SECURITY REPORT

AMÉRICA LATINA (EDIÇÃO 2025)

Panorama do estado atual da cibersegurança corporativa na América Latina: ameaças, vulnerabilidades, práticas e níveis de preparação diante de um ambiente sempre desafiador.

Progress. Protected.

Conteúdo

Sobre o ESET Security Report

O **ESET Security Report (ESR)** é um relatório anual elaborado pela ESET que oferece uma visão geral do estado da segurança nas empresas da América Latina, incluindo o Brasil.

Este documento baseia-se em pesquisas realizadas com 3.034 profissionais que trabalham em organizações de diversos setores em 15 países da região. A maioria dos entrevistados ocupa cargos na área de TI ou em áreas relacionadas à cibersegurança.

As informações extraídas da telemetria da ESET durante 2024 permitem contextualizar a percepção dos entrevistados sobre a atividade maliciosa detectada durante o último ano na América Latina.

O relatório aborda aspectos-chave revelados pelos questionários aplicados, como: a quantidade de incidentes sofridos, as ameaças mais ativas do último ano, a situação do ransomware na região, o grau de satisfação com o orçamento destinado à cibersegurança, as práticas de gestão mais frequentes, as principais preocupações em segurança digital e as medidas mais adotadas.

O **ESR 2025** oferece uma visão regional sobre a segurança digital das organizações, com o objetivo de contribuir para o fortalecimento da conscientização sobre a importância da cibersegurança para as empresas da América Latina.

27%

das organizações afirmaram ter sofrido um ciberataque no último ano

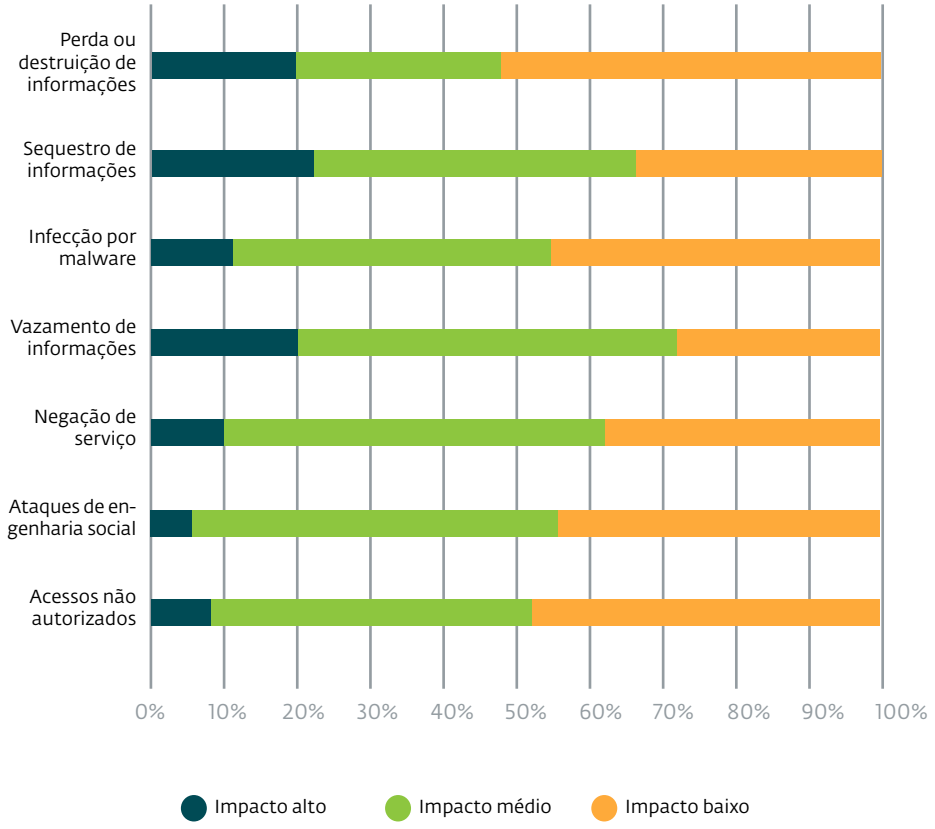
Embora isso represente uma queda de 3% em relação ao ano anterior, isso não se traduz necessariamente em menos ciberataques no âmbito corporativo. A realidade é que, entre as organizações entrevistadas que não detectaram tentativas de ciberataques, 2 em cada 5 também acreditam não ter tecnologia suficiente para ter certeza disso. Em outras palavras, 32% dos entrevistados não têm visibilidade suficiente para afirmar ou negar se sofreram um ciberataque em sua organização, e um subconjunto deles provavelmente foi vítima sem saber. A visibilidade é um aspecto-chave em cibersegurança: não é possível proteger o que está fora do alcance das ferramentas de proteção, sejam elas tecnológicas ou humanas.

