DIGI AMERICAS LATAM CISO

# INSIGHTS

OCTOBER 24, 2024

DIGI AMERICAS ALLIANCE MEMBERS

## DEFENSE MINISTER REINFORCES IMPORTANCE OF INVESTMENTS IN CYBERSECURITY - BRAZIL

Defense in Focus - During the Cyber Guardian Exercise 6.0, held in Brasília, the Minister of Defense, José Mucio Monteiro, highlighted the urgent need to increase investments in the area of cybersecurity. In a scenario where virtual attacks represent a growing threat to national sovereignty, the minister emphasized that protecting critical infrastructure is as important as preparing for traditional armed conflicts. The defense of critical infrastructure, such as nuclear and hydroelectric plants, telecommunications centers and transportation systems, is essential to maintain the security and stability of a country. However, these structures are increasingly vulnerable to sophisticated cyberattacks that can compromise vital operations and weaken national sovereignty. During the Cyber Guardian Exercise 6.0, Minister José Mucio Monteiro highlighted that, for Brazil, strengthening digital security must be a strategic priority.

## CYBERSECURITY: MORE THAN A REGULATORY AGENCY, BRAZIL NEEDS A GOVERNANCE STRUCTURE

Digital Convergence - Brazil has room for a governance structure for cybersecurity, not necessarily for a regulatory agency or a special government agency, says Leonardo Ferreira, Director of Privacy and Security for the Performance Management System of the Ministry of Management and Innovation. Speaking to CDTV, from the Digital Convergence portal, during the 2nd edition of Cyber.GOV, organized by Network Eventos, in Brasília, Ferreira noted that the country has structures that already pay close attention to cybersecurity, such as the federal police, Cert.br and the Secretariat of Digital Government itself. “But it is a fact that we need to have a governance structure that provides coordination and integration,” he pointed out. The Secretariat of Digital Governance will be responsible for the cybersecurity of the G20, an event that will take place in November in Rio de Janeiro and will bring together leaders from all over the world. “We have already held more than 100 meetings over the last few months and we are preparing a lot,” he emphasized, without, however, revealing details of the strategy to be adopted.

DIGI AMERICAS LATAM CISO

# INSIGHTS

OCTOBER 24, 2024

## ELECTORAL COURT WARNS OF SCAM WITH FAKE EMAIL ABOUT SUMMONS

Agencia Brasil - The Regional Electoral Court of São Paulo (TRE-SP) has issued a warning about fake e-mails that use the name of the Electoral Court to make fictitious summons for poll workers for the second round of the municipal elections. According to TRE-SP, the messages intend to capture the victims' personal data to carry out scams. "To attract people's attention, the fake message contains alarming content about the request for exemption from summoning a poll worker, informing that the fine would be R$1,064.10, plus 50% of the minimum wage, totaling R$1,770.10. It adds that "the fine will be sent in the IPTU or essential bills (electricity or water bills) of the poll worker's or parents' CPF", highlights the electoral court in a note.

## ESPERIDIÃO AMIN WARNS ABOUT CYBER DEFENSE CHALLENGES - BRAZIL

Senate Agency - Senator Esperidião Amin (PP-SC) highlighted, in a speech in the Plenary this Wednesday (16), the participation of parliamentarians in a cyber defense exercise carried out by the Higher School of Defense, in partnership with the Armed Forces. The senator informed that he was appointed rapporteur of the National Defense Plan of the Armed Forces and announced that he will include in the report the need to increase the budget allocated to cyber security. He emphasized that Brazil needs to adequately prepare to face these challenges.

## LAW PROPOSED TO REGULATE CYBERSPACE AND CYBERSECURITY - MEXICO

La Prensa - Mexico is a very attractive country for cybercriminals because it has a significant gap in terms of protection, said the president of the Special Attention Commission for Victims of the Congress of Mexico City, Ana Buendía García, who is promoting an initiative to create a general law that regulates cyberspace and cybersecurity. She considered it pertinent to add a section to article 73 of the Political Constitution of the United Mexican States, which allows the Congress of the Union to issue a General Law on Cyberspace and Cybersecurity, which should establish clear rules and have authorities empowered to regulate digital ecosystems, protect personal data and combat cybercrimes.

## OMA AIRPORT GROUP SUFFERS CYBERSECURITY ATTACK - MEXICO

Forbes - Grupo Aeroportuario del Centro Norte (OMA) reported on Friday that it was the victim of a cybersecurity incident without having identified any adverse effects on its operations so far. OMA, which manages 13 air terminals in the central-northern region of Mexico, said that the episode is related to unauthorized access to its information systems. "OMA's IT (Information Technology) team, in collaboration with external cybersecurity experts, is actively investigating the incident to determine its scope and ensure the protection of the integrity, confidentiality and availability of our systems," the company said in a statement.

