



# INSIGHTS

MARCH 6, 2025

## DIGI AMERICAS ALLIANCE MEMBERS



## **POLICÍA NACIONAL AVANZA HACIA LA ERA DIGITAL CON LA CREACIÓN DE LA DIRECCIÓN CENTRAL DE TRANSFORMACIÓN DIGITAL - REPÚBLICA DOMINICANA**

Gobierno de la República Dominicana - La Dirección Central de Planificación y Desarrollo (DIPLAN), de la Policía Nacional, presentó ante una comisión de altos oficiales la propuesta para definir los lineamientos operativos de la Dirección Central de Transformación Digital, una nueva dependencia que impulsará la modernización tecnológica de la Policía Nacional.

## **INICIA LA OBLIGACIÓN EN CHILE DE REPORTAR INCIDENTES DE CIBERSEGURIDAD A LA ANCI**

Alerta Geek - Las entidades tienen hasta un máximo de tres horas para informar. Una de las medidas más importantes en torno a la ciberseguridad en Chile ya está activa. Desde inicios de marzo, las empresas y organizaciones que prestan servicios esenciales en Chile están obligadas a reportar incidentes de ciberseguridad a la Agencia Nacional de Ciberseguridad (ANCI).

## **CON LA ACTUALIZACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, EL MINISTERIO TIC FORTALECE LA SEGURIDAD DIGITAL EN LAS ENTIDADES PÚBLICAS DEL PAÍS - COLOMBIA**

MinTIC - Día a día, las entidades públicas del país enfrentan un creciente riesgo de incidentes de seguridad digital. Esta situación llevó al Ministerio TIC a intensificar su compromiso con la protección de los activos informáticos y la garantía de la continuidad en la prestación de servicios a los ciudadanos. Como resultado, y consciente de la vulnerabilidad digital de las instituciones del Estado, la entidad ha desarrollado políticas y estrategias que le apuntan a garantizar el uso seguro y eficiente de las tecnologías de la información y las comunicaciones (TIC).

## **MINISTÉRIO DA JUSTIÇA E FEBRABAN LANÇAM ALIANÇA CONTRA FRAUDE DIGITAL - BRASIL**

E.M.FOCO - Em resposta ao aumento significativo de fraudes bancárias e digitais, o Ministério da Justiça e Segurança Pública do Brasil, em parceria com a Federação Brasileira de Bancos (Febraban), lançou uma iniciativa estratégica. Esta aliança busca reforçar a segurança digital, promovendo ações de prevenção e repressão a crimes cibernéticos. A colaboração entre o governo e o setor bancário visa criar um ambiente digital mais seguro, centralizando canais de denúncia e aprimorando a troca de informações entre as partes envolvidas. A iniciativa é resultado de um acordo técnico firmado anteriormente, com o objetivo de enfrentar os desafios impostos pelas fraudes modernas.

## **BRASIL E REINO UNIDO SE UNEM CONTRA ATAQUES DIGITAIS EM EXERCÍCIO GLOBAL; DEFESA CIBERNÉTICA E SEGURANÇA DIGITAL EM PAUTA**

sociadademilitar - A guerra digital já começou, e o Brasil está na linha de frente! O Comando de Defesa Cibernética (ComDCiber) do Exército Brasileiro participa do Defence Cyber Marvel 4 (DCM4), um dos mais sofisticados exercícios internacionais de guerra cibernética. Coordenado pelo Exército do Reino Unido, o evento, que acontece de 23 a 28 de fevereiro de 2025, tem sede em Seul, na Coreia do Sul. No entanto, a equipe mista de Brasil e Reino Unido presente nesse exercício de defesa atua remotamente a partir do Forte Marechal Rondon, em Brasília-DF.

## **PRIMER MINISTRO INSTA A DESARROLLAR EN CUBA LA IA Y CIBERSEGURIDAD**

Prensa Latina - El primer ministro de Cuba, Manuel Marrero, convocó a impulsar el desarrollo de tecnologías claves como la inteligencia artificial (IA), la ciberseguridad y la robótica, durante el balance del Ministerio de Comunicaciones, informó hoy el diario Granma. Durante la reunión presidida por el mandatario cubano Miguel Díaz-Canel, el jefe de Gobierno exhortó al organismo a elevar la calidad de los servicios, incrementar los ingresos en divisas y se refirió a la necesidad de mantener un control adecuado del comercio electrónico.

## **TSMC INVERTIRÁ MÁS DE 100 MIL MDD EN PLANTAS DE CHIPS EN EE. UU.**

dpl news - Taiwan Semiconductor Manufacturing Company Limited (TSMC), considerado el mayor fabricante de semiconductores del mundo, anunció en conjunto con el presidente de Estados Unidos, Donald Trump, una inversión histórica por 100 mil millones de dólares. Dicha inversión se enfocará en fortalecer su operación de fabricación de semiconductores en Arizona. Y, de acuerdo con la Casa Blanca, se trata de la mayor inversión extranjera directa en la historia de Estados Unidos.

