DIGI AMERICAS ALLIANCE MEMBERS

CIBERSEGURANÇA DEVE TER AGÊNCIA ESTATAL COM PARCERIA PRIVADA, CONCLUI DEBATE - BRASIL

LN21 - O Fórum Econômico Mundial (WEF, sigla em inglês) identifica a segurança cibernética como um dos 10 principais riscos globais (setor público e setor privado). Os ataques cibernéticos dobraram globalmente desde a pandemia. Os ataques estão se tornando cada vez mais sofisticados. O custo médio de uma violação de dados para uma instituição governamental em 2020 foi de US$ 4,441 milhões (aproxmadamente R$ 24 milhões). O Brasil tem um alto nível de digitalização, mas precisa amadurecer em segurança cibernética. Esses são alguns dos dados apresentados pelos participantes de uma audiência pública sobre os riscos internacionais à segurança digital, promovida pela Subcomissão Permanente de Defesa Cibernética, realizada na terça-feira (9).

R-CIBER APROFUNDA RELAÇÃO DAS TELES COM OPERADORAS DE DATA CENTERS - BRASIL

Teletime - A aprovação do novo Regulamento de Segurança Cibernética Aplicada ao Setor de Telecomunicações (R-Ciber) pela Anatel ampliou o rol de empresas que estão sujeitas, diretamente, ao arcabouço de regras do pacote. Mas a alteração das normas também traz mudanças na forma como as operadoras de telecomunicações se relacionam com fornecedores de processamento de dados e nuvens. Em entrevista ao TELETIME, a sócia da área de direito público e regulação do Veirano Advogados, Beatriz França, chamou atenção para o fato de que, com o novo texto, as fornecedoras de data center e nuvem passarão a ser demandadas pelas operadoras de telecomunicações (dentro das relações contratuais privadas entre elas) a cumprirem regras de cibersegurança da Anatel.

GSI/PR ADERE AO PROGRAMA GLOBAL DE CIBERSEGURANÇA DA AMAZON WEB SERVICES - BRASIL

Gov.br - OGabinete de Segurança Institucional da Presidência da República (GSI/PR) formalizou adesão, por meio da Secretaria de Segurança da Informação e Cibernética, ao Programa Global de Cibersegurança da Amazon Web Services, plataforma internacional que visa melhorar os serviços de segurança cibernética. A parceria permite a troca de conhecimentos, a realização de pesquisas conjuntas e capacitações,além da obtenção de dados sobre os impactos dos incidentes cibernéticos para a sociedade. O evento contou com a participação do Secretário de Segurança da Informação e Cibernética (SSIC)do GSI/PR, Dr. André Molina, do Coordenador-Geral do Centro de Prevenção, Tratamento e Respostas a Incidente Cibernéticos de Governo(CTIR Gov), Coronel Maier, e do Sr. Paulo Cunha, Executivo do Setor Público no Brasil da AWS junto a assessores da SSIC e executivos e assessores da AWS. Foi assinado formalmente o Termo de Adesão, sendo o respectivo Plano de Trabalho aprovado para execução conjunta no Centro de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos de Rede Governo(CTIR Gov).

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 12, 2024

ENTIDADES PROPÕEM POLÍTICA NACIONAL DE CIBERSEGURANÇA EM REUNIÃO COM DEPUTADOS - BRASIL

247 - A reunião realizada nesta segunda-feira (8) entre deputados do Grupo de Trabalho da Reforma Tributária e representantes de importantes entidades, como Consad (Conselho Nacional de Secretários de Estado de Administração), CLP (Centro de Liderança Pública), Ibap (Instituto Brasileiro de Administração Pública) e Conseplan (Conselho Nacional de Secretários de Estado de Planejamento), destacou a necessidade urgente de uma Política Nacional de Defesa e Cibersegurança. O encontro enfatizou a importância estratégica da segurança da informação para garantir a soberania nacional. Fabrício Marques, presidente do Conseplan, sublinhou a relevância do momento: “Esse é um momento decisivo para o futuro do Brasil. A proposta de Reforma Tributária precisa ter clareza sobre a importância estratégica da Segurança da Informação e da Segurança Cibernética para o país”. A segurança cibernética é crucial em um mundo cada vez mais digital, especialmente para um país como o Brasil, que lidera a digitalização de serviços e é um alvo frequente de ataques cibernéticos, disse.

