DIGI AMERICAS ALLIANCE MEMBERS

MÉXICO LANZA PLAN NACIONAL DE CIBERSEGURIDAD Y NUBE PARA IMPULSAR TRANSFORMACIÓN DIGITAL

Noti Press - El Gobierno de México, a través de la Agencia de Transformación Digital y Telecomunicaciones, presentó un proyecto conocido como el Plan Nacional de Ciberseguridad y Nube México. Este plan tiene como objetivo central garantizar la seguridad y resiliencia de los sistemas de información gubernamentales, optimizando el uso de infraestructura tecnológica para una administración más eficiente y transparente. Durante la presentación del proyecto en la mañanera del 14 de noviembre de 2024, el maestro José Antonio Peña Merino, quien lidera la agencia, explicó que la iniciativa busca unificar las capacidades tecnológicas del gobierno para lograr una mayor autonomía en el desarrollo de soluciones digitales. Esto no solo permite reducir costos operativos, sino también cerrar brechas de acceso a servicios públicos en toda la población.

INSEGURIDAD Y CIBERCRIMEN FRENAN EL DESPLIEGUE DE LAS REDES DE COMUNICACIÓN - MÉXICO

El Financiero - En México, la infraestructura de telecomunicaciones se ve cada vez más amenazada por el crimen organizado, lo que compromete el despliegue de redes de nueva generación como 5G. Alfredo Pacheco, director general de la Cámara Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías de la Información (Canieti), señaló que las empresas de telecomunicaciones enfrentan extorsiones y control de plazas que impiden el mantenimiento y expansión de las redes, además de la instalación de redes piratas usando infraestructura robada.

NOEMÍ LUNA EMPLAZA A LEGISLAR EN MATERIA DE CIBERSEGURIDAD TRAS DETECCIÓN DE MILES DE SITIOS WEB FALSOS - MÉXICO

Talla Política - La diputada Noemí Berenice Luna, coordinadora del Grupo Parlamentario del PAN, llamó a Morena a que acompañe las demandas de expertos y organizaciones, a fin de que se legisle en materia de ciberseguridad, pues la ausencia de regulación en este ámbito genera pérdidas millonarias por fraudes. Refirió que datos de la Secretaría de Seguridad y Protección Ciudadana (SSPC), a través del Registro Nacional de Incidentes Cibernéticos (RNIC), revelan que se detectaron 3 mil 888 sitios de internet apócrifos que se hacían pasar por dependencias gubernamentales para obtener datos personales y financieros, con el objetivo de cometer fraudes o propagar códigos maliciosos.

COMISIÓN AVALA LEYES DE CIBERSEGURIDAD Y DE PROTECCIÓN A DATOS PERSONALES

El Salvador - La comisión de Seguridad Nacional y Justicia de la Asamblea Legislativa avaló, tras una serie de modificaciones, la Ley de Ciberseguridad y seguridad de la información, así como la Ley de Protección de Datos Personales con solo los aportes de la Secretaría de Innovación de la Presidencia. La “Ley de Ciberseguridad y Seguridad de la Información”, que buscaría estructurar, regular y fiscalizar las medidas de ciberseguridad y seguridad de la información en poder de las instituciones públicas; también crea la Agencia de Seguridad del Estado también llamada “ACE”.

FORÇAS ARMADAS ATUARÃO NA SEGURANÇA DO G20 - BRASIL

Agencia Brasil - O Comando Militar do Leste informou que a operação para a Cúpula dos Líderes do G20 - nos dias 18 e 19 de novembro - envolverá meios da Marinha do Brasil, do Exército e da Força Aérea, em cooperação com o governo do estado, a prefeitura, agências diversas e órgãos de segurança pública. O Exército empregará aproximadamente 7.500 homens e mulheres, que atuarão em atividades como: escolta de autoridades; segurança de perímetros; proteção de infraestruturas críticas; patrulhamento de vias e áreas; ações de contraterrorismo; guerra eletrônica; defesa cibernética; defesa antiaérea; proteção contra drones; e defesa química, biológica, radiológica e nuclear. Será usados meios especializados e helicópteros.

EL PAÍS CONSOLIDA ESTRATEGIAS PARA ROBUSTECER LA SEGURIDAD INFORMÁTICA EN EL SECTOR FINANCIERO - COLOMBIA

MINTIC - Con el propósito de conocer nuevas iniciativas que fortalecen la ciberseguridad en el sector financiero, el ministro TIC, Mauricio Lizcano, recorrió hoy las instalaciones del Centro de Operaciones del Programa de colaboración e intercambio de información del sector financiero colombiano y Centro de Excelencia para la Ciberseguridad (CSIRT) de la Asociación Bancaria y de Entidades Financieras de Colombia (Asobancaria). En el encuentro, ratificó la importancia de crear alianzas estratégicas para fortalecer el Grupo de Respuesta a Emergencias Cibernéticas de Colombia (Colcert) con los CSIRT sectoriales, y ampliar así la seguridad cibernética en los diferentes sectores de la economía.

