DIGI AMERICAS ALLIANCE MEMBERS

REPÚBLICA DOMINICANA CONSTITUIRÁ SU NUEVO CYBER CLUSTER PARA FORTALECER LA CIBERSEGURIDAD NACIONAL

acento - La República Dominicana dará un nuevo paso en el fortalecimiento de su ecosistema de seguridad digital con la constitución oficial del Cyber Cluster República Dominicana, una iniciativa colaborativa que reunirá a empresas líderes, organismos estratégicos y actores clave del sector tecnológico y de ciberseguridad. La ceremonia oficial de firma de estatutos se llevará a cabo en el auditorio del Centro INDOTEL Cultura Digital, en un encuentro exclusivo para 50 invitados especiales del ecosistema empresarial, tecnológico e institucional.

EL SALVADOR IMPULSA LA CIBERSEGURIDAD COMO MOTOR DE DESARROLLO Y COMPETITIVIDAD

Escudo digital - Con el objetivo de ayudar a las empresas a proteger sus datos, evitar ataques de origen informático, digital, electrónico, virtual y computacional, y conocer los riesgos asociados al uso de la inteligencia artificial en fraudes, la Cámara de Comercio e Industria de El Salvador (Camarasal), a través de su Comité de Tecnología, convocó recientemente la denominada CyberWeek (Semana Cibernética) 2026, centrada en la ciberseguridad empresarial.

PANAMÁ, UN HUB LOGÍSTICO QUE ENFRENTA CRECIENTES RIESGOS CIBERNÉTICOS

Revista Summa - Panamá se ha consolidado como uno de los principales centros logísticos y financieros de América Latina. Su canal interoceánico, puertos, aeropuertos, cables submarinos y sistema financiero lo conectan con la economía global, pero esa misma relevancia lo ha convertido en un objetivo cada vez más atractivo para el cibercrimen. Entre 2025 y 2026, los ciberataques aumentaron un 25%, alcanzando un promedio de 2.600 intentos maliciosos semanales por organización y más de 3.300 en el sector financiero. Solo en mayo de 2026 se comprometieron 1,17 terabytes de información, mientras que recientes incidentes en banca y salud colocaron al país entre los más afectados por filtraciones de datos en la dark web.

DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 12, 2026

EXPERTA EN CIBERSEGURIDAD EXPLICA IMPORTANCIA A LA COMISIÓN DE ECONOMÍA QUE ELABORA NUEVO DICTAMEN A LEY - GUATEMALA

LaHora.gt - La comisión legislativa de Economía y Comercio Exterior discute la ley de Ciberseguridad, luego de que el Pleno decidió regresar a la comisión para un nuevo dictamen la iniciativa de ley 6347, ya que varios diputados y sectores se oponían a la propuesta que avanzó en el Hemiciclo. Anteriormente, solo la comisión de Asuntos de Seguridad Nacional había dictaminado esa iniciativa de ley, pero ahora serán las dos que presenten un dictamen por separado para iniciar su aprobación en el Hemiciclo.

BERMUDA WELCOMES GOOGLE SUBSEA CABLE LANDING

Marine Technology News - The Government of Bermuda welcomed the landing of Google's Nuvem and Sol subsea cable systems in Bermuda, describing the milestone as an investment in the island's digital infrastructure, economic resilience, and long-term competitiveness. The Nuvem and Sol cable systems will strengthen international connectivity, enhance network resilience, and support the growing demand for secure, reliable digital infrastructure worldwide.

CLAUDE FABLE 5 MARCA NOVA ERA DE I.A. COM LIMITES PROGRAMADOS DE SEGURANÇA; ENTENDA

Times Brasil - A Anthropic apresentou ao público o **Claude Fable 5**, um novo modelo de inteligência artificial que marca uma mudança importante na forma como a empresa disponibiliza sistemas avançados. A proposta combina maior capacidade de desempenho com um mecanismo de segurança integrado, que limita automaticamente o acesso a conteúdos considerados perigosos. O modelo faz parte da chamada "classe Mythos", uma geração de IA que, até então, tinha seu uso limitado a testes devido ao alto risco de uso indevido. Agora, com o Fable 5, a Anthropic amplia o acesso, mas mantém um controle rígido sobre temas sensíveis. Na prática, o sistema funciona de forma híbrida. O Claude Fable 5 atende normalmente às solicitações dos usuários, mas quando identifica perguntas relacionadas a tópicos como segurança cibernética ofensiva ou pesquisa biológica potencialmente perigosa, ele não responde diretamente.

