DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 10, 2025

DIGI AMERICAS ALLIANCE MEMBERS

ATAQUE HACKER: O QUE SABEMOS SOBRE GOLPE QUE DESVIOU R$ 541 MILHÕES - BRASIL

CNN Brasil - Um ataque hacker realizado nesta semana contra a empresa C&M Software resultou em um desvio de R$ 541 milhões da instituição de pagamento BMP. Até o momento, um homem, identificado como João Nazareno Roque, foi preso suspeito de estar envolvido no que é considerado pela Polícia Civil de São Paulo "o maior golpe cibernético contra instituições financeiras do país". De acordo com João Roque, o ponto inicial para o ataque hacker teria começado em março, em uma saída de bar no Jaraguá, bairro da zona Oeste de São Paulo. O suspeito, em depoimento à Polícia, disse que foi abordado por um outro homem, que teria afirmado que gostaria de conhecer os sistemas da empresa C&M Software, onde João trabalhava.

MINDEFENSA LANZA NUEVA ESTRATEGIA PARA COMBATIR DELITOS CIBERNÉTICOS: DE ESTO SE TRATA - COLOMBIA

Caracol Radio - En un contexto donde la digitalización ha impulsado la productividad tanto en el sector público como en el privado, Colombia enfrenta nuevos y complejos desafíos en materia de ciberseguridad. Tanto que aunque se han reducido en un 16% este año, van 24.959 delitos informáticos a nivel nacional.
No obstante, el ministerio de Defensa anunció que desde 2011, cuando se emitió el documento CONPES 3701, el país inició un camino institucional hacia la protección del entorno digital en el ámbito de la defensa.

MITIC Y SENADO CONVERSARON SOBRE ACCIONES PARA FORTALECER LA CIBERSEGURIDAD - PARAGUAY

dplnews - El ministro Gustavo Villate y el equipo técnico del Ministerio de Tecnologías de la Información y Comunicación (Mitic) se reunieron con miembros de la mesa directiva de la Cámara de Senadores para abordar aspectos de la ciberseguridad y gestiones que se llevan a cabo en ese ámbito. Uno de los puntos compartidos fue el fortalecimiento de la cultura de protección digital como el uso de contraseñas robustas, al considerar que la mayoría de los incidentes cibernéticos de los últimos meses se originaron a partir de claves débiles o sistemas no actualizados.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 10, 2025

DEL HACKEA A LA ESTRATEGIA DE CIBERSEGURIDAD SIN LEY - PARAGUAY

abc - Ciberataques constantes han puesto en evidencia la debilidad del entorno digital gubernamental en el que hasta el presidente Santiago Peña fue vulnerado, mientras el país evoluciona en un entorno de transformación tecnológica sin normativa y leyes para proteger y potenciar el ecosistema digital paraguayo. La Estrategia Nacional de Ciberseguridad 2025-2028 presentada de forma confidencial en el Palacio de Lopez, tras el hackeo de la cuenta de la red social X del Presidente de la República, busca frenar el asedio constante al ecosistema digital violentado en varias ocasiones hasta de forma irónica en contra del ministro responsable de las políticas públicas de este sector.

CON EL HACKEO A LAMBARÉ, SUMAN 32 ENTES PÚBLICOS ATACADOS POR CIBERDELINCUENTES - PARAGUAY

Ultima Hora - La Municipalidad de Lambaré y la Dirección Nacional de Contrataciones Públicas (DNCP) se suman a la lista de entes públicos que fueron hackeados por el grupo de ciberdelincuentes CyberTeam. Ambas fueron atacadas en horas de la tarde y noche del miércoles. Esto fue informado por el mismo grupo a través de su cuenta en X @cyberteam2009. En ambos casos, este grupo se burló de la ciberseguridad. Sobre Lambaré, posteó lo siguiente: “Adivina ¿quién se cayó otra vez? ¿Contraseña? lambare2010. Mientras Villate hablaba de seguridad, el CyberTeam ya estaba conectado, leyendo correos y eligiendo un fondo de pantalla”.