## LA UE PRIORIZA LA CIBERSEGURIDAD ANTE EL AUMENTO DE LOS ATAQUES HÍBRIDOS RUSOS

infobae - La vicepresidenta de la Comisión Europea para la Soberanía Tecnológica, la Seguridad y la Democracia, Hanna Virkkunen, y el ministro polaco de Digitalización, Krzysztof Gawkowski, coincidieron este miércoles en señalar la ciberseguridad como una prioridad fundamental para la Unión Europea (UE) ante el incremento de los ataques híbridos desde Rusia.

## LA IMPORTANCIA DE UNA ALFABETIZACIÓN MEDIÁTICA TEMPRANA EN LA ERA DE LA DESINFORMACIÓN

The Conversation - La creciente propagación de desinformación y contenidos maliciosos, reforzada por el uso de inteligencia artificial (IA), sitúa a los más jóvenes en el centro de la vulnerabilidad frente a discursos de odio y estereotipos discriminatorios. En este escenario, vemos cómo la cultura digital –esa convergencia de lo físico y lo digital– fusiona ambas realidades en una experiencia única e ininterrumpida. Desde edades cada vez más tempranas, las nuevas generaciones acceden a dispositivos móviles y a redes sociales, determinando su visión del mundo.

## COMO PUEDE LA IA AYUDAR A INCREMENTAR LAS CAPACIDADES DE CIBERSEGURIDAD

Forbes - La inteligencia artificial (IA) es uno de los avances tecnológicos más importantes de la era digital. En particular, la IA generativa (GenAI), que gracias a su capacidad de crear textos, imágenes y otros contenidos más realistas, ha pasado de ser considerada una herramienta divertida en línea a convertirse en una parte vital de muchos servicios y aplicaciones de los que dependen las organizaciones. Este cambio en la aplicación se produjo en un momento crucial. Con más personas trabajando de forma remota, las empresas comenzaron a depender de servicios basados en la nube y redes conectadas, incluidos dispositivos de Internet de las cosas (IoT) y equipos industriales. Estas redes se volvieron más complejas y fluidas, lo que hizo que fuera difícil para los sistemas de seguridad existentes y más tradicionales mantenerse al día.

## DHS SAYS CISA WON'T STOP LOOKING AT RUSSIAN CYBER THREATS - USA

Cyberscoop - The Department of Homeland Security said that its Cybersecurity and Infrastructure Security Agency will continue to pay attention to Russian cyber threats, contrary to media reports suggesting the opposite. The Guardian reported last week that a recent CISA memo setting out priorities for the agency didn't list Russia among them, while including Chinese threats and critical infrastructure protection. It further reported that analysts at the agency were verbally told not to follow or report on Russian cyber threats.



# INSIGHTS

MARCH 6, 2025

## THE EVOLVING DYNAMICS OF DDOS ATTACKS

Cyber Magazine - Distributed denial of service attacks levels are such that cybersecurity professionals must explore new methods of defence in order to stay secure. The cybersphere is in a precarious place. The digital frontier is expanding as more companies push for digital transformation, but as the infrastructure does, so does the attack surface. A new wave of Distributed Denial of Service (DDoS) attacks has introduced a significant variable into the cybersecurity equation. Yet as we delve into the current state of DDoS attacks, it becomes clear that this resurgence is not merely a rehashing of old tactics.

## IDENTITY: THE NEW CYBERSECURITY BATTLEGROUND

The Hacker News - The rapid adoption of cloud services, SaaS applications, and the shift to remote work have fundamentally reshaped how enterprises operate. These technological advances have created a world of opportunity but also brought about complexities that pose significant security threats. At the core of these vulnerabilities lies Identity—the gateway to enterprise security and the number one attack vector for bad actors. Explore the importance of modernizing Identity strategies and the benefits of centralizing Identity within your security ecosystem to safeguard your organization from costly breaches while enhancing operational efficiency.

## CYBERSECURITY NEWS: CISA DENIES CLAIMS, RANSOMWARE GROUP CLAIMS ATTACK, LATIN AMERICA'S SECURITY CRISIS

CISO Series - CISA denies claims of deprioritizing Russian threats. CISA is pushing back against reports that it has been directed to stop tracking Russian cyber threats, calling the claims “fake” and a risk to national security. This is an update to a story that first appeared over the weekend, in which The Guardian reported that a memo deprioritizing Russia was issued—an allegation that CISA and DHS officials deny, with one calling the report “garbage.” Meanwhile, The Record, The New York Times, and The Washington Post confirm that U.S. Cyber Command has been ordered to pause offensive cyber operations against Russia while negotiations over the war in Ukraine continue. Lawmakers on both sides are criticizing any shift, warning that it could weaken U.S. defenses against Russian cyber threats.

## HOW DIGITAL TWIN TECHNOLOGY CAN ENHANCE CYBERSECURITY

WEF - For many, the first thing that comes to mind when discussing digital twins is a 3D replica of real-world objects. But in reality there is more to it than that. A digital twin is a digital representation of a physical object, system, or process with synchronized bidirectional interaction with its real-world counterpart. They are primarily categorized into the following types: Component Twin, Product Twin, Process Twin, System Twin.