sim exploratório, com o objetivo de ampliar a capacidade decisória, identificar vulnerabilidades sistêmicas e antecipar possíveis futuros que impactem organizações públicas e privadas no Brasil e América Latina.

Por fim, o estudo passou por um processo de revisão técnica e validação externa, no qual versões parciais e a versão final foram submetidas a especialistas de diferentes países da América Latina, garantindo diversidade de perspectivas regionais. Essa revisão crítica teve como propósito avaliar a coerência dos achados, a robustez das inferências, a clareza conceitual e a aderência às práticas internacionais de análise prospectiva. As contribuições provenientes dessa etapa foram incorporadas para fortalecer o rigor metodológico e assegurar que o documento final represente uma interpretação sólida e defensável do ambiente de riscos projetado para 2026 e anos subsequentes.

Esse processo metodológico, integralmente fundamentado em *horizon scanning*, triangulação de fontes e análise qualitativa em conformidade com a ISO 31050, oferece uma estrutura de trabalho transparente e alinhada às melhores práticas internacionais para estudos de riscos emergentes de natureza sistêmica e prospectiva.

Limitações do Estudo e Escopo de Uso

Este estudo adota uma abordagem prospectiva, qualitativa e exploratória, alinhada aos princípios da ISO 31000 e às diretrizes específicas da ISO 31050 para a análise de riscos emergentes e cenários de incerteza profunda. Por essa razão, é fundamental esclarecer explicitamente suas limitações e o escopo adequado de uso de suas conclusões. O

objetivo central do estudo não é prever o futuro, estabelecer probabilidades matemáticas de eventos nem formular modelos econométricos ou projeções quantitativas. Seu propósito é ampliar a capacidade decisória de organizações públicas e privadas por meio da identificação de tendências estruturais, mapeamento de riscos convergentes, análise sistêmica e construção de cenários plausíveis que sirvam como base para planejamento estratégico, antecipação de ameaças e fortalecimento de resiliência institucional.

A metodologia empregada, fundamentada em *horizon scanning*, triangulação de fontes e análise interpretativa, privilegia a integração de múltiplas perspectivas e a identificação de padrões emergentes em um ambiente de incerteza, mas não tem a pretensão de oferecer previsões determinísticas, cálculos de probabilidade ou mensurações estatísticas de impacto. Essas abordagens, embora valiosas em outros contextos, seriam inadequadas para o tipo de fenômeno analisado, caracterizado por interdependência sistêmica, dinâmicas não lineares e eventos potencialmente disruptivos que escapam a modelos quantitativos tradicionais.

As conclusões apresentadas refletem uma síntese qualificada das evidências disponíveis no momento da elaboração do estudo, considerando os limites naturais das fontes utilizadas, bem como o fato de que tendências e riscos emergentes podem evoluir de forma rápida e inesperada. Assim, recomenda-se que os achados sejam utilizados como insumo estratégico complementar, e não como única base para decisões críticas. O estudo não substitui análises setoriais específicas, avaliações quantitativas internas, diagnósticos regulatórios ou estudos técnicos especializados em áreas como macroeconomia, clima, criminalidade ou tecnologia da informação.

Finalmente, por se tratar de um documento prospectivo, suas recomendações devem ser periodicamente revisitadas, ajustadas e validadas à luz de novos dados, mudanças geopolíticas e transformações tecnológicas. A utilidade do estudo reside justamente em sua capacidade de orientar decisões em contextos de incerteza, oferecer referências claras para monitoramento contínuo e sustentar processos de resiliência organizacional, e não em fornecer respostas definitivas sobre futuros específicos. Dentro desses limites, o estudo permanece plenamente coerente, metodologicamente sólido e adequado ao seu propósito estratégico.

Apêndice B – Lista de Fontes Consultadas

Este estudo baseia-se na análise aprofundada de **32 relatórios nacionais e internacionais publicados entre 2024 e 2025**, selecionados por sua relevância metodológica e capacidade de iluminar tendências, fontes de risco e transições sistêmicas pertinentes ao horizonte prospectivo de 2026 e além.

