

A importância e o impacto crescentes da privacidade

CISCO 2023 DATA PRIVACY BENCHMARK STUDY



Tabela de Conteúdos

Introdução	03
Principais conclusões	03
Metodologia	03
Resultados	
1: A economia e a importância da privacidade continuam fortes	04
2: Integração da privacidade em funções organizacionais e responsabilidades	09
3: Desconexão entre organizações e consumidores sobre dados e confiança	14
4: Apesar do desejo de localização de dados, fornecedores globais são vistos como mais seguros do que os fornecedores locais	18
Conclusão e recomendações	20
Satisfazendo o padrão de confiança de nossos clientes	20
Anexo	21
Sobre a série de relatórios de ciber-segurança	22

Introdução

A privacidade continua a aumentar em importância para organizações em todo o mundo e para aquelas que elas servem. A privacidade de dados continua sendo uma missão crítica e um investimento atraente para as organizações, como refletido em sua integração aos profissionais e processos empresariais, valor econômico e visibilidade para a alta administração e o Conselho de Administração. No entanto, as prioridades das organizações com relação ao uso de dados pessoais não estão totalmente alinhadas com as dos consumidores, especialmente quando se trata de usar Inteligência Artificial (IA) e automação para tomar decisões que afetam o indivíduo. Este relatório, nossa sexta revisão anual dos principais desafios de privacidade para as organizações, examina o impacto da privacidade em organizações em todo o mundo.

Metodologia

Os dados deste estudo são derivados da pesquisa Cisco Security Outcomes, na qual os respondentes eram anônimos para os pesquisadores e não informavam quem estava conduzindo o estudo. Usando a mesma metodologia dos anos anteriores, mais de 4.700 profissionais de segurança de 26 geografias¹ completou a pesquisa no verão de 2022. Os resultados da pesquisa representam as principais indústrias e uma mistura de tamanhos de empresas. (Ver [Anexo](#)) Dirigimos perguntas específicas sobre privacidade aos mais de 3100 respondentes que indicaram estar familiarizados com o programa de privacidade de dados em suas organizações. Neste relatório, também incluímos resultados relevantes da Cisco 2022 Consumer Privacy Survey², que foi concluída no verão de 2022 por 2600 adultos em 12 geografias.

¹ Austrália, Brasil, Canadá, Chile, China, Colômbia, França, Alemanha, Hong Kong, Índia, Indonésia, Itália, Japão, Malásia, México, Filipinas, Arábia Saudita, Singapura, Coreia do Sul, Espanha, Taiwan, Tailândia, Holanda, Reino Unido, EUA e Vietnã.

² Cisco 2022 Consumer Privacy Survey: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-survey-2022.pdf

Principais conclusões:

1. A privacidade continua a ser um investimento atrativo para organizações em todo o mundo, mesmo em um clima econômico difícil, proporcionando maiores benefícios médios em todos os setores, e um forte retorno sobre o investimento de 1,8 vezes.
2. Quase todas as organizações integraram a privacidade em suas prioridades e processos, com 98% dos entrevistados relatando métricas relacionadas à privacidade a seu Conselho de Diretores e 95% dos funcionários precisam saber como proteger a privacidade dos dados.
3. As organizações não estão totalmente sincronizadas com os consumidores quando se trata de criar confiança - especialmente no uso de seus dados pessoais para AI e tomada de decisão automatizada.

1: A economia e a importância da privacidade continuam fortes

A privacidade continuou sendo um fator crítico para as organizações em todo o mundo em 2022, com a grande maioria dos entrevistados confirmando o valor e a importância da privacidade. Noventa e cinco por cento (95%) dos entrevistados disseram que a privacidade é um imperativo comercial, acima dos 90% do ano passado. Noventa e quatro por cento (94%) disseram que seus clientes não comprariam deles se seus dados não estivessem devidamente protegidos, acima dos 90% de um ano atrás. E 95% disseram que a privacidade é uma parte integrante da cultura de suas organizações, acima dos 92%. Ver Figura 1.

