

DARKTRACE

Panorama das ameaças cibernéticas

na América Latina

2024–2026

Invasões baseadas em identidade,
extorsão viabilizada pela nuvem e
prioridades operacionais para de-
fensores regionais

Índice

02	Resumo Executivo	10	Setores e Países Mais Afetados
03	Principais Conclusões	11	Visão Geral por País
03	Metodologia	11	Colômbia
04	Panorama das ameaças e principais fatores determinantes	12	Chile
04	Tecnologia e expansão digital	12	México
04	Pressão geopolítica e estratégica	13	Brasil
04	Maturidade cibernética e Limitações de Capital Humano	13	Ecuador
05	A IA e o ambiente de ataque	14	Implicações Governamentais, Regulatórias e Estratégicas
05	Colaboração regional e resposta Governamental	15	Conclusão
06	Como os Ataques Evoluem na América Latina	16	Apêndice
07	Phishing, roubo de credenciais e a camada de e-mail	16	Análise do Malware Associado à Fraude do “Tribunal Colombiano”
08	A Evolução do Ransomware: da Criptografia de Dados à Extorsão e ao Abuso de Acesso	16	Análise do Malware SnappyBee / DEEDRAT
08	Malware, Infostealers e a Economia das Credenciais	17	Blind Eagle – Indicadores selecionados e Táticas, Técnicas e Procedimentos (TTPs)
08	Abuso de Ferramentas Legítimas: LOTL, VPN, RMM e SaaS	17	Perspectivas sobre a Detecção Proativa de Ameaças
10	Atividades de Ameaça Alinhadas a Interesses Estatais e Estratégicos	18	Bibliografia

Resumo Executivo

Entre 2024 e o início de 2026, o cenário de ameaças cibernéticas na América Latina passou por uma mudança significativa, tornando-se cada vez mais dominado por invasões baseadas em identidade e pela exploração de ambientes após o acesso inicial.

Em toda a região, os invasores têm contornado cada vez mais os controles de perímetro por meio do roubo de credenciais, do uso indevido de ferramentas de administração remota e da atuação dentro de fluxos legítimos de trabalho em nuvem e plataformas de Software como Serviço (SaaS), em vez de depender exclusivamente da exploração de vulnerabilidades para obter acesso às redes.



Essa mudança reflete tanto a rápida expansão digital da região quanto os diferentes níveis de maturidade cibernética entre os países. Os investimentos em nuvem híbrida, pagamentos digitais, telecomunicações, serviços baseados em inteligência artificial (IA) e modelos de trabalho distribuídos ampliaram significativamente a superfície de ataque, enquanto lacunas regulatórias, deficiências nas competências de segurança e limitações na visibilidade operacional permitiram que atores motivados por ganhos financeiros e grupos alinhados a Estados expandissem suas atividades de forma eficiente além das fronteiras nacionais.

Três tendências principais definem o cenário atual. Primeiro, o acesso por credenciais tornou-se altamente industrializado: infostealers, campanhas de phishing e ecossistemas de corretores de acesso agora fornecem acesso inicial confiável em larga escala. Segundo, as operações de ransomware evoluíram para modelos centrados na extorsão de dados e na exploração da visibilidade proporcionada por ambientes em nuvem, priorizando a exfiltração de informações e a pressão sobre as organizações em vez de se limitarem à criptografia de endpoints. Terceiro, as técnicas de living-off-the-land (LOTL) passaram a dominar cada vez mais as atividades pós-comprometimento, permitindo que os invasores se misturem às operações corporativas legítimas e evitem mecanismos de detecção baseados em assinaturas.

A telemetria da Darktrace em toda a região reforça essa transformação.

O phishing e o comprometimento de credenciais continuam sendo os principais vetores de acesso inicial, representando uma parcela significativa dos incidentes observados. Ao mesmo tempo, setores como educação, administração pública, serviços financeiros, manufatura e logística continuam entre os mais impactados. Colômbia, México, Brasil, Chile, Equador e Panamá refletem, cada um, uma combinação distinta de crescimento digital, exposição setorial e prioridades dos adversários.

Para os líderes de segurança na América Latina, o desafio não está apenas no aumento do volume de ataques, mas também na convergência das táticas utilizadas pelos adversários. Grupos motivados por ganhos financeiros, operadores regionais e atores vinculados a Estados recorrem cada vez mais aos mesmos métodos: credenciais comprometidas, uso de ferramentas confiáveis, persistência discreta e exfiltração rápida de dados. Nesse contexto, a resiliência cibernética depende da visibilidade sobre atividades relacionadas a identidades, ambientes SaaS, infraestrutura em nuvem e ferramentas de administração remota, bem como da capacidade de detectar anomalias comportamentais sutis, em vez de se concentrar exclusivamente na identificação de malware.

As organizações que continuarem a concentrar suas estratégias de segurança em controles de perímetro, sem reduzir a exposição associada às identidades e sem ampliar a visibilidade sobre atividades pós-comprometimento, permanecerão sujeitas a níveis crescentes de risco. O cenário operacional na região favorece cada vez mais os defensores capazes de identificar precocemente comportamentos anômalos de usuários, dispositivos e ambientes em nuvem, interromper rapidamente movimentos laterais e responder de forma eficaz a incidentes motivados por extorsão e roubo de dados.

Principais Conclusões

A **superfície de ataque na América Latina** foi redefinida pela rápida adoção de tecnologias digitais e de computação em nuvem, pela expansão das ferramentas de acesso remoto e pela ampla exposição de credenciais, deslocando o principal foco de risco da infraestrutura para a identidade.

A telemetria da Darktrace indica que o **phishing e o comprometimento de credenciais** continuam sendo os vetores de acesso inicial mais recorrentes, enquanto a engenharia social por e-mail segue afetando, em larga escala, tanto usuários comuns quanto contas privilegiadas.

A **evolução do ransomware** também transformou as prioridades dos adversários, direcionando seu foco para o acesso e a visibilidade em ambientes de nuvem e SaaS. Como resultado, os invasores têm privilegiado técnicas de living-off-the-land (LOTL) e o uso de ferramentas legítimas em detrimento da execução tradicional de malware.

Atores de ameaça como Blind Eagle (APT-C-36), SambaSpider e APT41 foram observados conduzindo operações contra infraestruturas críticas, instituições financeiras e organizações governamentais em diferentes países da América Latina.

As **disparidades regionais** na maturidade da segurança cibernética permanecem significativas, com economias em desenvolvimento enfrentando maior exposição a riscos devido a restrições de recursos, desafios operacionais e estruturas regulatórias fragmentadas.

Metodologia

Este relatório reúne múltiplas fontes de evidência para analisar a evolução das ameaças cibernéticas na América Latina. A análise regional principal baseia-se em dados de incidentes observados pela Darktrace entre 2024 e 2026, incluindo casos identificados na Colômbia, México, Brasil, Chile, Equador e Panamá. O relatório também incorpora dados de telemetria do Darktrace / EMAIL coletados entre outubro de 2025 e março de 2026, além de investigações direcionadas de detecção proativa de ameaças conduzidas entre janeiro de 2025 e abril de 2026.

O relatório distingue claramente entre os comportamentos observados pela Darktrace e as informações provenientes de fontes externas de contexto. As análises exclusivas da Darktrace baseiam-se na observação comportamental de atividades em ambientes de rede, nuvem, SaaS e identidade, em vez de depender exclusivamente de indicadores estáticos ou assinaturas de malware. As fontes externas são utilizadas para complementar o contexto regional, incluindo mudanças regulatórias, tendências de transformação digital em nível nacional e informações públicas sobre atividades de atores de ameaça relevantes.

Os perfis por país concentram-se em mercados de importância estratégica e com representatividade significativa nos casos analisados pela Darktrace. Assim, o relatório mantém seu foco na América Latina, sem abranger a região mais ampla da América Latina e do Caribe (LAC). Sempre que os dados se referirem a subconjuntos específicos da base de clientes ou a telemetrias de determinados produtos, esses recortes e períodos serão explicitamente indicados.

Panorama das ameaças e principais fatores determinantes

O risco cibernético na América Latina é cada vez mais influenciado pela combinação entre o rápido crescimento digital, a crescente adoção da computação em nuvem, os diferentes níveis de maturidade em segurança cibernética e as amplas oportunidades de monetização exploradas por agentes maliciosos. Embora isso não resulte em um cenário de ameaças homogêneo em toda a região, cria um modelo operacional amplamente consistente para os adversários: **obter acesso a baixo custo, misturar-se às atividades legítimas das organizações e monetizar rapidamente o acesso ou os dados comprometidos.**

Tecnologia e expansão digital

Em toda a América Latina, a contínua migração para ambientes de nuvem híbrida, aplicações empresariais SaaS, pagamentos digitais, fluxos de trabalho habilitados por inteligência artificial (IA) e conectividade de alta velocidade tem transformado significativamente a superfície de ataque ^[1]. O desafio de segurança não está na digitalização em si, mas na visibilidade fragmentada que frequentemente acompanha esse processo. À medida que as organizações expandem suas operações para ambientes distribuídos e baseados em nuvem, a identidade passa a atuar como o principal elo entre usuários, dispositivos, aplicações e terceiros, tornando a exposição e o comprometimento de credenciais riscos cada vez mais críticos ^[2].

