SECURITY REPORT
AMÉRICA LATINA 2024

12 dados
sobre o estado da cibersegurança das empresas da América Latina

20 ANOS
ESET LATAM

ESET Digital Security
Progress. Protected.

Sobre o ESET Security Report

O **ESET Security Report** (ESR) é um relatório anual produzido pela ESET que fornece uma visão geral do estado da segurança nas empresas da América Latina.

Este documento foi elaborado com base em pesquisas realizadas com 2.141 profissionais que trabalham em organizações de diversas áreas e em mais de dez países da América Latina, principalmente profissionais que ocupam cargos no setor de TI ou vinculados à segurança digital.

Além disso, o ESR 2024 complementa essas informações com dados extraídos da telemetria da ESET para o ano de 2023, o que permite contextualizar a percepção dos entrevistados em relação à atividade criminosa detectada pela ESET durante o último ano na América Latina.

Através da seleção dos dados mais relevantes obtidos pelos questionários aplicados, o relatório oferece uma visão a nível regional sobre a segurança das empresas, sem aprofundar em situações específicas, e aborda temas como a quantidade de incidentes de segurança que as empresas sofreram; as ameaças mais ativas durante o último ano; o estado do ransomware na América Latina; o grau de satisfação com o orçamento destinado à cibersegurança; as práticas de gestão mais adotadas; as preocupações em cibersegurança nas empresas e as medidas de segurança mais adotadas.

Esperamos que este relatório proporcione uma perspectiva sobre o estado da segurança digital a nível corporativo e contribua para melhorar a conscientização sobre a importância da cibersegurança para as empresas da América Latina.

Incidentes de segurança

30%

das organizações sofreram pelo menos um incidente de segurança em 2023

Além disso, 1 em cada 5 empresas na América Latina que afirmaram não terem sido afetadas por incidentes de segurança durante o último ano admitiram que não possuem a tecnologia necessária para garantir que não sofreram ataques. Isso sugere que existe um percentual de empresas que possivelmente foram alvo de ataques, mas não os detectaram.

Os setores que mais receberam tentativas de ataque foram órgãos governamentais, informática/tecnologia e bancos/finanças.

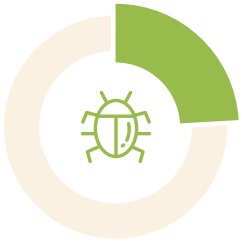
Quais foram as ameaças mais comuns na América Latina durante 2023?

Ao analisar os dados de telemetria da ESET e agrupar o total das detecções maliciosas registradas pela ESET em 2023 para a América Latina, observamos que o código malicioso com mais detecções corresponde a um **exploit** para a vulnerabilidade **CVE-2017-11882** no Microsoft Office.

Embora essa vulnerabilidade tenha sido corrigida há sete anos, ela continua sendo utilizada em campanhas que buscam distribuir malware na América Latina por meio de e-mails. Em 2023, observamos a existência de diversos exemplos de e-mails que circularam com documentos do Microsoft Office como anexos, utilizando técnicas de **e-mail spoofing**.

Essas campanhas foram registradas de forma contínua e, em muitos casos, propagavam malware multipropósito, como Trojans de Acesso Remoto (RAT, na sigla em inglês) como o Agent Tesla.

Os Trojans de Acesso Remoto (RAT) mais ativos na América Latina



Trojan.Win32/Ramnit

766869

Ramnit (24,1%)

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. Ele pode roubar informações, registrar teclas pressionadas e permitir que os cibercriminosos controlem remotamente o sistema infectado.

Backdoor.Win32/Rescoms

459604

Rescoms (14,4%)

Rescoms, também conhecido como Remcos, Remvio ou Socmer, é um RAT utilizado em campanhas de ciberespionagem. Ele pode coletar informações sensíveis, tirar capturas de tela e controlar a câmera e o microfone do dispositivo infectado.

Worm.Win32/Bundpil

215061

Bundpil (6,7%)

Bundpil é um RAT que se propaga principalmente por meio de anexos de e-mail maliciosos. Ele pode roubar credenciais, registrar teclas pressionadas e permitir que os cibercriminosos controlem o sistema afetado.

Worm.Win32/Phorpiex

198158

Phorpiex (6,2%)

Phorpiex (também conhecido como Trik) é um RAT que se propaga através de e-mails de spam e downloads de arquivos maliciosos. Ele pode roubar informações, se propagar para outros dispositivos e realizar ataques DDoS.