Figura 1: Importância da privacidade para as organizações



Fonte: Cisco 2023 Data Privacy Benchmark Study

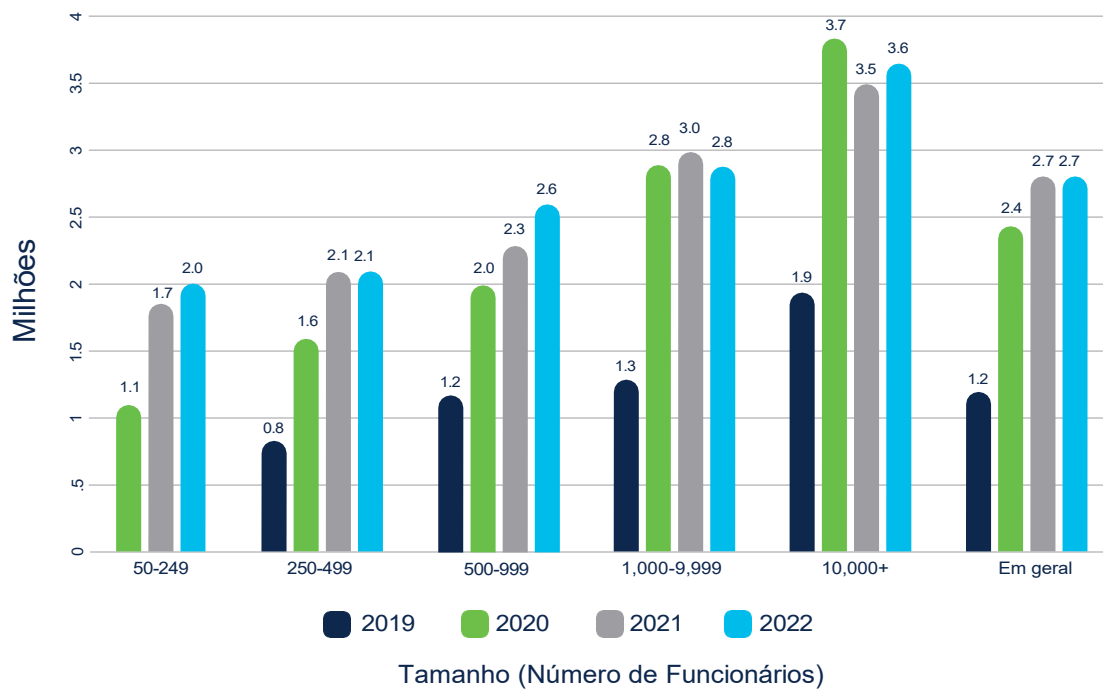


"A abordagem de uma organização em relação à privacidade afeta mais do que a conformidade. O investimento em privacidade impulsiona o valor dos negócios através de vendas, segurança, operações e, o mais importante, confiança".

Dev Stahlkopf, Vice Presidente Executivo

Apesar de um ambiente econômico difícil em 2022, os gastos com privacidade não diminuíram, e em alguns casos, cresceram em 2022. O gasto médio foi de 2,7 milhões de dólares, um aumento significativo em relação aos 1,2 milhões de dólares de apenas 3 anos atrás. O crescimento mais significativo de 2021 a 2022 ocorreu em organizações menores: os gastos em organizações com 50-249 funcionários aumentaram mais de 17% para US\$ 2,0 milhões a partir de US\$ 1,7 milhões. Em organizações com 500-999 funcionários, os gastos aumentaram mais de 13%, de US\$ 2,3 milhões para US\$ 2,6 milhões. Os gastos em organizações maiores permaneceram relativamente inalterados após aumentos acentuados de 2019 a 2020. Ver Figura 2.

