CPL.thalesgroup.com #2020DataThreat

THALES

A segurança de dados evolui para uma abordagem Zero Trust na América Latina

Relatório sobre ameaças a dados - Thales 2020

Edição para América Latina

RESEARCH AND ANALYSIS FROM:

IDC ANALYZE THE FUTURE

Sobre este estudo

Este relatório é sobre as conclusões de mais de 200 executivos latino-americanos do Brasil e do México e traz comparações e contraste com a pesquisa online global da IDC com 1.723 entrevistados com responsabilidade ou influência sobre TI e segurança de dados. Os entrevistados são de 16 países: os países latino-americanos da amostra mais Austrália, França, Alemanha, Índia, Indonésia, Japão, Malásia, Holanda, Nova Zelândia, Singapura, Coreia do Sul, Suécia, Reino Unido e Estados Unidos. As empresas representam uma série de indústrias, com ênfase principal em saúde, serviços financeiros, varejo, tecnologia e organizações governamentais federais. Os cargos variam entre executivos C-level, incluindo diretor executivo, diretor financeiro, diretor de dados, diretor de segurança da informação, diretor de ciência de dados, diretor de riscos, vice-presidente/vice-presidente sênior, administrador de TI, analista de segurança, engenheiro de segurança e administrador de sistemas. Os entrevistados representam empresas de diversos tamanhos, com a maioria tendo entre 500 e 10.000 funcionários. Esta pesquisa foi realizada em novembro de 2019. Para conclusões e análise global, acesse cpl.thalesgroup.com/data-threat-report.

Conteúdo

Nossos patrocinadores:

Sumário Executivo

As empresas enfrentam problemas atualmente em seus mercados e cadeias de logística que estão criando desafios diferentes dos que enfrentaram no passado. À medida que as empresas revisam, recalibram, e em alguns casos reinventam operações fundamentais, o sucesso agora mais do que nunca depende da adoção de tecnologias de transformação digital (DX) incluindo nuvem, tecnologia móvel e Internet das Coisas (IoT). A transformação digital desempenha um papel fundamental para ajudar empresas a se adaptarem às novas normas da atualidade, bem como para se preparar para as realidades empresariais após a pandemia de COVID-19.

No momento, a América Latina está atrasada em relação a outras regiões em termos de transformação digital. Mas este aparente problema, na verdade oferece às empresas latino-americanas uma oportunidade de ultrapassar outros países à medida que aceleram a transformação digital para transformar e evoluir seus negócios. A pesquisa da IDC mostra que para algumas empresas da América Latina, a transformação digital está realmente bem avançada. Vinte e sete por cento das empresas latino-americanas do nosso estudo disseram que estão agressivamente causando disrupção nos mercados em que participam ou que estão adquirindo capacidades digitais que permitem uma maior agilidade empresarial. Além disso, 57% das empresas desta região esperam ter até 25% das suas receitas geradas por serviços digitais (fonte: IDC, tendências de investimentos na América Latina no segundo semestre de 2019).

Embora a transformação digital possa ter um imenso valor, ela também torna a segurança de dados mais complexa. Isto é especialmente verdade nos tempos incertos da atualidade. À medida que a transformação digital acelera, as equipes de segurança precisam correr para alcançar as equipes de negócios/TI que podem estar criando ainda mais vulnerabilidades e aumentando dramaticamente os riscos para as empresas. As empresas dependem, e esta dependência está aumentando continuamente, da quantidade de dados armazenados em nuvem. As empresas latino-americanas estão chegando a um ponto crítico em que 49% de todos os dados são armazenados em nuvem, e 45% desses dados são confidenciais. Além disso, a maioria das empresas latino-americanas estão administrando ambientes de nuvem múltipla. Tudo isso torna os ambientes de dados atuais cada vez mais complexos. E a complexidade é um grande problema para a segurança de dados.

49%

dos **dados são armazenados em nuvem,** e **45% desses dados são confidenciais.**

73%

dos entrevistados latinos-americanos **acreditam que a computação quântica afetará suas empresas nos próximos cinco anos.**

No entanto, as empresas sofrem de dissonância cognitiva no que diz respeito à segurança de dados. Sessenta e dois por cento dos profissionais de segurança e TI da América Latina acreditam que não são nem um pouco vulneráveis. Mas suas empresas não estão implementando processos e investindo em tecnologias necessárias para proteger adequadamente contra o aumento de riscos a dados. Mais de metade das empresas foram violadas ou tiveram falhas em auditorias de segurança. E quando se trata de proteger dados em nuvem, a maioria das empresas espera, erroneamente, que seus provedores de nuvem cumpram ambas as partes de um modelo de responsabilidade que é compartilhado. Vinte e sete por cento das organizações na região consideram sua estratégia de nuvem como sua principal iniciativa ou o objetivo final de alcançar uma postura de segurança mais forte (fonte: Relatório de Segurança Cibernética da América Latina 2019, IDC).

O problema da dissonância cognitiva é mais extremo na América Latina do que em outras regiões globais, uma vez que a segurança de dados ainda representa uma pequena parte do orçamento total de segurança, em média, representa apenas 15% do orçamento total de TI. Quarenta e quatro por cento das empresas latino-americanas planejam aumentar os gastos com segurança de dados nos próximos 12 meses, cinco pontos percentuais a menos do que os 49% dos entrevistados globais que esperam que as despesas aumentem. Por outro lado, as empresas latino-americanas dizem que 37% do seu interesse em soluções de segurança está focado na segurança de dados, o que é uma porcentagem mais elevada do que em outras regiões. Este foco maior em dados foi provavelmente devido à nova lei de proteção de dados e privacidade estava para ser implementada no Brasil (Lei Geral de Proteção de Dados Pessoais -LGPD) mas sua aplicação foi adiada para 2021. Há outras iniciativas parecidas com diferentes padrões e penalidades em países como México, Colômbia, Chile e Argentina.

Nossos entrevistados da América Latina reconhecem que a computação quântica está chegando, o que promete complicar ainda mais a segurança de dados. Os requisitos de criptografia mudarão fundamentalmente quando a computação quântica estiver online, e 73% acreditam que ela afetará as empresas nos próximos cinco anos.

À medida que as empresas latino-americanas enfrentam desafios de segurança de dados cada vez maiores e mais complexos, tornam-se necessárias medidas mais inteligentes e melhores para tratar do tema. "As empresas latino-americanas precisam adotar uma abordagem multi-dimensional para a segurança de dados, assumindo responsabilidades de segurança compartilhadas na nuvem e adotando um modelo de gerenciamento de acesso de confiança zero que autentique e valide usuários e dispositivos que acessam aplicativos e redes, e também empregar soluções mais robustas de busca, proteção e prevenção de perda de dados e criptografia". É importante notar que a segurança de dados não deve prejudicar os esforços empresariais para realizar a transformação digital através do uso de estruturas flexíveis que conduzam à implementação discricionária do modelo de confiança.

A pandemia de COVID-19 muda tudo

O âmbito e a extensão da pandemia de COVID-19 criaram um problema para profissionais da área de recuperação de desastres e cibersegurança como nunca antes visto. Os departamentos de TI estão enfrentando condições adversas de operação e, além disso, muitos planos de backup que envolvem mudanças de localização geográfica ou instalações temporárias também são inadequados. Nunca antes tantas empresas foram forçadas a "se recuperar" e operar indefinidamente a partir do mesmo "desastre" em um período de tempo tão curto.

A nova realidade para muitos consiste em selecionar as práticas de segurança cibernética existentes - obter licenças para VPN, regras de firewall, e programas BYOD ao mesmo tempo que se constrói um plano que incorpora uma segurança cibernética mais dinâmica para uma maior resiliência no futuro.

Quando se trata de cibersegurança na era pós-COVID-19, há três questões importantes para as quais os diretores de informação precisam de respostas:

- Quais são as mudanças nos padrões de uso e arquitetura em meu ambiente de TI?
- Como estas mudanças afetam os riscos?
- Quais mudanças devo fazer em relação à minha postura de cibersegurança e ambiente de controle?

Com esta mudança completa da maneira de lidar com a segurança, pode-se esperar ver até um forte interesse em ferramentas de segurança de dados na era pós-COVID-19. Na verdade, os dados coletados pela IDC descobriram que 42% das empresas esperam que a demanda por investimentos em tecnologias de segurança de dados aumente devido à COVID-19. Tecnologias e ferramentas de segurança como recuperação de desastres, autenticação multi-fator e criptografia serão ainda mais relevantes à medida que empresas e outras organizações procuram proteger o acesso remoto dos funcionários e porque cada vez mais cargas de trabalho e dados são transferidos para a nuvem.

Fontes:

Lindstrom, P., 2020, COVID-19 Impact on Data Security Spend by Size of Business, IDC

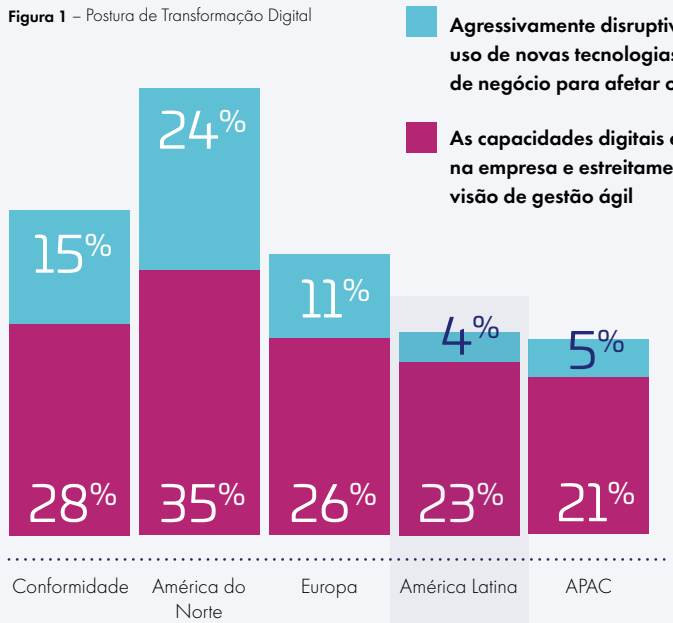
Dickson, F. and Westervelt, R., 2020, Post-COVID-19: A CIO Recovery Guide — Cybersecurity, IDC

01
Principais conclusões

Atraso da América Latina na Transformação Digital

Em todo o mundo, as empresas estão usando a transformação digital para reinventar totalmente seus negócios e aproveitar tecnologias digitais como nuvem, tecnologia móvel e Internet das Coisas. Mas esta tendência está mais lenta na América Latina do que em outras regiões. Trinta e sete por cento das organizações latino-americanas disseram que estão aplicando a transformação digital de maneira ad hoc. Vinte e sete por cento dos entrevistados latino-americanos disseram que estão agressivamente causando disrupção os mercados em que participam ou que estão adquirindo capacidades digitais que permitem uma maior agilidade empresarial (em comparação com a média global de 43%, ver Figura 1).

Figura 1 – Postura de Transformação Digital

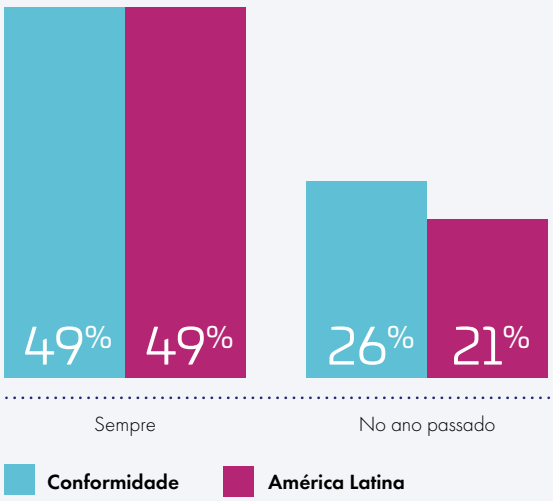


Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

"Apenas 27% dos entrevistados latino-americanos disseram que estão agressivamente causando disrupção nos mercados em que participam ou que estão adquirindo capacidades digitais que permitem uma maior agilidade empresarial".

