GlobalData.

SEGUNDO TRIMESTRE DE 2025

Segurança cibernética na América Latina

PATROCINADO POR

TANIUM

Conteúdo

Introdução

Segundo o centro de estudos latino-americano Canning House, a América Latina está em um ponto crucial. A "influência decrescente" do Ocidente deve oferecer à região mais democrática e diversificada do mundo em desenvolvimento uma oportunidade maior de brilhar no palco mundial. As atrações da região incluem um forte compromisso com a coexistência pacífica, respeito pela integridade territorial, direitos humanos, eleições livres na maioria dos países e o meio ambiente. Ela tem uma abundância de recursos naturais, muitos dos quais são fundamentais para a transição energética, e tem a ambição de reorganizar a arquitetura de segurança, diplomática e econômica do mundo para acomodar novas potências. Ela também desfruta de bons relacionamentos na África, Oriente Médio e Ásia, e desfruta de um substancial poder global, incluindo a função do Brasil em 2025 como presidente do fórum global de cooperação política e econômica do Sul do BRICS.

De acordo com um blog do Banco Mundial, um relatório publicado recentemente sobre economia de segurança cibernética para mercados emergentes destaca como a rápida digitalização pós-pandemia da América Latina superou a capacidade de segurança cibernética da região. Até 2024, a América Latina e o Caribe haviam se tornado a região de crescimento mais rápido do mundo para incidentes cibernéticos divulgados, com uma taxa média de crescimento anual de 25% na última década.

Este artigo discutirá como a América Latina está começando a assumir maior controle de seu cenário de segurança cibernética, incluindo a educação de seus usuários finais, a implementação de nova legislação de segurança cibernética em toda a região, desempenhando uma função fundamental nos movimentos internacionais de segurança cibernética. Todos esses elementos desempenharão seu papel no desenvolvimento da confiança cibernética da América Latina e, por fim, na promoção de sua resiliência cibernética.

HERIBERTO CABRERA

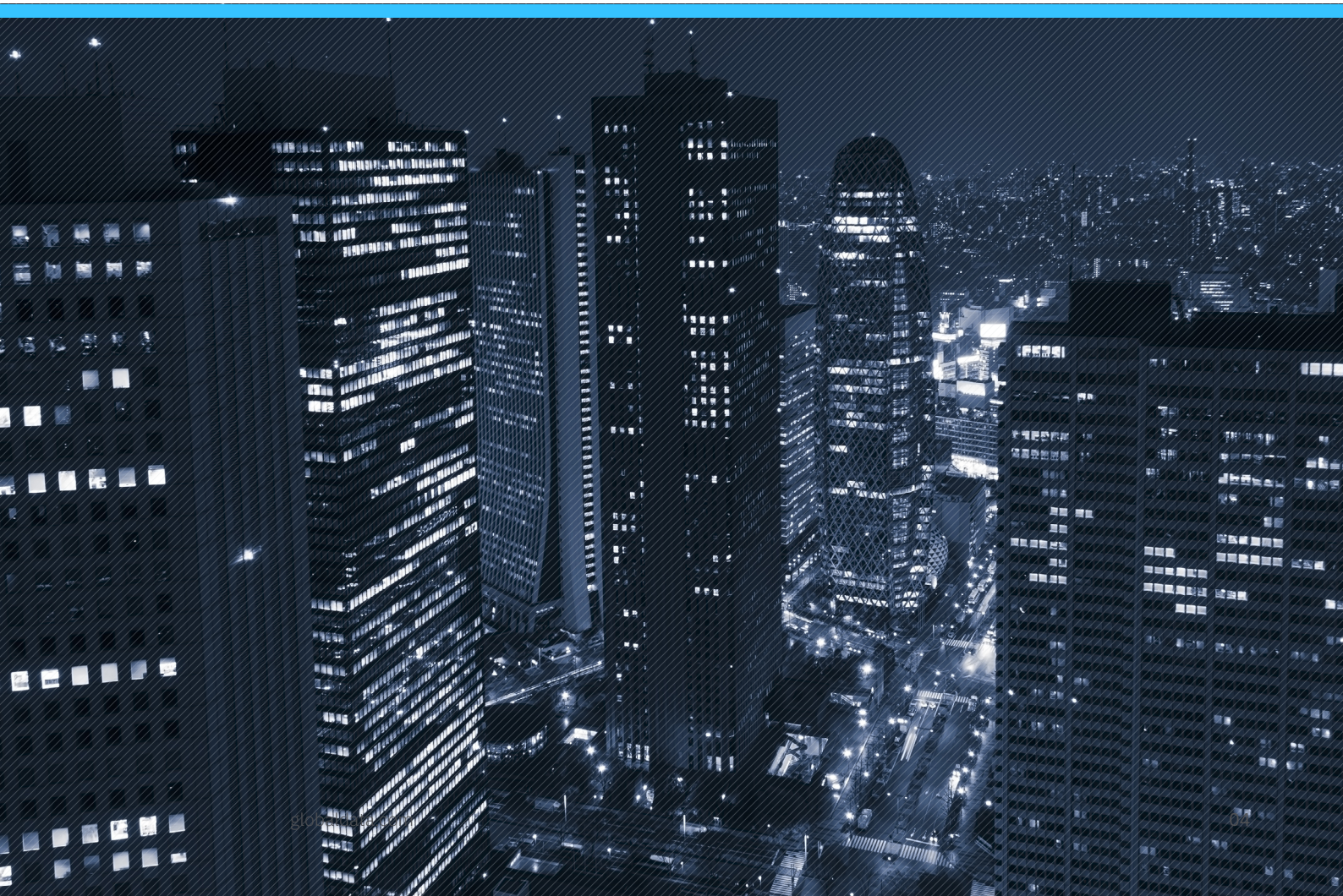
DIRETOR DE ENGENHARIA DE SOLUÇÕES TÉCNICAS, AMÉRICA LATINA, TANIUM

"O cenário de segurança cibernética na América Latina é uma combinação complexa de oportunidades e riscos, onde a rápida transformação digital colide com ameaças e riscos persistentes. No entanto, acredito firmemente que estabelecer visibilidade fundamental é fundamental para identificar riscos precocemente e prevenir ataques. Este artigo oferece percepções valiosas sobre os principais desafios que as empresas latino-americanas enfrentam e fornece exemplos do mundo real de como as organizações estão elevando com sucesso sua postura de segurança cibernética."

As implicações comerciais da segurança cibernética para a América Latina

As organizações na América Latina estão expostas a constante pressão de segurança cibernética, com um cenário de risco crescente e novos desafios operacionais contínuos. A frequência e a gravidade de violações de dados e incidentes cibernéticos estão aumentando. Agentes de ameaças cibernéticas estão aumentando seus esforços e evoluindo suas táticas para aproveitar organizações despreparadas ou despreparadas. Isso significa que a maioria das organizações. As superfícies de ataque estão se expandindo porque as forças de trabalho são mais remotas, há um aumento no uso de dispositivos da Internet das Coisas (IoT), maior prevalência de inteligência artificial (IA) em tecnologias cibernéticas, incluindo IA generativa e riscos geopolíticos crescentes.

Os países latino-americanos exibem a maior porcentagem de uso de ransomware em ataques a organizações (79%) em comparação com a média global (53%). Isso sugere que os agentes de ameaças veem as organizações na América Latina como sendo mais suscetíveis a ataques de ransomware em comparação com o resto do mundo e, portanto, visam-nas mais amplamente. Em termos de violações de dados, as descobertas do Relatório de Investigações de Violação de Dados de 2023 da Verizon mostram que “invasão de sistemas, engenharia social e ataques básicos a aplicativos da web representam 94% das violações” na América Latina. De acordo com o relatório de segurança cibernética de CISOs 2023 da América Latina, 71% dos líderes de segurança cibernética pesquisados disseram que os ataques cibernéticos em suas organizações aumentaram em relação ao ano anterior. Esse cenário desafiador de ataques cibernéticos explica por que a América Latina precisa aumentar seus gastos com segurança.



A América Latina está enfrentando os desafios de segurança cibernética enfrentados

O Brasil tornou-se um participante importante no mercado global do setor de segurança cibernética. Ela teve que, porque um aumento nas ameaças digitais, devido ao crescimento dos serviços on-line no país, juntamente com uma crescente digitalização dos serviços, levou a uma necessidade de investimentos mais robustos em segurança cibernética. De acordo com uma pesquisa, os ataques cibernéticos cresceram cerca de 70% no Brasil em um ano. A necessidade de maior investimento em segurança cibernética, por sua vez, aumentou a demanda por profissionais de segurança cibernética mais qualificados, bem como a necessidade de desenvolver soluções mais inovadoras.

Apesar do crescente número de ataques, o progresso do Brasil no desenvolvimento de seu setor de segurança cibernética fez com que ele fosse nomeado pela LinkedIn Economic Graph como ocupando a terceira posição global no crescimento do setor de segurança cibernética. A classificação baseia-se no aumento significativo do número de vagas e profissionais cibernéticos especializados no setor, bem como na importância da proteção cibernética para a continuidade dos serviços e segurança dos negócios.

A região da América Latina tornou-se um ímã para ataques cibernéticos. Atualmente, a América Latina recebe mais de 1.600 ataques cibernéticos por segundo. Além do crescimento dos ataques cibernéticos no Brasil, o México foi responsável por mais da metade de todas as ameaças cibernéticas relatadas na América Latina no primeiro semestre de 2024.