O crescimento das ferramentas de administração remota, dos modelos de TI terceirizados e da prestação de serviços por fornecedores externos também cria caminhos mais previsíveis e acessíveis para a atuação dos invasores após o comprometimento inicial ^{[3][4]}. Quando um agente malicioso obtém acesso legítimo ou compromete um endpoint, ferramentas confiáveis e amplamente utilizadas costumam oferecer alcance suficiente para manter a persistência, movimentar-se pelo ambiente e exfiltrar dados sem a necessidade de implantar malware personalizado, reduzindo assim a probabilidade de detecção ^[5].

Implicações de segurança: em uma região onde muitas organizações avançam rapidamente em seus processos de modernização digital, mas em ritmos distintos, os maiores ganhos em termos de redução de risco tendem a vir da obtenção de visibilidade unificada sobre atividades em ambientes locais, SaaS e de nuvem. Essa visibilidade é especialmente importante para monitorar usuários, contas de serviço e comportamentos administrativos incomuns, que frequentemente representam os primeiros indícios de comprometimento.

Pressão geopolítica e estratégica

A América Latina continua atraindo uma combinação de cibercrimes motivados por interesses financeiros, operadores com foco regional e atividades de invasão associadas a interesses estatais ^{[6][6]}. Entre estes últimos, os setores de telecomunicações, governo, serviços financeiros, logística e infraestrutura crítica apresentam elevado valor estratégico e de inteligência no longo prazo. Tanto fontes públicas quanto observações da Darktrace indicam um padrão recorrente de compromissos discretos e persistentes, mais alinhados à coleta estratégica de informações do que à interrupção imediata das operações.

Os investimentos chineses em infraestrutura digital e tecnologias estratégicas em diversas partes da região também acrescentam complexidade ao cenário geopolítico, especialmente em questões relacionadas à soberania digital, à dependência de fornecedores e à exposição estratégica ^[7]. Para os defensores, **a principal lição operacional é que nem todas as invasões têm como objetivo causar interrupções visíveis.** Muitas são concebidas para permanecer ocultas por longos períodos, coletando informações de forma contínua e discreta. Nesse contexto, a detecção baseada em comportamentos anômalos e a visibilidade ao longo do tempo tornam-se mais valiosas do que abordagens focadas exclusivamente no bloqueio de eventos isolados ou indicadores conhecidos de ameaça.

Maturidade cibernética e Limitações de Capital Humano

O nível de maturidade em segurança cibernética varia significativamente entre países e setores da América Latina ^[4]. Grandes organizações e operadores de infraestrutura crítica podem contar com controles específicos robustos, mas frequentemente ainda enfrentam desafios relacionados à integração de capacidades de detecção, à maturidade dos processos de resposta a incidentes e à disponibilidade de expertise interna em segurança de identidade e ambientes de nuvem ^[8]. Por outro lado, organizações de menor porte e entidades do setor público tendem a enfrentar restrições mais acentuadas de orçamento, recursos humanos especializados, ferramentas de segurança e supervisão de terceiros ^[9]. Essas disparidades criam condições favoráveis para o comprometimento de credenciais, a preparação de campanhas de ransomware e a execução de operações de engenharia social de baixo custo.

O desafio estratégico, portanto, vai além da adoção de tecnologia. Muitas organizações ainda operam de forma predominantemente reativa, com preparação limitada para responder a incidentes de extorsão, baixa coordenação entre áreas críticas e capacidade restrita para correlacionar atividades suspeitas em endpoints, e-mail, identidades e ambientes de nuvem. Essas lacunas aumentam a vantagem operacional dos invasores, permitindo que mantenham o acesso por mais tempo e ampliem as oportunidades de monetização antes de serem detectados.



A IA e o ambiente de ataque

A proliferação de ferramentas de IA generativa e agentiva está transformando de forma significativa o cenário de ameaças cibernéticas. A IA reduz barreiras para a criação de campanhas de engenharia social, facilita a tradução de conteúdo, viabiliza a produção de materiais fraudulentos altamente convincentes, auxilia no desenvolvimento de código e amplia a escala das operações maliciosas. Na América Latina, esse cenário contribui para o aumento da frequência e da sofisticação de campanhas de phishing, fraudes digitais e ataques automatizados, sem alterar substancialmente os objetivos centrais dos adversários ^{[8] [9]}.

Para os defensores, a principal implicação está relacionada à visibilidade.

À medida que serviços legítimos baseados em IA se tornam cada vez mais presentes no ambiente corporativo, distinguir usos legítimos de atividades potencialmente suspeitas torna-se mais complexo. Essa realidade cria oportunidades para táticas operacionais assistidas por IA, incluindo o uso experimental de assistentes baseados na web como canais discretos de comunicação, mecanismos de automação ou potenciais pontos de apoio para atividades maliciosas ^{[8] [10]}.

Colaboração regional e resposta Governamental

Iniciativas regionais, como a cooperação entre equipes de resposta a incidentes de segurança cibernética (CSIRTs), o Ciberlac, a RedGEALC e outros mecanismos de colaboração técnica, demonstram avanços no fortalecimento das capacidades cibernéticas na região ^{[11] [12]}.

No entanto, a realidade operacional permanece desigual. Embora haja progressos concretos em áreas como estratégias nacionais de cibersegurança, proteção de dados e requisitos de notificação de incidentes, os níveis de fiscalização, implementação e maturidade continuam variando significativamente entre países e setores ^{[11] [12]}.

Para os defensores, isso significa que a conformidade regulatória deve ser vista como um facilitador importante, mas não como uma garantia de resiliência. Na prática, a capacidade de resistir e responder a ameaças continua dependente de competências internas de detecção, de um planejamento robusto de resposta a incidentes e da habilidade de colaborar com parceiros nacionais e internacionais quando ocorrem eventos de segurança relevantes.



Como os Ataques Evoluem na América Latina

A telemetria da Darktrace entre 2024 e 2026 demonstra que os ataques observados na América Latina seguem, de forma consistente, um padrão bem definido: comprometimento de credenciais ou acesso inicial por meio de phishing, seguido pelo uso indevido de ferramentas legítimas e pela manutenção de uma presença discreta nos ambientes corporativos. Embora as cargas maliciosas, os setores-alvo e os atores de ameaça variem, a lógica operacional subjacente permanece notavelmente consistente.

O cenário de ameaças na América Latina é marcado por um ecossistema fragmentado de ransomware, pelo uso disseminado de credenciais comprometidas obtidas por infostealers e pela forte dependência de técnicas de living-off-the-land (LOTL) e de ferramentas de monitoramento e gerenciamento remoto (RMM). Ao mesmo tempo, a região registra uma presença crescente de atores patrocinados por Estados, incluindo grupos associados a interesses estratégicos chineses, além de diversos agentes de ameaça com foco regional.

O ransomware continua sendo uma ameaça predominante na região, embora muitas campanhas permaneçam sem atribuição definitiva. Ao mesmo tempo, os infostealers alimentam uma economia cada vez mais ampla de credenciais comprometidas, fornecendo acesso inicial para uma variedade de operações subsequentes. Campanhas como o ByteToBreach, um malware baseado em nuvem, e o SORVEPOTEL, distribuído via WhatsApp pelo grupo Water Saci e direcionado aos setores financeiro e de criptomoedas, demonstram a capacidade de inovação e adaptação do ecossistema regional de cibercrime.

Paralelamente, atividades associadas ao [SnappyBee/DEEDRAT](#), relacionadas à infraestrutura e operações atribuídas ao grupo [Salt Typhoon](#) observadas pela Darktrace no Brasil, evidenciam a continuidade de campanhas alinhadas a interesses estratégicos chineses. Em conjunto, essas tendências ilustram a crescente convergência entre o cibercrime motivado por ganhos financeiros, agentes de ameaça com foco regional e operações de natureza geopolítica.

Embora o phishing e o comprometimento de credenciais continuem sendo os principais vetores de ataque na América Latina, novas variantes e operações de ransomware continuam surgindo na região, incluindo atividades atribuídas aos grupos BlackSuit, Sauron, Medusa e Dire Wolf. Esses casos também refletem uma mudança significativa na dinâmica do ransomware, com os invasores priorizando cada vez mais a extorsão baseada no vazamento de dados em vez de depender exclusivamente da criptografia de sistemas e informações.

Phishing, roubo de credenciais e a camada de e-mail

Em 44% dos casos observados pela Darktrace em toda a região, malwares não relacionados a ransomware foram identificados após o comprometimento inicial de dispositivos por meio de campanhas de phishing ou do uso de credenciais comprometidas. Esse dado reforça o papel central da exposição de identidades e da interação dos usuários como fatores determinantes para as atividades pós-comprometimento observadas pelos invasores.

Esse padrão também é corroborado pelos dados de telemetria do Darktrace / EMAIL na América Latina. Entre outubro de 2025 e março de 2026:

O que isso significa? Uma autenticação robusta de e-mail, por si só, já não é suficiente para impedir ameaças modernas. Os invasores têm demonstrado capacidade de contornar mecanismos tradicionais de confiança ao adaptar continuamente suas técnicas de engenharia social e direcionar campanhas contra indivíduos e contas de alto valor.

