DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 6, 2025

DIGI AMERICAS ALLIANCE MEMBERS

aws Apple CHECK POINT CISCO CLOUDFLARE CROWDSTRIKE fluid attacks Google kriptos LUMU METABASE Q netskope paloalto NETWORKS Resecurity Schneider Electric SISAP Telefónica tenable Trellix TREND MICRO

CYBERSECURITY, A PRIORITY FOR THE FEDERAL GOVERNMENT - MEXICO

DineroEnImagen - For the first time, the federal government will have a General Directorate of Cybersecurity that designs, develops, executes and updates strategies and a governance framework for management in this area.
For the first time, the federal government will have a General Directorate of Cybersecurity that designs, develops, executes and updates strategies and a governance framework for management in this area.
Cybersecurity expert Victor Ruiz said that this is a very successful proposal and, as a plan, addresses many of the current needs of citizens to protect them from cyber threats.

SENATE ANNOUNCES FORUM ON AI AND CYBERSECURITY - DOMINICAN REPUBLIC

The President of the Senate, Ricardo de los Santos, announced that the international meeting Parliaments and Prosperity, Dominican Republic 2025 will work on a common legislative agenda with countries in the region to address key issues such as cybersecurity, health and artificial intelligence. Academics, businessmen and legislators will debate on Parliament and the digital agenda, cybersecurity, artificial intelligence, Parliament, health and social security, Parliament and economic growth and Parliament and legislation based on scientific knowledge.

THE US WILL COLLABORATE WITH COSTA RICA ON CYBERSECURITY, MIGRATION AND DRUG TRAFFICKING ISSUES

Yahoo! News - Costa Rican President Rodrigo Chaves and U.S. Secretary of State Marco Rubio confirmed on Tuesday that they will continue bilateral cooperation on cybersecurity, migration and drug trafficking. During Rubio's official visit to San Jose, the Secretary of State said that Costa Rica is a "model and example" country, as well as a "friend and ally," with which the United States shares common themes such as "values" and "history."

CHILE'S NATIONAL CYBERSECURITY AGENCY: FIRST STEPS, REFERENCES AND OBJECTIVES

dplnews - At the beginning of the year, the National Cybersecurity Agency of Chile (ANCI) began its operations. It is responsible for supervising, regulating and sanctioning public or private institutions that provide services in this area. In addition, it will define essential services and operators of vital importance and will dictate protocols, standards and general instructions to implement the Cybersecurity Framework Law.

EU TO FUND CYBERSECURITY TRAINING FOR COSTA RICAN SMES

crhoy.com - The Latin American and Caribbean Cyber Competence Centre (LAC4), in cooperation with the European Union (EU) delegations in Central America, invites Central American small and medium-sized enterprises (SMEs) to participate in a training session to strengthen cybersecurity skills. The activity, which will take place from March 19 to 21 in the city of Antigua, Guatemala, has the support of EUreCA and seeks to promote good cybersecurity practices. To this end, three companies from Panama, Costa Rica, Honduras, Guatemala, Belize, and El Salvador will be invited to an EU-funded face-to-face training session on cybersecurity.

CYBERSECURITY AND BUSINESS: THE CISO AS A LEADER IN THE DIGITAL AGE

LaVerdadNoticias - For years, the role of the Chief Information Security Officer (CISO) was limited to protecting systems and data, operating in the background within organizations. However, in the digital age, where cyberattacks can cost millions and affect a company's reputation in seconds, cybersecurity is no longer just a technical issue, but a matter of business and corporate strategy. Today, CISOs have a seat in the boardroom, with the opportunity — and responsibility — to become strategic partners of the business.

DEEPSEEK FROM A CYBERSECURITY PERSPECTIVE

Portal Innova - AI-powered chatbots continue to become more widespread, and the most recent one developed in China - DeepSeek - has generated worldwide expectation, not only at the user level, but also in the corporate sphere. New research from Sophos titled “Beyond the Hype: The Business Reality of AI for Cybersecurity” revealed that 89% of IT leaders are concerned about Generative AI failures and that these will negatively affect their companies’ cybersecurity strategies.

GLOBAL RANSOMWARE PAYMENTS PLUNGE BY A THIRD AMID CRACKDOWN

The Guardian - Ransomware payments fell by more than a third last year to $813m (£650m) as victims refused to pay cybercriminals and law enforcement cracked down on gangs, figures reveal.
The decline in such cyber-attacks – where access to a computer or its data is blocked and money is then demanded to release it – came despite a number of high-profile cases in 2024, with victims including NHS trusts in the UK and the US doughnut firm Krispy Kreme.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 6, 2025

LAW ENFORCEMENT TAKES DOWN TWO LARGEST CYBERCRIME FORUMS IN THE WORLD

Europol - A Europol-supported operation, led by German authorities and involving law enforcement from eight countries, has led to the takedown of the two largest cybercrime forums in the world. The two platforms, Cracked and Nulled, had more than 10 million users in total. Both of these underground economy forums offered a quick entry point into the cybercrime scene. These sites worked as one-stop shops and were used not only for discussions on cybercrime but also as marketplaces for illegal goods and cybercrime-as-a-service, such as stolen data, malware or hacking tools. Investigators estimate that suspects earned EUR 1 million in criminal profits.

5 RISK FACTORS FROM SUPPLY CHAIN INTERDEPENDENCIES IN A COMPLEX CYBERSECURITY LANDSCAPE

WEF - According to the World Economic Forum’s Global Cybersecurity Outlook 2025, the increasing reliance on complex supply chains is leading to a more uncertain and unpredictable cybersecurity landscape. Last year saw the most significant IT outage in history, highlighting the importance of safeguarding the cybersecurity ecosystem. Five key risk factors from supply chain interdependencies have been identified that contribute to an increasingly complex landscape.

‘THIS HAPPENS MORE FREQUENTLY THAN PEOPLE REALIZE’: ARUP CHIEF ON THE LESSONS LEARNED FROM A $25M DEEPFAKE CRIME

WEF -Fraudsters used an AI deepfake to steal $25 million from UK engineering firm Arup. Here, Arup's Chief Information Officer, Rob Greig, talks about the lessons learned. Cyber resilience in the face of increasing threats is a critical objective for any organization, according to the World Economic Forum white paper Unpacking Cyber Resilience.

THE CYBERSECURITY CRISIS: COMPANIES CAN’T FILL ROLES, WORKERS SHUT OUT

Forbes - Breaking into a cybersecurity career has never been easy and today it's more competitive than ever. At the same time, there is a well-documented cybersecurity talent shortage, with an estimated 4.8 million unfilled cybersecurity jobs globally, according to the 2024 ISC2 Cybersecurity Workforce Study. The demand for skilled professionals far outpaces supply, particularly in specialized fields such as cloud security, application security and incident response. Yet, despite this gap, companies continue to outsource critical security functions overseas rather than invest in developing homegrown talent. This has major implications not only for job seekers but also for national security.

CISA ADDS FOUR KNOWN EXPLOITED VULNERABILITIES TO CATALOG

CISA - CISA has added four new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.

- CVE-2024-45195 Apache OFBiz Forced Browsing Vulnerability
- CVE-2024-29059 Microsoft .NET Framework Information Disclosure Vulnerability
- CVE-2018-9276 Paessler PRTG Network Monitor OS Command Injection Vulnerability
- CVE-2018-19410 Paessler PRTG Network Monitor Local File Inclusion Vulnerability

These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.