Backdoor.Win32/RanumBot

121006

RanumBot (3,6%)

RanumBot é um RAT que se propaga principalmente por meio de anexos de e-mail e links maliciosos. Ele pode roubar informações, registrar teclas pressionadas e permitir que os atacantes controlem o sistema afetado.

81% dos ataques com exploits visaram vulnerabilidades antigas no Office

As campanhas de malspam que utilizaram **exploits** com maior número de detecções na América Latina durante 2023 destacaram duas vulnerabilidades do Microsoft Office descobertas há vários anos e para as quais existe um patch disponível, como a CVE-2017-11882 (45%) e a CVE-2012-0143 (36%).

> **Essas duas vulnerabilidades representam 81% das detecções de exploits** e estão associadas a campanhas em massa que se propagam por e-mail com anexos.

Quais foram as vulnerabilidades mais exploradas?

A **CVE-2017-11882** é uma vulnerabilidade no editor de equações do Microsoft Office. A utilização de exploits pode permitir que um atacante execute código arbitrário no computador vulnerável.

A **CVE-2012-0143** afeta principalmente o Microsoft Excel 2003 SP3. Ela ocorre porque o Excel não gerencia adequadamente a memória ao abrir arquivos. Essa falha é explorada através de exploits que permitem a execução de código arbitrário por meio de uma planilha especialmente projetada para ser maliciosa.

Esses tipos de exploits podem instalar outras famílias de malware ou até mesmo assumir o controle total do sistema, especialmente se o perfil do usuário tiver permissões de administrador.

Os 20% restantes das detecções estão distribuídos entre as seguintes vulnerabilidades:

LNK/Exploit.CVE-2010-2568
82281

Win32/Exploit.CVE-2017-0199
51451

Win32/Exploit.CVE-2012-0159
32052

JS/Exploit.CVE-2021-26855
24781

Win32/Exploit.CVE-2023-21716
17862

Outras vulnerabilidades que ganharam destaque:

CVE-2010-2568

- **Descrição:** Esta vulnerabilidade afeta o Microsoft Windows e Microsoft Windows Server. Permite que um atacante local ou remoto execute código arbitrário através de arquivos de atalho (.LNK ou .PIF) maliciosos.
- **Impacto:** Pode resultar na execução de código não autorizado no sistema afetado.

CVE-2017-0199

- **Descrição:** Esta vulnerabilidade afeta o Microsoft Word. Permite que os atacantes baixem e executem scripts do PowerShell em máquinas comprometidas.
- **Impacto:** Fornece acesso adicional aos atacantes.

CVE-2012-0159

- **Descrição:** Esta vulnerabilidade afeta vários produtos da Microsoft, incluindo Windows, Office e Silverlight. Permite que atacantes remotos executem código arbitrário através de arquivos de fonte TrueType (TTF) manipulados.
- **Impacto:** Pode resultar na execução de código não autorizado no sistema afetado.

CVE-2021-26855

- **Descrição:** Esta vulnerabilidade afeta o Microsoft Exchange Server. Permite que os atacantes se autentiquem como o servidor Exchange e enviem solicitações HTTP arbitrárias.
- **Impacto:** Pode resultar na execução remota de código no servidor Exchange.

CVE-2023-21716

- **Descrição:** Esta vulnerabilidade afeta o Microsoft Word. Permite que os atacantes executem código remoto com os privilégios da vítima ao abrir um documento RTF malicioso.
- **Impacto:** Fornece acesso não autorizado ao sistema.

O que acontece com a exploração das vulnerabilidades mais recentes?

É lógico que os atacantes explorem em grande medida vulnerabilidades antigas para comprometer a segurança de usuários e empresas na América Latina. No entanto, os dados de telemetria da ESET indicam que também há detecções para vulnerabilidades mais recentes. Isso mostra que o cibercrime é composto por um ecossistema heterogêneo de criminosos prontos para explorar o amplo espectro de vulnerabilidades existentes, mesmo que isso envolva ataques mais sofisticados ou o desenvolvimento de novos exploits.

A seguir, alguns exemplos de vulnerabilidades corrigidas em 2022 e 2023 para as quais foram detectadas tentativas de exploração:

CVE-2022-26904: Vulnerabilidade crítica no Windows 10 e Windows Server que permite escalonamento de privilégios no sistema.

