

DIGI
AMERICAS

LATAM

CISO

INSIGHTS

OCTOBER 23, 2025

DIGI AMERICAS ALLIANCE MEMBERS

Apple

aws

Batuta

CHECK POINT

CISCO

CLOUDFLARE

CROWDSTRIKE

fluid
attacks
we hack your software

Google

kriptos

LUMU

MasterCard

netskope

paloalto
NETWORKS

Resecurity

Schneider
Electric

SISAP
Sistemas Aplicativos

Strike

Telefónica

tenable

Trellix

TREND
MICRO

GUATEMALA AVANZA EN LA CONSTRUCCIÓN DE SU ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

Agencia Guatemalteca de Noticias - En un contexto global donde la tecnología avanza a gran velocidad, la seguridad digital se ha convertido en un componente estratégico tan relevante como las fronteras físicas. Conscientes de esta realidad, representantes del Gobierno de Guatemala y delegados de la Unión Internacional de Telecomunicaciones (UIT) se reunieron en la Superintendencia de Telecomunicaciones (SIT) para presentar los resultados de la Evaluación Nacional CIRT de Guatemala, Versión 1.0, un hito en la consolidación de una estrategia nacional de ciberseguridad.

LA ANCI Y EL TRIBUNAL CONSTITUCIONAL DE CHILE SUSCRIBEN UN CONVENIO DE COLABORACIÓN PARA FORTALECER LA CIBERSEGURIDAD INSTITUCIONAL

Segurilatam - La Agencia Nacional de Ciberseguridad (ANCI) y el Tribunal Constitucional de Chile firmaron, el 20 de octubre, un convenio de colaboración en materia de ciberseguridad. El objetivo es fortalecer la seguridad informática y establecer mecanismos conjuntos para la prevención, gestión y respuesta oportuna ante incidentes de ciberseguridad en Chile. El acuerdo contempla que el Tribunal Constitucional reportará los incidentes de ciberseguridad a través de la plataforma habilitada por la ANCI y desarrollará actividades conjuntas de colaboración, orientadas al fortalecimiento de sus capacidades técnicas y a la mejora continua de sus protocolos de seguridad digital.

CIBERDEFENSA EN TIEMPO REAL: CHILE PONE A PRUEBA SU ESCUDO DIGITAL ANTE AMENAZAS DEL FUTURO

ZM - En una época donde los conflictos ya no solo se libran en el terreno físico, sino en las profundidades invisibles de redes y sistemas informáticos, Chile adelanta el calendario al año 2035. Esta semana, el Ministerio de Defensa Nacional puso en marcha la segunda versión del ejercicio conjunto "Escudo Cibernético", una simulación de ciberataques a gran escala que —más allá de los titulares— revela una preocupación creciente: la necesidad de estar preparados para una guerra sin fronteras físicas, pero con impactos reales.



DIGI
AMERICAS

LATAM

CISO

INSIGHTS

OCTOBER 23, 2025

ACCIONES PARA FORTALECER LA CIBERSEGURIDAD EN ELECCIONES - COLOMBIA

Corrillos - A través del Equipo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT), el Ministerio TIC asumió la Secretaría Técnica del PMU Ciber Electoral, con el propósito de coordinar esfuerzos interinstitucionales que fortalezcan la seguridad digital y la transparencia de los próximos comicios. Fortalecer la ciberseguridad nacional y proteger la integridad de los procesos democráticos hacen parte de los propósitos con los que el Ministerio de Tecnologías de la Información y las Comunicaciones asume la Secretaría Técnica del Puesto de Mando Unificado (PMU) Ciber Electoral, de cara a los procesos electorales 2025-2026, que inician este domingo 189 de octubre.