A América Latina é uma das áreas menos preparadas do mundo para ataques cibernéticos, de acordo com um índice compilado pelas Nações Unidas. Vários motivos foram sugeridos para os desafios de segurança cibernética da região. Um dos problemas vem do que pode ser considerado uma mudança definitiva para um ambiente on-line e digital como resultado da pandemia da Covid-19, com a América Latina testemunhando notáveis inovações em áreas como fintech e comércio eletrônico.

O problema era que esforços e investimentos relacionados e necessários para manter os sistemas digitais seguros não seguiam, e, portanto, faltavam medidas eficazes de segurança cibernética.

De acordo com Louise Marie Hurel, fundadora da Latin American Cybersecurity Research Network, *"o espírito empreendedor e inovador da América Latina não vem com uma preocupação com a segurança"*, como noticiado no Americas Quarterly.

Um dos primeiros sinais de alerta foi um grande ataque de ransomware que afetou a Costa Rica em abril de 2022. O ataque afetou as exportações e expôs gigabytes de informações confidenciais on-line. Em retrospectiva, era um sinal de alerta, um alerta para toda a região da América Latina. Algumas nações responderam a isso. O Chile, em particular, respondeu. E alguns países têm começado com elogios a colocar proteções em prática. Mas o sinal vermelho de alerta ainda não foi levado em consideração por todos.

Um dos problemas é a falta de educação sobre o tema, que é aliado ao ingênuo cibernético. E a América Latina não é única em ter esse problema. De acordo com um estudo da IBM, 95% de todas as infrações cibernéticas começam por um erro humano. Um ataque de phishing bem-sucedido é aquele que faz com que alguém clique em um vídeo ou em

uma oferta imbatível que não pode resistir e, em seguida, instala malware que invade os sistemas de uma empresa. Uma violação muitas vezes permanecerá não detectada até que o ransomware comece ou os dados da empresa apareçam para venda na dark web.

Foi isso que aconteceu com toda a população da Argentina em 2021, depois que um hacker anônimo supostamente vazou toda a Lista nacional de registro de pessoas da Argentina, oferecendo informações selecionadas para venda em um fórum de dark web. Da mesma forma, os residentes de Medellín na Colômbia sofreram o impacto das consequências depois que uma empresa de serviços públicos, Empresas Públicas de Medellín (EPM), sofreu um ataque de ransomware em dezembro de 2022 realizado pelo grupo BlackCat/ALPHV, que interrompeu as operações da empresa.

Essa falta de conscientização pública, aliada à legislação cibernética ainda em maturação da América Latina, faz com que as equipes de segurança de TI tenham que pegar as peças.

Na página seguinte estão apenas alguns instantâneos da América Latina em 2024, que demonstram como as organizações latino-americanas vêm sofrendo com uma onda de violações cibernéticas.

O que esses ataques mostram é que, em toda a região da América Latina, as autoridades precisam reforçar a legislação de segurança cibernética. Assim como na Europa, onde uma série de ataques cibernéticos levou à Lei de Solidariedade Cibernética da UE, um vazamento de dados no Chile levou à ação imediata para enfrentar a situação. O Chile promulgou uma lei abrangente sobre segurança cibernética e framework de infraestrutura de informações críticas para melhorar o cenário de segurança digital do país. A nova lei estabeleceu a Agência Nacional de Segurança Cibernética (ANCI), que terá poderes regulatórios e de aplicação sobre entidades públicas e privadas, garantindo uma resposta coordenada a ameaças cibernéticas.

O desafio agora para outros países da América Latina é seguir a liderança do Chile e promulgar leis semelhantes para reforçar os próprios cenários de segurança digital dos países. Esse é especialmente o caso do Brasil, México e Colômbia.

Outra observação positiva diante do aumento dos riscos de ransomware e da necessidade de maior segurança de dados é que os funcionários públicos reconhecem a importância de fortalecer a segurança cibernética nos setores público e privado. Uma maneira de preencher lacunas na prontidão e resposta cibernéticas é avançar para criar uma cultura resiliente cibernética do zero. Uma ferramenta útil aqui é a Framework de Segurança Cibernética (CSF) 2.0 do Instituto Nacional de Padrões e Tecnologia (NIST) dos EUA, que pode ser adaptada para atender às necessidades locais.

2024: Um ano de ataques cibernéticos

JANEIRO

A maior provedora de internet do Paraguai, **Tigo**, foi vítima de um ataque de ransomware que comprometeu seu data center e afetou mais de 300 empresas. O grupo de ransomware Black Hunt criptografou mais de 330 servidores e comprometeu backups, páginas da web, e-mails e armazenamento na cloud.

ABRIL

O grupo mexicano de alimentos **Grupo Bimbo** sofreu um ataque cibernético que interrompeu as operações da cadeia de suprimentos e expôs dados confidenciais da empresa, exigindo protocolos de emergência para restaurar as operações.

JUNHO

A empresa mexicana de telecomunicações **Claro** sofreu acesso não autorizado que comprometeu milhões de registros de clientes, destacando vulnerabilidades consideráveis nos registros de segurança de telecomunicações.

JULHO

Um ataque a vários **sites do governo mexicano** levou a interrupções temporárias e desfiguração de sites por grupos hacktivistas.

Uma enorme violação de dados no Chile veio à tona. O vazamento de dados afetou mais de 10 milhões de pessoas, expondo informações pessoais confidenciais e levantando preocupações sobre a infraestrutura de proteção de dados do país. A violação foi rastreada até um banco de dados mal protegido, o que permitiu acesso não autorizado a milhões de registros pessoais.

AGOSTO

O portal do governo estadual de **Alagoas** no Brasil foi alvo de um ataque cibernético, interrompendo o acesso a serviços e dados essenciais por vários dias. O ataque foi atribuído a um grupo focado em instituições do governo.

A **Prefeitura de Ponta Grossa** no Brasil foi atingida por um ataque de ransomware aos sistemas administrativos da cidade, o que levou a uma suspensão de vários serviços públicos. Os invasores exigiram um resgate em criptomoedas.

O instituto mexicano de previdência social, o **Instituto Mexicano del Seguro Social** (IMSS), foi atingido por um ataque de ransomware que interrompeu os serviços e ameaçou a liberação de dados confidenciais de pacientes, a menos que um resgate fosse pago.

SETEMBRO

Empresas Públicas de Medellín (EPM) na Colômbia foram vítimas de uma invasão cibernética que atingiu os sistemas operacionais, causando interrupções no fornecimento de eletricidade e água em Medellín.

O **Hospital das Clínicas**, em São Paulo, Brasil, sofreu um ataque de ransomware que criptografou registros de pacientes, interrompendo serviços e levantando preocupações sobre segurança de dados de cuidados de saúde.

DEZEMBRO

A provedora estatal de energia da Costa Rica, **Refinadora Costarricense de Petróleo**, conhecida como RECOPE, sofreu um ataque de ransomware que exigiu uma mudança para operações manuais e uma chamada para especialistas dos EUA para obter ajuda.

Gastos da América Latina em segurança cibernética

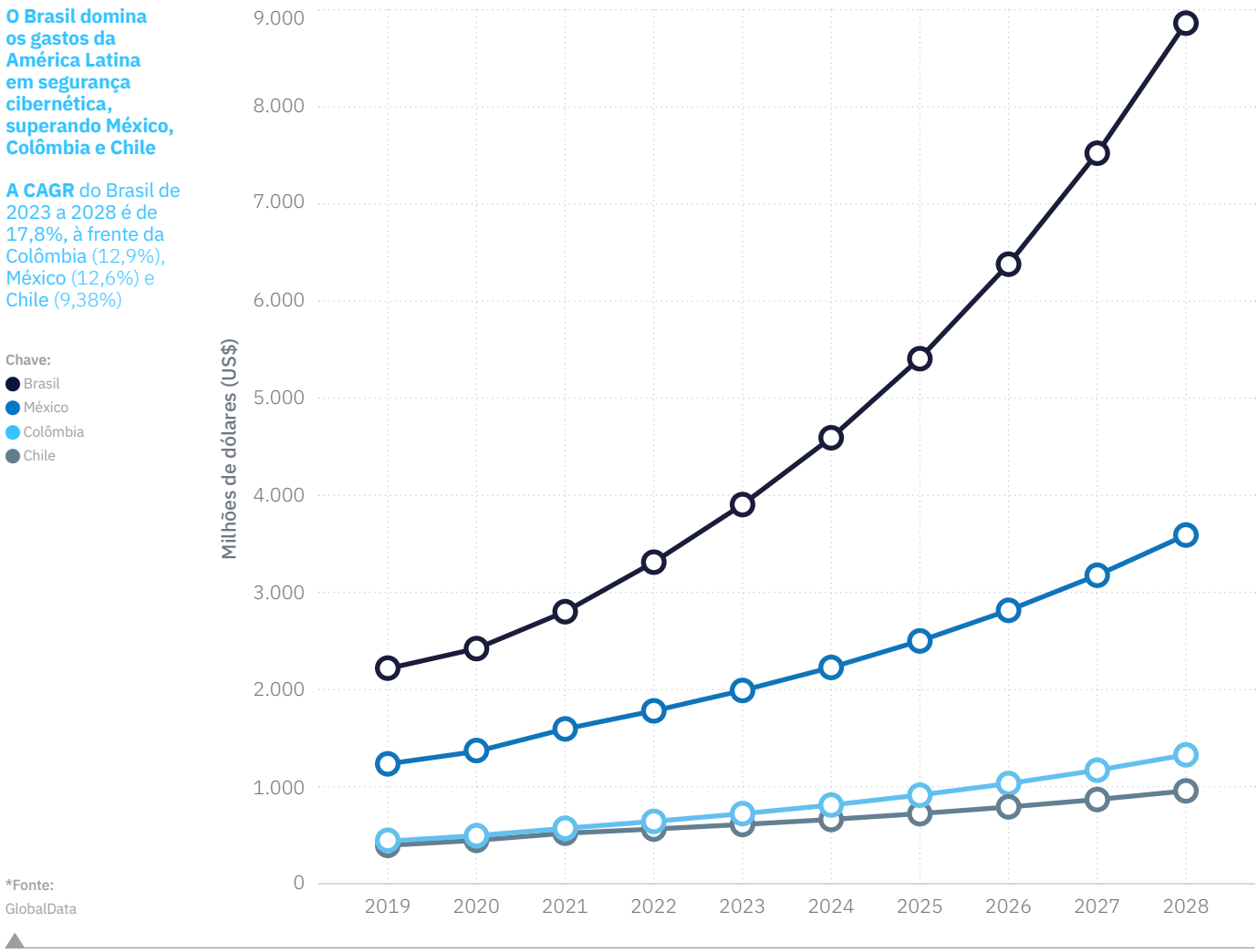
O Brasil tem confortavelmente o maior nível de gastos em segurança cibernética na América Latina. O país gastará cerca de US$ 9 bilhões em segurança cibernética em 2028. O México gastará US$ 3,6 bilhões, a Colômbia US$ 1,3 bilhão e o Chile cerca de US$ 1 bilhão. O restante da América do Sul e Central juntas quase corresponde aos gastos do México.

