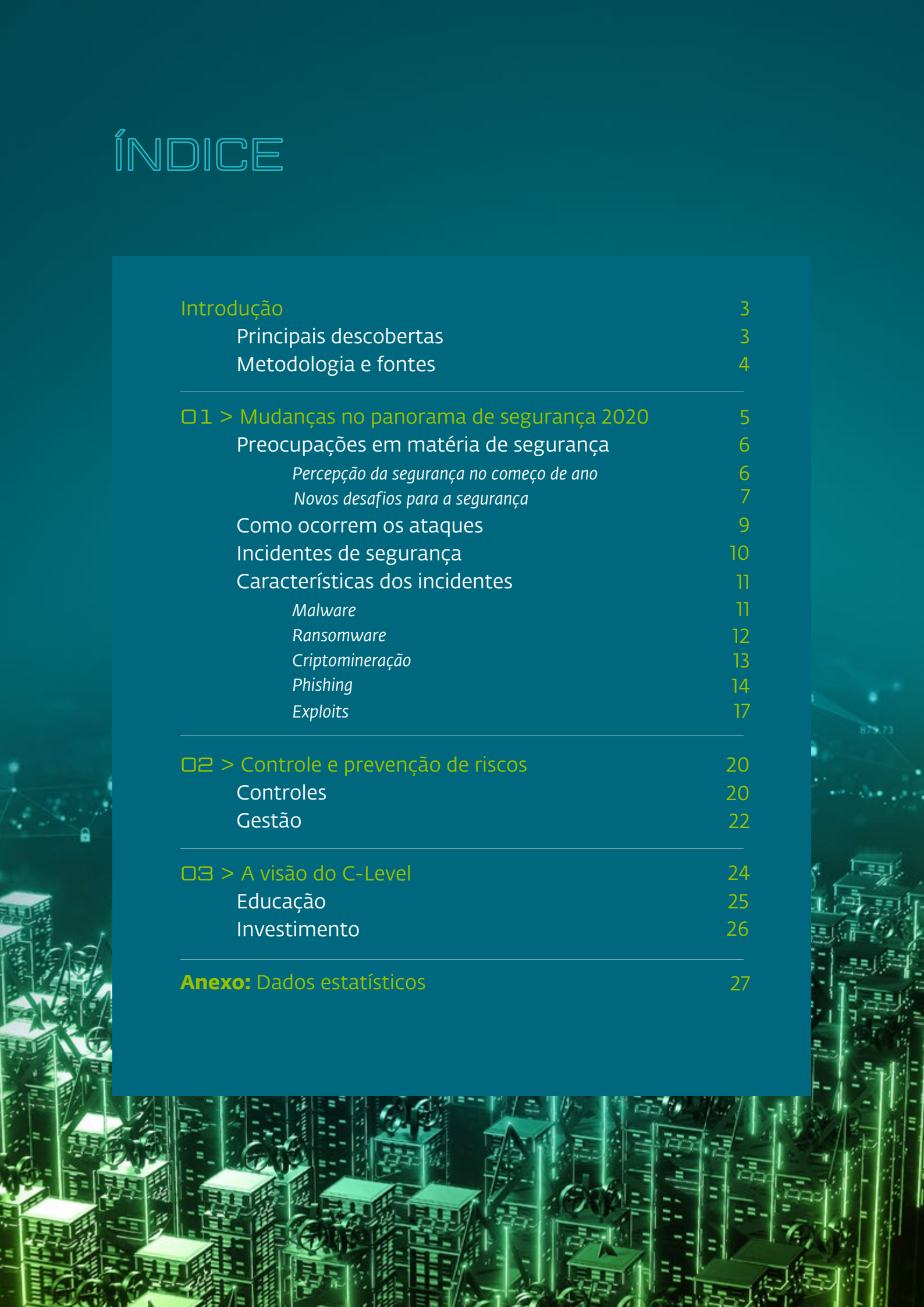
SECURITY REPORT

AMÉRICA LATINA 2020

ÍNDICE



Introdução

Conhecer o estado da informação nas empresas da América Latina, inclusive no Brasil, nos permite ter um panorama mais claro para entender o que estão fazendo em matéria de segurança digital, quais são suas preocupações e como atuam para proteger suas infraestruturas. É por isso que, há vários anos, coletamos informações de toda a América Latina através dos distintos eventos de segurança nos quais participamos e reunimos as respostas de quase 4000 empresas de diferentes tamanhos para elaborar este documento com o objetivo de refletir em um sentido amplo sobre a situação de segurança na região.

Dedicaremos a primeira parte do relatório para compreender as preocupações que as empresas têm em matéria de segurança. Observaremos a seguir os tipos de incidentes mais recorrentes e reconhecidos pelas próprias empresas para poder avaliar que controles se implementam na hora de proteger as redes corporativas. Por último, analisaremos como esses dados se relacionam com as preocupações que os profissionais de tecnologia dizem ter em relação à segurança de seus ativos digitais.

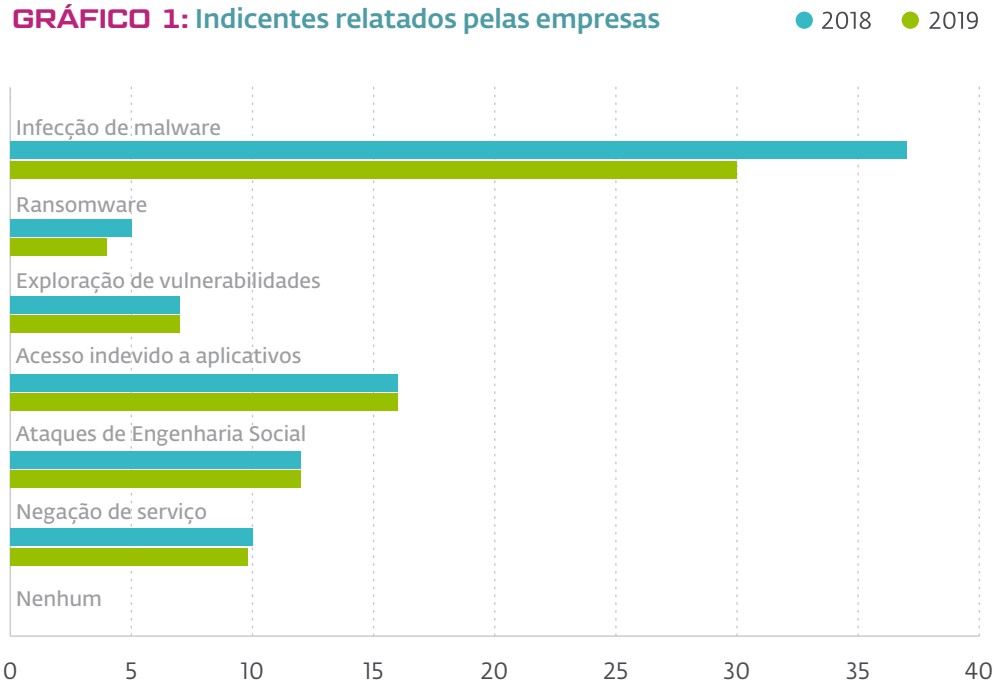
Acreditamos que esta análise reflete o estado da segurança da informação nas empresas da América Latina e esperamos que a leitura deste relatório seja de grande utilidade para que os responsáveis de segurança das empresas possam fazer suas próprias comparações e revisar suas práticas.

> Principais descobertas

É interessante ver como as empresas da região mantêm, em linhas gerais, os mesmos níveis de incidência de segurança que no ano anterior no que diz respeito a Ransomware, já que, ainda que continue sendo a ameaça mais midiática, sofreu uma pequena queda de 2%. O ano de 2019 deixou em evidência uma diminuição dos ataques massivos e uma transição para ataques direcionados a empresas, cujo objetivo a princípio é ampliar a possibilidade de êxito na cobrança de resgates econômicos. Por sua vez, ao comparar períodos, as infecções por códigos maliciosos refletiram uma queda de 8%. No entanto, apesar do número total de infecções entre os países da América Latina ter diminuído, em 2019, o Brasil teve um crescimento de 1,26% em relação ao ano anterior, passando de 11% (2018) para 12,26% (2019).

Ao longo do relatório, veremos quais são as principais características destas mudanças e como influem na gestão da segurança das empresas. Por outro lado, é interessante o fato de que somente 33% das empresas que participaram do ESET Security Report 2020 tinha um plano de continuidade do negócio. Ainda que seja pouco provável que uma organização tivesse um plano de resposta diante de uma pandemia, a transição em relação a modos de operação diferentes, como os que devem adotar prestes a finalizar o primeiro trimestre do ano, será sempre mais simples de executar para aquelas empresas que contem com planos de continuidade operacionais e aprovados.

GRÁFICO 1: Indicentes relatados pelas empresas



> Metodologia e fontes

Os dados foram coletados de pesquisas realizadas ao longo do ano em diferentes eventos de segurança dos quais participam representantes de diversas indústrias da região. Este novo relatório baseia sua análise nas respostas de mais de 3900 profissionais da segurança de organizações ao redor da América Latina.

Além disso, o relatório se compõe de dados administrados por empresas de diferentes tamanhos: este ano, 30% são representados por empresas com mais de 1000 funcionários; 11% empresas grandes de pelo menos 500 funcionários e 57% são de PMEs, entre as quais se incluem mais de dez tipos de indústrias. Além disso, cabe destacar que uma quarta parte do relatório corresponde à informação apresentada por executivos C-Level e se pode segmentar este último grupo em CISO (21%), CTO (40%) e CEO (37%).

O relatório coleta informações de empresas localizadas em 14 países da região, incluindo Brasil, Argentina, México, Colômbia, Chile e Guatemala.

01

Mudanças no panorama de segurança 2020

Durante 2019, ficou evidente o aumento na adoção de tecnologias promissoras em um contexto no qual os artigos cotidianos se tornam cada vez mais inteligentes e conectados. Neste sentido, as empresas estão incorporando estas tecnologias aos edifícios para aumentar sua eficiência operacional e economizar grandes quantias de dinheiro. As cidades até competem por implementar soluções inteligentes que permitam a elas exibir orgulhosamente as credenciais de cidade inteligente.

No entanto, isso coloca novos desafios no momento de mitigar novos ataques e evitar responsabilidades maiores em relação ao manejo dos dados pessoais (de funcionários, cidadãos, etc.). Ainda que a ideia de revolução digital nas empresas tenha sido inserida e instalada há alguns anos, entre os principais desafios que enfrentam hoje as corporações para seguir a linha da Transformação Digital, destaca o de considerar a cibersegurança como aspecto integral de cada um de seus processos. Ao não fazê-lo, será cada vez mais comum ver problemas associados a bases de dados mal configuradas (por exemplo, vazamento de informações massivas por uma má configuração de servidores), e que a adoção de novas tecnologias que buscam trazer maior segurança gere mais problemas que soluções (câmeras, controles de acesso biométricos, entre outros).

