DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 9, 2026

DIGI AMERICAS ALLIANCE MEMBERS

CHILE | ANCI PRESENTA SU PRIMER BALANCE ANUAL

dpl news - Con el fin del 2025 concluyó en la Agencia Nacional de Ciberseguridad (ANCI) su etapa de instalación, cumpliéndose un año de su creación y terminando el período de su primer director nacional, Daniel Álvarez Valenzuela. Con la presencia de autoridades de Gobierno, del Congreso, del Poder Judicial, fuerzas policiales, servicios públicos, gremios, academia y representantes internacionales, la Agencia Nacional de Ciberseguridad (ANCI) presentó su Primer Balance Anual, marcando un hito en la consolidación de la institucionalidad de ciberseguridad en Chile.

ARGENTINA CREA EL CENTRO NACIONAL DE CIBERSEGURIDAD

mobile time latino america - El gobierno de Argentina avanzó en una reorganización integral del Sistema de Inteligencia Nacional mediante un decreto el primero de enero de 2026, que introduce cambios estructurales en la gobernanza del ciberespacio y crea el Centro Nacional de Ciberseguridad (CNC) como nueva autoridad nacional en la materia. La medida redefine competencias entre organismos, separa formalmente las funciones de ciberseguridad y ciberinteligencia, y otorga un nuevo marco institucional para la protección de infraestructuras críticas digitales, redes de telecomunicaciones y activos estratégicos del Estado, de acuerdo con un boletín oficial.

MÉXICO PRESENTA SU PRIMER PLAN NACIONAL DE CIBERSEGURIDAD, CENTRADO EN LA CIBERRESILIENCIA Y LA PREVENCIÓN

El Español - Situar a México a la vanguardia internacional como un referente de la región en ciberresiliencia y contribuir a reducir el riesgo de ataques digitales, a partir de un modelo enfocado en la prevención. Esa es la meta con la que nace el Plan Nacional de Ciberseguridad de México, una iniciativa histórica que establece el primer marco de política especializada en ciberseguridad del país. Este plan, presentado por la ATDT, nace para “homologar respuestas ante cualquier amenaza a la infraestructura y sistemas en línea de las instituciones y entidades gubernamentales” y contempla una nueva política nacional y un marco federal que incluirá lineamientos con medidas obligatorias, capacitación a servidores públicos y reportes de incidencias, entre otras regulaciones que, esperan desde el Gobierno mexicano, poder publicar a lo largo de 2026.

DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 9, 2026

EXÉRCITO BRASILEIRO VAI AMPLIAR DEFESA CIBERNÉTICA COM USO DE INTELIGÊNCIA ARTIFICIAL; SAIBA COMO

Times Brasil - O Exército Brasileiro ganhará uma série de novas tecnologias e equipamentos. Isso porque, em novembro de 2025, a Lei Complementar 221 garantiu que R$ 30 bilhões fossem excluídos do arcabouço fiscal e destinados a investimentos para a defesa brasileira. Dessa forma, ao longo de 2026 e 2031, o PAC Militar deve passar a utilizar R$ 3 bilhões a cada ano para modernizar os recursos da defesa. Portanto, além de uma nova frota de blindados, o Centauro II-BR, o exército contará também com uma defesa cibernética expandida, que incluirá o uso de inteligência artificial (IA). A seguir, veja como a IA pode melhorar a defesa brasileira.

COSTA RICA FORTALECE SU POSICIÓN COMO HUB DE CENTROS DE CAPACIDAD GLOBAL

elmundo.cr - osta Rica continúa ofreciendo condiciones ideales para el establecimiento de centros de excelencia. A lo largo de los años, el país ha atraído una variedad de modelos de prestación de servicios, incluidos los Centros de Servicios Compartidos (SSC) y los Centros de Capacidad Global (GCC), cada uno contribuyendo al desarrollo y la diversificación del ecosistema de servicios empresariales. Estos centros permiten a las compañías multinacionales fortalecer operaciones, construir capacidades estratégicas, impulsar la innovación y mejorar la calidad de los procesos, al tiempo que optimizan la capacidad de respuesta a clientes en distintos husos horarios —un elemento clave del modelo global follow-the-sun que habilita colaboración continua y prestación constante de servicios—.