AVANZA FORO NACIONAL DE CIBERSEGURIDAD: HACIA MEJORES POLÍTICAS PÚBLICAS - CHILE

Senado - Como un importante hito fue calificada la segunda reunión del Foro Nacional de Ciberseguridad, iniciativa de innovación en generación de políticas públicas al alero del Senado que cuenta con la participación de expertas y expertos del ámbito público, privado, científico y militar. En la sesión de seguimiento del avance de esta iniciativa, el senador Kenneth Pugh, reconocido precursor de este foro, junto a la senadora Ximena Ordenes (quien por problemas de fuerza mayor no pudo asistir), detalló que ya cuentan con 452 inscritos y otros 81 profesionales se encuentran en proceso de participar en este organismo que permitirá canalizar inquietudes y fomentar la colaboración en el ámbito de la ciberseguridad en Chile.

CIBERCRIMEN: DELITOS CONTRA MENORES Y ACCESO ILÍCITO A REDES SOCIALES CONCENTRAN INVESTIGACIONES DE LA PDI - CHILE

Diario Concepcion - Un llamado de atención realizó la Policía de Investigaciones (PDI), debido al alto número de detenciones, producidas desde el año pasado a la fecha, relacionadas con delitos contra menores de edad, usando el acceso a internet y redes sociales como medio para acceder a niñas, niños y adolescentes. Así lo sostuvo el jefe de la Brigada Investigadora del Cibercrimen en la Región, subprefecto Andrés Contreras, en el contexto del aniversario 91 de la institución. “Desde el año pasado a la fecha, la cifra que llevamos de detenciones por este tipo de delitos está cerca de las 40 detenciones. Nosotros todavía tenemos investigaciones en curso respecto a ese delito”, indicó el oficial.

NIC CHILE REPORTA INCIDENTE EN CUENTAS DE USUARIOS DE CLIENTES

NIC - NIC Chile informa que hemos detectado la ocurrencia de un incidente de ciberseguridad que ha afectado a las cuentas de algunos de nuestros usuarios durante el día 3 de julio de 2024. En esta situación, nuestra evaluación inicial apunta a que un atacante aprovechó la debilidad de algunas contraseñas de cuentas de usuario de nuestros clientes, logrando tener acceso no autorizado a ellas y modificando en algunos casos la información asociada a sus servidores DNS. Continuamos analizando el incidente para establecer un diagnóstico definitivo.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 12, 2024

ITAÚ REPORTA INCIDENTE DE CIBERSEGURIDAD QUE PODRÍA AFECTA A CLIENTES DE RAPPICARD - CHILE

La Tercera - Este jueves Itaú reportó a través un comunicado un incidente de ciberseguridad que podría afectar los datos personales de los clientes de RappiCard de dicho banco. Según transparentó la entidad a sus usuarios, esta exposición sería únicamente para este producto en específico. El banco enfatizó en que el problema reportado sólo implicaría la exposición de datos de identificación y contacto, y descartó por completo que se hayan visto comprometidos datos transaccionales ni credenciales de acceso a la RappiCard.

ECUADOR Y LA UNIÓN EUROPEA REFUERZAN SU COOPERACIÓN EN SEGURIDAD

EEAS - Ecuador y la Unión Europea en Ecuador han dado pasos significativos en su trabajo conjunto para combatir el crimen organizado. A través de una serie de iniciativas recientes, ambos socios buscan fortalecer la cooperación en áreas clave como: la lucha contra el narcotráfico y el crimen organizado, la delincuencia y la ciberseguridad. Muestra de este compromiso es la reciente inauguración de la “Unidad de EUROPOL de la Policía Nacional del Ecuador” cuya apertura responde a la firma de un acuerdo bilateral octubre 2023 para establecer relaciones diplomáticas y policiales. Siendo los puertos europeos, uno de los principales destinos de la droga proveniente de Ecuador, la Unidad podrá disponer de un enlace directo con la Policía Nacional para el intercambio de información y ejecución de operaciones coordinadas con la UE para mejorar la lucha contra la delincuencia organizada transnacional.

