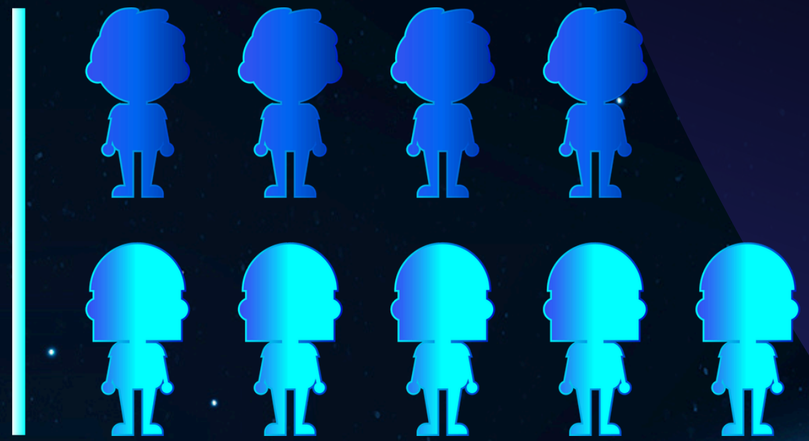
Child Online Safety and Critical Infrastructure Protection

Risks, Frameworks, and Policy Responses

Belisario Contreras

Introduction



Digital connectivity is rapidly expanding across Latin America, creating significant opportunities for inclusion, education, and economic growth.

At the same time, children face growing risks online including exploitation, harmful content, privacy violations, and cyberbullying.

This presentation examines regional gaps, international frameworks, and practical policy solutions for harmonized child online protection.

Why Child Online Protection Matters

01

Tech Reliance

Children increasingly rely on digital services for education, communication, entertainment, and civic participation.

02

Development

Internet access is now closely tied to social and economic development.

03

Emerging Tech

The rapid growth of AI, algorithmic systems, and connected platforms is reshaping online risks and opportunities.

Governments must balance meaningful connectivity with safety, privacy, and digital rights protections.

The Risk Landscape

Harms are growing in scale and complexity, especially as platforms and AI reshape the digital ecosystem.

Cyberbullying & Harassment

Psychological abuse, humiliation, intimidation, and peer-to-peer harms.

Disinformation

Manipulation, polarization, and degraded information quality.

Privacy & Data Misuse

Overcollection, profiling, behavioral advertising, and weak safeguards.

Online grooming & CSEA

Cross-border exploitation, abuse material, and predatory contact.

Harmful Content

Self-harm, sexual content, violence, and age-innapropriate materials.

Algorithmic Amplification

Systems that intensify exposure to harmful or addictive content.

Key Gaps & Tensions

01 Inconsistent definitions for “child,” “adolescent,” harmful content, and age thresholds.

02 Divergent platform obligations and unclear responsibilities for device manufacturers, ISPs, and digital services.

03 Limited child-specific cybersecurity strategies and uneven enforcement capacity.

04 Slow or inconsistent cross-border cooperation for evidence sharing, takedowns, traceback, and mutual legal assistance.

05 Balancing child safety with privacy, freedom of expression, and access to information remains a major policy challenge.

Core Tension:

Protect children without weakening privacy, expression, or meaningful access.

The answer is nuanced, rights-respecting design — not blunt content blocking.

Pathway to Regional Harmonization

01 Legal/Regulatory Harmonization

Model COP framework including harmonized definitions, minimum safeguards, reporting duties, and due-process safe harbors.

02 Technical interoperability

Shared incident schemas, secure evidence exchange, transparency APIs, and age-appropriate design standards.

03 Cross-boarder Cooperation

COP-focused MLA templates, urgent escalation channels, and designated online safety focal points.

04 Capacity-building

Regional training for judges, prosecutors, CERTs, regulators, and child protection organizations.

05 Multistakeholder governance

Oversight bodies, child participation, public reporting, peer learning, and human rights impact assessments.

06 Privacy-protecting safeguards

Risk-based methods using data minimization, age ranges, and minimal-attribute attestations.

Child Online Safety

Protecting children online is an ongoing commitment, not a one-time regulatory project.

Alignment:

Countries should align around shared principles while maintaining flexibility for domestic implementation.

Embed Safety:

Industry should embed safety- and privacy-by-design into products and services used by children.

Participation:

Resource civil society, educators, parents, child protection organizations, and children themselves.

Coordination:

Regional cooperation, technical coordination, and inclusive governance are essential to building safer digital environments.

Reevaluation:

Revisit principles as technology and safety evolve.

Critical Infrastructure Protection

01

Plan for OT Security

Organizations should establish clear ownership, accountability, and governance structures for operational technology security.

02

Map IT/OT Convergence

Operators should identify where IT and OT systems intersect and implement controls that reflect the risks of integrated environments.

03

Secure the Supply Chain

Governments and operators should establish baseline cybersecurity requirements across suppliers, vendors, and service providers.

04

Adopt Secure-by-Design Principles

Security should be embedded into technologies and services from the earliest stages of development and deployment.

05

Strengthen Incident Response

Organizations should improve information sharing, recovery planning, and coordinated response mechanisms.

06

Invest in Workforce Development

Countries should expand cybersecurity education, training programs, and OT-specific workforce initiatives.

Critical Infrastructure Protection

Protecting critical infrastructure is not simply a cybersecurity challenge; it is a strategic imperative for economic stability, public safety, and long-term national resilience.

Critical infrastructure security is increasingly central to economic development, public safety, and national resilience throughout Latin America.

The growing convergence of operational technology, cloud services, artificial intelligence, and global supply chains has transformed the threat landscape and expanded the attack surface facing essential sectors.

While governments and operators across the region have made meaningful progress, persistent gaps remain in operational technology security, supply chain risk management, workforce capacity, and coordinated incident response.

Building resilience will require sustained collaboration between governments, infrastructure operators, technology providers, and international partners.

Conclusions for Brazil

01

Clear governance and institutional responsibilities

Definitions of critical infrastructure and regulated entities should align with existing legal frameworks and clearly delineate institutional responsibilities to avoid overlap, regulatory conflict, and legal uncertainty.

02

Adopt a risk-based approach

Cybersecurity obligations should be proportionate to actual cyber risk, particularly regarding supply chain security, vulnerability management, and compliance obligations. Resources should focus on the systems and suppliers that present the greatest operational risk.

03

Recognize shared responsibility

Modern digital services—including cloud computing and managed services—operate through shared responsibility models. Effective legislation should allocate responsibilities clearly among service providers, operators, and customers rather than assuming one party controls every aspect of cybersecurity.

04

Promote legal certainty and practical implementation

Clear definitions, predictable compliance requirements, reasonable implementation timelines, and proportionate enforcement encourage investment, innovation, and stronger long-term cybersecurity outcomes.