DIGI AMERICAS ALLIANCE MEMBERS

A SUBCOMISSÃO PERMANENTE DE DEFESA CIBERNÉTICA (CREDC) VAI ANALISAR PROPOSTAS DE POLÍTICA NACIONAL DE CIBERSEGURANÇA E DE SISTEMA NACIONAL DE CIBERSEGURANÇA - BRASIL

Telesintese - O Senado instalou hoje, 14, a Subcomissão Permanente de Defesa Cibernética. Vinculada à Comissão de Relações Exteriores, buscará responder, entre outras perguntas, se é necessário criar uma Agência de Cibersegurança no Brasil. Conforme Esperidião Amin (PP-SC), presidente da subcomissão eleito nesta terça-feira, 14, os trabalhos vão até novembro, quando deverá ser entregue o relatório com as conclusões do colegiado. Com três membros titulares e igual número de suplentes, a criação foi proposta pelo próprio Amin, que em 2016 relatou a CPI dos Crimes Cibernéticos na Câmara dos Deputados.

MÉXICO IMPLEMENTA AVANZADAS MEDIDAS DE CIBERSEGURIDAD PARA EL CONTEO RÁPIDO ELECTORAL

DPL News - Con la jornada electoral del 2 de junio en el horizonte, el Instituto Nacional Electoral (INE) intensificó sus esfuerzos para garantizar la eficiencia y seguridad del Programa de Resultados Electorales Preliminares (PREP). En conferencia de prensa, se puso en relieve la importancia de las pruebas de ciberseguridad y el correcto funcionamiento del sistema, destacando la implementación de mecanismos robustos para asegurar la integridad del proceso electoral. Para mitigar cualquier interrupción en la conectividad a Internet, el sistema cuenta con un mecanismo de redundancia operativa. Si las actas no pueden ser transmitidas a través del sistema de PREP casilla, existe un mecanismo alternativo: los centros de acopio y transmisión de datos. Los responsables de las casillas pueden entregar el paquete electoral, que incluye una bolsa PREP con el acta correspondiente. Esta acta se escanea y, si no ha sido capturada previamente, se envía a digitalización.

LOS PUNTOS DE LA LEY DE SEGURIDAD DIGITAL EN ECUADOR QUE PREOCUPAN A LA INDUSTRIA

DPL News - La Cámara de Innovación y Tecnología de Ecuador (Citec) celebró que el Pleno de la Asamblea Nacional continúe con el debate del proyecto de Ley de Seguridad Digital y aún no se vote, ya que esperan que se puedan realizar los ajustes pertinentes que preocupan a la industria, afirmó a DPL News Diego Álvarez, secretario director de la Citec. El pasado 7 de mayo se debatió el proyecto de ley, en donde asistieron diversos actores del sector. La Asamblea Nacional destacó las participaciones de especialistas en ciberseguridad, quienes indicaron que la “iniciativa es una ventana de oportunidad en la generación de empleo para los jóvenes ecuatorianos”.

ADVIERTEN POR EL CRECIMIENTO EN URUGUAY DEL CIBERATAQUE "DATA EXTORTION": AFECTÓ A UN LICEO PRIVADO DE MONTEVIDEO

El Observador - La tecnología evoluciona y los hackers no se quedan atrás. En el último mes, los analistas en ciberseguridad advierten por una nueva modalidad que crece y que llama la atención: se llama data extortion (extorsión de datos) y tiene una leve diferencia respecto al ransomware. Mauro Eldritch, quien lidera un portal donde se publican todos los hackeos que ha habido en el país en el último tiempo (MeFiltraron), ha detectado un "interesante incremento" de este tipo de ataque.

COSTA RICA ES SEDE DE DIÁLOGO POLÍTICO DE ALTO NIVEL SOBRE GOBERNANZA DIGITAL DE LA ALIANZA DIGITAL EU-LAC

Revista Summa - Hoy dio inicio en el territorio costarricense un encuentro importante para el futuro digital de nuestra región. El EU-LAC Digital Alliance reúne a líderes y expertos para discutir temas clave como interoperabilidad, identidad digital y firmas transfronterizas. En el acto de inauguración participaron Paula Bogantes, Ministra de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica, Felice Zaccheo, DG INTPA, Comisión Europea, Edie Cux, Director Ejecutivo de la Comisión Presidencial de Gobierno Abierto y Digital de Guatemala (co-líder), Nele Leosk, Embajadora en Asuntos Digitales, Ministerio de Asuntos Exteriores de Estonia y Hannes Astok, Presidente del Consejo de Administración, e-Governance Academy (eGA), Estonia.

BANCO SANTANDER SUFRE HACKEO EN ESPAÑA, CHILE Y URUGUAY: ¿CÓMO SABER Y QUÉ HACER SI TE AFECTÓ?

Wired - Banco Santander ha confirmado que fue víctima de un ciberataque. El hackeo comprometió la información de clientes, colaboradores y ex empleados del grupo en Chile, España y Uruguay. La entidad financiera ha emitido una serie de recomendaciones para evitar afectaciones mayores. Santander comunicó a la Comisión Nacional del Mercado de Valores (CNMV) de España sobre “un acceso no autorizado” en sus sistemas. Aclaró que en la base de datos intervenida “no hay información transaccional ni credenciales o contraseñas de banca por internet. Las operaciones y los sistemas de Santander no están afectados y los clientes pueden seguir utilizando sus instrumentos financieros con seguridad”.

