GlobalData.

PRIMAVERA 2025

Ciberseguridad en América Latina

PATROCINADO POR

TANIUM

Contenido

Introducción

De acuerdo con Canning House, un centro de estudios sobre América Latina, América Latina se encuentra en una coyuntura clave. La "influencia decreciente" del Oeste debería ofrecer a la región más democrática y diversa del mundo en desarrollo una mayor oportunidad de brillar en el escenario mundial. Las atracciones de la región incluyen un fuerte compromiso con la coexistencia pacífica, el respeto por la integridad territorial, los derechos humanos, las elecciones libres en la mayoría de los países y el medio ambiente. Tiene una abundancia de recursos naturales, muchos de los cuales son fundamentales para la transición energética, y tiene ambiciones de reordenar la arquitectura de seguridad, diplomática y económica del mundo para adaptarse a nuevos poderes. También disfruta de buenas relaciones en África, Medio Oriente y Asia, y disfruta de un poder blando global sustancial, incluido el papel de Brasil en 2025 como presidente del foro de cooperación política y económica del Sur Global de BRICS.

De acuerdo con un blog del Banco Mundial, un informe recientemente publicado de Economía de la ciberseguridad en mercados emergentes destaca cómo la rápida digitalización posterior a la pandemia de América Latina ha superado la capacidad de ciberseguridad de la región. Para 2024, América Latina y el Caribe se habían convertido en la región de más rápido crecimiento del mundo para los incidentes cibernéticos divulgados, con una tasa de crecimiento anual promedio del 25 % en la última década.

Este documento analizará cómo América Latina está comenzando a tomar un mayor control de su panorama de ciberseguridad, incluida la educación de sus usuarios finales, la implementación de una nueva legislación de ciberseguridad en toda la región, y desempeña un papel clave en los movimientos internacionales de ciberseguridad. Todos estos elementos desempeñarán su papel en el desarrollo de la confianza cibernética de América Latina y, en última instancia, en el fomento de su resiliencia cibernética.

HERIBERTO CABRERA

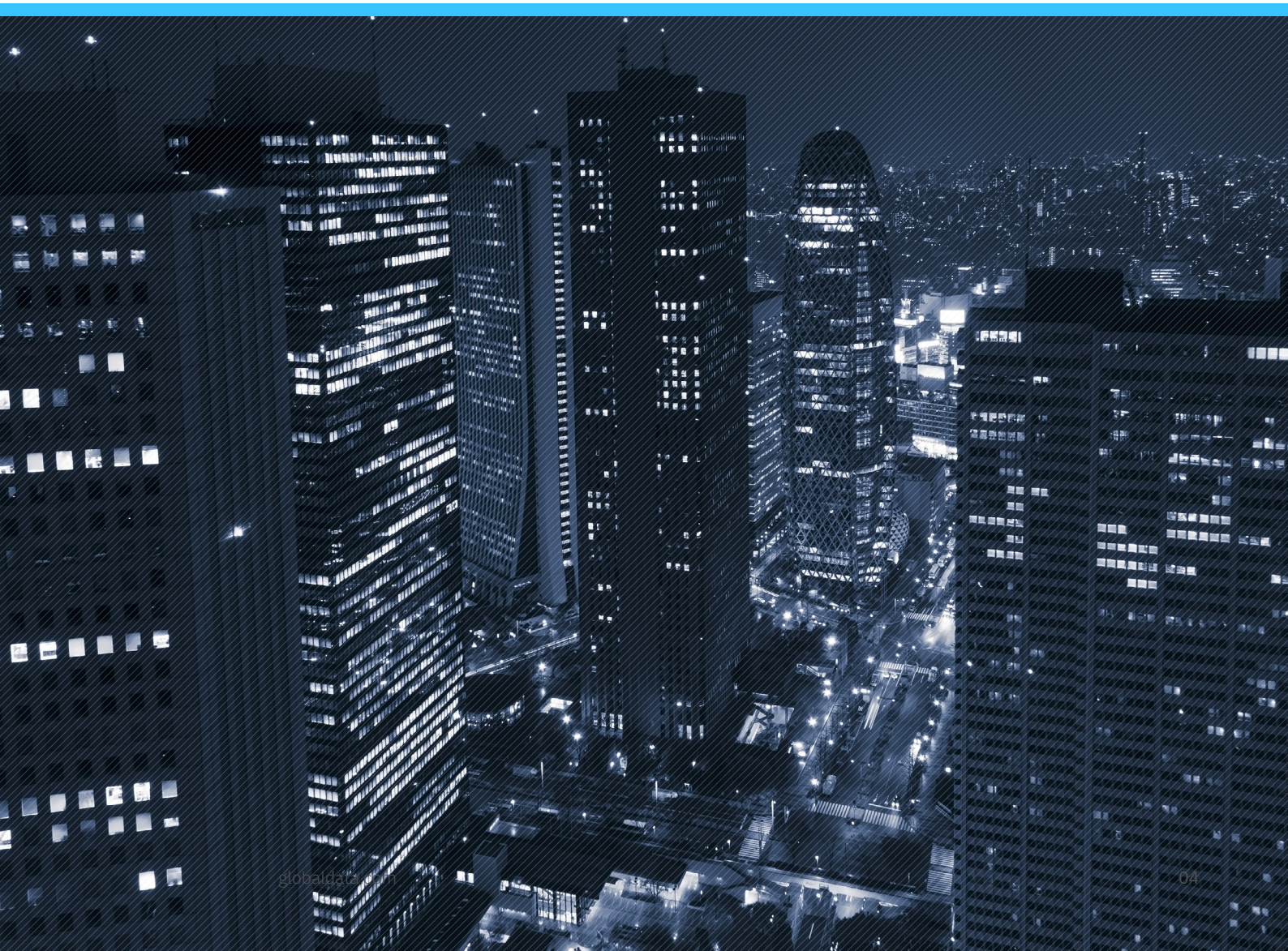
DIRECTOR DE INGENIERÍA DE SOLUCIONES TÉCNICAS, LATAM, TANIUM

"El panorama de la ciberseguridad en América Latina es una combinación compleja de oportunidades y riesgos, donde la transformación digital rápida choca con amenazas y riesgos persistentes. Sin embargo, creo firmemente que establecer una visibilidad fundamental es clave para identificar los riesgos de manera temprana y prevenir los ataques. Este documento ofrece información valiosa sobre los desafíos clave que enfrentan las empresas latinoamericanas y proporciona ejemplos del mundo real de cómo las organizaciones están elevando con éxito su postura de ciberseguridad".

Las implicaciones comerciales de la ciberseguridad para América Latina

Las organizaciones en América Latina están bajo una presión constante de ciberseguridad, con un panorama de riesgo creciente y nuevos desafíos operativos continuos. La frecuencia y gravedad de las filtraciones de datos y los incidentes cibernéticos están aumentando. Los actores de amenazas cibernéticas están intensificando sus esfuerzos y evolucionando sus tácticas para aprovechar las organizaciones no preparadas o poco preparadas. Y eso significa la mayoría de las organizaciones. Las superficies de ataque se están expandiendo porque las fuerzas de trabajo son más remotas, hay un aumento en el uso de dispositivos de Internet de las cosas (Internet of Things, IoT), una mayor prevalencia de inteligencia artificial (IA) en las tecnologías cibernéticas, incluida la IA generativa y riesgos geopolíticos crecientes.

Los países latinoamericanos muestran el mayor porcentaje de uso de ransomware en ataques a organizaciones (79 %) en comparación con el promedio global (53 %). Eso sugiere que los actores de amenazas ven a las organizaciones en América Latina como más susceptibles a los ataques de ransomware en comparación con el resto del mundo, y así las atacan más ampliamente. En términos de filtraciones de datos, los hallazgos del Informe de investigaciones de filtraciones de datos 2023 de Verizon muestran que “la intrusión de sistemas, la ingeniería social y los ataques básicos a aplicaciones web representan el 94 % de las filtraciones” en América Latina. Según el Informe de Ciberseguridad 2023 del CISO de América Latina, el 71 % de los líderes de ciberseguridad encuestados dijeron que los ataques cibernéticos a sus organizaciones aumentaron con respecto al año anterior. Ese desafiante panorama de ataques cibernéticos explica por qué América Latina necesita aumentar su gasto en seguridad.



América Latina está a la altura de los desafíos de ciberseguridad que enfrenta

Brasil se ha convertido en un actor clave en el mercado global en el sector de la ciberseguridad. Ha tenido que hacerlo, porque un aumento en las amenazas digitales, debido al crecimiento de los servicios en línea en el país, junto con una creciente digitalización de los servicios, ha llevado a una necesidad de inversiones más sólidas en ciberseguridad. Según una encuesta, los ataques cibernéticos crecieron alrededor del 70 % en Brasil en un año. La necesidad de una mayor inversión en ciberseguridad, a su vez, ha aumentado la demanda de profesionales de ciberseguridad más calificados, así como la necesidad de desarrollar soluciones más innovadoras.

A pesar de la creciente cantidad de ataques, el progreso de Brasil en el desarrollo de su industria de ciberseguridad ha llevado a que LinkedIn Economic Graph la designe como la tercera posición global en el crecimiento del sector de ciberseguridad. La clasificación se basa en el aumento significativo en la cantidad de vacantes y profesionales cibernéticos especializados en el sector, así como en la importancia de la protección cibernética para la continuidad de los servicios y la seguridad comercial.

La región de América Latina se ha convertido en un imán para los ataques cibernéticos. América Latina actualmente recibe más de 1600 ciberataques por segundo; además del crecimiento de los ciberataques en Brasil, México representó más de la mitad de todas las amenazas cibernéticas informadas en América Latina en la primera mitad de 2024.

América Latina es una de las áreas menos preparadas del mundo para los ataques cibernéticos, según un index compilado por las Naciones Unidas. Se han sugerido varias razones para los desafíos de ciberseguridad de la región. Uno de los problemas proviene de lo que podría considerarse un movimiento definitivo hacia un entorno digital en línea como resultado de la pandemia de Covid-19, donde América Latina es testigo de una notable innovación en áreas como la tecnología financiera y el comercio electrónico.

El problema fue que no se siguieron los esfuerzos e inversiones relacionados y necesarios para mantener seguros los sistemas digitales, por lo que han faltado medidas de ciberseguridad eficaces.

