EDIÇÃO AMÉRICA LATINA

THALES
Building a future we can all trust

SUMÁRIO EXECUTIVO DE 2021

Relatório sobre ameaças a dados de 2021

Segurança de dados na era de acelerada migração para nuvem e trabalho remoto.

#2021DataThreat

cpl.thalesgroup.com

Conteúdo

Sobre este estudo

A pandemia da COVID-19 teve um impacto imediato e dramático nas equipes de TI em todo o mundo, e seus efeitos de longo prazo ainda estão evoluindo. A edição latino-americana (LATAM) do relatório sobre ameaças a dados da Thales de 2021 examina diferentes aspectos desses impactos em uma ampla pesquisa com profissionais de segurança e líderes executivos. Neste relatório executivo procuramos entender como a América Latina enfrentou as ameaças resultantes da pandemia juntamente com as opiniões de participantes sobre vários aspectos da segurança de dados.

O relatório sobre ameaças a dados da Thales de 2021 baseia-se em uma pesquisa com mais de 2.600 profissionais de segurança e líderes executivos, incluindo 200 da América Latina.

451 Research

S&P Global
Market Intelligence

Fonte: 2021 Data Threat, pesquisa personalizada da 451 Research, parte da S&P Global Market Intelligence, encomendada pela Thales

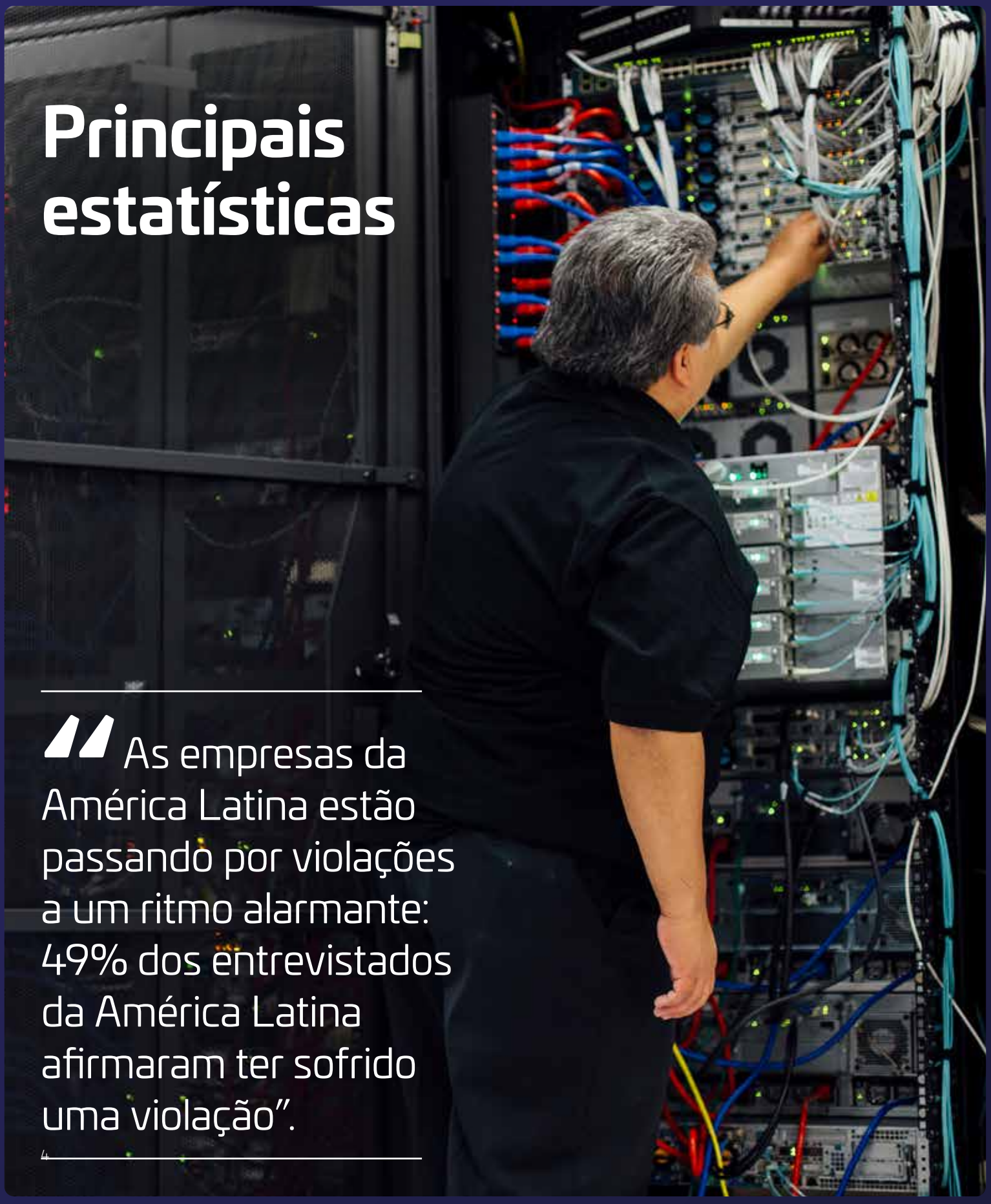
Nossos patrocinadores:

SENETAS versasec

KEYFACTOR

Adistec F9C Walking Together FIRST TECH

Principais estatísticas



“As empresas da América Latina estão passando por violações a um ritmo alarmante: 49% dos entrevistados da América Latina afirmaram ter sofrido uma violação”.

Os profissionais de segurança da América Latina estão enfrentando desafios, mas identificaram um caminho a ser seguido

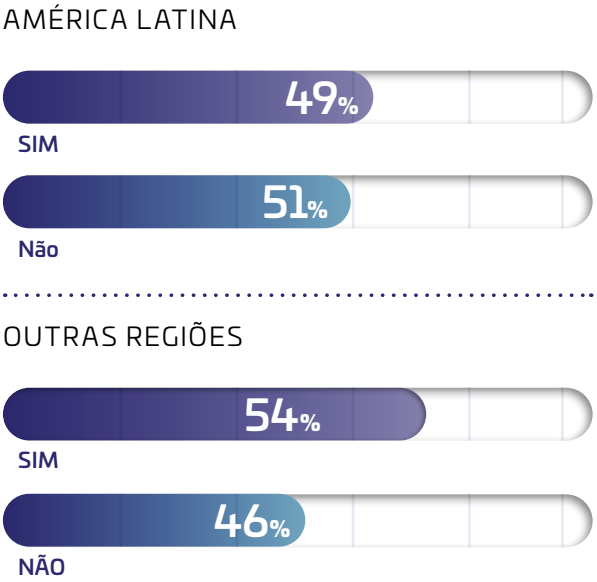
Os dados coletados dos países da América Latina espelham muitas das outras geografias que estudamos. Por exemplo, as empresas da América Latina estão passando por violações a um ritmo alarmante: 49% dos entrevistados da América Latina afirmaram ter sofrido uma violação. Além disso, cerca de um terço destes entrevistados sofreu uma violação no último ano. E o problema não está melhorando: 38% das empresas afirmaram ter visto um aumento no volume, gravidade e/ou escopo dos ciberataques nos últimos 12 meses. Embora estas porcentagens estejam abaixo da média global, os ataques nesta região ainda estão aumentando, e os profissionais de segurança estão se preparando para combate-los.

IMAGEM 1

Comparação das violações da América Latina com outras regiões

P: Sua empresa já sofreu alguma violação?

Entrevistados: América Latina e outras regiões



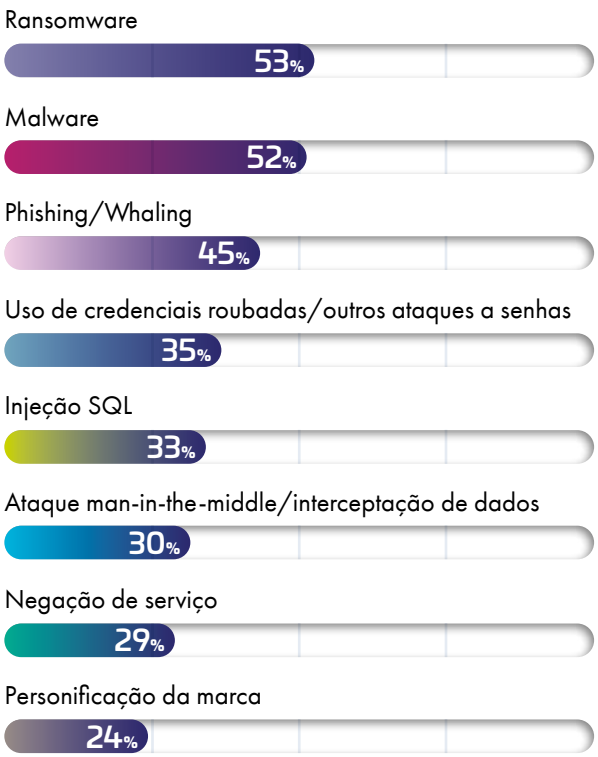
Fonte: pesquisa personalizada sobre ameaças a dados de 2021 da 451 Research

