DIGI AMERICAS LATAM CISO

# INSIGHTS

APRIL 16, 2026

DIGI AMERICAS ALLIANCE MEMBERS

## GOVERNMENT ACTIVATES CYBERSECURITY PLAN AFTER ATTACKS ON DIGECAM AND NATIONAL LABORATORY - GUATEMALA

Soy 502 - The Executive Branch announced that it is considering a series of actions to strengthen the protection of public institutions against cyberattacks. These actions will be carried out within the framework of the Digital Transformation Plan, which includes the implementation of the National Cybersecurity System, confirmed the Presidential Secretariat of Social Communication. These measures are being promoted in a recent context marked by cybersecurity incidents, including the attack on the General Directorate of Arms and Ammunition Control (Digecam), in which institutional information was compromised, as well as the attempted cyberattack on the National Health Laboratory.

## ANTI-MONEY LAUNDERING AND CYBERSECURITY LAWS TOP THE AGENDA - GUATEMALA

Congreso.gob.gt - At the request of Representative Jorge Mario Villagrán, head of the Blue bloc, initiative 6347, which promotes a cybersecurity law, was also included for its third debate. The purpose of this initiative is to establish a comprehensive legal framework to prevent, investigate, and punish cybercrimes, as well as to strengthen institutional capacities for responding to cyber incidents, thereby enhancing the security of Guatemalans against digital threats.

## ECA DIGITAL CHANGES INTERNET RULES FOR CHILDREN AND ADOLESCENTS: SEE HOW DATA PROTECTION WORKS AND WHAT TO DO TO ENSURE ONLINE SAFETY - BRAZIL

E.M. Foco - The increased presence of children and adolescents on the internet has led to the creation of new rules specifically for this audience in the online environment. With the so-called Digital ECA (Statute of Children and Adolescents), Brazil is now detailing how data protection, content moderation, advertising, and the responsibility of companies and legal guardians regarding the use of digital platforms by minors should function, bringing the virtual world closer to the guarantees already provided for in the Statute of Children and Adolescents.

DIGI AMERICAS LATAM CISO

# INSIGHTS

APRIL 16, 2026

## WHEN CYBER RISK ORIGINATES IN THE BOARDROOM - BRAZIL

Defesa Net - The biggest threat to companies' digital security doesn't come from sophisticated hackers: it comes from strategic decisions made by CEOs, CFOs, and CTOs who, without realizing it, open doors to attacks as devastating as any external intrusion. According to market data, data breaches involving third parties doubled last year. At least 82% of breaches affect data stored in the cloud, and more than 60% of corporate applications operate as "shadow IT"—outside the control of security teams. In Brazil, where only 5% of organizations have reached cybersecurity maturity, the average cost of a data breach already reaches R$ 7.19 million.

## SSPE PARTICIPATES IN INTERNATIONAL CYBERSECURITY TRAINING - MEXICO

TEl Diario de Chihuahua - An officer from the Chihuahua State Public Security Secretariat (SSPE), headed by Secretary Gilberto Loya, participated in an international cybersecurity leadership program held in the United States. The program aimed to strengthen technological and strategic capabilities in the prevention and combating of cybercrime. Representing Mexico was Daniel Aranda Viezcas, assigned to the Undersecretariat of Intelligence and Police Analysis, who participated in the event alongside delegations from countries such as Brazil, Guatemala, Argentina, Paraguay, Uruguay, and Chile.

## ARGENTINA ACCELERATES CYBERSECURITY AGREEMENT WITH THE UNITED STATES: SCOPE, CONTEXT, AND WHAT CHANGES

IT.Sitio- The Argentine government, led by Javier Milei, is moving forward with negotiations for a cybersecurity agreement with the United States with a specific objective: to strengthen the state's capacity to prevent and respond to cyberattacks in a context where it acknowledges structural limitations. The Executive branch seeks access to financing, technical cooperation, and equipment to reinforce state protection systems, in a context where it admits vulnerabilities in various areas of public administration. This initiative is not an isolated event. It forms part of a broader strategy of alignment with Washington on security, defense, and intelligence matters, which is redefining Argentina's international standing.

## ANTHROPIC AND OPENAI TIGHTEN CONTROLS IN RESPONSE TO GROWING AI CYBERSECURITY RISKS

Diario Bitcoin - Leading artificial intelligence companies Anthropic and OpenAI have begun implementing stricter measures to control access to their technologies in response to the growing cybersecurity risks posed by their models. What initially emerged as tools for everyday tasks has rapidly evolved into systems capable of identifying and exploiting critical vulnerabilities, raising concerns to the level of national security.

DIGI AMERICAS LATAM CISO

# INSIGHTS

APRIL 16, 2026

## FBI: RANSOMWARE STILL A TOP THREAT TO CRITICAL INFRASTRUCTURE - USA

Gov Tech - Ransomware continues to pose a serious threat to U.S. critical infrastructure, with more than 2,100 related incidents reported to federal authorities in 2025, according to the latest FBI Internet Crime Complaint Center (IC3) report. To put that number in perspective, IC3 reported roughly 1,100 data breach threats to critical infrastructure, which includes sectors such as health care, critical manufacturing, financial services, energy and agriculture, among others. Ransomware attacks directed at critical infrastructure are serious, possessing as they do the potential to disrupt operations, expose sensitive data and affect the delivery of public services.

## CYBERATTACKS TARGET US INFRASTRUCTURE, AND OTHER CYBERSECURITY NEWS

WEF - A new joint advisory from US agencies has said that cyber activity targeting critical infrastructure has escalated in recent weeks amid the conflict in the Middle East, highlighting how geopolitical tensions are increasingly playing out in cyberspace. Hackers are exploiting internet-exposed operational technology (OT) devices — which are connected to the internet for remote monitoring, exposing infrastructure to attacks — used across sectors including energy, water and local government systems. The advisory notes that the widespread use of these devices and their frequent exposure to the public internet make them an attractive target for hackers. In several cases, these events have already caused operational disruption and financial loss, with attackers manipulating data on industrial control interfaces and extracting sensitive system files.

## BRUTE-FORCE CYBERATTACKS ORIGINATING IN MIDDLE EAST SURGE IN Q1

Cybersecurity Dive - A surge of brute force authentication attacks targeted network devices during the first quarter of 2026, with the vast majority of threat activity coming from the Middle East. Almost 90% of the brute-force attacks originated from various Middle East locations, and the leading targets were SonicWall and Fortinet FortiGate devices. IP addresses alone are not considered a reliable indicator, but said it was “safe to assume” that a combination of state-linked and professional groups were involved. Attacks from opportunistic groups were also likely involved. Hackers have been aggressively scanning perimeter devices for weak or exposed credentials, according to the blog post.

## OAS AND MASTERCARD JOIN FORCES TO COMBAT CYBERCRIME

OAS - The Organization of American States (OAS) and the company Mastercard signed an agreement today to work together to strengthen cyber resilience in the Americas, during a ceremony held at the headquarters of the hemispheric institution in Washington, DC. The OAS Secretary for Multidimensional Security, Ivan Marques, highlighted how cybercrime, ransomware, and attacks on critical infrastructure are growing in scale and sophistication, affecting governments, businesses, and citizens alike. “Addressing these challenges requires more than government action alone. The private sector is at the forefront of innovation and expertise in cybersecurity. Companies like Mastercard are essential partners in securing financial systems and building trust in digital commerce,” added Secretary Marques, who signed the Memorandum of Understanding on behalf of the OAS Secretary General, Albert R. Ramdin.