Para os defensores na América Latina, o fator humano continua sendo, ao mesmo tempo, o principal ponto de entrada para os ataques e uma das melhores oportunidades para detecção precoce. A identificação rápida de comportamentos suspeitos, tentativas de comprometimento de credenciais e interações incomuns dos usuários pode reduzir significativamente o impacto operacional e financeiro de incidentes mais amplos.

MAIS DE
490,000

e-mails de phishing identificados na base regional de clientes



MAIS DE
19,400

utilizaram códigos QR como vetor de acesso

MAIS DE
18,400

e-mails de phishing foram enviados a partir de domínios recém-criados

48%

foram classificados como spear phishing

37%

incorporaram novas técnicas de engenharia social

70%

foram aprovados nos controles de autenticação DMARC



MAIS DE
55,000

desses e-mails foram direcionados a usuários VIP, representando mais de 11% de todas as tentativas de phishing observadas



A Evolução do Ransomware: da Criptografia de Dados à Extorsão e ao Abuso de Acesso

O ransomware continua sendo uma ameaça recorrente na América Latina, mas é cada vez mais inadequado tratá-lo como um problema centrado exclusivamente em malware. As atividades observadas no Brasil, Chile, Colômbia, Equador e México demonstram uma ênfase crescente na obtenção e manutenção de acesso, no movimento lateral, na interrupção de operações e na exfiltração de dados, em vez de se concentrarem apenas na criptografia de endpoints. Essa evolução acompanha tendências globais mais amplas, nas quais o potencial de extorsão é cada vez mais determinado pela visibilidade e pelo acesso a ambientes de nuvem, aplicações SaaS e dados sensíveis, e não apenas pela capacidade de bloquear dispositivos ou sistemas.

Os casos observados incluíram atividades atribuídas, ou potencialmente associadas, a grupos como [BlackSuit](#), Sauron, [Medusa](#), Dire Wolf, [Akira](#), [LockBit](#), [ShadowSyndicate](#) e [RansomHub](#), embora uma parcela significativa das operações tenha permanecido sem atribuição conclusiva. Essa fragmentação é particularmente relevante do ponto de vista operacional, pois demonstra que os defensores não podem depender exclusivamente da identificação de famílias ou variantes de ransomware para avaliar e compreender o risco. Em vez disso, a prioridade deve estar na detecção de comportamentos comuns que antecedem a fase de criptografia, incluindo o abuso de credenciais, atividades administrativas atípicas, escalonamento de privilégios, reconhecimento interno do ambiente, movimentação lateral e padrões incomuns de acesso ou transferência de dados. Esses comportamentos tendem a representar indicadores mais consistentes de comprometimento do que a atribuição a uma família específica de ransomware.

Entre os clientes da Darktrace na América Latina, setores que incluem educação, administração pública, logística, manufatura, mineração, saúde e serviços financeiros têm enfrentado incidentes envolvendo criptografia de dados, exfiltração de informações, acessos não autorizados e interrupções operacionais. Na prática, o ransomware na América Latina deve ser compreendido principalmente como um problema de acesso e exposição de dados, e não apenas como uma ameaça associada à criptografia de

Setores mais afetados entre os clientes da Darktrace na América Latina:

O setor de **Educação** foi o mais impactado, representando 18% de todos os incidentes observados. Em seguida, destacaram-se a **Administração Pública** e o **setor de Informação e Comunicação**, cada um responsável por 14% do total de incidentes registrados.

18% 14%

Os setores de **Manufatura** e Comércio Atacadista e Varejista registraram um crescimento expressivo no segundo semestre de 2025, com o número de casos observados dobrando em relação ao primeiro semestre do ano. Esse aumento foi acompanhado por uma elevação dos incidentes relacionados à propagação de malware, possivelmente associada à aceleração da transformação digital e à maior exposição de dados sensíveis e ativos críticos.

sistemas. Em muitos casos, o movimento lateral, a persistência no ambiente e o acesso a informações sensíveis geram impactos operacionais, financeiros e reputacionais significativamente maiores do que a própria fase de criptografia dos arquivos.

Malware, Infostealers e a Economia das Credenciais

Os casos de malware mais relevantes observados pela Darktrace na região revelam uma predominância de infostealers, malware bancário, carregadores (loaders) em múltiplas etapas e cadeias de ataque combinadas, em vez de cargas maliciosas puramente destrutivas.

[ViperSoftX](#) e o [AtomicStealer](#) foram identificados repetidamente na Colômbia e no México, especialmente no setor educacional, evidenciando a exposição contínua de ambientes com níveis mais baixos de maturidade em segurança cibernética. No México, observou-se a atividade do Horabot, enquanto o Equador registrou campanhas mais sofisticadas envolvendo malware como GOLDBACKDOOR, [GhostSocks](#) e [Amadey](#).

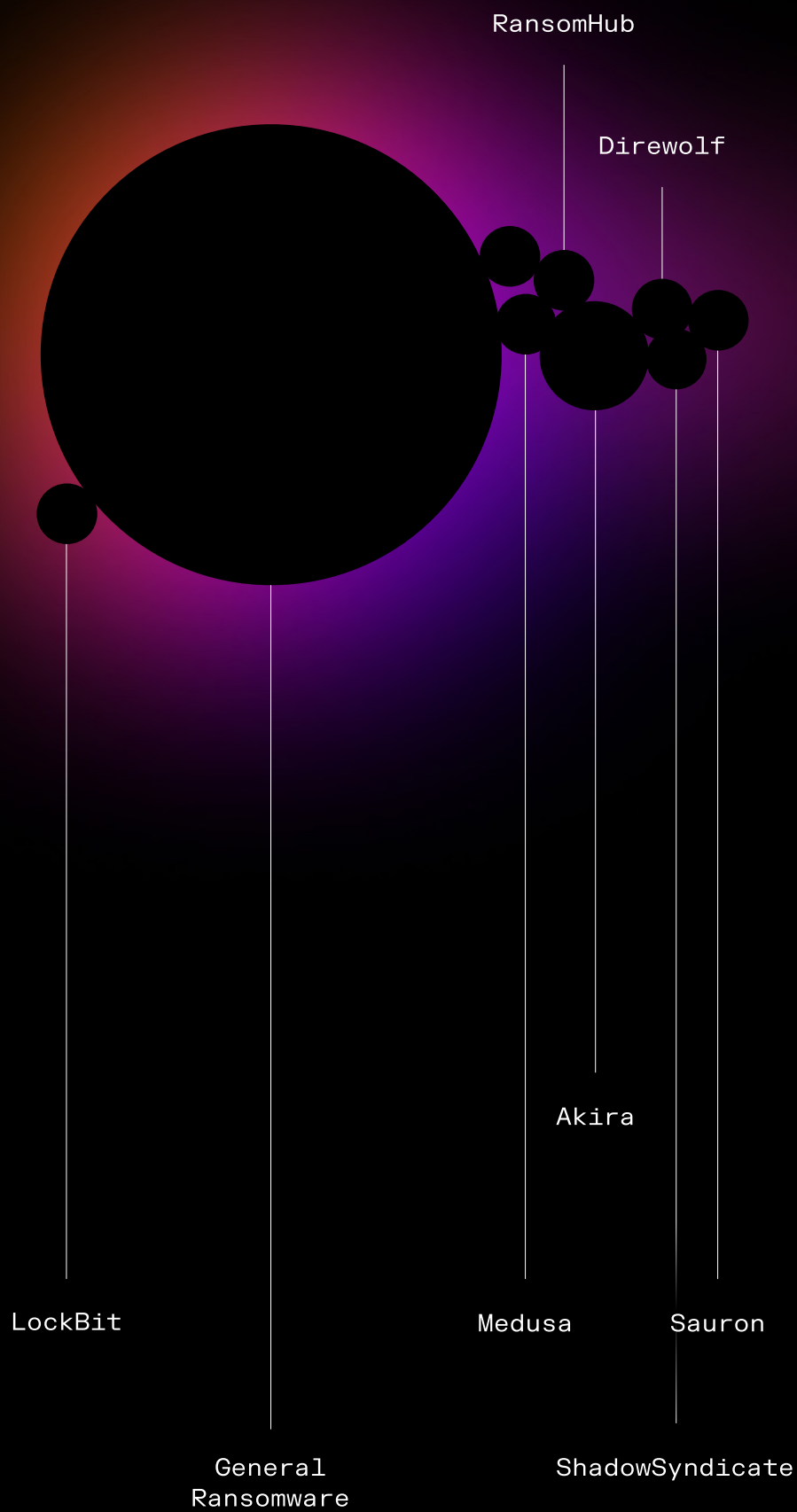
Em contraste, Chile e Brasil apresentaram maior incidência de campanhas oportunistas voltadas à mineração ilícita de criptomonedas e ao roubo de informações, particularmente em setores como agricultura, tecnologia e outros segmentos com forte dependência de ativos digitais.

Essa atividade evidencia a crescente industrialização do roubo de credenciais. Os infostealers deixaram de ser ameaças isoladas para se tornarem componentes centrais de uma economia de acesso cada vez mais sofisticada, na qual credenciais comprometidas, cookies de sessão, tokens de autenticação e outros artefatos de acesso são reutilizados, comercializados ou revendidos entre diferentes atores de ameaça. Essa dinâmica reduz significativamente o tempo entre o comprometimento inicial e uma invasão mais ampla, viabilizando fraudes, extorsões, comprometimentos de ambientes em nuvem e abusos de aplicações SaaS.