CVE-2022-21882: Vulnerabilidade no Windows 10 que também permite escalonamento de privilégios por um atacante.

CVE-2023-21608: Vulnerabilidade do tipo Use After Free no Adobe Acrobat Reader que pode permitir a execução de código arbitrário em um sistema comprometido.

CVE-2023-22515: Vulnerabilidade que afeta o Confluence Data Center e Server da Atlassian, permitindo que um atacante externo crie contas de administrador não autorizadas e acesse instâncias do Confluence, comprometendo a integridade e confidencialidade dos dados armazenados.

Essas vulnerabilidades representam riscos significativos e exigem atenção imediata para mitigar prejuízos potenciais.

Vulnerabilidades mais exploradas em sistemas operacionais diferentes do Windows

Top 3 de exploits para vulnerabilidades no Linux

Trojan.Linux/Exploit.CVE-2021-3493

- **CVE-2021-3493:** Afeta o kernel do Linux e permite que os atacantes executem código arbitrário através de BPF maliciosos.
- **Impacto:** Execução de código não autorizado.

Trojan.Linux/Exploit.CVE-2021-3490

- **CVE-2021-3490:** Afeta o kernel do Linux e permite que os atacantes executem código arbitrário através de eBPF.
- **Impacto:** Execução de código não autorizado.

Trojan.Linux/Exploit.CVE-2016-4557

- **CVE-2016-4557:** Afeta o kernel do Linux e o exploit permite que os atacantes obtenham privilégios ou causem negação de serviço.
- **Impacto:** Elevação de privilégios ou negação de serviço.

Top 3 de exploits para vulnerabilidades no Android

Trojan.Android/Exploit.CVE-2012-6636

- **CVE-2012-6636:** Afeta a API do Android e permite que os atacantes executem métodos arbitrários em objetos Java.
- **Impacto:** Execução de métodos arbitrários.

Trojan.Android/Exploit.CVE-2019-2215

- **CVE-2019-2215:** Afeta o Android e permite a elevação de privilégios de uma aplicação para o Kernel do Linux.
- **Impacto:** Execução de código com privilégios elevados.

Trojan.Android/Exploit.CVE-2016-5195

- **CVE-2016-5195:** Conhecida como "Dirty COW", a CVE-2016-5195 afeta o kernel do Linux e permite que os atacantes escrevam em mapeamentos de memória de apenas leitura.
- **Impacto:** Elevação de privilégios.

Top 3 de exploits para vulnerabilidades no OSx

Trojan.OSX/Exploit.CVE-2015-1130

- **CVE-2015-1130:** Afeta o Apple OS X e permite que usuários locais obtenham privilégios de administrador.
- **Impacto:** Elevação de privilégios.

Trojan.OSX/Exploit.CVE-2019-8565

- **CVE-2019-8565:** Afeta iOS e macOS e permite que um aplicativo malicioso obtenha privilégios de root.
- **Impacto:** Elevação de privilégios.

Trojan.OSX/Exploit.CVE-2018-4237

- **CVE-2018-4237:** Afeta iOS, macOS, tvOS e watchOS e permite que os atacantes ganhem privilégios através de um aplicativo manipulado.
- **Impacto:** Elevação de privilégios.

Ransomware

23%

das empresas foram alvo de pelo menos uma tentativa de ataque de ransomware nos últimos dois anos

Os setores que receberam mais tentativas de ataque de ransomware na América Latina foram Petróleo/Gás/Mineração (36%), Telecomunicações (31%), Serviços Públicos (30%) e Varejo/Atacado (29%).

Além disso, 96% das empresas e organizações da América Latina acreditam que o ransomware é uma ameaça preocupante.

86%

das empresas não estão dispostas a negociar o pagamento de um resgate

Embora 14% das empresas da América Latina tenham afirmado que estão dispostas a pagar um resgate, é importante lembrar que isso não garante a obtenção de uma ferramenta de descriptografia para recuperar os arquivos, nem que os dados roubados não serão publicados ou comercializados, nem que a reputação da organização não será afetada. Além disso, **pagar aos grupos de ransomware** contribui para o negócio do cibercrime e pode deixar a porta aberta para novas tentativas de ataque.