COSTA RICA REAFIRMA COMPROMISO CON LA IMPLEMENTACIÓN DE LA TECNOLOGÍA 5G

Summa - Este miércoles el Gobierno de Costa Rica reafirmó su compromiso con la seguridad y la privacidad de los ciudadanos en la implementación de la tecnología 5G, a pesar de enfrentar acciones judiciales que buscan detener el avance de esta importante tecnología. Desde agosto de 2023, el Gobierno ha promovido el decreto ejecutivo N°44196-MSP-MICITT que busca equilibrar los beneficios de la conectividad 5G con las medidas de ciberseguridad necesarias para proteger a empresas y usuarios. Sin embargo, este decreto ha sido objeto de recursos legales por parte de diversas entidades, incluyendo a una empresa fabricante de equipos y al sindicato Frente Interno de Trabajadores del ICE.

SERVICIOS DE CIBERSEGURIDAD EN EL PAÍS CRECEN 13% Y GENERAN $19 MILLONES - COSTA RICA

CRHoy - Los servicios de ciberseguridad en Costa Rica alcanzan un crecimiento del 13% en lo que llevamos del 2024. Este es el dato del reporte de Frost Radar de Frost & Sullivan, que indica el aumento del porcentaje con relación al año pasado, con ingresos de $19 millones. Según Marcelo Ruiz, director consultor de la firma de investigación en el campo de la tecnología y la innovación, Costa Rica es el país con más ataques de ransomware en Centro América, sin embargo, a partir de los ataques masivos del año 2022, ha cobrado mayor conciencia sobre la importancia de la ciberseguridad tanto en el sector privado como público. De acuerdo con el informe, uno de los principales aspectos positivos que se destacan a nivel nacional es que se cuenta con un Plan Nacional de Ciberseguridad con el apoyo de la Organización de Estados Americanos (OEA), adicional de los acuerdos de cooperación técnica con Honduras, Panamá, República Dominicana, Israel y de recursos con Estados Unidos y España.

DIGI AMERICAS LATAM CISO

INSIGHTS

JULY 12, 2024

ACCIONES PARA HACER DE COLOMBIA POTENCIA EN CIBERSEGURIDAD

La República - Trabajar desde las regiones para conectar a Colombia es un propósito del Gobierno. Y si hablamos de ciberseguridad, si no construimos una seguridad digital que inicie en los territorios, no será posible lograr una transformación real. De ahí que alcanzar una verdadera articulación de todos los sectores y áreas de conocimiento sea fundamental para lograr una protección total en el entorno digital.

A UN AÑO DE SU PUESTA EN MARCHA, DESTACAN EL TRABAJO DE LA DIRECCIÓN DE CIBERCRIMEN

Diario de Democracia - Autoridades del Ministerio de Seguridad bonaerense, del poder judicial, jefes policiales y del Municipio de Junín se reunieron en la Dirección de Investigaciones Cibercrimen de la División Región Norte, ubicada en el barrio Villa del Parque, al cumplirse el primer aniversario de su creación y puesta en marcha. Allí se destacó el trabajo de la dependencia y coincidieron en definirla como "fundamental para la investigación de hechos delictivos informáticos" Cabe recordar que Junín ha sido la primera ciudad de la provincia de Buenos Aires en contar con una oficina policial abocada a la investigación de delitos informáticos; la cual fue un resultado de la articulación de acciones impulsadas por el Municipio, las fuerzas policiales y la Justicia para la prevención.

