DIGI AMERICAS LATAM CISO

INSIGHTS

MAY 29, 2025

PARAGUAY FORMALIZES NATIONAL CYBERSECURITY STRATEGY 2025-2028

dpl news - The Paraguayan government published and formalized the National Cybersecurity Strategy (NCS) for the period 2025-2028, which will be implemented by the Ministry of Information and Communication Technologies (MITIC) to strengthen the country's digital security. The approval of the initiative follows a process of just over a year, which began in March 2024 and involved the government, the private sector, academia, and civil society. The NCS updates the previous eight-year-old instrument, the 2017 National Cybersecurity Plan.

CYBERSECURITY IN URUGUAY: THE PROGRESS THAT FEW ARE SEEING

msn - In this regional scenario, Uruguay emerges as one of the countries that was able to anticipate the trend. "Uruguay did a very good job," said Chain, who highlighted the role of the Agency for Electronic Government and Information Society: "AGESIC did an enormous job with everything related to information security." Although he recognizes that the country still faces significant challenges, especially regarding the digital education of the population, Chain emphasizes that "for a time, it was the priority, one of the priorities, to want to raise awareness."

ANATEL PRESENTS ADVANCES IN CONNECTIVITY AND DIGITAL SECURITY AT ADVISORY BOARD MEETING - BRAZIL

gov.br - Anatel presented, this Tuesday (20/5), the main regulatory, technological and institutional results and advances for the year 2024 to the Agency's Advisory Board, in a meeting held in Brasília. The meeting, chaired by Fabrício da Mota Alves, had as its main agenda the appreciation of the Annual Management Report, prepared under the coordination of the Executive Superintendence, with the participation and considerations of the executive superintendent, Gustavo Santana Borges, and a technical presentation led by Marcelo Monteiro, manager of Strategic Planning. Also present at the occasion was the superintendent of Granting and Service Resources, Vinicius Caram.

GOVERNMENT ANNOUNCES GROUP TO DEVELOP NATIONAL CYBERSECURITY PLAN - BRAZIL

Olhar Digital - The National Cybersecurity Committee (CNCiber) will create a thematic working group to develop the National Cybersecurity Plan. The plan aims to create recommendations for the technology market and digital service providers regarding cybersecurity in Brazil. The creation of the group was published in a resolution this Tuesday (27), in the Official Gazette of the Union (DOU). It will have representatives from the government, market and civil society.

CYBERSECURITY IN BRAZILIAN STATES

IDB - In 2024, in partnership with the GTD.GOV Cybersecurity Working Group, the IDB conducted a mapping of organizational configurations related to information security and cybersecurity in the 27 Brazilian federative units. This pioneering research analyzed, based on pre-structured questionnaires, policies, governance models and human capital for cybersecurity issues. The report offers the first insight into the puzzle of cybersecurity governance in Brazilian states.

PROTECTING DIGITAL PAYMENTS IN COLOMBIA: 5 KEYS TO SECURE TRANSACTIONS

Revista C-Level - With more than USD 13.5 billion in projected sales by 2027, e-commerce in Colombia is making steady progress. But along with the rise of digital transactions, risks are also multiplying: identity theft, phishing, smishing, vishing, device theft, and website cloning. Protecting digital payments in Colombia has become a priority.

INVISIBLE INFRASTRUCTURE - COLOMBIA

El Universal - In the digital age, data centers are as important as ports and highways were in the 20th century. They constitute the invisible infrastructure that makes everything from bank transfers to artificial intelligence possible. Colombia is lagging behind in this strategic infrastructure. Today, more than 80% of the data we use is processed outside the country, primarily in the US and Brazil. This generates greater latency, technological dependence, high costs, and cybersecurity risks. A country that aspires to reap digital dividends cannot depend on foreign infrastructure.