O maior crescimento nos gastos com segurança cibernética para países da América Latina, em particular Brasil, México, Colômbia e Chile, é em segurança de rede, que tem uma taxa de crescimento anual composta entre 2023 e 2028 de 21,3%. O próximo produto ou serviço de segurança cibernética mais importante é a segurança da web, com uma CAGR de 19,8% no mesmo período de tempo. Outras taxas de crescimento notáveis são para prevenção de fraudes e segurança transacional (19,3%) e segurança de aplicativos (19,2%).

O maior gasto é em serviços de segurança gerenciados, que tem uma CAGR de 15%. Outras taxas CAGR notáveis são filtragem de conteúdo e dispositivos anti-spam (15,9%), monitoramento de rede e controle de acesso (15,5%), autenticação multifator (12,3%) e segurança de endpoint (12,1%).

O Brasil domina os gastos da América Latina em segurança cibernética, superando México, Colômbia e Chile

A CAGR do Brasil de 2023 a 2028 é de 17,8%, à frente da Colômbia (12,9%), México (12,6%) e Chile (9,38%)

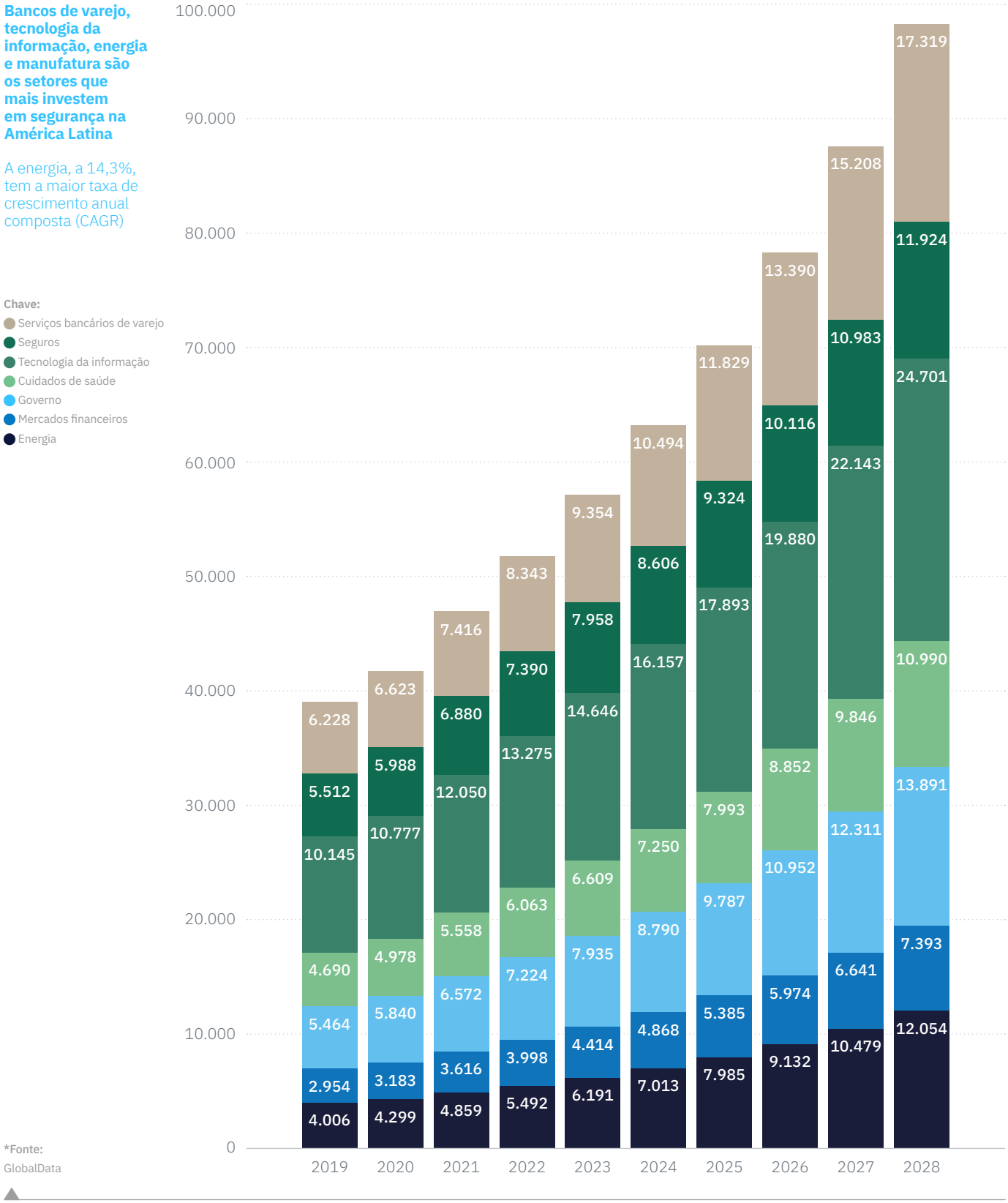


*Fonte: GlobalData

O gráfico abaixo mostra o detalhamento dos gastos com segurança por setor. Os destaques de setores são energia, cuidados de saúde, manufatura, mercados financeiros, governo, tecnologia da informação, seguros e banco de varejo. Os bancos de varejo são responsáveis pelos maiores gastos em segurança, seguidos por tecnologia da informação, fabricação e energia.

Bancos de varejo, tecnologia da informação, energia e manufatura são os setores que mais investem em segurança na América Latina

A energia, a 14,3%, tem a maior taxa de crescimento anual composta (CAGR)