EL CNCS: EL ÓRGANO GUBERNAMENTAL QUE VIGILA EL CIBERESPACIO DOMINICANO

Gob.do - La ciberseguridad y el ciberespacio son términos que continúan siendo utilizados con mucha frecuencia en República Dominica debido al avance y el uso continuo de la tecnología en múltiples facetas de la vida diaria; para el director ejecutivo del Centro Nacional De Ciberseguridad (CNCS), general PN Juan Gabriel Gautreaux Martínez, esos dos enunciados agrupan las medidas y los protocolos que se utilizan para proteger los activos digitales. Al ser invitado al programa MAPTV, Gautreaux Martínez destacó que el CNCS, entidad presidida por el Ministerio de la Presidencia, es el órgano gubernamental responsable de vigilar que esos protocolos y medidas sean cumplidos en el país.

EL CIBERCRIMEN SE REORGANIZA ANTE EL ACOSO POLICIAL

Expansion - Los ciberataques han decaído este año gracias a operaciones policiales de gran envergadura, lo que lleva a los grupos criminales en internet areorganizarse, incluso a lanzar amenazas físicas, según expertos. 2023 fue un año récord, tanto en número de ataques como en la cantidad extorsionada a las víctimas. "En los primeros cuatro meses de 2024, el número de incidentes reportados públicamente relacionados con ransomware (programas de chantaje) ha disminuido en comparación con los primeros cuatro meses de 2023", indicó a la AFP Allan Liska, experto en ciberseguridad de Recorded Future.

THE RISKS OF A LAST-MINUTE CYBERCRIME TREATY PROTOCOL

Global Initiative - One idea now gaining support among countries seeking a broad scope of crimes in the convention (a bloc led by Russia) is to begin a process of drafting a protocol to the convention – a supplementary agreement that would add a list of ‘additional crimes’ to the original treaty – even though the text of the convention itself is not yet final. Drawing comparisons to the negotiation process of the UN Convention against Transnational Organized Crime (UNTOC), the paper highlights crucial differences in political, practical, and legal contexts.

BUSINESSES ARE HARVESTING OUR BIOMETRIC DATA. THE PUBLIC NEEDS ASSURANCES ON SECURITY

The Conversation - Imagine walking through a bustling railway station. You're in a hurry, weaving through the crowd, unaware that cameras are not just watching you but also recognising you. These days, our biometric data is valuable to businesses for security purposes, to enhance customer experience or to improve their own efficiency. Biometrics, are unique physical or behavioural traits, and are part of our everyday lives. Among these, facial recognition is the most common. Facial recognition technology stems from a branch of AI called computer vision and is akin to giving sight to computers. The technology scans images or videos from devices including CCTV cameras and picks out faces.

AI-POWERED SUPER SOLDIERS ARE MORE THAN JUST A PIPE DREAM

Wired - The day is slowly turning into night, and the American special operators are growing concerned. They are deployed to a densely populated urban center in a politically volatile region, and local activity has grown increasingly frenetic in recent days, the roads and markets overflowing with more than the normal bustle of city life. Intelligence suggests the threat level in the city is high, but the specifics are vague, and the team needs to maintain a low profile—a firefight could bring known hostile elements down upon them. To assess potential threats, the Americans decide to take a more cautious approach. Eschewing conspicuous tactical gear in favor of blending in with potential crowds, an operator steps out into the neighborhood's main thoroughfare to see what he can see.

WHITE HOUSE WANTS TO BOOST CYBER FUNDS FOR FISCAL 2026

Cyberscoop - The White House wants federal agencies to ask for more money that would be used to improve the nation's cyber defenses, per a memo sent to agency heads Wednesday. In the document, Office of Management and Budget Director Shalanda Young and National Cyber Director Harry Coker Jr. directed agencies to review and align incoming budget requests to fit the Biden administration's national cyber strategy and implementation plan. The White House's ask fits with its directive that federal agencies move toward fully mature zero-trust architectures. Agencies will submit an updated zero-trust implementation plan to the OMB and ONCD within 120 days following the memo's release, and be on target by the end of fiscal 2026, the memo states.