DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 16, 2026

DIGI AMERICAS ALLIANCE MEMBERS

LAS ESTAFAS DIGITALES QUE MÁS CIRCULAN EN EL SALVADOR

ElSalvador.com - Las estafas continúan evolucionando en El Salvador. Plataformas falsas, perfiles clonados, programas imaginarios de inversión y mensajes intimidantes son parte de un ecosistema criminal que opera desde cualquier parte del mundo y que apunta a un objetivo concreto, robar dinero o información personal. De acuerdo con reportes recopilados por la Superintendencia del Sistema Financiero (SSF), estas son las modalidades más comunes que circulan actualmente en el país.

INDOTEL DECIDIDO A ENFRENTAR LOS CIBERDELITOS - REPÚBLICA DOMINICANA

El Nuevo Diario - La República Dominicana padece un flagelo causado por ilícitos cibernéticos, los cuales han sido traumáticos para el desenvolvimiento económico y social. Pero parece que, ¡por fin!, las autoridades han decidido poner freno a esta agravada situación. El Instituto Dominicano de las Telecomunicaciones (INDOTEL) en la necesidad de afrontar un mal que tiene mil formas de atacar a sus víctimas, y que, aunque es global, provoca también daños profundos, tangibles e intangibles, a la economía, a las finanzas, a las buenas prácticas sociales, a la sana convivencia, la certidumbre social y el bienestar del pueblo dominicano.

DEL POTENCIAL AL IMPACTO PRODUCTIVO: EL RETO DE LA IA EN RD

El Dinero - Los países de América Latina se enfrentan a la “trampa del desarrollo”: baja capacidad para crecer, alta desigualdad, baja movilidad social, así como capacidades institucionales y de gobernanza poco efectivas. Sin embargo, la inteligencia artificial (IA) se erige como una oportunidad estratégica para romper ese círculo y lograr las transformaciones indispensables en las economías y sociedades de la región, incorporándola para acelerar un desarrollo productivo, al tiempo de garantizar su uso ético y responsable. República Dominicana se ubica en el noveno lugar del Índice Latinoamericano de Inteligencia Artificial (ILIA) 2025, elaborado por la Comisión Económica para América Latina y el Caribe (Cepal).

DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 16, 2026

TENDENCIAS DEL ECOSISTEMA FINANCIERO DIGITAL EN PERÚ PARA EL 2026

El Comercio - El ecosistema financiero digital en Perú se encuentra en un punto de inflexión y crecimiento cada vez mayor. Según el Banco Central de la Reserva del Perú (BCR), durante el 2025, cada adulto en el país realizó en promedio 625 pagos digitales al año, lo que equivale a aproximadamente 1,7 transacciones electrónicas diarias. Demostrando así la preferencia de los peruanos por este tipo de operaciones. "Diario El Comercio. Todos los derechos reservados." Como resultado, el sector viene consolidándose como uno de los más dinámicos de la región, impulsado también por el crecimiento de la digitalización financiera que redefine la forma en que los peruanos realizan transacciones. "Diario El Comercio. Todos los derechos reservados."

LALIGA Y EL GOBIERNO FIRMAN UN ACUERDO PARA IMPULSAR LA CIBERSEGURIDAD Y LA LUCHA CONTRA EL ODIO ONLINE - ESPAÑA

teleprensa - LaLiga y la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (SETELECO), a través del Instituto Nacional de Ciberseguridad de España (INCIBE) han suscrito este miércoles un Memorando de Entendimiento (MoU) que establece un marco de cooperación institucional para reforzar la ciberseguridad, promover la confianza digital y fomentar un entorno online seguro y respetuoso. El acuerdo responde a la voluntad compartida de las partes de alinear esfuerzos entre el sector público y el deporte profesional para hacer frente a los retos derivados de la digitalización, especialmente en ámbitos como la prevención de ciberriesgos, la protección de la privacidad, la concienciación en ciberseguridad y la lucha contra el discurso de odio en el entorno digital, incluidos fenómenos como el ciberacoso, el racismo, la xenofobia o la discriminación.

