

DIGI
AMERICAS

LATAM

CISO

INSIGHTS

JULY 31, 2025

DIGI AMERICAS ALLIANCE MEMBERS



NEW ANATEL REGULATION INCREASES CYBERSECURITY RIGOR IN TELECOMMUNICATIONS - BRAZIL

Infor Channel - Resolution No. 740 of the National Telecommunications Agency (Anatel) defined the conduct and procedures to promote security in telecommunications networks and services in Brazil. In August 2024, Resolution No. 767 expanded the reporting obligations for information security incidents and the cybersecurity aspects of suppliers to be assessed by telecommunications service providers.

CYBER ALERT: LOSSES EXCEED R\$2 TRILLION IN BRAZIL AND INSURANCE IS STILL LITTLE USED - BRAZIL

CQCS - In early July, a hacker attack caused an estimated loss of nearly R\$1 billion to a technology company that connects financial institutions to the Central Bank's systems, specifically Pix. The damage is still under analysis, but the criminal activity diverted significant funds, compromising several institutions linked to the instant payments system.

PARAGUAY | SMART CITY: MITIC PRESENTS THE DIGITAL DISTRICT AS A MODEL OF INNOVATION

DPL News - Under the theme "The Future in Cities," the second day of the Smart City Paraguay 2025 event brought together leading figures from the technological, institutional, and academic fields on Tuesday, focused on designing sustainable and innovative urban solutions. In this context, the Ministry of Information and Communication Technologies (Mitic) shared details of its flagship Digital District project.

GOVERNMENT WARNS BANKS ABOUT NEW DATA THEFT TECHNIQUES WHEN UPDATING THEIR APPLICATIONS - PERU

infobae - With the arrival of new technologies, the risk also increases for banks and financial institutions with digital platforms. Recently, the National Digital Security Center (CNSD), in one of its latest alerts, warned of a new risk to data stored by banks. These threats target banking applications that use the supply chain. "Cybersecurity experts warn of new attacks targeting the banking sector and its supply chain using open source software," warns the Peruvian government agency.

CHILE ADVANCES IN THE IMPLEMENTATION OF THE CYBERSECURITY FRAMEWORK LAW: DANIEL ÁLVAREZ OUTLINES ANCI'S PRIORITIES AT A MEETING WITH AMCHAM PARTNERS

amchamCL - The director of the National Cybersecurity Agency (ANCI) highlighted the importance of strengthening basic measures and public-private collaboration to advance the implementation of the Cybersecurity Framework Law and strengthen the country's digital resilience. The Chilean-North American Chamber of Commerce (AMC), through its Digital Regulations Roundtable, organized a roundtable with Daniel Álvarez, National Director of the National Cybersecurity Agency (ANCI), to analyze progress in the implementation of the Cybersecurity Framework Law, the qualification of critical operators, and the country's priorities in this area.

ENERGY CYBERSECURITY IN CHILE: KEYS TO PROTECTING CRITICAL INFRASTRUCTURE

REDIMIN - The digitalization of the energy system has brought efficiency, but also increased exposure to cyberattacks. Protecting infrastructure is essential to avoid serious consequences. The Global Cybersecurity Outlook 2025 report warns that 60% of cyberattacks compromise electrical grids due to vulnerabilities in the supply chain. This situation underscores the importance of adopting preventive measures to protect critical infrastructure. Furthermore, the 2023 Global Crisis and Resilience Survey reveals that 87% of companies plan to allocate more resources to cyber resilience. However, the lack of security incident response plans puts the cybersecurity of electrical grids at risk.

ASSEMBLY COMMITTEE APPROVES KEY REPORT FOR DEBATE ON CYBERSECURITY LAW - ECUADOR

expresso - On July 25, the Sovereignty, Integration, and Comprehensive Security Commission approved, with nine votes, the report for the first debate of the draft Organic Law to Strengthen Cybersecurity. The document proposes a reform to the Digital and Audiovisual Transformation Law, with a technical vision and aligned with the current legal framework. According to the official statement, the new text corrects serious conceptual errors detected in previous versions, which confused areas such as cyberdefense, cybersecurity, and public safety. This confusion generated "overlapping powers and risks of unconstitutionality."

THE UNITED STATES AND THE EU SIGN A TRADE AGREEMENT THAT REDUCES TARIFFS AND GUARANTEES ACCESS TO ENERGY AND CHIPS

dpl news - After months of negotiations and threats of retaliation, the United States and the European Union (EU) have announced a comprehensive trade agreement, covering 44% of global GDP and impacting 800 million people. For the European organization, this represents "stability and predictability," while the United States notes that the agreement "rebalances the economic relationship" between the two partners.

NIST CONSORTIUM AND DRAFT GUIDELINES AIM TO IMPROVE SECURITY IN SOFTWARE DEVELOPMENT - USA

NIST - A NIST consortium including NCCoE computer security experts and 14 industry partners has drafted a high-level overview of guidelines it is developing to help organizations develop software in a secure, agile fashion and test for security vulnerabilities. NIST is soliciting comments from the public on the draft until Sept. 12, and the agency is planning a virtual event to showcase the project and gather feedback on Aug. 27. The consortium and draft guidelines respond to a June 2025 executive order to strengthen the nation's cybersecurity.

HOW A CYBER ALLIANCE TOOK DOWN RUSSIAN CYBERCRIME

CSIS - In a dramatic success and a global pushback against Russia's hybrid warfare operations, a mid-July joint international operation disrupted a massive Russian cybercrime network known as NoName057(16). Since 2022, this ideologically motivated hacktivist network has claimed responsibility for more than 1,500 distributed denial-of-service attacks (DDoS) against countries aligned with NATO.

TRUST IS THE NEW CURRENCY IN THE AI AGENT ECONOMY

WEF - The growth of the AI agent economy presents threats to trust levels – and opportunities to reimagine trust. Trust in AI is twofold, resting on perceptions of the technology's competence and intent. As autonomous AI proliferates, we must rethink trust across three different levels. Global trust levels are in decline, while the presence of AI agents in our daily lives and business systems is rapidly increasing.

PALO ALTO NETWORKS ANNOUNCES AGREEMENT TO ACQUIRE CYBERARK, THE IDENTITY SECURITY LEADER

Palo Alto Networks - Palo Alto Networks® (NASDAQ: PANW), the global cybersecurity leader, and CyberArk (NASDAQ: CYBR), the global leader in Identity Security, today announced that they have entered into a definitive agreement under which Palo Alto Networks will acquire CyberArk. This strategic combination will mark Palo Alto Networks' formal entry into Identity Security, establishing it as a core pillar of the company's multi-platform strategy.