23%

das empresas têm contratado um seguro contra riscos cibernéticos

Relatórios recentes indicam que a demanda por seguros cibernéticos cresceu globalmente nos anos da pandemia devido ao aumento dos ciberataques, à implementação de novas regulamentações e ao crescimento das economias digitais. De qualquer forma, é importante lembrar que a segurança de uma empresa deve estar focada em tomar todas as precauções possíveis e em tornar a organização cada vez mais segura.

O que aconteceu com o ransomware durante 2023 na América Latina?

> O **ransomware continuou sendo uma ameaça muito ativa** a nível global e também a nível regional na América Latina durante 2023.

Nossos relatórios e os de outras organizações coincidem que houve um aumento significativo nesse período, em comparação a 2022.

Na América Latina, foram detectados vários casos de ataques de ransomware durante 2023 que foram perpetrados por diferentes grupos que operam sob o modelo de ransomware as a service (RaaS).

Durante esse período, observou-se o uso de novas táticas e tecnologias, bem como a consolidação de outras estratégias como a dupla extorsão. Por exemplo, observou-se a prevalência de dois métodos de infecção inicial nos ataques de ransomware na América Latina: o uso de commodity malware através de e-mails ou a exploração de vulnerabilidades zero-day. Além dessa tendência, os grupos de ransomware continuaram tentando acessar os sistemas corporativos através da exploração de vulnerabilidades conhecidas em serviços expostos à internet, erros de configuração ou através do uso de credenciais roubadas.

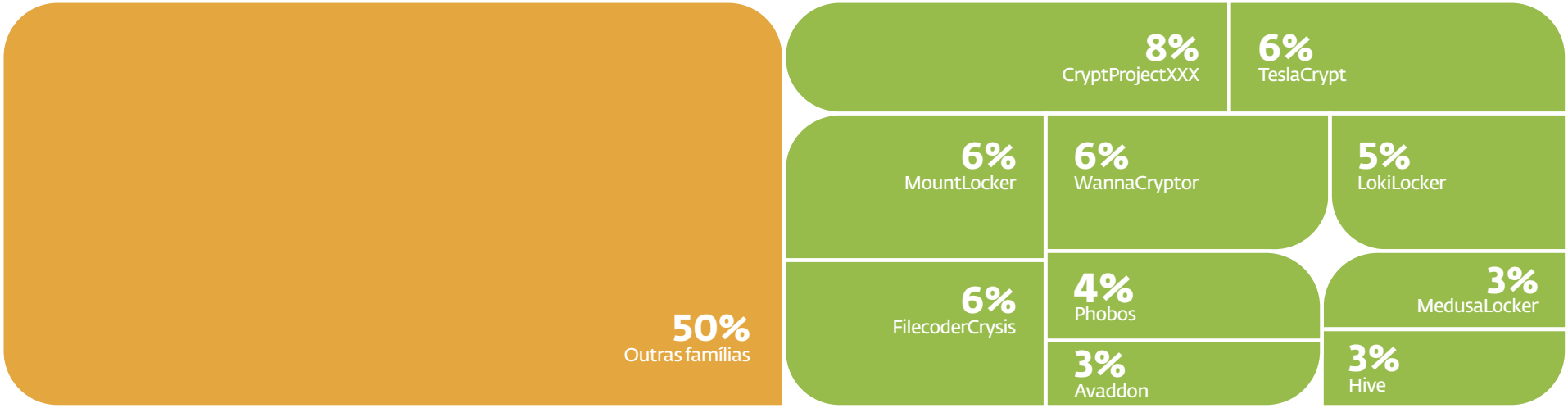
Outra das novas estratégias observadas em 2023 por parte dos grupos de ransomware foi o uso de malware do tipo wiper após o roubo e criptografia dos arquivos, e a implantação de outras variantes de ransomware durante um mesmo ataque.

Quais foram as 5 famílias de Ransomware com mais detecções na América Latina?

O ecossistema do ransomware é heterogêneo. Embora nos ataques de ransomware que mais atenção receberam observemos nomes de grupos de ransomware como LockBit, BlackCat, Clop ou Medusa, por citar alguns, é importante ter em mente que esses grupos utilizam longas cadeias de infecção e seus ataques costumam ser direcionados. Por essa razão, muitos ataques cujo objetivo final é a infecção com essas famílias de malware não são detectados nem vinculados a essas famílias porque são bloqueados pelas tecnologias da ESET em estágios mais iniciais, detectando os downloaders ou exploits utilizados para o acesso inicial, limitando as informações sobre o payload final de muitos desses ataques.