A aprendizagem automática, também conhecida como *Machine Learning* (ML), ganha cada vez mais terreno e graças a esta tecnologia muitas das tarefas foram simplificadas. Desde a análise de grandes quantidades de dados até o evitar de tarefas repetitivas com as quais lidar, a aprendizagem automática permite aos sistemas melhorar a forma em que abordam os problemas. No entanto, tal como mencionamos em nosso relatório de tendências 2020, em 2019 o ML ganhou notoriedade devido a outro assunto preocupante: o aumento das deepfakes. Esta tecnologia que faz com que o ditado popular "ver para crer" perca todo o sentido, pode ser aproveitada para prejudicar a reputação de figuras públicas ou até de influir na opinião pública. Tanto é assim que em 2019 foi relatado um caso de um engano no qual os atacantes utilizaram um software baseado em Inteligência Artificial para imitar a voz do CEO de uma empresa e convencer a vítima para que realize transferências monetárias para contas bancárias dos fraudadores.

A tecnologia ML também foi aplicada em um contexto menos sinistro, como é o caso do FaceApp, o *app* que permite envelhecer e rejuvenescer rostos. No entanto, a aplicação mostrou problemas vinculados à privacidade dos dados dos usuários e gerou preocupação; sobretudo para futuras implementações que façam uso dessa tecnologia de forma similar, como poderia ser, por exemplo, a tecnologia de reconhecimento facial como mecanismo de autenticação.

> Preocupações em matéria de segurança

Percepção da segurança no começo do ano

O panorama de incidentes e ameaças que introduzimos traz como consequência a preocupação das empresas pela segurança de sua informação. Se tivéssemos que colocar em uma ordem, 60% das organizações que responderam a pesquisa afirma que sua principal preocupação é o **acesso indevido à informação**. O pódio é complementado por **roubo de informação** (55%) e a **infecção por códigos maliciosos** (53%). Ainda assim, e tal como analisaremos mais adiante, surpreende a baixa implementação de controles de identificação, como ferramentas de múltiplo fator de autenticação, para evitar acessos indevidos.

60% DAS ORGANIZAÇÕES QUE RESPONDERAM A PESQUISA AFIRMA QUE SUA PRINCIPAL PREOCUPAÇÃO É O ACESSO INDEVIDO À INFORMAÇÃO.

Era de se esperar que essas fossem as principais preocupações para as empresas, já que se nos remetemos ao que ocorreu durante 2019, os casos de fuga de informação transformaram-se em notícia recorrente. De fato, ainda que tenha entrado em efeito o Regulamento Geral de Proteção de Dados (GDPR, por sua sigla em inglês) dentro da União Europeia, cujo alcance é global, o ano passado registrou casos de fugas de informação e de dados pessoais cada vez maiores com o passar dos meses. Trata-se de um problema que não afeta tanto empresas privadas, como órgãos governamentais. Em 2019, entre outras exposições de dados que ocorreram no Brasil, foram vazadas mais de 145 GB de informações de usuários de diversas empresas brasileiras que utilizam o servidor do Grupo BCI, que continha informações pessoais, físicas e jurídicas dos usuários, como número de RG, data de nascimento, e-mails e telefones dos usuários.

Neste contexto de vazamentos e exposições de dados, apesar do prazo para as punições ter sido adiado para agosto de 2021 devido a pandemia provocada pela Covid-19, a Lei Geral de Proteção de Dados (LGPD) ganha destaque no Brasil. A LGPD, que merece a atenção das empresas, foi inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR) e estabelece regras para uso, proteção e transparência de informações pessoais no Brasil.

Vale destacar também que, além das preocupações mencionadas, a privacidade da informação (46%) se aproxima do último posto do pódio como preocupação central para as empresas da região.

No que diz respeito a esse terceiro lugar, a infecção por códigos maliciosos leva consigo o problema desse tipo de ameaças: a grande maioria dos ataques que podem comprometer a segurança de uma empresa costuma estar associada a alguma variação de malware. A ampla variedade de ações maliciosas que este tipo de ameaças pode realizar, desde botnets a ransomware, é igualmente aproveitada em um amplo espectro de plataformas: desde computadores até dispositivos móveis sem deixar de fora os dispositivos IoT, o que faz com que a infecção através de malware seja um dos métodos mais usados pelos atacantes.

Vimos como os cibercriminosos usam técnicas variadas para propagar suas ameaças. Como por exemplo, 2019 estava apenas começando e uma vulnerabilidade no WinRAR tornou-se pública, e poucos dias depois começaram a surgir exploits e campanhas maliciosas que buscavam aproveitar a vulnerabilidade para propagar determinadas famílias de ransomware. O mesmo aconteceu com a vulnerabilidade do WhatsApp revelada na metade do ano que permitia o acesso ao dispositivo com uma simples chamada através dessa plataforma, colocando mais uma vez em risco dados sensíveis e pessoais das vítimas e/ou das empresas para as quais trabalhavam.

Novos desafios para a segurança

Mas este panorama da segurança se viu alterado pela situação extraordinária que tiveram que enfrentar as empresas como consequência da Covid-19, e o que isso implicou no momento de garantir a continuidade das operações. Segundo dados revelados a partir de pesquisas realizadas durante os últimos meses na região, quase 45% dos usuários recebeu tentativas de Phishing relacionados à pandemia e mais de 50% garantiu que a organização para a qual trabalham não trouxe as ferramentas de segurança necessárias para migrar para o teletrabalho nestas condições.

QUASE **45%** DOS USUÁRIOS RECEBEU TENTATIVAS DE PHISHING RELACIONADOS À PANDEMIA E MAIS DE 50% GARANTIU QUE A ORGANIZAÇÃO PARA A QUAL TRABALHAM NÃO TROUXE AS FERRAMENTAS DE SEGURANÇA NECESSÁRIAS PARA MIGRAR PARA O TELETRABALHO.

O novo cenário trazido pela pandemia somou novos desafios e preocupações às empresas ligadas ao fato de que o perímetro a proteger se estendeu consideravelmente. A seguir, apresentaremos alguns dos desafios acelerados por este fenômeno sanitário.

Aceleração dos processos de transformação digital

É evidente que o processo de transformação digital para muitas empresas começou há alguns anos, mas a pandemia expôs a necessidade de contar com meios alternativos para poder realizar as atividades cotidianas, como o trabalho remoto.

Neste sentido, ainda que no âmbito corporativo haja quem já tenha adotado estes mecanismos como uma opção para realizar suas funções, o que ajudou a que o impacto da crise provocada pela Covid-19 fosse menor na hora de continuar com suas operações, as organizações que ignoraram ou adiaram a decisão de levar adiante esta transição digital se viram afetadas pela falta de disponibilidade, integridade ou confidencialidade de suas informações.

A segurança deve estar em todo lado, não há limites físicos

O distanciamento social reafirmou uma premissa da qual falamos anteriormente: a segurança deve nos acompanhar a cada lugar e em todo momento. Ainda que as empresas invistam em recursos de toda espécie para proteger suas informações e infraestrutura tecnológica, muitas vezes se pensa somente em um espaço físico (por exemplo, um escritório).

As novas condições de trabalho expõem a necessidade de contar com mecanismos de proteção (entre eles, soluções de segurança e a aplicação de boas práticas), em todos os pontos desde onde são processados, armazenados ou transmitidos os dados.

AS NOVAS CONDIÇÕES DE TRABALHO EXPÕEM A NECESSIDADE DE CONTAR COM MECANISMOS DE PROTEÇÃO (ENTRE ELES, SOLUÇÕES DE SEGURANÇA E A APLICAÇÃO DE BOAS PRÁTICAS), EM TODOS OS PONTOS DESDE ONDE SÃO PROCESSADOS, ARMAZENADOS OU TRANSMITIDOS OS DADOS.

Planos de contingência postos à prova

A pandemia também mostrou a necessidade de implementar, revisar, testar, melhorar, e atualizar ferramentas como as de Análise de Impacto no Negócio (BIA); Avaliações de Riscos; Planos de Continuidade do Negócio (BCP); ou Planos de Recuperação (DRP). Ao mesmo tempo, deixou clara a importância de considerar o dispositivo, os lugares de trabalho, as tecnologias e os serviços críticos.

Ainda que um cenário desta natureza fosse muito difícil de prever, sua chegada tornou evidente o alto impacto para os negócios. De fato, ainda que novamente uma terceira parte das empresas que participaram do relatório este ano tivessem um plano de continuidade do negócio, reflete como empresas no geral não estão preparadas para responder a incidentes que comprometam a operacionalidade do negócio.

Por isso, o foco das organizações agora está em contar com medidas e planos de resposta que permitam garantir a continuidade dos processos comerciais.

Junto a estas condições, as preocupações das empresas começam a mudar e se dirigem também para a tomada de medidas que garantam maiores níveis de segurança no momento de se conectar a partir de redes Wi-Fi domésticas ou ao utilizar diferentes ferramentas de comunicação. Isso implica em desafios e as empresas agora devem implementar novas dinâmicas de capacitação e/ou conscientização para que seus colaboradores assumam a importância de proteger os dados sensíveis, tanto pessoais como corporativos.