Según Louise Marie Hurel, fundadora de la Red Latinoamericana de Investigación de Ciberseguridad, *"el espíritu emprendedor e innovador de América Latina no va acompañado de una preocupación por la seguridad"*, según se informó en Americas Quarterly.

Una de las primeras señales de advertencia fue un gran ataque de ransomware que afectó a Costa Rica en abril de 2022. El ataque afectó las exportaciones y expuso gigabytes de información confidencial en línea. En retrospectiva, era una señal de advertencia, una llamada de atención para toda la región de América Latina. Algunas naciones respondieron. Chile, en particular, lo hizo. Y algunos países han comenzado a colocar protecciones. Pero la luz roja de advertencia aún no ha sido atendida por todos.

Uno de los problemas es la falta de educación sobre el tema, que está relacionado con la ingenuidad digital. Y América Latina no es única que tiene ese problema. Según un estudio de IBM, el 95 % de todos los incidentes de ciberseguridad comienzan con un error humano. Un ataque de phishing exitoso es aquel que hace que alguien haga clic en un video o una oferta inmejorable a la que no puede resistirse y luego instala malware que invade los sistemas de una empresa. Una filtración a menudo permanecerá sin ser detectada hasta que comience el ransomware o hasta que los datos de la empresa aparezcan para la venta en la web oscura.

Esto es lo que le sucedió a toda la población argentina en 2021 después de que un pirata informático anónimo supuestamente filtrara la totalidad del Registro Nacional de Personas de Argentina, ofreciendo información selecta para la venta en un foro de web oscura. De manera similar, los residentes de Medellín en Colombia sufrieron la peor parte de las consecuencias después de que una empresa de servicios públicos, Empresas Públicas de Medellín (EPM), sufriera un ataque de ransomware en diciembre de 2022 llevado a cabo por el grupo BlackCat/ALPHV, que interrumpió las operaciones de la empresa.

Esta falta de concientización pública, junto con la legislación cibernética de América Latina que aún está madurando, hace que los equipos de seguridad de TI tengan la tarea de reparar los daños.

En la siguiente página se encuentran solo algunas instantáneas de toda América Latina en 2024, que demuestran cómo las organizaciones latinoamericanas han estado sufriendo de un asedio de incidentes de ciberseguridad.

Lo que muestran estos ataques es que en toda la región de América Latina, las autoridades necesitan reforzar la legislación sobre ciberseguridad. Al igual que en Europa, donde una serie de ciberataques condujeron a la Ley de Cibersolidaridad de la UE, una fuga de datos en Chile condujo a una acción inmediata para abordar la situación. Chile promulgó una Ley Marco de Infraestructura de Información Crítica y Ciberseguridad integral para mejorar el panorama de seguridad digital del país. La nueva ley estableció la Agencia Nacional de Ciberseguridad (ANCI), que tendrá poderes regulatorios y de ejecución sobre entidades públicas y privadas, lo que garantiza una respuesta coordinada a las amenazas cibernéticas.

El desafío actual para otros países de América Latina es seguir el liderazgo de Chile y promulgar leyes similares para reforzar los propios panoramas de seguridad digital de los países. Ese es especialmente el caso de Brasil, México y Colombia.

Otra nota positiva frente a la escalada de los riesgos de ransomware y la necesidad de una mayor seguridad de los datos es que los funcionarios del gobierno reconocen la importancia de fortalecer la ciberseguridad en los sectores público y privado. Una forma de cerrar las brechas en la preparación y respuesta cibernéticas es avanzar hacia la creación de una cultura ciberresiliente desde cero. Una herramienta útil aquí es el Marco de Ciberseguridad (Cybersecurity Framework, CSF) 2.0 del Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, NIST) de los EE. UU., que puede adaptarse para satisfacer las necesidades locales.

2024: Un año de ciberataques

ENERO

El proveedor de Internet más grande de Paraguay, **Tigo**, fue víctima de un ataque de ransomware que comprometió su centro de datos y afectó a más de 300 empresas. El grupo de ransomware Black Hunt encriptó más de 330 servidores y comprometió copias de seguridad, páginas web, correos electrónicos y almacenamiento en la nube.

ABRIL

El grupo de alimentos mexicano **Grupo Bimbo** sufrió un ataque cibernético que interrumpió las operaciones de la cadena de suministro y expuso datos confidenciales de la compañía, lo que requirió protocolos de emergencia para restaurar las operaciones.

JUNIO

La compañía mexicana de telecomunicaciones **Claro** sufrió acceso no autorizado que comprometió millones de registros de clientes, destacando vulnerabilidades considerables en los registros de seguridad de telecomunicaciones.

JULIO

Un ataque a varios **sitios web del gobierno mexicano** llevó a interrupciones temporales y a la desfiguración del sitio web por parte de grupos hacktivistas.

Una filtración masiva de datos en Chile salió a la luz. La fuga de datos afectó a más de 10 millones de personas, exponiendo información personal confidencial y planteando inquietudes sobre la infraestructura de protección de datos del país. La filtración se remonta a una base de datos mal protegida, lo que permitió el acceso no autorizado a millones de registros personales.

AGOSTO

El portal del gobierno estatal de **Alagoas** en Brasil fue objeto de un ataque cibernético, que alteró el acceso a los servicios y datos esenciales durante varios días. El ataque se atribuyó a un grupo enfocado en instituciones gubernamentales.

La **Prefeitura de Ponta Grossa** en Brasil fue golpeada por un ataque de ransomware en los sistemas administrativos de la ciudad, lo que llevó a la suspensión de varios servicios públicos. Los atacantes exigieron un rescate en criptomoneda.

El **Instituto Mexicano del Seguro Social** (IMSS) fue golpeado por un ataque de ransomware que interrumpió los servicios y amenazó con la divulgación de datos confidenciales de los pacientes, a menos que se pagara un rescate.

SEPTIEMBRE

Empresas Públicas de Medellín (EPM) en Colombia fue víctima de una intrusión cibernética que golpeó los sistemas operativos, causando interrupciones en el suministro de electricidad y agua en todo Medellín.

El **Hospital das Clínicas**, São Paulo, Brasil, sufrió un ataque de ransomware que encriptó los registros de los pacientes, interrumpiendo los servicios y planteando inquietudes sobre la seguridad de los datos de atención médica.

DICIEMBRE

El proveedor de energía estatal de Costa Rica, **Refinadora Costarricense de Petróleo**, conocido como RECOPE, sufrió un ataque de ransomware que requirió un cambio en las operaciones manuales y una llamada a expertos estadounidenses para obtener ayuda.

Gasto de América Latina en ciberseguridad

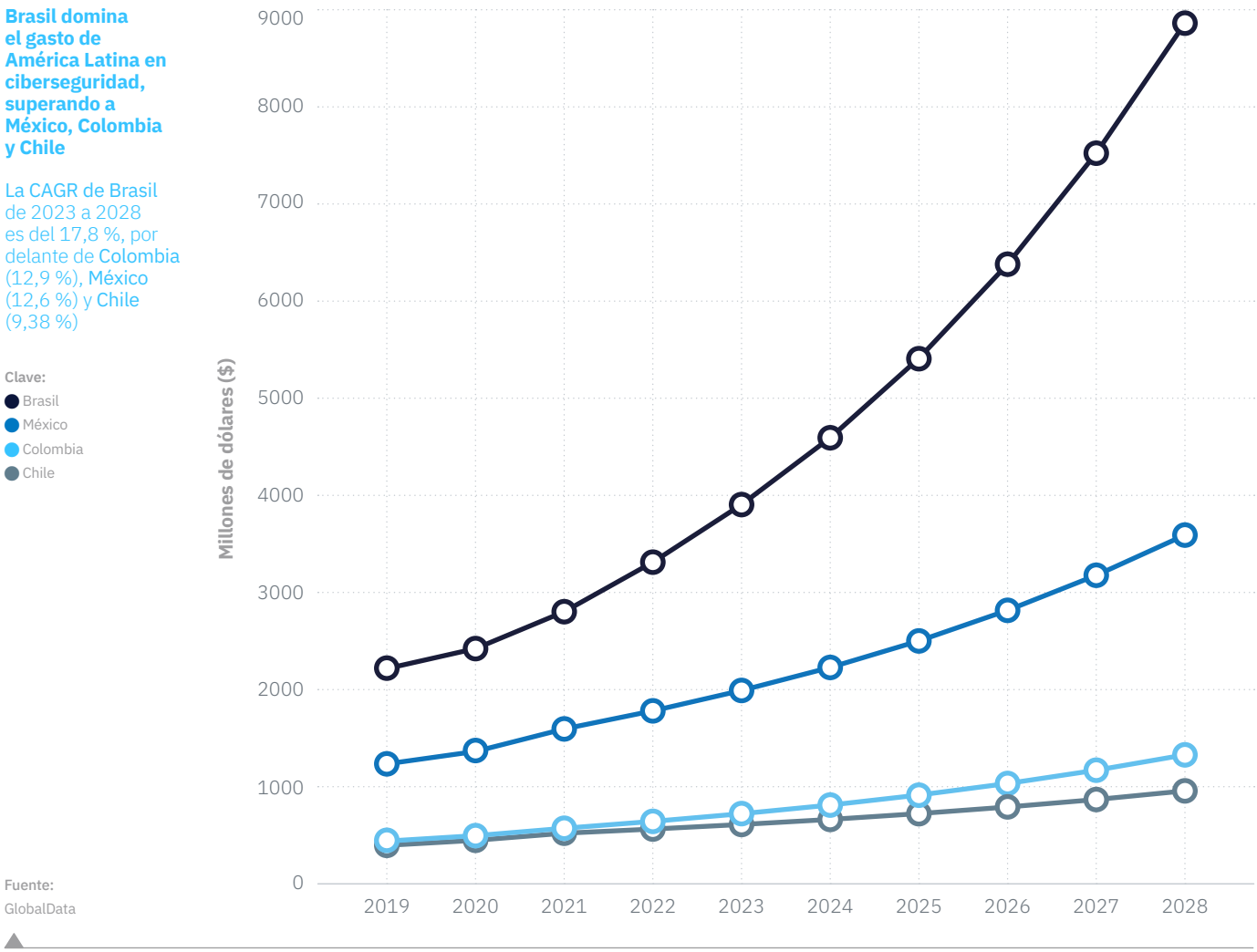
Brasil tiene cómodamente el mayor nivel de gasto en ciberseguridad en América Latina. El país gastará alrededor de $9 mil millones en ciberseguridad en 2028. México gastará $3600 millones, Colombia $1300 millones y Chile alrededor de $1000 millones. El resto de América del Sur y Central juntas casi coinciden con el gasto de México.