No Brasil, o percentual obteve um número semelhante, já que 25% das organizações afirmaram ter sofrido em um ciberataque no último ano.

Prejuízos à informação: os ciberataques com maior impacto

20% dos entrevistados que afirmaram ter sofrido sequestro, destruição ou vazamento de informações relataram um impacto negativo alto para a organização à qual pertencem. Essas organizações também sofreram consequências legais, perdas financeiras e até rompimento de contratos.

Ao contrário dos prejuízos físicos, a informação pode ser copiada, vendida ou apagada com facilidade, o que a torna um alvo atrativo para cibercriminosos, seja por lucro, espionagem ou sabotagem. Além disso, o impacto desses incidentes nem sempre é imediato. Em muitos casos, o verdadeiro prejuízo só se revela com o tempo. Uma organização pode saber que sofreu um vazamento, mas não saber como suas informações foram utilizadas. Se, mais tarde, um cliente ou parceiro comercial descobrir que seus dados foram comprometidos, isso pode gerar prejuízos financeiros e reputacionais, além de ações legais contra a empresa afetada.



Famílias de malware mais detectadas

Com base na telemetria da ESET, na América Latina identificamos as seguintes famílias como as principais detectadas:

Expiro (5,29%)

Expiro é um malware do tipo infostealer com capacidades de backdoor, que geralmente se propaga por meio de executáveis infectados. É usado para roubar informações sensíveis do sistema, como credenciais e dados do navegador, além de permitir o controle remoto do dispositivo comprometido.

Ramnit (3,41%)

Ramnit (também conhecido como Nimnul) é um trojan de acesso remoto (RAT) que se propaga principalmente por meio de arquivos executáveis e documentos maliciosos do Office. Pode roubar informações, registrar pressionamentos de tecla e permitir que os atacantes controlem remotamente o sistema infectado, podendo inclusive adotar capacidades de botnet.

Zurgop (2,04%)

Zurgop é um RAT com capacidades avançadas de espionagem e controle remoto. É distribuído via campanhas maliciosas por e-mail e pode roubar informações sensíveis, gravar áudio, capturar a tela e operar o dispositivo comprometido de forma encoberta.

Famílias de malware mais detectadas no Brasil

Também com base na telemetria da ESET, no Brasil identificamos as seguintes famílias como as mais detectadas:

Guildma (1,80%)

Guildma é uma família de trojans bancário de origem brasileira, especializada em roubar credenciais de acesso a bancos, e-mails e outros serviços online, principalmente por meio de campanhas de phishing e técnicas de engenharia social. É conhecida por evoluir constantemente, adicionar novas funcionalidades e visar vítimas na América Latina e em outros países.

Kryptik (1,65%)

Kryptik é uma família de trojans usada para distribuir e instalar outros malwares nos sistemas das vítimas, frequentemente utilizando técnicas de ofuscação para evitar a detecção por antivírus. Costuma ser empregada em ataques para roubo de dados, controle remoto e execução de cargas maliciosas diversas.

Zurgop (1,18%)

Assim como ocorre na América Latina (citamos anteriormente), essa família também tem recursos que empregam técnicas para evitar detecção e garantir persistência no sistema.

Vulnerabilidades mais detectadas

As vulnerabilidades são resultado de erros de programação ou de configuração em peças de software dos mais diversos tipos. Ao contrário dos vetores de infecção baseados em engenharia social, as vulnerabilidades, por serem pontos de entrada, não exigem interação dos usuários e, portanto, são menos propensas a serem detectadas sem uma abordagem reativa.

