DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 20, 2024

DIGI AMERICAS ALLIANCE MEMBERS

COSTA RICA: RECONOCEN FALTA DE ASESORES PARA LEGISLAR CIBERSEGURIDAD, PRIVACIDAD DE DATOS O 5G

TyN - La diputada y presidenta de la Comisión de Ciencia y Tecnología, Johanna Obando, así como el secretario de esa misma comisión, José Pablo Sibaja, reconocen falta de personal experto en tecnología en la Asamblea Legislativa que asesore a las diputaciones, que son las encargadas de legislar en temas como ciberseguridad, privacidad de los datos, desarrollo tecnológico, infraestructura, entre otros. Así lo indicaron durante un evento organizado por la Unión Costarricense de Cámaras y Asociaciones del Sector Empresarial Privado (Uccaep) la mañana de este martes 18 de junio.

GSI: SEM NOVA AGÊNCIA, PAÍS PERDEU 14% DO SEU PIB POR FALTA DE SEGURANÇA DA INFORMAÇÃO - BRASIL

Capital Digital - O Brasil pode ter perdido em 2023 cerca de R$ 1,5 trilhão com ciberataques, o que representa 14% do PIB registrado no ano passado e foi de R$ 10,5 trilhões. Essas cifras foram obtidas projetando o mesmo percentual apresentado no Fórum Econômico Mundial, que fixou em 14% do PIB mundial (U$ 10,5 trilhões), as perdas geradas na economia global com problemas de cibersegurança. Numa estimativa mais conservadora, feita pela Accenture, essa perda chegou aos R$ 500 bilhões. A avaliação foi feita pelo Assessor Especial GSI, Marcelo Malagutti, ao defender a criação da Agência Nacional de Cibersegurança (ANCiber), durante webinar da Fundação Getúlio Vargas sobre o tema: “Cibersegurança no Brasil: como construir uma estratégia e uma agência?”.

EXÉRCITO PUBLICA EDITAL E BUSCA RECURSOS PARA FAZER O GUARDIÃO CIBERNÉTICO 6.0 - BRASIL

Convergencia Digital - O Comando de Defesa Cibernética quer parceiros públicos e privados para organizar e viabilizar o exercício de guerra cibernética contra infraestruturas críticas, o Guardião Cibernético 6.0. Um chamamento público recebe sugestões e propostas por um mês. O Guardião Cibernético tem por objetivo criar um ambiente realista onde as infraestruturas críticas participantes precisam proteger seus sistemas de Tecnologia da Informação de ataques cibernéticos, contribuindo para o crescimento da resiliência cibernética do Brasil, por intermédio da atuação colaborativa das Forças Armadas, dos órgãos parceiros e das principais infraestruturas críticas do País, adotando técnicas de simulações construtiva e virtual.

BANXICO INFORMA SOBRE DOS CIBERATAQUES EN LO QUE VA DE 2024 - MEXICO

Informador - El Banco de México (Banxico) informó que durante el primer semestre del 2024 se registraron dos incidentes cibernéticos significativos contra dos instituciones financieras.En marzo pasado, una Sociedad Financiera Popular (Sofipo), cuyo nombre no se dio a conocer, sufrió una vulneración informática en su servicio de transferencias. Aunque los ciberdelincuentes atacaron el servicio de transferencias electrónicas que proporciona, los clientes no se vieron perjudicados, aseguró.

DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 20, 2024

ASÍ ESTÁN ESTAFANDO CON FALSA PÁGINA WEB DE EPM; SEÑALES PARA IDENTIFICAR EL PORTAL ORIGINAL - COLOMBIA

Semana - Cada vez más, los ciberdelincuentes encuentran nuevas formas de engañar a los usuarios y robarles mediante diversas artimañas, como la suplantación de identidad. Un caso reciente involucra a Empresas Públicas de Medellín (EPM), quienes el pasado viernes 14 de junio denunciaron a través de un comunicado que su página web había sido víctima de suplantación. Esta plataforma es crucial para que los ciudadanos realicen el pago de sus facturas. Según el comunicado, los delincuentes habrían modificado la dirección legítima de la empresa, “facturaweb.epm.com.co”, redirigiendo a los clientes a una cuenta bancaria controlada por terceros mediante la URL fraudulenta “facturaepm.com.co”.