A matriz analítica utilizada neste Relatório divide o conjunto de ameaças e tendências em seis Fontes de Risco, conforme definido no item 1.4.

Para as definições completas das Fontes de Risco (1 a 6) e dos Cenários Estruturantes (1 a 4), consulte os itens 1.4. e 1.5.

Tabela 19 – Relatórios e Eixos de Contribuição

Nº	Relatório/ Documento	Organização	Ano	Fontes de Risco Contribuintes	Cenários Contribuintes
1	*Global Risk Report 2024*	United Nations	2024	(i), (iv)	Cenário 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)	Cenário 2
4	*Global Trends 2040*	U.S. Intelligence Community	2021	(i), (ii)	Cenário 1
5	*Strategic Outlook 2025*	Think Tank Internacional	2025	(i), (vi)	Cenário 3
6	*Strategic Intelligence Estimate 2025*	Think Tank Militar / Inteligência	2025	(i), (ii)	Cenário 2
7	*Risk Report 2025*	Corporate & Economic Analysis	2025	(vi), (iv)	Cenário 4
8	*Polycrisis Introduction 2024*	Vários Autores / Policrises	2024	(i), (vi)	Matriz (riscos convergentes)
9	*Cenário Macroeconômico Global e Brasil 2025*	Instituição Econômica Brasileira	2025	(i), (vi)	Cenário 3
10	*FUSk - Fundación Sherman Kent – Primer Informe*	FUSK	2024 – 25	(vi), (iii)	Cenário 2
11	*Risk in Focus: Latin America 2026*	Corporate LATAM	2025	(vi), (iii)	Cenário 2

Nº	Relatório/ Documento	Organização	Ano	Fontes de Risco Contribuintes	Cenários Contribuintes
12	*Riesgo Político América Latina 2025*	CEIUC	2025	(vi), (i)	Cenário 2
13	*Global Riesgo Pronóstico 2025*	Crisis24	2025	(vi), (iii)	Cenário 2
14	*Global Safety Report 2025*	Gallup	2025	(vi), (iii)	Cenário 2
15	*Global Organized Crime Index 2025*	GI-TOC	2025	(iii), (vi)	Cenário 2
16	*2025 Security Benchmark Report*	Corporate Security Benchmark	2025	(v), (iii)	Cenário 4
17	*2025 CSO Survey*	Clarity Factory	2025	(v), (ii)	Cenário 1
18	*The State of Financial Crime 2025*	Consultoria Financeira Internacional	2025	(iii), (ii)	Cenário 2
19	*Global Terrorism Index 2025*	IEP	2025	(iii), (i)	Cenário 2
20	*Relatório Global de Auditoria Interna 2025*	IIA	2025	(vi), (ii)	Cenário 1
21	*Internal Audit Global Hot Topics 2025*	IIA	2025	(ii), (iii)	Cenário 4
22	*Propuesta Agers–IAI V5*	Agers / IAI	2025	(iv), (v)	Cenário 3
23	*Communications Security Annual Report 2024*	Communications Security Group	2024	(ii), (v)	Cenário 4
24	*Global Cybersecurity Outlook 2025*	WEF	2025	(ii), (v)	Cenário 4
25	*AI & Cybersecurity Report 2025*	WEF	2025	(ii), (v)	Cenário 1
26	*Microsoft Digital Defense Report 2025*	Microsoft	2025	(ii), (iii)	Cenário 2
27	*AI Security Framework*	IA Security Consortium	2025	(ii), (v)	Cenário 4
28	*Risk Radar 2025*	Healix	2025	(iv), (vi)	Cenário 3