CASA BLANCA CONFIRMA QUE FINANCIÓ COMPRA DE ‘SOFTWARE’ PEGASUS PARA COLOMBIA EN MEDIO DE LA LUCHA CONTRA EL NARCOTRÁFICO

Semana - Este jueves, el diario El Tiempo informó, basado en fuentes de la Casa Blanca en Washington y Bogotá, que Estados Unidos financió la adquisición del software Pegasus para Colombia, en medio de la lucha contra el narcotráfico. “Dos altos funcionarios de la administración de Joe Biden en Washington y otro más en Bogotá, autorizados oficialmente para hablar del tema, le revelaron en exclusiva a El Tiempo que el Gobierno de Estados Unidos no solo estuvo al tanto de la compra del software Pegasus en Colombia sino que, además, fue ese país el que financió su adquisición”, informó el mencionado periódico. “Para ayudar a garantizar este uso adecuado, se establecieron protocolos estrictos con controles y equilibrios. La estricta supervisión de esta herramienta se diseñó e implementó para garantizar que el software se utilizara para perseguir objetivos legítimos relacionados con el narcotráfico. No tenemos información que sugiera que el software se utilizó indebidamente para vigilar a figuras políticas colombianas”, afirmó una de las fuentes, según la noticia publicada por El Tiempo.

EMIRATOS ÁRABES UNIDOS Y URUGUAY FIRMAN ACUERDO PARA LA PREVENCIÓN DE ATAQUES CIBERNÉTICOS

Gub.Uy - El 17 de octubre representantes de Agesic y el Consejo de Seguridad Cibernética de Emiratos Árabes Unidos (EAU) firmaron un Memorándum de Entendimiento con el objetivo de fortalecer la cooperación entre ambos países para la detección y prevención de incidentes de seguridad de la información. El acuerdo establece un marco de colaboración entre EAU y Uruguay para facilitar el intercambio de conocimientos y buenas prácticas, así como el desarrollo de capacidades conjuntas en el ámbito de la ciberseguridad.

PRIMERA EDICIÓN DEL ENTRENAMIENTO URUGUAY CIBERSEGURO

Gub.Uy - Del 6 al 8 de noviembre se realizó la primera edición del entrenamiento Uruguay Ciberseguro, con el objetivo de fomentar el trabajo en equipo de diversas instituciones públicas y privadas, y desarrollar habilidades en ciberseguridad mediante ejercicios de simulación de respuesta ante incidentes cibernéticos. La primera edición de Uruguay Ciberseguro se centró en ejercicios prácticos que promovieron la interacción entre distintos equipos, lo que permitió trabajar de manera integral en la identificación, resolución y manejo de incidentes cibernéticos.

MÁS DE 60 SITIOS DEL ESTADO INACCESIBLES: ¿QUÉ SUCEDIÓ Y CUÁNDO SE CORRIGIÓ? - URUGUAY

Agesic asegura que no se perdió información en el incidente y que se trató de un problema en el acceso. Caída masiva: Más de 60 webs del Estado, incluyendo ministerios, DGI y la Corte Electoral, dejaron de estar accesibles para la ciudadanía desde el jueves a las 15:00. En la mañana ya se recompuso. Agesic aclara: La Aagencia de Gobierno Electrónico y Sociedad de la Información (Agesic) aseguró que la información siempre estuvo segura; el problema fue que el acceso estuvo caído. Posible causa: Falla en dos dispositivos de seguridad.

FELABAN CIERRA CON 40.000 MILLONES DE DÓLARES EN NEGOCIOS Y CIBERSEGURIDAD

Hoy - Édgar Alarcón , director ejecutivo de la Asociación de Bancos del Paraguay (Asoban), se hizo un balance positivo sobre la edición de este año. “La asamblea está terminando con resultados muy positivos. Los asistentes se van muy contentos, con nuevas experiencias y aprendizajes, especialmente en cuanto a negocios y la visión futura del sector bancario”, expresó Alarcón en entrevista con GEN. Uno de los temas recurrentes en los paneles de discusión fue el impacto de la tecnología en el sector bancario. Las entidades bancarias de la región, especialmente en Paraguay, están adoptando cada vez más tecnologías para ofrecer un mejor servicio a sus clientes.