Figura 2: Gastos com privacidade, 2019-2022

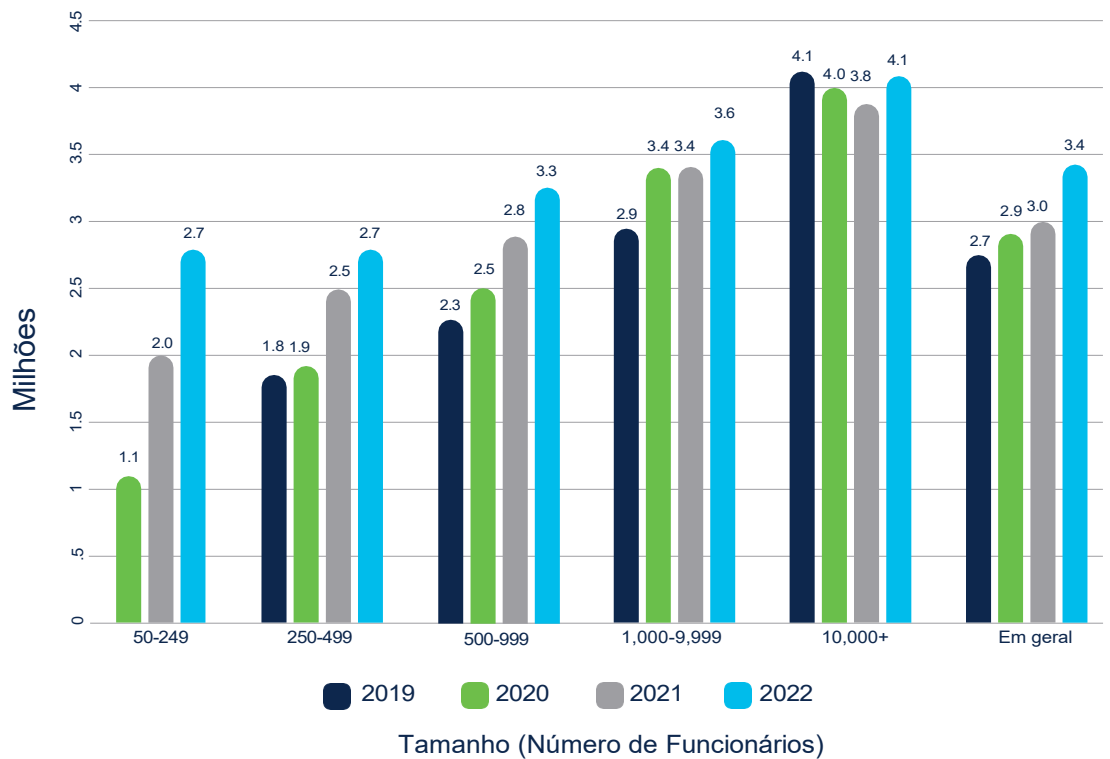


Nota: categoria 50-249 iniciada em 2020

Fonte: Cisco 2023 Data Privacy Benchmark Study

Ao mesmo tempo, o valor estimado em dólares dos benefícios da privacidade aumentou significativamente este ano. A estimativa média subiu mais de 13%, de US\$ 3,4 milhões no ano passado para US\$ 3,0 milhões, com ganhos significativos nos vários tamanhos de organizações. Os benefícios em organizações com 50-249 funcionários subiram 35% de US\$ 2,0 milhões para US\$ 2,7 milhões, e aqueles com 500-999 funcionários subiram 18% para US\$ 3,3 milhões de US\$ 2,8 milhões. Os benefícios estimados em organizações maiores de 1000-9999 funcionários e 10.000+ funcionários também aumentaram 6% e 8%, respectivamente, como mostrado na Figura 3.

Figura 3: Benefícios estimados de privacidade, 2019-2022

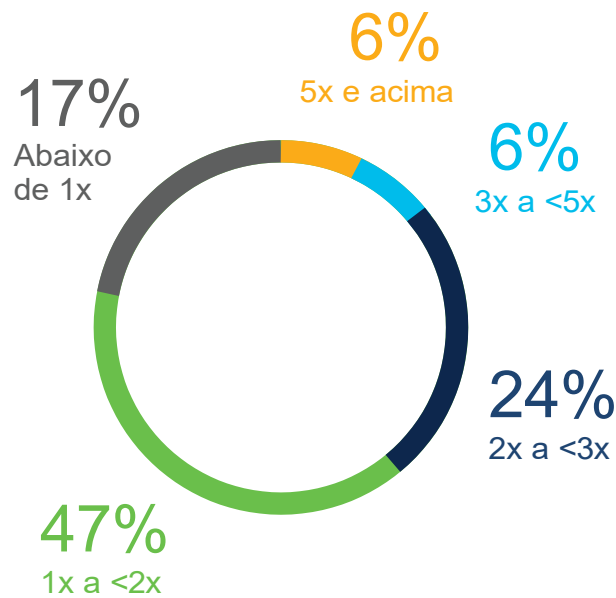


Nota: categoria 50-249 iniciada em 2020

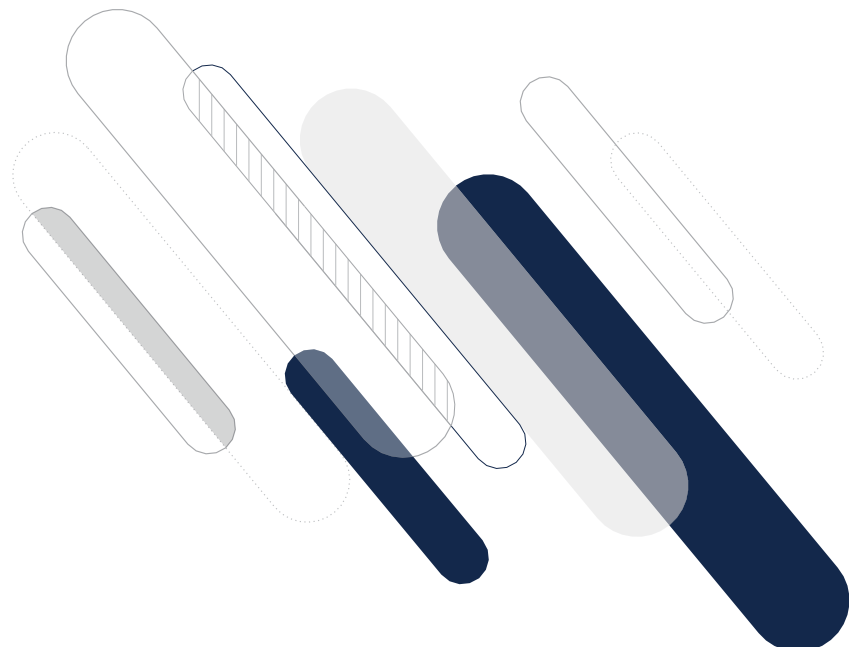
Fonte: Cisco 2023 Data Privacy Benchmark Study

Colocando os gastos e o valor em dólares estimado dos benefícios juntos, a privacidade continua sendo um investimento financeiro muito atraente para a maioria das organizações. A organização média está recebendo benefícios estimados em 1,8 vezes os gastos, como foi na pesquisa do ano passado. Trinta e seis por cento (36%) das organizações, acima dos 32% do ano passado, estão obtendo retornos de pelo menos o dobro de seus gastos, com muitas realizando retornos de 3 a 5 vezes o seu investimento. Ver Figura 4.