O que isso significa? Na América Latina, os infostealers devem ser encarados como indicadores precoces de um possível comprometimento mais abrangente. A presença de um malware aparentemente simples ou de baixo impacto pode representar apenas a fase inicial de uma cadeia de ataque maior, cujas consequências podem se estender muito além do dispositivo originalmente afetado.

Abuso de Ferramentas Legítimas: LOTL, VPN, RMM e SaaS

Uma das características mais marcantes das atividades observadas na região é o uso indevido de ferramentas legítimas e de funcionalidades nativas dos sistemas operacionais. Serviços de rede privada virtual (VPN), ferramentas de RMM, interpretadores de comando, aplicações SaaS acessadas por navegadores, componentes hospedados no GitHub e canais de administração em nuvem aparecem com frequência nos casos analisados pela Darktrace. Esse padrão reflete uma tendência mais ampla de substituição de implantes altamente detectáveis por técnicas que se confundem com as operações cotidianas das organizações. **Para os defensores, o desafio não está apenas em identificar a ferramenta utilizada, mas em compreender o contexto em que ela é empregada.** Atividades administrativas incomuns, acessos realizados fora do horário habitual, combinações atípicas de aplicações, anomalias geográficas, múltiplas tentativas de autenticação malsucedidas e novos destinos de tráfego de saída frequentemente representam os sinais mais relevantes de comprometimento. Em uma região onde muitas organizações dependem fortemente de fornecedores externos e de modelos terceirizados de prestação de serviços de TI, a visibilidade comportamental contextualizada torna-se um elemento essencial para a detecção precoce de ameaças e para a diferenciação entre atividade legítima e uso malicioso de ferramentas confiáveis.



Atividades de Ameaça Alinhadas a Interesses Estatais e Estratégicos

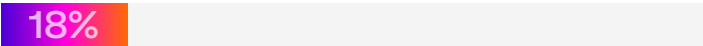
Embora o cibercrime motivado por ganhos financeiros continue representando o principal desafio operacional em grande parte da América Latina, ele não é o único fator que molda o cenário de ameaças da região [6]. As observações da Darktrace, em conjunto com informações de domínio público, também indicam uma presença crescente de atividades cibernéticas alinhadas a interesses estratégicos chineses [7].

Essas operações costumam se caracterizar pela exploração rápida de sistemas expostos à internet, pela manutenção de acesso persistente e discreto, pelo uso de técnicas como DLL sideloading, tunelamento de DNS, infraestrutura em nuvem e pelo abuso de ferramentas legítimas de administração remota. Esse modelo operacional está refletido nas atividades associadas ao ShadowPad observadas no Panamá, na Colômbia e no Brasil, bem como nas campanhas envolvendo o [PlugX](#) no Chile e nas atividades do SnappyBee/DEEDRAT relacionadas ao grupo Salt Typhoon no Brasil. Esses casos foram analisados no relatório [Crimson Echo](#) da Darktrace, que utilizou análise comportamental para contextualizar e compreender padrões de intrusão associados a atores ligados à China.

Essas invasões são importantes porque têm como alvo setores de valor estratégico, como instituições financeiras, telecomunicações, governo, energia, mineração e funções administrativas. Além disso, seu tempo de permanência tende a ser mais longo e discreto do que o observado no cibercrime tradicional. Para os defensores da região, a principal lição é que nem toda atividade de alto impacto é motivada por extorsão. Algumas invasões são mais bem compreendidas como operações estratégicas de coleta de informações que exploram as mesmas lacunas de visibilidade utilizadas por campanhas motivadas por interesses financeiros.

Setores e Países Mais Afetados

No conjunto de casos observados pela Darktrace, o setor de Educação foi o mais impactado, representando 18% de todos os incidentes registrados, seguido pela Administração Pública e pelo setor de Informação e Comunicação. Os setores de Manufatura e Comércio Atacadista e Varejista também apresentaram crescimento entre o primeiro e o segundo semestre de 2025, indicando uma pressão crescente sobre ambientes comerciais com elevada exposição digital.



A Colômbia foi consistentemente o país mais afetado entre a base de clientes observada pela Darktrace na América Latina, seguida por México, Brasil, Equador, Chile e Panamá. Essa classificação não deve ser interpretada como um retrato completo do risco cibernético na região, mas sim como um indicativo dos países onde a Darktrace tem observado, de forma recorrente, atividades significativas de invasão e onde as lições operacionais derivadas desses casos são mais relevantes.



Visão Geral por País

Os perfis dos países a seguir enfocam os mercados mais claramente representados nos casos analisados pela Darktrace e mais relevantes para o atual panorama da região, que combina expansão digital, exposição setorial e comportamento dos adversários. Cada seção está estruturada em torno do contexto de mercado, das principais ameaças, das observações da Darktrace, do ambiente regulatório em evolução e das implicações práticas para os defensores.

Colômbia

A Colômbia se destaca tanto pelo volume de ataques quanto pela diversidade de alvos. O rápido crescimento do setor de fintechs, a adoção da computação em nuvem e dos serviços digitais ampliaram a superfície de ataque do país, enquanto a relevância do setor público, a concentração de instituições financeiras e a volatilidade política continuam atraindo uma ampla gama de agentes maliciosos [13]. Grandes centros urbanos, como Bogotá e Medellín, tornaram-se cada vez mais dependentes de dados, serviços digitais e ambientes em nuvem, aumentando o valor estratégico do acesso a credenciais, aplicações SaaS e infraestruturas híbridas [14] [15] [16].

Relatórios públicos de 2024 e 2025 indicam que a Colômbia continuou sendo um dos países mais visados da América Latina, especialmente nos setores governamental, financeiro e de saúde [17].

O Blind Eagle (APT-C-36) permanece como o agente de ameaça mais persistente e visível no país, com múltiplas campanhas de intrusão que utilizam phishing, documentos maliciosos, trojans de acesso remoto (RATs) e infraestrutura de DNS dinâmico [18] [19]. Paralelamente, malwares bancários, corretores de acesso inicial (IABs) e grupos de ransomware continuam explorando a importância econômica da Colômbia e os diferentes níveis de maturidade em segurança digital observados no país [6] [20] [21].



As observações da Darktrace estão em linha com esse cenário. A Colômbia foi responsável por quase um quarto dos casos observados na América Latina no conjunto de casos analisados entre 2024 e 2025. As atividades mais frequentes envolveram programas de roubo de informações, malware associado à China e diversos padrões relacionados ao Blind Eagle. Os setores mais impactados incluíram administração pública e defesa, além de organizações financeiras e seguradoras. A sobreposição entre cibercrime e atividades de espionagem torna a Colômbia um importante indicador para o restante da região.

Um caso de fraude judicial observado na Colômbia ilustra como campanhas de engenharia social adaptadas ao contexto local continuam sendo eficazes. Nessa operação, os agentes maliciosos utilizaram uma notificação judicial falsa distribuída por meio de um arquivo de atalho para acionar a execução de comandos via PowerShell e HTA, estabelecer persistência e iniciar comunicações com uma infraestrutura de comando e controle (C2).

A relevância do caso reside não apenas na cadeia de infecção utilizada, mas também na adaptação do conteúdo ao contexto local e na rapidez com que os usuários podem ser induzidos à execução de atividades maliciosas quando temas jurídicos, financeiros ou cívicos são explorados.

O ambiente regulatório colombiano continua em evolução, com a Estratégia Nacional Digital e o marco de proteção de dados buscando fortalecer a confiança, a governança e a resiliência digital [22] [23]. No entanto, assim como em outros mercados, a ambição das políticas não se traduz automaticamente em capacidade operacional. As equipes de segurança ainda precisam de uma melhor detecção de acessos por meio de phishing, implantação de RATs e atividades C2 de saída.

Implicações para os defensores: as equipes de segurança na Colômbia devem priorizar a proteção contra acessos obtidos por phishing e o monitoramento de atividades pós-comprometimento, em vez de tratar anexos maliciosos como o estágio final do ataque. Dado o volume de atividades associadas a ameaças persistentes avançadas (APTs), a detecção precoce de mecanismos de persistência, comunicações de saída anômalas e comportamentos administrativos suspeitos continua sendo fundamental.



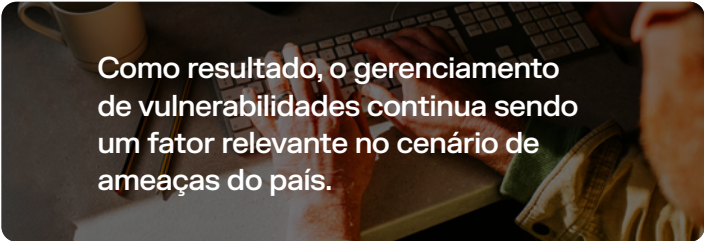
Chile

O ambiente digital do Chile é caracterizado pelo forte crescimento da infraestrutura tecnológica, pela expansão da capacidade dos data centers, pela rápida implantação do 5G e pela crescente adoção da computação em nuvem, tornando o país um mercado atraente tanto para investimentos legítimos quanto para ataques cibernéticos [24]. À medida que mais serviços empresariais e fluxos de trabalho industriais migram para ambientes digitais, a exposição do país se estende além dos ataques tradicionais a endpoints, abrangendo riscos relacionados à infraestrutura, aos provedores de serviços e aos setores críticos [24].

