DIGI AMERICAS LATAM CISO

INSIGHTS

SEPTEMBER 25, 2025

DIGI AMERICAS ALLIANCE MEMBERS

CIBERSEGURIDAD EN REPÚBLICA DOMINICANA: ESTRATEGIA 2030, CIFRAS Y ACCIONES CLAVE PARA BLINDAR EL ENTORNO DIGITAL

Revista Mercado - La ciberseguridad en RD se ha convertido en una prioridad nacional ante el crecimiento acelerado de amenazas digitales que afectan tanto al sector público como privado. En el primer semestre de 2025, República Dominicana fue blanco de más de 233 millones de intentos de ciberataques, con una velocidad de reconocimiento que alcanzó los 36,000 intentos por segundo. Frente a este panorama, el país ha respondido con acciones concretas como la firma de acuerdos interinstitucionales y la implementación de la Estrategia Nacional de Ciberseguridad 2030, la cual contempla más de 50 actividades específicas y busca consolidar un entorno digital seguro, inclusivo y confiable, posicionando a República Dominicana como líder regional en defensa digital.

AGENCIA NACIONAL DE CIBERSEGURIDAD APRUEBA NÓMINA PRELIMINAR DE OPERADORES DE IMPORTANCIA VITAL E INICIA CONSULTA PÚBLICA - CHILE

Carey - El 16 de septiembre de 2025, la Agencia Nacional de Ciberseguridad (ANCI) aprobó la nómina preliminar de Operadores de Importancia Vital (“OIV”) del primer proceso de calificación bajo la Ley N°21.663, Marco de Ciberseguridad. Esta resolución constituye un hito en la implementación del nuevo marco regulatorio, al identificar a los sujetos obligados a cumplir con exigencias reforzadas para la protección de servicios esenciales.

CHILE: SECTOR SALUD PÚBLICA Y PYMES PROVEEDORAS SON LOS MÁS REZAGADOS EN CIBERSEGURIDAD

Diario de Valdivia - Más allá de la normativa, la debilidad está en la protección y prevención proactiva de ataques, además de la ausencia de una estrategia de inversión consistente en ciberseguridad en ambos sectores. La fiscalización y la auto-reportabilidad obligada son parte esencial de la nueva regulación. La vulneración de las plataformas del Ministerio de Salud en 2016 y del Instituto de Salud Pública este año, son ejemplo del necesario fortalecimiento de la ciberseguridad en el sector de salud pública, y también de la pequeña y mediana empresa que lo abastece.

DIGI AMERICAS LATAM CISO

INSIGHTS

SEPTEMBER 25, 2025

“ALTA DEMANDA Y DEPENDENCIA ELÉCTRICA”: LOS DESAFÍOS QUE TIENE CHILE PRODUCTO DEL CONSUMO ENERGÉTICO DE LAS NUEVAS TECNOLOGÍAS - CHILE

TrendTIC - Hoy en día las nuevas tecnologías, la masiva proliferación de dispositivos móviles (IoT) y el gran avance de la IA están aumentando significativamente la dependencia de la generación energética. Más que una alerta, representa una serie de desafíos cruciales. Según la Agencia Internacional de Energía (IEA, por sus siglas en inglés), la demanda mundial de energía creció un 2,2% en 2024, superando el promedio de la última década. Este incremento fue del 4,3% de la demanda de electricidad, impulsado por temperaturas récord, la electrificación y la digitalización. En este último punto, la expansión de los centros de datos cumple un rol fundamental.

CIBERSEGURANÇA NO SETOR ELÉTRICO: COMO PROTEGER O SISTEMA BRASILEIRO DE ATAQUES VIRTUAIS - BRASIL

Cenario Energia - Com a digitalização das redes e o avanço das smart grids, especialistas alertam para os riscos de ataques cibernéticos que podem causar apagões, prejuízos milionários e ameaçar a confiabilidade da energia no Brasil. A transformação digital do setor elétrico trouxe ganhos de eficiência, mas também abriu novas brechas para ataques cibernéticos.

GEOPOLÍTICA DO FUTURO: ESPAÇO SIDERAL E CIBERESPAÇO COMO NOVOS HEARTLANDS - BRASIL

Defesa em Foco - No século XX, o poder foi disputado em terra, mar e ar. Mas no século XXI, a geopolítica ganha novos territórios: o espaço sideral e o ciberespaço. Quem dominar esses domínios poderá influenciar não apenas países, mas todo o sistema internacional. O espaço sideral, antes palco da corrida espacial entre Estados Unidos e União Soviética, tornou-se um domínio estratégico permanente. Hoje, satélites de comunicação, observação e navegação são fundamentais para o funcionamento da economia global, desde transações financeiras até a agricultura de precisão.