Figura 4: Gama de ROI para os respondentes



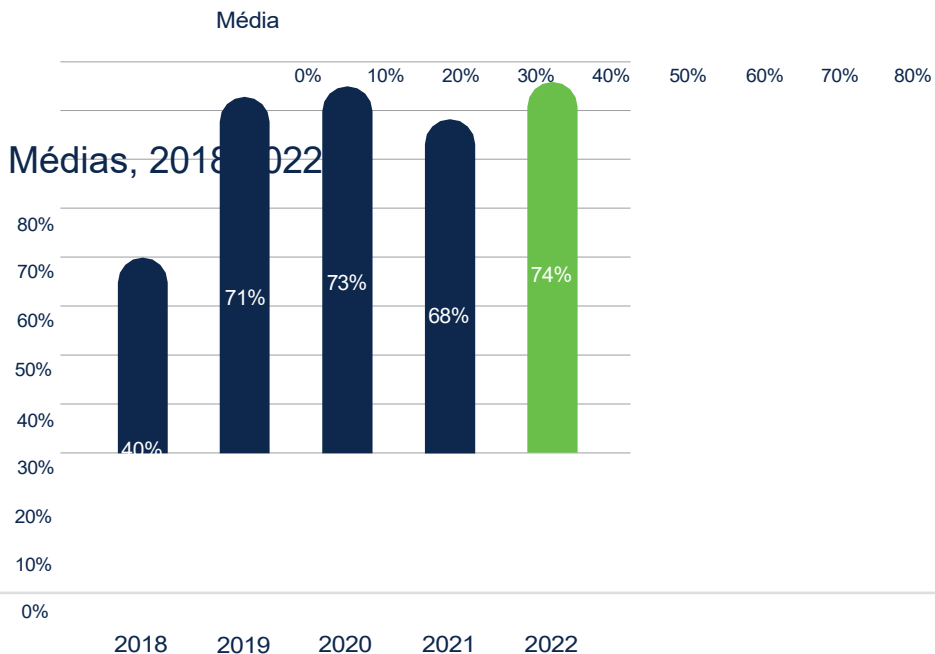
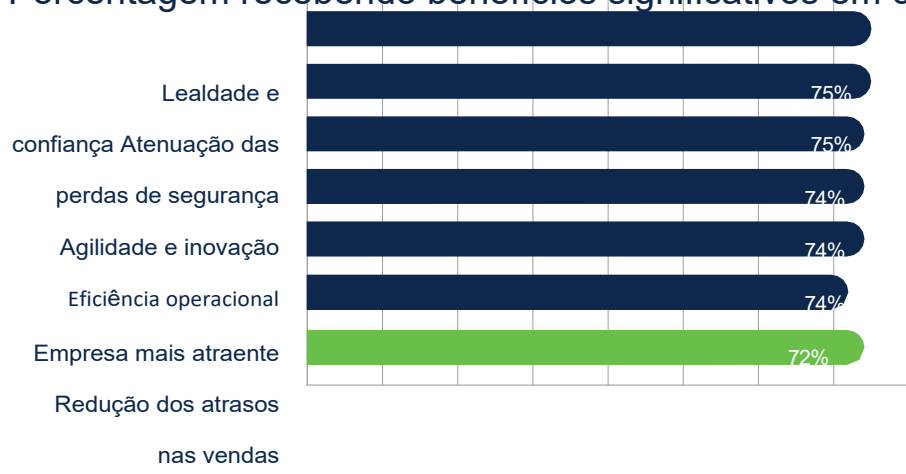
Fonte: Cisco 2023 Data Privacy Benchmark Study



Continuamos a perguntar aos entrevistados sobre áreas específicas de benefícios potenciais da privacidade, incluindo a redução de atrasos nas vendas, a mitigação de perdas por violação de dados, permitindo a inovação, alcançando eficiência operacional, construindo confiança com os clientes e tornando sua empresa mais atraente. Entre os entrevistados deste ano, mais de 70% indicaram que estavam obtendo benefícios "significativos" ou "muito significativos" de cada uma dessas áreas. A média entre as seis áreas foi de 74%, representando um aumento significativo em relação à média de 40% de resposta em nossa primeira pesquisa de 2018 e 6% acima do ano passado. Ver Figura 5.

Figura 5: Organizações que reconhecem os benefícios comerciais do investimento em privacidade