APRUEBAN INTEGRACIÓN DE COMISIÓN DE CIBERSEGURIDAD - MÉXICO

Senado - El Pleno del Senado de la República aprobó un acuerdo de la Junta de Coordinación Política (Jucopo) por el que se integra la Comisión Ordinaria de Ciberseguridad, que presidirá el senador Alejandro Moreno Cárdenas, del Grupo Parlamentario del PRI. La secretaría de dicho órgano legislativo se conformará por las senadoras Jesús Lucía Trasviña Waldenrath y Alejandra Berenice Arias Trevilla, de Morena. En tanto, sus integrantes son Cecilia Guadalupe Guadiana Mandujano y Saúl Monreal Ávila, de Morena; Ivideliza Reyes Hernández, del PAN; y Ruth Miriam González Silva, del PVEM.

CYBER RESILIENCE BECOMES KEY AS AI THREATS OUTPACE SECURITY - MÉXICO

Mexico Business News - The volume and complexity of cyberthreats, driven by emerging technologies like AI and automation, are outpacing the capabilities of traditional security models. This reality forces a necessary strategic shift for organizations: moving from a prevention-focused approach to one of operational cyber resilience. This landscape is turning cyber resilience from a technical IT function into a pillar of corporate strategy and risk management.

COSTA RICA HOPS ON LATAM-EUROPE CABLE, DATA EXCHANGE ECOSYSTEM

bnamericas - Costa Rica became the latest country to join the Ellalink Europe-LatAm submarine cable and its BELLA II data exchange initiative. The country's participation in the program was formalized with a memorandum of understanding (MoU) signed between the science, innovation, technology and telecommunications ministry (MICITT) and the Latin American Advanced Networks Cooperation, RedCLARA, which is in charge of overseeing the collaboration.



DIGI
AMERICAS

LATAM

CISO

INSIGHTS

OCTOBER 23, 2025

NCSC WARNS DATA CENTRES FACE RISING CYBERSECURITY THREATS - UNITED KINGDOM

Data centre magazine - The UK is facing a sharp increase in cyber attacks, with the National Cyber Security Centre (NCSC) warning that cybersecurity has become a matter of national resilience. Its Annual Review 2025 reveals that the organisation handled 204 nationally significant cyber incidents over the past year, more than double the 89 managed the previous year. In total, the NCSC responded to 429 incidents, including 18 categorised as “highly significant” due to their potential to disrupt essential national services such as energy networks, healthcare systems and government operations. The findings reinforce the urgency for organisations to design digital infrastructure – particularly data centres and cloud environments – with resilience built in from the start.

GOOGLE QUANTUM AI SHOWS 13,000× SPEEDUP OVER WORLD’S FASTEST SUPERCOMPUTER IN PHYSICS SIMULATION

The Quantum Insider - Google Quantum AI has reported a physics experiment that pushes quantum computing further into what researchers call the “beyond-classical” regime, where even the world’s most powerful supercomputers fail to keep up. In a paper published in Nature, the team describes using its 65-qubit superconducting processor to measure a subtle quantum interference phenomenon called the second-order out-of-time-order correlator, or OTOC(2).

HOW TO SECURE THE DIGITAL FUTURE: RESILIENCE, TRUST AND LEADERSHIP

WEF - Global challenges have become inseparable, making collaboration across disciplines more important than ever. Experts from the Global Future Councils met with global cybersecurity leaders in Dubai to discuss interconnected challenges. Here are their reflections on digital resilience, trust and leadership in an increasingly intertwined world. Amid profound geopolitical and geo-economic realignments, and as rapid advances in technology reshape the global security landscape, economic resilience, societal trust, sustainability and cybersecurity are now part of the same equation.

NOT JUST SPIES AND SABOTEURS: SATELLITE OPERATORS SAY CYBERCRIME IS A CONSTANT THREAT

Air and Space Forces Magazine - When the Space Force discusses the cyber threats faced by the service or the commercial satellite providers it uses, it typically frames the issue as a nation-state one: attacks from an adversary designed to cut off communication links and other space-based systems that U.S. forces on the ground rely upon, as the Russians did to Ukrainian Viasat terminals just before their full-scale invasion in 2022. But for cyber defenders in the commercial space sector responsible for day-to-day operations, the reality is rather different: Like other providers of vital services—hospitals, universities, and local governments—satellite companies face a daily onslaught of mostly low-level cyberattacks designed to install ransomware or facilitate other financially motivated crimes.