El mayor crecimiento en el gasto en ciberseguridad para los países de América Latina, en particular Brasil, México, Colombia y Chile, es en seguridad de red, que tiene una tasa de crecimiento anual compuesta entre 2023 y 2028 del 21,3 %. El siguiente producto o servicio de ciberseguridad más importante es la seguridad web, con una CAGR del 19,8 % durante el mismo período de tiempo. Otras tasas de crecimiento notables son para la prevención del fraude y la seguridad transaccional (19,3 %) y la seguridad de las aplicaciones (19,2 %).

El mayor gasto es en servicios de seguridad administrados, que tienen una CAGR del 15 %. Otras tasas de CAGR notables son el filtrado de contenido y los dispositivos antispam (15,9 %), el monitoreo de la red y el control de acceso (15,5 %), la autenticación multifactor (12,3 %) y la seguridad de endpoint (12,1 %).

Brasil domina el gasto de América Latina en ciberseguridad, superando a México, Colombia y Chile

La CAGR de Brasil de 2023 a 2028 es del 17,8 %, por delante de Colombia (12,9 %), México (12,6 %) y Chile (9,38 %)

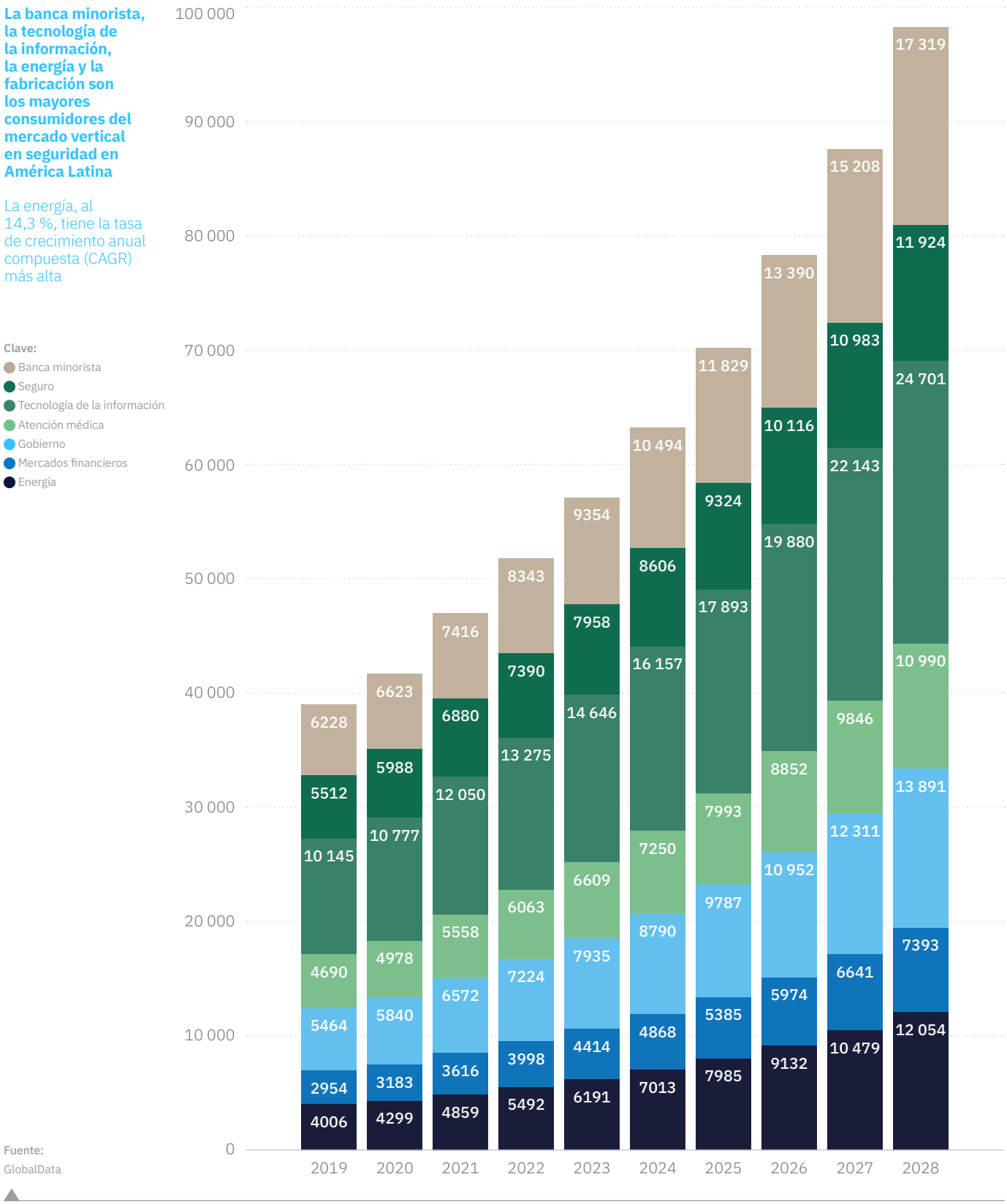


Fuente: GlobalData

El siguiente cuadro muestra el desglose del gasto en seguridad por vertical. La vertical que se presenta es energía, atención médica, fabricación, mercados financieros, gobierno, tecnología de la información, seguros y banca minorista. La banca minorista representa el mayor gasto en seguridad, seguido de tecnología de la información, fabricación y energía.

La banca minorista, la tecnología de la información, la energía y la fabricación son los mayores consumidores del mercado vertical en seguridad en América Latina

La energía, al 14,3 %, tiene la tasa de crecimiento anual compuesta (CAGR) más alta

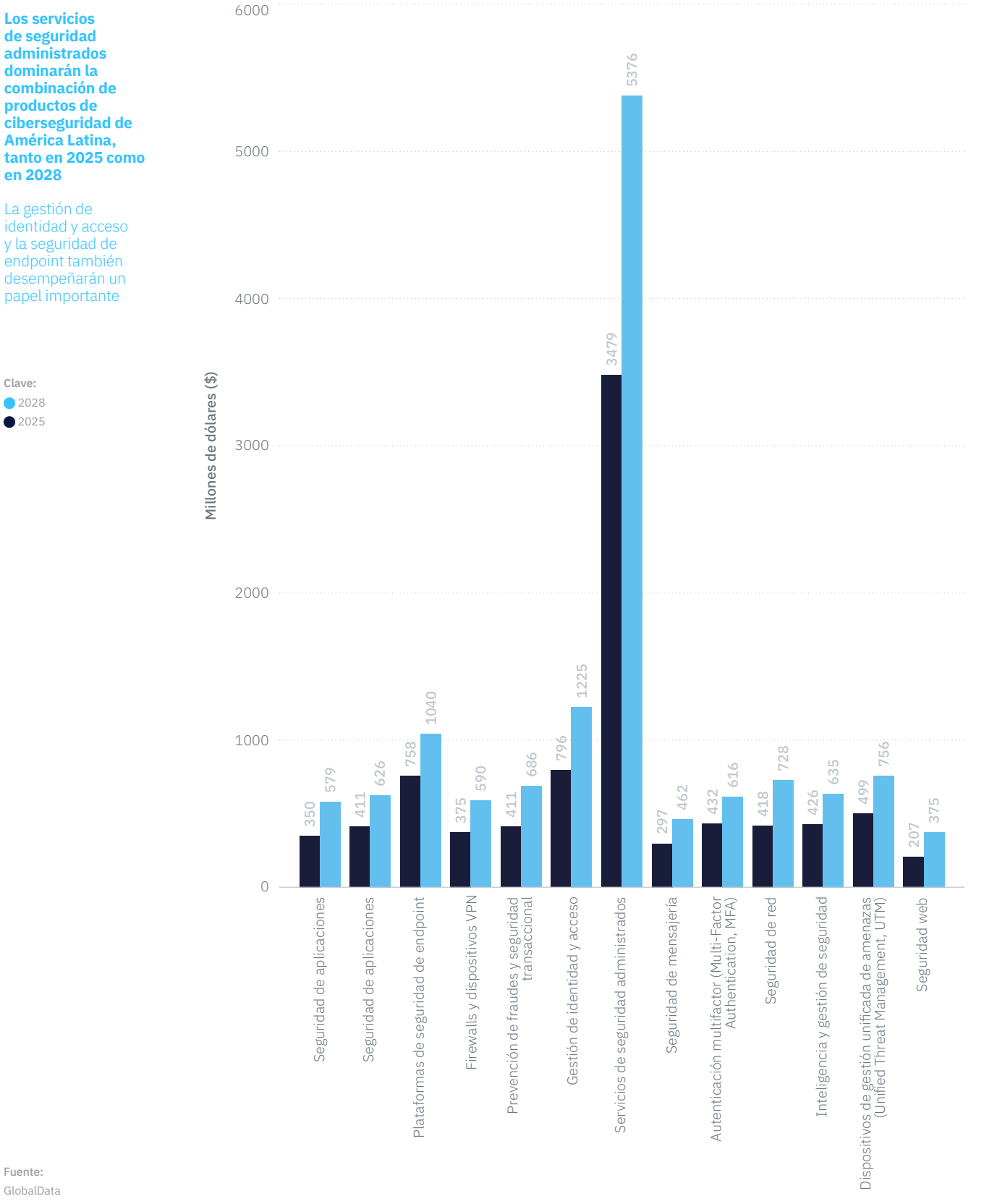


Fuente:
GlobalData

El siguiente cuadro detalla los gastos en ciberseguridad de América Latina para 2025 y 2028 por producto. Las áreas de productos con la tasa de crecimiento anual compuesta más sólida (de 2023 a 2028) son seguridad de aplicaciones (20,43 %), prevención de fraudes y seguridad transaccional (20,45 %), seguridad web (21,04 %) y seguridad de red (22,68 %).

