DIGI AMERICAS ALLIANCE MEMBERS

MINISTRO DA DEFESA REFORÇA IMPORTÂNCIA DE INVESTIMENTOS EM CIBERSEGURANÇA - BRASIL

Defesa em Foco - Durante o Exercício Guardião Cibernético 6.0, realizado em Brasília, o Ministro da Defesa, José Mucio Monteiro, ressaltou a necessidade urgente de ampliar investimentos na área de cibersegurança. Em um cenário onde ataques virtuais representam uma crescente ameaça à soberania nacional, o ministro destacou que proteger infraestruturas críticas é tão importante quanto se preparar para conflitos armados tradicionais. A defesa de infraestruturas críticas, como usinas nucleares e hidrelétricas, centros de telecomunicação e sistemas de transporte, é essencial para manter a segurança e estabilidade de um país. No entanto, essas estruturas estão cada vez mais vulneráveis a ataques cibernéticos sofisticados que podem comprometer operações vitais e fragilizar a soberania nacional. Durante o Exercício Guardião Cibernético 6.0, o Ministro José Mucio Monteiro destacou que, para o Brasil, o fortalecimento da segurança digital deve ser uma prioridade estratégica.

CIBERSEGURANÇA: MAIS QUE AGÊNCIA REGULADORA, BRASIL PRECISA DE ESTRUTURA DE GOVERNANÇA

Convergencia Digital - O Brasil tem espaço para uma estrutura de governança para a cibersegurança, não necessariamente para uma agência reguladora ou uma autarquia em regime especial, pontua o diretor de Privacidade e Segurança do Sistema de Gestão de Desempenho do Ministério da Gestão e Inovação, Leonardo Ferreira. À CDTV, do portal Convergência Digital, durante a 2ª edição do Cyber.GOV, organizado pela Network Eventos, em Brasília, Ferreira observou que o país possui estruturas que já olham atentamente à cibersegurança como a polícia federal, o Cert.br e própria Secretaria de Governo Digital. “Mas é fato que temos de ter uma estrutura de governança que faça a coordenação e a integração”, assinalou. Caberá à Secretaria de Governança Digital fazer a cibersegurança do G20, evento que acontece em Novembro, no Rio de Janeiro, e que vai reunir líderes de todo o mundo. “Já fizemos mais de 100 reuniões ao longo desses últimos meses e estamos nos preparando muito”, salientou, sem no entanto, abrir detalhes da estratégia a ser adotada.

DIGI AMERICAS LATAM CISO

INSIGHTS

OCTOBER 24, 2024

JUSTIÇA ELEITORAL ALERTA PARA GOLPE COM FALSO E-MAIL SOBRE CONVOCAÇÃO

Agencia Brasil - O Tribunal Regional Eleitoral de São Paulo (TRE-SP) emitiu um alerta sobre falsas mensagens de e-mail que utilizam o nome da Justiça Eleitoral para fazer convocações fictícias de mesários para o segundo turno das eleições municipais. De acordo com o TRE-SP, as mensagens pretendem captar dados pessoais das vítimas para realizar golpes. “Para atrair a atenção das pessoas, a mensagem falsa traz um conteúdo alarmante sobre a solicitação de dispensa para a convocação de mesário, informando que a multa seria R$1.064,10, acrescido de 50% do salário mínimo, totalizando R$ 1.770,10. Acrescenta que “a multa será enviada no IPTU ou contas essenciais (contas de Energia ou Água) do CPF do mesário ou dos pais”, destaca em nota o tribunal eleitoral.

ESPERIDIÃO AMIN ALERTA SOBRE DESAFIOS DA DEFESA CIBERNÉTICA - BRASIL

Agência Senado - O senador Esperidião Amin (PP-SC) destacou, em pronunciamento no Plenário nesta quarta-feira (16), a participação de parlamentares em um exercício de defesa cibernética realizado pela Escola Superior de Defesa, em parceria com as Forças Armadas. O senador informou que foi designado relator do Plano de Defesa Nacional das Forças Armadas e anunciou que incluirá no relatório a necessidade de reforçar o orçamento destinado à segurança cibernética. Ele enfatizou que o Brasil precisa se preparar adequadamente para enfrentar esses desafios.