DIGI AMERICAS LATAM CISO

# INSIGHTS

OCTOBER 24, 2024

## COLOMBIAN FINANCIAL SECTOR RECEIVES 45 CYBERATTACKS PER SECOND: MINTIC

Caracol - In a report delivered by the Ministry of Information and Communications Technology (ICT), it was found that so far this year, the country has received nearly 24,000 million cyberattacks, where the most affected sector was the financial sector with 98%. The ICT Minister, Mauricio Lizcano, mentioned that the most affected people are those with the lowest resources. Within the minister's strategy is to strengthen the Colombian Cyber Emergency Response Group (ColCert), invest in cybersecurity operations centers (SOC) and stressed the importance of training and educating the general population to reduce the effectiveness of these attacks. The minister also highlighted the Ciberpaz program, which has a component of 'Digital Security and Trust', which seeks to promote the safe and responsible use of ICTs.

## MINTIC ANNOUNCES FINANCIAL CYBERSECURITY STRATEGY WITH ARTIFICIAL INTELLIGENCE - COLOMBIA

El Frente - At the opening of the 17th Congress on Security, Cyber Threats, Fraud and Experience (SAFE), the Minister of Information and Communications Technology (ICT), Mauricio Lizcano, highlighted the importance of artificial intelligence in the country's financial cybersecurity. During the event organized by Asobancaria, the Minister shared the ICT Ministry's strategy to protect citizens, institutions and companies from the growing cyber threats.

## COLOMBIA SUSPENDED FROM EGMONT GROUP FOLLOWING GUSTAVO PETRO'S SPEECH OVER PEGASUS SPYWARE

Finance Colombia - As a result of Gustavo Petro revealing clasified information about the Pegasus spyware, the President of the Egmont Group of Financial Intelligence Units, Elżbieta Franków-Jaśkiewicz, confirmed the suspension of Colombia from the program, and said: “Due to recent actions involving FIU Colombia and the unauthorized disclosure of information provided by one of our members, the Egmont Group Heads of FIU have confirmed the suspension of FIU Colombia’s access to the Egmont Secure Web (ESW). The Egmont Group is a global organization of 177 Financial Intelligence Units (FIUs) that supports international efforts to combat money laundering, terrorist financing, and related crimes.

## CNEA OFFERS CYBERSECURITY SERVICES FOR INSTITUTIONS AND COMPANIES - ARGENTINA

Argentina.gob - Cybersecurity plays a fundamental role in protecting the information and systems of institutions and companies, both public and private. The National Atomic Energy Commission (CNEA) provides computer security services to support the organization's research and development work. Some of these services, such as training and audits of applications and infrastructure to detect possible vulnerabilities, are also available to external clients. One of the training courses offered by the Computer Security Department of the Information and Communications Technology Department of the CNEA seeks to raise awareness of cybersecurity among end users. "The objective is to raise awareness about the main risks to which we are exposed every day in terms of computer security and how to defend ourselves.

DIGI AMERICAS LATAM CISO

# INSIGHTS

OCTOBER 24, 2024

## INDOTEL PROMOTES DIGITAL SECURITY WITH THE LAUNCH OF THE "ELECTRONIC TRUST LIST" - DOMINICAN REPUBLIC

El Nuevo Diario - The Dominican Institute of Telecommunications (INDOTEL) launched its Electronic Trust List, a new step towards the development of the digital environment of the Dominican Republic, whose initiative seeks to strengthen the security of electronic transactions and guarantee the validity of digital signatures at a global level. The implementation of this Electronic Trust List positions the country as a benchmark in the adoption of electronic trust services and reaffirms INDOTEL's commitment to the digital modernization of the country, improving technological security and opening opportunities for international cooperation.

## INDOTEL PROMOTES CYBERSECURITY EDUCATION FOR YOUNG DOMINICANS - DOMINICAN REPUBLIC

Digital Newspaper - The Dominican Institute of Telecommunications (INDOTEL) has launched an educational program designed to promote the safe use of the Internet among children and adolescents. This initiative begins with the participation of more than 100 students from the Fabio Amable Mota Technological Institute. The program, which will run for six months, is focused on adolescents aged 14 to 15, who will receive training on best practices to ensure their online safety and the responsible use of essential technologies.

## COSTA RICA STRENGTHENS ITS CYBERSECURITY WITH HISTORIC INVESTMENT AND INTERNATIONAL COOPERATION

El Mundo - The Ministry of Science, Innovation, Technology and Telecommunications (Micitt) reported on the historic 446% increase in investment to strengthen the country's cybersecurity and counter the growing number of cyberattacks, which in 2023 alone reached 882 million attempts. This investment has allowed the creation of the Cybersecurity Directorate, incident response teams (SOC-CR and CSIRT-CR), the implementation of cutting-edge protection systems in government institutions, and the training of thousands of Costa Ricans in digital security.