PAÍSES DE LATINOAMÉRICA FORTALECERÁN CAPACIDADES EN CIBERSEGURIDAD CON APOYO DE CHILE Y LA UNIÓN EUROPEA

EEAS - En las dependencias del Palacio de La Moneda se firmó un acuerdo para desarrollar el proyecto de cooperación triangular “Fortalecimiento y desarrollo de capacidades en América Latina y el Caribe en materia de ciberseguridad”, que apuesta por incrementar la resiliencia cibernética de los países latinoamericanos, contribuyendo así a un entorno digital más seguro y estable a nivel global. Esta iniciativa se enmarca en la Alianza Digital UE-ALC que busca promover la colaboración entre la Unión Europea y América Latina en asuntos digitales clave a través del diálogo e iniciativas conjuntas, fomentando una transformación digital centrada en el ser humano en ambas regiones.

TSA PROPOSES NEW CYBERSECURITY RULES

ExecutiveGov - The agency said Wednesday the proposal will mandate cyber risk management and reporting requirements for particular surface transportation operators. Under the proposal, certain pipeline, freight railroad, passenger railroad and rail transit owners and operators are required to establish and maintain a cyber risk management program. The owners and operators of the surface transportation systems also need to report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency previously, they were only required to report to the TSA. Finally, each high-risk pipeline owner and operator will designate a physical security coordinator to report physical security issues to the TSA.

UNPACKING CYBER RESILIENCE - WEF REPORT

WEF - Resilience in the face of cyber risk is a critical objective for any organization dependent on digital technologies and data. This places it on the radar for almost all business leaders in 2024. The globalization of our supply chains, the complexity of technology stacks and the continued appetite to innovate with digital have led to continued aggregation of systemic cyber risk. Effective cyber resilience is complex. How we achieve it and the controls we use are highly context dependent; what works in the face of one type of threat may not work as well for another. For example, defending against ransomware is very different from defending against denial of service, and defending against accidental failures in a system requires different solutions from defending against a malign threat actor seeking to attack for reasons of sabotage, theft or financial gain.

HOW PIONEERING PUBLIC-PRIVATE COLLABORATION IN THE FINANCIAL SECTOR CAN HELP SECURE ITS QUANTUM FUTURE

WEF - Recent advancements in quantum computing have raised the technology's role as a disrupter, significantly increasing the potential for actors in the financial sector to gain a competitive edge. Quantum technology promises breakthrough capabilities in algorithmic methodology such as portfolio optimization, Monte Carlo simulations and complex calculations, fueling projected investment growth from $80 million in 2022 to $19 billion by 2032. An increasing number of collaborations and research and development highlight financial services as a first mover in quantum computing. For example, JPMorgan Chase and PayPal are using IBM Quantum, to research optimization problems related to fraud detection.

COLLABORATIONS BETWEEN INDUSTRY EXPERTS AND THE PUBLIC SECTOR ARE DISRUPTING CYBERCRIMINALS. HERE'S HOW

WEF - An estimated 25.5% of the world's population was impacted by cyber-enabled fraud in 2023. The impact of the profits this generates for criminals goes further than the immediate victims. In 2023, the United Nations reported that at least 220,000 people had been trafficked in South-East Asia, some from as far away as Africa and Latin America, and forced to run online scams. A new white paper from the World Economic Forum, Disrupting Cybercrime Networks: A Collaboration Framework explores how to build on the success of existing partnerships to accelerate the disruption of cybercriminal activities. Here we examine some of its learnings and recommendations.

THE UN CYBERCRIME CONVENTION THREATENS SECURITY RESEARCH. THE US SHOULD DO SOMETHING ABOUT IT

CyberScoop - The United Nations' recent adoption of a new cybercrime convention has sparked significant discussion within the global cybersecurity community. While the UN Convention Against Cybercrime aims to enhance international cooperation to combat malicious hacking, the convention raises serious concerns for those involved in security research and ethical hacking. The treaty's provisions related to security research conflict with best practices encouraged by the U.S. government and federal policies that protect good-faith security research from prosecution. Despite these and other concerns, the treaty is expected to receive final approval from the General Assembly by the end of the year.

WHAT COULD THE TRUMP ADMINISTRATION MEAN FOR CYBERSECURITY?

Information Week - The results of the 2024 US presidential election kicked off a flurry of speculation about what changes a second Donald Trump administration will bring in terms of policy, including cybersecurity. InformationWeek spoke to three experts in the cybersecurity space about potential shifts and how security leaders can prepare while the industry awaits change. In 2020, Trump fired Cybersecurity and Infrastructure Security Agency (CISA) Director Christopher Krebs after he attested to the security of the election, despite Trump's unsupported claims to the contrary. It seems that the federal agency could face a significant shakeup under a second Trump administration.