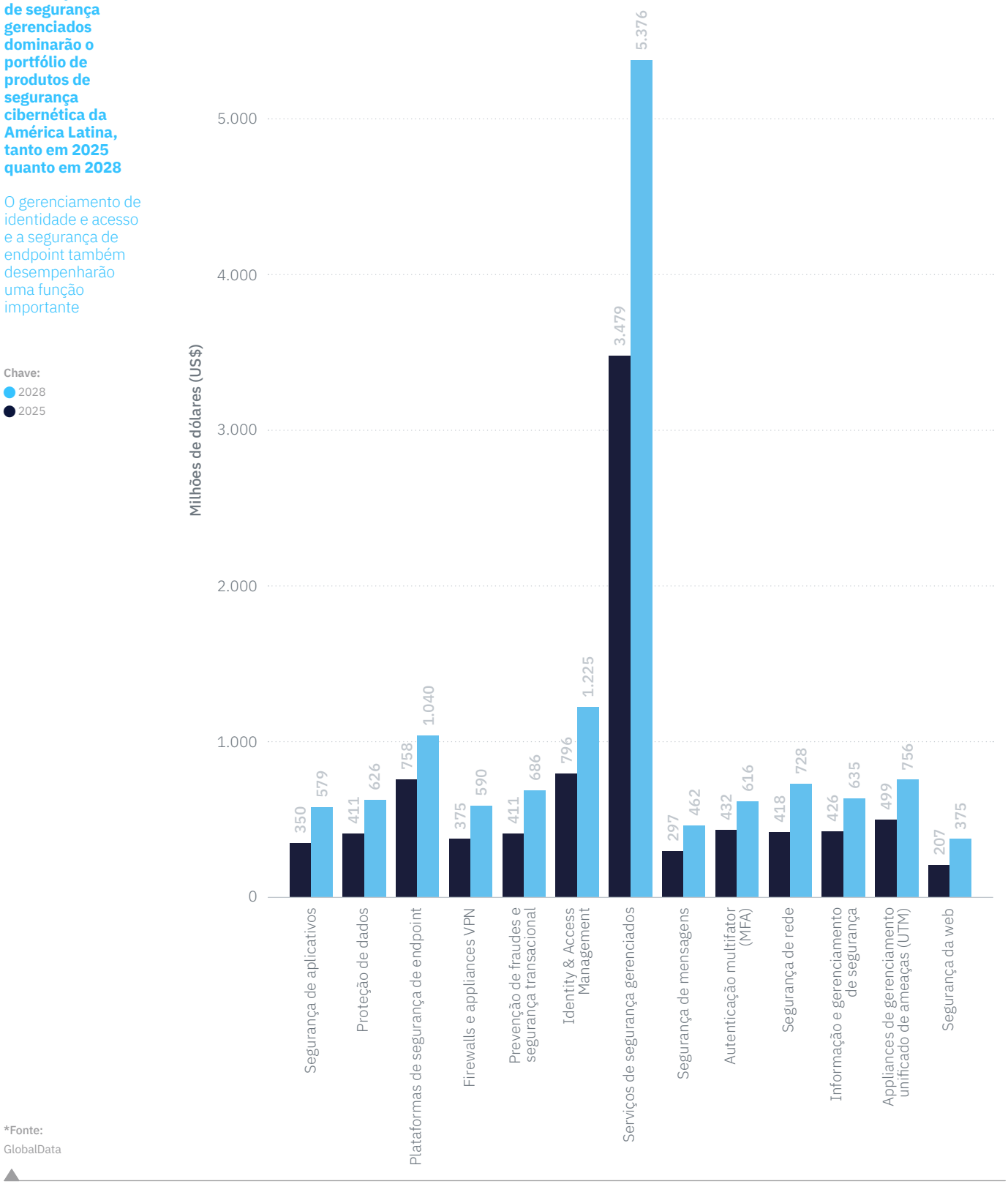


*Fonte: GlobalData

O gráfico abaixo detalha os gastos com segurança cibernética na América Latina para 2025 e 2028 por produto. As áreas de produtos com a taxa de crescimento anual composta mais forte (de 2023 a 2028) são segurança de aplicativos (20,43%), prevenção de fraudes e segurança transacional (20,45%), segurança da web (21,04%) e segurança de rede (22,68%).

Os serviços de segurança gerenciados dominarão o portfólio de produtos de segurança cibernética da América Latina, tanto em 2025 quanto em 2028

O gerenciamento de identidade e acesso e a segurança de endpoint também desempenharão uma função importante



*Fonte:
GlobalData

Conformidade e regulamentação

Em seu Panorama global de segurança cibernética de 2024, o Fórum Econômico Mundial (WEF) mencionou a "desigualdade cibernética" entre certas regiões como um problema preocupante, descrevendo o menor número de organizações cibernéticas resilientes autorrelatadas na América Latina e na África (em comparação com números mais altos na América do Norte e na Europa) como uma lacuna que "não surpreendentemente... tende a espelhar outros indicadores de desenvolvimento global".

No centro dessas questões na América Latina está a falta de conformidade e regulamentação eficazes de segurança cibernética. Mas as coisas estão começando a mudar. O Chile promulgou uma lei abrangente sobre segurança cibernética e framework de infraestrutura de informações críticas para melhorar o cenário de segurança digital do país. E agora outros países também estão seguindo o exemplo.

BRASIL

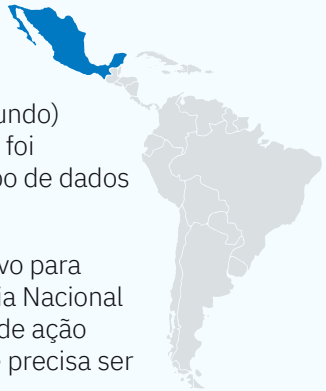
A segurança cibernética no Brasil viu um marco regulatório significativo com a criação da Política Nacional de Segurança Cibernética no final de 2023.

A Política Nacional de Segurança Cibernética, conhecida como PNCiber, destina-se a melhorar a segurança cibernética nacional e a alinhá-la às melhores práticas internacionais. O lançamento da PNCiber foi acompanhado pela criação do Comitê Nacional de segurança cibernética (CNCiber), um importante desenvolvimento de monitoramento para supervisionar a implementação e a evolução da política, bem como avaliar e propor atualizações a ela.

A PNCiber foi criada para orientar as atividades de segurança cibernética no país. Os princípios da PNCiber incluem soberania nacional, garantia de direitos fundamentais, prevenção de ataques cibernéticos, resiliência a incidentes cibernéticos, educação e desenvolvimento tecnológico em segurança cibernética, cooperação entre entidades públicas e privadas e cooperação técnica internacional. O lançamento da PNCiber demonstra a crescente atenção do governo à segurança cibernética e abre caminho para o desenvolvimento de uma cultura de segurança digital no país.

Da mesma forma, a Política Nacional de Segurança Cibernética é um marco importante na proteção da infraestrutura digital do Brasil e exigirá colaboração e adaptação contínuas às mudanças no cenário de ameaças cibernéticas para alcançar seu potencial total de segurança e privacidade de dados.

MÉXICO



De acordo com uma estimativa, o México tem a maior taxa de crimes cibernéticos na América Latina.

Essa avaliação se baseia no tamanho de sua economia (a décima quinta maior do mundo) e no grau de penetração da internet no país (que está em 83,2%). O México também foi responsável pela segunda maior porcentagem (17%) de anúncios on-line sobre roubo de dados de ransomware na América Latina.

Criar uma estratégia nacional de segurança cibernética é um desenvolvimento positivo para tentar prevenir ataques cibernéticos. Mas não é uma garantia de sucesso. A Estratégia Nacional de Segurança Cibernética (ENCS) do México, publicada em 2017, sofreu com a falta de ação eficaz. E, ainda assim, a ENCS ainda oferece um possível ponto de partida para o que precisa ser feito para tornar o México mais resistente à segurança cibernética.

O México dedicou seu tempo adotando uma lei nacional de segurança cibernética. As disposições legais sobre segurança cibernética foram, em vez disso, espalhadas por leis em diferentes setores, como finanças, telecomunicações, mão de obra, proteção ao consumidor e propriedade intelectual. Foi só em abril de 2023 que o Congresso mexicano finalmente introduziu um projeto de lei nacional de segurança cibernética.

Suas disposições mais importantes incluem: desenvolver proteções legais específicas para direitos digitais (por exemplo, inclusão digital, neutralidade líquida e proteção do consumidor on-line); exigir que empresas privadas colaborem com o governo para abordar questões de segurança cibernética; criar uma Agência Nacional de Segurança Cibernética controlada por executivos para coordenar esforços de segurança cibernética e tomar contramedidas para combater atividades cibernéticas maliciosas.

COLÔMBIA

Em 2022, o governo colombiano emitiu uma legislação, o Decreto 338, que estabeleceu diretrizes gerais para a governança da segurança digital, com a qual buscou combinar e impulsionar o desenvolvimento jurídico, os avanços técnicos, bem como o conhecimento estadual e privado para fortalecer a segurança cibernética do país.

Esse decreto fortaleceu a linha de trabalho da segurança digital na Colômbia, o que é necessário para a proteção de infraestrutura nacional e industrial crítica que está na extremidade receptora de ataques de malware e ransomware globalmente.

O Decreto 338 compromete o Ministério de Tecnologias da Informação e Comunicações da Colômbia a aumentar o inventário de infraestruturas públicas cibernéticas nacionais críticas e serviços essenciais no ciberespaço, atualizando-as a cada dois anos. A legislação também prometeu a criação de CSIRTs (Equipes de resposta e incidentes de segurança computacional) setoriais, bem como uma Plataforma Nacional para Notificação e Monitoramento de Incidentes de Segurança Digital, um espaço que servirá para a notificação e gestão de incidentes de segurança cibernética.

Em um resumo da economia digital da Colômbia, publicado em setembro de 2024, a International Trade Administration, parte do Departamento de Comércio dos EUA, observou que o Decreto 338 melhoraria a segurança digital, mas acrescentou que a conformidade pode ser exigente, particularmente para empresas menores que precisam de mais recursos e conhecimento.

CHILE

A lei de segurança cibernética do Chile é a estrela de ouro para a América Latina. O Chile seguiu em direção a um cenário cibernético mais resiliente para seus cidadãos e para a região da América Latina em 26 de março de 2024, quando promulgou a nova Lei de Framework de Segurança Cibernética e Infraestrutura de Informações Críticas.

O novo framework e os regulamentos que ele cria permitem que o Chile fortaleça sua segurança digital.

Uma parte fundamental é a nova Agência Nacional de Segurança Cibernética (ANCI) do Chile, que é projetada ao longo das linhas de agências de segurança cibernética em outros países, como a Agência de Segurança Cibernética e Infraestrutura dos EUA (CISA) e o Centro Nacional de Segurança Cibernética do Reino Unido (NCSC-UK). A ANCI terá poderes consultivos, regulatórios, de supervisão e sanções, tanto para organizações públicas quanto para organizações privadas.

A nova lei do Chile também estabelece “serviços essenciais”, que devem seguir os requisitos da ANCI. Esses serviços essenciais incluem infraestrutura crítica, bancos, transporte, setor de energia, telecomunicações, cuidados de saúde, indústria farmacêutica e tecnologia da informação. As empresas nesses setores deverão ter planos de segurança cibernética, ser revisadas regularmente e realizar exercícios de simulação de segurança cibernética.

A lei estabelece os requisitos mínimos que as entidades abrangidas devem implementar para prevenir e mitigar incidentes de segurança cibernética e também inclui requisitos de resposta a incidentes para ajudar agências e empresas a responder melhor a incidentes de segurança cibernética. Ela também exige relatórios necessários para que o governo possa rastrear incidentes e coordenar respostas adicionais, se necessário.