LGPD x Pandemia provocada pela Covid-19

Como destacamos anteriormente, devido a pandemia provocada pela Covid-19, muitas ações têm sido adiadas. Uma delas é a data de vigência para aplicação de sanções por violações da LGPD. Apesar do adiamento do prazo para as penalidades relacionadas ao descumprimento da LGPD ter sido aprovado, a Medida Provisória (MP) nº 959/2020, que sugere que a norma (com exceção das punições) entre em vigor a partir do dia 03 de maio de 2021, ainda não foi votada pelo

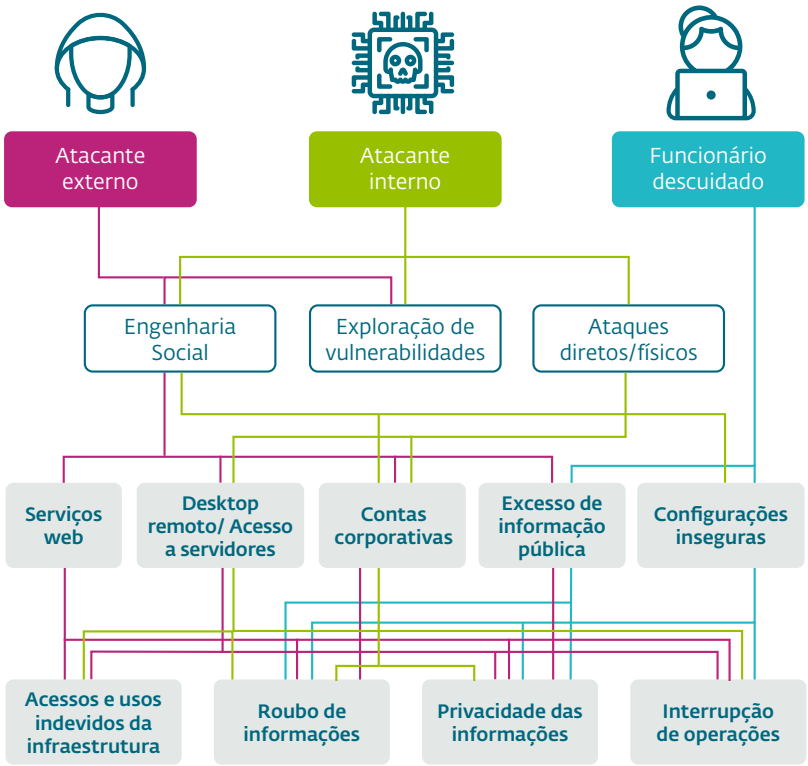
congresso e pode estar longe de ser sancionada. Caso o texto da MP não seja aprovado, a medida pode perder validade, fazendo com que o prazo para que as regras começarem a valer seja antecipado para agosto de 2020, como prevê a lei que estabeleceu a Autoridade Nacional de Proteção de Dados (ANPD). Apesar dessas indefinições quanto as datas de vigência da LGPD, as empresas não podem esquecer a importância de adequar-se as novas normas, observando as principais abordagens sobre a proteção dos dados administrados pelo negócio. Em caso de descumprimento da lei, a empresa ou responsável pelo serviço pode receber desde advertências a multas que podem chegar a até R$ 50 milhões.

AS EMPRESAS NÃO PODEM ESQUECER A IMPORTÂNCIA DE ADEQUAR-SE AS NOVAS NORMAS, OBSERVANDO AS PRINCIPAIS ABORDAGENS SOBRE A PROTEÇÃO DOS DADOS ADMINISTRADOS PELO NEGÓCIO.

> Como ocorrem os ataques

Dada a ampla variedade de ameaças que pode afetar às empresas, e conhecendo suas principais preocupações em matéria de segurança, é importante identificar quais são os diferentes vetores pelos quais pode chegar um ataque, para poder tomar as medidas de controle mais adequadas.

No Laboratório de Pesquisa da ESET, elaboramos um diagrama com as vias mais utilizadas na execução dos ataques, segundo tenham identificado nossas soluções de segurança em tentativas dirigidas a nossos clientes ao redor da América Latina. Foi levado em consideração que, ainda que muitas vezes os ataques cheguem de fora da organização, é possível que ocorram dentro da empresa, inclusive por descuidos ou más práticas de segurança.



Em qualquer caso, a **engenharia social** e a **exploração de vulnerabilidades** continuam sendo os principais vetores que podem ser usados por atacantes para comprometer os diferentes serviços que uma empresa utiliza. Uma vez conseguido o acesso, podem levar adiante diferentes tipos de **ações maliciosas**.

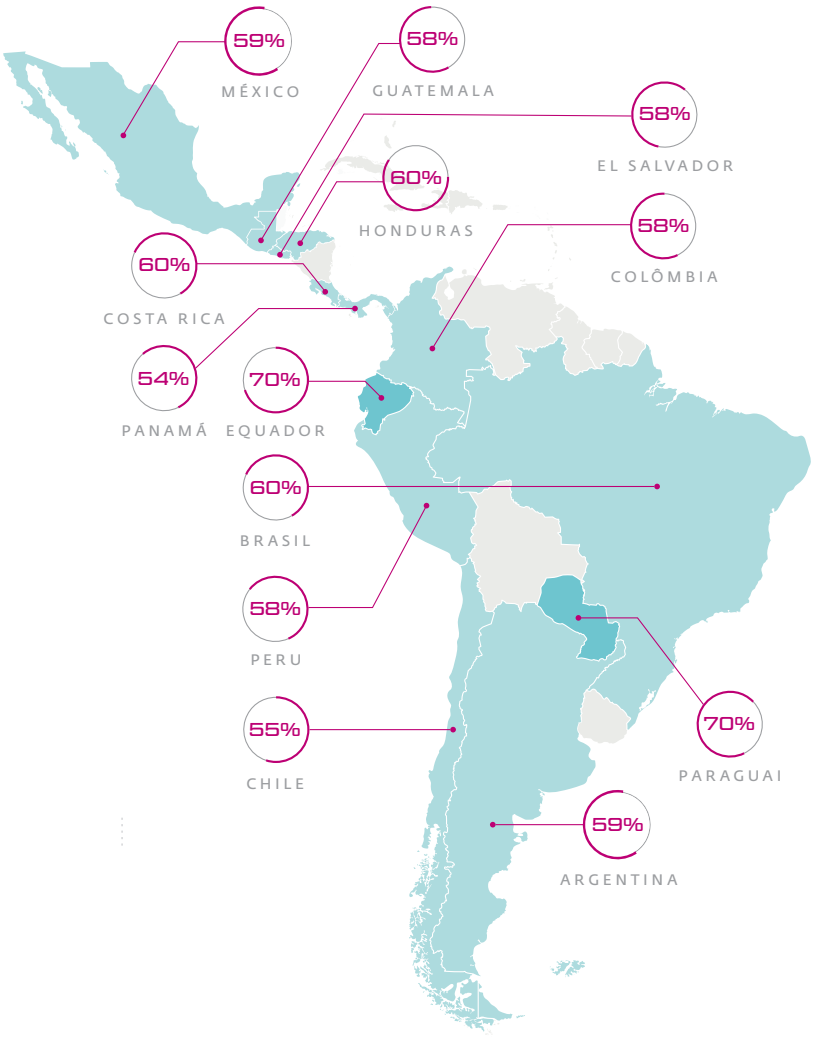
A ENGENHARIA SOCIAL E A EXPLORAÇÃO DE VULNERABILIDADES CONTINUAM SENDO OS PRINCIPAIS VETORES QUE PODEM SER USADOS POR ATACANTES PARA COMPROMETER OS DIFERENTES SERVIÇOS QUE UMA EMPRESA UTILIZA.

Independente do caminho ou do ator que esteja por trás do incidente de segurança, tanto a continuidade do negócio, como a reputação da empresa, podem ser afetadas.

> Incidentes de segurança

Das preocupações, passamos aos incidentes. Para isso, é importante entender o nível dos incidentes que se apresentam, e é a partir da análise dos dados administrados por organizações de toda a América Latina que podemos afirmar que 60% das empresas sofreu ao menos um incidente de segurança, número que se mantém em relação ao ano anterior. A infecção por códigos maliciosos também conserva seu lugar, sendo o incidente mais recorrente: 1 de cada 3 empresas sofreu uma infecção com algum código malicioso, incluindo ransomware.

GRÁFICO 2: Empresas com incidentes de segurança



60% DAS EMPRESAS SOFREU AO MENOS UM INCIDENTE DE SEGURANÇA EM 2019.

Algo que surge da revisão das informações coletadas é que dentro dos incidentes relacionados à infecção por códigos maliciosos (32%), só 18% está relacionado a ransomware, o que indica uma incidência de 6% sobre o total das empresas. Isso se traduz em uma queda em relação a 2019, ano no qual o ransomware tinha registrado uma incidência de 8%.

> Características dos incidentes

Mais além de conhecer quais foram os incidentes com maior presença nos diferentes países da região, resulta também interessante conhecer que tipo de ameaças esteve por trás de cada uma delas. Faremos uma trajetória pelas principais famílias de malware vistas na região, detalhando suas características, dedicando um parágrafo especial para o ransomware e a criptomineração; duas ameaças muito presentes na América Latina junto com o *phishing* e os *exploits*.

Malware

Entre os códigos maliciosos detectados na região, os mais relevantes foram:

- </> Ramnit
- </> ProxyChanger
- </> Emotet
- </> Bondat
- </> Exploit.CVE-2012-0143.A

< Win32/Ramnit > Código malicioso utilizado principalmente para roubar dados confidenciais relacionados a serviços bancários dos usuários. Propaga-se através de dispositivos removíveis e uma de suas principais características é a capacidade de infectar o Master Boot Record (MBR) para manter sua persistência no sistema operacional.

< JS/ProxyChanger > Trata-se de um malware do tipo *trojan* escrito em JavaScript. Tem como função impedir que o usuário acesse websites para redirecionar o tráfico para sites de atacantes.

< Win32/Emotet > Este código malicioso se ocupa principalmente da distribuição de outras famílias de *trojans* bancários. É conhecido por sua arquitetura modular, seus métodos de persistência e sua capacidade de autopropagação, além de suas características polimórficas que tentam fugir da detecção baseada em assinaturas.

< JS/Bondat > Worm escrito em JavaScript que tem como função principal infectar sistemas Windows para uni-los a um botnet. Funciona como um vetor de infecção inicial, já que também descarrega novos arquivos capazes de realizar outras

ações maliciosas. Seu meio de propagação são os meios removíveis, utilizando arquivos LNK.

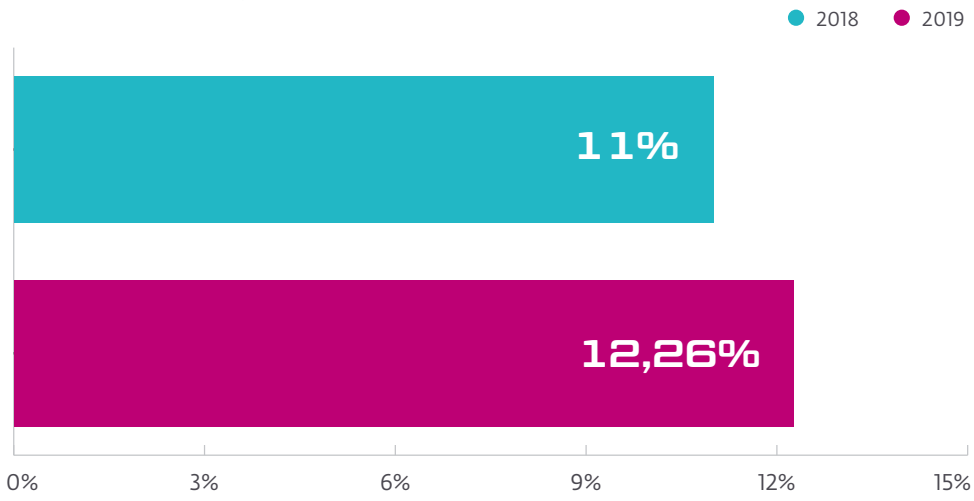
< Exploit.CVE-2012-0143 > É uma vulnerabilidade de 2012 e que permite a um atacante externo executar código de maneira arbitraria a partir de um erro no manejo da memória do Microsoft Excel 2003 SP3 e Office 2008 para Mac.