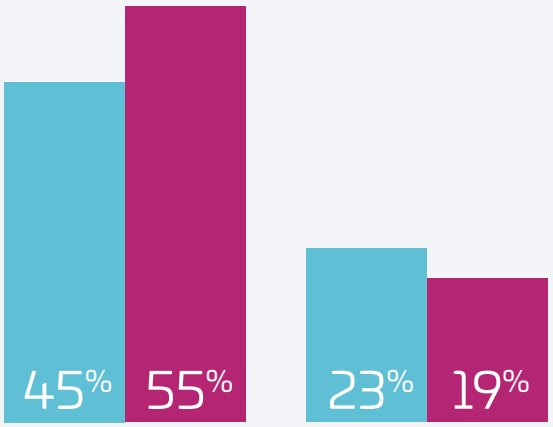
Mas nenhuma empresa está imune a ameaças à segurança de dados, com 49% dos entrevistados latino-americanos declarando que já sofreram vazamento de dados, e 21% dizendo que sofreram alguma violação no ano passado (ver Figuras 2a e 2b). Outros 17% das empresas latino-americanas relataram que não passaram em uma auditoria de conformidade no ano passado. Nosso estudo mostra médias de violações na América Latina semelhantes a da amostra global, embora a conscientização do público possa ser menor, pois poucos países da América Latina têm leis sobre divulgação pública para casos de violações ou falhas de conformidade.

Figura 2a – Taxas de incidentes de violação



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

Figura 2a – Taxas de incidentes de violação por país



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

49%

dos entrevistados latino-americanos tiveram seus dados vazados e 21% desses casos ocorreram no ano passado.

17%

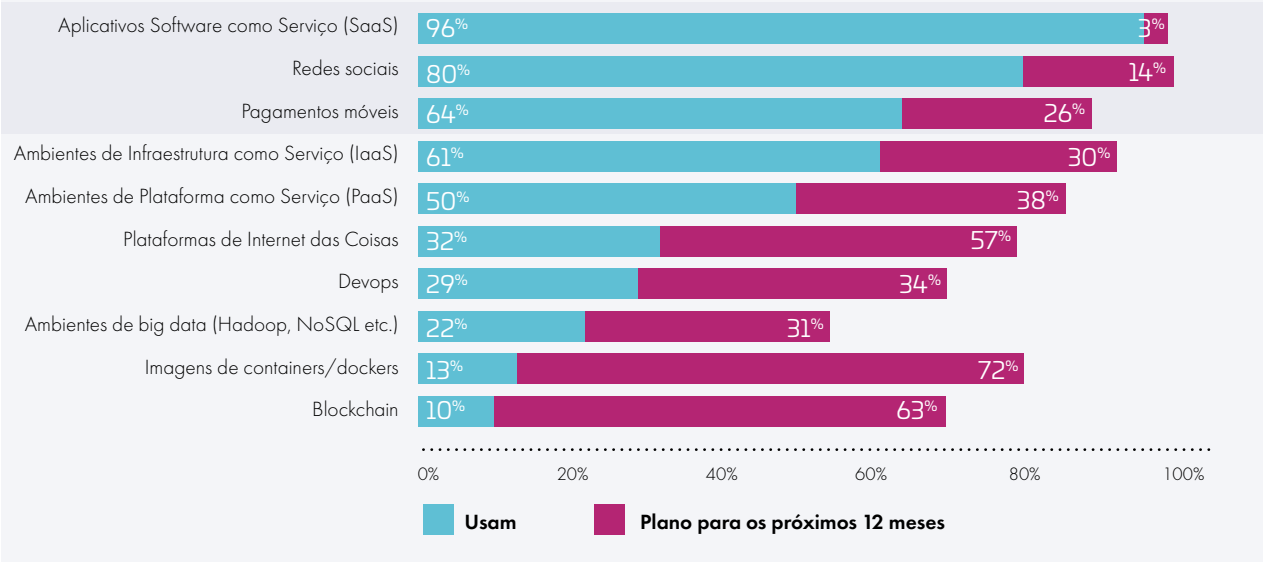
das empresas latino-americanas relataram que não passaram em uma auditoria de conformidade no ano passado.

As empresas que se transformam digitalmente estão percebendo novas vantagens competitivas, mas enfrentam novos desafios de segurança de dados causados pela transformação digital. A transformação digital está ligada à vulnerabilidade: quanto mais transformação digital uma empresa faz, mais provável que tenha sofrido um vazamento de dados. As empresas com foco digital (as que tomam decisões estratégicas, organizacionais, tecnológicas e financeiras que levarão à transformação digital nos próximos anos) podem também estar mais expostas a ameaça de dados. Um maior nível de sofisticação também pode significar que é mais provável que estejam cientes de que tiveram dados vazados. Empresas com nível menor de sofisticação podem ter menos exposição, ou podem simplesmente ignorar que tiveram dados vazados.

As empresas armazenam seus dados confidenciais em uma vasta gama de tecnologias

As empresas latino-americanas estão adotando diversas tecnologias da 3ª Plataforma, que incluem nuvem, tecnologia móvel, redes sociais, big data e IoT. 96% das empresas latino-americanas usam aplicativos SaaS (ver Figura 3). Redes sociais e pagamentos móveis também têm altos níveis de adoção, enquanto os ambientes de nuvem IaaS e PaaS e IoT têm altos níveis de adoção planejada. Observe que muitas destas tecnologias, como IoT e dispositivos móveis, são tecnologias de borda, o que fortalece a mensagem de que a exposição de dados está muito além do limite tradicional da rede.

Figura 3 – Níveis de adoção de tecnologias – Empresas latino-americanas



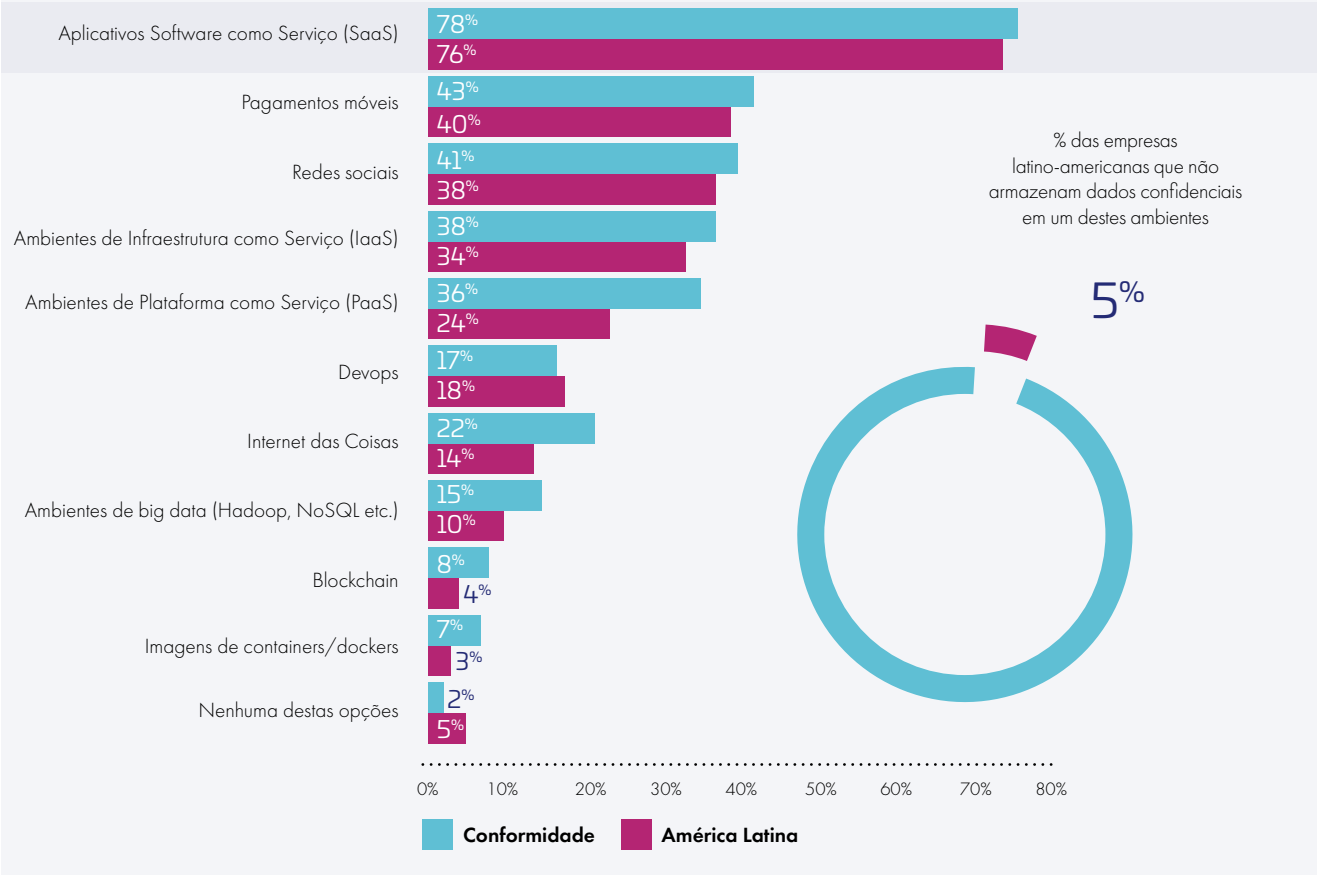
Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

76%

das empresas latino-americanas armazenam dados confidenciais em aplicativos SaaS, 34% em IaaS, e 24% em ambientes PaaS.

Do mesmo modo, muitas empresas latino-americanas estão guardando dados confidenciais ou regulamentados em diversos ambientes. Setenta e seis por cento das empresas armazenam dados confidenciais em aplicativos SaaS, 34% em IaaS, e 24% em ambientes PaaS. Noventa e cinco por cento das empresas latino-americanas entrevistadas armazenam dados em pelo menos um dos ambientes tecnológicos da nossa pesquisa (ver Figura 4).

Figura 4 – Ambientes tecnológicos utilizados para armazenar dados confidenciais/regulamentados



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

À medida que as empresas ampliam o uso de tecnologias de nuvem, móveis, sociais, big data e IoT utilizando provedores terceirizados, os dados confidenciais ficam potencialmente mais vulneráveis. Desta forma, a segurança de perímetro pouco faz para proteger os dados não locais, o que mostra a necessidade de adoção de uma abordagem menos privilegiada de acesso e proteção de dados para segurança. Esta abordagem menos privilegiada de segurança elimina a abordagem binária de confiança/não-confiança da realidade local e perimetral de ontem e requer, em vez disso, uma abordagem de validação e verificação contínua centrada na identidade, fornecendo proteções tanto de rede como de acesso a aplicativos. Do mesmo modo, tecnologias como criptografia e tokenização asseguram que, se as medidas de menos privilégio falharem e os dados forem hackeados, vazados, ou se os dispositivos físicos forem roubados, os dados estejam devidamente protegidos.

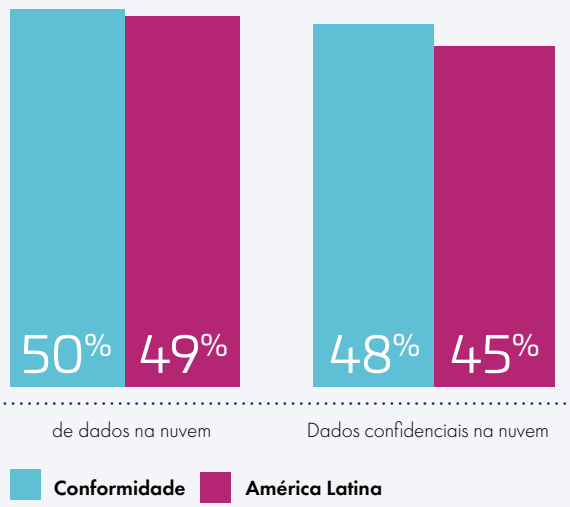
As nuvens representam o principal ambiente de grande risco para os dados

Todas as empresas latino-americanas entrevistadas armazenam dados confidenciais na nuvem. Os dados armazenados na nuvem estão se aproximando de um ponto de inflexão, com os entrevistados do nosso estudo dizendo que estimam que 49% dos dados estão na nuvem, um pouco menos do que a amostra global de 50%. Mais importante ainda, os entrevistados latino-americanos disseram que 45% desses dados em nuvem são confidenciais, e 100% das empresas latino-americanas disseram que armazenam pelo menos alguns dados confidenciais em nuvem (ver Figura 5). Os entrevistados brasileiros disseram que 47% dos seus dados em nuvens são confidenciais, o que coloca o país em quarto lugar em todo o nosso estudo, atrás apenas da Nova Zelândia (56%), dos EUA (54%), e da Coreia do Sul (48%).

100%

dos entrevistados latino-americanos disseram que pelo menos alguns dos seus dados confidenciais em nuvem não estão criptografados.