CIBERCRIMEN 2025: INTELIGENCIA ARTIFICIAL, HACKTIVISMO Y EL COLAPSO DEL PERÍMETRO DIGITAL

Infobae - Durante el primer semestre de 2025, el escenario de ciberseguridad global se volvió más crítico, más complejo y profundamente transversal. El crecimiento sostenido del cibercrimen, impulsado por tecnologías emergentes y tensiones geopolíticas, desafía la capacidad de reacción de gobiernos, empresas y usuarios. El sector salud, por primera vez en el año, se convierte en un objetivo buscando afectar al público en cuestiones sumamente sensibles, presionando como nunca a la industria. Datos personales, historias clínicas y exámenes médicos están a la orden del día, cerca del 39% de las amenazas provienen de plataformas móviles mediante técnicas de phishing. No se trata solo de datos, hablamos de dificultades operativas, tratamientos revelados, confidencialidad vulnerada. El impacto es físico, emocional y financiero.

AUSENCIA DE LA CIBERSEGURIDAD: FRAUDES DIGITALES, PROBLEMA GRAVE PARA INTERNAUTAS

Diaro de Yucatan - “La evolución de los defraudadores en la era digital, ya no se trata del defraudador común que te vendía espejitos en la calle, ahora se han sofisticado con las nuevas tecnologías, y la manera de obtener información es a través del fraude cibernético, que no debe confundirse con los ciberataques”, advirtió Rafael Cortez Melecio, presidente nacional del Consejo de Empresarios en Tecnología, Innovaciones y Comunicaciones (Cetic). Los ciberataques, según Cortez Melecio, implican que un “hacker” penetra sistemas expuestos en Internet para obtener información, y en gran parte, se debe también por la falta de cultura de ciberseguridad.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 10, 2025

SECURITY COALITION URGES CONGRESS TO RENEW 2015 CISA LAW - USA

Cybersecurity Dive - Congress must reauthorize a cybersecurity threat information sharing law before it expires in October, a group of leading technology companies told lawmakers on Monday. The 2015 Cybersecurity Information Sharing Act “has enabled rapid dissemination of actionable threat intelligence to protect networks before an incident occurs, more coordinated responses to cyber incidents; and improved situational awareness across multiple sectors,” the Hacking Policy Council said in a letter to House and Senate homeland-security committee leaders.

QANTAS CONFIRMS PERSONAL DATA OF OVER A MILLION CUSTOMERS LEAKED IN BREACH - AUSTRALIA

Reuters - Australia's Qantas Airways (QAN.AX), opens new tab said on Wednesday more than a million customers had their phone number, birth date or home address accessed in one of the country's biggest cyber breaches in years. The airline operator said that another four million customers had just their name and email address taken during the hack.

SCATTERED SPIDER POSES SERIOUS RISK TO SEVERAL HUNDRED MAJOR COMPANIES

Cybersecurity Dive - The cybercrime group Scattered Spider’s tactics put a group of roughly 300 major companies at heightened risk of attack, according to a new report from security firm CyberCube. The 287 firms represent approximately 2% of organizations with revenues above $500 million, according to CyberCube’s analysis of more than 15,000 companies in key global markets. The analysis covers eight regions, including the U.S., the U.K., Canada, Australia, Germany, France, Japan and Singapore.

NEED TO DEVELOP OT CYBERSECURITY PROGRAMS TO BRIDGE IT AND ENGINEERING CULTURES, DEFEND FROM CYBER THREATS

Industrial Cyber - Mature OT cybersecurity programs span beyond perimeter defenses, with an emphasis on deep visibility, continuous risk assessment, and strong governance reflecting the unique conditions and needs of OT (operational technology) environments. The roadmap accounts for legacy systems, scattered industrial installations, multilayer network segmentation, secure remote access to the plant, and asset inventories that are up to date, even as critical equipment ages. But most industrial companies are still stuck using legacy risk models designed for the way our systems used to be, rather than the way they are today. The question remains, however, is most, if not all, of the installed base is not hardened for modern threats, including ransomware, nation-state, and supply chain compromise, and leaves critical industrial environments at risk.

CYBERSECURITY COMPLIANCE: THE COSTS, RISKS AND RACE TO CERTIFICATION

Forbes - For companies in the defense industrial base, Cybersecurity Maturity Model Certification will soon be a prerequisite for doing business. And as CMMC compliance rollout deadlines loom, the Department of Defense isn’t mincing words. “CMMC started under Trump 1,” said Katie Arrington, performing the duties of the DoD Chief Information Officer and a key architect of the program. “It will finish and be implemented under Trump 2.” She made these comments in a keynote at the AFCEA International TechNet Cyber convention in May.