Los servicios de seguridad administrados dominarán la combinación de productos de ciberseguridad de América Latina, tanto en 2025 como en 2028

La gestión de identidad y acceso y la seguridad de endpoint también desempeñarán un papel importante



Fuente:
GlobalData

Cumplimiento y regulación

En su Perspectiva de Ciberseguridad Global 2024, el Foro Económico Mundial (World Economic Forum, WEF) hizo referencia a la "inequidad cibernética" entre ciertas geografías como un problema preocupante, describiendo la baja cantidad de organizaciones ciber resilientes autoinformadas en América Latina y África (en comparación con las mayores cantidades en América del Norte y Europa) como una brecha que "no es sorprendente... tiende a reflejar otros indicadores de desarrollo global".

En el centro de estos problemas en América Latina se encuentra la falta de cumplimiento y regulación eficaces de ciberseguridad. Pero las cosas están comenzando a cambiar. Chile promulgó una Ley Marco de Infraestructura de Información Crítica y Ciberseguridad integral para mejorar el panorama de seguridad digital del país. Y ahora otros países también siguen el ejemplo.

BRASIL

La ciberseguridad en Brasil vio un hito regulatorio significativo con la creación de la Política Nacional de Ciberseguridad a fines de 2023.

La Política Nacional de Ciberseguridad, conocida como PNCiber, tiene como objetivo mejorar la ciberseguridad nacional y alinearla con las prácticas recomendadas internacionales. El lanzamiento de PNCiber estuvo acompañado por la creación del Comité Nacional de Ciberseguridad (CNCiber), un importante desarrollo de monitoreo diseñado para supervisar la implementación y evolución de la política, así como para evaluarla y proponerle actualizaciones.

El PNCiber se creó para guiar las actividades de ciberseguridad en el país. Los principios de PNCiber incluyen la soberanía nacional, la garantía de derechos fundamentales, la prevención de ataques cibernéticos, la resiliencia a incidentes cibernéticos, la educación y el desarrollo tecnológico en ciberseguridad, la cooperación entre entidades públicas y privadas, y la cooperación técnica internacional. El lanzamiento de PNCiber demuestra la creciente atención del gobierno a la ciberseguridad y allana el camino para el desarrollo de una cultura de seguridad digital en el país.

De manera similar, la Política Nacional de Ciberseguridad es un hito importante en la protección de la infraestructura digital de Brasil y requerirá colaboración y adaptación continuas a los cambios en el panorama de las amenazas cibernéticas para lograr su pleno potencial de seguridad y privacidad de datos.

MÉXICO

Según una estimación, México tiene la tasa más alta de delitos cibernéticos en América Latina.

Esa evaluación se basa en el tamaño de su economía (la decimoquinta más grande del mundo) y el grado de penetración de Internet en el país (que se sitúa en 83,2 %). México también representó el segundo porcentaje más alto (17 %) de anuncios en línea relacionados con el robo de datos de ransomware en América Latina.

Crear una Estrategia Nacional de Ciberseguridad es un desarrollo positivo para intentar prevenir los ataques cibernéticos. Pero no es una garantía de éxito. La Estrategia Nacional de Ciberseguridad (ENCS) de México, publicada en 2017, ha sufrido una falta de acción efectiva. Y sin embargo, la ENCS aún ofrece un posible punto de partida para lo que se debe hacer para hacer que México sea más resistente a la cibernética.

México se tomó su tiempo para adoptar una ley nacional de ciberseguridad. En cambio, las disposiciones legales sobre ciberseguridad se extendieron a través de leyes en diferentes sectores, como finanzas, telecomunicaciones, mano de obra, protección al consumidor y propiedad intelectual. No fue hasta abril de 2023 que el Congreso Mexicano finalmente presentó un proyecto de ley nacional de ciberseguridad.

Sus disposiciones más importantes incluyen: el desarrollo de protecciones legales específicas para los derechos digitales (por ejemplo, inclusión digital, neutralidad neta y protección del consumidor en línea); la exigencia de que las empresas privadas colaboren con el gobierno para abordar asuntos de ciberseguridad; la creación de una Agencia Nacional de Ciberseguridad controlada por ejecutivos para coordinar los esfuerzos de ciberseguridad y la implementación de contramedidas para combatir la actividad cibernética maliciosa.

COLOMBIA

En 2022, el gobierno colombiano emitió una legislación, Decreto 338, que estableció pautas generales para el gobierno de la seguridad digital, con las que buscó combinar y fomentar el desarrollo legal, los avances técnicos, así como el conocimiento estatal y privado para fortalecer la ciberseguridad del país.

Este decreto fortaleció la línea de trabajo de la seguridad digital en Colombia, que es necesaria para la protección de la infraestructura nacional e industrial crítica que está en el extremo receptor de ataques de malware y ransomware a nivel mundial.

El Decreto 338 compromete al Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia a aumentar el inventario de infraestructuras críticas cibernéticas públicas nacionales y servicios esenciales en el ciberespacio, actualizándolas cada dos años. La legislación también prometió la creación de equipos sectoriales de respuesta ante incidentes de seguridad informática (Computer Security Incident & Response Teams, CSIRT), así como una plataforma nacional para la notificación y monitoreo de incidentes de seguridad digital, un espacio que servirá para la notificación y gestión de incidentes de ciberseguridad.

En un resumen de la economía digital de Colombia, publicado en septiembre de 2024, la Administración de Comercio Internacional, parte del Departamento de Comercio de los EE. UU., señaló que el Decreto 338 mejoraría la seguridad digital, pero agregó que el cumplimiento puede ser exigente, particularmente para las empresas más pequeñas que necesitan más recursos y experiencia.

CHILE

La ley de ciberseguridad de Chile es la estrella de oro para América Latina. Chile se movió hacia un panorama cibernético más resiliente para sus ciudadanos y la región de América Latina el 26 de marzo de 2024, cuando promulgó la nueva Ley Marco de Infraestructura de Información Crítica y Ciberseguridad.

El nuevo marco y las regulaciones que crea permiten a Chile fortalecer su seguridad digital.

Una parte clave es la nueva Agencia Nacional de Ciberseguridad (ANCI) de Chile, que está diseñada junto a las líneas de agencias de ciberseguridad en otros países, como la Agencia de Seguridad de Infraestructura y Ciberseguridad (Cybersecurity and Infrastructure Security Agency, CISA) de los EE. UU. y el Centro Nacional de Seguridad Cibernética (National Cyber Security Centre UK, NCSC-UK) del Reino Unido. ANCI tendrá facultades de asesoramiento, regulación, supervisión y sanciones, tanto para organizaciones públicas como privadas.

La nueva ley de Chile también establece “servicios esenciales”, que deben cumplir con los requisitos de ANCI. Estos servicios esenciales incluyen infraestructura crítica, banca, transporte, el sector energético, telecomunicaciones, atención médica, la industria farmacéutica y tecnología de la información. Las empresas de estos sectores deberán tener planes de ciberseguridad, ser revisados regularmente y realizar ejercicios de simulación de ciberseguridad.

La ley establece requisitos mínimos que las entidades cubiertas deben implementar para prevenir y mitigar incidentes de ciberseguridad, y también incluye requisitos de respuesta ante incidentes para ayudar a las agencias y empresas a responder mejor a los incidentes de ciberseguridad. También exige la presentación de informes requeridos para que el gobierno pueda hacer un seguimiento de los incidentes y coordinar respuestas adicionales si es necesario.

El panorama cambiante de las amenazas cibernéticas en América Latina

En 2024, Brasil ocupó la presidencia del grupo del G20 de las veinte economías más grandes del mundo. El año culminó con la cumbre del G20 en Río de Janeiro, que analizó los desafíos más apremiantes del mundo. Uno podría argumentar que la ciberseguridad debería haberse agregado a la lista de temas analizados junto con la inclusión social, la reforma de gobierno global y las transiciones energéticas porque la creciente influencia internacional de Brasil lo está convirtiendo en un objetivo para los ciberdelincuentes.

Cuanto más grande sea el perfil creciente de Brasil en el escenario mundial, más riesgo correrá, tanto de amenazas cibernéticas del extranjero como de un ecosistema criminal próspero desde adentro. Brasil es ahora el quinto país más poblado del mundo y, en 2025, asumirá el liderazgo del foro intergubernamental BRICS ahora ampliado de países en desarrollo, que Brasil fundó originalmente con Rusia, India y China, y más adelante Sudáfrica.

Sin embargo, hay algunas clasificaciones que Brasil tal vez preferiría perder. Por ejemplo, Brasil es el segundo país más objetivo del grupo de ransomware como servicio RansomHub, basado en listados en su sitio de fugas, según una publicación de blog del Grupo de Análisis de Amenazas de Google.

“A medida que crece la influencia de Brasil, también crece su huella digital, lo que la convierte en un objetivo cada vez más atractivo para las amenazas cibernéticas originadas tanto por actores nacionales como globales”, dice la publicación del blog. “Al mismo tiempo, el panorama de amenazas en Brasil está conformado por un mercado cibercriminal nacional”. Esos ciberdelincuentes incluyen principalmente hackers de habla portuguesa brasileños, que están llevando a cabo tomas de cuentas, fraude de tarjetas, exfiltración de datos financieros mediante malware bancario y ransomware en toda América Latina.

No solo Brasil está viendo un interés cibernético no deseado. En México, Fresnillo, el productor principal de plata más grande del mundo y el productor de oro más grande de México, admitió en julio de 2024 que los atacantes obtuvieron acceso a los datos almacenados en sus sistemas durante un ataque cibernético reciente. La compañía minera reveló en una presentación ante la Bolsa de Valores de Londres que fue “el objeto de un incidente de seguridad cibernética que ha dado lugar a un acceso no autorizado a ciertos sistemas y datos de TI”.

Al descubrir el ataque, Fresnillo dijo que había iniciado medidas de respuesta para contener la filtración, y sus expertos en TI están investigando y evaluando el impacto del incidente en coordinación con especialistas forenses externos.

Lo siguiente resume el estado de las tendencias de ciberseguridad en toda América Latina.