O cenário em evolução das ameaças cibernéticas na América Latina

Em 2024, o Brasil ocupou a presidência do grupo G20 das vinte maiores economias do mundo. O ano culminou na cúpula do G20 no Rio de Janeiro, que discutiu os desafios mais urgentes do mundo. Pode-se argumentar que a segurança cibernética deveria ter sido adicionada à lista de tópicos discutidos juntamente com a inclusão social, a reforma da governança global e as transições energéticas, porque a crescente influência internacional do Brasil está tornando-a um alvo para criminosos cibernéticos.

Quanto maior o perfil de crescimento do Brasil no cenário mundial, mais ele está em risco, tanto de ameaças cibernéticas do exterior quanto de um ecossistema criminoso próspero de dentro para fora. O Brasil é agora o quinto país mais populoso do mundo e, em 2025, assumirá a liderança do fórum intergovernamental do BRICS, agora expandido, de países em desenvolvimento, que o Brasil fundou originalmente com a Rússia, Índia e China, e mais tarde com a África do Sul.

Há, no entanto, algumas classificações que o Brasil talvez prefira perder. Por exemplo, o Brasil é o segundo país mais visado do grupo de ransomware como serviço RansomHub, com base em listagens em seu site de vazamento, de acordo com uma publicação no blog do Grupo de análise de ameaças do Google.

"À medida que a influência do Brasil cresce, o mesmo acontece com sua presença digital, tornando-o um alvo cada vez mais atraente para ameaças cibernéticas provenientes tanto de agentes globais quanto domésticos", diz a publicação do blog. "Ao mesmo tempo, o cenário de ameaças no Brasil é moldado por um mercado nacional de crimes cibernéticos." Esses criminosos cibernéticos incluem principalmente hackers que falam português do Brasil, que estão realizando aquisições de contas, fraude de cartão, exfiltração de dados financeiros usando malware bancário e ransomware em toda a América Latina.

Não é apenas o Brasil que está vendo um interesse cibernético indesejado. No México, a Fresnillo, maior produtora de prata primária do mundo e maior produtora de ouro do México, admitiu em julho de 2024 que os criminosos ganharam acesso a dados armazenados em seus sistemas durante um ataque cibernético recente. A mineração da empresa revelou em um comunicado à Bolsa de Valores de Londres que ela era "o assunto de um incidente de segurança cibernética que resultou em acesso não autorizado a determinados sistemas e dados de TI".

Ao descobrir o ataque, a Fresnillo disse que havia iniciado medidas de resposta para conter a violação, e seus especialistas em TI estão investigando e avaliando o impacto do incidente em coordenação com especialistas forenses externos.

A seguir, um resumo do estado das tendências de segurança cibernética na América Latina.

Uma imagem desafiadora

Mais de 1.600 ataques cibernéticos são relatados na América Latina por segundo, tornando os ataques cibernéticos um dos problemas de segurança que mais cresce na área. Ao mesmo tempo, os danos econômicos dos ataques cibernéticos excedem 1% de alguns países do PIB das Américas e aumentam para 6% se infraestruturas críticas forem atacadas. O volume e a sofisticação dos ataques cibernéticos registrados na América Latina estão em ascensão, com organizações em países como Brasil e México classificadas entre as principais metas globais para criminosos cibernéticos. Ambos os países são particularmente atraentes para os hackers devido à combinação da região de digitalização crescente e imaturidade generalizada da segurança cibernética.

Preocupações com a geopolítica

Um cenário geopolítico complexo e em constante mudança tem as mesmas implicações sérias para a segurança cibernética na América Latina que no resto do mundo. Nenhuma região pode se dar ao luxo de ser complacente com ameaças cibernéticas de criminosos, "hacktivistas" ou estados hostis, e o mínimo de toda a América Latina. Espera-se que os países em desenvolvimento, incluindo os da América Latina, respondam efetivamente às ameaças cibernéticas, mas não têm os fatores estruturais para fazê-lo. As disparidades no desenvolvimento em toda a região significam que as necessidades de segurança cibernética de diferentes países podem variar significativamente. As capacidades de defesa cibernética do Brasil são geralmente bem consideradas, embora ainda não sejam tão sofisticadas quanto as dos estados ocidentais ou tão bem organizadas quanto as do Chile. Enquanto isso, quando se trata de questões geopolíticas globais, o Brasil não faz parceria total com os estados norte-americanos e europeus, mas se envolveu cautelosamente na cooperação cibernética com a China e a Rússia e apoiou algumas de suas iniciativas. A função do Brasil na governança cibernética e sua posição em relação às normas cibernéticas internacionais serão moldados por seu interesse estratégico em manter uma posição independente e influente em assuntos globais.

Lacuna de habilidades e lacuna de responsabilidade

Uma geopolítica complexa e em constante mudança Há uma lacuna substancial nas habilidades de segurança cibernética em todo o mundo, com a demanda superando significativamente a oferta. De acordo com a Análise de cargos da GlobalData, o número médio de vagas de segurança cibernética abertas por mês globalmente em 2022 foi pouco inferior a 180.000. O número médio de trabalhos de segurança cibernética fechados por mês foi significativamente menor em um pouco mais de 60.000.

Uma pesquisa de 2022 do Fórum Econômico Mundial descobriu que 59% das empresas teriam dificuldades para responder a um ataque cibernético devido à escassez de talentos e habilidades em segurança cibernética. Os criminosos cibernéticos exploram lacunas de habilidades nas organizações para extrair informações. A falta geral de pessoal de segurança cibernética em todos os lugares agrava o problema.

Na América Latina, há uma lacuna estimada na força de trabalho de segurança cibernética no México e no Brasil de quase 516.000 pessoas. Isso significa que a escassez de pessoal de segurança cibernética no México está atrás apenas da escassez nos Estados Unidos. No entanto, há um crescimento notável nos cargos cibernéticos. A taxa de crescimento para profissionais cibernéticos no México em 2024 foi de 64,6%, contra uma taxa de crescimento de 27,3% para outras profissões. A taxa de crescimento do Chile foi de 28,7%, contra uma taxa de crescimento para outras profissões de 2,9%.

IA impulsiona temores de engenharia social

Embora outras tecnologias, como soluções em cloud, tenham se tornado mais comuns na região nos últimos anos, com problemas semelhantes em torno de pessoas, processos e tecnologia continuando — por exemplo, até 41% das organizações na América Latina têm lutado para preencher funções de segurança em cloud desde 2022 — a IA rapidamente se tornou o novo vetor de defesa e ataque no último ano. A IA geradora fornecerá aos agentes de ameaças novas ferramentas poderosas para conduzir engenharia social convincente em escala. Modelos avançados de linguagem natural, como ChatGPT, permitirão que os invasores transmitam e-mails de phishing e mensagens de texto personalizados e direcionados que parecem notavelmente humanos. Tentativas de manipular funcionários por meio de mídias sociais devem aumentar. À medida que essa tecnologia avança, podemos ver grupos de ameaças usarem deepfakes para espalhar informações incorretas ou comprometer alvos de alto valor por meio de ataques de engenharia social personalizados em canais de comunicação.

Gerenciar o problema das pessoas

Um dos principais desafios na América Latina é garantir que os funcionários estejam adequadamente cientes dos problemas cibernéticos que enfrentam. Isso significa ter que se adaptar a novos padrões e regulamentos, melhorar a colaboração ou aumentar os orçamentos para treinamento e educação sobre questões de segurança cibernética. A educação é fundamental porque 41% dos ataques cibernéticos no Brasil tiveram sucesso nos últimos dois anos. No entanto, 60% das organizações dizem que estão quase inteiramente focadas em combater ataques bem-sucedidos em vez de tentar evitá-los. 72% das empresas acreditam que sua organização seria mais bem-sucedida na defesa contra ataques cibernéticos se dedicasse mais recursos à segurança cibernética preventiva. Isso significa criar estratégias para convencer os conselhos a obter orçamentos maiores, garantindo que eles entendam totalmente os riscos representados por ataques cibernéticos e não superando o problema das pessoas.

Um cenário de ameaças em expansão

O cenário de ameaças enfrentado pelas empresas latino-americanas está se expandindo continuamente além das defesas cibernéticas atuais. Muitos dos maiores riscos de 2023 foram exacerbados em 2024. Um escalonamento de ataques de ransomware, engenharia social preditiva baseada em IA abrindo novas ameaças e a falta de arquiteturas de confiança zero necessárias significam que as ameaças permanecem significativas para as empresas em toda a região. Portanto, o fortalecimento do escudo que as empresas usam para se protegerem dessas ameaças cibernéticas está se tornando necessário por meio do treinamento de profissionais de segurança cibernética e legislação adequada. A segurança cibernética é agora uma preocupação primária para organizações na América Latina.

Ransomware: uma das principais ameaças cibernéticas direcionadas à América Latina

A América Latina continua sendo um alvo importante para ataques de ransomware de 2023 até o momento. Mais de 100 ataques de ransomware foram relatados, com o Lockbit liderando com 59 ataques, seguidos por Alphv, Clop e outros. O setor de manufatura tem sido o mais atingido, passando por 18 ataques, seguidos por serviços financeiros e tecnologia, cada um com 10 ataques. Varejo e logística também enfrentaram interrupções significativas. Uma das preocupações específicas é a venda de dados comprometidos, incluindo contas de e-mail e bancos de dados confidenciais, que prevalecem, destacando as vulnerabilidades regionais de segurança cibernética. Campanhas avançadas de malware estão cada vez mais visando os setores financeiro, tecnológico e governamental.

