DIGI AMERICAS ALLIANCE MEMBERS

EL MAP REÚNE A LOS DIRECTORES DE TECNOLOGÍA Y CIBERSEGURIDAD DEL ESTADO - REPÚBLICA DOMINICANA

DiaroDigitalRD - El Ministerio de Administración Pública (MAP), a través del Viceministerio de Innovación y Tecnología, reunió a directores y encargados de tecnología y ciberseguridad del sector público para definir la estrategia de transformación digital y fortalecer la eficiencia gubernamental mediante el uso de tecnologías innovadoras. El ministro del MAP, Sigmund Freund, destacó que la digitalización del Estado es fundamental para ofrecer servicios más ágiles, accesibles y transparentes.

PRESIDENTE DEL INDOTEL SE REÚNE CON SUBSECRETARIA ADJUNTA DE EE. UU. PARA AFIANZAR LAZOS COOPERACIÓN EN CIBERSEGURIDAD - REPÚBLICA DOMINICANA

El presidente del Consejo Directivo del Instituto Dominicano de las Telecomunicaciones (Indotel), Guido Gómez Mazara, se reunió con la subsecretaría principal adjunta del Departamento de Estado de los Estados Unidos para la Oficina de Ciberespacio y Política Digital, Jennifer Bachus, con quien intercambió estrategias para fortalecer la ciberseguridad en la República Dominicana, a fin de tener un futuro digital más robusto y seguro.

MITIC INFORMA SOBRE AVANCES EN ESTRATEGIAS SOBRE CIBERSEGURIDAD Y AGENDA DIGITAL - PARAGUAY

La Nacion - El Ministerio de Tecnologías de la Información y Comunicación (Mitic) publicó su “Memoria anual” con respecto al 2024 en la cual exponen todas las acciones promovidas por esta institución durante el año pasado. Entre estas se destacan hechos como la identidad digital, asistencias técnicas, entre otras. Uno de los pilares fundamentales, según afirmó la propia institución, fue la ciberseguridad y en este sentido, se gestionaron más de 1.800 incidentes y además, se formuló la Estrategia Nacional de Ciberseguridad que se extiende hasta el 2028 y que fue desarrollada en colaboración con la Organización de los Estados Americanos (OEA).

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 13, 2025

TRT-RS INTENSIFICA DEFESA CIBERNÉTICA FRENTE A AVANÇO DE ATAQUES HACKERS - BRASIL

Justica Do Trabalho - Nos últimos anos, o Brasil tem figurado entre os principais alvos de ataques cibernéticos no mundo, segundo dados de relatórios especializados. Essa realidade tem levado instituições públicas e privadas a reforçarem suas estruturas de segurança digital. No Tribunal Regional do Trabalho da 4ª Região (TRT-RS), essa preocupação é constante, como relata o diretor da Secretaria de Tecnologia da Informação e Comunicações (SETIC), André Farias: “Centenas de milhares de tentativas de ações maliciosas são registradas todos os dias, 24 horas por dia, todas devidamente bloqueadas pelos sistemas de segurança da informação”.

REGULAMENTAÇÕES E TENDÊNCIAS DE CIBERSEGURANÇA EM 2025: O QUE ESPERAR - BRASIL

Inforchannel - A cibersegurança segue como uma das maiores preocupações globais para 2025, especialmente diante do aumento exponencial de ataques e violações de Dados. O cenário é impulsionado por avanços na Inteligência Artificial (IA), e pela crescente sofisticação dos cibercriminosos. Por um lado, a IA desempenha um papel ainda mais crucial na proteção das infraestruturas digitais das empresas, e por outro, essa tecnologia tem sido muito aproveitada por hackers, exigindo uma preparação forte por parte das empresas.

“DESENVOLVER TECNOLOGIA SEM RESPEITO À PRIVACIDADE NÃO DEVERIA SER OPÇÃO”, AFIRMA DRA. PATRÍCIA PECK

ITForum - Em entrevista ao IT Forum, a Dra. Patrícia Peck, especialista em direito digital e CEO do escritório Peck Advogados explica: “Estamos num processo de formação de uma cultura empresarial que incorpora o conceito de privacy by design, ou seja, a privacidade deve ser integrada desde a concepção de produtos e soluções tecnológicas”.

ALCALDÍA DE CALI REFUERZA SU CIBERSEGURIDAD ANTE EL AUMENTO DE CIBERATAQUES EN COLOMBIA

Alcaldía de Cali - Para garantizar la protección de la información y prevenir ciberataques, la Alcaldía de Cali, a través de Datic, ha implementado un servidor SOC-SIEM. Este sistema monitorea y protege la infraestructura tecnológica distrital, asegurando la integridad de los datos de los ciudadanos. El servidor opera las 24 horas del día, los siete días de la semana, analizando continuamente la seguridad digital y generando alertas para los administradores tecnológicos. Esto permite una respuesta inmediata ante posibles amenazas y refuerza la protección de los sistemas del Distrito.

