DIGI AMERICAS LATAM CISO

INSIGHTS

MARCH 6, 2025

DIGI AMERICAS ALLIANCE MEMBERS

NATIONAL POLICE ADVANCES TOWARDS THE DIGITAL ERA WITH THE CREATION OF THE CENTRAL DIRECTORATE OF DIGITAL TRANSFORMATION - DOMINICAN REPUBLIC

Government of the Dominican Republic - The Central Directorate of Planning and Development (DIPLAN) of the National Police presented to a commission of high-ranking officers the proposal to define the operational guidelines of the Central Directorate of Digital Transformation, a new department that will promote the technological modernization of the National Police.

CHILE BEGINS THE OBLIGATION TO REPORT CYBERSECURITY INCIDENTS TO THE ANCI

Geek Alert - Entities have up to a maximum of three hours to report. One of the most important measures regarding cybersecurity in Chile is already active. Since the beginning of March, companies and organizations that provide essential services in Chile are required to report cybersecurity incidents to the National Cybersecurity Agency (ANCI).

WITH THE UPDATE OF THE INFORMATION SECURITY AND PRIVACY MODEL, THE ICT MINISTRY STRENGTHENS DIGITAL SECURITY IN THE COUNTRY'S PUBLIC ENTITIES - COLOMBIA

MinTIC - Every day, public entities in the country face an increasing risk of digital security incidents. This situation led the ICT Ministry to intensify its commitment to the protection of IT assets and the guarantee of continuity in the provision of services to citizens. As a result, and aware of the digital vulnerability of State institutions, the entity has developed policies and strategies that aim to guarantee the safe and efficient use of information and communications technologies (ICT).

DIGI AMERICAS LATAM CISO

INSIGHTS

MARCH 6, 2025

MINISTRY OF JUSTICE AND FEBRABAN LAUNCH ALLIANCE AGAINST DIGITAL FRAUD - BRASIL

E.M.FOCO - In response to the significant increase in banking and digital fraud, the Brazilian Ministry of Justice and Public Security, in partnership with the Brazilian Federation of Banks (Febraban), has launched a strategic initiative. This alliance seeks to strengthen digital security by promoting actions to prevent and repress cybercrimes. The collaboration between the government and the banking sector aims to create a safer digital environment, centralizing reporting channels and improving the exchange of information between the parties involved. The initiative is the result of a previously signed technical agreement, with the aim of addressing the challenges posed by modern fraud.

BRAZIL AND THE UNITED KINGDOM JOIN FORCES AGAINST DIGITAL ATTACKS IN GLOBAL EXERCISE; CYBER DEFENSE AND DIGITAL SECURITY ON THE AGENDA

sociedademilitar - The digital war has already begun, and Brazil is on the front line! The Brazilian Army's Cyber Defense Command (ComDCiber) is participating in Defense Cyber Marvel 4 (DCM4), one of the most sophisticated international cyber warfare exercises. Coordinated by the United Kingdom Army, the event, which takes place from February 23 to 28, 2025, is based in Seoul, South Korea. However, the mixed team from Brazil and the United Kingdom present in this defense exercise operates remotely from Forte Marechal Rondon, in Brasília-DF.

PRIME MINISTER URGES DEVELOPMENT OF AI AND CYBERSECURITY IN CUBA

Prensa Latina - Cuban Prime Minister Manuel Marrero called for promoting the development of key technologies such as artificial intelligence (AI), cybersecurity and robotics during the review of the Ministry of Communications, Granma newspaper reported today. During the meeting chaired by Cuban President Miguel Díaz-Canel, the head of government urged the organization to improve the quality of services, increase foreign exchange earnings and referred to the need to maintain adequate control of electronic commerce.

TSMC TO INVEST OVER $100 BILLION IN US CHIP PLANTS

dpl news - Taiwan Semiconductor Manufacturing Company Limited (TSMC), considered the largest semiconductor manufacturer in the world, announced together with the President of the United States, Donald Trump, a historic investment of 100 billion dollars. This investment will focus on strengthening its semiconductor manufacturing operation in Arizona. And, according to the White House, it is the largest foreign direct investment in the history of the United States.