Nº	Relatório/ Documento	Organização	Ano	Fontes de Risco Contribuintes	Cenários Contribuintes
29	*The Future of the Risk Management Profession 2025*	Consultoria Especializada	2025	(ii), (vi)	Cenário 1
30	*Estudo t-Risk – Riscos Corporativos 2025*	Plataforma t-Risk	2025	(v), (ii)	Apoio transversal
31	*Risk in Focus 2026 – Middle East. 2025*	IIA	2025	(ii), (vi)	Cenário 1
32	*White papers e briefs adicionais (IA–Cyber)*	WEF	2025	(ii), (v)	Cenários 1 e 4

Apêndice C – Glossário de Siglas

O presente glossário reúne as siglas utilizadas ao longo deste estudo e tem como objetivo apoiar a leitura técnica, reduzir ambiguidade e reforçar a coerência conceitual com as normas de gestão de riscos da família ISO 31000 e com a ABNT. Os significados são apresentados em português, com indicação do termo original quando relevante, e sempre contextualizados ao uso específico neste relatório.

Tabela 20 – Glossário de Siglas

Sigla	Termo por extenso	Definição aplicada neste estudo
ABNT	*Associação Brasileira de Normas Técnicas*	Entidade responsável pela normalização técnica no Brasil, incluindo a adoção nacional das normas ISO de gestão de riscos, como ABNT NBR ISO 31000 e ABNT ISO/TS 31050.
COSO	*Committee of Sponsoring Organizations of the Treadway Commission*	Estrutura de referência internacional para gestão de riscos corporativos e controles internos, utilizada aqui como base para discutir maturidade de governança de riscos, especialmente em serviços financeiros e no setor corporativo em geral.
ESG	*Ambiental, Social e Governança (Environmental, Social and Governance)*	Abordagem integrada de avaliação de desempenho de organizações em aspectos ambientais, sociais e de governança. No estudo, ESG aparece como eixo de pressão regulatória, de risco reputacional e de vantagem competitiva em diversos setores, como agronegócio, energia e finanças.
ERM	*Enterprise Risk Management*	Modelo de gestão de riscos em nível corporativo, que integra riscos estratégicos, operacionais, financeiros, de conformidade e de reputação. O estudo dialoga com o conceito de ERM ao propor uma visão integrada de cenários, setores e continuidade de negócios.
EUA	*Estados Unidos da América*	Principal referência de comparação internacional para capacidades de segurança, inovação tecnológica, mercado financeiro e governança de riscos, especialmente nos capítulos setoriais.
EUI	*União Europeia (em inglês European Union, UE em português)*	Bloco regional utilizado como referência para padrões regulatórios, governança climática, proteção de dados, auditoria algorítmica e integração de cadeias produtivas. No texto em português é referido, como União Europeia.
EWI	*Early Warning Indicator (Indicador de Alerta Precoce)*	Indicadores quantitativos ou qualitativos desenhados para captar sinais antecipatórios de mudanças de cenário, ruptura ou deterioração de risco. No relatório, os