Una imagen desafiante

Se informan más de 1600 ciberataques en América Latina por segundo, lo que hace que los ciberataques sean uno de los problemas de seguridad de más rápido crecimiento en el área. Al mismo tiempo, los daños económicos de los ciberataques superan el 1 % de algunos países en el PIB de América y aumentan al 6 % si se atacan infraestructuras críticas. El volumen y la sofisticación de los ciberataques registrados en América Latina están en aumento, con organizaciones en países como Brasil y México clasificadas entre los principales objetivos globales para los ciberdelincuentes. Ambos países son particularmente atractivos para los hackers debido a la combinación de la región de una mayor digitalización y la inmadurez generalizada de la ciberseguridad.

Inquietudes sobre la geopolítica

Un panorama geopolítico complejo y a menudo cambiante tiene las mismas consecuencias graves para la ciberseguridad dentro de América Latina que en el resto del mundo. Ninguna región puede darse el lujo de ser complaciente con las amenazas cibernéticas de delincuentes, "hacktivistas" u estados hostiles, y menos aún América Latina. Se espera que los países en desarrollo, incluidos los de América Latina, respondan eficazmente a las amenazas cibernéticas, pero carecen de los factores estructurales para hacerlo. Las disparidades en el desarrollo en toda la región significan que las necesidades de ciberseguridad de diferentes países pueden variar significativamente. Las capacidades de defensa cibernética de Brasil están generalmente bien consideradas, aunque aún no son tan sofisticadas como las de los estados occidentales o tan bien organizadas como las de Chile. Mientras tanto, cuando se trata de asuntos geopolíticos globales, Brasil no se asocia completamente con los estados de América del Norte y Europa, pero ha participado cautelosamente en la cooperación cibernética con China y Rusia y ha apoyado algunas de sus iniciativas. El papel de Brasil en el gobierno cibernético y su postura sobre las normas cibernéticas internacionales se verán forjados por su interés estratégico en mantener una posición independiente e influyente en los asuntos globales.

Brecha de habilidades y brecha de responsabilidad

Una geopolítica compleja y a menudo cambiante, existe una brecha sustancial en las habilidades de ciberseguridad en todo el mundo, con una demanda que supera significativamente la oferta. De acuerdo con Job Analytics de GlobalData, la cantidad promedio de trabajos abiertos de ciberseguridad por mes a nivel mundial en 2022 fue de poco menos de 180 000. La cantidad promedio de empleos cerrados en ciberseguridad por mes fue significativamente menor a un poco más de 60 000.

Una encuesta de 2022 realizada por el Foro Económico Mundial descubrió que el 59 % de las empresas tendría dificultades para responder a un ciberataque debido a la escasez de talentos y habilidades de ciberseguridad. Los atacantes cibernéticos explotan las brechas de habilidades en las organizaciones para extraer información. La falta general de personal de ciberseguridad en todas partes agrava el problema.

En América Latina, existe una brecha estimada en la fuerza laboral de ciberseguridad en México y Brasil de casi 516 000 personas. Esto significa que la escasez de personal de ciberseguridad en México es la segunda en comparación con la escasez en los Estados Unidos. Sin embargo, hay un crecimiento notable en los trabajos cibernéticos. La tasa de crecimiento para los profesionales cibernéticos en México en 2024 fue del 64,6 %, frente a una tasa de crecimiento del 27,3 % para otras profesiones. La tasa de crecimiento de Chile fue del 28,7 %, frente a una tasa de crecimiento para otras profesiones del 2,9 %.

La IA impulsa los miedos de la ingeniería social

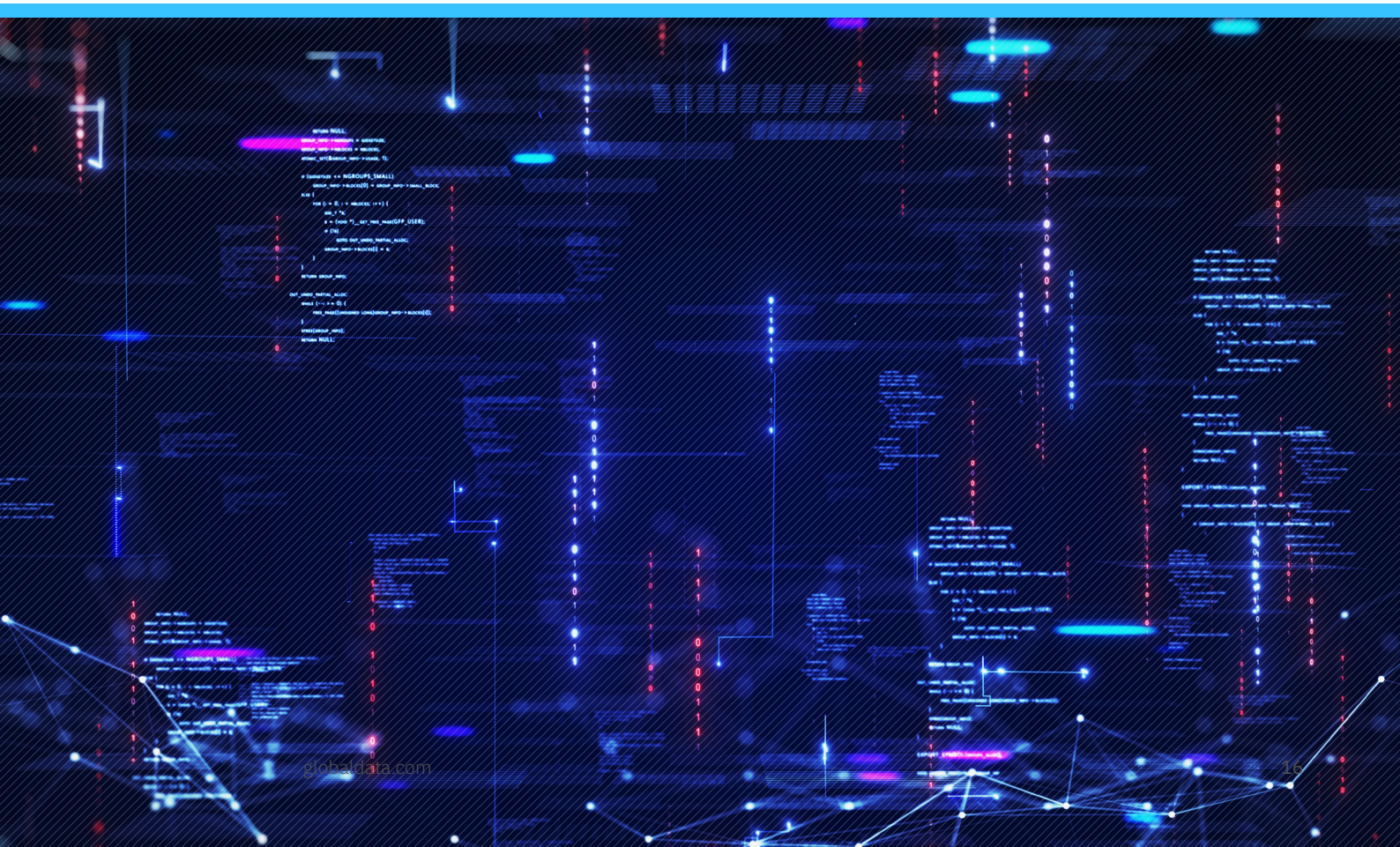
Si bien otras tecnologías como las soluciones en la nube se han vuelto más comunes en la región en los últimos años, los problemas similares en torno a las personas, los procesos y la tecnología continúan, por ejemplo, hasta el 41 % de las organizaciones en América Latina han estado luchando para cubrir las funciones de seguridad en la nube desde 2022, la IA se ha convertido rápidamente en el nuevo vector de defensa y ataque durante el último año. La IA generativa proporcionará a los perpetradores nuevas herramientas poderosas para llevar a cabo ingeniería social convincente a escala. Los modelos avanzados de lenguaje natural como ChatGPT permitirán a los atacantes enviar correos electrónicos y mensajes de texto personalizados y dirigidos que parecen notablemente humanos. Los intentos de manipular al personal a través de las redes sociales están listos para aumentar. A medida que esta tecnología avanza, es posible que veamos que los grupos de amenazas utilizan deepfakes para difundir información errónea o comprometer objetivos de alto valor a través de ataques de ingeniería social personalizados en todos los canales de comunicación.

Manejar el problema de las personas

Uno de los principales desafíos en América Latina es garantizar que los empleados sean adecuadamente conscientes de los problemas cibernéticos que enfrentan. Eso significa tener que adaptarse a nuevos estándares y regulaciones, mejorar la colaboración o aumentar los presupuestos para la capacitación y la educación sobre problemas de ciberseguridad. La educación es clave porque el 41 % de los ciberataques en Brasil han tenido éxito en los últimos dos años. Sin embargo, el 60 % de las organizaciones dicen que se centran casi por completo en combatir ataques exitosos en lugar de intentar prevenirlos. El 72 % de las empresas creen que su organización sería más exitosa en la defensa contra los ciberataques si dedicara más recursos a la ciberseguridad preventiva. Eso significa crear estrategias para convencer a las juntas directivas de mayores presupuestos al asegurarse de que comprendan completamente los riesgos que representan los ataques cibernéticos y al no solucionar el problema de las personas.

Un panorama de amenazas en expansión

El panorama de amenazas que enfrentan las empresas latinoamericanas se está expandiendo continuamente más allá de las defensas cibernéticas actuales. Muchos de los riesgos más grandes de 2023 se han exacerbado en 2024. Una escalada de los ataques de ransomware, la ingeniería social predictiva basada en IA que abre nuevas amenazas y la falta de arquitecturas necesarias de confianza cero significa que las amenazas siguen siendo significativas para las empresas de toda la región. Por lo tanto, el fortalecimiento del escudo que las empresas utilizan para protegerse de estas amenazas cibernéticas es cada vez más necesario a través de la capacitación de profesionales de ciberseguridad y la legislación adecuada. La ciberseguridad es ahora una preocupación principal para las organizaciones de América Latina.



Ransomware: una de las principales amenazas cibernéticas dirigidas a América Latina

América Latina sigue siendo un objetivo importante para los ataques de ransomware desde 2023 hasta el presente. Se han informado más de 100 ataques de ransomware, y Lockbit lidera con 59 ataques, seguidos de Alphv, Clop y otros. El sector manufacturero ha sido el más afectado, con 18 ataques, seguidos de servicios financieros y tecnología, cada uno con 10.