PROPONEN LEY PARA REGULAR CIBERESPACIO Y TAMBIÉN LA CIBERSEGURIDAD - MÉXICO

La Prensa - México es un país muy atractivo para los ciberdelincuentes al presentar un rezago significativo en materia de protección, aseguró la presidenta de la Comisión de Atención Especial a Víctimas del Congreso de la Ciudad de México, Ana Buendía García, quien promueve mediante una iniciativa crear una ley general que regule el ciberespacio y la ciberseguridad. Consideró pertinente adicionar una fracción al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, que permita al Congreso de la Unión expedir una Ley General en materia de Ciberespacio y Ciberseguridad, misma que deberá establecer reglas claras y el contar con autoridades facultadas para regular los ecosistemas digitales, proteger los datos personales y combatir los ciberdelitos.

GRUPO AEROPORTUARIO OMA SUFRE ATAQUE DE CIBERSEGURIDAD - MÉXICO

Forbes - El Grupo Aeroportuario del Centro Norte (OMA) informó este viernes que fue víctima de un incidente de ciberseguridad sin que hasta ahora haya identificado efectos adversos en sus operaciones. OMA, que administra 13 terminales aéreas en la región centro-norte en México, dijo que el episodio está relacionado con un acceso no autorizado a sus sistemas de información. “El equipo de TI (Tecnologías de la Información) de OMA, en colaboración con expertos externos en ciberseguridad, está investigando activamente el incidente para determinar su alcance y garantizar la protección de la integridad, confidencialidad y disponibilidad de nuestros sistemas”, dijo la empresa en un comunicado.

DIGI AMERICAS LATAM CISO

INSIGHTS

OCTOBER 24, 2024

SECTOR FINANCIERO EN COLOMBIA RECIBE 45 CIBERATAQUES POR SEGUNDO: MINTIC

Caracol - En un balance entregado por el Ministerio de Tecnologías de la Información y las Comunicaciones (TIC), se encontró que en lo corrido de este año, el país recibió cerca de 24,000 millones de ciberataques, donde el sector más afectado fue el financiero con un 98%. El ministro TIC, Mauricio Lizcano, mencionó que las personas más afectadas son las de más bajos recursos. Dentro de la estrategia del ministro esta fortalecer el Grupo de Respuestas a Emergencias Cibernéticas de Colombia (ColCert), invertir en centros de operaciones de ciberseguridad (SOC) y subrayo la importancia de capacitar y educar a la población en general para bajar la efectividad de estos ataques. También el ministro destacó el programa Ciberpaz, que cuenta con un componente de 'Seguridad y confianza digital', que busca fomentar el uso seguro y responsable de las TIC

MINTIC ANUNCIA ESTRATEGIA DE CIBERSEGURIDAD FINANCIERA CON INTELIGENCIA ARTIFICIAL - COLOMBIA

El Frente - En la apertura del 17° Congreso de Seguridad, Amenazas Cibernéticas, Fraude y Experiencia (SAFE), el ministro de Tecnologías de la Información y las Comunicaciones (TIC), Mauricio Lizcano, destacó la importancia de la inteligencia artificial en la ciberseguridad financiera del país. Durante el evento organizado por Asobancaria, el Ministro socializó la estrategia del Ministerio TIC para proteger a la ciudadanía, instituciones y empresas de las crecientes amenazas cibernéticas.

COLOMBIA SUSPENDED FROM EGMONT GROUP FOLLOWING GUSTAVO PETRO'S SPEECH OVER PEGASUS SPYWARE

Finance Colombia - As a result of Gustavo Petro revealing clasified information about the Pegasus spyware, the President of the Egmont Group of Financial Intelligence Units, Elżbieta Franków-Jaśkiewicz, confirmed the suspension of Colombia from the program, and said: "Due to recent actions involving FIU Colombia and the unauthorized disclosure of information provided by one of our members, the Egmont Group Heads of FIU have confirmed the suspension of FIU Colombia's access to the Egmont Secure Web (ESW). The Egmont Group is a global organization of 177 Financial Intelligence Units (FIUs) that supports international efforts to combat money laundering, terrorist financing, and related crimes.