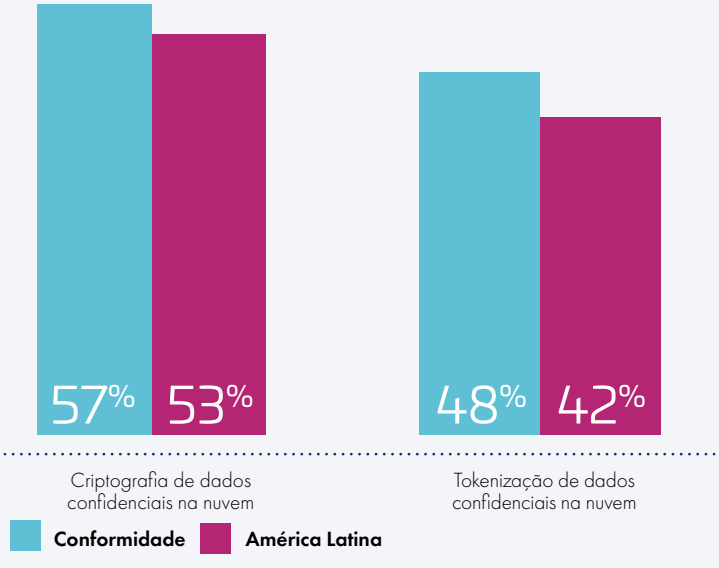
Figura 5 – Dados armazenados em ambientes de nuvem



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

À medida que os dados mais confidenciais são armazenados em ambientes de nuvem, aumentam os riscos de segurança dos dados No entanto, apesar desta significativa exposição de dados confidenciais, as médias de criptografia de dados e tokenização são baixas. Na verdade, 100% dos entrevistados latino-americanos disseram que pelo menos alguns dos seus dados confidenciais em nuvem não estão criptografados. Apenas 53% dos dados confidenciais armazenados em ambientes de nuvem são protegidos por criptografia e menos de metade, 42%, estão protegidos por tokenização (ver Figura 6).

Figura 6 – Segurança de dados confidenciais na nuvem

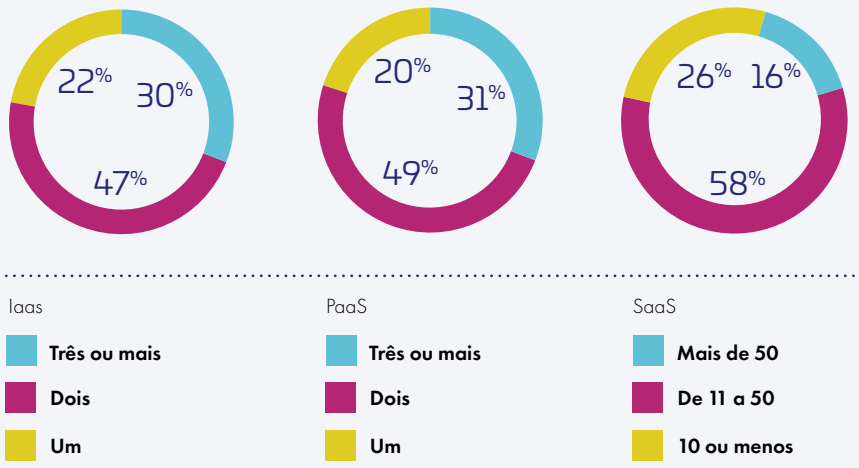


Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

A complexidade dos ambientes corporativos é um dos principais problemas da segurança dos dados, uma vez que a nuvem múltipla se tornou a regra

Quanto mais dados migram para a nuvem, mais complexa fica a segurança. Esta complexidade é frequentemente causada pelo uso de múltiplos ambientes de nuvem e múltiplos sistemas de gestão de chaves de criptografia. Isso é verdade na América Latina; embora a América Latina utilize, em média, menos ambientes de nuvens do que outras regiões pesquisadas, a maioria das empresas latino-americanas usam ambientes em nuvens múltiplas. Trinta por cento das organizações latino-americanas utilizam três ou mais provedores de IaaS, 31% trabalham com mais de três fornecedores de PaaS, e 16% precisam administrar mais de 50 aplicativos SaaS (ver Figura 7). Em comparação, a América do Norte (com 35%) tem mais do dobro de empresas com mais de 50 aplicativos SaaS.

Figura 7 – Número de provedores de IaaS/PaaS em empresas europeias



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

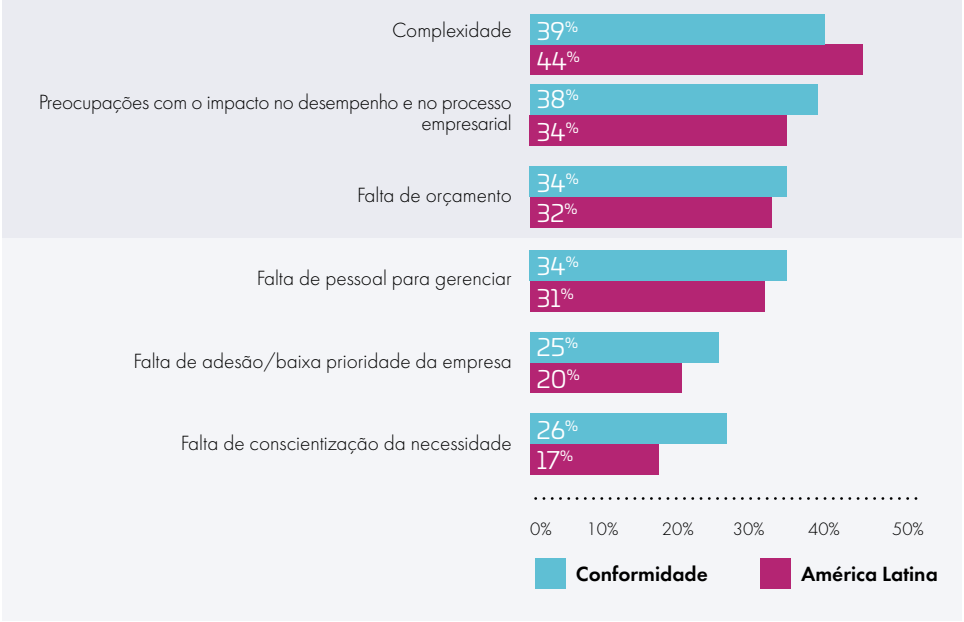
44%

dos entrevistados latino americanos disseram que a complexidade é a principal barreira à implementação da segurança de dados.

"Trinta por cento das organizações latino-americanas utilizam três ou mais provedores de IaaS, 31% trabalham com mais de três fornecedores de PaaS, e 16% precisam administrar mais de 50 aplicativos SaaS".

A complexidade resultante, incluindo a orquestração de soluções de gerenciamento de chaves de cada provedor de nuvem em ambiente de nuvem múltipla, está complicando a vida dos profissionais de segurança. A preocupação com a complexidade é de longe a principal barreira à implementação da segurança de dados (44%), e é um problema especial nesta região, com mais entrevistados latino-americanos preocupados com a complexidade do que em qualquer outra região. Esta conclusão é consistente com o fato da América Latina estar menos avançada na transformação digital do que qualquer outra região. Outras preocupações importantes são o impacto da segurança dos dados no desempenho e processo organizacional (34%) e a falta de orçamento (32%) (ver Figura 8).

Figura 8 – Barreiras à implementação da segurança de dados



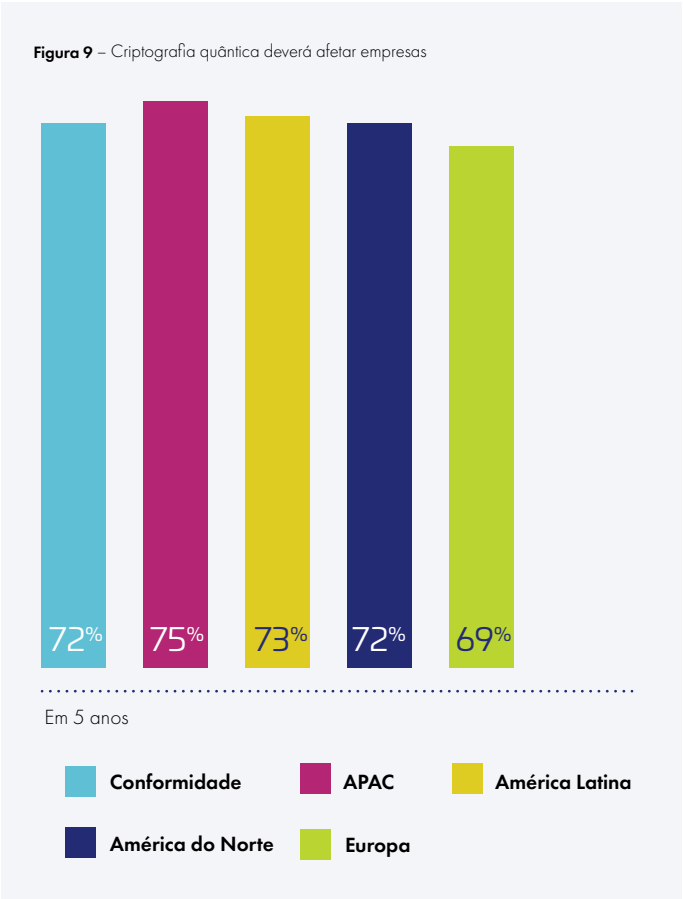
Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

"Há mais entrevistados latino-americanos preocupados com a complexidade do que em qualquer outra região".

As preocupações com a segurança dos dados na computação quântica já são visíveis

A segurança de dados só ficará mais difícil com a chegada da computação quântica. O impacto da computação quântica já é visível, uma vez que 73% das empresas latino-americanas acreditam que ela afetará suas operações criptográficas nos próximos cinco anos (ver Figura 9). Os requisitos de criptografia destacam uma questão crítica de segurança causada pelo poder da computação quântica. Oitenta e nove por cento dos entrevistados estão preocupados que a computação quântica deixe dados confidenciais expostos, com 40% muito/extremamente preocupados.

Figura 9 – Criptografia quântica deverá afetar empresas



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

89%

dos entrevistados latino-americanos estão preocupados que a computação quântica exponha dados confidenciais.

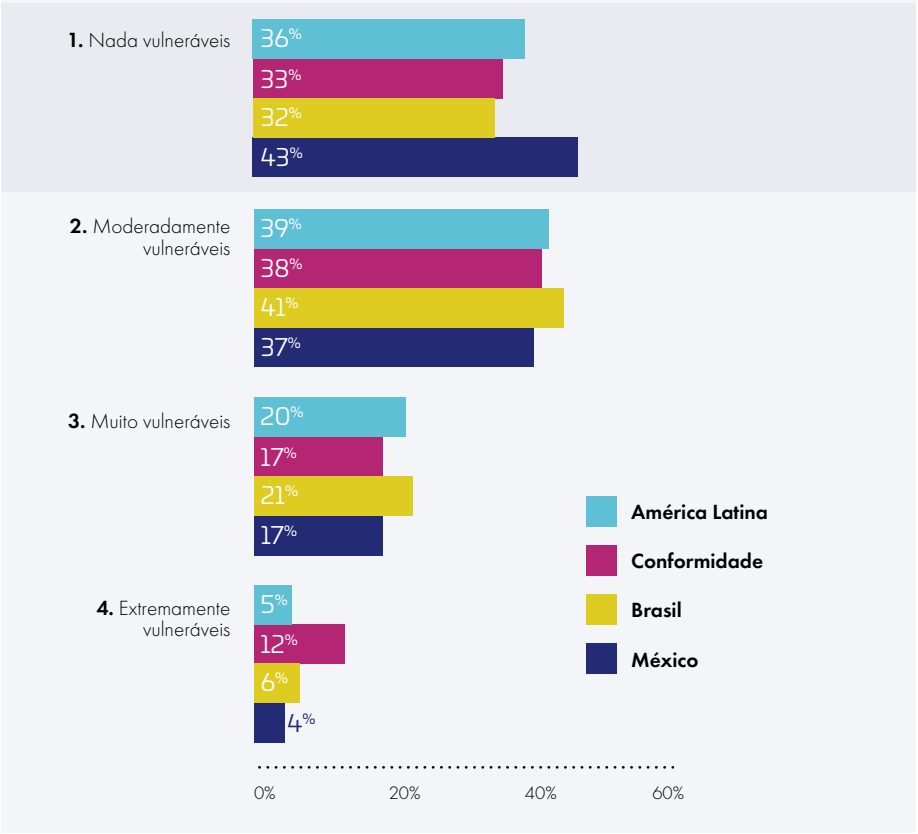
Os principais planos para compensar as ameaças da computação quântica são o gerenciamento de chaves com uso de gerador quântico seguro de números aleatórios (34%), mudança radical da arquitetura de TI e de cibersegurança (33%), e afastamento da criptografia simétrica (32%). Mas muitas empresas latino-americanas não sabem o que devem fazer, embora possam surgir ameaças dentro dos próximos cinco anos. Vinte e um por cento dos entrevistados planejam instalar sistemas críticos completamente offline e 8% não têm quaisquer planos.