IMAGEM 2

Maior aumento de ataques que utilizam ransomware, malware e phishing/whaling

P: De que tipos de ataques/ameaças você tem visto um aumento?

Entrevistados: América Latina



Fonte: pesquisa personalizada sobre ameaças a dados de 2021 da 451 Research

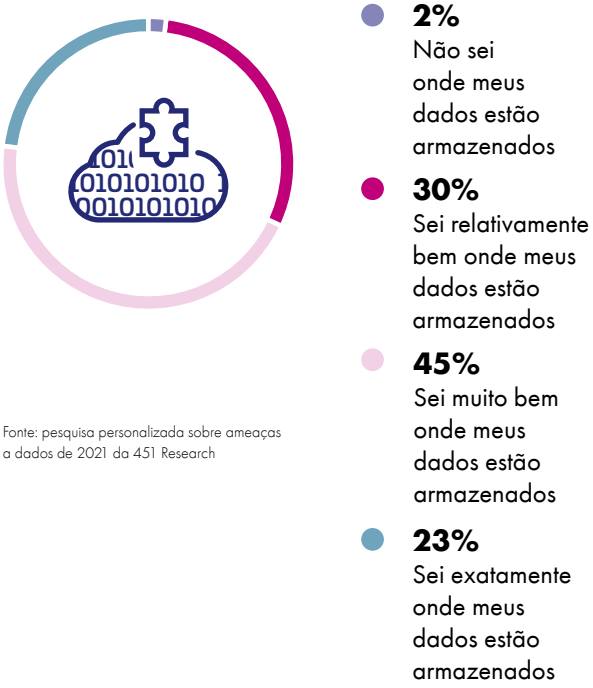
Um número maior de ataques a dados mostra ainda que os países da América Latina têm experimentado o aumento de ataques como ransomware (53%), malware (52%) e phishing/whaling (45%), o que é consistente com os resultados globais. Com o aumento do número de ataques, estas empresas estão empregando diferentes tecnologias para proteger seus dados. Os entrevistados consideram a gestão de chaves e módulos de segurança de hardware (42%) como a escolha mais eficaz para proteger dados confidenciais contra ataques cibernéticos, seguida pela criptografia (40%). Não surpreendentemente, a criptografia/gestão de chaves também teve prioridade de gastos na América Latina (46%).

IMAGEM 3

Apenas aproximadamente um terço dos entrevistados da América Latina têm conhecimento completo de onde seus dados são armazenados

P: Você sabe onde todos os seus dados estão armazenados?

Entrevistados: América Latina



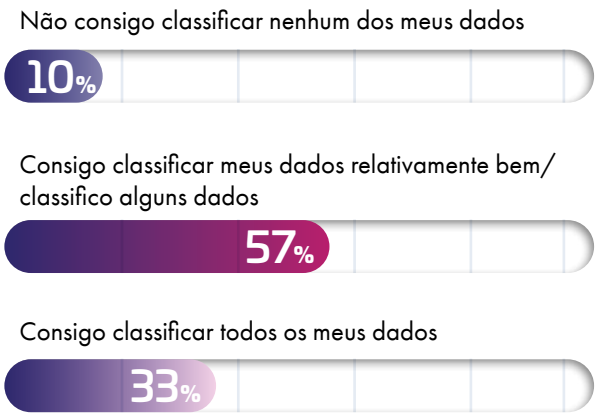
Fonte: pesquisa personalizada sobre ameaças a dados de 2021 da 451 Research

IMAGEM 4

Somente um terço dos entrevistados da América Latina sabe classificar totalmente seus dados

P: Você consegue classificar todos os seus dados?