LA CNEA OFRECE SERVICIOS DE CIBERSEGURIDAD PARA INSTITUCIONES Y EMPRESAS - ARGENTINA

Argentina.gob - La ciberseguridad cumple un rol fundamental para la protección de la información y los sistemas de las instituciones y empresas, tanto públicas como privadas. En la Comisión Nacional de Energía Atómica (CNEA) se prestan servicios de seguridad informática para acompañar la labor de investigación y desarrollo del organismo. Algunos de esos servicios, como capacitaciones y auditorías de aplicaciones e infraestructura para detectar posibles vulnerabilidades, también están disponibles para clientes externos. Una de las capacitaciones que ofrece el Departamento de Seguridad Informática de la Gerencia de Tecnología de la Información y de las Comunicaciones de la CNEA busca concientizar en ciberseguridad a los usuarios finales. "El objetivo es generar conciencia sobre cuáles son los principales riesgos a los que estamos expuestos día a día en materia de seguridad informática y cómo defenderse.

DIGI AMERICAS LATAM CISO

INSIGHTS

OCTOBER 24, 2024

INDOTEL IMPULSA SEGURIDAD DIGITAL CON LANZAMIENTO DE «LISTA ELECTRÓNICA DE CONFIANZA» - REP. DOMINICANA

El Nuevo Diario - El Instituto Dominicano de las Telecomunicaciones (INDOTEL), lanzó su Lista Electrónica de Confianza, un nuevo paso hacia el desarrollo del entorno digital de República Dominicana, cuya iniciativa busca robustecer la seguridad de las transacciones electrónicas y garantizar la validez de las firmas digitales a nivel global. La implementación de esta Lista Electrónica de Confianza, posiciona al país como un referente en la adopción de servicios electrónicos de confianza y reafirma el compromiso de INDOTEL con la modernización digital del país, mejorando la seguridad tecnológica y abriendo oportunidades de cooperación internacional.

INDOTEL IMPULSA EDUCACIÓN SOBRE CIBERSEGURIDAD EN JÓVENES DOMINICANOS - REP. DOMINICANA

Diario Digital - El Instituto Dominicano de las Telecomunicaciones (INDOTEL) ha puesto en marcha un programa educativo diseñado para fomentar el uso seguro de Internet entre niños, niñas y adolescentes. Esta iniciativa se inicia con la participación de más de 100 estudiantes del Instituto Tecnológico Fabio Amable Mota. El programa, que se desarrollará a lo largo de seis meses, está enfocado en adolescentes de 14 a 15 años, quienes recibirán capacitación sobre las mejores prácticas para garantizar su seguridad en línea y el uso responsable de tecnologías esenciales.

COSTA RICA FORTALECE SU CIBERSEGURIDAD CON INVERSIÓN HISTÓRICA Y COOPERACIÓN INTERNACIONAL

El Mundo - El Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (Micitt) informó sobre el histórico aumento del 446% en la inversión para fortalecer la ciberseguridad del país y contrarrestar el creciente número de ciberataques, que solo en 2023, alcanzaron los 882 millones de intentos. Esta inversión ha permitido la creación de la Dirección de Ciberseguridad, equipos de respuesta a incidentes (SOC-CR y CSIRT-CR), la implementación de sistemas de protección de vanguardia en instituciones gubernamentales y la capacitación de miles de costarricenses en seguridad digital.

LABORATORIO NACIONAL DE CIBERSEGURIDAD MONITOREARÁ DARK Y DEEP WEB

CRHoy - Con el apoyo de la Unión Europea (UE), se establecerá en el país un laboratorio de ciberinteligencia, otro forense informático y una red segura de intercambio de información para las instituciones públicas.
Se trata de un nuevo proyecto que se suma a los esfuerzos para fortalecer las capacidades nacionales para prevenir y responder a ciberataques. Mediante esta cooperación se fortalecerá la capacidad para anticipar ciberataques, pues el laboratorio de ciberinteligencia hará monitoreo de la dark web y la deep web para identificar posibles amenazas de forma proactiva, con lo que se espera tener una respuesta más rápida y efectiva ante los desafíos de los cibercriminales.