Por outro lado, no diverso ecossistema do ransomware existem muitos códigos maliciosos que são distribuídos de forma massiva e com menos etapas, até mesmo tentando executar o ransomware diretamente a partir de um executável ou arquivo anexado.

Famílias de ransomware mais detectadas | 2023 | LATAM



CryptProjectXXX

- **Características:** Distribuído através de kits de exploração como Angler e Neutrino. Tem a capacidade de criptografar arquivos além de roubar credenciais de diferentes aplicativos.
- **Impacto:** Criptografia de arquivos e roubo de informações.

TeslaCrypt

- **Características:** Conhecido por atacar usuários gamers, criptografa arquivos de jogos e outros tipos de arquivos dentro do sistema afetado.
- **Impacto:** Criptografia de arquivos e extorsão econômica.

MountLocker

- **Características:** Operando como Ransomware-as-a-Service (RaaS), utiliza ChaCha20 para a criptografia de arquivos e RSA-2048 para a criptografia de chaves. Possui uma funcionalidade opcional de exclusão que, se o resgate não for pago no tempo especificado, todos os arquivos do sistema serão eliminados e o MBR sobrescrito, inutilizando o sistema.
- **Impacto:** Criptografia de arquivos, exclusão de dados e possível inutilização do sistema.

Crysis (también conocido como Dharma)

- **Características:** Geralmente se infiltra através de portas RDP expostas. Criptografa arquivos e demanda um resgate. Elimina todos os pontos de restauração do sistema, dificultando a recuperação dos arquivos.
- **Impacto:** Criptografia de arquivos e eliminação de pontos de restauração.

LokiLocker

- **Características:** Criptografa arquivos com AES e protege as chaves com RSA. Se o resgate não for pago no tempo especificado, tem a capacidade de excluir todos os arquivos do sistema e sobrescrever o MBR, inutilizando o sistema.
- **Impacto:** Criptografia de arquivos e potencial exclusão total do sistema.

Orçamento destinado à cibersegurança

62%

das organizações consideram que o orçamento destinado à cibersegurança não é suficiente

Entre as áreas que responderam o nosso questionário, observa-se que aquelas que relataram os menores níveis de orçamento são Governo, Agricultura e Pecuária, com 79% das instituições participantes da pesquisa, seguidas por Varejo/Atacado, com 74%, e Petróleo, Gás e Mineração, com 69%.

Os setores mais satisfeitos com o orçamento destinado são Informática e Tecnologia (54%) e Telecomunicações (51%).

Preocupações das organizações

28%

das empresas consideram que a cibersegurança é um assunto de máxima preocupação

Para entender a importância da cibersegurança para as empresas da América Latina, avaliamos o nível de preocupação associado a diversos riscos, como acessos indevidos aos sistemas, falta de disponibilidade de serviços críticos, extorsão, roubo ou vazamento de informações e uso malicioso de recursos e infraestrutura. Segundo a percepção das empresas participantes de nossa pesquisa, 28% consideram que esses riscos são de máxima preocupação, enquanto 42% os classificam como de alta preocupação.

Nível de preocupação que a cibersegurança representa para as empresas

28%
Máxima preocupação

42%
Alta preocupação

20%
Preocupação significativa

7%
Preocupação moderada

3%
Mínima preocupação

A principal preocupação do C-Level (77%) é a Falta de Disponibilidade de serviços críticos, o que se alinha com a continuidade operacional do negócio.

As principais preocupações para as equipes técnicas (Administradores de Rede/ Analistas/Suporte) são o Acesso Indevido a sistemas (79%) e o Roubo/Vazamento de informações (79%).

Adoção de medidas de segurança

85%

das empresas possuem soluções de backup

Questionamos quais são as tecnologias de segurança mais utilizadas pelas empresas atualmente e descobrimos que o Firewall é a mais amplamente implementada, presente em 88% das organizações, seguido por soluções de backup (85%) e VPN (80%). Além disso, as soluções antimalware são amplamente adotadas, com 64% das empresas utilizando essa tecnologia.

No caso de órgãos governamentais, o Firewall é a tecnologia mais implementada (94%), enquanto em setores como Bancário, Informática e Tecnologia, Hidrocarbonetos, Varejo, Saúde e Serviços Públicos, as soluções de backup são as mais comuns.