"Muitas empresas latino-americanas não sabem o que devem fazer, embora possam surgir ameaças à computação quântica dentro dos próximos cinco anos.

A noção de segurança de dados das empresas em comparação com a realidade

Apesar das ameaças generalizadas e cada vez maiores à segurança dos dados, 36% dos entrevistados latino-americanos afirmaram que "não estão nem um pouco vulneráveis" às ameaças internas, e 22% afirmaram que "não estão nem um pouco vulneráveis" às ameaças externas, acima da média global de 33% e 18% para essas duas perguntas, respectivamente. O México acredita ser menos vulnerável a ameaças internas, com 43% afirmando que "não estão nada vulneráveis", e o Brasil com 32%. (ver Figura 10).

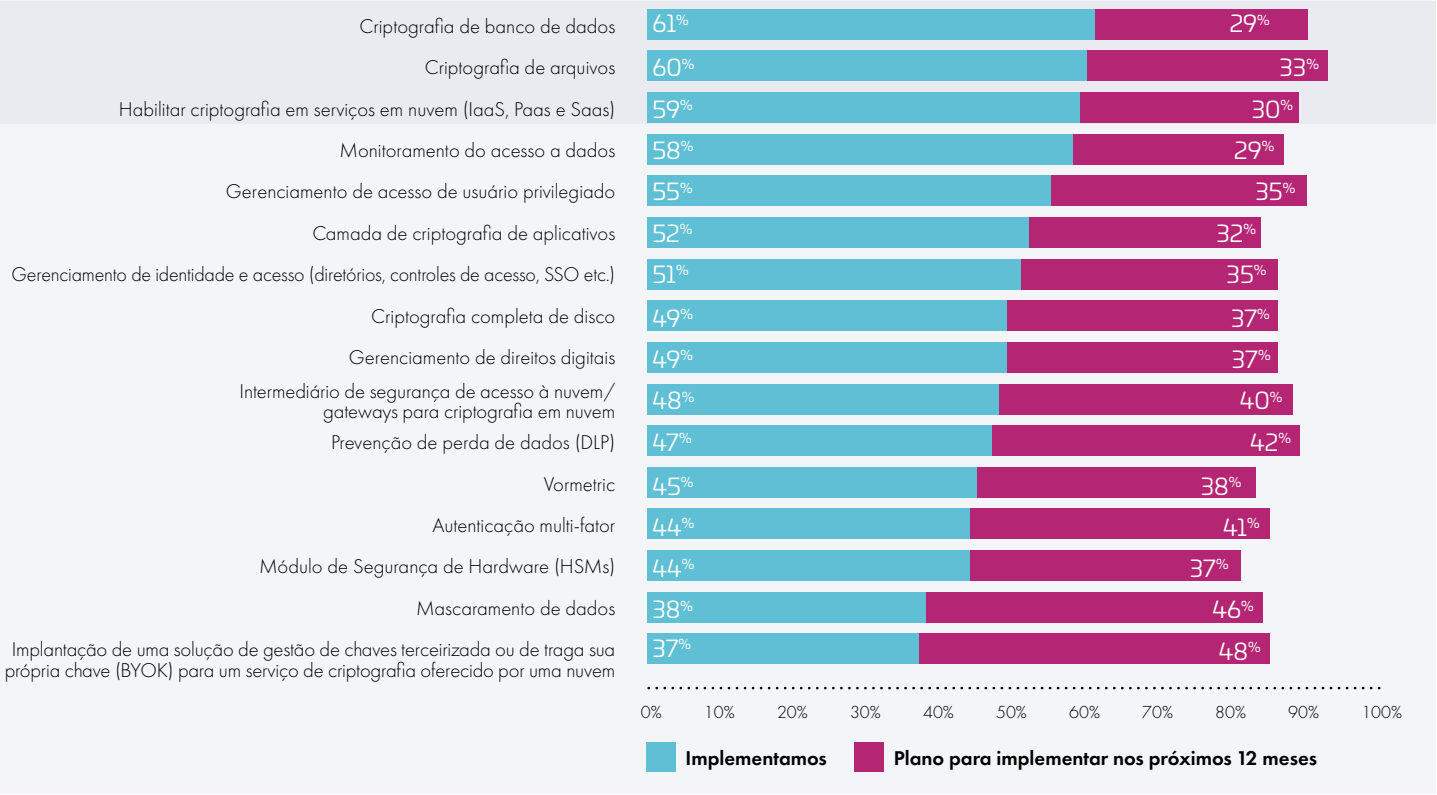
Figura 10 – Vulnerabilidade para ameaças à segurança de dados internos



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

Esta baixa vulnerabilidade percebida aponta para uma desconexão entre percepção e a realidade. Esta confiança não é apoiada por práticas de segurança de dados ou investimentos. As empresas latino-americanas não mudaram significativamente suas posições de segurança utilizando ferramentas que as tornariam realmente menos vulneráveis, mesmo após a série de ataques na área de finanças durante 2018 e ataques que afetaram infraestruturas críticas do México em 2019. Como mencionado anteriormente, as médias de criptografia e tokenização de dados confidenciais em nuvem são baixas. Além disso, apenas 60% dos entrevistados utilizam a criptografia de arquivos (em comparação com 61% da amostra total), enquanto 61% usam a criptografia de bancos de dados (ligeiramente superior à amostra global que é de 59%) (ver Figura 11).

Figura 11 – Implementação de ferramentas de criptografia e segurança de dados em empresas da América Latina



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

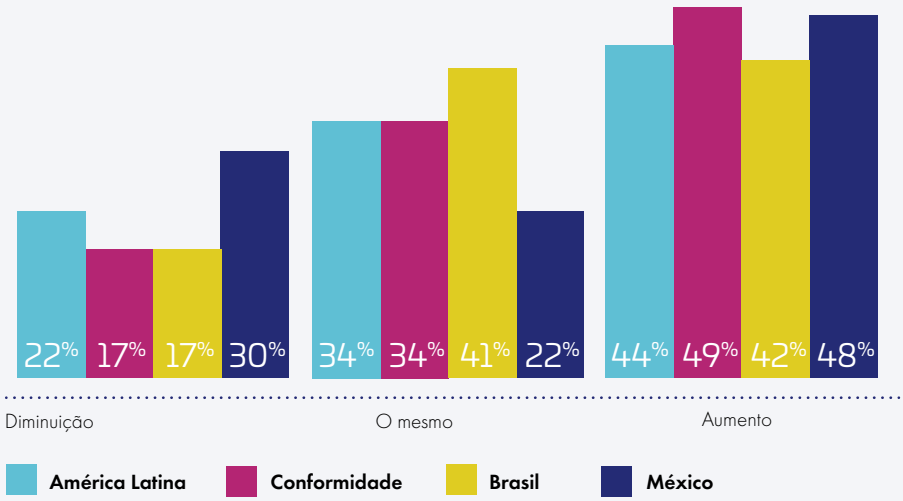
61%

dos entrevistados latino-americanos fazem a criptografia de bancos de dados e 60% utilizam a criptografia de arquivos.

Os gastos com segurança de dados estão aumentando, mas são inferiores à média global

As empresas latino-americanas planejam gastar mais dinheiro em segurança de dados no próximo ano. Quarenta e quatro por cento dos entrevistados latino-americanos disseram que gastariam um pouco ou muito mais em segurança de dados nos próximos 12 meses, o que é inferior à média total (49%). Mas o aumento do orçamento de segurança de dados está diminuindo rapidamente, e mais de uma em cada cinco empresas latino-americanas planeja diminuir os gastos com segurança de dados em 2020 (ver Figura 12). Em termos de países, o México se destaca, com 30% das empresas mexicanas planejando diminuir as despesas com a segurança de dados em 2020, em comparação com apenas 17% no Brasil e 17% do total de empresas.

Figura 12 – Gastos com segurança de dados - América Latina



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

30%

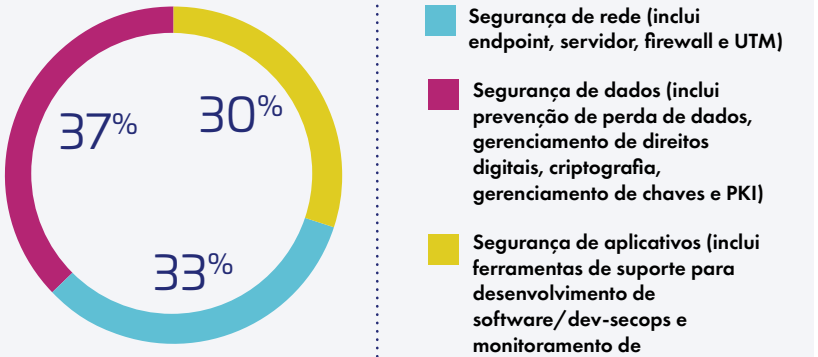
das empresas mexicanas planeja diminuir as despesas com a segurança de dados em 2020, em comparação com apenas 17% no Brasil e 17% do total de empresas.

15%

do orçamento de segurança de TI é gasto com a segurança de dados na América Latina.

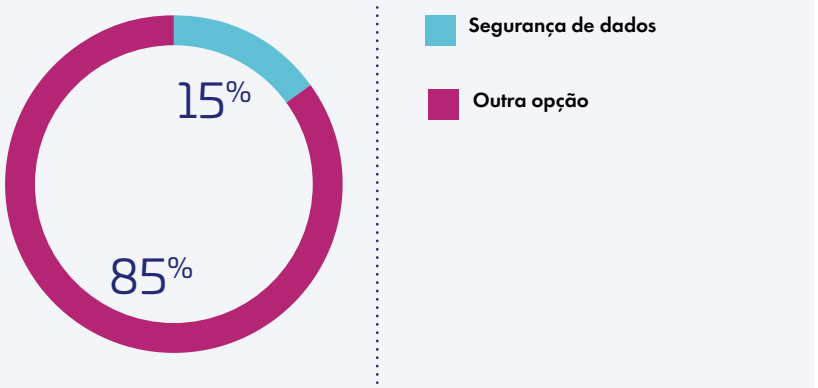
As empresas latino-americanas concentram predominantemente seu interesse na segurança de dados (37%), seguidas da segurança de redes (33%) e da segurança de aplicativos (30%), o que poderia levar a uma mudança na forma como a região está efetivamente investindo. Atualmente, as empresas utilizam 40% - 45% dos seus orçamentos em segurança de redes (fonte: relatório sobre soluções de segurança na América Latina, 2019, IDC). Esta é uma abordagem apropriada, uma vez que as iniciativas de transformação digital mudaram fundamentalmente de natureza e expandiram o perímetro; as empresas precisam pensar além do simples enfoque na proteção de rede. Notavelmente, a América Latina tem o maior foco na segurança de dados do que qualquer outra região da amostra, e superior ao total global (34%), o que indica que a América Latina está à frente da curva quando se trata de deslocar o foco da segurança para estar mais de acordo com as causas atuais de ameaça. Mas os entrevistados latino-americanos não estão necessariamente justificando suas ações, uma vez que os gastos com segurança de dados não estão de acordo com essa taxa de atenção e apenas uma média de 15% dos orçamentos de segurança de TI são gastos em segurança de dados (ver Figuras 13a e 13b).

Figura 13a – Proporção do foco em segurança nas empresas da América Latina



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

Figura 13b – Proporção do orçamento latino-americano de segurança de TI dedicado à segurança de dados



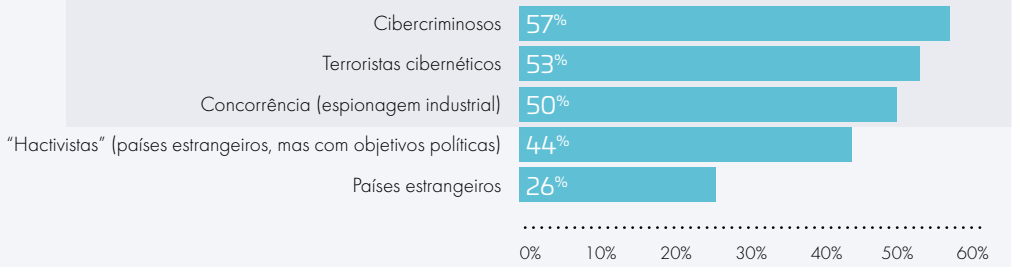
Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

Demonstrando ainda uma desconexão entre os orçamentos de segurança e o foco dos departamentos de segurança, os entrevistados latino-americanos acreditam que agentes mal-intencionados criam riscos aos dados com ameaça intencional de causar danos, o que representaria a maior ameaça à segurança de dados. Cinquenta e sete por cento estão preocupados com cibercriminosos que causam danos ou fazem com que a empresa tenha uma imagem ruim perante o público, seguidos por preocupações com terroristas cibernéticos (53%) e espionagem industrial (50%). Curiosamente, os entrevistados latino-americanos estão menos preocupados com problemas cotidianos que podem na realidade constituir uma maior ameaça e sobre os quais têm mais controle, incluindo o acesso de provedores de serviços (42%), contas de gestão executiva (40%) e parceiros com acesso interno (39%) (ver Figuras 14 e 15). As empresas devem ter cuidado com o excesso tanto de quantidade como amplitude de contas, uma vez que o risco de ameaça aos dados internos é muitas vezes maior devido ao descuido do que ao comportamento mal-intencionado.