Entre 2024 e meados de 2026, o Chile registrou um aumento significativo no número de ataques cibernéticos reportados, com atividades envolvendo ransomware, phishing e malware afetando os setores governamental, de energia, de telecomunicações e empresarial [6][25]. Relatórios públicos também destacaram atividades associadas ao Horabot e a campanhas criminosas mais amplas direcionadas a ambientes de língua espanhola [26]. A lógica operacional permanece consistente: acesso induzido pelo usuário, exploração de sistemas expostos e atividades subsequentes voltadas para extorsão.

Os dados de casos da Darktrace entre 2024 e 2026 mostram que o Chile foi particularmente afetado no setor educacional, com incidentes relevantes envolvendo mineração de criptomoedas, ransomware e programas de roubo de informações.

Quase 50% dos casos observados envolveram a exploração de vulnerabilidades de hardware ou software, incluindo atividades relacionadas ao Cleo e o uso indevido de ferramentas como Atera e Splashtop. Esse cenário diferencia o Chile, em certa medida, de países onde o roubo de credenciais e o phishing predominam de forma mais ampla como vetores de acesso inicial.



O Chile também é um dos mercados mais ativos em termos de desenvolvimento regulatório. Sua Política Nacional de Cibersegurança, a criação da Agência Nacional de Cibersegurança (ANCI), requisitos mais rigorosos de notificação de incidentes e um marco de proteção de dados significativamente atualizado apontam para um ambiente regulatório em constante amadurecimento [26][28]. No entanto, o avanço regulatório não elimina a necessidade prática de fortalecer a disciplina na aplicação de patches, detectar sinais iniciais de ransomware e ampliar a visibilidade sobre ambientes de educação, tecnologia e serviços críticos.

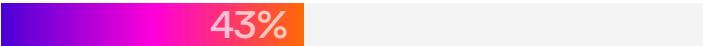
Implicações para os defensores: As organizações no Chile devem continuar priorizando o gerenciamento de vulnerabilidades e a aplicação rápida de patches. Esses esforços, porém, devem ser complementados por monitoramento comportamental capaz de detectar preparativos para ransomware, escalonamento de privilégios e movimentação lateral. Os primeiros indicadores de comprometimento costumam surgir muito antes de o ataque atingir sua fase final.

México

O papel do México como um importante polo de manufatura, logística, terceirização e serviços digitais faz do país um dos mercados cibernéticos de maior relevância estratégica na América Latina [27][28]. O crescimento contínuo dos serviços de TI, dos investimentos em nuvem, das iniciativas de cidades inteligentes e da transformação digital impulsionada pela IA amplia tanto a escala quanto a diversidade dos sistemas expostos [27][28][29]. Ao mesmo tempo, aumenta a dependência de prestadores de serviços terceirizados, criando novas oportunidades para o comprometimento da cadeia de suprimentos e para invasões relacionadas a parceiros comerciais [27][28][29].

Relatórios públicos indicam que o México continua sendo um dos países mais visados da região, enfrentando pressão constante de grupos de ransomware, malware bancário com motivação financeira, comprometimentos da cadeia de suprimentos e campanhas de phishing, incluindo operações atribuídas a atores ligados ao Estado ou estrategicamente alinhados [6].

O tamanho do país, sua base industrial e sua integração às cadeias de suprimentos norte-americanas o tornam um alvo atrativo tanto para cibercriminosos quanto para operações de espionagem. Cerca de 43% das organizações mexicanas relataram ataques à cadeia de suprimentos, destacando como relações de confiança com parceiros e fornecedores continuam sendo exploradas como vetores de acesso [29].



As observações da Darktrace posicionam o México entre os países mais afetados no conjunto de dados de 2024 a 2025. As atividades observadas incluíram exfiltração de dados, ransomware, comprometimento de serviços SaaS e acessos não autorizados, com os setores de manufatura, comércio atacadista e varejista, transporte e armazenamento entre os mais impactados.

O caso Water Saci ilustra de forma particularmente clara como grupos regionais de cibercrime vêm adaptando suas técnicas ao comportamento dos usuários locais. Nesse caso, mensagens de phishing distribuídas via WhatsApp, recuperação de instaladores, download de componentes hospedados no GitHub e comunicações externas suspeitas foram combinados em uma cadeia de invasão provavelmente motivada por interesses financeiros e direcionada ao setor financeiro.

O ambiente regulatório mexicano também continua evoluindo, com iniciativas recentes de cibersegurança e uma postura mais ativa do setor público em relação à arquitetura de segurança e à gestão de riscos [30][31]. Como parte desses esforços, o governo mexicano lançou o Plano Nacional de Segurança Cibernética 2025-2030, uma estratégia abrangente que reconhece a IA e as tecnologias em nuvem tanto como áreas de exposição quanto como ferramentas importantes para a mitigação de ameaças cibernéticas e o fortalecimento das defesas nacionais [29][30][31]. No entanto, o desafio operacional permanece significativo: uma economia ampla e altamente interconectada, com dependências externas extensas, diferentes níveis de maturidade entre fornecedores e exposição contínua ao roubo de credenciais e ao abuso de acesso.

Implicações para os defensores: as organizações mexicanas devem priorizar a segurança de ambientes SaaS, a proteção de credenciais e o monitoramento de vetores de acesso externos e conexões com terceiros. Como os invasores podem obter acesso por meio de parceiros, prestadores de serviços ou plataformas de colaboração, a detecção precoce de atividades anômalas continua sendo essencial.

Brasil

A dimensão do Brasil, seu sistema financeiro, a digitalização da agricultura, o crescimento dos data centers e os investimentos em infraestrutura de IA fazem do país tanto um líder regional em inovação quanto um alvo cibernético de alta relevância [32][33][34]. Serviços financeiros essenciais, o ecossistema PIX, a conectividade no setor de agrotecnologia e as fortes dependências de nuvem e telecomunicações ampliam o conjunto de oportunidades de invasão disponíveis tanto para cibercriminosos quanto para atores com motivações estratégicas [34][35][36].

As atividades maliciosas observadas no Brasil incluem malware bancário, ransomware, roubo de credenciais, campanhas distribuídas via WhatsApp, ecossistemas de corretores de acesso e operações de espionagem alinhadas a interesses estatais [37][38]. Relatórios públicos identificam consistentemente o país como um mercado de alto valor para malware financeiro e ransomware, enquanto as observações da Darktrace indicam que o Brasil também merece atenção especial em relação a táticas de espionagem associadas ou vinculadas à China em setores estratégicos.

Nos casos analisados pela Darktrace entre 2024 e 2025, o Brasil apresentou atividade recorrente nos setores agrícola e financeiro, incluindo malware, comprometimentos relacionados a SaaS e campanhas de roubo de informações. O caso SnappyBee/DEEDRAT é particularmente relevante por ilustrar como um ator de ameaça ligado à China explorou uma vulnerabilidade no **Citrix NetScaler**, além de utilizar SoftEther VPN, beaconing e comportamentos de exfiltração de dados para conduzir uma operação de espionagem de longo prazo contra uma organização brasileira de TI. Esse caso representa um perfil de risco distinto do malware bancário regional, embora explore muitas das mesmas lacunas de visibilidade. Uma análise mais detalhada de atividades associadas à China pode ser encontrada no relatório Crimson Echo da Darktrace.

O relatório **“The State of Cybersecurity in the UK, US and Brazilian Healthcare Sectors”** (O Estado da Segurança Cibernética nos Setores de Saúde do Reino Unido, dos EUA e do Brasil), da Darktrace, identifica um modelo de ameaça específico para o Brasil, no qual ataques cibernéticos têm como alvo, de forma crescente, pacientes e prestadores de serviços de cirurgia estética simultaneamente, utilizando dados médicos altamente sensíveis para coação direta e exigência de pagamento. Nesse contexto, os agentes maliciosos priorizam a monetização no nível do paciente, e não apenas das instituições, utilizando dados roubados para possibilitar extorsões direcionadas, em vez de depender exclusivamente das interrupções associadas ao ransomware tradicional.

Essa abordagem reflete uma adaptação ao contexto da saúde no Brasil e ao comportamento dos pacientes, em um cenário no qual a sensibilidade relacionada à privacidade e a fragmentação da segurança entre clínicas criam oportunidades para extorsão tanto de indivíduos quanto de prestadores de serviços.

O ambiente regulatório e estratégico do Brasil continua evoluindo por meio da Política Nacional de Cibersegurança, dos requisitos da Lei Geral de Proteção de Dados Pessoais (LGPD) e de propostas voltadas ao fortalecimento da supervisão institucional [39][40][41][42]. No entanto, os profissionais de segurança no país continuam atuando em um ambiente no qual o cibercrime e a espionagem convergem cada vez mais em torno de identidades, ambientes em nuvem e canais baseados em ferramentas legítimas.