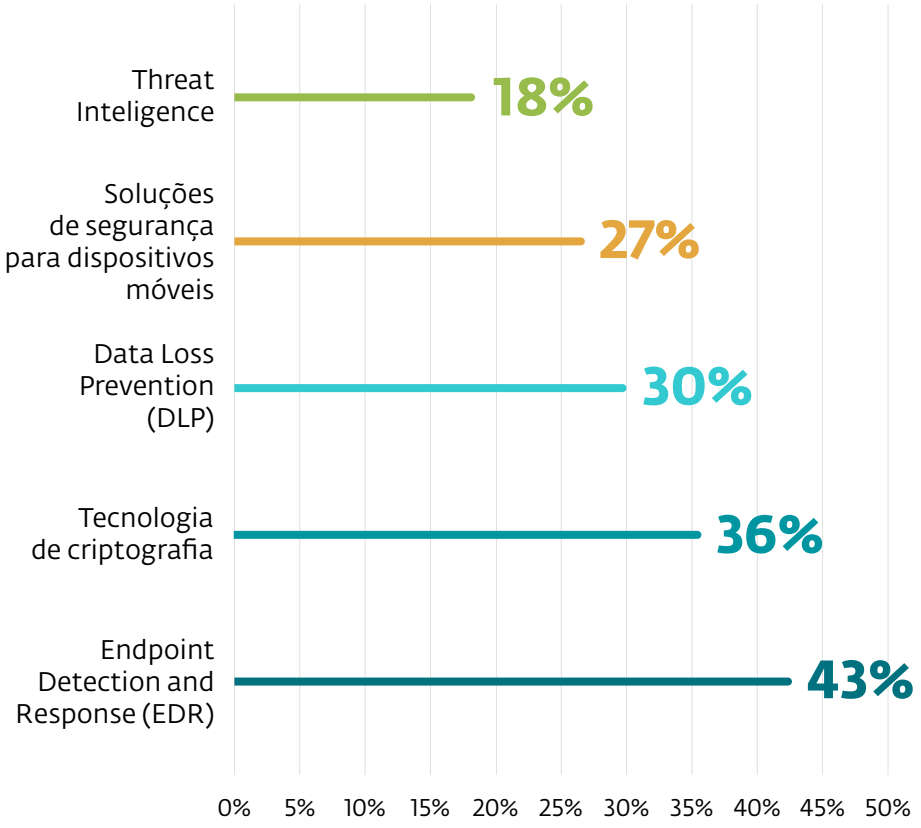
Tecnologias de segurança Implementadas por menos de 50% das organizações

Certas tecnologias avançadas de segurança, **como soluções de EDR**, permitem enfrentar a constante evolução das ameaças cibernéticas e novas TTPs usadas em ataques. No entanto, essas tecnologias têm baixos níveis de adoção em empresas da América Latina: **apenas 2 em cada 5 empresas participantes de nossa pesquisa as implementam**.

Além disso, o uso de senhas fracas é a causa de muitas invasões por meio de ataques de brute force. Contudo, apenas **50% das empresas garantem ter autenticação em dois fatores**, apesar de ser uma alternativa eficaz para combater esse problema.

Incorporar alternativas que permitam realizar **Threat Intelligence** para conhecer os adversários e ser mais eficientes na distribuição de recursos em segurança é um grande avanço na maturidade das organizações. No entanto, essa tecnologia é a menos adotada na região: **apenas 1 em cada 5 empresas conta com essa tecnologia**.

Por outro lado, embora o vazamento de dados seja a maior preocupação das empresas, **apenas 30% das organizações possuem uma solução de DLP**.



Práticas e políticas de gestão

83%

das organizações possuem uma política de cibersegurança implementada

Dentro das práticas e políticas de gestão de cibersegurança mais adotadas pelas empresas na América Latina, a política de segurança é a prática de gestão mais difundida, com 83% das empresas afirmando tê-la. Em seguida, estão o plano de resposta a incidentes, implementado por apenas 52% das organizações, e o plano de continuidade de negócios, com 46% de adoção.