57%

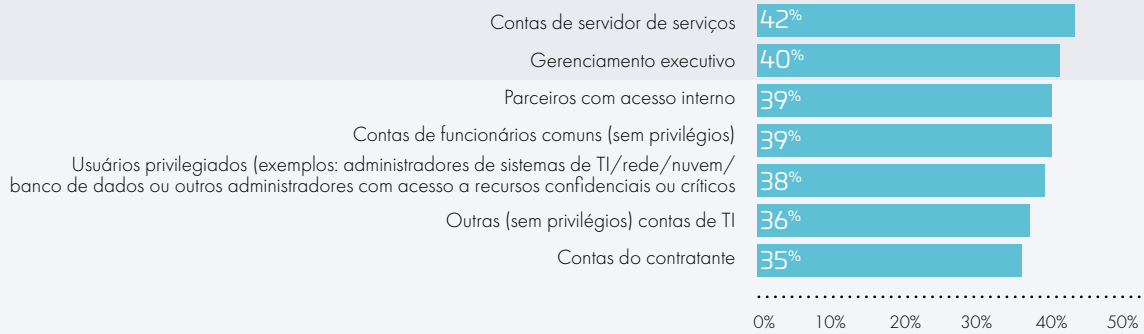
dos entrevistados latino-americanos estão preocupados com cibercriminosos que prejudicam ou fazem com que a empresa tenha uma imagem ruim perante o público.

Figura 14 – Violações de dados por fraudadores



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

Figura 15 – Ameaças internas a dados



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

02

A segurança dos dados em nuvem está em um momento crítico

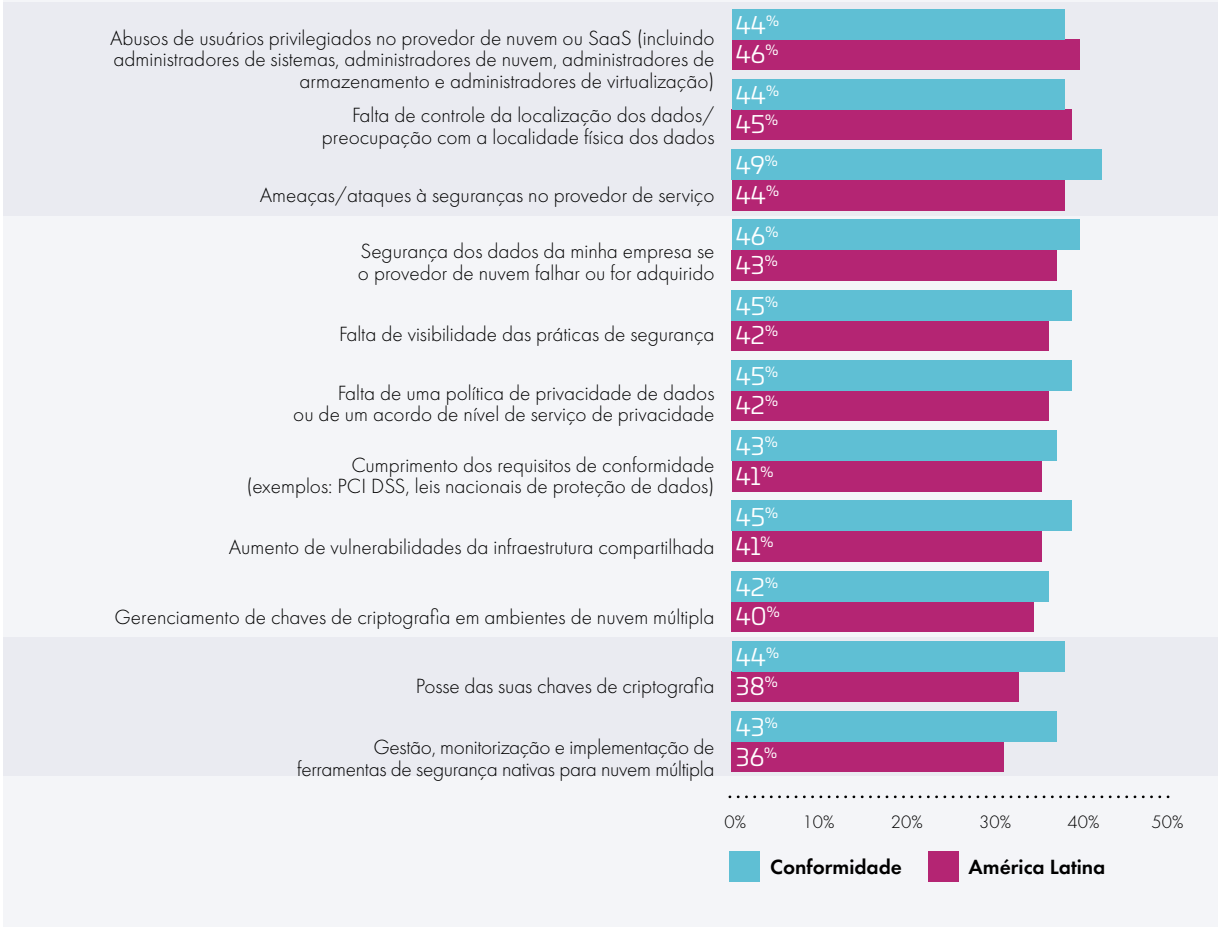
Quase metade (49%) dos dados empresariais latino-americanos são armazenados em nuvem atualmente, sendo que muitos deles são confidenciais. À medida que o número de dados em nuvem se aproxima de um marco, os departamentos de segurança de TI devem agora, mais do que nunca, adotar e ter sua parte do modelo de responsabilidade compartilhada em nuvem. As empresas devem implementar as melhores práticas de segurança de dados, uma vez que o provedor de nuvem na maioria das vezes não garante a segurança dos dados. No entanto, 41% das empresas da América Latina veem sua estratégia de nuvem como tendo um impacto em seus planos para melhorar sua postura de cibersegurança. Por outro lado, 27% das organizações na região consideram a adoção da nuvem como sua principal iniciativa ou objetivo final para alcançar uma postura de segurança mais forte (fonte: Relatório de Segurança Cibernética da América Latina 2019, IDC).

Os entrevistados latino-americanos estão preocupados com muitos problemas da segurança de dados armazenados em nuvem. No entanto, as empresas estão mais preocupadas com problemas com seus provedores de nuvem, como o acesso dos provedores a dados, a falta de controle sobre onde residem os dados, e as violações que acontecem no provedor. Embora sejam preocupações válidas, a possibilidade real destes itens resultarem em problemas de segurança é bastante baixa. Estas mesmas empresas estão menos preocupadas com questões sobre as quais têm controle direto, e que representam maiores vulnerabilidades em potencial, como o gerenciamento de chaves de criptografia (ver Figura 16). Curiosamente, esta falta de atenção a questões sobre as quais há controle é ainda maior na América Latina do que na amostra global.

41%

das empresas da América Latina veem sua estratégia de nuvem como tendo um impacto em seus planos para melhorar sua postura de cibersegurança.

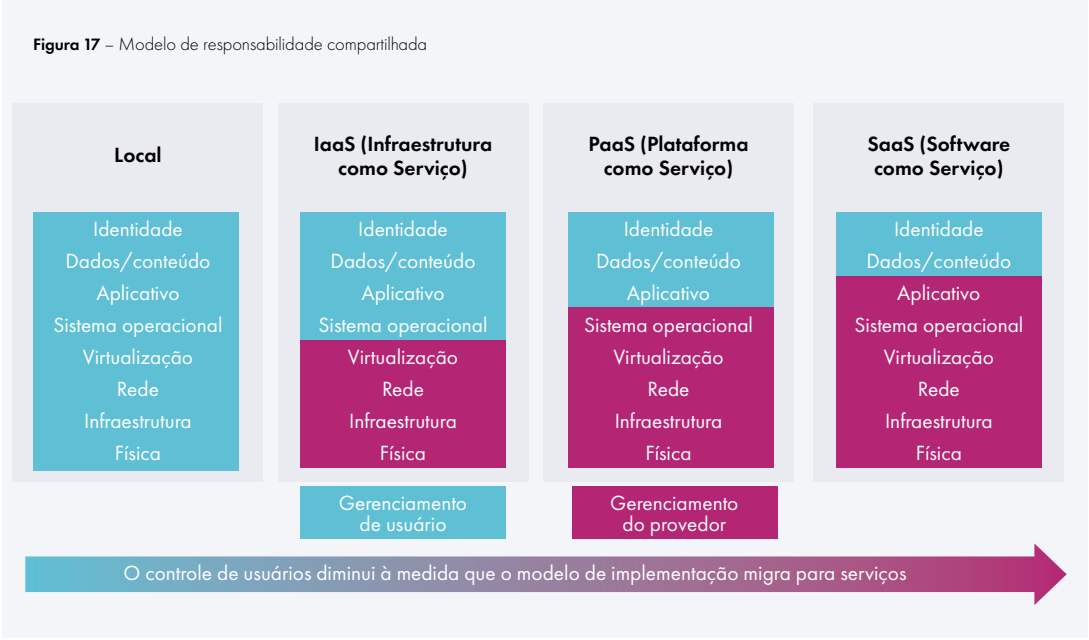
Figura 16 – Preocupações com a segurança



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

Esta diferença entre as ameaças que os entrevistados percebem e aquelas em que deveriam realmente se concentrar implica que os pesquisados não consideraram muito a segurança dos dados em mundo em que a nuvem está em primeiro lugar. Cada tipo de ambiente de nuvem requer uma mudança na responsabilidade pela segurança de identidades, dados, aplicativos, sistemas operacionais, virtualização de servidores, rede, infraestrutura e hardware. As empresas latino-americanas devem colocar seu foco da segurança em nuvem na parte do modelo de responsabilidade compartilhada em que a empresa pode influenciar a segurança dos seus dados (ver Figura 17).