Merecem uma menção especial os trojans bancários. Estes códigos maliciosos que são utilizados para roubar informações financeiras dos usuários têm uma atuação muito alta na América Latina, ganhando destaque no Brasil, onde existem famílias de trojans específicos que apresentam características comuns entre si. Neste sentido, a maioria dos trojans bancários presentes na América Latina que foram analisados durante 2019 e que estamos acompanhando em 2020, convertem o dispositivo da vítima em um computador zumbi, de tal maneira que se conectam ao servidor de C&C e permanecem ali à espera de receber qualquer comando enviado pelo servidor. Uma vez recebido o comando, ele é executado e esperam a chegada de um novo. Algumas famílias representativas deste tipo de ameaças presentes na região são Amavaldo, Casbaneiro, Mispadu, Guildma ou Grandoreiro.

Ransomware

Em termos gerais, o número de casos de ransomware mostra uma tendência decrescente pelo terceiro ano consecutivo na América Latina. Em 2017, a quantidade de empresas afetadas por esta variante de malware foi de 18%, enquanto em 2018 a porcentagem caiu para 8% e em 2019, registrando apenas 6%. Como destacamos anteriormente, apesar disso, em 2019, o Brasil teve um crescimento de 1,26% em relação ao ano anterior, passando de 11% (2018) para 12,26% (2019).

GRÁFICO 3: Infecções por ransomware no Brasil



A novidade do ransomware como ameaça predileta para os cibercriminosos diminuiu em importância se analisarmos o cenário geral em toda a América Latina, exceto no Brasil, mas está sendo amplamente utilizado em ataques mais direcionados. É comum nos encontrarmos com ameaças que geram a interrupção das

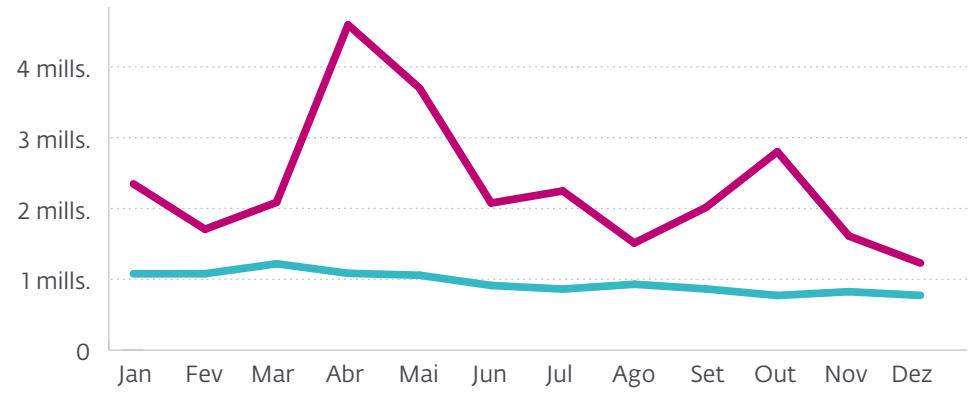
operações de negócio, expõem informações sensíveis e exigem pagamentos de resgate maiores. Por este motivo, dado o alto impacto que pode ter na operação da empresa, o ransomware não deve ser ignorado no momento de realizar as análises de risco da empresa e tomar medidas de controle, tanto preventivas como corretivas.

Criptomineração

Outra variante de código malicioso cuja evolução vale a pena mencionar corresponde à mineração de criptomoedas. Ainda que o mercado da criptomineração continue em crescimento, e as estatísticas mostrem que uma parte é realizada a partir de ataques de criptojacking, que utilizam os recursos das vítimas em favor dos cibercriminosos, durante 2019 se registrou um decréscimo em sua atividade em comparação a 2018. Isso indica que, igual ao Ransomware, ainda que o registro de ataques tenha diminuído, é seu modo de execução que foi modificado. Isto é, trata-se de ações direcionadas que buscam atacar infraestruturas mais preparadas para a tarefa, dado que, ao possivelmente ter servidores com maior capacidade de processamento, funcionamento contínuo e maior largura de banda, entre outras características, tornam-se um alvo mais atrativo para minerar criptomoedas. Isso acontece porque será necessária uma menor quantidade de computadores infectados para ter uma capacidade de processamento atrativa para a mineração, especialmente se comparado ao alto número de dispositivos necessários para afetar usuários domésticos.

AINDA QUE O REGISTRO DE ATAQUES TENHA DIMINUÍDO, É SEU MODO DE EXECUÇÃO QUE FOI MODIFICADO

GRÁFICO 4: Detecções de criptomineração ao longo do ano



Deixando de lado os códigos maliciosos, 18% das empresas assegurou ter sofrido acessos indevidos à informação, enquanto 15% disse ter sido vítima de técnicas de engenharia social, sendo este o incidente com maior crescimento dos últimos meses.

A ENGENHARIA SOCIAL FOI O INCIDENTE COM MAIOR CRESCIMENTO NOS ÚLTIMOS MESES DE 2019.

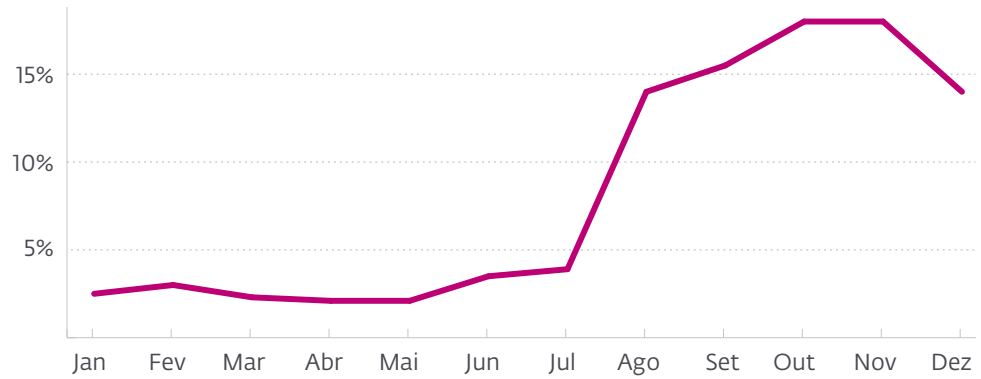
Phishing

É possível que o incremento no número de incidentes associados à engenharia social esteja ligado à ampla variedade de campanhas que vimos durante 2018. Diversas marcas reconhecidas foram utilizadas como gancho e novos vetores de ataque se somaram à lista. O e-mail deixou de ser a única via para lançar mensagens de phishing, e outras ferramentas de mensagem como o WhatsApp e o SMS foram muito utilizadas para estes fins. Mais uma vez, parece chamativa a pouca proteção em dispositivos móveis utilizados pelas empresas, dado que apenas 12% garantiu implementar soluções de segurança para dispositivos móveis. Ainda mais preocupante pode ser isso se levado em consideração que através dos dispositivos móveis se manipula e se compartilha cada vez mais informações sensíveis do negócio.

É importante entender que, ainda que muitos ataques de engenharia social apenas busquem roubar credenciais de usuários finais (de serviços de streaming, e-mail, redes sociais, entre outros), não é difícil que tais usuários utilizem as mesmas senhas em suas contas pessoais e em ambientes corporativos. Por outro lado, é preciso mencionar a existência de ataques que trazem associados *trojans* bancários, como o Emotet, ou ameaças tipo Spyware que conservam sua persistência nos dispositivos afetados esperando a chegada de novas informações úteis para seus propósitos.

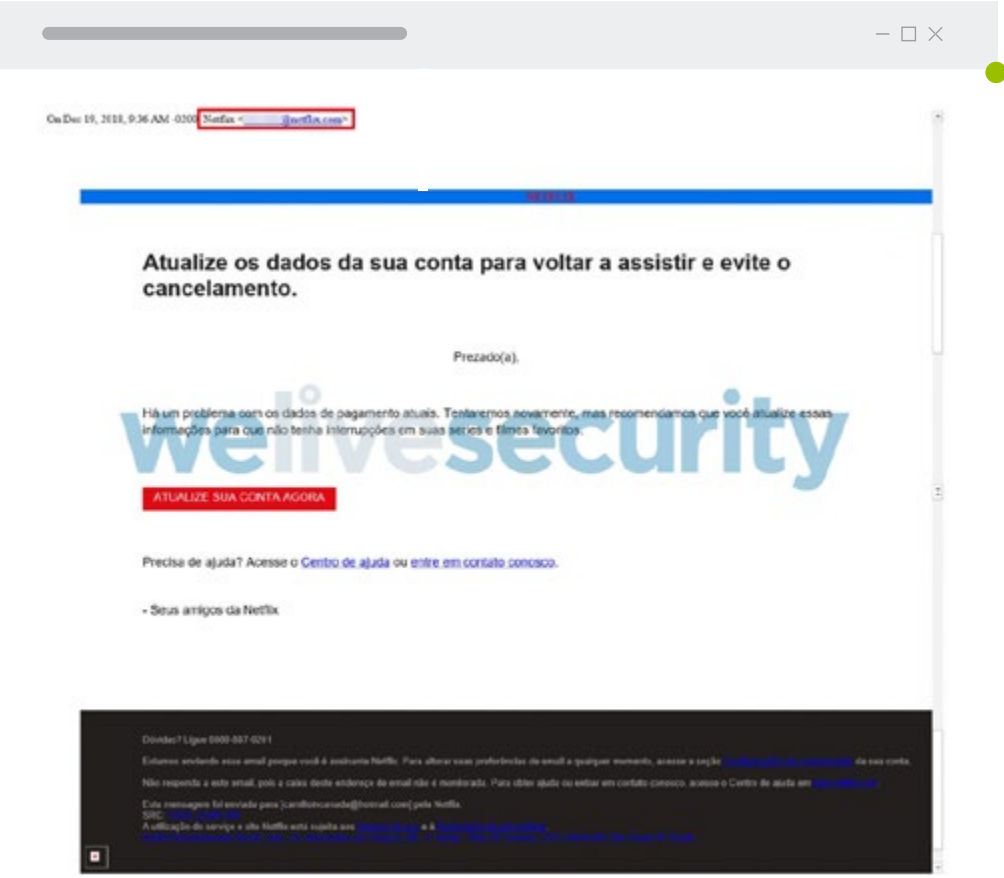
No que diz respeito a detecções de phishing, é evidente um notável aumento durante a segunda metade de 2019, particularmente ao ver os picos registrados no último trimestre.