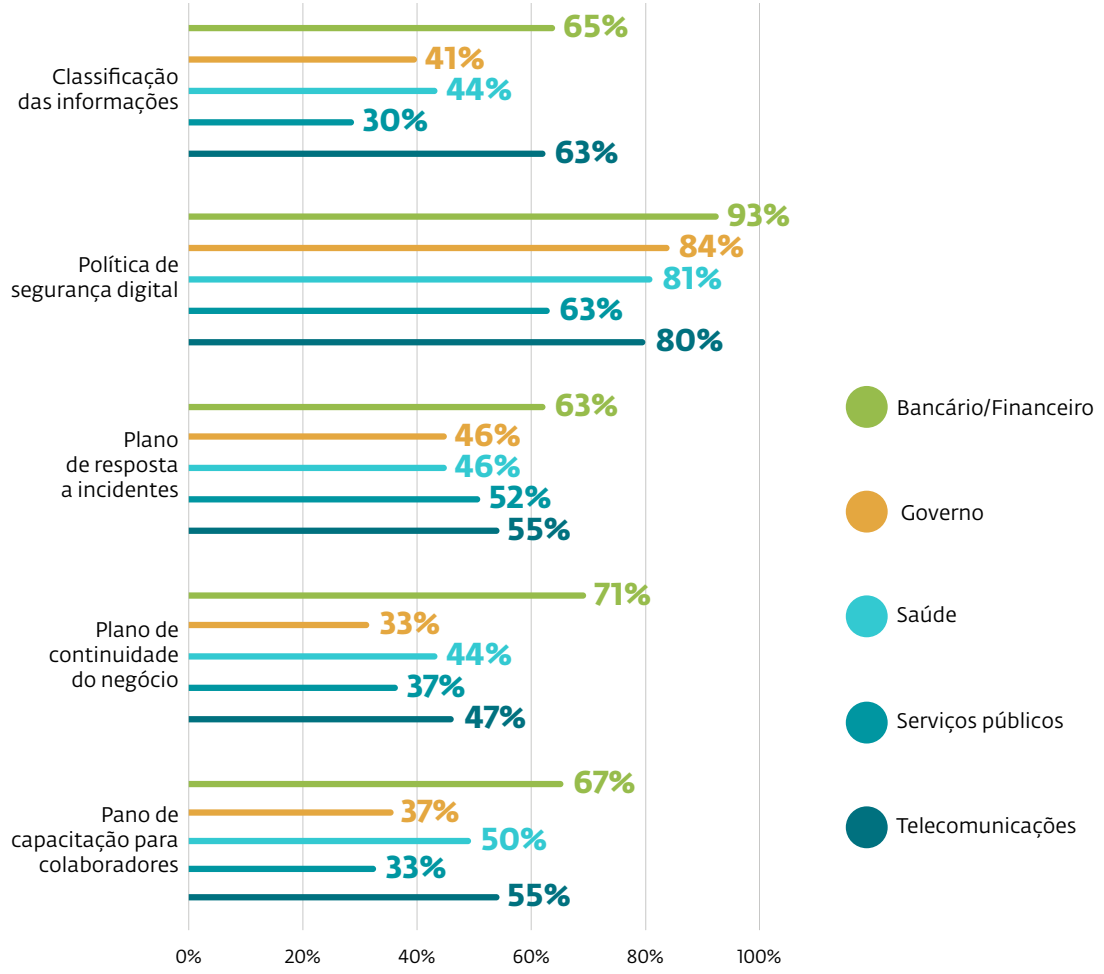
Os programas de capacitação, por outro lado, ainda têm uma adesão relativamente baixa, com apenas metade das empresas incorporando o treinamento em seu plano de ação. De fato, apenas 25% das empresas realizam mais de duas capacitações por ano, enquanto 32% realizam essas atividades apenas uma vez ao ano.

Quais são os setores com mais medidas de segurança implementadas?

O setor bancário e financeiro é o que apresenta os melhores níveis de adoção de práticas de gestão. Embora todos os setores possam melhorar, é nos setores governamental e de serviços públicos onde há mais oportunidade de crescimento, considerando que ambos são parte fundamental das infraestruturas críticas e, portanto, é importante garantir altos padrões de proteção.

Um dos vetores de ataque mais utilizados em campanhas maliciosas na América Latina é a exploração de vulnerabilidades. Embora 2 em cada 5 empresas apliquem patches de segurança em seus sistemas mais de duas vezes por ano, cerca de 25% o faz apenas uma vez por ano, deixando as organizações expostas por mais tempo à exploração de novas vulnerabilidades.