Entrevistados: América Latina



Fonte: pesquisa personalizada sobre ameaças a dados de 2021 da 451 Research

No entanto, ainda há trabalho a ser feito. Infelizmente, apenas 23% das empresas de países da América Latina têm conhecimento completo do local onde seus dados são armazenados (24% em outras regiões), e apenas um terço é capaz de classificar completamente seus dados (31% em outras regiões).

46%

dos entrevistados da América Latina disseram que a criptografia/gestão de chaves era sua prioridade de investimento.

A COVID-19 traz novos desafios à segurança

A COVID-19 tem afetado os processos empresariais, mudando as formas de interação dos funcionários com seu trabalho, uns com os outros e com o mundo exterior. Por isso, o trabalho do profissional de segurança se transformou com a mudança do trabalho do ambiente de escritório para o trabalho remoto. Além disso, a maior ênfase à nuvem aumentou o ritmo de sua adoção que já estava em andamento, aumentando a complexidade necessária para proteger os negócios.

Com relação à preparação para a pandemia, a América Latina ficou dentro da média global. Apenas 24% dos entrevistados relataram que sua infraestrutura de segurança estava "muito preparada" para lidar com os diversos de riscos associados ao novo ambiente operacional de negócios. Pouco menos da metade dos entrevistados da América Latina (46%) não estavam preparados até certo ponto (28% estavam "um pouco despreparados" e 18% "nada preparados").

O choque da pandemia e os arranjos de trabalho remoto subsequentes também mudaram a mentalidade em relação à segurança; 86% dos entrevistados estavam "um pouco" ou "muito" preocupados com os riscos e ameaças à segurança devido ao trabalho remoto de funcionários (40% "muito preocupados" e 46% "relativamente preocupados"). Não surpreendentemente, o investimento mais importante durante a COVID-19 foi em segurança e privacidade - 46% das empresas seguiram este caminho. Outros planos de gastos incluíram investimentos em infraestrutura e nuvem (28% dos entrevistados) e investimentos em nuvem distribuída (26%).

24%

dos entrevistados relataram que sua infraestrutura de segurança estava "muito preparada" para lidar com os diversos de riscos associados ao novo ambiente operacional de negócios.

86%

dos entrevistados estavam "relativamente" ou "muito" preocupados com os riscos e ameaças à segurança com os riscos e ameaças à segurança devido ao trabalho remoto de funcionários.