Implicações para os defensores: os sistemas financeiros, as infraestruturas de grande porte e a expansão digital estratégica do Brasil fazem do país um alvo prioritário tanto para cibercriminosos quanto para atores voltados à espionagem. A detecção de uso indevido de credenciais, acessos remotos anômalos, comportamentos incomuns em VPNs e movimentações atípicas de dados deve ser tratada como um indicador operacional de alta prioridade.



Ecuador

O Equador representa uma faceta diferente, mas igualmente relevante, do panorama regional de ameaças. A infraestrutura digital do país tem sido fortemente influenciada pela dependência das telecomunicações, pela conectividade rural desigual e pelos esforços contínuos de expansão dos serviços digitais [43][44][45]. À medida que a conectividade avança e o comércio eletrônico, a governança digital e a prestação de serviços online se expandem, a maturidade em segurança nem sempre evolui no mesmo ritmo.

Relatórios públicos destacam ataques de ransomware, vazamentos de dados, exposições causadas por ameaças internas e ataques distribuídos de negação de serviço (DDoS) que afetam órgãos governamentais e serviços essenciais [46][47][48][49]. O cenário de ameaças do Equador é definido menos pelo volume de ataques e mais pela resiliência, pela visibilidade e pelas consequências associadas à limitada profundidade defensiva em setores-chave.

O conjunto de casos observados pela Darktrace no Equador é menor do que o registrado na Colômbia ou no México, mas permanece amplamente alinhado às tendências nacionais de ameaças. Metade dos casos observados envolveu ataques baseados em malware no setor de transporte e armazenamento, enquanto outros incidentes incluíram o uso indevido do WinReg e a exfiltração de dados, afetando organizações dos setores de manufatura e saúde. Atividades de malware em múltiplas camadas, incluindo o GOLDBACKDOOR e componentes relacionados, sugerem que mesmo um volume menor de casos pode representar risco significativo de persistência e exploração subsequente.

O ambiente regulatório do Equador continua amadurecendo por meio de iniciativas como a Estratégia Nacional de Cibersegurança, o desenvolvimento do regime de proteção de dados pessoais e o debate contínuo sobre inteligência artificial e regulamentação de dados [50][51][52]. No entanto, para muitas organizações, especialmente aquelas com visibilidade limitada e equipes de segurança reduzidas, o desafio permanece essencialmente operacional: estabelecer referências de comportamento, monitorar atividades anômalas e manter a prontidão para responder a incidentes.

Implicações para os defensores: como a visibilidade costuma ser limitada em diversos ambientes, as organizações no Equador devem priorizar o monitoramento comportamental e a detecção de anomalias, especialmente em atividades relacionadas a malware, abuso do Registro do Windows, comunicações de saída incomuns e tentativas de exfiltração de dados.

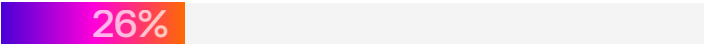
Implicações Governamentais, Regulatórias e Estratégicas

A regulamentação em segurança cibernética na América Latina está avançando, mas a realidade operacional ainda não acompanha esse ritmo. Muitos países adotaram leis mais rigorosas de proteção de dados, estratégias nacionais de cibersegurança, requisitos de notificação de incidentes e mecanismos de supervisão de infraestruturas críticas [53][54][55][56][57]. No entanto, a fiscalização, a coordenação e a capacidade operacional permanecem inconsistentes, e a distância entre a ambição das políticas públicas e a implementação efetiva das medidas de segurança continua significativa [1][6].

Esse cenário é relevante porque o ambiente de ameaças evolui mais rapidamente do que o ambiente de conformidade. As organizações já enfrentam desafios relacionados ao roubo de credenciais, à extorsão e ao uso indevido de ferramentas legítimas, independentemente do grau de maturidade dos marcos regulatórios em áreas como governança de nuvem, resposta a incidentes transfronteiriços e riscos associados à IA. Na prática, regulamentações mais rigorosas não se traduzem automaticamente em centros de operações de segurança (SOCs) mais capacitados, equipes de resposta a incidentes mais bem treinadas ou visibilidade abrangente sobre ambientes de identidade e nuvem.

Os desafios operacionais continuam expressivos em toda a região. O crescimento digital frequentemente superou os investimentos em segurança, enquanto muitas organizações ainda enfrentam escassez de profissionais qualificados, responsabilidades fragmentadas, requisitos limitados de divulgação de incidentes e coordenação insuficiente entre os setores público e privado [56][57].

Em muitos casos, existe uma diferença significativa entre a ambição tecnológica e a maturidade em segurança. Enquanto os ataques cibernéticos na região aumentam em até 26% ao ano, os investimentos em TI corporativa e infraestrutura digital na América Latina devem alcançar quase US\$ 118 bilhões, mas os orçamentos de segurança continuam significativamente inferiores [1][59].



De acordo com o Fórum Econômico Mundial, 65% das organizações na América Latina não dispõem das competências essenciais necessárias para atingir seus objetivos de segurança, e muitas relatam uma grave escassez de profissionais especializados em resposta a incidentes e engenharia DevSecOps [56]. **Apenas 12% dos líderes de TI pesquisados afirmam ter alto nível de confiança em suas equipes de segurança cibernética [56].**



Esses desafios afetam não apenas a prevenção, mas também a velocidade de resposta, a qualidade das evidências coletadas e a capacidade de compartilhar informações defensivas de forma oportuna entre setores e países.

Questões relacionadas à soberania dos dados e à dependência estratégica tornaram-se cada vez mais relevantes. Investimentos estrangeiros em infraestrutura, concentração de serviços em nuvem e dependência de provedores de telecomunicações tornam mais complexas as discussões sobre controle de dados e resposta a incidentes. Para algumas organizações, especialmente em setores regulados, isso acrescenta uma camada adicional de governança a um desafio já complexo do ponto de vista técnico. A visibilidade sobre onde os dados estão armazenados, quem pode acessá-los e com que rapidez atividades suspeitas podem ser investigadas passou a ser um requisito estratégico, e não apenas uma questão de conformidade.

Ao mesmo tempo, há avanços concretos. Brasil, Chile, Colômbia, Equador e México vêm fortalecendo suas estruturas de governança por diferentes caminhos, incluindo mecanismos de notificação de incidentes, estratégias nacionais, fiscalização da proteção de dados, adoção de princípios de confiança zero (zero trust) e criação de instituições especializadas em segurança cibernética [52][57][58][60]. Esses avanços devem ser vistos como uma base para o fortalecimento da resiliência, e não como substitutos das capacidades internas das organizações.

O que isso significa? Para as organizações que operam na América Latina, a conformidade regulatória, por si só, não equivale à segurança. A resiliência operacional depende da capacidade interna de detecção, da prontidão para responder a incidentes, da governança sobre identidades e ambientes em nuvem e da capacidade de coordenar rapidamente as partes interessadas das áreas jurídica, técnica e executiva.

Conclusão

O panorama das ameaças cibernéticas na América Latina já não é definido principalmente por campanhas altamente visíveis, centradas na exploração de vulnerabilidades e no uso de malware. A região enfrenta atualmente um ambiente mais diversificado, no qual o roubo de credenciais, o uso indevido de SaaS, os infostealers, a extorsão baseada em nuvem e a persistência discreta ocupam posição central tanto no cibercrime quanto nas atividades de invasão com objetivos estratégicos.

Três prioridades se destacam para os líderes de segurança. A primeira é reduzir a exposição de identidades por meio de uma proteção mais robusta das credenciais, do monitoramento do uso indevido de contas e de um controle mais eficaz sobre contas privilegiadas e contas de serviço. A segunda é ampliar a visibilidade sobre atividades em ambientes SaaS, na nuvem e em ferramentas de administração remota, permitindo que as táticas utilizadas após o acesso inicial sejam detectadas antes de resultar em perda de dados ou extorsão. A terceira é fortalecer a prontidão organizacional por meio do planejamento de resposta baseado em cenários, especialmente para comprometimentos decorrentes de phishing, preparação para ransomware e movimentação suspeita de dados.

Para os líderes de segurança na América Latina, a prioridade não é apenas fortalecer a defesa, mas adaptar-se à forma como os ataques ocorrem atualmente. O comprometimento de identidades, o uso indevido de SaaS e a persistência discreta definem o ambiente operacional. As organizações capazes de identificar anomalias comportamentais precocemente, reduzir a exposição de credenciais e responder rapidamente a atividades pós-comprometimento estarão mais bem posicionadas para gerenciar os riscos na região.

Apêndice

O apêndice apresenta detalhes técnicos que servem de base para os estudos de caso selecionados e discutidos no relatório principal.

■ Apêndice A.

Análise do Malware Associado à Fraude do “Tribunal Colombiano”

Nesse caso, o agente de ameaça disfarçou o malware como uma notificação judicial colombiana legítima denominada “Radicado Judicial.pdf.lnk”. O arquivo de atalho iniciou o PowerShell de forma silenciosa, contornou as restrições de execução e criou um mecanismo de preparação baseado em HTA na pasta temporária. Em seguida, a cadeia de ataque utilizou uma técnica de download semelhante ao wget para obter um arquivo remoto adicional e executá-lo por meio do mshta.exe.