Figura 17 – Modelo de responsabilidade compartilhada



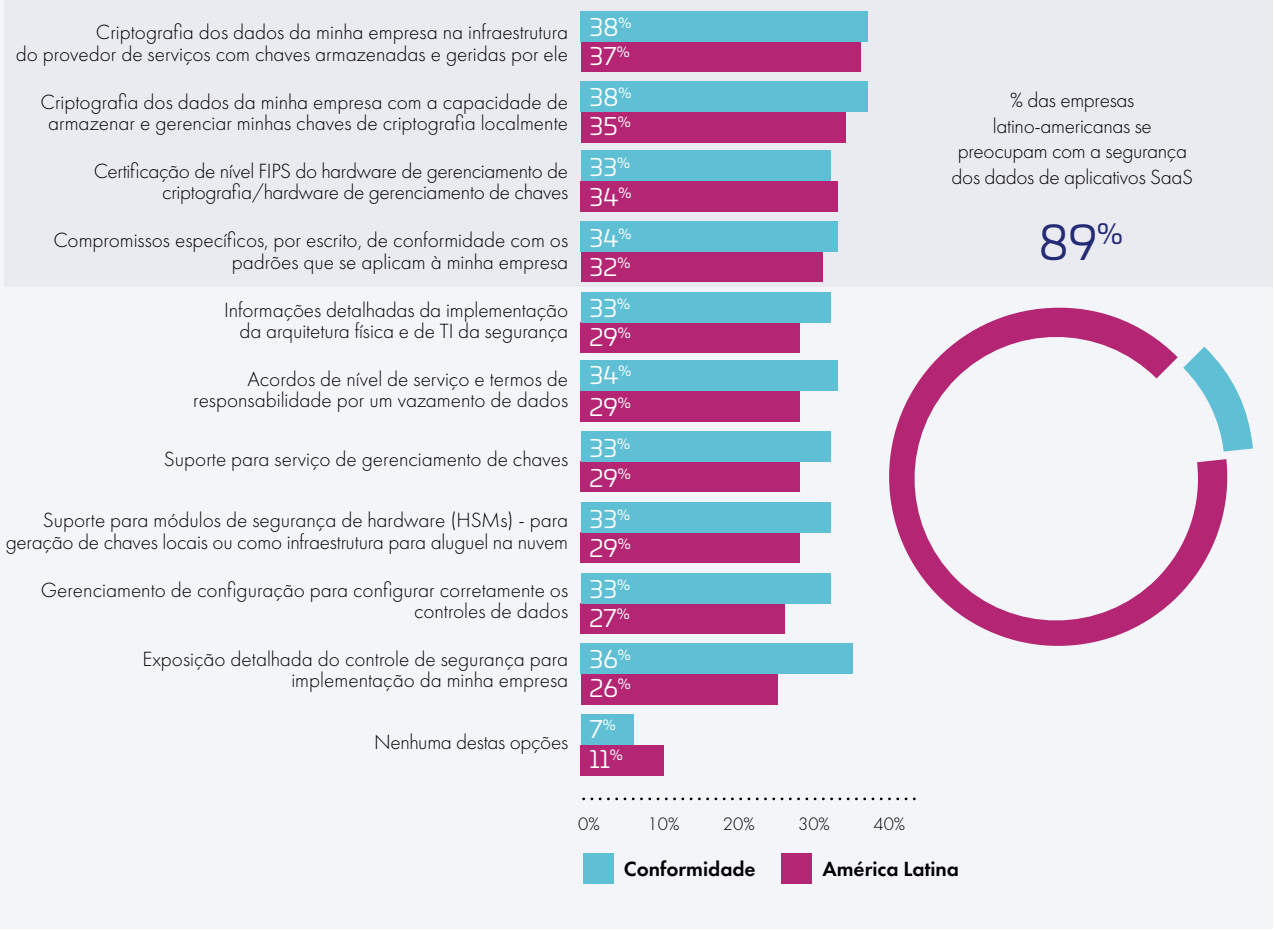
Fonte: IDC, novembro de 2019

"As empresas latino-americanas devem colocar seu foco da segurança em nuvem na parte do modelo de responsabilidade compartilhada em que a empresa pode influenciar a segurança dos seus dados".

As preocupações com a segurança da nuvem também aumentam à medida que as empresas implantam mais dados em ambientes SaaS, IaaS, e PaaS.

De acordo com nosso estudo, 89% dos entrevistados latino-americanos têm pelo menos alguma preocupação com a segurança dos dados de aplicativos SaaS. As preocupações com a segurança em ambientes SaaS abrangem diversos riscos, com a criptografia de dados, armazenamento de chaves locais, e certificação de nível FIPS liderando a lista (ver Figura 18).

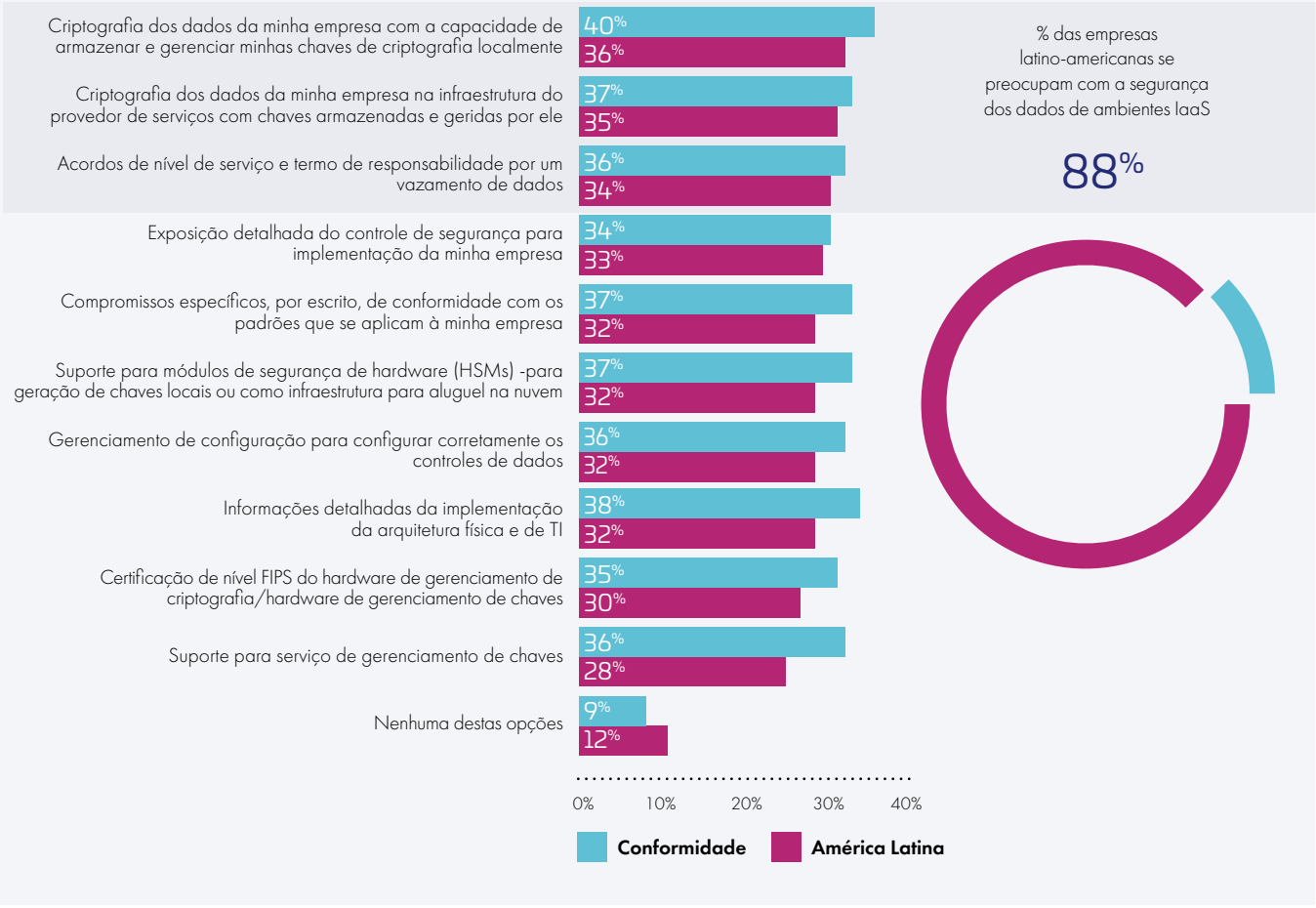
Figura 18 – Preocupações com a segurança de SaaS



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

Oitenta e oito por cento dos entrevistados da América Latina têm pelo menos alguma preocupação com a segurança dos dados em ambientes IaaS. À semelhança do SaaS, as preocupações de segurança com ambientes IaaS abrangem também diversas questões de armazenamento de chaves locais, criptografia de dados, e acordos de nível de serviço como principais preocupações (ver Figura 19).

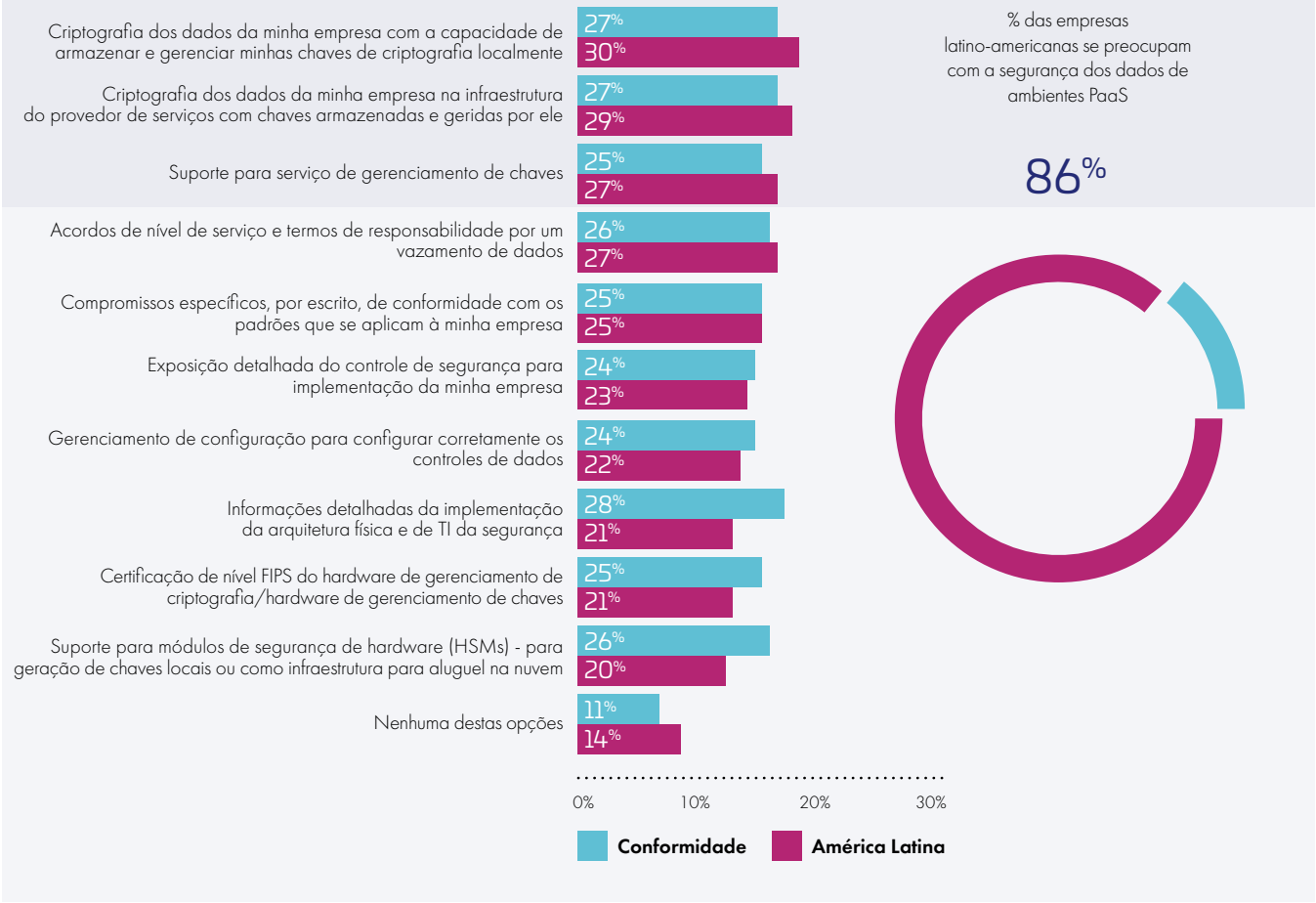
Figura 19 – Preocupações com a segurança de IaaS



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

Oitenta e seis por cento dos entrevistados latino-americanos também têm pelo menos alguma preocupação com a segurança dos dados em ambientes PaaS, com armazenamento local de chaves, criptografia de dados, gerenciamento de chaves como serviço, e acordos de nível de serviço liderando a lista (ver Figura 20). Esta preocupação aumentará à medida que as empresas mudam seu foco em IaaS para implantações PaaS para ajudar o desenvolvimento de aplicativos e iniciativas de modernização de aplicativos para a transformação digital.

Figura 20 – Preocupações com a segurança de PaaS



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

Um componente crítico da transformação digital é a ponta. A transformação digital cria oportunidades para novas tecnologias que envolvem empresas e consumidores onde estes se encontram, mas introduz novas complexidades à medida que as empresas levam uma quantidade crescente de dados e poder de computação para a ponta. Um aumento das tecnologias de ponta exige que a segurança se afaste da segurança tradicional das empresas e mesmo da nuvem. As tecnologias móvel e IoT são exemplos específicos disso, mas big data, containers e devops são também tecnologias que ajudam a expandir e a personalizar a computação de ponta.