GRÁFICO 5: Detecções de Phishing durante 2019



Ao longo de 2019, também fomos testemunhas de grandes fugas de informação como o vazamento de dados da Vivo que expôs informações, como nome, RG, CPF, e-mail, telefone, data de nascimento e nome da mãe, de 24 milhões de clientes; também foram vazadas mais de 145 GB de informações de usuários de di-

versas empresas brasileiras que utilizam o servidor do Grupo BCI, como citamos anteriormente. É importante ter em conta que ao tornar todos esses dados públicos, torna-se mais simples para os atacantes criarem campanhas de phishing mais direcionadas e efetivas ao aproveitar esta informação. A título de exemplo, veremos a seguir um dos e-mails mais recorrentes e frequentemente utilizados, que substituem a identidade de serviços ou marcas reconhecidas.



Campanha de Phishing via e-mail que se faz passar pela Netflix

O aumento na frequência com a qual vemos circular este tipo de campanhas não deve ser pensado unicamente como uma consequência direta da exposição de informações pessoais do usuário. Como mencionamos anteriormente, é a soma de todos os pequenos dados e detalhes o que pode aproveitar um atacante no momento de lançar ataques mais direcionados. Daqui se percebe o fato de que apenas esse tipo de campanhas registrou uma alta atividade durante 2019. A circulação de campanhas falsas através de diferentes aplicativos de mensagem (principalmente WhatsApp) nas quais se prometem cupons ou promoções por aniversários, buscam fazer publicidade, mas em muitos casos também obter informações pessoais de quem recebe as mensagens, e é este outro fator chave no incremento de fugas de dados. Dessas fraudes surge precisamente a possibilidade de utilizar informações pessoais contra pessoas desprevenidas em ataques mais sofisticados e direcionados. No começo de 2019 se conhecia o vazamento de

mais de 2.200 milhões de senhas, endereços de e-mail e nomes de usuário com a publicação de cinco pastas (Collection#1 a #5) que coletavam estas informações provenientes de distintas brechas. Foi esse evento o que marcou 2019 como o ano dos dados pessoais e da privacidade.

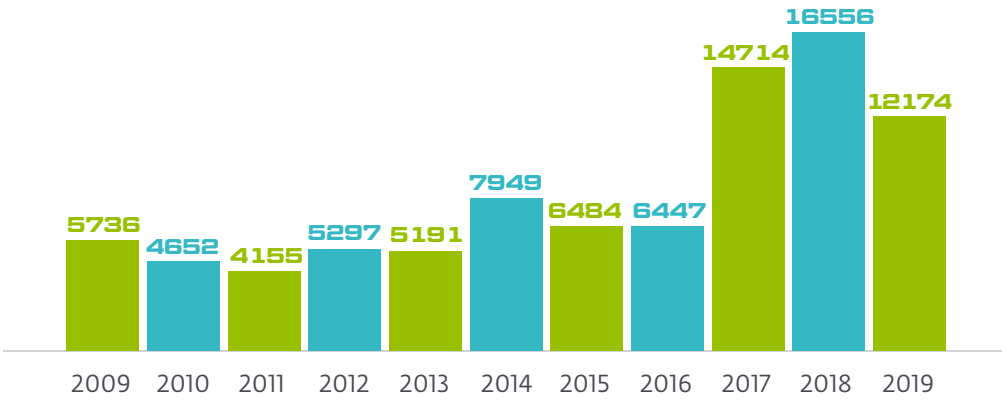
Campanha de Phishing via whatsapp que se faz passar pelo Spotify

Ainda que aquela brecha tenha sido a maior, não foi a única. Ao longo do ano se apresentaram novos casos que as empresas se viram obrigadas a relatar ao envolver os dados de seus usuários, sob o dever de cumprir com as novas regulamentações.

É importante ressaltar que as fraudes baseadas em engenharia social foram evoluindo e conseguiram, em muitos casos, aumentar sua efetividade. Neste sentido, os cibercriminosos passaram de utilizar simples sites de phishing para incorporar certificados SSL falsos ou gratuitos com o objetivo de se aproveitar do desconhecimento do usuário sobre o funcionamento do protocolo HTTPS, passando pelos ataques homográficos que tomaram maior relevância ao suplantar a identidade de empresas e marcas reconhecidas.

Outro dos incidentes com altos níveis de ocorrência entre as empresas da América Latina foi a exploração de vulnerabilidades, sofrido por 8% das empresas pesquisadas. Talvez uma das questões mais interessantes ao abordar este tipo de incidentes seja o fato de que a quantidade de detecções de vulnerabilidades informada durante 2019 registrou uma queda significativa em relação a 2018 e 2017 e, ainda assim, o impacto nas empresas se manteve praticamente igual.

GRÁFICO 6: Número de detecções de vulnerabilidades relatadas



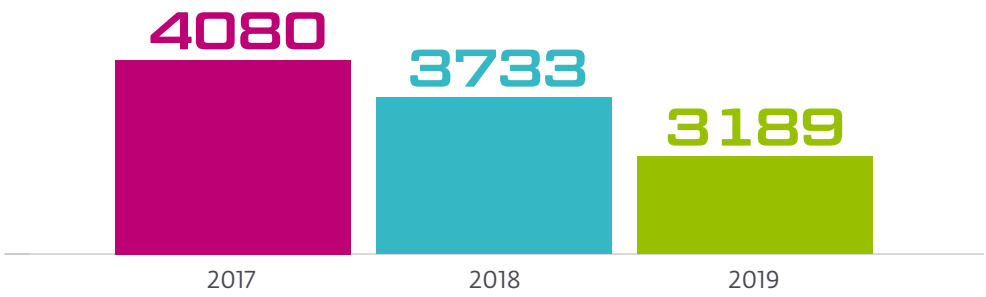
De todas as formas, os números continuam sendo preocupantes se observamos a incidência nas empresas e consideramos a quantidade de tecnologia que deve se manter constantemente atualizada para evitar ser vítima deste tipo de explorações.

Exploits

O outro elemento desta combinação são os *exploits*. O que são? Trata-se de códigos que, além de mostrar a existência de uma falha, expõem também a presença de uma vulnerabilidade. Isto é, que pode ser aproveitada por um atacante para comprometer a confidencialidade, integridade e disponibilidade da informação.

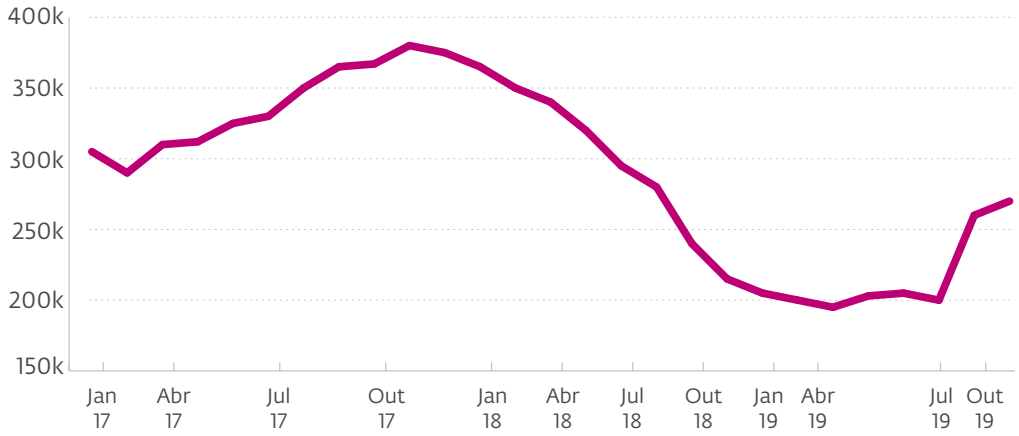
Ao longo dos últimos três anos detectou-se um comportamento decrescente na quantidade de variantes detectadas e associadas a *exploits*, mas isso está longe de poder ser associado à diminuição do risco para empresas. Uma análise detalhada da telemetria da ESET nestes últimos anos relata que, desde a aparição do infame Wannacry, os cibercriminosos estão atentos ao descobrimento de novas vulnerabilidades para tentar aproveitá-las em suas últimas campanhas.

GRÁFICO 7: Número de variantes detectadas e associadas a exploits



No seguinte gráfico, nota-se a média móvel da quantidade de hashes únicos detectados por mês nos últimos três anos associados a detecções de exploits na América Latina. Durante 2017, fica evidente o comportamento crescente na quantidade de novos hashes detectados, chegando ao seu máximo em outubro, mês no qual muda a tendência. Este crescimento encontra sua explicação no uso intensivo dos cibercriminosos de EternalBlue, a família de exploits que aproveitava as vulnerabilidades do SMB, utilizado em diferentes tipos de códigos maliciosos muito além do Wannacry.

GRÁFICO 8: Média móvel de quantidade de hashes únicos detectados por mês associadas a detecções de exploits na América Latina

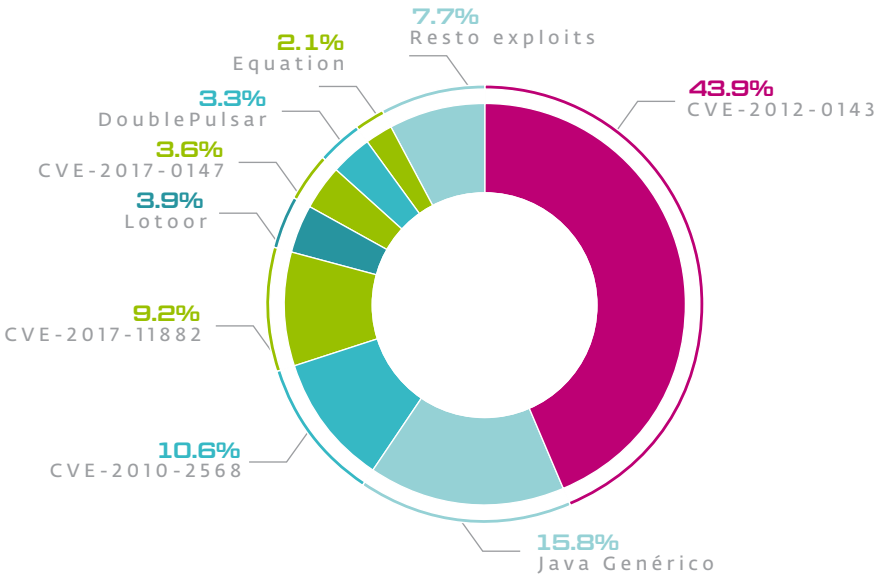


Ao longo de 2018 não foram registradas grandes variações na aparição de novos hashes associados com exploits, apesar do máximo histórico na quantidade de vulnerabilidades relatadas e do registro de vulnerabilidades importantes como Spectre, Meltdown e PowerPool, ainda que não tenham sido utilizadas de forma massiva em campanhas maliciosas. Já em 2019, vemos um novo ponto de inflexão na tendência, próximo ao mês de junho, quando passou a ser conhecida a vulnerabilidade BlueKeep que, em novembro de 2019, derivou em um novo máximo na quantidade de detecções. Até 2020 foi registrado um comportamento com tendência decrescente, algo que provavelmente será mantido até o aparecimento de uma nova vulnerabilidade que tenha as características adequadas para ser usada em campanhas maliciosas.