Os setores visados pelo ransomware

Os ataques de ransomware afetaram predominantemente os seguintes setores:

Fabricação: aproximadamente 18 ataques, tornando-o o setor mais afetado. Esses ataques interromperam as linhas de produção e causaram perdas financeiras significativas.

Serviços financeiros: cerca de 10 ataques, direcionados a bancos, empresas de investimento e outras instituições financeiras, muitas vezes levando a violações de dados e fraude financeira.

Tecnologia: aproximadamente 10 ataques, impactando serviços de TI, empresas de software e provedores de tecnologia, levando a violações de dados e interrupção operacional.

Lojas de varejo: cerca de nove ataques, causando interrupções nas cadeias de suprimentos e perdas financeiras devido a pagamentos de resgate e violações de dados.

Logística: aproximadamente 7 ataques, afetando serviços de transporte e armazenamento, levando a atrasos e impactos financeiros.

Educação: cerca de 5 ataques, direcionados a escolas, universidades e instituições educacionais, muitas vezes levando a violações de dados e interrupção operacional.

Jurídico: aproximadamente 5 ataques, impactando escritórios de advocacia e serviços jurídicos, levando a violações de informações confidenciais de clientes.

Energia: aproximadamente 4 ataques, direcionados a concessionárias e fornecedores de energia, levando a interrupções operacionais significativas.

Governo: aproximadamente 4 ataques, impactando agências e serviços do governo, levando a violações de dados e interrupção operacional.

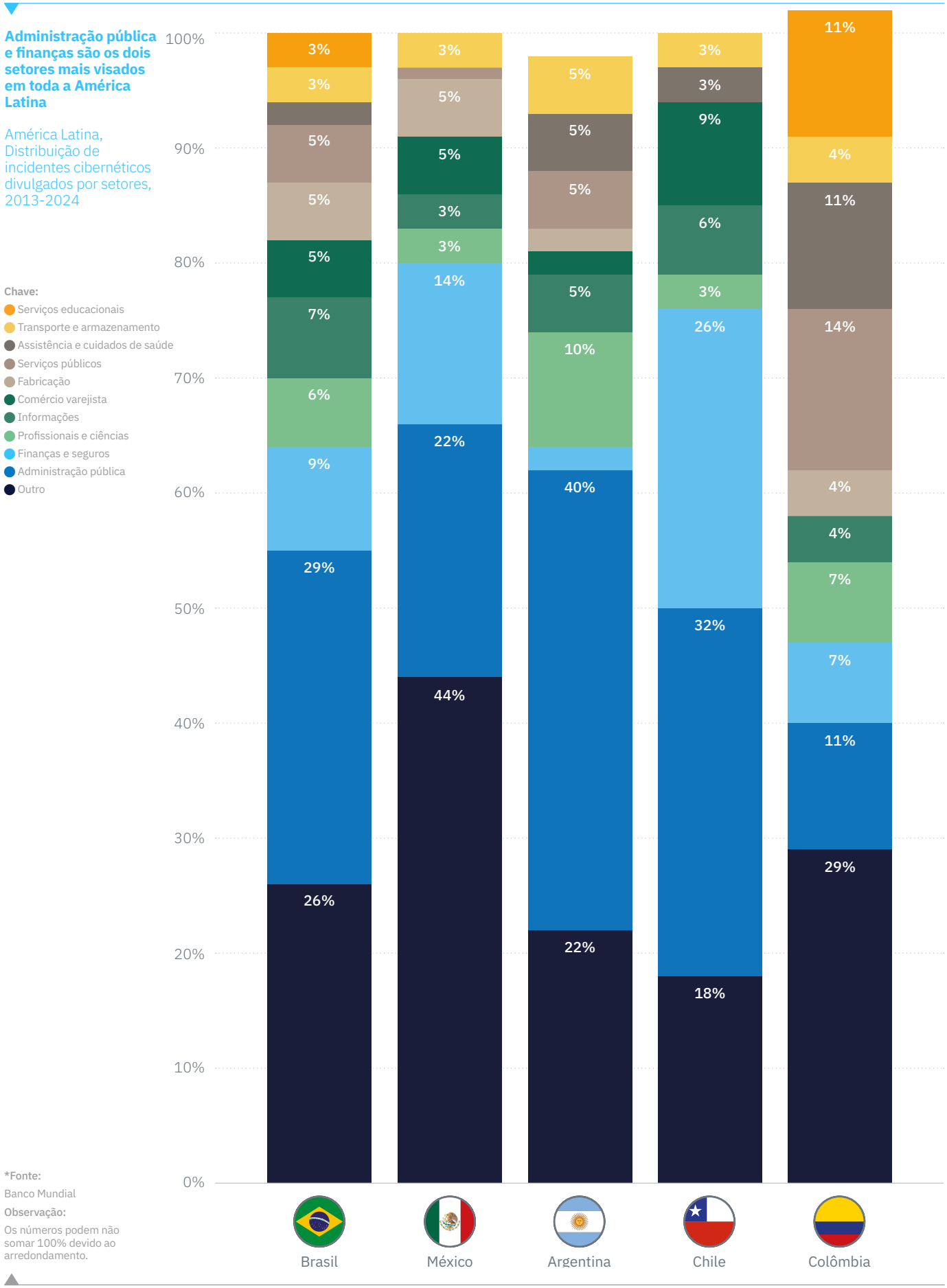
O gráfico na página seguinte indica quantos incidentes cibernéticos na América Latina evoluíram além de apenas buscar ganhos financeiros, especialmente em países em desenvolvimento, onde 59% dos incidentes cibernéticos são politicamente direcionados, de acordo com o relatório Cybersecurity Economics for Emerging Markets publicado pelo Banco Mundial. A América Latina viu uma mudança para o que é descrito como incidentes “híbridos”. Por exemplo, um ataque de ransomware a instituições do governo que causou perdas econômicas de cerca de 2,4% do PIB (Costa Rica, 2022); violações de dados a agências públicas que expuseram registros confidenciais de quase todos os cidadãos (Equador, 2019; Argentina, 2022); um ataque de malware que provocou a paralisação de todas as agências bancárias públicas (Chile, 2020); e um incidente cibernético que impediu cidadãos estrangeiros de votar durante a eleição presidencial (Equador, 2023).

A imagem do Brasil, México, Colômbia e Chile segue essa tendência. No Brasil, 29% dos incidentes cibernéticos estão na administração pública; no México, 22%; Colômbia, 11%; e Chile, 32%. Finanças e seguros também são áreas para atividades significativas. No Brasil, o setor financeiro e de seguros tem sido alvo em 9% dos casos; no México, 14%; Colômbia, 7%; e Chile, o maior número, 26%.

Outros setores notáveis no Brasil são informações, 7%; profissionais e serviços, 6%; e varejo, 5%. No México, o varejo e a manufatura são responsáveis por 5% dos ataques cibernéticos. Na Colômbia, as áreas de preocupação são serviços públicos, 14%, e cuidados de saúde, 11%. No Chile, 9% dos ataques estão no varejo e 6% em informações.

Administração pública e finanças são os dois setores mais visados em toda a América Latina

América Latina, Distribuição de incidentes cibernéticos divulgados por setores, 2013-2024



*Fonte:
Banco Mundial

Observação:
Os números podem não somar 100% devido ao arredondamento.

A visão do CISO: principais conclusões das entrevistas com CISOs na América Latina

As seguintes conclusões podem ser tiradas de uma pesquisa com diretores de segurança da informação (CISO) realizada pelo relatório de CISOs da América Latina em 2024.

Para entender melhor o cenário de segurança cibernética na América Latina, mais de 150 CISOs e outros profissionais de alto nível na região foram pesquisados. O objetivo da pesquisa foi obter uma visão geral do que os profissionais de segurança cibernética na região pensam sobre tópicos como RMFs, o uso de infraestrutura de segurança cibernética baseada em cloud pública para mitigar riscos e muito mais.

As recomendações da política incluíram investir em "construção de capacidade humana" para combater as preocupações de CISOs sobre treinamento insuficiente e conscientização sobre ameaças cibernéticas, e o estabelecimento de estruturas de gestão de risco. Vários países latino-americanos tomaram medidas para desenvolver estruturas de segurança cibernética como parte de suas agendas digitais. Mas muitas agências do governo não são obrigadas a relatar incidentes ou seguir as melhores práticas.

A recomendação de um framework voluntário de gestão de risco combinaria o estabelecimento de uma agência de segurança cibernética de governança mista, uma CSIRT nacional, em países que ainda não implementaram uma, e a criação de bancos de dados de incidentes cibernéticos específicos do setor. A criação da agência e da equipe de resposta se combinaria com ações legislativas e regulatórias, como promulgar leis abrangentes de segurança cibernética, implementar requisitos obrigatórios de relatórios para incidentes de segurança cibernética em um local centralizado e fornecer incentivos para a participação do setor privado em iniciativas de segurança cibernética.

Outras recomendações cobrem o investimento em tecnologia de segurança cibernética e a adoção de soluções de cloud pública, e melhores sistemas centralizados de relatórios e treinamento para melhorar a colaboração em diferentes setores e agências.