Porcentagem recebendo benefícios significativos em cada área, 2022

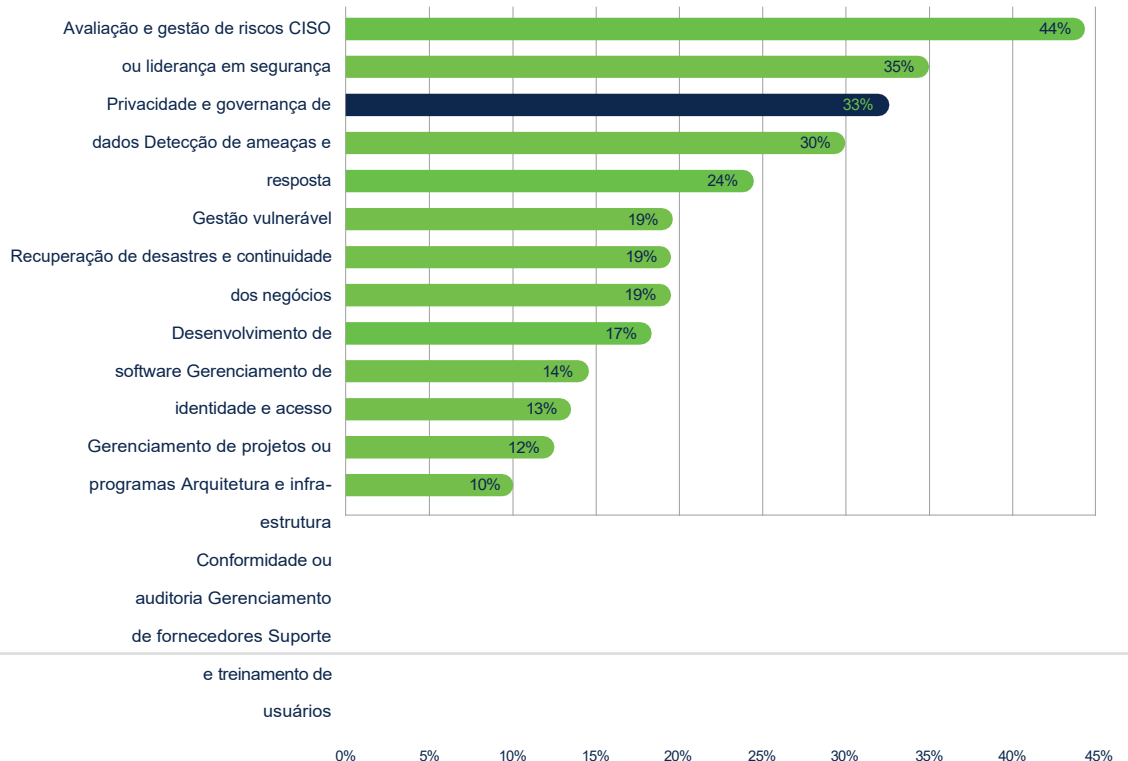


2: Integração da privacidade nas funções e responsabilidades organizacionais

Com a privacidade como uma prioridade comercial crítica, mais organizações estão reconhecendo que todos em toda a organização desempenham um papel vital na proteção de dados pessoais. Na pesquisa deste ano, 95% dos entrevistados disseram que "todos os seus funcionários" precisam saber como proteger a privacidade dos dados.

Além disso, as habilidades de privacidade são particularmente críticas entre aqueles que são diretamente responsáveis por manter os dados seguros. Os profissionais de segurança que completaram nossa pesquisa foram solicitados a definir suas três principais áreas de responsabilidade: Um terço (33%) desses entrevistados selecionou "Privacidade e Governança de Dados", ficando apenas atrás de "Avaliação e Gerenciamento de Riscos" (44%) e "CISO ou Liderança em Segurança" (35%). Ver Figura 6.

Figura 6: Principais responsabilidades de trabalho entre os profissionais de segurança



Fonte: Cisco 2023 Data Privacy Benchmark Study

Estes dados mostram que as organizações reconhecem a necessidade de habilidades de privacidade entre todos os funcionários e com competências específicas para as equipes de segurança para garantir que aqueles que estão autorizados a acessar e trabalhar com os dados os tratarão de forma apropriada. Curiosamente, esta porcentagem foi bastante consistente em todo o mundo com médias regionais nas Américas, APJC, e EMEA de 32-33%. Nenhum país foi inferior a 23% e somente a China foi superior a 50%, como mostrado na Figura 7.

Figura 7: Porcentagem de entrevistados identificando a privacidade como responsabilidade profissional, por geografia

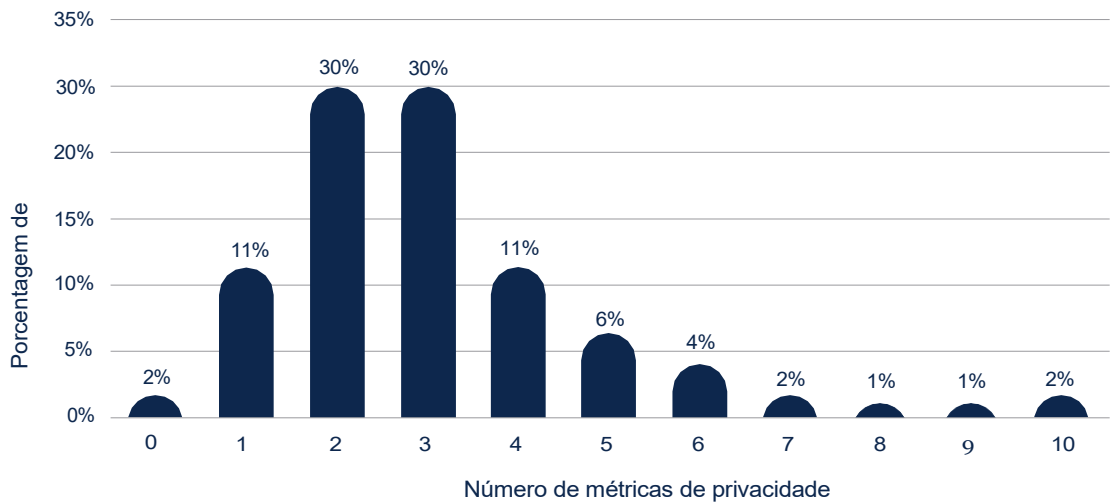


Fonte: Cisco 2023 Data Privacy Benchmark Study



Outra indicação importante da importância da privacidade para a organização é o uso de métricas de privacidade, especialmente quando elas são reportadas à gerência executiva e ao Conselho de Administração. Entre as organizações da pesquisa deste ano, 98% estão reportando uma ou mais métricas relacionadas à privacidade à Diretoria, acima dos 94% da pesquisa do ano passado. Veja a Figura 8 abaixo.