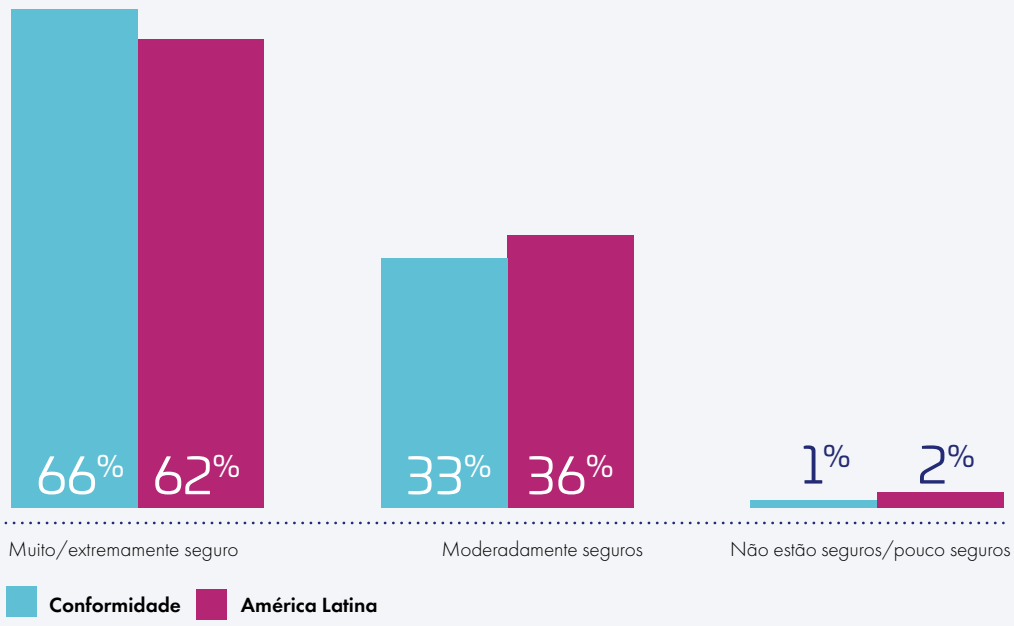
Com a expansão do uso das tecnologias de transformação digital, a busca de dados sensíveis e o gerenciamento de chaves assumem um papel ainda mais crítico na segurança de dados. No entanto, a busca de dados e o gerenciamento de chaves não são vistas como preocupações grandes pelas empresas latino-americanas, criando potenciais lacunas nas práticas de segurança de dados.

Noventa e oito por cento das empresas latino-americanas deste estudo sentem-se pelo menos um pouco seguras à medida que levam mais dados para novos desenvolvimentos tecnológicos, embora em menor medida do que a amostra global (99%). Sessenta e dois por cento dos entrevistados latino-americanos sentem-se muito ou extremamente seguros, em comparação com 66% da amostra global (ver Figura 21).

98%

das empresas latino-americanas se consideram pelo menos moderadamente seguras, mesmo colocando mais dados em novas implantações tecnológicas.

Figura 21 – Nível de segurança de instalações de novas tecnologias



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

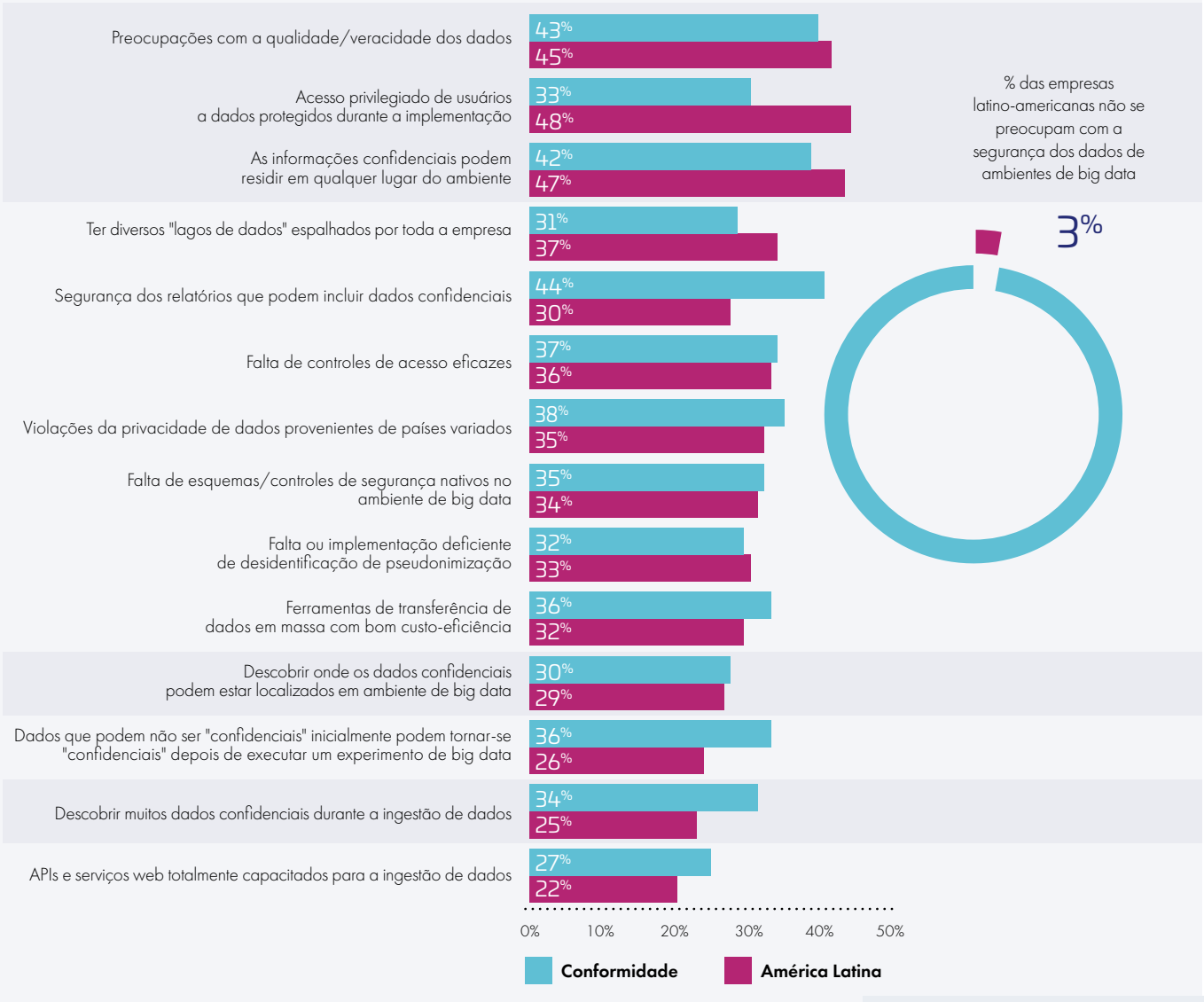
03

Preocupações com a segurança e métodos de proteção de dados

Preocupações com a segurança de big data

Noventa e sete por cento dos entrevistados latino-americanos estão preocupados com a segurança dos dados em seus ambientes de big data. As principais grandes preocupações em matéria de segurança de dados são a qualidade dos dados, o acesso privilegiado dos usuários, e os dados residentes em qualquer parte do ambiente. No entanto, as preocupações com a busca de dados são muito baixas, incluindo a busca de dados confidenciais em ambiente de big data (29%) e durante a ingestão de dados (25%) (ver Figura 22). Os principais métodos para amenizar as grandes preocupações com a segurança de dados incluem a criptografia de dados, certificações de conformidade e uma autenticação mais forte.

Figura 22 –Preocupações com big data



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

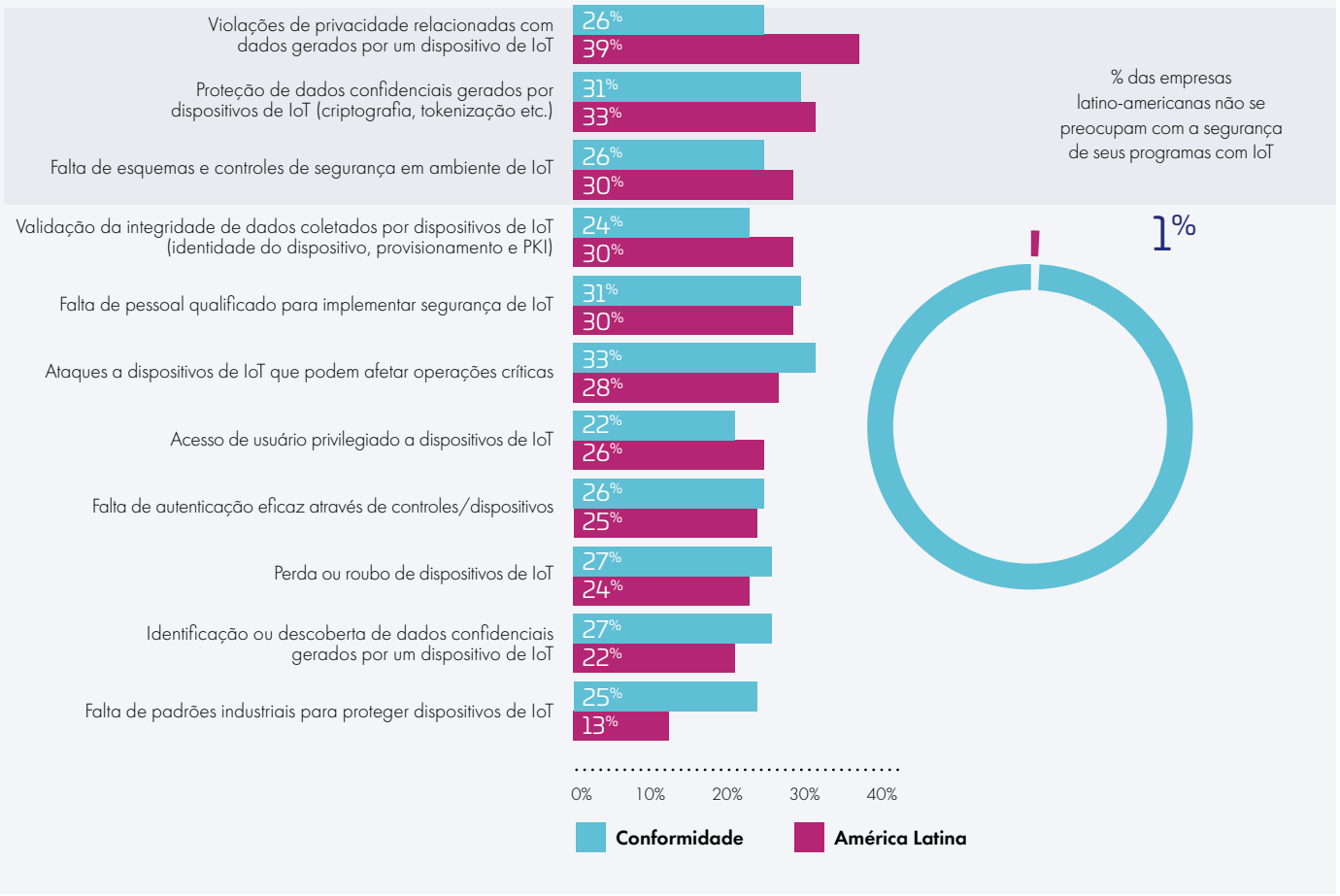
97%

dos entrevistados latino-americanos estão preocupados com a segurança dos dados em seus ambientes de big data.

Preocupações com a segurança da Internet das Coisas (IoT)

Todas as empresas latino-americanas pesquisadas estão preocupadas com a segurança de dados em ambientes de IoT. As preocupações de segurança em ambientes de IoT incluem a privacidade dos dados, criptografia/tokenização e falta de estruturas de segurança (ver Figura 23). A criptografia/tokenização de dados, autenticação de identidade digital, e anti-malware são utilizadas para resolver as principais preocupações com a segurança de ambientes de IoT. À medida que os dispositivos IoT são instalados, o gerenciamento de chaves se torna cada vez mais importante para implementar eficazmente a segurança de identidade e a criptografia de dados nestes dispositivos IoT. No entanto, as empresas latino-americanas concentram-se principalmente na segurança de redes e na aplicação de políticas para abordar o problema de segurança de projetos de IoT.

