DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 16, 2026

DIGI AMERICAS ALLIANCE MEMBERS

THE MOST COMMON DIGITAL SCAMS IN EL SALVADOR

ElSalvador.com - Scams continue to evolve in El Salvador. Fake platforms, cloned profiles, fictitious investment programs, and intimidating messages are part of a criminal ecosystem that operates from anywhere in the world and aims for one specific goal: stealing money or personal information. According to reports compiled by the Superintendency of the Financial System (SSF), these are the most common scams currently circulating in the country.

INDOTEL DETERMINED TO CONFRONT CYBERCRIME - DOMINICAN REPUBLIC

The Dominican Republic is suffering from a scourge caused by cybercrimes, which have been traumatic for its economic and social development. But it seems that, finally, the authorities have decided to put a stop to this aggravated situation. The Dominican Telecommunications Institute (INDOTEL) recognizes the need to confront a problem that has a thousand ways of attacking its victims, and which, although global, also causes profound, tangible and intangible damage to the economy, finances, good social practices, healthy coexistence, social certainty, and the well-being of the Dominican people.

FROM POTENTIAL TO PRODUCTIVE IMPACT: THE CHALLENGE OF AI IN THE DOMINICAN REPUBLIC

Money - Latin American countries face the “development trap”: low growth capacity, high inequality, low social mobility, and ineffective institutional and governance capacities. However, artificial intelligence (AI) presents a strategic opportunity to break this cycle and achieve the essential transformations in the region's economies and societies, incorporating it to accelerate productive development while ensuring its ethical and responsible use. The Dominican Republic ranks ninth in the 2025 Latin American Artificial Intelligence Index (ILIA), prepared by the Economic Commission for Latin America and the Caribbean (ECLAC).

DIGI AMERICAS LATAM CISO

INSIGHTS

JANUARY 16, 2026

TRENDS IN THE DIGITAL FINANCIAL ECOSYSTEM IN PERU FOR 2026

El Comercio - The digital financial ecosystem in Peru is at a turning point and experiencing rapid growth. According to the Central Reserve Bank of Peru (BCR), by 2025, each adult in the country was projected to make an average of 625 digital payments per year, equivalent to approximately 1.7 electronic transactions per day. This demonstrates Peruvians' preference for this type of transaction. "El Comercio Newspaper. All rights reserved." As a result, the sector is consolidating itself as one of the most dynamic in the region, driven also by the growth of financial digitization, which is redefining how Peruvians conduct transactions. "El Comercio Newspaper. All rights reserved."

LALIGA AND THE GOVERNMENT SIGN AN AGREEMENT TO BOOST CYBERSECURITY AND THE FIGHT AGAINST ONLINE HATE - SPAIN

Teleprensa - LaLiga and the State Secretariat for Telecommunications and Digital Infrastructure (SETELECO), through the Spanish National Cybersecurity Institute (INCIBE), signed a Memorandum of Understanding (MoU) this Wednesday establishing a framework for institutional cooperation to strengthen cybersecurity, promote digital trust, and foster a safe and respectful online environment. The agreement reflects the shared commitment of both parties to align efforts between the public sector and professional sports to address the challenges arising from digitalization, particularly in areas such as cyber risk prevention, privacy protection, cybersecurity awareness, and combating hate speech in the digital environment, including phenomena such as cyberbullying, racism, xenophobia, and discrimination.

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.

DPL NEWS 2026 PREDICTIONS | CENTRAL AMERICA AND THE CARIBBEAN: DIGITAL TRANSFORMATION, 5G AND TECHNOLOGICAL SOVEREIGNTY CONTINUE

dpls news - In 2025, Central America made progress in modernizing its digital infrastructure, driven by the consolidation of 4G networks and more robust regulatory frameworks. Regionally, the year ended with progress in digitization, cybersecurity, and 5G deployments, albeit at a slow pace. While Costa Rica, Guatemala, and El Salvador already operate commercial fifth-generation networks, Honduras and Nicaragua remain in the planning phase. At the same time, efforts to strengthen cybersecurity gained importance given the modernization of public systems and the growing regional call for an Artificial Intelligence (AI) law that establishes principles of ethical use, transparency, and accountability.

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.