Na América Latina, há uma tendência que se consolida a cada ano: as vulnerabilidades mais exploradas têm muitos anos de existência, chegando a ter mais de uma década em alguns casos, e já contam com correções disponibilizadas pelos fabricantes. Isso indica que o problema não está na quantidade ou gravidade das vulnerabilidades, mas sim na falta de aplicação dos patches disponíveis, seja por desconhecimento ou pela falta de pessoal capacitado.

Especificamente, as vulnerabilidades mais exploradas segundo a telemetria da ESET na América Latina em 2024 são:

CVE-2012-0143

Vulnerabilidade no Microsoft Excel que permite a execução remota de código arbitrário, que pode ser malicioso. Em 2017, a família de ransomware DoppelPaymer usou essa vulnerabilidade em campanhas na América Latina.

CVE-2012-0159

Vulnerabilidade no Microsoft Windows que também permite acesso remoto sem necessidade de autenticação ao sistema vulnerável. A falha foi descoberta em 2012 e foi usada, por exemplo, em campanhas de ransomware icônicas como as do Petya e NotPetya anos depois.

CVE-2016-3316

Vulnerabilidade em versões antigas do Microsoft Word para sistemas Mac e Windows, que permite executar código arbitrário via criação de um documento malicioso.
Esse tipo de ataque pode ser feito por e-mail, enganando a vítima a abrir o arquivo. Ao ser aberto, o código é executado sem o conhecimento do usuário.

CVE-2021-26855

Vulnerabilidade no Microsoft Exchange que explora funcionalidades de conexões HTTPS do servidor para autenticar usuários externos (potencialmente maliciosos). Foi noticiada em 2021, quando foi usada em sua versão Zero-Day em campanhas contra empresas de alto nível no mundo todo.

CVE-2017-11882

Vulnerabilidade no Microsoft Office e no Microsoft Wordpad, similar à CVE-2016-3316, explorada com a criação de arquivos com características específicas. É usada por cibercriminosos para distribuir diversos tipos de malware, como o Agent Tesla e outros trojans de acesso remoto.

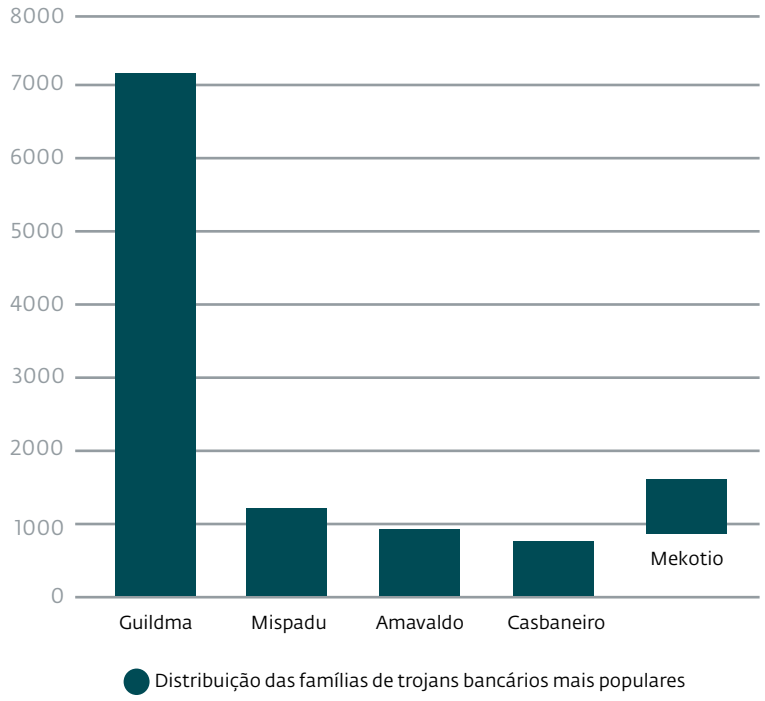
Trojans bancários: presença constante na América Latina

A presença de trojans bancários na América Latina se mantém constante ao longo do tempo, com períodos de maior e menor atividade, mas sem desaparecer do panorama de ameaças. As famílias mais detectadas na região, considerando a quantidade de arquivos únicos associados, são Guildma e Mispadu, ambas superando amplamente os mil arquivos identificados. Em seguida vêm Amavaldo, Casbaneiro e Mekotio, que também apresentam forte presença, mas com menor volume.