Figura 23 – Preocupações com a segurança da Internet das Coisas



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

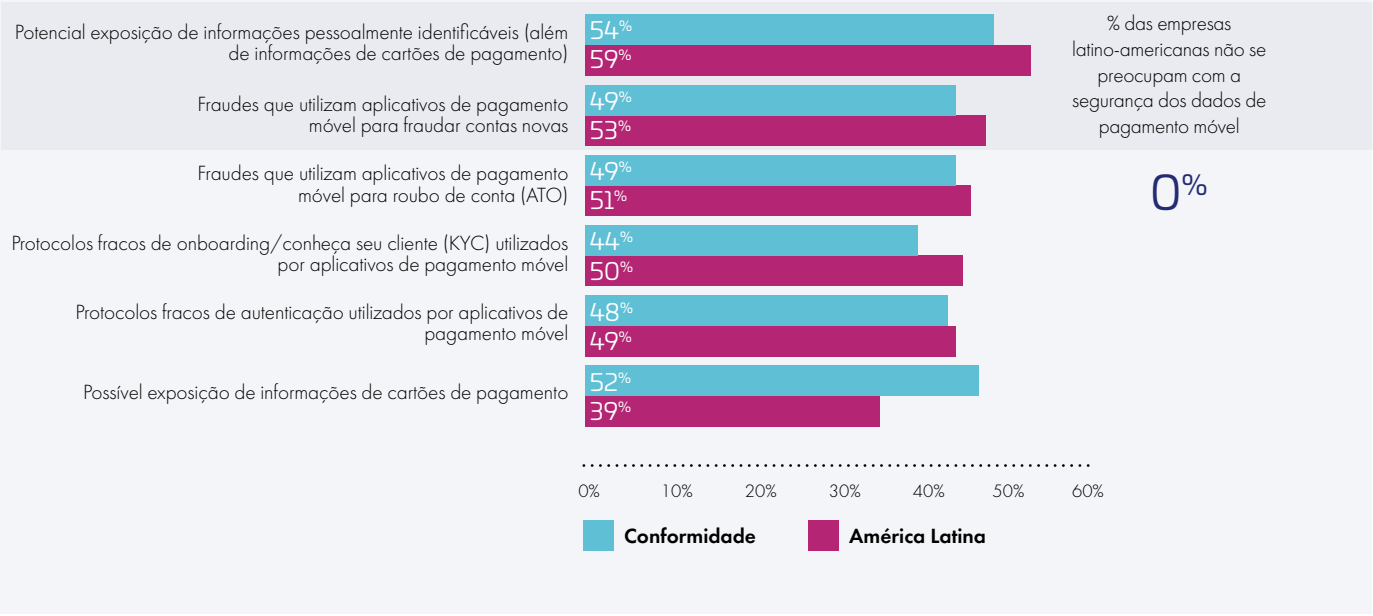
99%

das empresas latino-americanas se preocupam com a segurança dos dados de seus programas com IoT.

Preocupações com a segurança dos pagamentos móveis

Cem por cento dos entrevistados latino-americanos têm pelo menos alguma preocupação com a segurança dos dados de pagamentos móveis. Os entrevistados se preocupam muito com a segurança dos pagamentos móveis, como deveriam. A exposição de informações de identificação pessoal e criminosos que utilizam aplicativos de pagamento móvel para novas fraudes e aquisições de contas são as principais preocupações (ver Figura 24). Muitas soluções são levadas em conta para resolver o problema de segurança dos pagamentos móveis. Entre as principais estão protocolos criptografados de rede sem fio, telas de bloqueio e criptografia de dados.

Figura 24 – Preocupações com a segurança dos pagamentos móveis



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

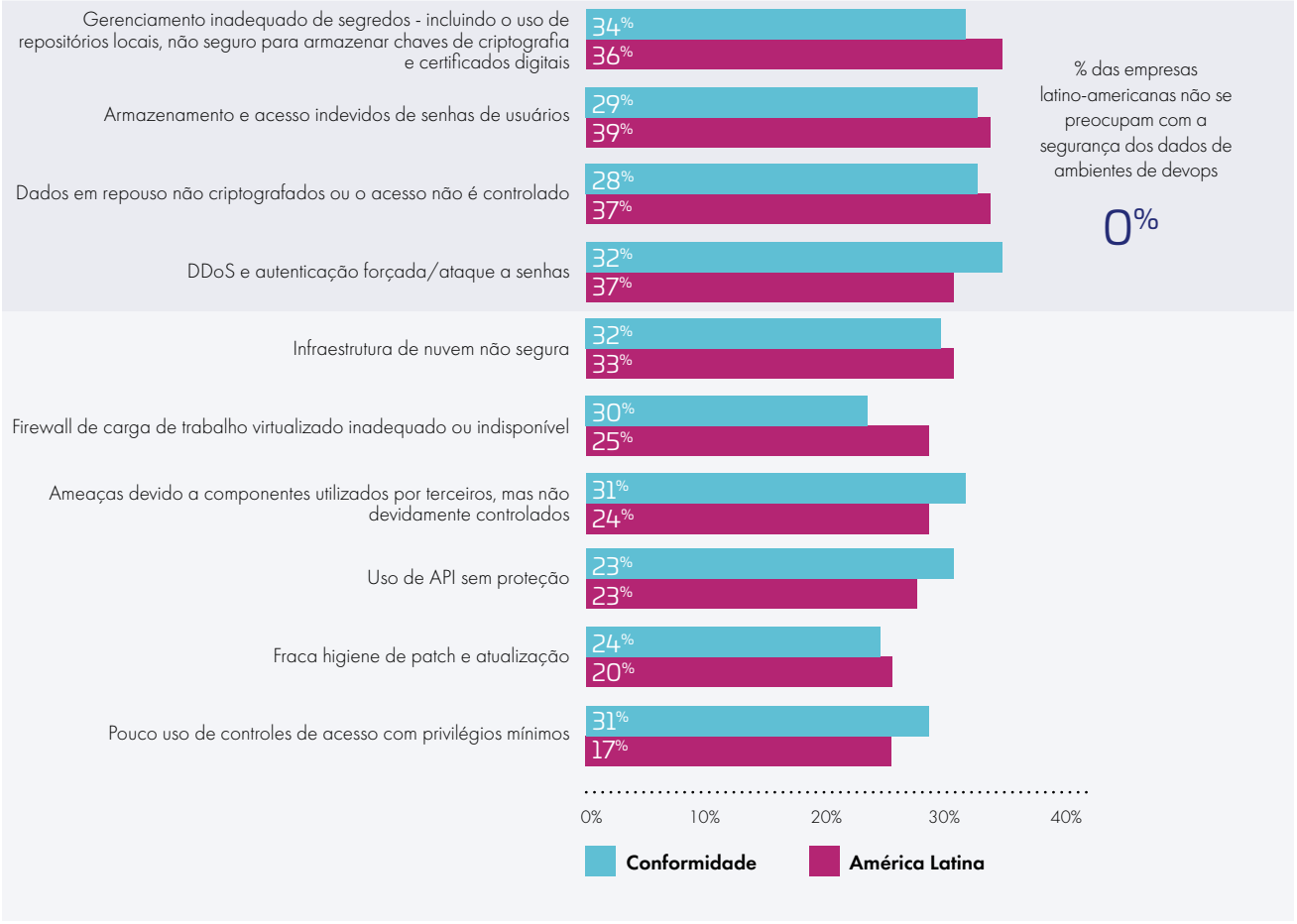
100%

dos entrevistados latino-americanos têm pelo menos alguma preocupação com a segurança dos dados de pagamentos móveis.

Preocupações com a segurança de devops

Quando se trata de ambientes devops, 100% dos entrevistados latino-americanos estão preocupados com a segurança dos dados desses ambientes. As maiores preocupações dos entrevistados são: gestão de segredos, armazenamento de senhas e criptografia de dados em repouso (ver Figura 25). Muitas abordagens diferentes estão sendo levadas em conta para diminuir as preocupações de segurança de ambientes devops, sendo as principais: criptografia/tokenização de dados em repouso, comunicação segura usando HTTPS e gestão de acesso.

Figura 25 – Preocupações com devops



Fonte: relatório sobre ameaça a dados da Thales de 2020 e da IDC de novembro de 2019

100%

dos entrevistados latino-americanos estão preocupados com a segurança dos dados em ambientes de devops.

04

Orientação/ dicas importantes da IDC

As empresas latino-americanas enfrentam cada vez mais desafios, e desafios mais complexos, à segurança de dados na implementação das suas estratégias de nuvem e transformação digital, especialmente durante a realidade da COVID-19 e da preparação para os possíveis cenários pós-pandêmicos. A seguir estão orientações e principais dicas da IDC e para ajudar estas empresas a melhorar sua postura de segurança de dados e para desenvolver políticas de segurança:

- **As soluções de segurança de dados, especialmente a criptografia, são fundamentais para as empresas permanecerem atentas à realidade dos riscos aos dados na era pós-COVID-19.** Este ponto é especialmente relevante, uma vez que a situação atual de trabalho em casa forçou funcionários a acessar e modificar maiores quantidades de dados corporativos fora do local de trabalho, por vezes em dispositivos BYO. Mesmo que uma empresa perca visibilidade sobre o local de residência dos dados, são necessárias tecnologias de segurança de dados como a criptografia para proteger os dados corporativos de uma maneira independente da localização.

- **Estamos seguros de que os funcionários regressarão ao local de trabalho?** As empresas precisam de novos métodos de segurança de dados para proteger o cenário de TI na era pós-COVID-19 à medida que os dados migram para fora da empresa e para a nuvem e regressam ao local de trabalho, uma vez que não se sabe se os funcionários optarão por regressar ao escritório. Os governos da América Latina têm diferentes capacidades econômicas para impedir a propagação da pandemia, e as infraestruturas sanitárias também representam um desafio. Assim, poderíamos esperar um tempo maior para o regresso aos escritórios e, enquanto isso, as empresas têm que cuidar de suas preocupações de segurança relacionadas ao trabalho remoto. A migração para o trabalho em casa pode ser permanente para muitos. A proteção de dados na era pós-COVID-19 começa com a criptografia, passa para a criptografia inteligente com controles de acesso integrados, e acaba se tornando uma gestão integrada de direitos e prevenção abrangente da perda de dados com base na adoção de uma abordagem de acesso menos privilegiado a dados e realizada por plataformas de identidade ricas em características, uma vez que em muitos casos de uso o perímetro da era pós-COVID-19 reside nos próprios dados.

- **Investir em ferramentas de segurança de dados modernas, híbridas e de nuvem múltipla que fazem o modelo de responsabilidade compartilhada funcionar à medida que as empresas latino-americanas procuram recuperar o atraso nas iniciativas de transformação digital.** A América Latina está atrasada em relação a outras regiões em termos de transformação digital e terá de dar um salto em relação a outros países à medida que a usam para transformar seus negócios no futuro, especialmente porque procuram se adaptar às mudanças ocasionadas pela pandemia de COVID-19 na economia atual. As empresas devem focar em soluções que possam simplificar o panorama da segurança de dados e reduzir a complexidade em ambientes de nuvem múltipla e outros já existentes, bem como em tecnologias de transformação digital modernas para nuvem. Em um modelo de responsabilidade compartilhada, as empresas não precisam confiar demasiadamente em provedores de serviços para medidas de segurança de dados. As empresas devem também considerar ter todos os elementos da segurança de dados diretamente em seu controle, como identidade, criptografia (tanto em trânsito como em repouso), gerenciamento de chaves, tokenização e prevenção de perda de dados.

- **Levar em consideração um modelo de confiança zero para proteger dados.** As empresas devem continuar a se concentrar na segurança da rede, uma vez que visam controlar o acesso no perímetro. A segurança dos dados deve ir além da borda tradicional, seja em nuvem, ambientes virtuais, data centers, ou outras tecnologias de transformação digital. Estes ambientes de dados exigem um modelo de confiança zero mais persistente que não torne a segurança dos dados como problema de outra parte.

- **Aumentar o foco em soluções de busca de dados e centralização do gerenciamento de chaves para fortalecer a segurança dos dados.** As preocupações com a segurança dos dados devem evoluir à medida que o limite se expande com uma maior adoção de ambientes de big data, dispositivos IoT, pagamentos móveis, containers, e ambientes devops. Uma maior ênfase na busca de dados confidenciais nestes ambientes, bem como nos ambientes já existentes, fortalecer a segurança dos dados sabendo onde se encontram os dados confidenciais e como acessá-los. Além disso, a criptografia de dados confidenciais é fundamental, e as empresas devem centralizar o gerenciamento de chaves para ajudar a simplificar a criptografia em ambiente complexos.

- **O impacto da computação quântica na criptografia já é visível.** A segurança dos dados não se tornará mais fácil, uma vez que o poder da computação quântica pode expor dados confidenciais rapidamente. As empresas devem começar a planejar suas infraestruturas e ajustes do gerenciamento de chaves para tratar de mudanças fundamentais na criptografia causadas pela computação quântica.

- **Foco nos verdadeiros fatores de ameaças.** Sim, os fraudadores estão aprimorando seus métodos diariamente Os profissionais de segurança precisam evoluir continuamente para poder combater as ameaças. Mas concentre-se nos fatores de ameaça sob controle direto. Tenha cuidado com o fornecimento excessivo de quantidade e amplitude de contas, tanto interna como externamente, para provedores de serviços.

Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 ou +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: CPL_Sales_AMS_TG@thalesgroup.com

> cpl.thalesgroup.com <

cpl.thalesgroup.com/latam-data-threat-report

#2020DataThreat

Escritórios: Argentina, Brasil, Colômbia e México