DIGI AMERICAS ALLIANCE MEMBERS

REMARKS: NATIONAL CYBER DIRECTOR COKER AT LATAM CISO

The White House - It is a privilege and a pleasure to be speaking in front of such a distinguished group of cyber leaders and trusted partners from Latin America and the Caribbean. Your work is essential to protecting the shared values that our citizens cherish. Because we are living in a time of unprecedented opportunity. A time where the choices we make will shape the digital ecosystem for decades to come. President Biden has called this “a decisive decade.” And, to no surprise, I agree with him. We have a rare chance to collectively architect the systems that we want. Systems ensuring our mutual economic opportunity and regional security.

RODRIGO CHAVES HACE LLAMADO PARA UNA AMÉRICA LATINA MÁS CIBERSEGURA - LATAM CISO SUMMIT

DPL - Rodrigo Chaves, presidente de Costa Rica, hizo un llamado a los países latinoamericanos para construir en conjunto una región con mayor seguridad cibernética a través de la colaboración entre países. Durante el Latam CISO Summit 2024, Rodrigo Chaves celebró la realización de eventos sobre ciberseguridad, pues aseguró que es necesario debatir y compartir experiencias para enfrentar los nuevos retos de la ciberseguridad. “Compartir sus experiencias, debatir sobre las últimas tendencias y retos, y proponer soluciones estratégicas que fortalezcan nuestra seguridad en el espacio cibernético en América Latina”, comentó el presidente de Costa Rica en un mensaje de apertura.

FALTA INTERÉS POLÍTICO Y CONOCIMIENTO EN CIBERSEGURIDAD A LEGISLATIVO DE MÉXICO: ALEJANDRA LAGUNES - LATAM CISO SUMMIT

DPL - El Poder Legislativo de México carece de interés y conocimiento para poder aprobar una ley de ciberseguridad, aseveró Alejandra Lagunes, senadora en la pasada legislatura. Durante el Latam CISO Summit 2024, Lagunes acusó que el grueso de los legisladores no tienen el conocimiento para reconocer la importancia en la vida económica, política y social que tiene la ciberseguridad. “No hay interés político y hay poco conocimiento dentro del Poder Legislativo sobre la ciberseguridad”, aseveró Alejandra Lagunes.

COSTA RICA QUIERE SER LA ESTONIA DE AMÉRICA LATINA EN CIBERSEGURIDAD: PAULA BOGANTES

DPL - “El ciberataque de 2022 nos puso de rodillas”, relató Paula Bogantes, ministra de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica. Esa es la razón por la cual los gobiernos deben comprender la importancia de la ciberseguridad, al tiempo que “Costa Rica quiere ser la Estonia de América Latina en ciberseguridad”. En 2022, el país centroamericano sufrió un devastador ciberataque perpetrado por el grupo de ransomware Conti, vinculado a Rusia. El ataque afectó múltiples instituciones gubernamentales, paralizando servicios clave como la recaudación de impuestos y las aduanas, causando una crisis de seguridad informática a nivel nacional.

LOS CIBERDELINCUENTES ATACAN EN LA NUBE Y UTILIZAN INTELIGENCIA ARTIFICIAL: CROWDSTRIKE - LATAM CISO SUMMIT

DPL - Los ciberdelincuentes se están desplazando hacia la Nube y están utilizando la Inteligencia Artificial para atacar los sistemas críticos de los países, advirtió Shawn Henry, Chief Security Officer de CrowdStrike. Durante la Cumbre CISO Latam, el directivo de la empresa de ciberseguridad señaló que las cadenas de abastecimientos, las tecnologías emergentes, los incidentes como las fallas eléctricas, las actualizaciones defectuosas de software (refiriéndose a la que tuvo Crowdstrike semanas atrás) y los desastres naturales como terremotos, requieren que las organizaciones y las empresas sean más resilientes.

LA INTELIGENCIA DE RIESGOS PREDICE CIBERAMENAZAS Y PROTEGE EL NEGOCIO - LATAM CISO SUMMIT

DPL - La ciberinteligencia y la medición del ciberriesgo permiten tomar mejores decisiones para prevenir vulnerabilidades, ciberataques y no afectar los negocios, coincidieron especialistas en gestión de riesgos de ciberseguridad participantes en el Latam CISO Summit 2024. Douglas Rocha, CISO (Chief Information Security Officer) de Banco BS2, explicó que es estratégico “traducir los riesgos de ciberseguridad a la Junta de Administración” de las empresas. La clave de la inteligencia de datos “consiste en explicar cómo la ciberseguridad afecta los negocios”.

ESTADOS UNIDOS INVIERTE 300 MILLONES DE DÓLARES PARA 5G EN COSTA RICA - LATAM CISO SUMMIT

DPL - El Banco de Exportación e Importación de Estados Unidos está financiando con 300 millones de dólares para apoyar las iniciativas 5G de Costa Rica, reveló Harry Coker Jr., director Nacional de Ciberseguridad de la Casa Blanca. Costa Rica se encuentra en proceso de licitar frecuencias para 5G. El gobierno del presidente Rodrigo Chaves publicó un decreto en materia de seguridad para los futuros despliegues de 5G, pero restringe a proveedores de origen chino.