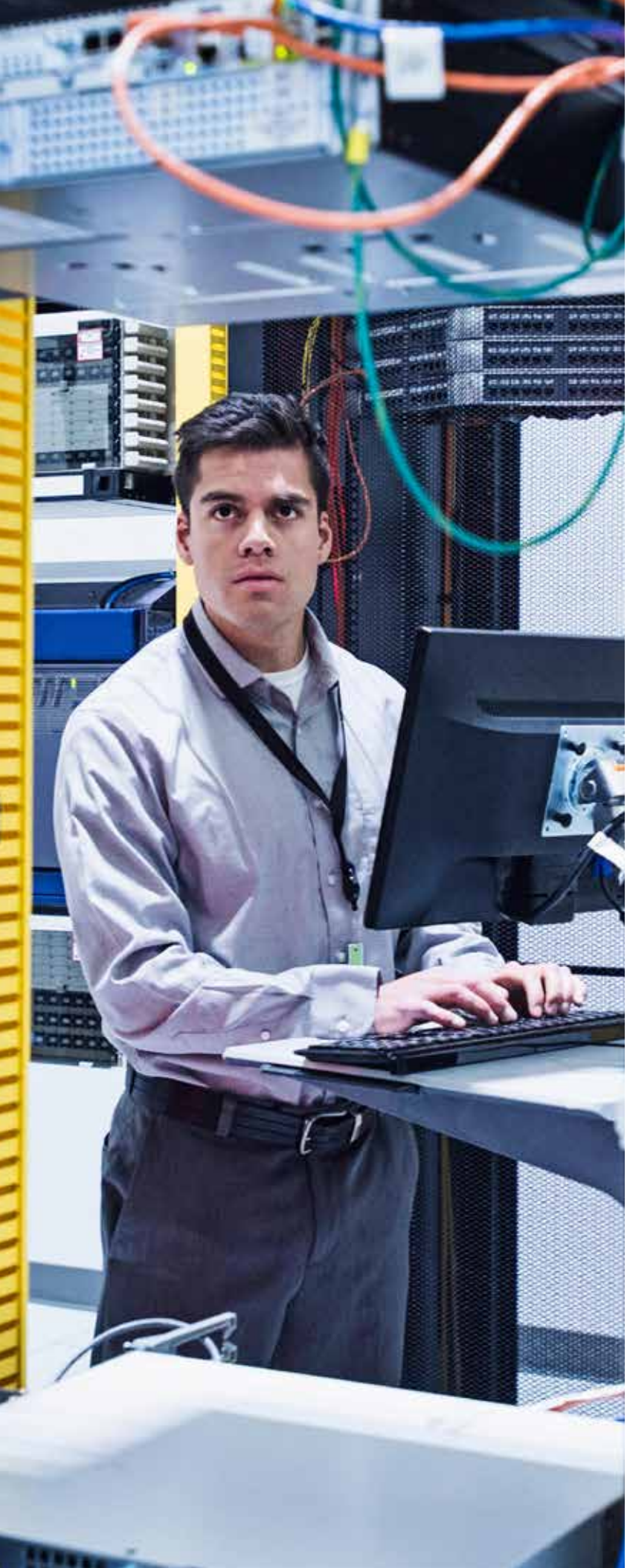


IMAGEM 5

Preocupação com riscos/ ameaças à segurança/ ameaças devido ao trabalho remoto de funcionários.

P: Quão preocupado você está com riscos/ ameaças à segurança devido ao trabalho remoto de funcionários?

Entrevistados: América Latina

- **40%** Muito preocupado
- **46%** Relativamente preocupado
- **11%** Relativamente despreocupado
- **2%** Nada preocupado

Fonte: pesquisa personalizada sobre ameaças a dados de 2021 da 451 Research

Cresce o interesse em estratégias de confiança zero

Com os funcionários das empresas trabalhando remotamente devido à pandemia, muitas técnicas de segurança que exigiam um ambiente de rede corporativa controlada precisaram ser ajustadas para acomodar funcionários que estavam em sua maioria em casa. Com este desenvolvimento, as estratégias de confiança zero que se concentram em métodos baseados em identidade para conceder acesso a recursos e dados ganharam popularidade. Especificamente, 28% das empresas da América Latina disseram que estão utilizando uma estratégia formal de confiança zero e adotaram ativamente uma política de zero confiança. Uma porcentagem semelhante (28%) dos entrevistados observou que a confiança zero molda em grande parte a estratégia utilizada para segurança em nuvem. Um número ainda maior (42%) utiliza "alguns conceitos" da política de confiança zero, o que possivelmente significa uma maior adoção das tecnologias que virão.

Trabalho remoto e confiança zero

As empresas demonstraram uma confiança dúbia em seus produtos de segurança de acesso atuais e, consequentemente, em sua capacidade de possibilitar que seus funcionários trabalhem remotamente de forma segura e fácil. Muitas questões relativas ao fornecimento adequado de dados e aplicativos já estavam presentes em empresas antes da pandemia, portanto, esta mudança dramática no ambiente de trabalho só complicou ainda mais as coisas. Houve uma divisão quase uniforme entre aqueles que estavam confiantes em sua tecnologia de acesso atual e aqueles que não estavam: quase metade (49%) das empresas estavam de "um pouco" a "muito" confiantes em suas soluções de segurança de acesso atuais para permitir que seus trabalhadores realizassem seus trabalhos de forma segura e fácil, enquanto 51% estavam "relativamente" ou "nada" confiantes.

IMAGEM 6

Nível de confiança das empresas em sua capacidade de proporcionar um trabalho remoto seguro

P: Em que medida você está confiante de que suas tecnologias atuais de segurança de acesso podem efetivamente permitir que os funcionários trabalhem remotamente de forma segura e fácil?