Sigla	Termo por extenso	Definição aplicada neste estudo
		EWI são organizados em um radar de sinais para apoiar monitoramento estratégico contínuo.
GI-TOC	*Global Initiative Against Transnational Organized Crime*	Organização internacional que produz o Global *Organized Crime Index*. Neste estudo, GI-TOC é referência empírica para análise de crime organizado transnacional, mercados ilícitos e seus impactos na América Latina.
GRC	*Governance, Risk and Compliance*	Abordagem integrada de governança, gestão de riscos e conformidade. Embora o foco do relatório seja macro estratégico, GRC aparece como referência de estrutura organizacional para conectar riscos, controles, auditoria e segurança corporativa.
IA	*Inteligência Artificial*	Conjunto de técnicas computacionais de aprendizado de máquina, modelos estatísticos e sistemas automatizados de decisão, que ampliam eficiência e também introduzem novos riscos digitais, éticos, regulatórios e de segurança, em especial em ambientes de alta complexidade e interdependência.
IAG	*Inteligência Artificial Generativa*	Subconjunto da Inteligência Artificial capaz de gerar textos, imagens, voz, código e outros conteúdos com base em grandes modelos de linguagem ou modelos multimodais. No estudo, IAG é tratada como vetor tanto de inovação quanto de risco, especialmente em fraudes digitais, desinformação e *deepfakes*.
ICS	*Industrial Control Systems (Sistemas de Controle Industrial)*	Conjunto de sistemas, sensores, atuadores e softwares que controlam processos físicos em indústrias, energia, saneamento, transporte e outras infraestruturas críticas. São alvos prioritários de ataques cibernéticos que podem gerar impactos físicos relevantes na operação.
ICS-5	*Integrated Corporate Security em cinco camadas*	Estrutura conceitual utilizada no estudo para organizar segurança corporativa em cinco camadas integradas: governança e estratégia; proteção de pessoas e ativos físicos; segurança digital e de dados; gestão de fornecedores e cadeia de valor; inteligência de riscos e continuidade de negócios. Funciona como referência para arquiteturas de segurança convergente.
IoT	*Internet das Coisas (Internet of Things)*	Rede de dispositivos físicos conectados que coletam e transmitem dados, muitas vezes associados a sensores em ambientes industriais, urbanos, logísticos ou de consumo. No estudo, aparece como vetor de aumento de superfície de ataque cibernético e de complexidade operacional.

Sigla	Termo por extenso	Definição aplicada neste estudo
ISO	*International Organization for Standardization*	Organização internacional que desenvolve normas técnicas, incluindo a ISO 31000 e a ISO/TS 31050, referências centrais para a abordagem de gestão de riscos e riscos emergentes adotada neste relatório.
ISO 31000	*ISO 31000: Gestão de Riscos Diretrizes*	Norma internacional que estabelece princípios, estrutura e processo para gestão de riscos. No estudo, é o arcabouço geral de referência para o processo de gestão de riscos corporativos e para a lógica de fontes de risco, análise, avaliação e tratamento.
ISO/TS 31050	*ISO/TS 31050: Gestão de Riscos emergentes*	Especificação técnica que oferece orientações complementares à ISO 31000 para lidar com riscos emergentes, incerteza estrutural, sinais antecipatórios e *foresight*. Sustenta metodologicamente o uso de cenários, radar de sinais e exercícios de *foresight* neste relatório.
IT	*Information Technology (Tecnologia da Informação)*	Conjunto de infraestruturas, redes, sistemas e aplicações digitais voltados ao processamento, armazenamento e transmissão de dados. Aparece em contraste e integração com OT em ambientes de manufatura, energia, finanças e serviços digitais.
KYC	*Know Your Customer*	Conjunto de procedimentos e controles para conhecer, validar e monitorar clientes. No contexto de serviços financeiros e combate a crimes financeiros, é um pilar de prevenção à lavagem de dinheiro, financiamento ao terrorismo e fraudes.
KPI	*Key Performance Indicator (Indicador-chave de Desempenho)*	Indicadores utilizados para monitorar desempenho e resultados organizacionais. No estudo, são mencionados em contraste com indicadores de risco e com EWI, que têm foco preditivo e de alerta.
OCDE	*Organização para a Cooperação e Desenvolvimento Econômico*	Organismo internacional que produz estudos e benchmarks sobre economia, comércio, governança e integridade. No relatório, é referência para análises de comércio internacional, fluxos de bens, padrões regulatórios e indicadores econômicos.
OEA	*Organização dos Estados Americanos*	Organismo regional que reúne países do continente americano. No estudo, aparece como referência institucional ligada à governança democrática, à estabilidade política e à cooperação regional.
ONU	*Organização das Nações Unidas*	Organização internacional que apoia cooperação entre Estados em temas como paz e segurança, direitos humanos, desenvolvimento e clima. É fonte de dados e