Distribuição de exploits na América Latina durante 2019

O seguinte gráfico mostra como tem sido a distribuição dos *exploits* com maiores registros durante 2019 na América Latina:

GRÁFICO 9: Maiores índices de exploits registrados na América Latina durante 2019



No que diz respeito à distribuição por país, 50% das detecções da região esteve concentrada no México (20,8%), Peru (18,4%) e Colômbia (11,1%); seguidas pelo Brasil (10,3%), Argentina (7,4%) e Guatemala (7,1%).

Essas análises deixam em evidência o risco associado à exploração de vulnerabilidades, um problema latente para as empresas, seja pelo uso em ataques massivos ou direcionados.

50% DAS DETECÇÕES DA REGIÃO ESTEVE CONCENTRADA NO MÉXICO (**20,8%**), PERU (**18,4%**) E COLÔMBIA (**11,1%**); SEGUIDAS PELO BRASIL (**10,3%**), ARGENTINA (**7,4%**) E GUATEMALA (**7,1%**).

02

Controle e prevenção de riscos

Diante do panorama apresentado, e compreendendo que são múltiplas as vias pelas quais um atacante pode chegar a comprometer a segurança de uma organização, é necessário entender como as empresas da região se protegem e onde podem estar as opções de melhora para incrementar os níveis de proteção.

A segurança da informação deve ser abordada a partir de um enfoque por camadas que não devem estar somente baseadas em tecnologia. Talvez, quando se fale de controle de segurança, o primeiro que venha à cabeça de muitos seja contar com tecnologias de proteção. Ainda que isso seja absolutamente necessário, também é preciso contar com políticas e planos para administrar a segurança da informação, assim como também com planos contínuos de capacitação dos colaboradores.

Este último se vê refletido precisamente em que quase 98% das empresas na região conta com algum controle baseado na tecnologia, que pode incluir desde uma solução de segurança até um DLP. No entanto, 39% das empresas ainda não conta com políticas de segurança e apenas 28% classificam suas informações.

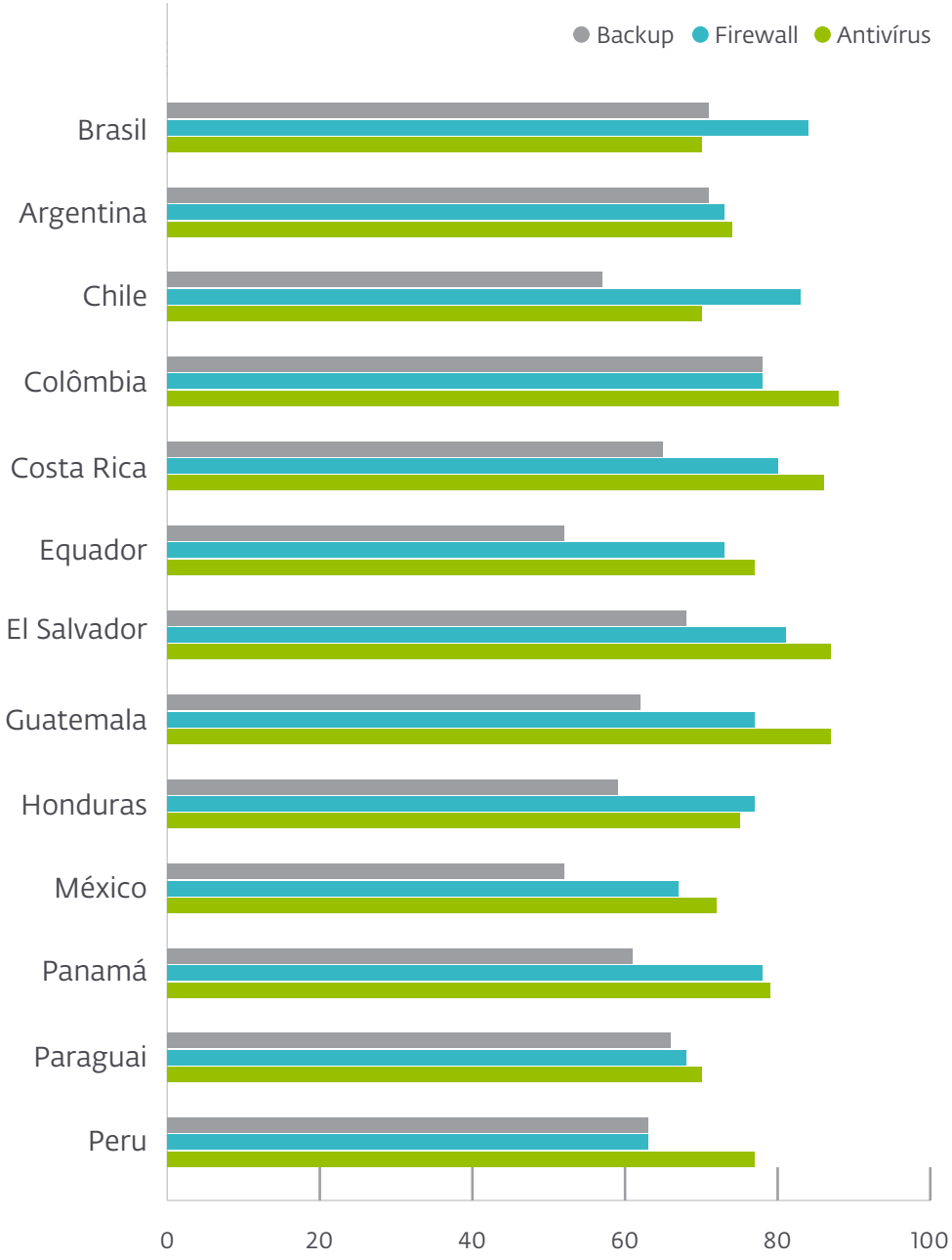
39% DAS EMPRESAS AINDA NÃO CONTA COM POLÍTICAS DE SEGURANÇA E APENAS **28%** CLASSIFICAM SUAS INFORMAÇÕES

> Controles

Uma das questões mais surpreendentes é que as medidas mais básicas de controle, aquelas que se poderia esperar ver em todas as empresas como uma solução de segurança antivírus, um backup (como gestão e não cópias isoladas) ou uma solução de Firewall, não estão realmente implementadas na totalidade das empresas que participaram da pesquisa. De fato, este número chega a apenas 48% nas organizações abordadas.

O antivírus continua sendo a ferramenta de controle mais utilizada (78%), localizado como a primeira linha de defesa contra os atacantes. Não obstante, ainda que se trate de uma tecnologia fundamental que deve estar implementada, existe ainda 22% de empresas que não contam com uma solução antivírus entre suas barreiras de proteção.

GRÁFICO 9: Níveis de implementação de controles básicos de segurança por país



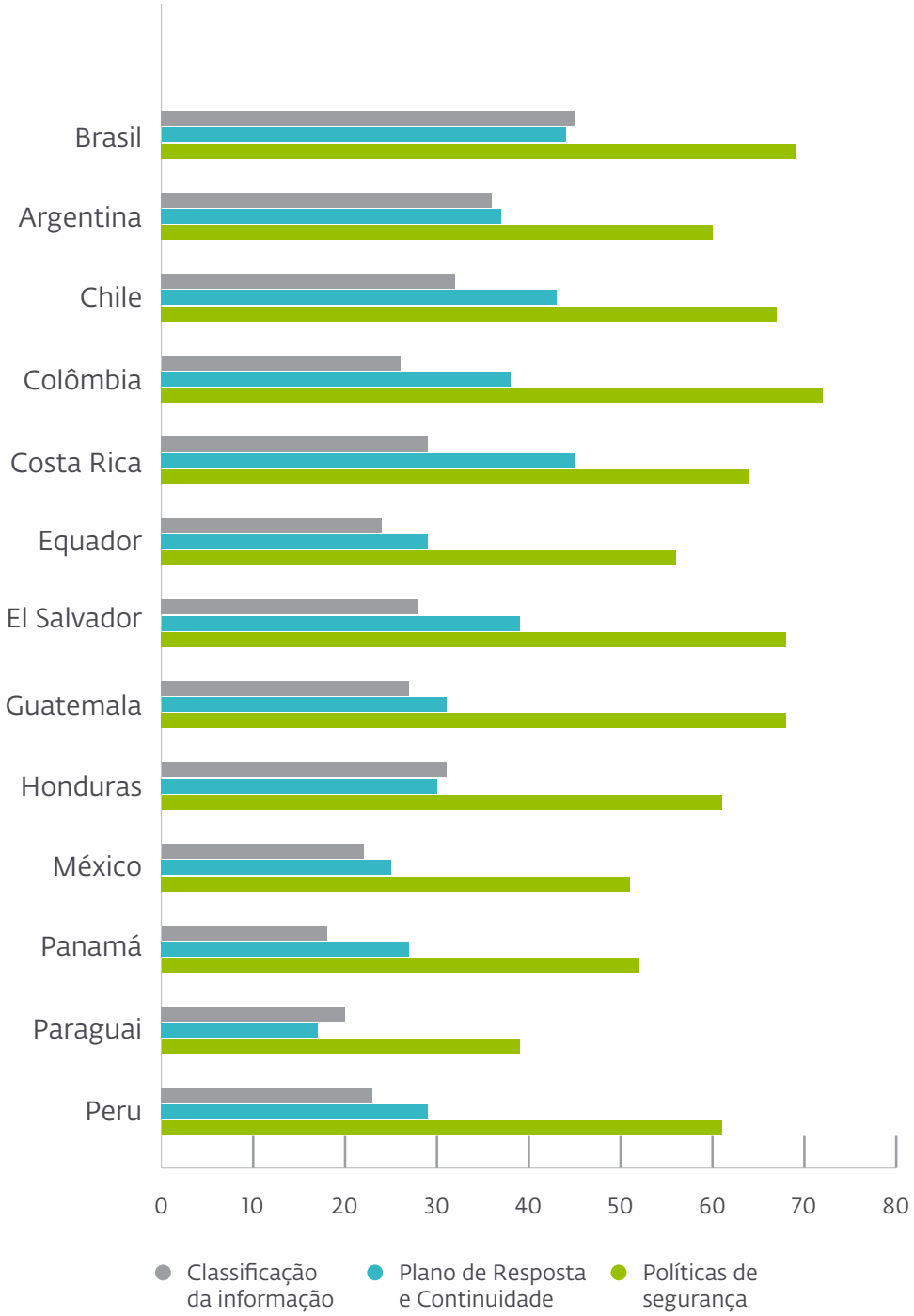
Dado o amplo leque de possibilidades que têm os atacantes para comprometer a segurança de uma empresa, nos últimos anos foram aparecendo novas tecnologias para complementar a proteção. No entanto, notamos que sua adoção ainda é bastante baixa. Por exemplo, um segundo fator de autenticação é considerado apenas por 17% das empresas que participaram da pesquisa (apenas superior a 13% da medição do ano anterior) e o mesmo valor se registra para as empresas que contam com um EDR (16% em 2018). Ambas as soluções se veem superadas apenas por 19% das empresas que criptografam suas informações (18% em 2018).