DISTINGUEN A SENADOR PUGH POR SU CONTRIBUCIÓN EN ESTRATEGIAS COMUNES PARA LA CIBERSEGURIDAD - CHILE

Senado - Rumania tiene una responsabilidad de coordinar los 27 estados europeos para desarrollar competencias de ciberseguridad. En esa línea, el gobierno de ese país reconoció la labor del senador Kenneth Pugh en la construcción de lazos diplomáticos entre ambos países, y en la elaboración de estrategias comunes para la ciberseguridad, facilitando así las inversiones entre Chile y Rumania. La distinción fue otorgada por el Presidente de Rumania, Klaus Werner Iohannis a través de su representante en Chile, el embajador, Floricel Mocanu. A la ceremonia, realizada en la sede de la Embajada asistieron además, el presidente del Senado, José García Ruminot y el senador José Miguel Insulza.

U. DE CHILE COMPARTIRÁ HERRAMIENTAS DE CIBERSEGURIDAD CON RED DE INVESTIGACIÓN Y EDUCACIÓN DE CHILE (REUNA)

UChile - La Vicerrectoría de Tecnologías de la Información, a través de la Oficina de Seguridad de la Información (OSI), firmó un convenio de cooperación con la Red de Investigación y Educación de Chile (REUNA), plataforma integrada por más de 40 universidades, centros de investigación de excelencia y grupos astronómicos internacionales presentes en nuestro país. El acuerdo permitirá poner a disposición de todas las universidades e instituciones socias de esta Red herramientas de monitoreo automatizado de vulnerabilidades. De esta manera, contribuirá a la realización de análisis preventivos, mediante pruebas de concepto, con el objetivo de identificar tempranamente posibles incidentes de seguridad informática.

LA ESTRATEGIA NACIONAL EN CIBERSEGURIDAD QUE TRABAJA EL GOBIERNO, ¿QUÉ VA A IMPLICAR Y CÓMO SE COMBATE EL CIBERCRIMEN? - URUGUAY

El Pais - Las amenazas en ciberseguridad cada vez son más peligrosas, más sofisticadas, más recurrentes y más cercanas a cada empresa y persona. “Todos debemos pensar que fuimos hackeados o que lo seremos en algún momento”, dicen los expertos en la materia. Ante este contexto, el gobierno uruguayo trabaja en su Estrategia Nacional de Ciberseguridad (ENC), que incorpora “agentes de investigación” fuera del radar popular, unifica una visión de Estado y se centra en las personas. La creación de la ENC se enmarca dentro de la Agenda Uruguay Digital 2025 presentada por la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Agesic), que busca mitigar riesgos de ciberseguridad y garantizar la disponibilidad de los activos críticos de información.

DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 20, 2024

LAS FUERZAS ARMADAS CONTINÚAN COLABORANDO CON LA CIBERSEGURIDAD NACIONAL - URUGUAY

Gub.uy - En el mes de junio, expertos del Departamento de Defensa de los Estados Unidos (SOUTHCOM & Guardia Nacional de Connecticut) realizan exposiciones para público cívico-militar, referente a ciberseguridad. En esta instancia, el Estado Mayor de la Defensa convocó a los responsables en Ciberseguridad de las Infraestructuras del Estado, a presenciar una exposición del Departamento de Defensa de los Estados Unidos (SOUTHCOM & Guardia Nacional de Connecticut) consistente en exposiciones de expertos de Áreas de Inteligencia de Amenazas, Despliegue Internacional de Grupos de Respuesta de Incidentes Mayores e implementación y mejores prácticas de un Centro de Operaciones de Ciberseguridad (SOC).