Sigla	Termo por extenso	Definição aplicada neste estudo
		relatórios utilizados como insumo para o panorama global e para riscos climáticos, migratórios e humanitários.
OT	*Operational Technology (Tecnologia Operacional)*	Tecnologias associadas à operação de processos físicos, como sistemas de controle, sensores industriais e automação de plantas produtivas. Quando integradas com TI, ampliam tanto a eficiência quanto o risco, especialmente em segurança cibernética de infraestruturas críticas.
OT / IT	*Integração entre Operational Technology e Information Technology*	Expressão usada para caracterizar ambientes em que sistemas industriais e sistemas de informação estão cada vez mais conectados. Essa integração aumenta eficiência, porém expande a superfície de ataque cibernético e exige governança de riscos integrada.
PIB	*Produto Interno Bruto*	Medida do valor total de bens e serviços produzidos em uma economia. Utilizada no estudo para discutir crescimento econômico, capacidade de investimento e impacto de choques de risco em diferentes países e regiões.
UE	*União Europeia*	Bloco de países europeus, utilizado como referência de comparação em clima, regulação tecnológica, proteção de dados, governança de IA, padrões ambientais e modelos de integração econômica e regulatória.
WEF	*World Economic Forum (Fórum Econômico Mundial)*	Organização internacional que produz o *Global Risks Report* e outros estudos sobre riscos globais, tecnologia, economia e governança. É uma das principais fontes deste relatório para análise de tendências sistêmicas e riscos emergentes.

Apêndice D – Créditos e Agradecimentos

A elaboração deste **Estudo de Cenários de Riscos e Estratégias para 2026 e Além – Brasil e América Latina** somente foi possível graças à contribuição técnica, intelectual e institucional de diversos profissionais, organizações parceiras e especialistas que dedicaram tempo, conhecimento e análises críticas.

Este documento consolida mais de um ano de observação contínua, consultas a fontes internacionais, análises comparativas, exercícios de *foresight* e integração das metodologias previstas na ISO 31000 e na ISO/TS 31050. Sua construção exigiu rigor metodológico, interdisciplinaridade e um esforço colaborativo permanente.

A **Plataforma t-Risk** agradece profundamente a todos que contribuíram para este estudo, seja na fase de coleta de dados, revisão técnica, leitura crítica ou validação dos cenários prospectivos.

Equipe de Pesquisa e Análise

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

Revisão Técnica, Metodológica e Contribuições

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

- Diego Escobal – Diretor de Vea Consultoria de Segurança
  LinkedIn: https://www.linkedin.com/in/diegoescobaldigitalizacion/
- Diego Serpa, CPP – Gerente de Segurança na 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 e Gestor em Segurança da Informação na Núcleo Consultoria em Segurança
  LinkedIn: https://www.linkedin.com/in/edisonfontes/
- Hélio Jorge Paixão – Assessor de Informações Estratégicas no 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 – Sócio Consultor na Núcleo Consultoria em Segurança
  LinkedIn: https://www.linkedin.com/in/jo%C3%A3o-jaouiche-38bb0a69/
- Marcelo de Sá Dias – Auditor de Conformidade, Pós-graduado em Administração de Empresas pela FAAP e em Direção de Segurança Empresarial pela Universidade Comillas
  LinkedIn: https://www.linkedin.com/in/marcelo-de-s%C3%A1-6bb0a458/
- Ricardo Franco Coelho – Administrador de Empresas na TrendServ Multiserviços Corporativos
  LinkedIn: https://www.linkedin.com/in/ricardofcoelho/
- Ricardo Oscar Botta, CPP – Head Consultant na LatinRisk Argentina
  LinkedIn: https://www.linkedin.com/in/ricardo-botta/
- Ronivon Alves de Oliveira – Coordenador de segurança Empresarial na Lundin Mining e Diretor do Comitê de Segurança na Mineração na ABSEG
  LinkedIn: https://www.linkedin.com/in/ronivon-oliveira-cpai-2a95aa36/
- Víctor Escobal Morales – Diretor VEA Consultores de Riesgos
  LinkedIn: https://www.linkedin.com/in/v%C3%ADctor-escobal-morales-807b953/
- Wanderson Gloor – Diretor Unidade de Negócios São Paulo na Anjos da Guarda
  LinkedIn: https://www.linkedin.com/in/wandersongloor/