¿QUÉ GRANDES DESAFÍOS AFRONTA LATINOAMÉRICA Y EL CARIBE PARA FORTALECER SU CIBERSEGURIDAD?

SeguriLATAM - La ciberseguridad continúa siendo una de las asignaturas pendientes para América Latina y el Caribe. Así lo concluye el informe Cybersecurity Report 2025: Vulnerability and Maturity Challenges to Bridging the Gaps in Latin America and the Caribbean, elaborado por la Organización de los Estados Americanos. Un documento que advierte de que la región aún presenta importantes brechas de madurez, capacidades y recursos frente a un entorno digital cada vez más complejo y expuesto a amenazas. Uno de los principales desafíos identificados es la desigualdad en materia de ciberseguridad. El informe señala que los países de la región registran algunos de los niveles más bajos de resiliencia cibernética autoevaluada a nivel mundial, una situación que los hace más vulnerables a ataques capaces de afectar infraestructuras críticas, servicios esenciales, la actividad económica y la confianza ciudadana en los sistemas digitales.

DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 12, 2026

CISA ISSUES BINDING OPERATIONAL DIRECTIVE OUTLINING STEPS FOR AGENCIES TO ADDRESS VULNERABILITY MANAGEMENT - USA

Inside Cybersecurity - The Cybersecurity and Infrastructure Security Agency has issued a binding operational directive ordering civilian agencies to take steps on vulnerability management through a risk-based approach based on four criteria areas, as part of the government's work to implement a June 2 executive order on frontier artificial intelligence models. "In 2021 CISA established the Known Exploited Vulnerabilities catalog pursuant to BOD 22-01, which directed agencies to aggressively remediate known exploited vulnerabilities (KEVs), protect federal assets, and reduce cyber incidents.

WARNER PROPOSES BILL TO FORCE CISA UPDATES TO CRITICAL INFRASTRUCTURE CYBERSECURITY PLANS AMID AI-DRIVEN THREATS - USA

Industrial Cyber - A U.S. Senator introduced a bill that would require the Cybersecurity and Infrastructure Security Agency (CISA) to update cybersecurity plans across all critical infrastructure sectors and assess emerging technology-driven risks. Titled 'Combat Emerging Threats to Critical Infrastructure Act of 2026,' the legislation comes amid growing concerns that advances in AI (artificial intelligence) could accelerate cyberattacks against essential services and critical infrastructure. Warner said the measure is intended to ensure that government, industry, regulators, and cybersecurity experts regularly refresh defensive plans to address increasingly sophisticated threats, including those enabled by AI.

THE CYBER THREAT TO THE 2026 WORLD CUP

CSIS - Major events present a vastly expanded attack surface—but also tend to act as a mirror, reflecting the geopolitical tensions of the moment. The 2026 FIFA World Cup takes the usual complexity of a major event and multiplies it on three fronts: First, it takes place across three international jurisdictions (the United States, Canada, and Mexico), and 16 host cities within them. Second, it significantly scales the digital attack surface across networks, supporting digital infrastructure and the millions of mobile devices present. And third, it takes place against the backdrop of ongoing geopolitical conflicts, including the Russia-Ukraine war and the now reignited U.S.-Israel-Iran conflict—but also coincides with the United States' 250th anniversary celebrations. Alone, each front presents its own type of cyber risk, but together, they present a cumulative set of risks that makes securing this tournament somewhat unique.

CHECK POINT REPORTS RANSOMWARE ATTACKS JUMP 48% YEAR OVER YEAR DESPITE DECLINE IN OVERALL CYBERATTACK ACTIVITY

Industrial Cyber - Global cyberattack activity eased in May 2026 following April's sharp rebound, but the broader threat landscape remained volatile, according to research from Check Point Research. Organizations experienced an average of 2,055 weekly cyberattacks during the month, representing a 2% increase year-over-year despite a 7% decline from April. Education remained the most targeted sector, averaging 4,641 weekly attacks per organization, while government and telecommunications also continued to face elevated attack volumes.