Figura 8: Número de métricas de privacidade reportadas à Diretoria



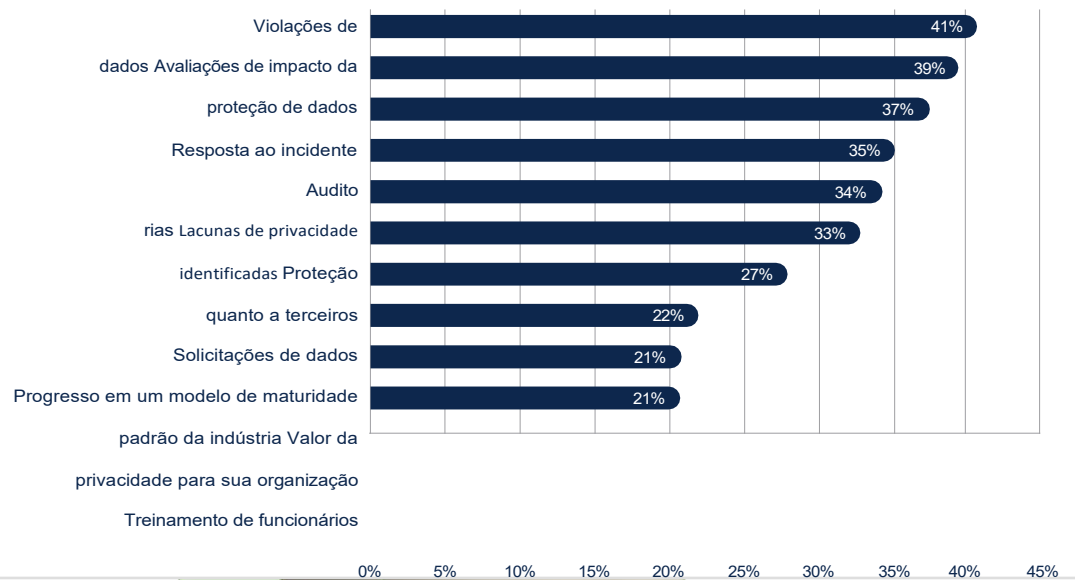
Fonte: Cisco 2023 Data Privacy Benchmark Study

"Quando se trata de ganhar e construir confiança, o cumprimento não é suficiente".

Harvey Jang, Vice Presidente e Diretor de Privacidade, Cisco

Enquanto alguns relatam até 10 métricas de privacidade, o número médio foi de 3,1, o que representa um aumento de 19% em relação aos 2,6 da pesquisa do ano passado. As métricas mais relatadas incluem a situação de quaisquer violações de dados (41%), avaliações de impacto de proteção de dados (39%) e resposta a incidentes (37%), conforme descrito na Figura 9.