APENAS **17%** DAS EMPRESAS PESQUISADAS CONTA COM UMA FERRAMENTA DE FATOR DUPLO DE AUTENTICAÇÃO.

> Gestão

Como mencionamos, a tecnologia não é tudo no campo da segurança da informação, por isso é necessário complementá-la com uma gestão adequada. Ainda que os níveis de implementação de políticas de segurança acumulem uma porcentagem alta (61% das empresas declararam contar com elas) os números ainda não são os ótimos. Em países como o Paraguai, menos da metade das empresas pesquisadas disse contar com este tipo de controles (39%) e no México apenas 51%, isto é, 1 de cada 2 empresas assegura tê-los implementado.

GRÁFICO 10: Níveis de implementação de práticas de gestão para a segurança por país



Cabe destacar que, das empresas que contam com uma política de backup entre suas implementações de segurança, apenas 71% conta com uma política de classificação da informação.

Ao analisar os dados, é preocupante também que apenas uma terceira parte (33%) das empresas que participaram da pesquisa conte com um plano de continuidade do negócio, número que não se modifica em relação ao ano anterior, apesar do avanço da tecnologia e das campanhas de conscientização. De fato, é crucial que as empresas saibam como responder no caso de ocorrer um incidente que possa por em risco as operações do negócio. Não se trata unicamente de ter uma resposta rápida e eficiente para a recuperação do incidente, mas também de adotar uma medida a mais de proteção para identificar as falhas e evitar que incidentes similares voltem a acontecer no futuro. Além disso, deve se destacar o impacto que isso poderia ter em suas finanças e em sua reputação frente a sua cadeia de valor (clientes e associados).

APENAS **33%** DAS EMPRESAS PESQUISADAS CONTE COM UM PLANO DE CONTINUIDADE DO NEGÓCIO

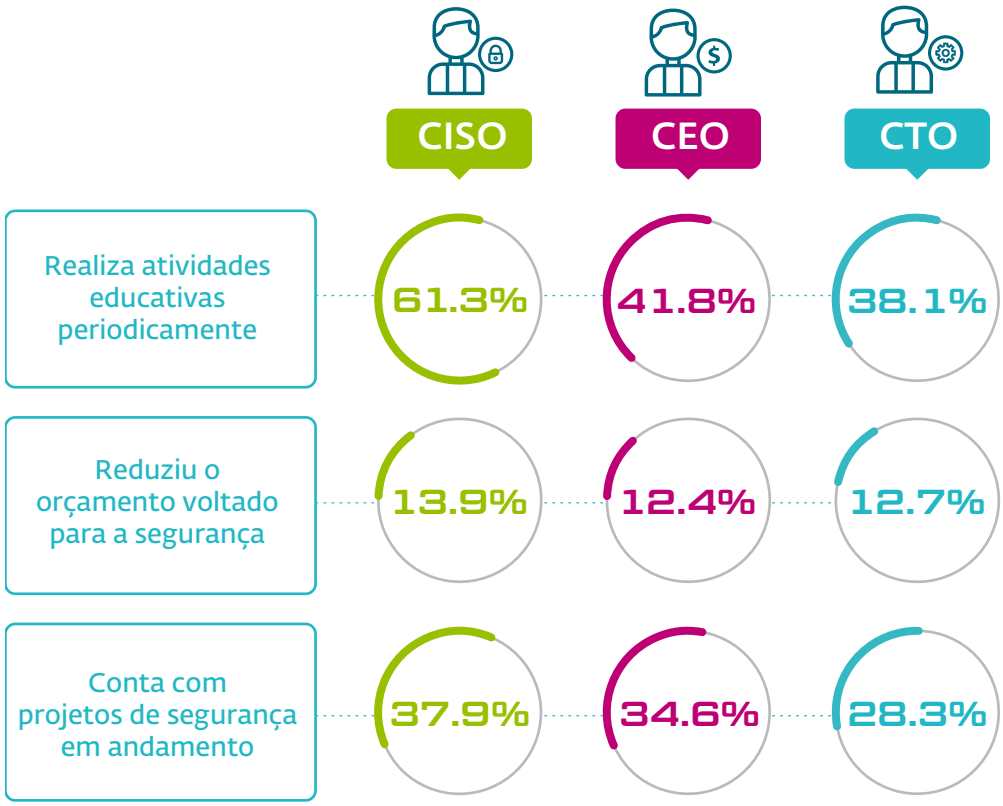
A baixa adoção de metodologias para a classificação da informação das empresas é outro aspecto preocupante. Em nível regional, este tipo de práticas chega a apenas 28% das empresas que participaram da pesquisa. Já mencionamos que 2019 teve recordes históricos em casos de fugas de informação e brechas de segurança. Por isso, é necessário que as empresas saibam onde estão armazenadas suas informações e que características têm para poder implementar os controles que realmente necessitam.

03

A visão do C-Level

Diante do panorama de incidentes apresentado, as preocupações recorrentes e a adoção de controles, parece interessante entender como estão organizadas as empresas para enfrentar os desafios relacionados, precisamente, com a gestão da segurança da informação. Além dos controles de segurança, entram em jogo aqui novas dimensões que ampliam o alcance da gestão.

Dentro das pesquisas direcionadas ao C-Level, obtivemos informações a respeito das atividades ligadas à educação dentro das organizações, as variações de orçamento destinado à segurança e o desenvolvimento de projetos de segurança.



Sem dúvidas, aquelas empresas que contam com um CISO encarregado das atividades de segurança parecem ter um melhor cenário para o desenvolvimento de uma estratégia de segurança, mais além da adoção de tecnologias de segurança. Por exemplo, a implemen-

tação de atividades periódicas de educação naquelas empresas onde haja um CISO (61,3%) é maior que naquelas onde não existe essa figura (41,8% e 38%).

O orçamento para desenvolver este tipo de atividades será sempre um fator fundamental e, ainda que em linhas gerais, a porcentagem de empresas que reduziu seu orçamento em segurança seja menor que 15%, (cifra que em 2018 era menor em empresas que contavam com um CISO), este período pode se ver afetado por variáveis macroeconômicas da região.

> Educação

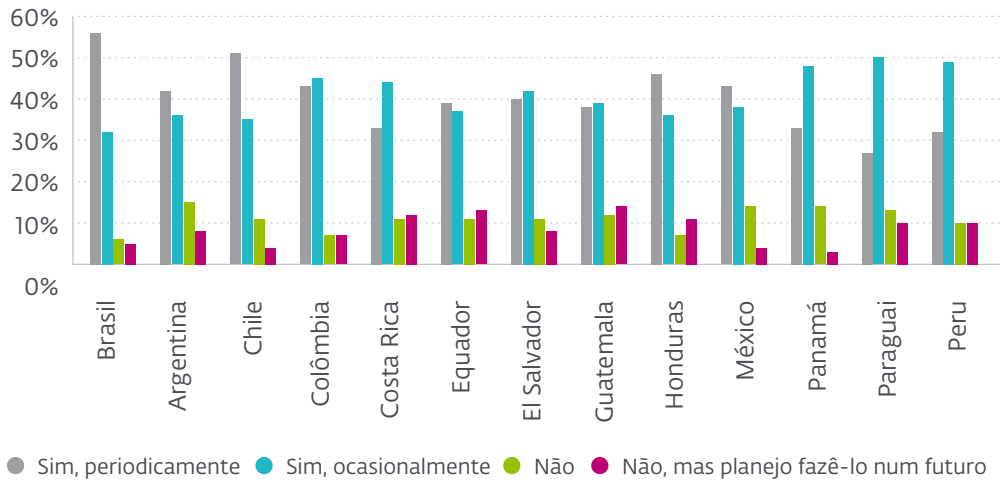
Novamente, cabe destacar que a figura de um responsável de segurança gera um movimento positivo nas atividades e projetos relacionados com a segurança dentro da empresa. Mas que impacto tem a realização destas atividades?

Incidentes com códigos maliciosos
A incidência deste tipo de ataques caiu de **34%** a **29%** naquelas empresas que implementam capacitações de segurança de forma periódica.

A porcentagem de empresas que realizou atividades periódicas de educação e se viu afetada por incidentes de segurança é menor que o daquelas empresas nas quais não se leva adiante este tipo de atividades.

Ainda que não haja maneira de medir de forma direta a incidência deste tipo de atividades, é possível identificar o papel que tem o nível de educação dos usuários como fator diferencial para garantir a segurança da informação. Isso é importante já que a gestão da segurança é um processo integral cuja análise não se pode limitar unicamente à tecnologia e aos controles que se implementam.

GRÁFICO 11: Executa atividades de conscientização



> Investimento

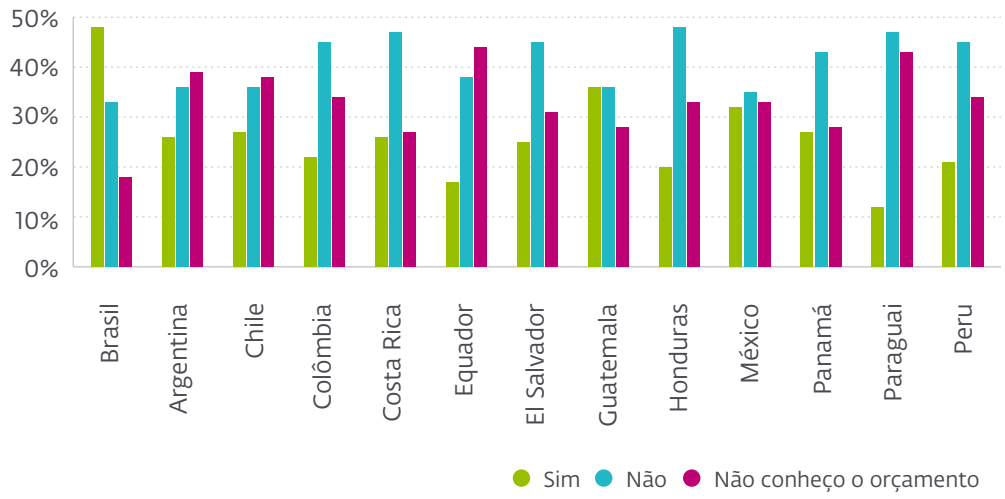
Talvez uma das queixas mais recorrentes que acontece no interior de muitas empresas é a falta de orçamento para a área de segurança. Essa reclamação manteve números similares (64%) ao longo do tempo, ainda que em 2019 a porcentagem de empresas que manifestou a falta de orçamento foi de 75%.