Quando se trata dos gastos dos setores em segurança cibernética, de acordo com a GlobalData, os setores mais notáveis para o Brasil, México, Colômbia e Chile são bancos, varejo, TI, fabricação e energia. No Brasil, as receitas de segurança cibernética bancária serão responsáveis por US$ 645 milhões em 2028; TI e varejo, US$ 477 milhões; e fabricação, US$ 339 milhões. No México, em 2028, os gastos com TI serão responsáveis por US$ 272 milhões; varejo, US$ 221 milhões; fabricação, US$ 195 milhões; e energia, US$ 170 milhões. Na Colômbia, até 2028, são os gastos de varejo, US$ 141 milhões, que representam os maiores gastos, seguidos de perto por serviços bancários, US$ 138 milhões, energia, US$ 120 milhões e serviços públicos, US$ 51 milhões. No Chile, os maiores gastos em 2028 serão no varejo, US$ 128 milhões, seguidos por energia, US$ 56 milhões, serviços públicos, US$ 46 milhões; e fabricação, US$ 44 milhões.

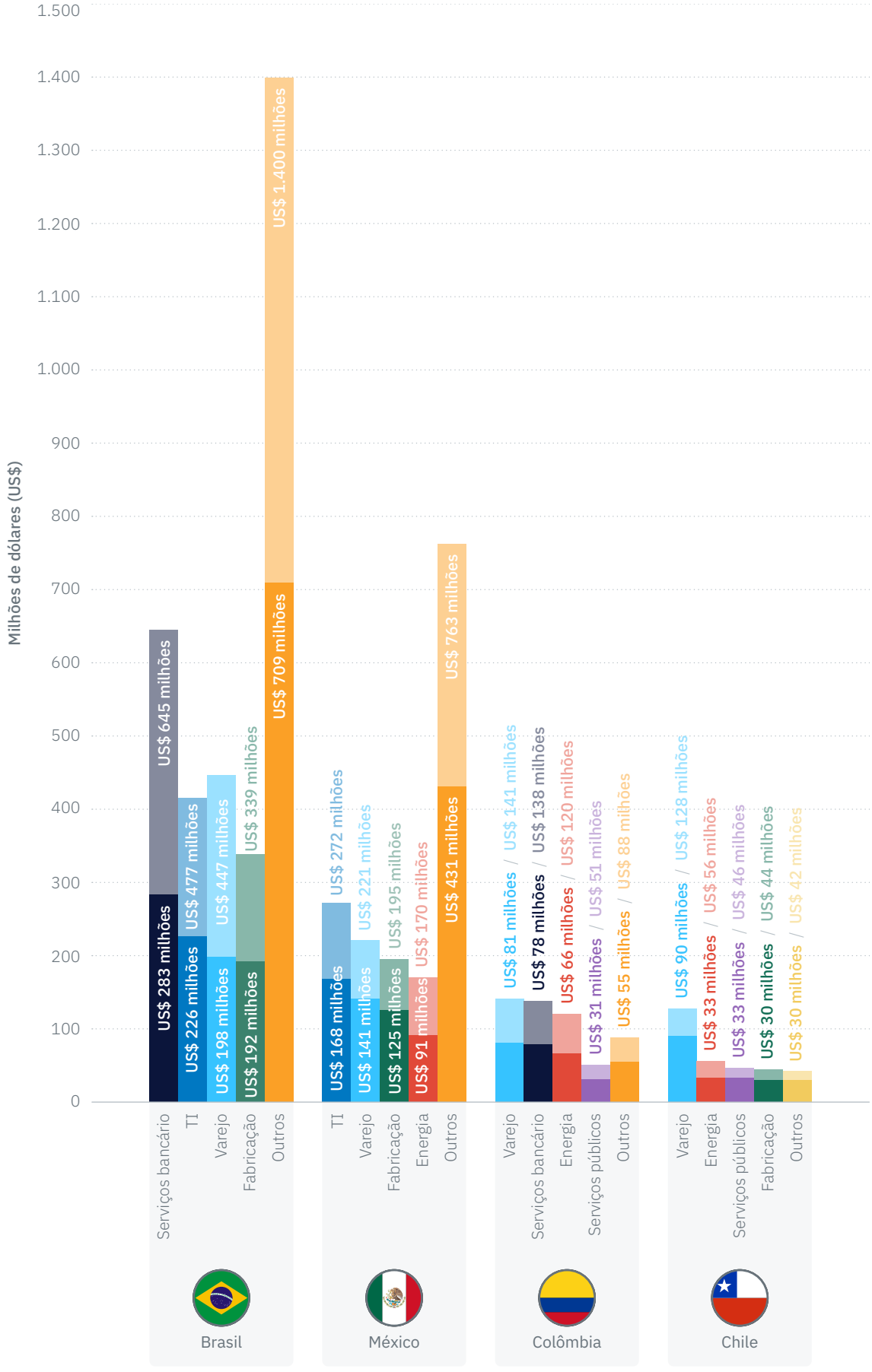
Serviços bancários, varejo, TI, fabricação e energia são os principais impulsionadores dos gastos com segurança cibernética na América Latina

Receita do mercado de segurança cibernética em 2024 e 2028 pelos cinco principais setores em países selecionados da América Latina

Chave

Cores sólidas = 2024

Cores coloridas = 2028



*Fonte:
GlobalData

Observação:
O segmento Outros inclui agricultura, artes, entretenimento, recreação, atacado, serviços profissionais e de negócios, construção e engenharia, serviços relacionados a TIC, serviços diversos e imóveis, aluguel e arrendamento.

O mapa de exposição da GlobalData abaixo fornece uma ideia geral do nível de atividade relacionada à segurança cibernética em cada um dos quatro países da América Latina e como eles se comparam entre si. Notícias relacionadas à segurança cibernética, publicações em mídias sociais, registros de empresas, pedidos de patentes e negócios são rastreados com base em qual país eles ocorrem.

O mapa mostra que o Brasil é o mais propenso e proativo em termos de segurança cibernética na América Latina, seguido pelo México e, em seguida, estreitamente unido pela Colômbia e pelo Chile.

O Brasil é, de longe, o mais ativo em termos de notícias e negócios relacionados à segurança cibernética. A contagem de notícias do Brasil para segurança cibernética é o dobro do México e quase seis vezes a da Colômbia e do Chile. Os negócios do Brasil e seus registros sobre segurança cibernética são três vezes os do México. A Colômbia e o Chile são muito semelhantes em seus números de negócios e registros, mas a contagem de vagas em segurança cibernética na Colômbia é duas vezes e meia a do Chile. Uma surpresa é que as vagas em segurança cibernética no México contam com 19.069, superando confortavelmente os 14.928 do Brasil. Mas em todas as outras áreas: notícias, negócios, registros e mídias sociais, o Brasil está significativamente à frente do México.

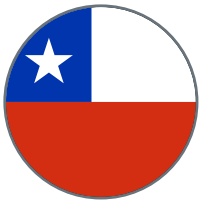
Olhando mais de perto para os vagas relacionados à segurança cibernética publicados nos países da América Latina nos últimos dois anos, de 2023 a 2025, Brasil e México viram um crescimento de mais de 40% no número de vagas relacionados à segurança cibernética publicados em 2023e 2024. O aumento percentual do México de 47% superou marginalmente o do Brasil em 45%.

Ainda está no início de 2025, mas os dados para vagas em janeiro de 2025 já mostram que o México está criando significativamente mais vagas do que o Brasil. O México publicou 1.012 vagas relacionados à segurança cibernética em comparação com 691 vagas no Brasil.

Embora a Colômbia e o Chile também tenham visto um crescimento significativo nas vagas relacionadas à segurança cibernética de 49% e 47%, respectivamente, os totais de 4.460 vagas para a Colômbia em 2024 e 1.810 para o Chile no mesmo ano estão bem abaixo dos números de vagas para o Brasil de 9.528 e 12.979 para o México.

Mapa de exposição à segurança cibernética segmentado por países selecionados da América Latina ● e vagas relacionadas à segurança cibernética publicadas em países selecionados da América Latina entre 2023 e janeiro de 2025 ●



	Brasil	México	Colômbia	Chile
Notícias	294	142	51	59
Ofertas	77	21	12	13
Vagas	14.928	19.069	5.471	1.962
Arquivamentos	2.162	749	239	283
Mídias sociais	1.007	839	218	180
2023	6.569	8.800	2.992	1.233
2024	9.528	12.979	4.460	1.810
Janeiro de 2025	691	1.012	290	154

*Fonte:
GlobalData

Observação:
O mapa de exposição da GlobalData permite determinar o foco estratégico das empresas em temas, setores, locais, etc., com base no nível de consideração dos últimos cinco anos concluídos e o ano atual ou o período relevante disponível para diferentes conjuntos de dados alternativos. Quanto mais escura a tonalidade, maior a atividade naquela combinação e vice-versa. Dados extraídos em 06 de fevereiro de 2025.

A TecPar alcança visibilidade em tempo real, resposta de segurança mais rápida e operações de TI simplificadas com a Tanium

ESTUDO DE CASO

Brasil TecPar

A operadora brasileira Brasil TecPar enfrentou desafios significativos para obter visibilidade e controle sobre seu ambiente de TI em rápida expansão, impulsionado pelo ritmo acelerado de fusões e aquisições (M&A) e pelo crescimento da base de clientes. A empresa, que tem mais de dois milhões de clientes conectados, recorreu à Tanium e à sua parceira brasileira Secureway para gerenciar sua infraestrutura.

O Brasil TecPar teve um rápido crescimento por meio de várias aquisições que ajudaram a expandir sua base de clientes para mais de 2 milhões. Mas esse rápido crescimento e as complexidades das aquisições e fusões resultaram em um ambiente de TI fragmentado e dinâmico, com diversos endpoints espalhados por sistemas e regiões distintas.