Figura 9: Métricas de privacidade reportadas à Diretoria

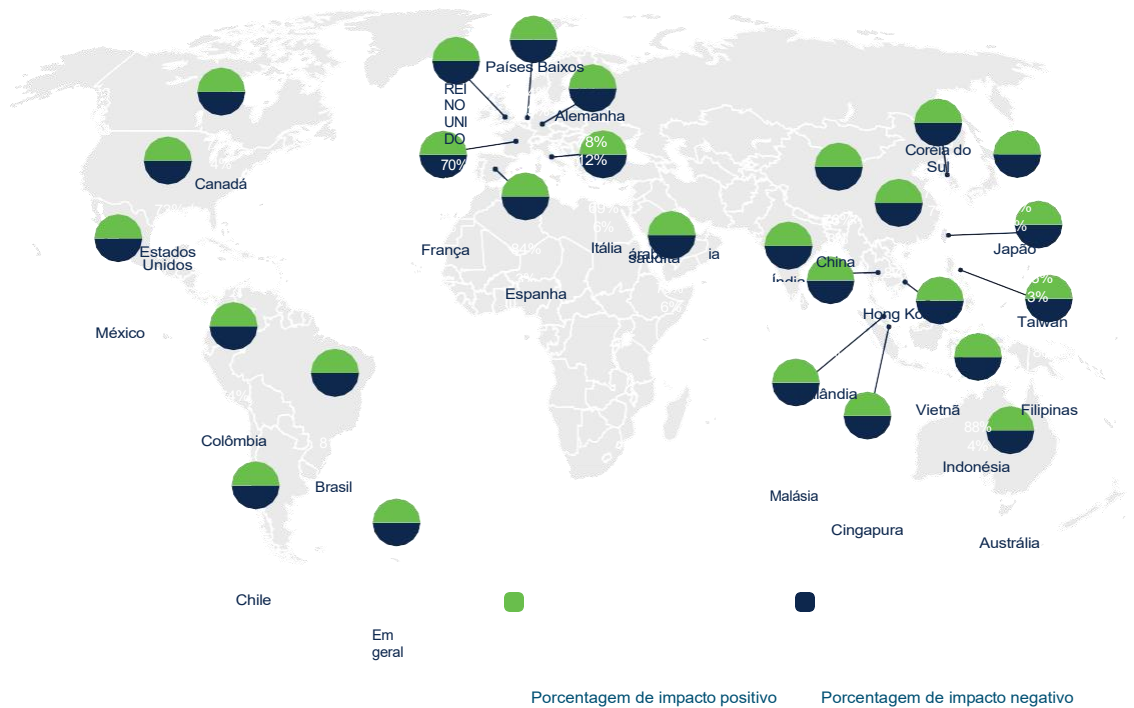


Fonte: Cisco 2023 Data Privacy Benchmark Study

A legislação de privacidade continua a ser muito bem recebida em todo o mundo. Essas leis desempenham um papel importante para ajudar a garantir que os governos responsabilizem as organizações pela forma como administram os dados pessoais, e 157 países (acima dos 145 do ano passado) agora têm leis de privacidade em vigor³.

Embora o cumprimento dessas leis muitas vezes envolva esforço e custo significativos (por exemplo, catalogar dados, manter registros de atividades de processamento, implementar controles - privacidade por projeto, responder a solicitações de usuários), as organizações reconhecem o impacto positivo em suas organizações. Setenta e nove por cento (79%) de todos os entrevistados corporativos disseram que as leis de privacidade tiveram um impacto positivo, 14% foram neutras, e apenas 6% indicaram que as leis tiveram um impacto negativo. Os percentuais positivos foram bastante consistentes entre as regiões, com 77% nas Américas, 79% na EMEA, e 81% na APJC. Por país, as porcentagens médias mais altas foram na Índia (92%), Chile (90%), França, Indonésia e Vietnã (88%). Ver Figura 10.

Figura 10: Reação às leis de privacidade em todo o mundo



Fonte: Cisco 2023 Data Privacy Benchmark Study

³ Fonte: Privacy Laws & Business 2022. <https://www.privacylaws.com/reports-gateway/articles/int176/int176newdplaws/>

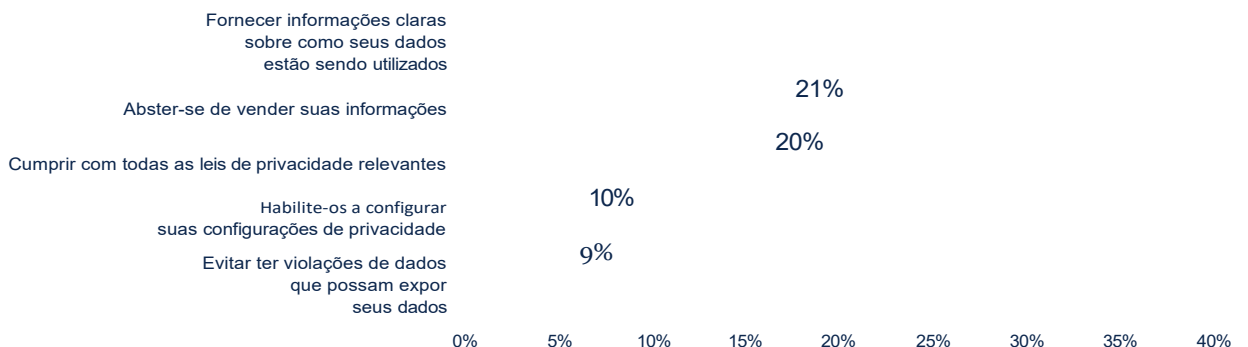
3: Desconexão entre organizações e consumidores com relação a dados e confiança

Os clientes compartilham voluntariamente seus dados pessoais com organizações para obter bens e serviços, juntamente com uma experiência personalizada e sob medida. Os clientes esperam que as organizações sejam transparentes sobre suas práticas e tratem seus dados pessoais adequadamente - um aspecto significativo para ganhar e construir confiança. Conforme descrito na Pesquisa de Privacidade do Consumidor Cisco 2022, 76% dos consumidores disseram que não comprariam de uma organização na qual não confiam seus dados, e 81% concordaram que a forma como uma organização trata seus dados é indicativa de como ela vê e respeita seus clientes.

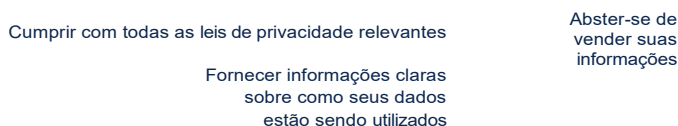
Entre as organizações que responderam à Pesquisa de Privacidade de Dados de Referência deste ano, 96% concordaram que têm uma obrigação ética de tratar os dados corretamente, acima dos 92% da pesquisa do ano passado. No entanto, suas prioridades não são totalmente consistentes com aquelas expressas pelos consumidores. A transparência - fornecendo informações facilmente acessíveis e claras sobre como seus dados estão sendo utilizados - foi a principal prioridade para os entrevistados (39%) na pesquisa com os consumidores. Quase o dobro dos entrevistados selecionou a transparência como a prioridade máxima em comparação com a não venda de informações pessoais ou o cumprimento das leis de privacidade. No entanto, na pesquisa deste ano com organizações, os entrevistados sentiram que a conformidade é a prioridade mais importante para a construção da confiança do cliente (citada em 30%), seguida pela transparência (26%). Certamente, as organizações precisam cumprir as leis de privacidade, mas quando se trata de ganhar e construir confiança, a conformidade não é suficiente. Os consumidores consideram a conformidade legal como um "dado adquirido", com transparência mais como um diferencial. Ver Figura 11.

