DIGI AMERICAS ALLIANCE MEMBERS

Apple aws Batuta CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE
fluid attacks we hack your software Google kriptos LUMU netskope paloalto NETWORKS
Resecurity Schneider Electric SISAP Sistemas Aplicativos SOPHOS tenable Trellix TrendAI

COLOMBIA: OECD PRESENTS DIAGNOSIS ON DIGITAL CONNECTIVITY AND COMMUNICATIONS MARKETS

trendTIC – The Organisation for Economic Co-operation and Development (OECD) yesterday presented the report “Digital Connectivity Review in Colombia,” a diagnostic study analyzing the transformation of communications markets in the country and offering guidelines to strengthen competition, investment, and digital inclusion. The presentation took place within the framework of the Colombia Digital Summit 2026, a regional meeting in Cartagena that brings together authorities, regulators, international experts, and leaders from the technology sector to discuss connectivity, regulation, artificial intelligence, and the digital economy.

THE 2026 WORLD CUP TRIGGERS ALERTS ABOUT DIGITAL SCAMS IN MEXICO

Addictware - The 2026 World Cup, hosted by Mexico, the USA, and Canada, is considered by cybersecurity experts to be a high-risk digital event due to the enormous economic and digital activity it generates through ticket sales, streaming subscriptions, travel and accommodation bookings, and a peak season for e-commerce. We analyze the most common scams that take advantage of these types of massive events, where the combination of excitement, urgency, and willingness to buy creates the perfect environment for digital fraud.

CONFERENCE HIGHLIGHTS THE ROLE OF THE JUDICIARY IN PROTECTING CHILDREN AND ADOLESCENTS IN THE DIGITAL ENVIRONMENT - BRAZIL

STJ - The VII Ibero-American Conference on Children's Rights ended this Wednesday (25), in the external auditorium of the Superior Court of Justice (STJ). During two days, the event brought together national and foreign experts in a major debate on the challenges of protecting children and adolescents in the digital environment, with emphasis on Law 15.211/2025 (Digital Statute of Children and Adolescents – ECA Digital), which recently came into force in Brazil.

ORGANIZATIONS URGE URGENT APPROVAL OF REDATA AND DATA CENTER AGREEMENT - BRAZIL

Teletime - Several entities operating in the Information and Communication Technology (ICT) sector – including Telcomp, Associação Neo, and Brasscom – released a manifesto on Tuesday, the 24th, requesting the urgent approval of the Special Tax Regime for Data Center Services (Redata) and an agreement within the scope of the National Council of Finance Policy (Confaz) to reduce the ICMS (Value-Added Tax) on data center equipment. The capex of a large data center (100 MW) in Brazil is, on average, 34% higher than that of a similar structure in the United States. The difference, according to the entities, is the tax burden on capital goods and technology, with the ICMS representing approximately 64% of this taxation.

CISCO REDEFINES SECURITY FOR THE AGENTIC WORKFORCE

dpl News - Cisco today announced security innovations designed for the AI agent ecosystem, where software not only answers questions but also performs actions. At the RSA Conference 2026, Cisco is showcasing solutions to address AI security issues and remove one of the key barriers to agent adoption. By establishing trusted identities, enforcing strict Zero Trust Access controls, hardening agents before deployment, applying runtime barriers, and providing Security Operations Center (SOC) teams with the tools to stop threats at machine speed, Cisco is building security at the foundation of the emerging AI economy.

CHECK POINT SOFTWARE LAUNCHES COMPREHENSIVE SECURITY ARCHITECTURE TO PROTECT CHILE'S NEW AI INFRASTRUCTURE, AMID A DATA CENTER INVESTMENT BOOM

Security & Defense – Check Point® Software Technologies Ltd., a pioneer and global leader in cybersecurity solutions, has launched its AI Factory Security Architecture Blueprint: a comprehensive, vendor-proven reference architecture designed to protect private AI infrastructure from the hardware to the application layer. The announcement comes at a critical time for Chile, which is consolidating its position as the second-largest data center market in Latin America and facing a radically new attack surface that conventional solutions cannot cover.

HOW GEOPOLITICS IS INFLUENCING CYBERSECURITY

El Mostrador – In 2026, geopolitics will continue to be the primary factor influencing overall cybersecurity risk mitigation strategies. The latest version of the World Economic Forum (WEF) and Accenture study showed that 64% of organizations worldwide are considering geopolitically motivated cyberattacks, such as disruptions to critical infrastructure or espionage. In fact, 91% of the largest organizations have modified their cybersecurity strategies due to geopolitical volatility.

FCC BANS NEW FOREIGN-MADE ROUTERS OVER SUPPLY CHAIN AND CYBER RISK CONCERNS - USA

The Hacker News - The U.S. Federal Communications Commission (FCC) said on Monday that it was banning the import of new, foreign-made consumer routers, citing "unacceptable" risks to cyber and national security. The action was designed to safeguard Americans and the underlying communications networks the country relies on, FCC Chairman Brendan Carr said in a post on X. The development means that new models of foreign-produced routers will no longer be eligible for marketing or sale in the U.S. The move comes in the wake of a national security determination provided by Executive Branch Agencies, Carr added.

NIST EXPANDS CSF 2.0 TOOLKIT WITH QUICK-START GUIDES ALIGNING CYBER RISK, RISK MANAGEMENT, WORKFORCE STRATEGY - USA

Industrial Cyber - The U.S. NIST (National Institute of Standards and Technology) released two new NIST Cybersecurity Framework (CSF) 2.0 quick-start guides (QSG), adding to an expanding portfolio of implementation resources that offer tailored pathways for different audiences to engage with CSF 2.0. One document positions cybersecurity risk as a core component of enterprise risk management and integrates it with workforce planning to improve how organizations assess, communicate, and respond to threats, while the other explains what informative references are and how they support achieving the outcomes of CSF 2.0. NIST published the final version of NIST Special Publication (SP) 1308, NIST Cybersecurity Framework 2.0: Cybersecurity, Enterprise Risk Management, and Workforce Management Quick-Start Guide, which draws on concepts and practices from enterprise risk management, cybersecurity risk management, and workforce management to help organizations improve communication about cybersecurity risks, plan workforce decisions, and implement risk-informed responses.

TRUMP ADMINISTRATION'S EO ON CYBERCRIME AND A CYBER STRATEGY FOR AMERICA - USA

The National Law Review - On Friday, March 6, 2026, the White House issued a sweeping Executive Order (EO) titled, "Combating Cybercrime, Fraud, and Predatory Schemes Against American Citizens." The EO reflects what most organizations already know all too well: cybercrime is no longer an episodic threat. It is a relentless, organized enterprise that is inflicting devastating financial, operational, and human harm across the globe and, in particular, in the United States. The Trump Administration also published in March a Cyber Strategy for America, laying out six pillars underpinning the cyber strategy: Shape Adversary Behavior, Promote Common Sense Regulation, Modernize and Security Federal Government Networks, Secure Critical Infrastructure, Sustain Superiority in Critical Technologies, and Build Talent and Capacity.

CYBERCRIME DISRUPTION DEMANDS GLOBAL TRUST AND COORDINATION - UK

Gov Info Security - Dismantling cybercrime groups requires more than technical capability. It demands trust, coordinated strategy and cross-border collaboration, said Paul Foster, head of the National Cyber Crime Unit at the U.K.'s National Crime Agency, or NCA. Cross-border law enforcement collaboration has matured significantly since the pandemic. A renewed push beginning early 2023 - among Five Eyes agencies, European partners and Europol - produced a shared incident response framework built around four principles: collect, store, analyze and engage. But underpinning every operation is something more fundamental, he said.