O componente HTA exibiu uma notificação judicial falsa, enquanto o VBScript instalava, em segundo plano, uma carga útil oculta do PowerShell. A carga útil analisava o sistema da vítima, coletava informações sobre o host e o antivírus e estabelecia persistência por meio de tarefas agendadas, mecanismos de inicialização e chaves do Registro do Windows. A chave de Registro “iRaNKfje” e uma tarefa agendada denominada “qbbxljYk” foram utilizadas para manter a execução.

Posteriormente, o malware estabeleceu comunicação com a infraestrutura de C2 em love.negro[.]ink, enviando informações do sistema e solicitando repetidamente novas instruções. As funcionalidades disponíveis incluíam a execução de comandos PowerShell, o envio e a execução de arquivos adicionais, a coleta de informações sobre janelas ativas, o download de conteúdo remoto e a autorremissão. O uso de um user-agent personalizado, de solicitações HTTP POST direcionadas a um endpoint não padrão e da identificação do host indicava fortemente uma atividade de comando e controle, em vez de um comportamento legítimo de usuário ou aplicação.

Entre os indicadores selecionados associados às organizações colombianas comprometidas estavam os endereços 45.83.31[.]136, 172.94.9[.]23 e love.negro[.]ink:4448. O caso demonstra a eficácia contínua de campanhas de phishing com temáticas jurídicas e administrativas altamente adaptadas ao contexto local, combinadas com execução baseada em scripts e mecanismos de persistência simples, porém eficazes.

■ Apêndice B.

Análise do Malware SnappyBee / DEEDRAT

O SnappyBee é composto por uma DLL carregadora e por um arquivo de dados criptografado associado, que contém o código malicioso. Ele é frequentemente executado por meio de DLL sideloading em aplicações legítimas e assinadas, incluindo softwares relacionados a produtos de segurança, com o objetivo de reduzir a visibilidade da execução maliciosa. Entre os nomes de amostras observadas estão DgApi.dll e ImfsbDLL.dll.

Quando carregada, a DLL utiliza a funçãoDllMain para interceptar StartServiceCtrlDispatcherW e redirecionar a execução para o carregador. Uma vez ativado, o malware localiza um arquivo de dados, como o dbindex.dat, aloca memória para seu conteúdo, descriptografa o shellcode utilizando RC4, marca a região de memória como executável e inicia um processo de descompactação em múltiplas etapas. Nos estágios posteriores, as funções da API são resolvidas por meio de uma varredura do PEB baseada em hash, evitando o armazenamento direto de nomes de funções sensíveis e dificultando a análise.

A carga útil principal, então, descriptografa e carrega na memória funcionalidades semelhantes a plug-ins, estabelecendo comunicações de C2 e fornecendo ao operador amplo controle sobre o host comprometido. Em campanhas relatadas anteriormente, o Salt Typhoon utilizou o SnappyBee para manter a persistência e implantar ferramentas adicionais, como o DEMODEx. O caso brasileiro destacado neste relatório demonstra a relevância dessa técnica para setores estratégicos da América Latina e para ambientes com infraestrutura de borda exposta.

Blind Eagle – Indicadores selecionados e Táticas, Técnicas e Procedimentos (TTPs)

Os indicadores selecionados incluíram o user-agent Microsoft-Web-DAV-MiniRedir/10.0.19045, o endereço IP 62[.]60[.]226[.]112, o caminho da carga útil hxxp[://62[.]60[.]226[.]112/file/3601_2042.exe, o endpoint de DNS dinâmico 21ene[.]ip-ddns[.]com e o nome de host diciembrenotasenclub[.]longmusic[.]com.

As TTPs observadas e reportadas incluíram comprometimento por drive-by, exploração de aplicações expostas ao público, anexos de spear phishing, execução de Visual Basic e PowerShell, comunicação com domínios e endereços IP incomuns, utilização de portas não padrão, transferência de ferramentas de acesso inicial, comportamento de geração de domínios, mascaramento (masquerading), exfiltração por meio de canais de C2 e exfiltração para serviços de armazenamento de texto ou plataformas em nuvem.

Perspectivas sobre a Detecção Proativa de Ameaças

O esforço de detecção de ameaças da Darktrace para este relatório concentrou-se em duas abordagens complementares: a criação de perfis orientados por atores de ameaça, utilizando o Modelo Diamante de Análise de Intrusão (Diamond Model of Intrusion Analysis), e buscas baseadas em hipóteses construídas em torno de TTPs recorrentes, padrões comportamentais esperados e infraestrutura conhecida. O objetivo não foi produzir dossiês exaustivos sobre os atores analisados, mas verificar se os relatórios públicos e as observações anteriores da Darktrace se refletiam em atividades reais e relevantes para a região observadas em toda a base de clientes.

BLIND EAGLE (APT-C-36)

Hipótese: O Blind Eagle continuaria utilizando e-mails de phishing e arquivos isca que, em última instância, instalam VBScript, PowerShell e mecanismos de acesso baseados em RAT, utilizando infraestrutura de DNS dinâmico e canais comuns de comando e controle (C2) para facilitar a persistência e a exfiltração de dados.

Procedimento: A Darktrace combinou indicadores conhecidos, convenções esperadas de nomenclatura de arquivos, infraestrutura de DNS dinâmico e a lógica da Linguagem de Consulta de Eventos (Event Query Language - EQL) para identificar comportamentos recorrentes na cadeia de ataque em toda a base de clientes. Modelos existentes da Darktrace também foram utilizados para destacar tarefas agendadas suspeitas, downloads de malware e conexões de saída incomuns.

Nossas observações: a Darktrace identificou comunicações recorrentes com infraestruturas associadas ao Remcos e diversos endpoints de DNS dinâmico vinculados a padrões conhecidos de VBScript.

Duas cadeias completas de ataque incluíram exfiltração para endpoints do paste[.]ee, enquanto outros casos apresentaram comportamentos em estágios iniciais ou intermediários fortemente alinhados às técnicas utilizadas pelo grupo Blind Eagle ao longo de 2025 e no início de 2026.

Importância: As descobertas reforçam a persistência de cadeias de invasão baseadas em phishing na América Latina e demonstram como ferramentas de baixo custo podem ser reutilizadas em larga escala em diferentes setores e países. Para os defensores, o sucesso contínuo dessas técnicas destaca a necessidade de monitorar a execução de scripts, a criação de tarefas agendadas, conexões de saída incomuns e comportamentos anômalos relacionados ao download de arquivos por parte dos usuários.

EARTH ALUX

Hipótese: O Earth Alux exploraria sistemas vulneráveis expostos à internet, utilizaria métodos de execução de baixo ruído e mecanismos de comando baseados em nuvem e, posteriormente, realizaria a exfiltração de dados por meio de armazenamento controlado pelo invasor ou de canais ocultos.

Procedimento: devido à quantidade limitada de indicadores disponíveis publicamente, a Darktrace adotou uma abordagem baseada em TTPs, com uso reduzido de IOCs, focando em atividades suspeitas relacionadas a sistemas expostos à internet, conectividade externa incomum, possíveis infraestruturas de comando e controle (C2) e exfiltração para destinos de armazenamento em nuvem.

Nossas observações: A investigação priorizou padrões comportamentais em vez de uma assinatura específica associada a um único agente de ameaça, refletindo a forma como atores avançados reduzem sua dependência de infraestruturas fixas. O foco no comportamento continua sendo a abordagem mais adequada para identificar campanhas mais furtivas que exploram sistemas expostos e serviços legítimos.

Importância: A relevância do Earth Alux para a América Latina está diretamente relacionada ao seu modelo operacional: exploração de infraestrutura exposta, seguida de persistência discreta e exfiltração por meio da nuvem. Esse modelo se aplica diretamente a organizações da região que expandem seus serviços voltados para a internet sem realizar investimentos equivalentes em monitoramento e capacidades de detecção em ambientes de nuvem.

APLICAÇÕES DE IA GENERATIVA E AGENTIVA

Hipótese: Atores maliciosos poderiam experimentar assistentes de IA com capacidades de navegação na web ou recuperação de informações como canais encobertos de comunicação, permitindo que informações sensíveis fossem incorporadas a solicitações estruturadas e que instruções dos invasores fossem transmitidas de forma indireta.

Procedimento: A Darktrace mapeou a cadeia de ataque descrita publicamente como "IA como proxy de C2" para comportamentos prováveis de rede e de plataforma. Em seguida, utilizou a Linguagem de Consulta de Eventos (Event Query Language - EQL) e a lógica de seus modelos para identificar acessos suspeitos a serviços de IA, como OpenAI, Perplexity, DeepSeek, Copilot, Gemini, Claude, Grok, Janitor AI e Flow XO, quando esses acessos estavam associados a indicadores de beaconing, comportamentos semelhantes a algoritmos de geração de domínios (DGA) ou sinais de exfiltração de dados.

Nossas observações: a investigação concentrou-se em combinações incomuns entre acessos de saída para serviços de IA e outros indicadores sugestivos de atividades de C2 ou de exfiltração de dados em múltiplas etapas. Trata-se de uma área emergente, mas cada vez mais relevante à medida que as plataformas de IA passam a ser utilizadas de forma rotineira em ambientes corporativos.