MGI PARTICIPA DE EXERCÍCIO DE SEGURANÇA CIBERNÉTICA EM PREPARAÇÃO PARA A COP 30 - BRASIL

Gov.br - O Ministério da Gestão e da Inovação em Serviços Públicos (MGI) participou, na última semana, da 7ª edição do Exercício Guardião Cibernético, considerado o maior do hemisfério sul voltado à defesa cibernética. Este ano, o evento contou com 160 instituições e aconteceu simultaneamente em Brasília (DF) e Belém (PA), que sediará a 30ª Conferência da ONU sobre Mudanças Climáticas (COP30) em novembro de 2025. No Guardião Cibernético são simulados incidentes que comprometam o funcionamento de infraestruturas críticas ou de serviços essenciais, e são desenvolvidos e treinados os protocolos para resposta a esses incidentes e mitigação dos seus efeitos. O exercício desse ano contou ainda o módulo Gabinete Temático - Cabos Submarinos e Domínio Gov.br, em que o MGI atua como um dos coordenadores, simulando possíveis ataques que ameacem a segurança ou a soberania nacional.

DIGI AMERICAS LATAM CISO

INSIGHTS

SEPTEMBER 25, 2025

EE. UU. BUSCA TRAER LA MANUFACTURA DE CHIPS DE "VUELTA A CASA" CON APOYO DE MÉXICO

DPL News - El gobierno de Estados Unidos busca "traer la manufactura de vuelta a casa": actualmente trabaja en ello y necesita que "México desempeñe un papel clave en ese proceso", expuso Mark Johnson, jefe Adjunto de la Misión Comercial de la Embajada de EE. UU. en el país. El encargado de Negocios de la Embajada de EE.UU., Johnson aseguró que el país norteamericano "no tolerará la dependencia de países como China para tecnología crítica", como los semiconductores. En ese sentido, felicitó al gobierno mexicano por los aranceles que impuso recientemente a los países con los que no tiene un acuerdo comercial.

GOBIERNOS LATINOAMERICANOS ENFRENTAN RETOS TECNOLÓGICOS Y DE CIBERSEGURIDAD EN CENTROS DE DATOS PROPIOS: DIGI AMERICAS

DPL News - Los Centros de Datos gubernamentales presentan desafíos, y en América Latina no es la excepción. Digi Americas publicó el informe Los desafíos de los Centros de Datos gubernamentales en la construcción de infraestructuras digitales resilientes, en el que aborda una paradoja en la política de infraestructura digital de América Latina: la creencia de que construir y operar Centros de Datos propios es la mejor manera de proteger la información sensible.

SECRET SERVICE SAYS IT DISMANTLED EXTENSIVE TELECOM THREAT IN NYC AREA - USA

Cyberscoop - he Secret Service said Tuesday that it disrupted a network of electronic devices in the New York City area that posed imminent telecommunications-based threats to U.S. government officials and potentially the United Nations General Assembly meeting currently underway. The range of threats included enabling encrypted communications between threat groups and criminals, or disabling cell towers and conducting denial-of-service attacks to shut down cell communications in the region.

CISA SHARES LESSONS LEARNED FROM AN INCIDENT RESPONSE ENGAGEMENT - USA

CISA - CISA began incident response efforts at a U.S. federal civilian executive branch (FCEB) agency following the detection of potential malicious activity identified through security alerts generated by the agency's endpoint detection and response (EDR) tool. CISA identified three lessons learned from the engagement that illuminate how to effectively mitigate risk, prepare for, and respond to incidents: vulnerabilities were not promptly remediated, the agency did not test or exercise their incident response plan (IRP), and EDR alerts were not continuously reviewed.

HEALTHCARE CYBERSECURITY: THE URGENCY OF NOW

Forbes - Healthcare exists at the intersection of trust and vulnerability. Every medical record, test result, and insurance claim is more than just data on a computer; it represents a person's identity, medical history, and, in many cases, the road to care. For years, I've warned in papers and briefings that the healthcare sector is particularly vulnerable. The most recent figures confirm that warning: healthcare breaches remain among the most common and costly in any business, and the gap between where healthcare security is and where it needs to be is expanding.