El comercio minorista y la logística también han enfrentado interrupciones significativas. Una de las preocupaciones particulares es la venta de datos comprometidos, incluidas las cuentas de correo electrónico y las bases de datos confidenciales, que es prevalente, destacando las vulnerabilidades regionales de ciberseguridad. Las campañas avanzadas de malware se dirigen cada vez más a los sectores de finanzas, tecnología y gobierno.

Los sectores objetivo del ransomware

Los ataques de ransomware han afectado predominantemente a los siguientes sectores:

Fabricación:Aproximadamente 18 ataques, lo que lo convierte en el sector más afectado. Estos ataques han interrumpido las líneas de producción y han causado pérdidas financieras significativas.

Servicios financieros: Alrededor de 10 ataques, dirigidos a bancos, empresas de inversión y otras instituciones financieras, que a menudo conducen a violaciones de datos y fraude financiero.

Tecnología: Aproximadamente 10 ataques, que afectan los servicios de TI, las empresas de software y los proveedores de tecnología, lo que provoca filtraciones de datos e interrupciones operativas.

Venta al por menor: Alrededor de 9 ataques, que causan interrupciones en las cadenas de suministro y pérdidas financieras debido a pagos de rescate y filtraciones de datos.

Logística: Aproximadamente 7 ataques, que afectan los servicios de transporte y almacenamiento, lo que provoca retrasos e impactos financieros.

Educación: Alrededor de 5 ataques, dirigidos a escuelas, universidades e instituciones educativas, que a menudo conducen a filtraciones de datos e interrupciones operativas.

Legal: Aproximadamente 5 ataques, que afectan a firmas de abogados y servicios legales, lo que conduce a filtraciones de información confidencial de clientes.

Energía: Aproximadamente 4 ataques, dirigidos a los proveedores de servicios públicos y energía, que conducen a interrupciones operativas significativas.

Gobierno: Aproximadamente 4 ataques, que afectan a agencias y servicios gubernamentales, lo que provoca filtraciones de datos e interrupción operativa.

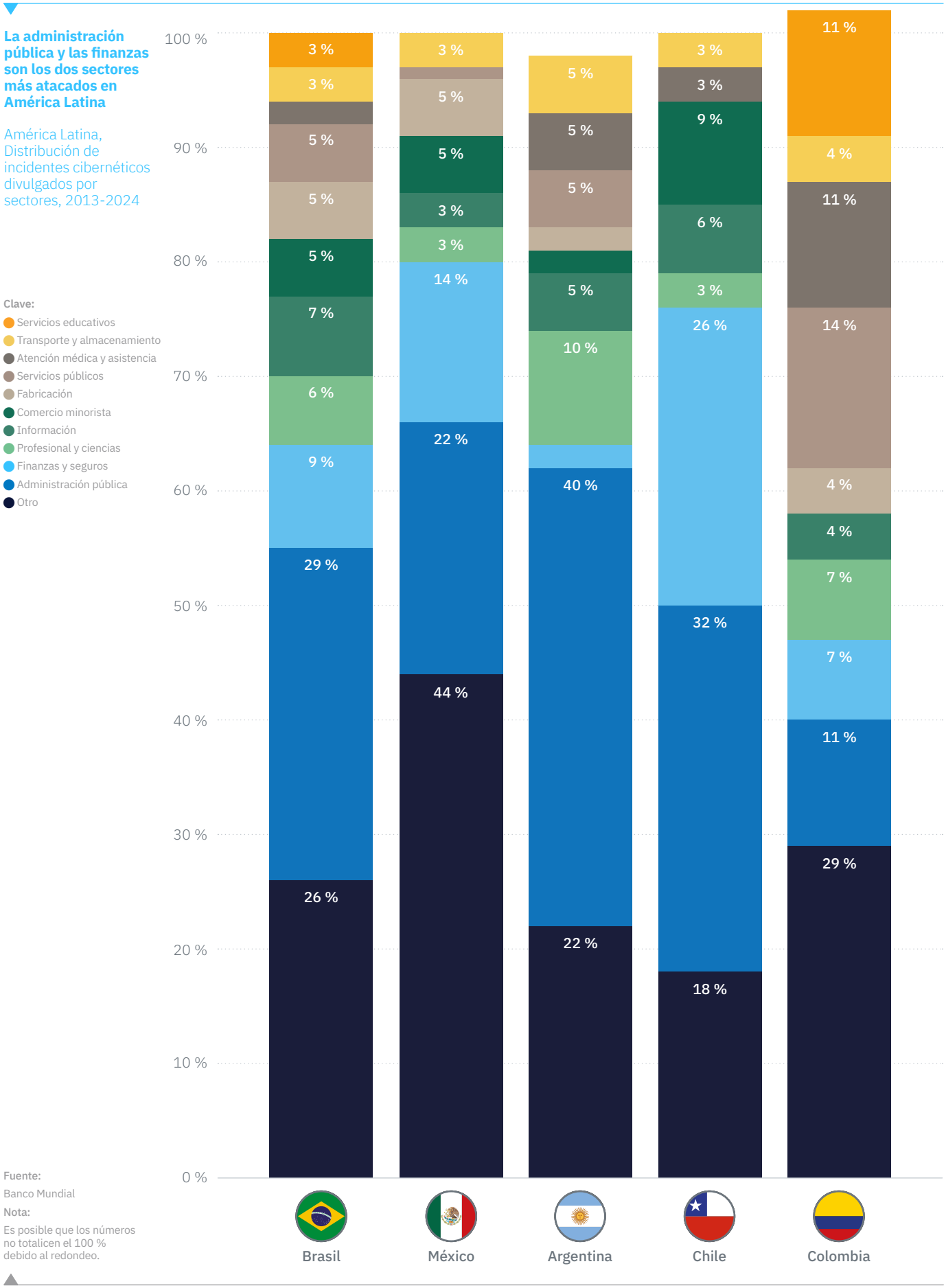
El gráfico de la página siguiente indica cuántos incidentes cibernéticos en América Latina han evolucionado más allá de solo apuntar a ganancias financieras, especialmente en países en desarrollo, donde el 59 % de los incidentes cibernéticos están impulsados políticamente, según el informe de Ciberseguridad económica para mercados emergentes publicado por el Banco Mundial. América Latina ha visto un cambio en lo que se describe como incidentes "híbridos". Por ejemplo, un ataque de ransomware a instituciones gubernamentales que causó pérdidas económicas de alrededor del 2,4 % del PIB (Costa Rica, 2022); filtraciones de datos de agencias públicas que expusieron registros confidenciales de casi todos los ciudadanos (Ecuador, 2019; Argentina, 2022); un ataque de malware que provocó el cierre de todas las sucursales bancarias públicas (Chile, 2020); y un incidente cibernético que impidió que los ciudadanos extranjeros emitieran sus votos durante las elecciones presidenciales (Ecuador, 2023).

El panorama de Brasil, México, Colombia y Chile sigue esta tendencia. En Brasil, el 29 % de los incidentes cibernéticos son de administración pública; en México, el 22 %; Colombia, el 11 %; y Chile, el 32 %. Las finanzas y los seguros también son áreas de actividad significativa. En Brasil, el sector financiero y de seguros ha sido el objetivo en el 9 % de los casos; en México, el 14 %; Colombia, el 7 %; y Chile, el mayor número, el 26 %.

Otros sectores destacados en Brasil son la información, el 7 %; los profesionales y los servicios, el 6 %; y los minoristas, el 5 %. En México, el comercio minorista y la fabricación representan el 5 % de los ataques cibernéticos. En Colombia, las áreas de preocupación son los servicios públicos, el 14 % y la atención médica, el 11 %. En Chile, el 9 % de los ataques están en el comercio minorista y el 6 % en información.

La administración pública y las finanzas son los dos sectores más atacados en América Latina

América Latina, Distribución de incidentes cibernéticos divulgados por sectores, 2013-2024



Fuente:
Banco Mundial

Nota:
Es posible que los números no totalicen el 100 % debido al redondeo.

La visión del CISO: conclusiones clave de las entrevistas del CISO en toda América Latina

Las siguientes conclusiones pueden extraerse de una encuesta de directores de seguridad de la información (CISO) realizada por el informe del CISO de América Latina en 2024.

Para comprender mejor el panorama de la ciberseguridad en América Latina, se encuestaron más de 150 CISO y otros profesionales de alto nivel en la región. El objetivo de la encuesta fue obtener una descripción general de lo que piensan los profesionales de ciberseguridad en la región sobre temas como los RMF, el uso de infraestructura de ciberseguridad pública basada en la nube para mitigar el riesgo y más.

Las recomendaciones de la política incluyeron invertir en el "desarrollo de la capacidad humana" para contrarrestar las preocupaciones del CISO sobre la capacitación insuficiente y la concientización sobre amenazas cibernéticas, y el establecimiento de marcos de gestión de riesgos. Varios países de América Latina han tomado medidas para desarrollar marcos de ciberseguridad como parte de sus agendas digitales. Pero muchas agencias gubernamentales no están obligadas a informar incidentes ni a seguir las prácticas recomendadas.

La recomendación de un marco voluntario de gestión de riesgos combinaría el establecimiento de una agencia de ciberseguridad de gobierno mixto, un CSIRT nacional, en países que aún no han implementado uno, y la creación de bases de datos de incidentes cibernéticos específicas del sector. La creación de la agencia y el equipo de respuesta se combinaría con acciones legislativas y regulatorias, como la promulgación de leyes integrales de ciberseguridad, la implementación de requisitos de generación de informes obligatorios para incidentes de ciberseguridad en una ubicación centralizada y la provisión de incentivos para la participación del sector privado en iniciativas de ciberseguridad.

Otras recomendaciones cubren la inversión en tecnología de ciberseguridad y la adopción de soluciones de nube pública, y sistemas de generación de informes y capacitación mejor centralizados para mejorar la colaboración entre diferentes sectores y agencias.