Esses trojans têm como foco principal o roubo de credenciais bancárias, utilizando técnicas de phishing, sobreposição de janelas e controle remoto do dispositivo.
Sua disseminação normalmente ocorre por meio de campanhas maliciosas por e-mail, instaladores falsos e downloads disfarçados de sites comprometidos. Apesar de ações de desarticulação e campanhas de conscientização, essa atividade segue como uma das mais persistentes da América Latina.

O Brasil lidera o ranking de detecções de trojans bancários na América Latina, concentrando **61% dos casos registrados** entre todos os países.

Arquivos únicos associados às famílias de trojans bancários mais populares



22%

das organizações afirmaram ter sofrido um ataque de ransomware nos últimos dois anos

O ransomware continua sendo uma das ameaças mais temidas por seu alto impacto, apesar de ser um dos tipos de malware com menor número de arquivos únicos associados, pouco mais de 15.000 em toda a região em 2024, muito abaixo de outras categorias como trojans ou spyware. Sua notoriedade não está no volume, mas sim nos danos que causa: interrupções operacionais, perdas econômicas e exposição de informações sensíveis.

Nos últimos anos, consolidou-se também uma tendência de mudança na seleção das vítimas. Em vez de campanhas massivas direcionadas a milhares de usuários individuais, os atacantes agora miram alvos corporativos específicos para maximizar o dano e o lucro econômico. Essa estratégia, conhecida como big game hunting, combina a extorsão pelo sequestro de dados com a ameaça de vazamento, transformando cada incidente em uma crise potencial para a organização vítima, que vai muito além da simples perda de dados.

No Brasil, o percentual de organizações que afirmam ter sofrido um ataque de ransomware no mesmo período **é ainda mais alto: 29%**.

Grande preocupação, mas pouca preparação

95%

dos entrevistados afirmaram sentir preocupação especial com o ransomware como ameaça cibernética: o que não surpreende, considerando o impacto financeiro e operacional que esses ataques podem causar em uma organização.

No entanto, a adoção de tecnologias e práticas-chave para prevenir uma infecção ou minimizar suas consequências continua baixa. Menos da metade das organizações entrevistadas afirma aplicar soluções como Data Loss Prevention (DLP), tecnologias de criptografia ou práticas de classificação da informação. A única exceção notável é o backup de dados, com 85% de adoção, o que sugere que o foco corporativo ainda está mais voltado para recuperação do que para prevenção.

Isso deixa uma lacuna significativa de segurança, especialmente considerando o quão dinâmico e desafiador é o mundo das ameaças digitais.

No Brasil, o cenário foi semelhante ao de outros países da América Latina: **94% dos entrevistados demonstraram preocupação** com a possibilidade de um ataque de ransomware.

O ransomware na América Latina

Em 2024, o ransomware esteve por trás de numerosos ataques na América Latina. Universidades, centros de saúde, empresas e órgãos governamentais da Argentina, Brasil, Chile, Colômbia, México, Peru, entre outros, foram alvo de algum grupo de ransomware.

Entre os grupos mais ativos do ano, destacam-se: LockBit 3.0, Vice Society, ALPHV (BlackCat), Medusa. No entanto, o grupo com maior protagonismo foi o RansomHub, que, desde seu surgimento no início do ano, conseguiu atingir mais de 200 organizações em todo o mundo.

Também foi observada a atividade de grupos emergentes como Qiulong e Cactus, que direcionaram seus recursos e atenção para ataques na região.

72% das organizações ainda não contrataram um seguro contra riscos cibernéticos

A ausência de seguro cibernético na maioria das organizações entrevistadas revela uma vulnerabilidade significativa diante do crescimento constante das ameaças digitais. Embora o seguro não atue na prevenção de incidentes, ele é uma ferramenta importante para auxiliar na mitigação de impactos financeiros e operacionais após um incidente.