DIGI AMERICAS LATAM CISO

INSIGHTS

MARCH 6, 2025

EU PRIORITISES CYBERSECURITY AS RUSSIAN HYBRID ATTACKS RISE

infobae - The Vice-President of the European Commission for Technological Sovereignty, Security and Democracy, Hanna Virkkunen, and the Polish Minister for Digitalisation, Krzysztof Gawkowski, agreed this Wednesday to highlight cybersecurity as a fundamental priority for the European Union (EU) in the face of the increase in hybrid attacks from Russia.

THE IMPORTANCE OF EARLY MEDIA LITERACY IN THE AGE OF MISINFORMATION

The Conversation - The growing spread of misinformation and malicious content, reinforced by the use of artificial intelligence (AI), places young people at the centre of vulnerability to hate speech and discriminatory stereotypes. In this scenario, we see how phygital culture – the convergence of the physical and the digital – fuses both realities into a single, uninterrupted experience. From increasingly early ages, new generations access mobile devices and social networks, determining their vision of the world.

HOW AI CAN HELP INCREASE CYBERSECURITY CAPABILITIES

Forbes - Artificial intelligence (AI) is one of the most important technological advancements of the digital age. In particular, generative AI (GenAI), which thanks to its ability to create more realistic text, images, and other content, has gone from being considered a fun online tool to becoming a vital part of many services and applications that organizations rely on. This change in application came at a crucial time. With more people working remotely, companies began to rely on cloud-based services and connected networks, including Internet of Things (IoT) devices and industrial equipment. These networks became more complex and fluid, making it difficult for existing, more traditional security systems to keep up.

DHS SAYS CISA WON'T STOP LOOKING AT RUSSIAN CYBER THREATS - USA

Cyberscoop - The Department of Homeland Security said that its Cybersecurity and Infrastructure Security Agency will continue to pay attention to Russian cyber threats, contrary to media reports suggesting the opposite. The Guardian reported last week that a recent CISA memo setting out priorities for the agency didn't list Russia among them, while including Chinese threats and critical infrastructure protection. It further reported that analysts at the agency were verbally told not to follow or report on Russian cyber threats.

DIGI AMERICAS LATAM CISO

INSIGHTS

MARCH 6, 2025

THE EVOLVING DYNAMICS OF DDOS ATTACKS

Cyber Magazine - Distributed denial of service attacks levels are such that cybersecurity professionals must explore new methods of defence in order to stay secure. The cybersphere is in a precarious place. The digital frontier is expanding as more companies push for digital transformation, but as the infrastructure does, so does the attack surface. A new wave of Distributed Denial of Service (DDoS) attacks has introduced a significant variable into the cybersecurity equation. Yet as we delve into the current state of DDoS attacks, it becomes clear that this resurgence is not merely a rehashing of old tactics.

IDENTITY: THE NEW CYBERSECURITY BATTLEGROUND

The Hacker News - The rapid adoption of cloud services, SaaS applications, and the shift to remote work have fundamentally reshaped how enterprises operate. These technological advances have created a world of opportunity but also brought about complexities that pose significant security threats. At the core of these vulnerabilities lies Identity—the gateway to enterprise security and the number one attack vector for bad actors. Explore the importance of modernizing Identity strategies and the benefits of centralizing Identity within your security ecosystem to safeguard your organization from costly breaches while enhancing operational efficiency.

CYBERSECURITY NEWS: CISA DENIES CLAIMS, RANSOMWARE GROUP CLAIMS ATTACK, LATIN AMERICA'S SECURITY CRISIS

CISO Series - CISA denies claims of deprioritizing Russian threats. CISA is pushing back against reports that it has been directed to stop tracking Russian cyber threats, calling the claims “fake” and a risk to national security. This is an update to a story that first appeared over the weekend, in which The Guardian reported that a memo deprioritizing Russia was issued—an allegation that CISA and DHS officials deny, with one calling the report “garbage.” Meanwhile, The Record, The New York Times, and The Washington Post confirm that U.S. Cyber Command has been ordered to pause offensive cyber operations against Russia while negotiations over the war in Ukraine continue. Lawmakers on both sides are criticizing any shift, warning that it could weaken U.S. defenses against Russian cyber threats.

HOW DIGITAL TWIN TECHNOLOGY CAN ENHANCE CYBERSECURITY

WEF - For many, the first thing that comes to mind when discussing digital twins is a 3D replica of real-world objects. But in reality there is more to it than that. A digital twin is a digital representation of a physical object, system, or process with synchronized bidirectional interaction with its real-world counterpart. They are primarily categorized into the following types: Component Twin, Product Twin, Process Twin, System Twin.