¿NUBES TRANSPARENTES? UNA NECESIDAD PARA MEJORAR LA CIBERSEGURIDAD - LATAM CISO SUMMIT

DPL - Cuando existen brechas de seguridad y ciberataques, es necesario que las empresas, gobiernos y proveedores de Nube colaboren de forma transparente para poder protegerse, coincidieron especialistas en el tema durante el Latam Ciso Summit 2024. Jason Merrick, senior vicepresidente de Producto en Tenable, aseveró que todos deben ser capaces de ser transparentes y ejemplificó con las alianzas que su empresa tiene con otros proveedores de Nube. “Tenemos que ser capaces de proveer transparencia. Tenemos alianzas con Amazon, Palo Alto, para poder compartir información y cada vez que hay un incidente podamos trabajarlo con nuestros clientes. Se trata de un ecosistema, compartir información privilegiada para saber todos qué es lo que sucedió”, comentó el ejecutivo.

LOS CIBERDELINCUENTES ATACAN EN LA NUBE Y UTILIZAN INTELIGENCIA ARTIFICIAL: CROWDSTRIKE - LATAM CISO SUMMIT

DPL - Los ciberdelincuentes se están desplazando hacia la Nube y están utilizando la Inteligencia Artificial para atacar los sistemas críticos de los países, advirtió Shawn Henry, Chief Security Officer de CrowdStrike. Durante la Cumbre CISO Latam, el directivo de la empresa de ciberseguridad señaló que las cadenas de abastecimientos, las tecnologías emergentes, los incidentes como las fallas eléctricas, las actualizaciones defectuosas de software (refiriéndose a la que tuvo Crowdstrike semanas atrás) y los desastres naturales como terremotos, requieren que las organizaciones y las empresas sean más resilientes.

FALTAN ESPECIALISTAS PARA ENFRENTAR LA CIBERSEGURIDAD - LATAM CISO SUMMIT

DPL - “La ciberseguridad es un problema humano, pero no existen suficientes personas para defendernos de los ciberataques”, planteó Mauricio Nanne, director de Seguridad de la Información de SISAP. Mencionó que tenemos que aprender a defendernos de las nuevas técnicas de los ciberataques, como el empleo de la Inteligencia Artificial. La razón es porque los humanos son profesionales de TI, pero todavía no de ciberseguridad. Estos especialistas no están disciplinados para proteger todos los días la seguridad.

EL FUTURO CIBERSEGURO REQUIERE FUERZA LABORAL ESPECIALIZADA: DAVID HOFFMAN - LATAM CISO SUMMIT

DPL - El futuro digital requiere una fuerza laboral especializada en ciberseguridad, aseguró David Hoffman, profesor de políticas públicas de la Universidad de Duke. Los datos se han vuelto cada vez más complejos y valiosos, y la ciberseguridad es cada vez más importante para los gobiernos y las organizaciones, por lo cual se requieren cada vez más expertos en el tema. Hoffman pidió superar la subrrepresentación de las mujeres en la industria de la ciberseguridad y propuso un programa de investigación en la región para desarrollar talento especializado en seguridad cibernética.

TITULAR DE MITIC ANUNCIA COOPERACIÓN DE ISRAEL EN CIBERSEGURIDAD - PARAGUAY

La Nación - Atendiendo a la reciente reapertura de la embajada de Israel en Paraguay, el titular del Ministerio de Tecnologías de la Información y Comunicación (Mitic), Gustavo Villate, remarcó que se empezarán a vislumbrar fortalecimientos bilaterales y en áreas estratégicas para el desarrollo nacional. “Seguiremos fortaleciendo los lazos, de hecho, venimos trabajando con Israel en temas de ciberseguridad espacial, donde tienen una fortaleza importante. Para nosotros, trabajar con nuestros aliados estratégicos es más que fundamental”, refirió el secretario de Estado.

HACKEO A PÁGINA DEL SAT EN SINALOA: ¿CRIMEN ORGANIZADO ESTÁ DETRÁS DEL ATAQUE? ESTO DICEN EXPERTOS- MÉXICO

El Financiero - Los ataques cibernéticos a las páginas web del Servicio de Administración Tributaria del Estado de Sinaloa (SATES) y del Colegio de Bachilleres del Estado de Sinaloa (Cobaes) en el que se muestra un ‘narcomensaje’ comprometen la información personal de los ciudadanos de la entidad, lo cual es muy peligroso porque hasta ahora se desconoce si el grupo de cibercriminales está ligado a organizaciones criminales de Sinaloa.

OPERACIÓN KAERB: DESARTICULAN UNA RED DE CIBERCRIMEN LIDERADA POR UN ARGENTINO

R2820 - Desde el Ministerio de Seguridad de la Nación destacaron que se logró la desarticulación de una Red Cibercriminal Internacional cuyo accionar se inicia con el robo de teléfonos celulares y se vincula a diversos delitos cibernéticos (como por ejemplo, acceso indebido, robo de datos, extorsiones, fraude). La reciente Operación presentada por la Secretaria de Seguridad, Alejandra Monteoliva, junto a las fuerzas de seguridad intervinientes, reveló la existencia de una sofisticada red criminal dedicada a configurar una multiplicidad de delitos asistidos tecnológicamente, teniendo como preferencia teléfonos celulares de alta gama, para luego obtener mediante engaño las credenciales de acceso no solo al dispositivo de la víctima, sino también a toda su información y aplicaciones.