Ainda assim, é fundamental lembrar que seguros não substituem uma estratégia de cibersegurança robusta. A proteção proativa, baseada em prevenção, monitoramento e resposta rápida, continua sendo essencial para reduzir riscos e garantir a continuidade dos negócios.

No Brasil, o cenário é semelhante: **73% das organizações** ainda não contrataram um seguro contra riscos cibernéticos.

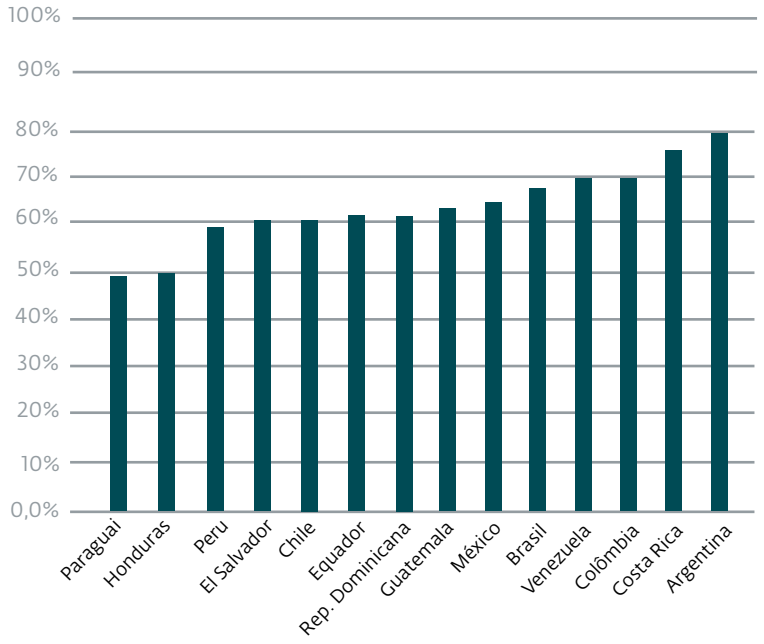
38%

das organizações não implementam uma solução antimalware centralizada

Embora as soluções antivírus ou antimalware estejam entre as três tecnologias mais adotadas, atrás apenas das soluções de firewall (88%) e backup (85%), o percentual de uso ainda é considerado baixo.

Entre os países com menor taxa de adoção de antivírus centralizado estão: Paraguai (49,5%), Honduras (51%), Peru (58,5%).

Percentual de adoção de soluções antimalware centralizadas



Apenas 1 em cada 4 empresas protege os dispositivos móveis corporativos

Os dispositivos móveis corporativos são interessantes para cibercriminosos devido à quantidade de informações que armazenam e ao tratamento negligente que colaboradores e empresas costumam dar à cibersegurança desses dispositivos.

As ameaças, nesse caso, se manifestam por meio de e-mails maliciosos visualizados em telas menores que as de computadores, aplicativos maliciosos disponíveis em lojas oficiais e até **instaladores web, como PWAs, acionados por pop-ups que passam despercebidos.**

Ferramentas de Threat Intelligence: as menos adotadas

Apenas 19% das organizações entrevistadas afirmaram utilizar alguma ferramenta de inteligência de ameaças, desde feeds de notícias, listas atualizáveis em tempo real ou baseadas em regras, até bancos de dados e APIs interativas, gratuitas (inclusive algumas de código aberto) ou pagas.

Os cibercriminosos costumam direcionar suas campanhas a empresas com setores, tamanhos, países ou regiões semelhantes, por isso a coleta de informações é uma ferramenta valiosa de previsão. Observar sobreposições de táticas, técnicas e procedimentos usados nas ameaças cibernéticas mais frequentes atualmente permite às organizações realizarem uma análise interna de seu estado de proteção, considerando: as soluções implementadas, os procedimentos a seguir e as práticas de gestão a serem adotadas.
.