O gerenciamento desse ambiente tornou-se cada vez mais difícil para a TecPar, com lacunas de visibilidade, gerenciamento inconsistente de patches e crescentes vulnerabilidades de segurança. Como resultado, a equipe de TI se esforçou para manter o controle sobre a infraestrutura, enfrentando desafios na identificação de vulnerabilidades e no gerenciamento eficiente de endpoints. A diversidade de sistemas operacionais (Windows, Linux, macOS e Solaris) complicou ainda mais a situação, dificultando a garantia de atualizações de segurança consistentes em toda a rede. O que a Brasil TecPar precisava era de uma solução para retomar o controle, integrar os novos ativos e reforçar sua postura de segurança.

Para enfrentar seus desafios de TI, a Brasil TecPar fez parceria com a Secureway para implementar a plataforma da Tanium, devido às suas capacidades de visibilidade em tempo real e gerenciamento de endpoints. A solução da Tanium ajuda a Brasil TecPar a gerenciar sua infraestrutura complexa e crescente, ajudando a equipe de TI a monitorar e gerenciar todos os endpoints a partir de um único console, independentemente do sistema operacional.

A plataforma da Tanium permite que a Brasil TecPar automatize o gerenciamento de patches em toda a rede, melhorando drasticamente os tempos de resposta a vulnerabilidades e reduzindo a carga de trabalho manual nas equipes de TI. A capacidade de identificar, rastrear e remediar vulnerabilidades em tempo real garante que a Brasil TecPar possa manter a segurança e a estabilidade de seus sistemas à medida que a empresa continua a crescer.

Resultado

A Brasil TecPar alcança um controle de TI aprimorado, maior segurança e significativas economias operacionais. Com a Tanium, a Brasil TecPar ganhou visibilidade total sobre seu complexo e crescente ambiente de TI, permitindo o controle preciso e em tempo real de todos os endpoints. As informações em tempo real da plataforma também melhoram a tomada de decisões, permitindo que a equipe de TI identifique e resolva vulnerabilidades mais rapidamente do que nunca.

O console de gerenciamento centralizado da Tanium automatiza as medidas de correção, atualização e segurança, reduzindo o esforço manual e garantindo que toda a infraestrutura esteja segura e atualizada. Levando a eficiências operacionais significativas, permitindo que a equipe de TI aloque tempo e recursos para projetos mais estratégicos.

Como resultado, a Brasil TecPar pode manter uma forte postura de segurança enquanto continua a expandir e atender mais clientes.

Resumo

- **100%** de visibilidade de todos os dispositivos conectados em diversos sistemas operacionais.
- **30%** de tempo de resposta mais rápido às vulnerabilidades de segurança após a integração com a Tanium.
- **Um** único console gerencia todos os patches e atualizações de segurança usando a Tanium.
- **Economias operacionais** obtidas por meio da automação de processos de TI e da otimização de recursos.

Visão geral da TacPar

- **Setor:** Telecomunicações
- **Tamanho:** 3.200 funcionários
- **Sede**: São Paulo, Brasil
- **Receita:** R$ 1 bilhão (2023)

"Manter a visibilidade completa de nossos ativos é essencial para garantir a segurança de nossas informações e impulsionar ainda mais o sucesso de nossos negócios."

IGOR ALVES COSTA
GERENTE DE SEGURANÇA DA INFORMAÇÃO, BRASIL TECPAR

Recomendações

1

É MELHOR PREVENIR DO QUE CURAR

Não importa onde você esteja no mundo, quando se trata de aumentos nos ataques cibernéticos, prevenir ataques é uma aposta melhor do que tentar encontrar uma cura para eles. Investir em medidas preventivas de segurança cibernética reduzirá os custos no longo prazo, porque é sempre mais caro se recuperar de um ataque de segurança cibernética do que evitar um. No entanto, apesar de avisos constantes sobre ameaças a operações de negócios de ataques cibernéticos, as organizações fecham consistentemente o portão estável apenas depois que o cavalo se aparafusa, embora saibam que a abordagem reativa sempre significa aumento de custos.

2

VOCÊ NÃO PODE CORRIGIR O QUE NÃO PODE VER

A segurança de endpoint eficaz requer uma visão abrangente de todos os dispositivos em sua rede. As organizações gerenciam milhares de endpoints em redes distribuídas e híbridas, e identificar todos os dispositivos, servidores e conexões de cloud continua sendo a prioridade número um para executivos de TI. O problema é que as violações de segurança modernas são cada vez mais sofisticadas e, no futuro, mais habilitadas para IA, dificultando cada vez mais a proteção de sua rede apenas com as defesas de segurança tradicionais. Somente adotando uma plataforma eficaz em tempo real que fornece dados críticos novos para ajudar as organizações a ficarem à frente das ameaças, as equipes de segurança e TI podem reduzir os riscos descobrindo e gerenciando endpoints, reduzir a superfície de ataque com atualizações rápidas e fornecer os patches necessários para reduzir as vulnerabilidades.

3

UMA FONTE ÚNICA DA VERDADE

A infraestrutura e o ferramental legados não fornecem um quadro completo da rede corporativa e, portanto, oferecem apenas uma solução parcial para problemas individuais. As equipes de segurança e operações muitas vezes precisam gerenciar com informações incompletas e datadas fornecidas por ferramentas de gerenciamento de vulnerabilidades legadas, o que resulta em ambas as equipes lidando apenas com dados, deixando vulnerabilidades que nunca se tornam totalmente remediadas. O atrito segue-se entre duas equipes que devem funcionar perfeitamente como uma só para garantir eficiência operacional e proteção de segurança cibernética sólida para a organização. O atrito desencoraja a colaboração e afeta os resultados dos negócios. As equipes devem trabalhar em conjunto, decompor silos e compartilhar dados de forma eficaz. Ter uma visão em tempo real de todos os endpoints facilita a rápida identificação e remediação de vulnerabilidades. Uma postura proativa não apenas reforça a segurança de uma organização, mas também simplifica as operações e reduz os custos.

4

QUANDO OS COMPROMISSOS DE CONFORMIDADE CRESCEM, A VISIBILIDADE TOTAL DOS ATIVOS É FUNDAMENTAL

As organizações latino-americanas estão enfrentando o desafio de requisitos de conformidade cada vez maiores. Mas as demandas de conformidade se tornam muito mais gerenciáveis quando você pode ver e controlar cada endpoint, identificar sistemas não compatíveis, identificar dispositivos que não estão atendendo aos padrões de conformidade e priorizar riscos críticos analisando lacunas de conformidade e focando nas questões mais importantes a serem abordadas. O monitoramento contínuo também significa que as organizações podem manter a visibilidade em tempo real de seu status de conformidade por meio de verificações contínuas. Quem avisa, amigo é.

5

A IMPORTÂNCIA DA RESILIÊNCIA

Para as organizações latino-americanas, a marca de sua habilidade de lidar com ameaças cibernéticas não é muito sobre evitar ataques, porque há muitos para evitar, mas quão resilientes eles são a esses ataques. A marca de uma abordagem de segurança cibernética eficaz é a rapidez com que você pode começar a trabalhar novamente. Na América Latina, ter fortes frameworks de gestão de risco é um bom começo. De acordo com uma pesquisa do Fórum Econômico Mundial, quase três quartos (72%) integraram um framework de gestão de risco em sua estratégia de segurança cibernética. E 94% dos entrevistados concordam que essas frameworks podem melhorar a resiliência organizacional às ameaças cibernéticas.

6

MAIS AUTOMAÇÃO, EQUIPES DE SEGURANÇA MAIS EFICIENTES

Com habilidades de segurança em uma equipe premium e cibernética precisando ser mais eficiente como resultado, as organizações na América Latina se beneficiarão da automação de operações comuns de TI e tarefas de segurança em tempo real. Uma plataforma automatizada ajuda as equipes de TI e segurança a aumentar sua eficiência automatizando tarefas repetitivas, um benefício significativo dada a escassez de habilidades e restrições orçamentárias enfrentadas pela maioria das organizações. Ao corrigir servidores e corrigir vulnerabilidades, as organizações normalmente precisam parar todos os serviços e confirmar que estão desligados antes de prosseguir. Usando uma plataforma automatizada, as empresas podem controlar serviços específicos, verificar seu status e implantar patches dentro dessa plataforma.

Patrocinador

O Tanium Autonomous Endpoint Management (AEM) oferece a solução mais abrangente para gerenciar endpoints de forma inteligente em todos os setores, fornecendo recursos para descoberta de ativos e inventário, gerenciamento de vulnerabilidades, gerenciamento de endpoints, resposta a incidentes, risco e conformidade e experiência digital do funcionário. A plataforma suporta 34 milhões de endpoints em todo o mundo, incluindo 40% das empresas Fortune 100, oferecendo operações cada vez mais eficientes e uma postura de segurança aprimorada em escala, com confiança e em tempo real. Para mais informações sobre The Power of Certainty™, acesse www.tanium.com e siga-nos no LinkedIn e X.

Somos o provedor de informações confiável e padrão-ouro para os maiores setores do mundo

Temos um histórico comprovado em ajudar milhares de empresas, organizações do governo e profissionais do setor a lucrar com decisões mais rápidas e informadas.

Nossa abordagem exclusiva, orientada por dados, conduzida por pessoas e impulsionada por tecnologia, gera a informação confiável, acionável e voltada para o futuro de que você precisa para prever o que está por vir e evitar pontos cegos.

Aproveitando nossos dados exclusivos, análise especializada e soluções inovadoras, oferecemos acesso a capacidades inigualáveis por meio de uma plataforma.

MATRIZ

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

Tel.: +44 20 7936 6400

GlobalDataPlc
GlobalDataPlc
GlobalData.com