DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 10, 2026

DIGI AMERICAS ALLIANCE MEMBERS

PERÚ REALIZARÁ CUARTO SIMULACRO NACIONAL DE CIBERATAQUES PARA FORTALECER LA SEGURIDAD DIGITAL DEL PAÍS

gob.pe - Con el fin de fortalecer las capacidades de preparación y respuesta frente a incidentes de seguridad digital, la Presidencia del Consejo de Ministros (PCM), a través de la Secretaría de Gobierno y Transformación Digital, realizará el próximo jueves 16 de julio el Simulacro de Ataques Cibernéticos 2026 – SIMAC 2026, un ejercicio nacional que reunirá a entidades públicas y privadas para evaluar sus procedimientos de detección, análisis, contención, recuperación y coordinación ante escenarios realistas de ciberataques.

PAGOS DIGITALES Y CIBERSEGURIDAD: EL DESAFÍO QUE CHILE NO PUEDE POSTERGAR

Forbes Chile - En Chile, el avance de los pagos digitales ha sido sostenido y significativo. En la última década, su uso se ha cuadruplicado, alcanzando más de 370 transacciones por persona al año, según cifras del Banco Central de Chile. A esto se suma que el volumen transado ya supera el 100% del PIB, de acuerdo con el Informe de Sistemas de Pago de la misma institución, lo que refleja un nivel de adopción que posiciona al país entre los más avanzados de la región.

EXPERTO EN CIBERSEGURIDAD POR NUEVA LEY DE PROTECCIÓN DE DATOS PERSONALES: «SE ACABÓ EL SÍNDROME DE DIÓGENES DE LAS EMPRESAS CON NUESTROS DATOS» - CHILE

Futuro.cl - El próximo 1 de diciembre de 2026 marcará un antes y un después en la privacidad de los chilenos con la entrada en vigor de la nueva Ley de Protección de Datos Personales. Esta normativa no solo crea una Agencia especializada, sino que transforma la naturaleza de nuestra información: los datos pasan a ser considerados propiedad de los ciudadanos, exigiendo un consentimiento explícito para cualquier tratamiento.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 10, 2026

SENADO CRIA FRENTE PARLAMENTAR DE INTELIGÊNCIA ARTIFICIAL - BRASIL

Poder360 - O Senado Federal criou a Frente Parlamentar Mista de Inteligência Artificial, Proteção de Dados e Segurança Digital. A Resolução nº 19, de 2026, foi promulgada pelo presidente do Senado, Davi Alcolumbre (União Brasil-AP), e divulgada no DOU (Diário Oficial da União) nesta 6ª feira (10.jul.2026). Leia a íntegra (PDF – 287 KB). O novo órgão tem caráter suprapartidário, natureza não governamental e duração indeterminada. A frente reúne senadores e deputados federais que assinarem a ata de instalação, com possibilidade de adesão posterior por outros congressistas.

GUARDIÃO CIBERNÉTICO 2026 REUNIRÁ MAIS DE 240 ORGANIZAÇÕES EM SIMULAÇÃO NACIONAL DE ATAQUES DIGITAIS - BRASIL

Contabeis - O Exercício Guardião Cibernético 2026 (EGC 2026) será realizado entre 21 e 25 de setembro, reunindo mais de 240 organizações em uma simulação nacional de defesa contra ataques cibernéticos. Considerado o maior exercício de defesa cibernética do Hemisfério Sul, o evento contará com a participação das Forças Armadas, órgãos governamentais, agências reguladoras, instituições de ensino e empresas responsáveis por infraestruturas críticas do país.

O BRASIL, OS DATA CENTER E AS OPORTUNIDADES DE CRESCIMENTO

Be News - A corrida global por capacidade de processamento de dados, acelerada pelo crescimento exponencial da inteligência artificial, acaba impulsionando grandes investimentos em infraestrutura. São medidas necessárias para a operação de data centers de escala industrial, que consomem de 100 a centenas de megawatts e demandam energia confiável, conectividade de alta velocidade e segurança física e cibernética. São unidades que estão sendo instaladas com urgência em países que reúnem as condições certas. O estudo da Fundação Getúlio Vargas (FGV) apresentado esta semana demonstra que um único empreendimento desses de 100 MW pode adicionar R$ 1,5 bilhão ao PIB brasileiro e gerar 12.560 empregos diretos e indiretos. O Brasil tem vantagens estruturais reais para atrair esses investimentos. O que ainda falta — e o que o estudo identifica com honestidade — é a decisão política de transformar essas vantagens em política pública integrada.