EM 2019, **75%** DAS EMPRESAS MANIFESTOU A FALTA DE ORÇAMENTO DESTINADO À ÁREA DE SEGURANÇA.

A variação do orçamento atribuído aos projetos de segurança sofreu uma notável queda em relação ao ano anterior, que se mantinha em uma média de 40%. Este ano, apenas 20% das empresas disse ter aumentado o orçamento de segurança em relação ao ano anterior e, ainda que mude de acordo com o tamanho da empresa, apenas 9% o reduziu.

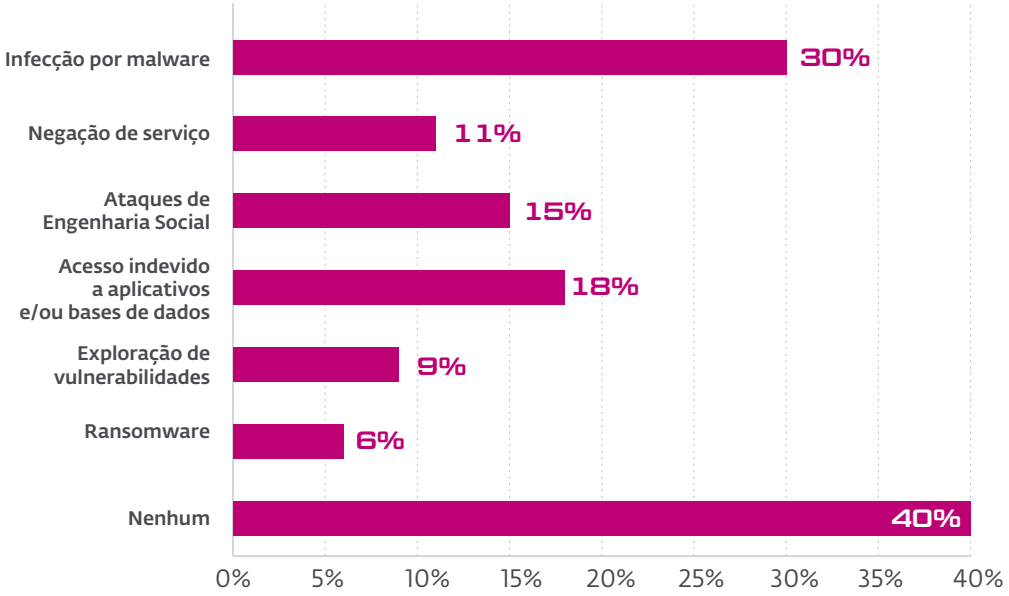
Estes números refletem a necessidade de que as empresas pensem em alternativas diferentes para desenvolver seus projetos de segurança. Talvez seja necessário um maior esforço na hora de investir tempo e recursos para alcançar resultados ótimos.

GRÁFICO 12: Considera suficiente o orçamento atribuído para a área de segurança da sua empresa?

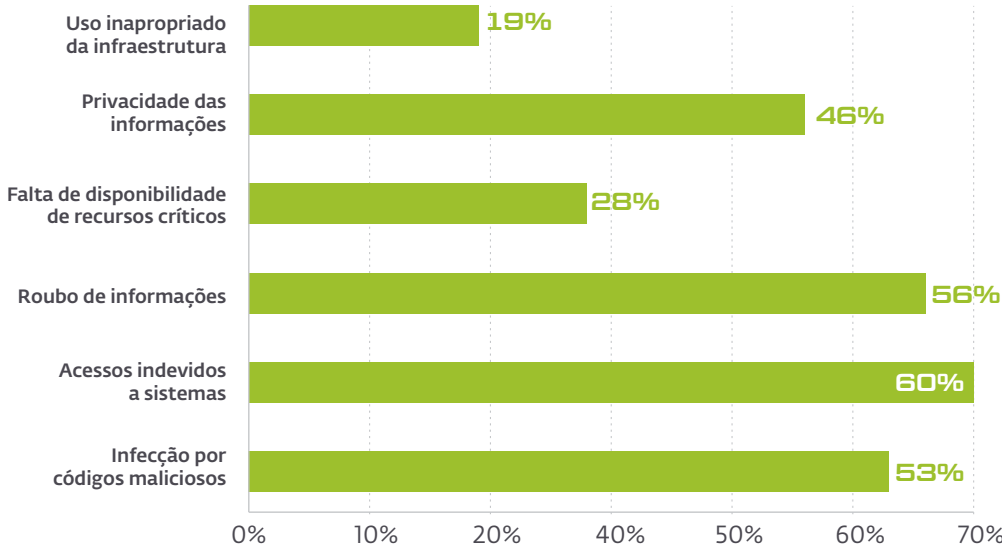


Anexo:
dados estatísticos

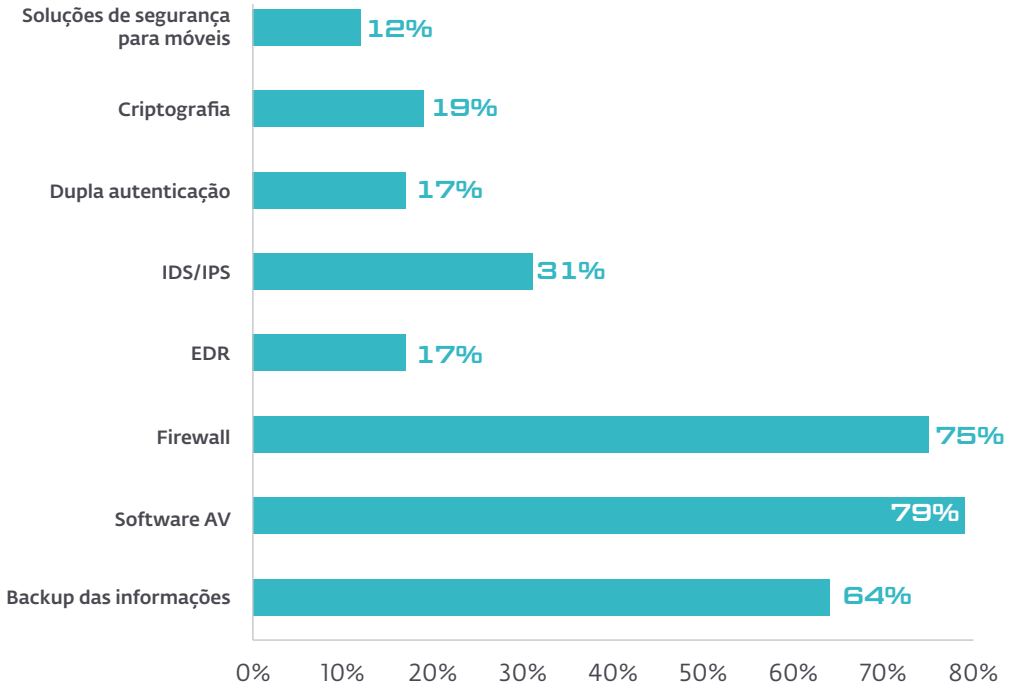
INCIDENTES DE SEGURANÇA



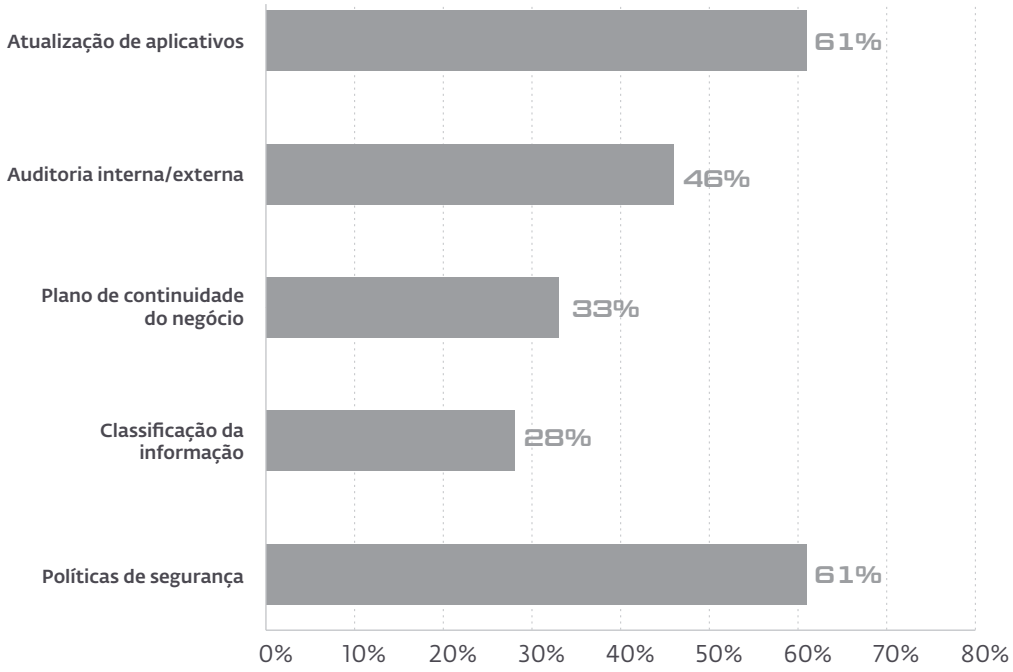
PREOCUPAÇÕES RELACIONADAS À SEGURANÇA



CONTROLES BASEADOS EM TECNOLOGIA



CONTROLES BASEADOS EM GESTÃO



SOBRE A ESET

+ 110 milhões de usuários em todo o mundo	**13** centros de pesquisa e desenvolvimento no mundo
+ 400 mil clientes corporativos	**200** países e territórios

Para mais informações sobre a ESET, visite: www.eset.com/br

Para estar atualizado sobre as principais notícias relacionadas com a segurança da informação, visite: www.welivesecurity.com/br