BIBLIOTECA NACIONAL FIRMA ACUERDO CON CENTRO NACIONAL DE CIBERSEGURIDAD - REP. DOMINICANA

M.N - La Biblioteca Nacional Pedro Henríquez Ureña (BNPHU) y el Centro Nacional de Ciberseguridad (CNCS), dependencia del Ministerio de la Presidencia, firmaron un acuerdo de cooperación interinstitucional, para promover una cultura de ciberseguridad para la protección efectiva del Estado. El acuerdo fue firmado por Juan Gabriel Gautreaux Martínez, director del CNCS, y por Rafael Peralta Romero, director de la BNPHU. Ambas instituciones acordaron el establecimiento de mecanismos de coordinación, interacción, cooperación y reciprocidad que faciliten la realización de actividades de interés y beneficio mutuo.

ESTAS SON LAS ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD DE LOS PAÍSES LATINOAMERICANOS

Segurilatam - Es innegable que Latinoamérica, en general, está en pleno crecimiento en materia de ciberseguridad. Y aunque no todos los países van al mismo ritmo ni disfrutan de la misma madurez, los gobiernos de cada uno de ellos ya se han puesto manos a la obra para conseguir que tanto sus organismos públicos como el sector privado se vean afectados lo menos posible ante cualquier eventualidad procedente del ciberespacio. Un ejemplo de ello lo constituyen las diversas estrategias nacionales de ciberseguridad con las que cuentan los países latinoamericanos. Cada una con sus particularidades, incluso algunas de ellas con variaciones en su denominación, pero que persiguen un objetivo común: protegerse, gestionar y recuperarse de la manera más eficaz y con mayor celeridad factible ante un ciberataque.

CYBERCRIME BILL IN FOCUS - BARBADOS

Barbados Today - The Government of Barbados recently walked back on the Cybercrime Bill 2024, sending it to a Joint Select Committee after it was passed in the House of Assembly. This development has been welcomed by many as it afforded citizens, locally and abroad, the opportunity to weigh in on the merits and demerits of the Bill before it is passed. In reviewing the Bill, several laudable ideals were noted: • Combating cybercrime: The Bill aims to criminalise various cybercrimes including illegal access to computer systems, data modification, denial-of-service attacks, and cyberstalking. It also outlines procedures for investigating and prosecuting these offences. • Protection of interests: It seeks to safeguard legitimate business interests in the digital landscape by deterring cyberattacks and data breaches. • International cooperation: The Bill facilitates collaboration with other countries on cybercrime investigations and extradition of cybercriminals.

PNP SPOKESMAN URGES 'SWIFT' ACTION TO BOOST GOVERNMENT CYBERSECURITY - JAMAICA

Jamaica Gleaner - The Opposition Spokesman on Technology Dr Andre Haughton is urging the Government to take "swift and decisive" action to stem the "troubling surge" of cyberattacks on state institutions. His call follows news that the Bureau of Standards Jamaica (BSJ) was the victim of a ransomware attack in February. The agency has spent over $36 million on efforts to recover, and strengthen its information technology systems. Over the last 12 months, the state-owned oil refinery Petrojam and the regulator, the Financial Services Commission suffered similar attacks.

OPTIMIZING THE SUPPLY CHAIN WITH A DATA LAKEHOUSE

MIT - When a commercial ship travels from the port of Ras Tanura in Saudi Arabia to Tokyo Bay, it’s not only carrying cargo; it’s also transporting millions of data points across a wide array of partners and complex technology systems. Consider, for example, Maersk. The global shipping container and logistics company has more than 100,000 employees, offices in 120 countries, and operates about 800 container ships that can each hold 18,000 tractor-trailer containers. From manufacture to delivery, the items within these containers carry hundreds or thousands of data points, highlighting the amount of supply chain data organizations manage on a daily basis.

GLOBAL FINANCIAL STABILITY AT RISK DUE TO CYBER THREATS, IMF WARNS. HERE'S WHAT TO KNOW

WEF - Global financial stability is under threat from the increasing frequency and sophistication of cyberattacks, according to a new report by the International Monetary Fund (IMF). The risk of extreme losses from cyberattacks is also increasing, the report notes, leaving the financial sector uniquely exposed to cyber threats as operations involve vast amounts of sensitive data and transactions. For financial institutions, the result of a cyberattack could mean funding challenges, reputational damage and could even lead to insolvency. Moreover, experts warn that for the wider financial sector, major attacks could undermine confidence in the system, disrupt critical services and spill over to other sectors.

SEC RULE FOR FINANCE FIRMS BOOSTS DISCLOSURE REQUIREMENTS

CSO - The SEC announced rule changes for some financial companies that will require more customer disclosures when security incidents impact their personal information as well as mandate incident response programs. The new rule, however, is unlikely to change anything for enterprise financial companies as they were either already required to make such disclosures or already had incident response programs in place. “Over the last 24 years, the nature, scale, and impact of data breaches has transformed substantially,” said SEC chair Gary Gensler in a statement. “These amendments will help protect the privacy of customers’ financial data. The basic idea for covered firms is if you’ve got a breach, then you’ve got to notify. That’s good for investors.”

CONGRESO DE HACKERS - DRAGONJAR SECURITY CONFERENCE 2024

DragonJAR Security Conference es un evento realizado anualmente con foco en la seguridad informática en español. Este año contaremos con 19 invitados de ocho países distintos, desafíos técnicos y seremos el primer evento en Colombia con un badge electrónico que incluirá conectividad con diferentes protocolos como Wi-Fi, Bluetooth, Zigbee y Thread. Además, será compatible con otros badges de congresos emblemáticos de la región, como la Ekoparty. Tendremos charlas que van desde la disección del malware que causó apagones en Ucrania, cómo se realizan pruebas de seguridad en tecnología aeroespacial y satélites, pasando por cómo auditar y asegurar tecnología en la nube, temas técnicos como fuzzing y de concientización para adultos mayores, además de explicar casos de ransomware y cómo se han resuelto, entre otras temáticas.