BANCO BISA ENTREGA HERRAMIENTAS EN FAVOR DE LA CIBERSEGURIDAD EMPRESARIAL - BOLIVIA

Fides - “Seguridad de la Información en las empresas” es una iniciativa basada en la educación, concienciación y colaboración de Banco BISA y se enfoca en fortalecer la resiliencia colectiva frente a las amenazas cibernéticas a través de encuentros con especialistas. En ese contexto, se realizaron eventos regionales en La Paz,Cochabamba y Santa Cruz en los que participaron representantes de empresas y personeros del BISA especializado en el ámbito informático. El objetivo principal de estos eventos fue subrayar la importancia de la ciberseguridad en el contexto del creciente uso de servicios y canales digitales en Bolivia.

CISA LEADS FIRST TABLETOP EXERCISE FOR AI CYBERSECURITY

CyberScoop - Looking to build its incident response muscles before artificial intelligence becomes an even greater threat, the federal government on Thursday held its first tabletop for the burgeoning technology, bringing in partners from across the country and abroad for the exercise. The Cybersecurity and Infrastructure Security Agency led the tabletop under the Joint Cyber Defense Collaborative, the operational arm of the cyber defense agency that is focused on working with industry, alongside 50 AI experts from 15 companies and several international cyber defense agencies.

FBI TAKES DOWN ARMY OF ‘ZOMBIE’ COMPUTERS. HERE WHAT TO KNOW

WEF - In late May 2024, the US Federal Bureau of Investigation made an arrest in a case it described at something “ripped from a screenplay”. The operation took down a botnet that had infected millions of computers with malware in nearly 200 countries. Selling access to this network enabled crimes, including billions of dollars of financial fraud, identity theft, bomb threats and access to child exploitation materials around the world. The alleged operator used the proceeds to buy fast cars, luxury watches and properties in multiple countries. The service, known as “911 S5”, is thought to have been the world’s biggest-ever example of a botnet. And it comes as the share of web traffic caused by harmful bots is rising year-on-year.

DIGI AMERICAS LATAM CISO

INSIGHTS

JUNE 20, 2024

STATEMENT FROM NATIONAL SECURITY ADVISOR JAKE SULLIVAN ON THE GLOBAL EFFORT TOSTRENGTHEN THE CYBERSECURITY OF ENERGY SUPPLY CHAINS

The White House - Energy systems around the world face continuous cyber attacks and are vulnerable to disruption. As new digital clean energy technologies are integrated, we must ensure they are cyber secure to prevent destruction or disruption in services. This is a global issue and at the G7 Leaders' Summit in Apulia, President Biden and G7 leaders committed to taking critical action to strengthen the cybersecurity of the global supply chain of key technologies used to manage and operate electricity, oil, and natural gas systems across the world. The G7 will work to establish a collective cybersecurity framework for operational technologies for both manufacturers and operators. This builds on the White House Council on Supply Chain Resilience's work to strengthen supply chains critical to America's economic and national security. It also builds upon the efforts of the U.S. Department of Energy (DOE) and Idaho National Laboratory which have brought tremendous expertise to bear in securing operational technologies to date.

THE NEW FRONT IN CHINA'S CYBER CAMPAIGN AGAINST AMERICA

The Economist - The island of Guam, a tiny American territory that lies more than 6,000km west of Hawaii, has long known that it would take a battering in any Sino-American war. The island's expanding airfields and ports serve as springboards for American ships, subs and bombers. In the opening hours of a conflict, these would be subject to wave after wave of Chinese missiles. But an advance party of attackers seems to have lurked quietly within Guam's infrastructure for years. In mid-2021 a Chinese hacking group—later dubbed Volt Typhoon—burrowed deep inside the island's communication systems. The intrusions had no obvious utility for espionage. They were intended, as America's government would later conclude, for "disruptive or destructive cyber-attacks against…critical infrastructure in the event of a major crisis or conflict". Sabotage, in short.