Entrevistados: América Latina

- **21%** Muito confiante
- **28%** Relativamente confiante
- **30%** Relativamente não confiante
- **20%** Nada confiante

Em uma tentativa de resolver esta questão, 43% das empresas se voltaram para o acesso condicional. Quase a mesma porcentagem implantou acesso à rede com política de confiança zero e perímetro definido por software, enquanto 38% optou por implantar um gerenciamento de acesso baseado em nuvem, como identidade como serviço ou single sign-on, porcentagens de acordo com a média global.

Gerenciamento de chaves, criptografia e tokenização são as principais opções para proteger dados em nuvem

As empresas continuam a transferir suas estratégias para a nuvem para capturar os muitos benefícios que ela oferece: resposta mais rápida às necessidades comerciais, redução de custos, implementação mais eficiente de recursos e lançamentos mais rápidos de produtos e serviços. Por sua vez, para atingir objetivos específicos, elas estão começando a utilizar a nuvem para armazenar dados confidenciais. Em geral, a maioria (77%) dos entrevistados da América Latina disse ter colocado até metade das cargas de trabalho e dos dados da empresa em nuvem.

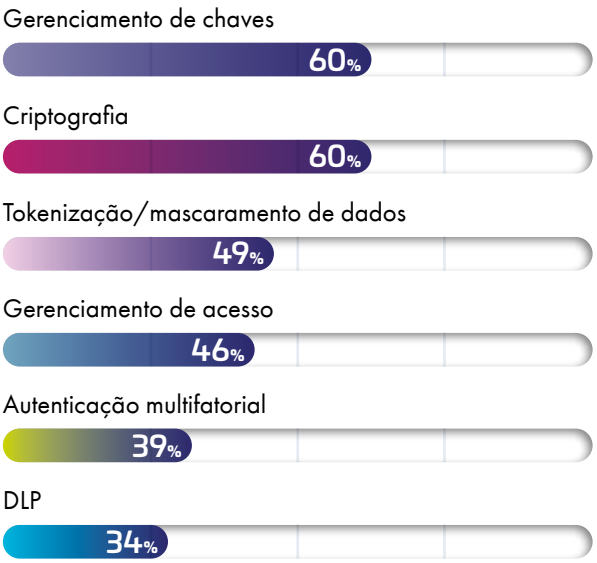
À medida que as empresas transferem mais de seus dados confidencias para a nuvem, estratégias para proteger esses dados são justificáveis particularmente porque um terço dessas empresas sofreu ataques a seus dados que envolveram dados e aplicativos na nuvem (ligeiramente abaixo da média global de 41%), enquanto apenas no último ano, 40% sofreram um ataque ou não passaram em uma auditoria envolvendo dados e aplicativos na nuvem. Para ajudar a evitar violações de dados confidenciais guardados em nuvem, as empresas escolheram gerenciamento de chaves (60%), criptografia (60%) e tokenização e mascaramento de dados (49%) como as principais opções para proteger dados confidenciais mantidos em nuvem. Entretanto, quando se trata de proteger esses dados na prática, uma grande parte dos dados confidenciais guardados em nuvem permanece não criptografada - em relação a dados confidenciais armazenados em nuvem, apenas 20% das empresas criptografam mais da metade deles.

IMAGEM 7

Gerenciamento de chaves, criptografia, tokenização e mascaramento de dados são as principais tecnologias utilizadas para proteger dados confidenciais em nuvem

P: Quais tecnologias de segurança sua empresa utiliza para proteger dados confidenciais em nuvem?

Entrevistados: América Latina



Fonte: pesquisa personalizada sobre ameaças a dados de 2021 da 451 Research

40%

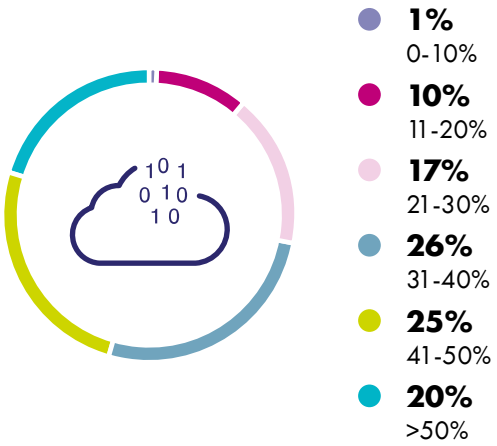
sofreram uma violação ou não passaram em uma auditoria envolvendo dados e aplicativos, apenas no último ano.