Importância: Mesmo que essas técnicas ainda estejam em estágio exploratório, o uso de IA para apoiar atividades de C2 demonstra como invasores podem ocultar comunicações maliciosas em serviços legítimos, reduzindo ainda mais a relação sinal-ruído para as equipes de defesa. Organizações que já permitem o uso amplo de ferramentas de IA precisam de maior contexto sobre quem utiliza determinados serviços, com que frequência e em que sequência essas interações ocorrem em relação a outros comportamentos suspeitos.

Bibliografia

- [1] [Online]. Available: <https://edgeuno.com/2026-connectivity-ai-edge/>
- [2] [Online]. Available: <https://identitymanagementinstitute.org/identity-threats-reshaping-cybersecurity/>
- [3] [Online]. Available: <https://diesec.com/2026/04/legitimate-tool-abuse>
- [4] [Online]. Available: <https://www.darkreading.com/threat-intelligence/latin-americas-cyber-maturity-lags-threat-landscape>
- [5] [Online]. Available: <https://www.crowdstrike.com/en-us/blog/2025-latam-threat-landscape-report-deep-dive>
- [6] [Online]. Available: <https://www.recordedfuture.com/research/latin-america-and-the-caribbean-cybercrime-landscape>
- [7] [Online]. Available: <https://www.csis.org/analysis/chinas-expanding-interests-latin-america-development-leverage-coercion-and-crime>
- [8] [Online]. Available: <https://privatebank.jpmorgan.com/latam/en/insights/markets-and-investing/ideas-and-insights/the-cybersecurity-imperative-latin-americas-challenge-and-opportunity>
- [9] [Online]. Available: <https://blog.checkpoint.com/security/securing-latin-america-in-2025-how-ai-and-cyber-threat-intelligence-are-reshaping-the-cyber-security-landscape>
- [10] [Online]. Available: <https://www.redgealc.org/contenido-general/noticias/colombia-realizo-cumbre-de-inteligencia-artificial>
- [11] [Online]. Available: <https://www.redgealc.org/contenido-general/noticias/idforo>
- [12] [Online]. Available: <https://www.redgealc.org/contenido-general/noticias/se-presentaron-avances-de-idlac-en-washington-dc>
- [13] [Online]. Available: <https://www.galileo-ft.com/blog/whats-driving-colombias-fintech-revolution-in-2025-data-driven-market-analysis>
- [14] [Online]. Available: <https://alcor.com/software-development-colombia>
- [15] [Online]. Available: <https://www.trade.gov/country-commercial-guides/colombia-information-and-communication-technology-ict>
- [16] [Online]. Available: <https://www.datacubereseach.com/colombia-cloud-computing-market>
- [17] [Online]. Available: <https://www.ventasdeseguridad.com/en/news/latest-news/431-enterprises/25510-colombia-accounts-for-one-out-of-every-four-cyberattacks-in-latin-america.html>
- [18] [Online]. Available: <https://blog.checkpoint.com/research/the-growing-danger-of-blind-eagle-one-of-latin-americas-most-dangerous-cyber-criminal-groups-targets-colombia>
- [19] [Online]. Available: <https://thehackernews.com/2025/08/blind-eagles-five-clusters-target.html>
- [20] [Online]. Available: <https://www.kiteworks.com/cybersecurity-risk-management/latin-america-cyber-threat-landscape-2026-intel-471-report>
- [21] [Online]. Available: <https://www.ibm.com/think/insights/unveiling-latest-banking-trojan-threats-latam>
- [22] [Online]. Available: <https://accesspartnership.com/opinion/access-alert-colombia-releases-national-digital-strategy-2023-2026>
- [23] [Online]. Available: <https://www.trade.gov/country-commercial-guides/colombia-digital-economy>
- [24] [Online]. Available: <https://www.trade.gov/country-commercial-guides/chile-information-technologies>
- [25] [Online]. Available: <https://thehackernews.com/2025/05/horabot-malware-targets-6-latin.html>
- [26] [Online]. Available: <https://www.trade.gov/market-intelligence/chile-information-technology-new-cybersecurity-framework-law>
- [27] [Online]. Available: <https://alcor.com/overview-of-the-technology-industry-in-mexico/>
- [28] [Online]. Available: <https://alcor.com/outsourcing-to-latin-america/>

-
- [29] [Online]. Available: <https://mexicobusiness.news/cybersecurity/news/many-mexican-firms-hit-supply-chain-cyberattacks-kaspersky>
- [30] [Online]. Available: <https://mexicobusiness.news/cybersecurity/news/mexico-unveils-national-cybersecurity-plan-2025-2030>
- [31] [Online]. Available: <https://mexicobusiness.news/cybersecurity/news/mexico-mandates-zero-trust-across-federal-agencies>
- [32] [Online]. Available: <https://investmentpolicy.unctad.org/investment-policy-monitor/measures/4930/launches-the-brazilian-artificial-intelligence-plan-2024-2028>
- [33] [Online]. Available: <https://www.itic.org/news-events/techwonk-blog/realizing-brazils-ai-ambition-through-futureproof-regulation>
- [34] [Online]. Available: <https://blog.equinix.com/blog/2025/05/07/the-digital-pulse-of-latin-america-brazils-rise-as-a-global-tech-innovator>
- [35] [Online]. Available: <https://blog.lacnic.net/en/the-perfect-storm-the-largest-cyberattack-on-brazils-financial-system>
- [36] [Online]. Available: <https://www.forbes.com/sites/angelicamarideoliveira/2023/09/27/brazil-is-the-worlds-second-most-vulnerable-country-to-cyberattacks>
- [37] [Online]. Available: <https://socradar.io/wp-content/uploads/2024/10/SOCRadar-Brazil-Threat-Landscape-Report-2024.pdf>
- [38] [Online]. Available: <https://medium.com/aardvark-infinity/comprehensive-list-of-brazilian-apt-groups-4cfbec72a1d6>
- [39] [Online]. Available: <https://www.mattosfilho.com.br/en/unico/cybersecurity-strategy-decree>
- [40] [Online]. Available: <https://digi-tracker.com/regulations/national-cybersecurity-policy-pnciber/?format=pdf&content-Lang=eng-GB&v=1>
- [41] [Online]. Available: <https://iclg.com/practice-areas/data-protection-laws-and-regulations/brazil>
- [42] [Online]. Available: <https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/brazil>
- [43] [Online]. Available: <https://www.trade.gov/country-commercial-guides/ecuador-digital-economy>
- [44] [Online]. Available: <https://www.bnamerica.com/en/features/spotlight-ecuadors-new-digital-transformation-policy>
- [45] [Online]. Available: <https://freedomhouse.org/country/ecuador/freedom-net/2024>
- [46] [Online]. Available: <https://www.dexpose.io/tengu-ransomware-targets-anfibius-in-ecuador>
- [47] [Online]. Available: <https://appcheck-ng.com/ecuador-citizens-data-leak>
- [48] [Online]. Available: https://link.springer.com/chapter/10.1007/978-981-96-8563-9_44
- [49] [Online]. Available: <https://eandt.theiet.org/2019/04/17/ecuador-faced-40-million-ddos-attacks-after-assange-arrest>
- [50] [Online]. Available: <https://database.cyberpolicyportal.org/entity/v939ugxukzg?file=1658911956789x9ant1tq6k.pdf&page=1>
- [51] [Online]. Available: <https://www.telecomunicaciones.gob.ec/el-gobierno-nacional-presento-la-estrategia-nacional-de-ciberseguridad>
- [52] [Online]. Available: <https://www.dlapiperdataprotection.com/index.html?t=law&c=EC>
- [53] [Online]. Available: <https://www.centerforcybersecuritypolicy.org/insights-and-research/bridging-the-cybersecurity-gap-in-latam-how-isacs-enhance-regional-cooperation>
- [54] [Online]. Available: <https://www.weforum.org/stories/2024/05/latin-america-cybersecurity-report-ransomware-attacks>
- [55] S. Smart, Business, Human Rights, Technology, and Transitional Justice in Latin America: Tracing Connections, Palgrave Macmillan, 2025.
- [56] [Online]. Available: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026_Regional_Analysis_Latin-America_and_the_Caribbean.pdf
- [57] [Online]. Available: https://api.gcforum.org/api/files/public/upload/39c147e6-27f2-418c-99ea-c5a1890a0c8b_Bridging-the-Gender-Gap-in-Cybersecurity.pdf
- [58] [Online]. Available: <https://iapp.org/news/a/brazils-lgpd-now-in-effect-what-does-this-mean-for-enforcement>
- [59] [Online]. Available: <https://blog.checkpoint.com/research/latin-america-sees-sharpest-rise-in-cyber-attacks-in-december-2025-as-ransomware-activity-accelerates/>
- [60] [Online]. Available: <https://fpf.org/blog/chiles-new-data-protection-law-context-overview-and-key-takeaways>

■ **Sobre a Darktrace**

Darktrace é líder global em IA para cibersegurança e ajuda as organizações a se manterem à frente de um cenário de ameaças em constante evolução. Fundada em 2013 em Cambridge, Reino Unido, Darktrace fornece uma plataforma essencial de cibersegurança para proteger organizações contra ameaças desconhecidas por meio de IA que aprende, em tempo real, com o comportamento específico de cada empresa. A plataforma e os serviços da Darktrace contam com o suporte de 2.300 empregados e protegem cerca de 10.000 clientes em todo o mundo. Para saber mais, visite o site da Darktrace: darktrace.com.