Acessos indevidos a sistemas e roubo de informação: as maiores preocupações das empresas

Mais da metade das organizações entrevistadas classificou os acessos não autorizados como a maior preocupação diante de possíveis ciberataques, com baixa dispersão nas respostas, o que indica um grande consenso sobre o risco que representam os cibercriminosos. Seja por credenciais comprometidas, erros de configuração ou ataques direcionados, os cibercriminosos podem obter acesso a infraestruturas e informações, comprometendo a segurança da organização.

O roubo de informação obteve uma média de 4,3 em 5 pontos no índice de preocupação das empresas entrevistadas, o que mostra que esse tipo de ameaça é visto como um risco significativo no mundo corporativo.

Essa preocupação se confirma com os dados: entre os que sofreram ataques desse tipo, 21,6% afirmaram que o roubo de informação teve alto impacto, sendo o ataque mais danoso entre os relatados.

Metade das organizações não possui um plano de continuidade de negócios

Apenas 47% das organizações entrevistadas afirmaram contar com um plano prático para recuperar e restaurar as operações em caso de uma interrupção, seja ela acidental ou intencional, como em um ciberataque. Isso é especialmente preocupante do ponto de vista econômico: além da perda de dados ou sistemas, a recuperação após um ataque pode facilmente ultrapassar centenas de milhares de dólares, entre o tempo de inatividade, recuperação, multas regulatórias e danos reputacionais. Sem um plano preparado, um único incidente pode comprometer a viabilidade econômica de uma empresa, especialmente em setores onde cada minuto de inatividade representa alto custo operacional.

1 em cada 4

empresas nunca realizou um pentest

Isso torna o pentesting um dos exercícios de cibersegurança menos praticados pelas organizações entrevistadas,ficando bem atrás de outras atividades, como a análise de vulnerabilidades. Além disso, entre as empresas que afirmaram realizar testes de intrusão regularmente, metade o faz apenas uma vez por ano. O pentesting é fundamental para identificar pontos de entrada vulneráveis, como falhas de configuração ou serviços expostos, antes que sejam explorados por cibercriminosos, permitindo a correção preventiva e o fortalecimento da segurança.

Treinamentos: uma necessidade ainda não consolidada

Menos da metade das organizações afirmou ter um plano estruturado de treinamento para seus colaboradores. Embora 31% realizem capacitações uma vez por ano e 29% o façam duas vezes por ano, essas ações geralmente são feitas de forma isolada, sem um foco estratégico contínuo.

Contar com um plano estruturado faz uma grande diferença. Esse tipo de abordagem envolve revisões periódicas, atualizações constantes de conteúdo e a adaptação dos treinamentos a novas ameaças e cenários. Ações pontuais, se não forem acompanhadas de monitoramento e avaliação, podem não atingir o mesmo nível de impacto.

A ESET® é uma empresa que oferece soluções de segurança digital de ponta para prevenir ataques.

Seu enfoque combina o poder da inteligência artificial com a experiência humana para antecipar-se às ameaças cibernéticas conhecidas e emergentes, protegendo empresas, infraestruturas críticas e pessoas. Seja para proteção de endpoints, nuvem ou dispositivos móveis, nossas soluções e serviços nativos de IA e baseados em nuvem são altamente eficazes e fáceis de usar. A tecnologia da ESET inclui: detecção e resposta robustas, criptografia ultrassegura e autenticação multifator.

Com defesa em tempo real 24 horas por dia, 7 dias por semana, e um forte suporte local, mantemos as pessoas protegidas e os negócios funcionando sem interrupções. Em um cenário digital em constante evolução, exigem-se abordagens progressivas em segurança digital, e a ESET assume esse compromisso. Além disso, oferece pesquisa de classe mundial, inteligência avançada contra ameaças e é respaldada por centros de pesquisa e desenvolvimento globais, incluindo a América Latina, com uma sólida rede global de parceiros comerciais.

Para saber mais, acesse https://www.eset.com/br/ ou siga-nos no LinkedIn, Facebook, Instagram.

Sobre a ESET

+ 110 milhões de usuários em todo o mundo

+ 500 mil clientes corporativos

11 centros de pesquisa e desenvolvimento no mundo

Presente em **200** países e territórios

ESET®

Digital Security
Progress. Protected.

esetbrasil @esetbr ESET Brasil