DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 20, 2026

DIGI AMERICAS ALLIANCE MEMBERS

INSTITUIÇÕES FINANCEIRAS TÊM QUE SE ADAPTAR ÀS NOVAS EXIGÊNCIAS DE SEGURANÇA CIBERNÉTICA - BRASIL

Infor Channel - As instituições financeiras autorizadas a funcionar pelo Banco Central do Brasil têm até o dia 1º de março para se adequarem às novas exigências de Segurança Cibernética determinadas pela Resolução CMN nº 5.274/2025, publicada em dezembro do ano passado, pelo Conselho Monetário Nacional. Essa Resolução altera a Resolução CMN nº 4.893/2021, que dispõe sobre a política de Segurança Cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de Dados e de Computação em Nuvem a serem observados pelas instituições financeiras.

COMPUTAÇÃO QUÂNTICA EM 2026: COMO A NOVA TECNOLOGIA PODE REDEFINIR A SEGURANÇA GLOBAL - BRASIL

RealTime1 - Enquanto a inteligência artificial domina o debate público, uma transformação ainda mais profunda avança nos laboratórios de grandes potências: a computação quântica. Diferente dos computadores tradicionais, que operam com bits (0 e 1), máquinas quânticas utilizam qubits, capazes de processar múltiplos estados simultaneamente. O potencial é disruptivo. A computação quântica promete resolver problemas considerados intratáveis por supercomputadores atuais — da descoberta de novos materiais à otimização logística complexa. Mas há um ponto crítico: segurança digital.

MUNDIAL 2026 PONE A PRUEBA CIBERSEGURIDAD - MÉXICO

Yo Influyo - México se prepara para recibir uno de los eventos deportivos más importantes del planeta: la Copa Mundial de Futbol 2026. La expectativa se concentra en la logística, la derrama económica y el turismo, pero hay otro frente que ya genera alertas entre autoridades y especialistas: la seguridad digital. La combinación de millones de visitantes, un aumento acelerado del comercio electrónico y el manejo masivo de datos personales coloca a la infraestructura tecnológica del país ante una presión inédita. El torneo, que México compartirá con Estados Unidos y Canadá, implicará un incremento extraordinario en transacciones electrónicas, servicios en línea, compras digitales y operaciones financieras en tiempo real.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 20, 2026

IDENTITY EMERGES AS CYBERSECURITY'S NEW CONTROL LAYER – MÉXICO

Mexico Business News - Cyber risk keeps escalating from a technical issue to a systemic economic and reputational threat. Mexico's rise among the most targeted ransomware markets, combined with projections of tens of millions of additional attacks tied to the 2026 World Cup, reinforces that scale events now amplify national attack surfaces. The landmark acquisition of CyberArk by Palo Alto Networks formalized identity security as foundational to zero trust and AI-era defense. Simultaneously, LLM-enabled malware demonstrated that advanced attacks no longer require advanced skills. The narrative is clear: cybersecurity investment is moving from reactive defense to ROI-driven identity governance as a board-level priority.

TREASURY ANNOUNCES PUBLIC-PRIVATE INITIATIVE TO STRENGTHEN CYBERSECURITY AND RISK MANAGEMENT FOR AI – USA

U.S. Treasury - In support of the President's AI Action Plan, the U.S. Department of the Treasury today announced the conclusion of a major public-private initiative to strengthen cybersecurity and risk management for artificial intelligence (AI) in the financial services sector. Over the course of February, Treasury will release a series of six resources developed in partnership with industry and federal and state regulatory partners to enable secure and resilient AI across the U.S. financial system. "As this Administration has made clear, it is imperative that the United States take the lead on developing innovative uses for artificial intelligence, and nowhere is that more important than in the financial sector," said Secretary of the Treasury Scott Bessent. "This work demonstrates that government and industry can come together to support secure AI adoption that increases the resilience of our financial system."

DOD LEADERS WARN AI, CRYPTOCURRENCY 'LOWERS THE BAR' FOR CYBERCRIMINALS – USA

Defense Scoop - Top Defense Department officials focused on combating cybercrime said Thursday that artificial intelligence and cryptocurrency are making it easier for nefarious actors to threaten national security and circumvent traditional financial tracking systems. The warning comes amid what the officials described as a rapidly changing threat environment, one that allows for low-level criminals to adopt sophisticated cyber exploitation methods and adversarial countries to obscure their actions, often in tandem.

LA CEPAL ALERTA QUE FRAGILIDAD DIGITAL AMENAZA ESTABILIDAD EN EL CARIBE

El Dinero - La **Comisión Económica para América Latina y el Caribe (Cepal)** advirtió que la vulnerabilidad estructural de la infraestructura digital del Caribe puede comprometer la **estabilidad económica** y la continuidad gubernamental de los Estados, y propuso crear un mecanismo de respaldo internacional para proteger **información crítica** ante desastres naturales, ciberataques y fallas de conectividad. Así lo establece el estudio Embajadas de Datos: un enfoque innovador para fortalecer la resiliencia digital en el Caribe, elaborado por Tyra Greene y Dimitris Heráclеo, presentado de manera virtual por el organismo regional.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 20, 2026