IMAGEM 8

Um quinto das empresas criptografa mais de 50% de seus dados confidenciais

P: Que porcentagem de seus dados confidenciais armazenados em nuvem é criptografada?

Entrevistados: América Latina



Fonte: pesquisa personalizada sobre ameaças a dados de 2021 da 451 Research

Estratégias multinuvens aumentam a complexidade

Proteger a nuvem se torna mais desafiador à medida que diferentes provedores de nuvem são adotados. Os entrevistados da América Latina utilizam diversos provedores de nuvem, sendo o mais popular a AWS (58%), seguida da Azure (40%) e da GCP (24%). Essas empresas também misturam os serviços de diferentes provedores de nuvem para atender às necessidades de seus negócios, com 50% dos entrevistados trabalhando com dois provedores de PaaS e 20% com três. Para implementações SaaS, 37% dos entrevistados usaram 26-50 aplicativos SaaS, enquanto 22% usaram mais de 50.

> “Os entrevistados indicaram a complexidade como o principal desafio da implementação da segurança de dados”.

O gerenciamento de chaves também se torna um problema quando são utilizadas múltiplas plataformas de nuvem, aumentando a complexidade do seu desafio. Pouco mais de um terço (34%) das organizações da LATAM usam de cinco a sete produtos de gerenciamento de chaves, que podem variar de fornecedores de gerenciamento de chaves corporativos a soluções de origem local, planilhas e arquivos simples e HSMs. Além disso, 15% das empresas afirmaram utilizar de 8 a 10 produtos para fazer o gerenciamento de chaves.

> “As empresas também devem escolher como criptografam e onde gerenciam suas chaves”.

Estratégias multinuvens aumentam a complexidade - continuação

As empresas também devem escolher como criptografam e onde gerenciam suas chaves. Um terço das empresas depende "muito" ou "totalmente" de seu provedor de nuvem para criptografar dados em ambientes IaaS e PaaS, enquanto 15% usam somente as ferramentas do provedor de nuvem e 20% preferem criptografá-los internamente. Com relação ao gerenciamento de chaves, 31% dos entrevistados utilizam seu provedor de nuvem para controlar "todas ou a maioria" das chaves de criptografia, e 17% controlam suas próprias chaves. Quase um quarto (23%) dos entrevistados disse que seu provedor de nuvem controla todas as suas chaves de criptografia. Ao gerenciar suas próprias chaves, as empresas podem acrescentar uma camada extra de segurança, protegendo essas informações de ataques ao provedor de nuvem e de ataques internos Em outros casos, as informações não são armazenadas com o provedor de nuvem por razões de conformidade. Para alguns dados não críticos, o armazenamento em nuvem pode ser a melhor opção, mas para dados altamente confidenciais as empresas necessitam de mais proteção, o que outras opções de segurança podem oferecer.

Avançando

Como a pandemia continua a afetar empresas em todo o mundo, a maioria continua a enfrentar uma série de ataques e violações como malware, ransomware e phishing, independentemente de sua localização geográfica. Além disso, devido à continuação da exigência de trabalho remoto, as equipes de segurança precisam lidar com novos cenários, além da complexidade apresentada por múltiplas nuvens, ambientes híbridos e uso abrangente de aplicativos. Para capturar totalmente os benefícios da nuvem - como respostas mais rápidas às necessidades comerciais, redução de custos, implantações mais eficientes de recursos e lançamentos mais rápidos de produtos e serviços - as empresas precisarão fornecer acesso a dados e serviços de forma rápida, conveniente e, o mais importante, de maneira segura. Com a conscientização sobre os diversos desafios que enfrentam e conhecimento das muitas ferramentas à sua disposição, as empresas da América Latina estão no caminho para capturar esses benefícios, reduzindo ao mesmo tempo a probabilidade de ciberataques bem sucedidos.

THALES

Building a future we can all trust

Entre em contato conosco

Para saber as localizações de todos os escritórios e obter informações de contato, acesse cpl.thalesgroup.com/contact-us

Para baixar o relatório completo com recomendações da 451 Research, acesse

cpl.thalesgroup.com/data-threat-report