GOBIERNO SE INTEGRA A LA INICIATIVA DE LA UNIÓN EUROPEA SOBRE CIBERSEGURIDAD Y CIBERCRIMEN - GUATEMALA

Prensa Libre - En un comunicado conjunto, emitido este martes 17 de septiembre, la Unión Europea (EU) en Guatemala y la Comisión Presidencial de Gobierno Abierto y Electrónico anunció la adhesión de Guatemala al Centro de Competencia Cibernética de América Latina y el Caribe (LAC4). Según explicaron ambas entidades, esta decisión se ha tomado para apoyar y mejorar el ejercicio de las dependencias del Organismo Ejecutivo en materia de ciberseguridad en el país, tales como el Comité Nacional de Seguridad Cibernética, Ministerio de Gobernación y Ministerio de la Defensa, entre otras.

WHAT WE KNOW ABOUT THE HEZBOLLAH PAGERS THAT EXPLODED IN LEBANON

CBS - A Hungarian official told CBS News Thursday that a Bulgaria-based company had purchased pagers from Taiwan that were eventually sold to Hezbollah, before exploding in the hands, pockets and bags of thousands of the Iran-backed militant group's members earlier this week in Lebanon. Hungarian outlet Telex had reported Wednesday that a Sofia-based company called Norta Global Ltd. Was behind a deal to sell the pagers and that a Hungarian firm connected with the transaction had not manufactured or sold the pagers. A Hungarian official told CBS News those reports were accurate. The new information about the origin of the exploding pagers came a day after Taiwanese company Gold Apollo said it had authorized the use of its trademarked branding on the pagers that exploded Tuesday across Lebanon and Syria, but that the devices were actually manufactured and sold by Bac Consulting KFT — a company based in Budapest, Hungary.

STRENGTHENING CYBERSECURITY: LESSONS FROM GUYANA'S DEFENCE INITIATIVE

Barbados Today - Technology can't be overlooked, especially with its rapid advancement, transforming warfare through innovations like combat drones. These advancements introduce new challenges and opportunities in the field of defence." With these words, Guyana's President Mohamed Irfaan Ali breathed life into what is likely the region's first National Defence Institute (NDI). The NDI, launched in Guyana, holds a broad mandate encompassing national security, including military strategy and tactics, with a key objective set by President Ali: to analyse gang movements and other transnational security threats. By addressing these cross-border challenges, the NDI underscores the need for regional cooperation, particularly in cyber defence and intelligence sharing. As the Caribbean faces increasing susceptibility to cyberattacks, the NDI is well-positioned to become a regional leader in cybersecurity preparedness.

SPOTIFY JOINS META IN OPEN LETTER TO EU DECRYING 'INCONSISTENT REGULATORY DECISION MAKING'

Digital Music News - Meta, Spotify, and several other companies and researchers have signed the open letter claiming that Europe has become less competitive and risks falling behind in the age of AI. The signatories seek "harmonized, consistent, quick and clear decisions" from data privacy regulators to "enable European data to be used in AI training for the benefit of Europeans." The letter specifically takes issue with the General Data Protection Regulation (GDPR) which passed in 2018. Specifically, Meta has stopped plans to harvest data from European users to train AI models after privacy regulators put pressure on the company and have issued fines for failing to respect privacy laws.

IS PATIENCE WANING WITH EFFORTS TO MODERATE CONTENT ON SOCIAL MEDIA?

WEF - Shortly after Hamas launched its surprise attack on Israel last October, channels used by the terrorist group on Telegram lit up with images of the ensuing atrocities. The response? A restriction of those channels that reportedly didn't do much restricting. Nearly a year later, Telegram's steady cultivation of a reputation as a free-speech bastion, sometimes to an extreme degree, has hit a glitch with the arrest of its founder and CEO in Paris. Pavel Durov has been compelled to remain in France, where he's under investigation for alleged complicity in criminal activity on his popular platform. "I got interviewed by police for 4 days," he posted on his channel. "No innovator will ever build new tools if they know they can be personally held responsible for potential abuse of those tools."

SDIM24: HOW PREVENTION-FIRST STRATEGIES AND ZERO TRUST CAN ENHANCE CLOUD SECURITY

WEF - In today's cloud-driven world, cyber security is a fundamental strategic consideration. CNAPPs have consequently gained popularity as a means of securing critical cloud environments. These security solutions are designed to protect cloud-native applications throughout their lifecycle, from development to deployment. Although CNAPPs help identify and manage risks, they primarily focus on alerting users and suggesting remediation rather than preventing attacks. As organizations rapidly adopt cloud technologies, the evolving threat landscape exposes the limitations of CNAPPs, making their security promises incomplete.