EL CRIMEN DIGITAL YA OPERA A VELOCIDAD RÉCORD Y LA IDENTIDAD SE CONVIERTE EN LA NUEVA VULNERABILIDAD

Technocio - En 2025, el 25% más veloz de los ataques robó datos en 72 minutos y el 87% de las intrusiones cruzó múltiples superficies a la vez. Unit 42, el equipo de investigación y respuesta a incidentes de Palo Alto Networks publicó su Global Incident Response Report 2026, un análisis de más de 750 casos atendidos entre 2024 y 2025 que muestra un cambio de ritmo en el delito digital y confirma que la identidad —es decir, las cuentas y permisos de usuarios y servicios que dan acceso a sistemas y datos; por ejemplo, el usuario y contraseña de un empleado— es hoy la vía más usada para entrar y moverse dentro de las organizaciones. En 2025, el 25% más veloz de los ataques robó datos en 72 minutos y el 87% de las intrusiones cruzó múltiples superficies a la vez. Además, casi 90% de las investigaciones incluyó fallas de identidad como factor determinante, y 99% de las identidades en la nube tenía privilegios excesivos.

CIBERSEGURIDAD Y RESILIENCIA EN LOS SERVICIOS ESENCIALES

Segurilatam - En un escenario global marcado por la incertidumbre, la interdependencia y el aumento de las amenazas híbridas, proteger los servicios esenciales y las infraestructuras críticas que los sustentan se ha convertido en una prioridad estratégica para cualquier país. No obstante, no es una preocupación reciente. En España, la atención a estos activos se remonta, al menos, a 2011, con el desarrollo de la Ley 8/2011, que establecía medidas para la protección de las infraestructuras críticas y que ya reconocía la dependencia creciente de estos servicios respecto de las tecnologías de la información y la comunicación.

NUEVA ALIANZA ENTRE CLOUDFLARE Y MASTERCARD AUTOMATIZA LA DEFENSA CONTRA CIBERAMENAZAS

Panama24Horas - Cloudflare, empresa de conectividad cloud, y Mastercard anunciaron una asociación estratégica diseñada para desarrollar herramientas de protección destinadas a pequeñas empresas, infraestructuras críticas y gobiernos. El objetivo principal de este acuerdo es defender a estas organizaciones de las ciberamenazas actuales sin obstaculizar su capacidad de innovación tecnológica. La alianza combina las funciones de monitoreo de superficie de ataque de Recorded Future y RiskRecon de Mastercard con el conjunto de soluciones de seguridad de aplicaciones de Cloudflare. Esta unión permite a millones de usuarios mapear, priorizar y automatizar la corrección de riesgos ocultos en sus entornos conectados a internet a través de una plataforma unificada.

EVOLVING RANSOMWARE TACTICS WITH AI-ENHANCED ATTACKS AND RANSOMWARE AS A SERVICE

FinancierWorldwide - The UK government has estimated that the cost of cyber attacks to UK businesses is more than £14bn and suggests that the UK is the most targeted country by threat actors in Europe. According to a 2025 survey by the Home Office, 612,000 businesses identified a cyber attack in the preceding 12 months – and those are just the businesses that submitted a report, with the true figure likely to be significantly higher. Developments in ransomware as a service (RaaS) and subsequently artificial intelligence (AI) have led to these attacks becoming increasingly sophisticated and complex, meaning more than ever businesses need to proactively manage and improve the resilience of their systems.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 20, 2026

CYBERSECURITY GUIDANCE FOR DATA CENTER POWER AND COOLING INFRASTRUCTURE SYSTEMS

Data Center Dynamics - Network connected power, cooling, and environmental systems increase operational visibility and efficiency but also expand the cyber attack surface. This whitepaper outlines a practical framework to evaluate vendors, harden OT networks, and embed cybersecurity across design, installation, and operations. Vendor security maturity and lifecycle alignment: How to assess secure development lifecycle practices, independent certifications, vulnerability management processes, and transparency to ensure infrastructure is secure by design. Defense in depth and zero trust network architecture: Best practices for perimeter hardening, VLAN segmentation, firewall configuration, encrypted protocols, least privilege access, and continuous verification across OT environments. Operational vigilance and incident readiness: How to maintain firmware updates, preserve security settings, monitor anomalies, implement structured incident response plans, and leverage managed cybersecurity services to sustain resilience over time.

THE CYBER THREATS TO WATCH IN 2026 – AND OTHER CYBERSECURITY NEWS

WEF - Accelerating AI adoption, geopolitical fragmentation and widening cyber inequity are reshaping the global risk landscape, finds the latest Global Cybersecurity Outlook from the World Economic Forum.
Based on data from 800 global leaders, the 2026 report reveals that as attacks grow faster, become more complex and unevenly distributed, organizations and governments face rising pressure to adapt amid persistent sovereignty challenges and widening capability gaps. In the face of these challenges, three clear themes emerge: AI is supercharging the cyber arms race, geopolitics is a defining feature of cybersecurity, and cyber-enabled fraud is threatening CEOs and households alike.

HACKERS EXPLOIT ZERO-DAY FLAW IN DELL RECOVERPOINT FOR VIRTUAL MACHINES

Cybersecurity Dive - Threat actors are weaponizing a zero-day vulnerability in Dell RecoverPoint for Virtual Machines in a cyberattack campaign that drops a novel backdoor, according to new findings from Mandiant and Google Threat Intelligence Group. The product allows users to manage backup and disaster recovery for VMware virtual machines. The vulnerability, listed as CVE-2026-22769, is a hardcoded credential vulnerability that can allow an unauthenticated attacker to gain access to an underlying system and maintain root-level persistence. The vulnerability has a severity score of 10.