EMPRESA DE CIBERSEGURIDAD CROWDSTRIKE COMPRA LA STARTUP SGNL POR 740 MILLONES DE DÓLARES

infobae - La empresa de ciberseguridad y tecnología CrowdStrike anunció este jueves un acuerdo para la adquisición de la empresa emergente SGNL, especializada en la protección de identidades de inteligencia artificial (IA), por un monto de unos 740 millones de dólares. "Estamos comprometidos con nuestros clientes en proporcionarles las tecnologías que necesitan para proteger todo tipo de identidades en la era de la inteligencia artificial", destacó CrowdStrike en el comunicado en el que anunció el acuerdo de adquisición de la empresa emergente SGNL. El acuerdo está valorado en un total de unos 740 millones de dólares, que se espera que se cierre en el primer trimestre fiscal de 2027, según recogen varios medios económicos

CISA ADDS TWO KNOWN EXPLOITED VULNERABILITIES TO CATALOG

CISA.gov - CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.

- CVE-2009-0556 Microsoft Office PowerPoint Code Injection Vulnerability
- CVE-2025-37164 HPE OneView Code Injection Vulnerability

These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise. Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities established the KEV Catalog as a living list of known Common Vulnerabilities and Exposures (CVEs) that carry significant risk to the federal enterprise. BOD 22-01 requires Federal Civilian Executive Branch (FCEB) agencies to remediate identified vulnerabilities by the due date to protect FCEB networks against active threats. See the BOD 22-01 Fact Sheet for more information.

DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 9, 2026

ENHANCING PORT SECURITY: FIVE ESSENTIAL STRATEGIES FOR LATIN AMERICA

Maritime Fair Trade - Latin America's ports are grappling with significant security challenges, heavily influenced by rising drug-related violence and cyber threats. The region has seen a surge in criminal activities linked to its ports, most notably with Ecuador's Guayaquil where drug gangs are engaging in violent turf wars. Chile has similarly experienced increased crime tied to port activities. A 2021 report by the Organization of American States (OAS) reveals that ports in the Western Hemisphere are vulnerable to cyberattacks due to rapid digitalization. These attacks, often involving ransomware, can paralyze operations, as illustrated by the 2017 NotPetya incident that caused substantial financial losses for Maersk.

COMPLEX ROUTING, MISCONFIGURATIONS EXPLOITED FOR DOMAIN SPOOFING IN PHISHING ATTACKS

Security Week - Threat actors have been observed abusing complex routing and improperly configured spoof protections in phishing attacks, Microsoft warns. By spoofing legitimate domains, the attackers make their phishing emails more effective, as they appear to have been sent internally. The attack vector, Microsoft says, has been used in opportunistic campaigns powered by phishing-as-a-service (PhaaS) platforms such as Tycoon2FA, targeting several industries. The phishing messages contain lures related to document sharing, HR communication, invoices, password resets, and voicemails, leading to the compromise of credentials that may be abused for business email compromise (BEC) or data theft.

HOW CYBER WARFARE IS BECOMING THE FIRST STRIKE IN MODERN CONFLICTS

The Street - The pre-dawn raid that saw U.S. special operations forces seize President Nicolás Maduro of Venezuela and his wife, Cilia Flores, reportedly began with cyber-attacks that cut off power to large areas of the South American country's capital city to allow planes and helicopters to strike key military sites. President Donald Trump suggested that the U.S. used cyberattacks or other technical capabilities to cut power off in Caracas, according to Politico. Last month, Venezuelan national oil and gas company PDVSA, or Petróleos de Venezuela, S.A., accused the U.S. government of carrying out a cyberattack that led to delays in operations across the country. Whether or not cyberattacks were the decisive factor in Caracas, the episode highlights how digital warfare has become a standard opening move in modern conflicts.

CLOUDFLARE POURS COLD WATER ON 'BGP WEIRDNESS PRECEDED US ATTACK ON VENEZUELA' THEORY

The Register - Cloudflare has poured cold water on a theory that the USA's incursion into Venezuela coincided with a cyberattack on telecoms infrastructure. The theory came from red team engineer Graham Helton who, on his personal blog noted that President Trump said the USA used "certain expertise" to turn off lights in the Venezuelan city of Caracas before the attack, and that the chairman of the Joint Chiefs of Staff, general Dan Caine, said US Cyber Command played a role too. "While we can't say with certainty what caused this route leak, our data suggests that it's likely cause was more mundane," Herdes wrote. "That's in part because BGP route leaks happen all of the time, and they have always been part of the Internet — most often for reasons that aren't malicious."