DIGI AMERICAS ALLIANCE MEMBERS

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

GLOBAL CYBERSECURITY OUTLOOK 2025 – NAVIGATING THROUGH RISING CYBER COMPLEXITIES

WEF - The World Economic Forum's Global Cybersecurity Outlook 2025 report released today highlights the increasing complexity in the cyber landscape, which has significant implications for organizations and nations. This complexity arises from the rapid growth of emerging technologies, prevailing geopolitical uncertainty, the evolution of threats, regulatory challenges, vulnerabilities in supply chain interdependencies and the growing cyber skills gap.

THE GOVERNMENT CREATED A CYBERSECURITY STRENGTHENING PROGRAM - ARGENTINA

Ambito - The national government has officially created a program to strengthen cybersecurity and investigate cybercrime (ForCIC). According to the details, the purpose of the measure is to prevent and investigate computer crimes, including fraud, the distribution of child abuse material, and attacks against public safety, among others. The program also seeks to form an alliance between the provinces and the Autonomous City of Buenos Aires through the 24/7 Unit to strengthen the prevention and investigation of this type of crime. The government assured that the measure "does not involve any budgetary expenditure."

THE GOVERNMENT APPROVED THE FEDERAL PLAN FOR THE PREVENTION OF CYBERCRIME AND STRATEGIC MANAGEMENT OF CYBERSECURITY - ARGENTINA

Infobae - In the midst of the reforms implemented in terms of security, the national government created the Federal Plan for the Prevention of Cybercrime and Strategic Management of Cybersecurity, with the objective of preventing, investigating and providing solutions to the needs of citizens who have been harmed by organized crime. It will be applied in a transversal manner, so all police and security forces will be included.

CHILE INGRESA A LA COUNTER RANSOMWARE INITIATIVE

Ministry of Foreign Affairs - Chile officially joined today (January 13) the Counter Ransomware Initiative (CRI), an international initiative whose objective is to generate collective resilience and design political approaches to confront the threat of ransomware, one of the main types of cyberattacks worldwide, which consists of malicious programs that hold data and devices hostage until a ransom is paid.

WHAT WILL THE "COMPUTER EMERGENCY RESPONSE" CENTER PROPOSED BY THE CYBERSECURITY LAW DO? - GUATEMALA

Prensa Libre - The Cybersecurity bill pending discussion in Congress proposes the creation of an Interinstitutional Security Center for Technical Response to Computer Incidents in Guatemala (CSIRT-GT), according to Jorge Villagrán, president of the National Security Affairs Commission for 2024. For his part, Germán López, a member of the Cybersecurity Banking Community (Bancert), in Guatemala there is still no organization in charge of responding to attacks on the web.

SENATE ANALYZES HOW TO REGULATE ARTIFICIAL INTELLIGENCE - MEXICO

El Sol de México - Six talks are organized to listen to academics and companies to reach a consensus on how to regulate it. The Senate of the Republic is analyzing how to regulate Artificial Intelligence (AI), which is why it began a series of talks with academic institutions and companies, said Rolando Zapata Bello, president of the Commission for Analysis, Monitoring and Evaluation on the Application and Development of Artificial Intelligence. "It cannot be that such a relevant activity that is becoming increasingly important does not have regulation. This gap must be filled with a regulatory framework that promotes balance: regulating, but without inhibiting technological development," said the PRI legislator.

CYBERSECURITY AS A PENDING ISSUE FOR CRITICAL INFRASTRUCTURES

Segurilatam - Latin America is one of the regions most targeted by cybercriminals. And within it, critical infrastructures and essential services are a juicy target due to the criticality - excuse the redundancy - of their systems. Hence, cybersecurity must be one of the main strategic axes of this type of organization. But where should those responsible for cybersecurity of critical infrastructures have the greatest impact?

THE GOVERNMENT PROMOTES A LAW THAT WILL CREATE A NATIONAL CYBERSECURITY CENTER - SPAIN

Infobae - The Council of Ministers approved this Tuesday the draft Law on Cybersecurity Coordination and Governance, which provides for the creation of a National Cybersecurity Center and specific measures to be adopted by vital sectors, both public and private, to strengthen their protection against cyberattacks.

THE EXECUTIVE APPROVES THE DRAFT OF THE CYBERSECURITY GOVERNANCE LAW THAT AFFECTS BANKING, TRANSPORT AND ENERGY - SPAIN

Euorpa Press - The Council of Ministers approved this Tuesday the draft of the Law on Coordination and Governance of Cybersecurity, a regulation that, in compliance with a European directive, seeks to increase security in the face of "serious threats" to public or private entities in sectors related to energy, transport, banking and financial markets, as well as the health sector and infrastructure.

BIDEN ADMINISTRATION LAUNCHES CYBERSECURITY EXECUTIVE ORDER - USA

CNBC -The Biden administration on Thursday announced an executive order on cybersecurity that imposes new standards for companies selling to the U.S. government and calls for greater disclosure from software providers. The White House is looking to put in place new rules “to strengthen America’s digital foundations,” Anne Neuberger, deputy national security advisor for cybersecurity and emerging technology, said in a briefing with reporters on Wednesday.

CISA RELEASES THE JCDC AI CYBERSECURITY COLLABORATION PLAYBOOK AND FACT SHEET - USA

CISA - Today, CISA released the JCDC AI Cybersecurity Collaboration Playbook and Fact Sheet to foster operational collaboration among government, industry, and international partners and strengthen artificial intelligence (AI) cybersecurity. The playbook provides voluntary information-sharing processes that, if adopted, can help protect organizations from emerging AI threats.

HOW AI-DRIVEN FRAUD CHALLENGES THE GLOBAL ECONOMY – AND WAYS TO COMBAT IT

WEF - Cybercrime is draining resources from businesses and governments worldwide. Global cybercrime is expected to cost $10.5 trillion annually by 2025, up from $3 trillion in 2015. To put it in perspective, if annual cybercrime were a country, it would have the third-largest gross domestic product (GDP) worldwide.
Fraud, a common type of cybercrime, is poised for unprecedented acceleration thanks to the advent of generative AI (GenAI).

WHY USING IT CYBERSECURITY TO PROTECT OT PUTS INDUSTRIAL ORGANIZATIONS AT RISK

WEF- Rising cyberattacks on operational technology (OT) systems endanger critical infrastructure, impacting energy, water and manufacturing globally. CEOs must distinguish between IT and OT cybersecurity to protect data and industrial operations effectively. Tailored OT cybersecurity controls – such as ICS response plans and defensible architectures – can safeguard critical systems and ensure operational continuity.

BIDEN'S CYBER AMBASSADOR URGES TRUMP NOT TO CEDE GROUND TO RUSSIA AND CHINA IN GLOBAL TECH FIGHT - USA

Wired - America's outgoing cyber ambassador has a warning for his successors in the incoming Trump administration: Stay engaged with tech and digital security debates on the world stage, because otherwise, Russia and China will fill the void."An increasingly isolationist United States creates or amplifies a lot of problems that we're not going to be able to turn our backs on," says Nathaniel Fick, who has spent almost two and a half years as the US's first ambassador at large for cyberspace and digital policy. "We may not be interested in the world, but the world is interested in us."

HOW BUSINESSES ARE COPING WITH EVER-INCREASING GEOPOLITICAL RISKS

WEF - Businesses worldwide are embracing digital evolution. Yet cybersecurity implications inevitably emerge as technologies evolve and push us into a new era of connectivity. Adopting new technologies, devices and platforms increases potential points of compromise, widening an organization's attack surface. Having more digital systems to configure, integrate and manage leads to greater complexity and an increased likelihood of error.