## NATIONAL CYBERSECURITY LABORATORY WILL MONITOR DARK AND DEEP WEB

CRHoy - With the support of the European Union (EU), a cyber intelligence laboratory, a computer forensics laboratory and a secure information exchange network for public institutions will be established in the country. This is a new project that adds to the efforts to strengthen national capacities to prevent and respond to cyberattacks. Through this cooperation, the capacity to anticipate cyberattacks will be strengthened, as the cyberintelligence laboratory will monitor the dark web and the deep web to proactively identify possible threats, which is expected to lead to a faster and more effective response to the challenges of cybercriminals.

DIGI AMERICAS LATAM CISO

# INSIGHTS

OCTOBER 24, 2024

## UNITED ARAB EMIRATES AND URUGUAY SIGN AGREEMENT TO PREVENT CYBER ATTACKS

Gub.uy - On October 17, representatives of Agesic and the Cyber Security Council of the United Arab Emirates (UAE) signed a Memorandum of Understanding with the aim of strengthening cooperation between both countries for the detection and prevention of information security incidents. The agreement establishes a framework for collaboration between the UAE and Uruguay to facilitate the exchange of knowledge and good practices, as well as the development of joint capabilities in the field of cybersecurity. The areas of cooperation planned are: exchange of information on risks related to information security; collaboration in the management and joint response to security incidents; dissemination of good practices and experiences in cybersecurity; exchange of educational and training resources; formation of joint working groups specialized in cybersecurity; and research advice, among other topics.

## THE CYBERCRIME BILL: A NECESSARY SHIELD FOR BARBADOS' DIGITAL FUTURE

Barbados Today - The rise of cyber threats has made cybersecurity a global priority. In Barbados, the Cybercrime Bill is a crucial step toward protecting the nation from digital crimes. While some Bajans may express concerns about the Bill's implications, it is vital to recognise the daily risks the country faces due to resistance to these protections. Many Bajans are apprehensive about the Cybercrime Bill due to fears about privacy, government overreach, or the potential criminalisation of minor online infractions. These concerns, while understandable, often stem from a limited understanding of how cyber threats evolve and impact both personal and national security.

## BDF CYBER UNIT LEADING INVESTIGATION INTO REVENUE AUTHORITY HACK - BARBADOS

Barbados Today - Three weeks after a major data breach at the Barbados Revenue Authority led to personal information and vehicle registration documents being offered for sale online, officials say there's no evidence any of the stolen data was used for fraud or other harmful activities. Minister of Industry, Innovation, Science, and Technology Marsha Caddle sought to downplay the fallout from the breach while announcing a programme to put the public and civil servants on guard for cyber threats.

## WHY THE NEW NIST STANDARDS MEAN QUANTUM CRYPTOGRAPHY MAY JUST HAVE COME OF AGE

WEF - Quantum computing creates enormous economic and scientific opportunities, given its ability to significantly boost computing power. However, quantum computing – which employs quantum mechanics to solve some complex computing problems – can also render some of the current encryption algorithms obsolete, posing serious cybersecurity risks. The current state of quantum technology overall is still nascent, but short- and long-term predictions suggest great potential for a technology that could open new opportunities in the cybersecurity area. While quantum computers are still in the development stage, experts expect that quantum computers will have encryption-breaking capabilities within the next decade, threatening the "security and privacy of individuals, organizations and entire nations".

DIGI AMERICAS LATAM CISO

# INSIGHTS

OCTOBER 24, 2024

## WE MUST REDUCE COMPLEXITY TO ENSURE STRONG CYBERSECURITY. HERE'S WHY

WEF - Complexity has fascinated me throughout my career. From algorithms in computer science to the threat landscape in cybersecurity, complexity and its resulting variance create fascinating challenges. But the reality is complexity is the enemy of security. Fundamentally, complexity in cybersecurity means a lack of visibility. The sheer number of components and point products in many modern networks makes identifying vulnerabilities, let alone remediating them, challenging. Moreover, the infrastructure itself is dynamic (software-defined networking) and without a clear picture of what's happening, building strong structural defences is difficult.

## HOW CYBERSECURITY CAN HELP PUSH THE BOUNDARIES OF ENERGY TRANSITION INNOVATION

WEF - Cybersecurity is often seen as preparing for failure. It's also often seen as a concern for digital leaders only. But cybersecurity can have a significant impact right across an organization. Cyberattacks affect market capitalization and research shows cyber-resilient organizations provide 50% more value to their shareholders. Thinking about cybersecurity as loss avoidance and a digital-only issue misses key intangibles that can boost organizational value: trust, reputation, stakeholder confidence and the technical capacity needed to support rapid innovation. Cyber-resilient organizations, on the other hand, are able to continue to meet primary business goals and also even unlock additional value.