ANALYSIS OF CYBERSECURITY LAW INITIATIVE PROGRESS - GUATEMALA

Congreso.gob.gt - In order to advance the analysis of Initiative 6347, the Cybersecurity Law, the National Security Affairs Committee, chaired by Representative Jorge Mario Villagrán, held a hybrid meeting with the technical advisory panel to address Title III, which addresses precautionary, procedural, and procedural measures. Representatives Felipe Alejos, José Pablo Mendoza, and Rodrigo Pellecer participated virtually, while Congressmembers Darwin Lucas and Mirna Godoy Palala attended in person.

GUATEMALA AND THE U.S. STRENGTHEN TIES IN TECHNOLOGICAL INNOVATION

Republica - It's news. The U.S. ambassador to Guatemala, Tobin Bradley, welcomed Silicon Valley investors interested in exploring opportunities in the country's technology sector to his residence. During the meeting, potential investments were discussed in key areas such as artificial intelligence, cybersecurity, and data management. Bradley emphasized that the world of technology is moving fast, and that the U.S. and Guatemala are moving with it. He also underscored the importance of bilateral collaboration to open new markets and strengthen the security and prosperity of both countries and the region.

CYBERATTACKS IN LATIN AMERICA: ALARMING TRENDS AND EMERGING DEFENSE STRATEGIES

Reporte Diario - IBM's 2025 X-Force Threat Intelligence Index reveals a troubling picture of the cyber landscape in Latin America. The region accounted for 8% of all incidents responded to by X-Force in 2024, a decrease from 12% the previous year, but still an alarming figure. Cybercriminals continue to adapt their tactics, focusing on stealthier and more profitable methods, such as credential theft and the use of infostealers.

NEW GUIDANCE FOR SIEM AND SOAR IMPLEMENTATION

CISA - Today, CISA, in collaboration with the Australian Signals Directorate’s Australian Cyber Security Centre (ASD’s ACSC) and other international and U.S. partners, released new guidance for organizations seeking to procure Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms. This guidance includes the following three resources: Implementing SIEM and SOAR Platforms – Executive Guidance outlines how executives can enhance their organization’s cybersecurity framework by implementing these technologies to improve visibility into network activities, enabling swift detection and response to cyber threats. Implementing SIEM and SOAR Platforms – Practitioner Guidance focuses on how practitioners can quickly identify and respond to potential cybersecurity threats and leverage these technologies to streamline incident response processes by automating predefined actions based on detected anomalies. Priority Logs for SIEM Ingestion – Practitioner Guidance offers insights for prioritizing log ingestion into a SIEM, ensuring that critical data sources are effectively collected and analyzed to enhance threat detection and incident response capabilities tailored for organizations.

THE DOUBLE-EDGED SWORD OF CYBERSECURITY INNOVATIONS

JPMorgan - In an era defined by accelerating cyberthreats and technological disruption, founders face a complex, evolving landscape. Regardless of industry, this is a reality for startups, whether they’re developing a first prototype, fine-tuning a go-to-market strategy or preparing to go public. The same advances in artificial intelligence (AI), cloud computing and automation that enhance companies’ defenses are simultaneously exploited by adversaries. On the horizon, quantum computing promises to reshape encryption and cryptanalysis, making data protection and offensive capabilities more powerful.

STATE OF HEALTHCARE CYBERSECURITY: PROGRESS AND PITFALLS

Govinfosecurity - While the healthcare sector is making progress in cyber resilience, it still faces deep-rooted challenges, including collaboration, cyber workforce issues and budget constraints, necessitating a constant demand for adaptation and re-prioritization as adversaries shift their tactics, said security experts Phil Englert and Murad Dikeidek. Information sharing can be vital to helping the overall sector better understand the threats it is facing, yet there's still uncertainty at many organization about the level of details healthcare providers should disclose, he said.

WHY AI IS THE NEW CYBERSECURITY BATTLEGROUND

Forbes - Artificial intelligence has quickly grown from a capability to an architecture. As models evolve from backend add-ons to the central engine of modern applications, security leaders are facing a new kind of battlefield. The objective not simply about protecting data or infrastructure—it's about securing the intelligence itself. In this new approach, AI models don't just inform decisions—they are decision-makers. They interpret, respond, and sometimes act autonomously. That shift demands a fundamental rethink of how we define risk, build trust, and defend digital systems.