Editoração e Desenho Gráfico

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

Agradecimento Especial

A **Plataforma t-Risk** reconhece o apoio de todos aqueles que contribuíram com *insights*, documentos, dados, críticas construtivas e validações metodológicas ao longo do desenvolvimento deste relatório. A pluralidade de perspectivas e a colaboração entre especialistas de diferentes setores fortaleceram a precisão e a utilidade estratégica deste estudo.

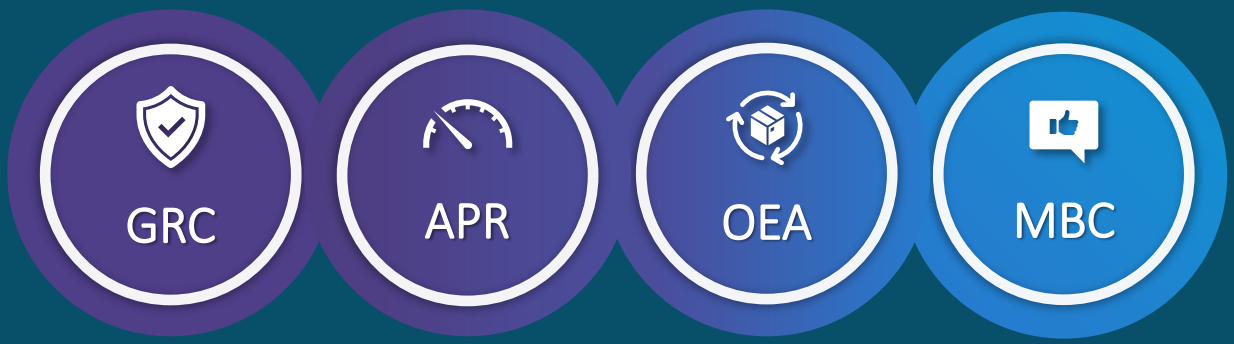
Agradecemos também às instituições nacionais e internacionais que disponibilizam publicamente seus relatórios de riscos, permitindo que análises como esta sejam construídas com base em evidências sólidas e comparáveis.

Nota Final

Este estudo representa um esforço contínuo de inteligência de riscos e antecipa um futuro marcado por complexidade, incerteza e interdependência. A t-Risk mantém o compromisso de atualizar periodicamente suas análises e seguir contribuindo para o fortalecimento da capacidade de resiliência das organizações brasileiras e latino-americanas.

Softwares t-Risk

Conheça todos os módulos e ferramentas da Plataforma Total Risk.



Módulo Gestão de Riscos Corporativos

Gestão de riscos integrados e estratégicos.

Módulo Análise Preliminar de Riscos

Análise prévia e operacional dos riscos.

Módulo Operador Econômico Autorizado

Gerenciamento dos riscos logísticos - OEA.

Módulo Background Check

Due Diligence Digital para gestão de riscos de terceiros.

Módulo Avaliação de Maturidade

Análise do nível de maturidade organizacional em gestão de riscos.

Módulo AVSEC Aeroportos

Gestão de riscos de segurança da aviação civil (Security).

Aplicativo de Avaliação de Riscos

APP mobile completo para identificação de riscos.

IA Vision Pro

Inteligência Artificial criada pela t-Risk para potencializar a gestão de riscos corporativos.


TURBINE SUAS ANÁLISES DE RISCOS
COM A INTELIGÊNCIA ARTIFICIAL DA
T-RISK!
Acesse agora mesmo e
confira mais essa novidade.
CLIQUE AQUI

www.totalrisk.com.br

· 2026 ·