Cuando se trata del gasto de las industrias en ciberseguridad, según GlobalData, los sectores más notables para Brasil, México, Colombia y Chile son la banca, el comercio minorista, la TI, la fabricación y la energía. En Brasil, los ingresos de ciberseguridad bancaria representarán $645 millones en 2028; TI y comercio minorista, $477 millones; y fabricación, $339 millones. En México, en 2028, el gasto en TI representará $272 millones; el minorista, $221 millones; la fabricación, $195 millones y la energía, $170 millones. En Colombia, para 2028, el gasto minorista, de $141 millones, representa el mayor gasto, seguido de cerca por la banca, $138 millones, energía, $120 millones y servicios públicos, $51 millones. En Chile, el mayor gasto en 2028 será en ventas minoristas, $128 millones, seguido de energía, $56 millones, servicios públicos, $46 millones y fabricación, $44 millones.

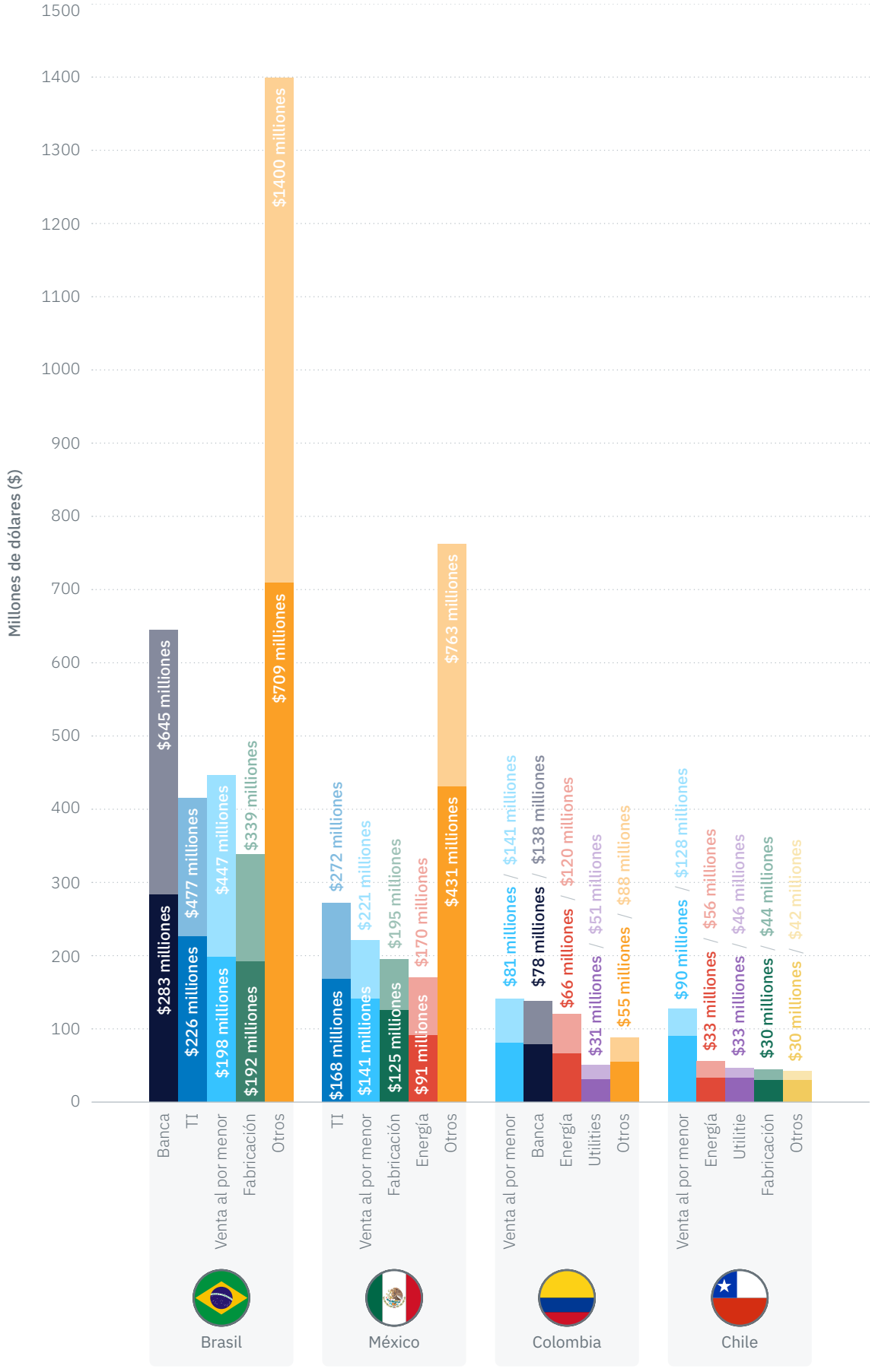
La banca, el comercio minorista, la TI, la fabricación y la energía son los impulsores clave del gasto en ciberseguridad en América Latina

Ingresos del mercado de ciberseguridad en 2024 y 2028 por las cinco principales industrias en países latinoamericanos seleccionados

Clave

Colores sólidos = 2024

Colores atenuados = 2028



Fuente:
GlobalData

Nota:
El segmento Otros incluye agricultura, arte, entretenimiento, recreación, venta mayorista, servicios profesionales y de negocios, construcción e ingeniería, servicios relacionados con TIC, servicios varios y bienes raíces, alquiler y arrendamiento.

El mapa de exposición de GlobalData a continuación proporciona una idea general del nivel de actividad relacionada con la ciberseguridad que ocurre en cada uno de los cuatro países de América Latina y cómo se comparan entre sí. Las noticias relacionadas con la ciberseguridad, las publicaciones en redes sociales, las presentaciones de la compañía, las solicitudes de patentes y los acuerdos se rastrean en función del país en el que ocurren.

El mapa muestra que Brasil es el más propenso y proactivo en términos de ciberseguridad en América Latina, seguido por México y luego estrechamente juntos tanto por Colombia como por Chile.

Brasil es, por mucho, el más activo en términos de noticias y acuerdos relacionados con la ciberseguridad. El número de noticias de Brasil para ciberseguridad es el doble del de México y casi seis veces el de Colombia y Chile. Los acuerdos de Brasil y sus presentaciones sobre ciberseguridad son tres veces los de México. Colombia y Chile son muy similares en su cantidad de acuerdos y presentaciones, pero el número de trabajos en ciberseguridad de Colombia es más de dos veces y media el de Chile. Una sorpresa es que la cantidad de puestos de trabajo de ciberseguridad de México es de 19 069 y supera cómodamente a los 14 928 empleados de Brasil. Pero en todas las demás áreas: noticias, acuerdos, presentaciones y redes sociales, Brasil está significativamente por delante de México.

Al observar más de cerca los trabajos relacionados con la ciberseguridad publicados en los últimos dos años desde 2023 hasta 2025, tanto Brasil como México vieron un crecimiento de más del 40 % en la cantidad de trabajos relacionados con la ciberseguridad publicados en 2023 y 2024. El aumento porcentual de México del 47 % superó marginalmente al de Brasil en un 45 %.

Recién comienza 2025, pero los datos de empleos en enero de 2025 ya muestran que México crea significativamente más empleos que Brasil. México publicó 1012 empleos relacionados con la ciberseguridad en comparación con 691 empleos para Brasil.

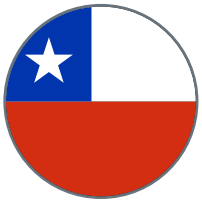
Aunque Colombia y Chile también han visto un crecimiento significativo en los trabajos relacionados con la ciberseguridad del 49 % y el 47 %, respectivamente, los totales de 4460 empleos para Colombia en 2024 y 1810 para Chile en el mismo año están muy por debajo de las cifras de trabajos para Brasil de 9528 y 12 979 para México.

Mapa de exposición de ciberseguridad segmentado por países latinoamericanos selectos ● y trabajos relacionados con la ciberseguridad publicados en países latinoamericanos selectos entre 2023 y enero de 2025 ●


Brasil


México


Colombia


Chile

	Brasil	México	Colombia	Chile
Noticias	294	142	51	59
Acuerdos	77	21	12	13
Trabajos	14 928	19 069	5471	1962
Presentaciones	2162	749	239	283
Redes sociales	1007	839	218	180
2023	6569	8800	2992	1233
2024	9528	12 979	4460	1810
Enero de 2025	691	1012	290	154

Fuente:
GlobalData

Nota:
El mapa de exposición de GlobalData permite determinar el enfoque estratégico de las empresas en temas, sectores, ubicaciones, etc. en función del nivel de consideración de los últimos 5 años completados y el año actual o el período relevante disponible para diferentes conjuntos de datos alternativos. Más oscuro el tono, mayor actividad en esa combinación y viceversa. Datos extraídos el 06 de febrero de 2025.

TecPar logra visibilidad en tiempo real, respuesta de seguridad más rápida y operaciones de TI optimizadas con Tanium

ESTUDIO DE CASO

Brasil TecPar

Brasil TecPar, una de las empresas de telecomunicaciones líderes de Brasil, enfrentó importantes desafíos para obtener visibilidad y control sobre su entorno de TI en rápida expansión, impulsado por las actividades aceleradas de fusiones y adquisiciones (Merger and Acquisition, M&A) y el crecimiento del cliente. La empresa, que cuenta con más de dos millones de clientes conectados, recurrió a Tanium y a su socio en Brasil, Secureway, para administrar su infraestructura.

Brasil TecPar había visto un rápido crecimiento a través de múltiples adquisiciones que ayudaron a expandir su base de clientes a más de 2 millones. Pero esta rápida expansión y complejidades de fusiones y adquisiciones dieron lugar a un entorno de TI fragmentado y dinámico con numerosos puntos finales en diversos sistemas y regiones.

La gestión de este entorno se volvió cada vez más difícil para TecPar, con brechas de visibilidad, gestión de parches inconsistente y vulnerabilidades de seguridad crecientes. Como resultado, el equipo de TI tuvo dificultades para mantener el control sobre la infraestructura, enfrentándose a desafíos para identificar vulnerabilidades y gestionar puntos finales de manera eficiente. La diversidad de sistemas operativos (Windows, Linux, macOS y Solaris) complicó aún más la situación, lo que dificultó garantizar actualizaciones de seguridad consistentes en toda la red. Lo que Brasil TecPar necesitaba era una solución para ayudar a recuperar el control, integrar nuevos activos y reforzar su postura de seguridad.