LOS 5 SECTORES MÁS VULNERABLES ANTE CIBERATAQUES EN GUATEMALA (UNO ES EL GOBIERNO)

Prensa Libre - Los recientes ataques cibernéticos contra instituciones públicas en Guatemala volvieron a evidenciar la vulnerabilidad de la infraestructura tecnológica del país. En los últimos meses, la Dirección General de Control de Armas y Municiones (Digecam) fue blanco de un incidente en el que se sustrajo información de propietarios de armas de fuego. Posteriormente, también se reportó la vulneración del portal Tu Empleo, del Ministerio de Trabajo (Mintrab), además de otros incidentes dirigidos contra entidades estatales.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 10, 2026

PRESENTAN UN PROYECTO DE LEY PARA FORTALECER LA CIBERSEGURIDAD Y PROTEGER LOS DATOS DE LOS MENDOCINOS - ARGENTINA

Diario San Rafael - El Gobierno de Mendoza presentó en el Senado provincial un proyecto de ley de ciberseguridad destinado a fortalecer la protección de la infraestructura tecnológica del Estado y de los datos personales de los mendocinos. La iniciativa apunta a establecer un marco legal que permita prevenir y responder ante ataques informáticos, asegurando además la continuidad de servicios esenciales como seguridad, salud, educación, transporte y energía.

CÓMO LA CONECTIVIDAD Y LA INTELIGENCIA ARTIFICIAL ESTÁN TRANSFORMANDO A LAS EMPRESAS EN AMÉRICA LATINA

IT Sitio - La transformación digital atraviesa una nueva etapa en América Latina. Si durante los últimos años el foco estuvo puesto en la adopción de infraestructura tecnológica y la migración hacia entornos digitales, hoy las organizaciones buscan un objetivo mucho más ambicioso: integrar tecnologías capaces de generar eficiencia, mejorar la productividad y aportar un retorno de inversión medible. En este escenario, la conectividad, la inteligencia artificial (IA), la ciberseguridad y la infraestructura crítica dejaron de ser iniciativas independientes para convertirse en piezas de una estrategia integral. Empresas de sectores como telecomunicaciones, salud, educación, industria, retail y gobierno están redefiniendo sus planes de inversión con el objetivo de construir ecosistemas tecnológicos preparados para responder a las exigencias actuales y futuras del negocio.

LA PRÓXIMA CRISIS DE CIBERSEGURIDAD NO SERÁ UN ATAQUE. SERÁ UNA DECISIÓN QUE NO TOMAMOS A TIEMPO

Entrepreneur - Existe una constante en la historia de la innovación: las organizaciones rara vez fracasan porque una tecnología las tome por sorpresa. Lo hacen, casi siempre, porque interpretaron las primeras señales de cambio como asuntos demasiado lejanos para alterar las decisiones que tomaban en el presente. Ocurrió con internet cuando todavía parecía un experimento académico, volvió a suceder con la computación en la nube y más recientemente con la inteligencia artificial (IA). Hoy, todo indica que estamos frente a un momento similar con la computación cuántica. No porque las empresas desconozcan que viene en camino, sino porque muchas siguen convencidas de que todavía tienen tiempo para prepararse.

RECORDED FUTURE LLEGA A COLOMBIA ANTE REPUNTE HISTÓRICO DE CIBERATAQUES

Impactotic - na nueva empresa especializada en ciberseguridad y prevención del fraude anunció su llegada a Colombia con la garantía de fortalecer la defensa de entidades públicas y privadas frente a un entorno digital cada vez más hostil. La firma de inteligencia de amenazas, con sede en Boston y presencia en más de 80 países, en sectores puntuales como gobierno, banca e infraestructura crítica, llega en medio de un repunte histórico de delitos informáticos.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 10, 2026

GOOGLE AND THE FBI TARGET MASSIVE BOTNET THAT QUIETLY USED HOME DEVICES TO MASK CYBERCRIME

CNET - The FBI, in partnership with Google and other tech companies, struck a massive blow against NetNut, a public-facing residential network proxy service that secretly hosted a botnet controlling approximately 2 million Android TVs and similar smart home devices. The network was being used for password-spraying, credential attacks and other malicious activity. Residential proxy botnets make malicious traffic appear like normal internet use, allowing everyday devices to be secretly hijacked by cybercriminals to conduct illegal activities using your home internet. Infected home devices were often preloaded with malicious software used by the botnet, which made traditional home security practices less effective at detecting and stopping the problem.

WHY THE WORLD NEEDS A CITIZENS' CYBERATTACK FRAMEWORK

WEF - When a major brand or piece of critical national infrastructure suffers a cyberattack, it makes national headlines. Governments convene, regulators act and the cybersecurity industry mobilizes. When a single parent is defrauded out of their savings, or a teenager's intimate images are shared without consent, the response is fractured, slow, and too often, non-existent. To many, it makes sense to prioritize these large attacks, but there is a bigger picture. Attacks against individuals are happening on a vast scale, and the cumulative impact, especially over the long term, is likely to be catastrophic for society. How are we going to run our economies and public services digitally when there is a loss of trust in interacting online?