CYBERSECURITY BECOMES A NATIONAL PRIORITY: THE WEEK IN CYBER - MEXICO

Mexico Business News - Cybersecurity emerged as a matter of institutional resilience rather than IT hygiene. Public-sector readiness around the 2026 World Cup, DHS's heavy investment in anti-drone systems, and coordinated responses from UNAM and IPN illustrate how cyber risk now intersects with public safety and national events. At the same time, Fortinet's warning about AI-driven, narrative-based attacks reframed threats as campaigns targeting trust and decision-making, not just systems. Cybersecurity strategy is shifting toward continuous, intelligence-led operations aligned with regulatory and geopolitical realities.

PREDICCIONES DPL NEWS 2026 | CENTROAMÉRICA Y EL CARIBE: SIGUE LA TRANSFORMACIÓN DIGITAL, 5G Y SOBERANÍA TECNOLÓGICA

dpls news - En 2025, Centroamérica avanzó en la modernización de su infraestructura digital, impulsada por la consolidación de las redes 4G y por marcos regulatorios más robustos. A nivel regional, el año cerró con progresos en digitalización, ciberseguridad y despliegues de 5G, aunque con ritmos lentos. Mientras Costa Rica, Guatemala y El Salvador ya operan redes comerciales de quinta generación, Honduras y Nicaragua permanecen en fase de planificación. Al mismo tiempo, los esfuerzos por reforzar la ciberseguridad cobraron relevancia ante la modernización de los sistemas públicos y el creciente llamado regional para contar con una ley de Inteligencia Artificial (IA) que establezca principios de uso ético, transparencia y responsabilidad.

DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 16, 2026

U.S. CYBER CAPABILITIES TO DETER AND DISRUPT MALIGN FOREIGN ACTIVITY TARGETING THE HOMELAND

CSIS - Emily Harding testified before the House Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection about how the United States can strengthen its approach to offensive cyber operations as part of a broader national security framework, including the evolving roles of federal agencies and the private sector.

CISA, UK NCSC, FBI UNVEIL PRINCIPLES TO COMBAT CYBER RISKS IN OT - USA AND UNITED KINGDOM

CISA - Today, the Cybersecurity and Infrastructure Security Agency (CISA), United Kingdom's National Cyber Security Centre (NCSC-UK), Federal Bureau of Investigation (FBI) and international partners released Secure Connectivity Principles for Operational Technology. This joint guidance, led by NCSC-UK, helps organizations mitigate exposed and insecure connectivity and protect networks from highly capable and opportunistic cyber threat actors, including nation state-sponsored actors. Operational technology (OT) network environments are increasingly interconnected, delivering benefits like real-time analytics, remote monitoring and predictive maintenance. However, this connectivity also heightens the risk to cyber intrusions that could cause physical harm, environmental damage, or disrupt essential services. This guide offers owners and operators a framework with clear goals for designing secure connectivity into their environments.

GOVERNMENT CYBER ACTION PLAN - UNITED KINGDOM

Gov.uk - The first duty of this government is to keep the country safe; that never changes. In today's volatile world, security extends beyond physical borders into the digital realm. Hostile states and criminal groups are actively probing our defences, seeking to disrupt our way of life and undermine our national interest. We are not starting from scratch; we are scaling what works, learning from successes across the public sector and our international partners. This plan will go further than we have before, prioritising cyber resilience and ensuring we have strong central leadership driving cross-government response. It will enable departments, through central services and targeted support, and will see the launch of a new Government Cyber Profession which will not only ensure we continue to attract and retain the best talent but also support development skills throughout the UK. This is more than just a change; it is a steadfast commitment to defending the state and protecting the daily lives of working people. By fixing these foundations, we will build a government that is resilient, secure, and ready for national renewal.

GLOBAL CYBERSECURITY OUTLOOK 2026

World Economic Forum - The World Economic Forum's Global Cybersecurity Outlook 2026, written in collaboration with Accenture, examines the cybersecurity trends that will affect economies and societies in the year to come. The report explores how accelerating AI adoption, geopolitical fragmentation and widening cyber inequity are reshaping the global risk landscape. As attacks grow faster, more complex and more unevenly distributed, organizations and governments face rising pressure to adapt amid persistent sovereignty challenges and widening capability gaps. Drawing on leaders' perspectives, the report provides actionable insights to inform strategy, investment and policy.