Para abordar sus desafíos de TI, Brasil TecPar se asoció con Secureway para implementar la plataforma de Tanium por su visibilidad en tiempo real y capacidades de gestión de endpoints. La solución de Tanium ayuda a Brasil TecPar a administrar su infraestructura compleja y creciente, lo que ayuda al equipo de TI a monitorear y administrar todos los puntos finales desde una sola consola, independientemente del sistema operativo.

La plataforma de Tanium permite a Brasil TecPar automatizar la gestión de parches en toda su red, mejorando drásticamente los tiempos de respuesta a las vulnerabilidades y reduciendo la carga de trabajo manual en los equipos de TI. La capacidad de identificar, rastrear y corregir vulnerabilidades en tiempo real garantiza que Brasil TecPar pueda mantener la seguridad y estabilidad de sus sistemas a medida que la empresa continúa creciendo.

Resultado

Brasil TecPar logra un mejor control de TI, mayor seguridad y ahorros operativos considerables. Con Tanium, Brasil TecPar obtuvo visibilidad total sobre su entorno de TI complejo y en expansión, lo que permitió un control preciso y en tiempo real de todos los puntos finales. Las perspectivas en tiempo real de la plataforma también mejoran la toma de decisiones, lo que permite al equipo de TI identificar y resolver vulnerabilidades más rápido que nunca.

La consola de administración centralizada de Tanium automatiza las medidas de parches, actualización y seguridad, lo que reduce el esfuerzo manual y garantiza que toda la infraestructura esté segura y actualizada. Esto conduce a eficiencias operativas considerables, lo que permite al personal de TI asignar tiempo y recursos a proyectos más estratégicos.

Como resultado, Brasil TecPar puede mantener una postura de seguridad sólida mientras continúa expandiéndose y atendiendo a más clientes.

Resumen

- **100 %** de visibilidad sobre todos los dispositivos conectados en diversos sistemas operativos.
- **30 %** de tiempo de respuesta más rápido a las vulnerabilidades de seguridad después de la integración con Tanium.
- **Una** consola administra todos los parches y actualizaciones de seguridad mediante Tanium.
- **Ahorros operativos** que se logran mediante la automatización de los procesos de TI y la optimización de los recursos.

TacPar de un vistazo

- **Industria:** Telecomunicaciones
- **Tamaño:** 3200 empleados
- **Oficinas centrales**: São Paulo, Brasil
- **Ingreso:** 1 millón de reales (2023)

"Mantener una visibilidad completa de nuestros activos es esencial para garantizar la seguridad de nuestra información e impulsar aún más el éxito de nuestro negocio".

IGOR ALVES COSTA
GERENTE DE SEGURIDAD DE LA INFORMACIÓN, BRASIL TECPAR

Recomendaciones

1

LA PREVENCIÓN ES MEJOR QUE LA CURA

No importa en qué parte del mundo se encuentre, cuando se trata de aumentos en los ataques cibernéticos, prevenir los ataques es una mejor opción que tratar de encontrar una cura para ellos. Invertir en medidas preventivas de ciberseguridad reducirá los costos a largo plazo, porque siempre es más costoso recuperarse de un ataque de ciberseguridad que prevenir uno. Sin embargo, a pesar de las constantes advertencias sobre las amenazas a las operaciones comerciales por ataques cibernéticos, las organizaciones solo toman medidas una vez que el problema ya ocurrió, aunque saben que el enfoque reactivo siempre significa mayores costos.

2

NO PUEDE ASEGURAR LO QUE NO PUEDE VER

La seguridad de endpoint efectiva requiere tener una vista integral de cada dispositivo en su red. Las organizaciones administran miles de endpoints en redes híbridas distribuidas, e identificar todos los dispositivos, servidores y conexiones en la nube sigue siendo la prioridad número uno para los ejecutivos de TI. El problema es que las brechas de seguridad modernas son cada vez más sofisticadas y, en el futuro, más habilitadas por IA, lo que dificulta cada vez más la protección de su red solo con defensas de seguridad tradicionales. Solo al adoptar una plataforma efectiva en tiempo real que proporcione datos críticos nuevos para ayudar a las organizaciones a mantenerse a la vanguardia de las amenazas, los equipos de seguridad y TI pueden reducir el riesgo al descubrir y gestionar endpoints, reducir la superficie de ataque con actualizaciones rápidas y entregar los parches necesarios para reducir las vulnerabilidades.

3

UNA FUENTE ÚNICA DE VERDAD

La infraestructura y las herramientas heredadas no proporcionan un panorama completo de la red corporativa y, por lo tanto, ofrecen solo una solución parcial para problemas individuales. Los equipos de operaciones y seguridad a menudo tienen que gestionar con información incompleta y antigua proporcionada por herramientas de gestión de vulnerabilidades heredadas, lo que da como resultado que ambos equipos solo afronten los datos, dejando vulnerabilidades que nunca se corrigen por completo. Sigue la fricción entre dos equipos que deben funcionar sin problemas como uno solo para garantizar la eficiencia operativa y una protección sólida de ciberseguridad para la organización. La fricción desalienta la colaboración e impacta en los resultados comerciales. Los equipos deben trabajar en conjunto, desglosar los silos y compartir datos de manera efectiva. Tener una vista en tiempo real de todos los endpoints facilita la identificación rápida y la corrección de vulnerabilidades. Una postura proactiva no solo refuerza la seguridad de una organización, sino que también agiliza las operaciones y reduce los costos.

4

CUANDO LOS COMPROMISOS DE CUMPLIMIENTO CRECEN, LA VISIBILIDAD COMPLETA DE LOS ACTIVOS ES LA PRIORIDAD

Las organizaciones latinoamericanas enfrentan el desafío de los requisitos de cumplimiento en constante crecimiento. Sin embargo, las demandas de cumplimiento se vuelven mucho más manejables cuando se puede ver y controlar cada endpoint, identificar sistemas que no cumplen con las normas, identificar dispositivos que no cumplen con los estándares de cumplimiento y priorizar los riesgos críticos mediante el análisis de brechas de cumplimiento y enfocarse en los problemas más importantes que deben abordarse. El monitoreo continuo también significa que las organizaciones pueden mantener la visibilidad en tiempo real de su estado de cumplimiento a través de escaneos continuos. Quien está advertido, está preparado.

5

LA IMPORTANCIA DE LA RESILIENCIA

Para las organizaciones latinoamericanas, la marca de su capacidad para sobrellevar las amenazas cibernéticas no se trata tanto de evitar ataques, porque hay demasiados que evitar, sino de cuán resilientes son a esos ataques. La marca de un enfoque de ciberseguridad eficaz es la rapidez con la que puede ponerse en marcha nuevamente. En América Latina, tener marcos sólidos de gestión de riesgos es un buen comienzo. Según una encuesta del Foro Económico Mundial, casi tres cuartos (72 %) han integrado un marco de gestión de riesgos en su estrategia de ciberseguridad. Y el 94 % de los encuestados están de acuerdo en que dichos marcos pueden mejorar la resiliencia organizacional a las amenazas cibernéticas.

6

MÁS AUTOMATIZACIÓN, EQUIPOS DE SEGURIDAD MÁS EFICIENTES

Con habilidades de seguridad en un nivel superior y equipos cibernéticos que necesitan ser más eficientes como resultado, las organizaciones en América Latina se beneficiarán de la automatización de las operaciones comunes de TI y las tareas de seguridad en tiempo real. Una plataforma automatizada ayuda a los equipos de TI y seguridad a aumentar su eficiencia mediante la automatización de tareas repetitivas, un beneficio significativo dada la escasez de habilidades y las limitaciones presupuestarias que enfrenta la mayoría de las organizaciones. Al parchar servidores y remediar vulnerabilidades, las organizaciones generalmente necesitan detener todos los servicios y confirmar que están desactivados antes de continuar. Al utilizar una plataforma automatizada, las empresas pueden controlar servicios específicos, verificar su estado e implementar parches dentro de esa plataforma.

Patrocinador

Gestión de endpoints autónoma (AEM) de Tanium ofrece la solución más completa para gestionar de manera inteligente los endpoints en todas las industrias, proporcionando capacidades para el descubrimiento y el inventario de activos, la gestión de vulnerabilidades, la gestión de endpoints, la respuesta ante incidentes, el riesgo y el cumplimiento, y la experiencia digital de los empleados. La plataforma admite 34 millones de endpoints en todo el mundo, incluido el 40 % de las empresas Fortune 100, lo que ofrece operaciones cada vez más eficientes y una mejor postura de seguridad a escala, con confianza y en tiempo real. Para obtener más información sobre The Power of Certainty™, visite www.tanium.com y síganos en LinkedIn y X.

Somos el proveedor de inteligencia confiable y estándar de oro para las industrias más grandes del mundo

Tenemos un historial comprobado en ayudar a miles de empresas, organizaciones gubernamentales y profesionales de la industria a beneficiarse de decisiones más rápidas e informadas.

Nuestro enfoque único impulsado por datos, dirigido por humanos e impulsado por tecnología crea la inteligencia confiable, procesable y prospectiva que necesita para predecir el futuro y evitar puntos ciegos.

Al aprovechar nuestros datos únicos, análisis de expertos y soluciones innovadoras, le brindamos acceso a capacidades inigualables a través de una plataforma.

OFICINA CENTRAL

John Carpenter House
7 Carmelite Street
Londres
EC4Y 0AN
Reino Unido

Tel.: +44 20 7936 6400

GlobalDataPlc
GlobalDataPlc
GlobalData.com

DESCARGO DE RESPONSABILIDAD

Todos los derechos reservados. Ninguna parte de esta publicación puede reproducirse, almacenarse en un sistema de recuperación ni transmitirse de ninguna forma por ningún medio, electrónico, mecánico, fotocopiado, grabación o de otro modo, sin el permiso previo del editor, GlobalData. Se cree que los hechos de este informe son correctos al momento de la publicación, pero no se pueden garantizar. Tenga en cuenta que los hallazgos, las conclusiones y las recomendaciones que GlobalData ofrece se basarán en la información recopilada de buena fe tanto de fuentes primarias como secundarias, cuya precisión no siempre estamos en condiciones de garantizar. Como tal, GlobalData no puede aceptar responsabilidad alguna por las medidas tomadas en función de cualquier información que posteriormente pueda resultar incorrecta.