DIGI AMERICAS LATAM CISO

INSIGHTS

OCTOBER 24, 2024

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. Las áreas de cooperación previstas son: intercambio de información sobre riesgos relacionados con la seguridad de la información; colaboración en la gestión y respuesta conjunta ante incidentes de seguridad; difusión de buenas prácticas y experiencias en materia de ciberseguridad; intercambio de recursos educativos y formativos; conformación de grupos de trabajos conjuntos especializados en ciberseguridad; y asesoría para la investigación, entre otros temas.

THE CYBERCRIME BILL: A NECESSARY SHIELD FOR BARBADOS' DIGITAL FUTURE

Barbados Today - The rise of cyber threats has made cybersecurity a global priority. In Barbados, the Cybercrime Bill is a crucial step toward protecting the nation from digital crimes. While some Bajans may express concerns about the Bill's implications, it is vital to recognise the daily risks the country faces due to resistance to these protections. Many Bajans are apprehensive about the Cybercrime Bill due to fears about privacy, government overreach, or the potential criminalisation of minor online infractions. These concerns, while understandable, often stem from a limited understanding of how cyber threats evolve and impact both personal and national security.

BDF CYBER UNIT LEADING INVESTIGATION INTO REVENUE AUTHORITY HACK - BARBADOS

Barbados Today - Three weeks after a major data breach at the Barbados Revenue Authority led to personal information and vehicle registration documents being offered for sale online, officials say there's no evidence any of the stolen data was used for fraud or other harmful activities. Minister of Industry, Innovation, Science, and Technology Marsha Caddle sought to downplay the fallout from the breach while announcing a programme to put the public and civil servants on guard for cyber threats.

WHY THE NEW NIST STANDARDS MEAN QUANTUM CRYPTOGRAPHY MAY JUST HAVE COME OF AGE

WEF - Quantum computing creates enormous economic and scientific opportunities, given its ability to significantly boost computing power. However, quantum computing – which employs quantum mechanics to solve some complex computing problems – can also render some of the current encryption algorithms obsolete, posing serious cybersecurity risks. The current state of quantum technology overall is still nascent, but short- and long-term predictions suggest great potential for a technology that could open new opportunities in the cybersecurity area. While quantum computers are still in the development stage, experts expect that quantum computers will have encryption-breaking capabilities within the next decade, threatening the "security and privacy of individuals, organizations and entire nations".

DIGI AMERICAS LATAM CISO

INSIGHTS

OCTOBER 24, 2024

WE MUST REDUCE COMPLEXITY TO ENSURE STRONG CYBERSECURITY. HERE'S WHY

WEF - Complexity has fascinated me throughout my career. From algorithms in computer science to the threat landscape in cybersecurity, complexity and its resulting variance create fascinating challenges. But the reality is complexity is the enemy of security. Fundamentally, complexity in cybersecurity means a lack of visibility. The sheer number of components and point products in many modern networks makes identifying vulnerabilities, let alone remediating them, challenging. Moreover, the infrastructure itself is dynamic (software-defined networking) and without a clear picture of what's happening, building strong structural defences is difficult.

HOW CYBERSECURITY CAN HELP PUSH THE BOUNDARIES OF ENERGY TRANSITION INNOVATION

WEF - Cybersecurity is often seen as preparing for failure. It's also often seen as a concern for digital leaders only. But cybersecurity can have a significant impact right across an organization. Cyberattacks affect market capitalization and research shows cyber-resilient organizations provide 50% more value to their shareholders. Thinking about cybersecurity as loss avoidance and a digital-only issue misses key intangibles that can boost organizational value: trust, reputation, stakeholder confidence and the technical capacity needed to support rapid innovation. Cyber-resilient organizations, on the other hand, are able to continue to meet primary business goals and also even unlock additional value.