Práticas de gestão mais adotadas em diferentes setores



69% das empresas realizam análises de risco de segurança pelo menos uma vez ao ano

As análises de risco são uma ferramenta crucial para entender o estado de segurança da organização e direcionar os recursos humanos e econômicos de forma adequada. 69% das empresas que respondem a nossa pesquisa realizam essa prática de gestão pelo menos uma vez ao ano.

Realizar pentesting para verificar a eficácia das medidas de proteção é uma prática comum. Embora 64% das empresas que responderam o nosso questionário tenham realizado isso pelo menos uma vez, 25% das empresas nunca realizaram essa atividade.

Trabalho remoto

77%

considera que sua organização está preparada para trabalhar de forma remota e segura

Muitas organizações na América Latina não retornaram totalmente ao trabalho presencial após a pandemia. Das empresas que responderam o nosso questionário, 62% atualmente operam sob um modelo de trabalho híbrido, enquanto apenas 3% mantêm um modelo totalmente remoto.

Os órgãos governamentais são os que mais frequentemente (54%) adotam um modelo presencial de trabalho, em contraste com setores como Bancário/Finanças (73%) ou Informática/Tecnologia (73%), que optam por um esquema híbrido.

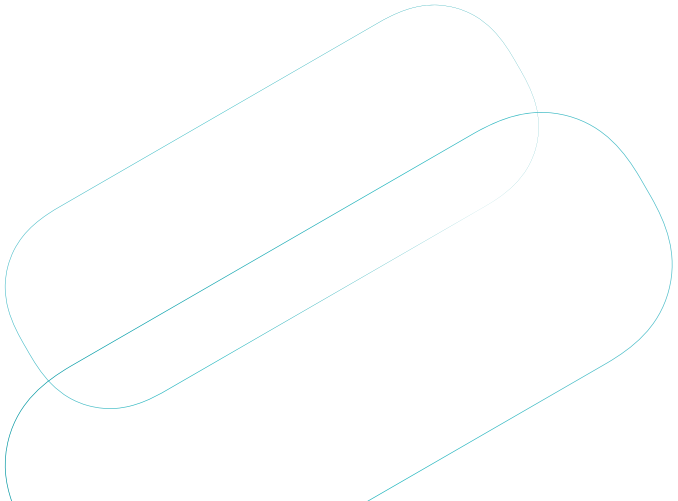
Os setores que apresentam maior percepção de insegurança em relação ao trabalho remoto são Educação (45%) e Logística e Transporte (33%).

Opinião dos colaboradores das empresas

27%

dos colaboradores recebem treinamentos periódicos sobre cibersegurança

Cursos de treinamento (47%) e palestras internas (33%) são os métodos mais utilizados pelas empresas para conscientizar seus colaboradores. Embora 51% dos colaboradores que participaram de nossa pesquisa afirmem receber treinamentos esporádicos de suas empresas, 1 em cada 5 declarou não receber esse tipo de formação. Além disso, 1 em cada 4 colaboradores afirmou não se sentir capacitado em temas de cibersegurança, e apenas 16% se sentem capacitados para identificar possíveis ataques.



Sobre a ESET

A **ESET**® é uma empresa que oferece soluções de segurança digital avançadas para prevenir ataques antes que aconteçam.

Integrando inteligência artificial com expertise humana, a ESET está na vanguarda das ameaças cibernéticas conhecidas e emergentes, protegendo empresas, infraestruturas críticas e pessoas. Suas soluções abrangem proteção para endpoints, nuvem e dispositivos móveis, utilizando tecnologias nativas de IA e baseadas em nuvem, que são altamente eficazes e fáceis de usar.

A tecnologia da ESET oferece detecção e resposta robustas, criptografia segura e autenticação multifatorial. Com suporte local e defesa em tempo real 24/7, garantimos operações seguras e contínuas. Em um ambiente digital dinâmico, comprometemo-nos com a segurança progressiva, proporcionando pesquisa de ponta e inteligência de ameaças global. Contamos com centros de pesquisa e desenvolvimento, inclusive na América Latina, e uma rede global de parceiros comerciais.

Para mais informações, acesse www.eset.com.br ou siga-nos no LinkedIn, Facebook e Instagram.

SOBRE ESET

+ 110 milhões de usuários em todo o mundo

+ 400 mil clientes corporativos

13 centros globais de pesquisa e investigação

200 países