MÉXICO PODRÁ COMBATIR EL CIBERCRIMEN MEDIANTE COLABORACIÓN PÚBLICO-PRIVADA

dplnews - El cibercrimen representa una amenaza creciente a nivel mundial, y su impacto económico podría alcanzar los 10.5 trillones de dólares anuales, lo que pone en evidencia la urgente necesidad de una respuesta coordinada entre el gobierno y la iniciativa privada, dijo Gonzalo Gacía-Belenguer, director del Hub de Ciberseguridad del Tec de Monterrey. El experto refirió que los ataques cibernéticos no sólo afectan la economía, sino que también pueden interrumpir las operaciones de empresas, crear crisis de reputación y vulnerar la seguridad de los ciudadanos.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 13, 2025

INTERNET SEGURO: CIBERSEGURIDAD EMPRESARIAL, RETOS Y ESTRATEGIAS EN LA ERA DE LA IA

ImpactoTIC - La ciberseguridad empresarial es un desafío creciente ante el aumento de ciberataques. A pesar de mayores inversiones en protección, solo el 32 % de las empresas confían plenamente en su capacidad de recuperación. Los ciberataques continúan siendo la principal causa de interrupciones en los servicios empresariales, lo que ha impulsado a las compañías a fortalecer sus estrategias de seguridad digital.

PRIORIDADES DE LAS JUNTAS DIRECTIVAS DE AMÉRICA EN 2025

EY - La incertidumbre persiste a medida que las fuerzas dinámicas dan forma al contexto empresarial. Las juntas directivas adaptarán su supervisión para ayudar a la dirección a actuar con intención y confianza. Para respaldar la transformación, las juntas directivas guiarán las revisiones del portafolio, conectarán la supervisión de la seguridad tecnológica y la innovación, y fomentarán la competitividad del talento. Las juntas directivas priorizarán la planificación de escenarios en función de los resultados geopolíticos, económicos, laborales y climáticos para crear resiliencia y permitir la agilidad.

GOOGLE: CYBER CRIME MESHES WITH CYBER WARFARE AS STATES ENLIST GANGS

ComputerWeekly.com - A report from the Google Threat Intelligence Group depicts China, Russia, Iran and North Korea as a bloc using cyber criminal gangs to attack the national security of western countries. The Google Threat Intelligence Group’s report, Cyber crime: A multifaceted national security threat, says western policymakers should be taking cyber criminality just as seriously as operations conducted by nation states. The report looks at how nation states hostile to the North Atlantic countries, such as Russia, China, Iran and North Korea, are increasingly co-opting cyber criminal groups to forward their geopolitical and economic ambitions. It also looks at the deep societal impact of cyber crime, from economic destabilisation to its toll on critical infrastructure, including healthcare.

HOW THE G7’S NEW AI REPORTING FRAMEWORK COULD SHAPE THE FUTURE OF AI GOVERNANCE

OECD.AI - On 7 February 2025, the OECD launched the reporting framework for monitoring the application of the Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems. This milestone marks a significant advancement in international AI governance, reinforcing the G7’s commitment to ensuring the safe, secure, and trustworthy development, deployment, and use of advanced AI systems.

DIGI AMERICAS LATAM CISO

INSIGHTS

FEBRUARY 13, 2025

THE DIGITAL SHIELD: USING CYBER DIPLOMACY TO STRENGTHEN NATIONAL CYBER RESILIENCE

Georgetown Security Studies - In the modern security environment, unconventional, asymmetric security challenges become increasingly dangerous since adversaries seek cheap and easy ways to confront stronger opponents by exploiting vulnerabilities without engaging in direct, conventional warfare. The cyberspace has emerged as a critical domain which national security systems have to engage with. As cyber-attacks grow more sophisticated, governments recognize that addressing cyber-related issues to strengthen national cyber resilience requires a comprehensive, whole-of-government approach. In this process, cyber diplomacy is a vital aspect of cybersecurity. Cyber diplomacy involves facilitating the development of international cooperation frameworks, norms of behavior, information sharing, and trust-building among nations.

QUANTUM SECURITY MARKET SURGE FUELED BY ESCALATING CYBERSECURITY THREATS DRIVER: A MAJOR CATALYST IN THE EVOLUTION OF THE QUANTUM SECURITY MARKET IN 2025

openPR - How Is the Quantum Security Market Projected to Grow, and What Is Its Market Size?
The scale of the quantum security market has expanded massively in past years. It is set to escalate from a worth of $1.14 billion in 2024 to $1.7 billion in 2025, reflecting a compound annual growth rate (CAGR) of 49.0%. The historic period's expansion has been propelled by the need for advanced simulation and modeling, compounded complexity in automotive systems, heightened emphasis on cybersecurity, collective research efforts, and regulatory pressures.