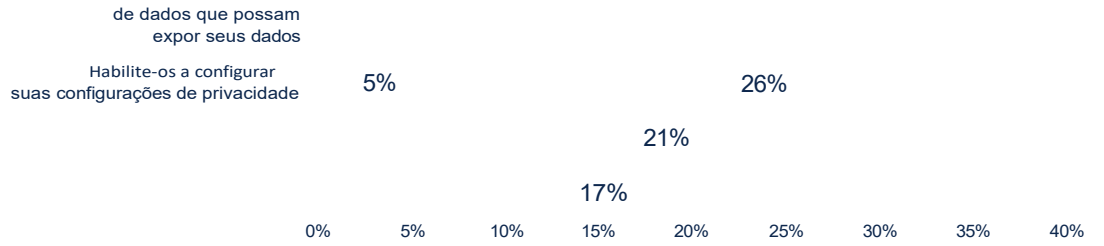
Figura 11: Prioridades para a construção da confiança dos consumidores

Visão do consumidor

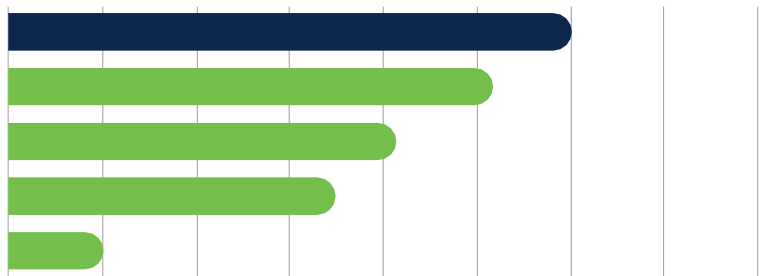
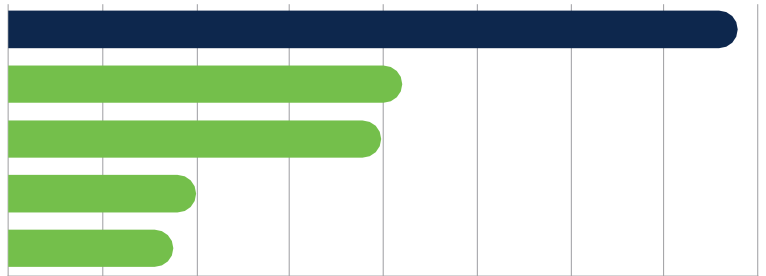


Visão organizacional





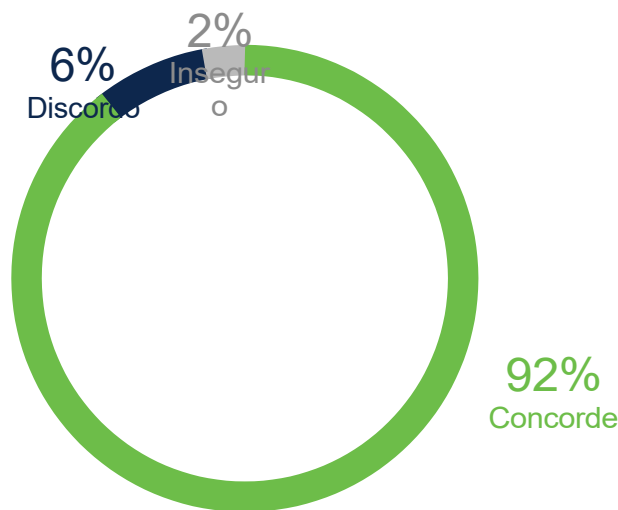
Fonte: Cisco 2023 Data Privacy Benchmark Study



Esta desconexão também pode ser vista quando se trata do uso da Inteligência Artificial (IA). Enquanto os consumidores geralmente apóiam a IA e muitos até estão dispostos a compartilhar seus dados anonimizados para ajudar a construir melhores soluções de IA, a tomada de decisão automatizada continua sendo uma área de preocupação. Pode ser difícil para os consumidores compreender os algoritmos e as decisões automatizadas que podem ter impacto direto sobre eles, como ao se qualificar para um empréstimo ou obter uma entrevista de emprego. Noventa e seis por cento (96%) das organizações em nossa pesquisa acreditam que já têm processos em vigor para atender aos padrões responsáveis e éticos que os clientes esperam, o que representa um aumento em relação aos 87% do ano passado. No entanto, a maioria dos consumidores não vê as coisas dessa maneira.

Como relatado na Pesquisa de Privacidade do Consumidor Cisco 2022, 60% dos consumidores estão preocupados com a forma como as organizações aplicam e usam a IA atualmente, e 65% já perderam a confiança nas organizações sobre suas práticas de IA. Felizmente, as organizações podem estar começando a receber a mensagem de que não estão fazendo o suficiente. Noventa e dois por cento (92%) dos entrevistados disseram que quando se trata da aplicação e uso da IA em suas soluções, sua organização precisa fazer mais para assegurar aos clientes que seus dados estão sendo usados apenas para os fins pretendidos e legítimos. Veja a Figura 12.

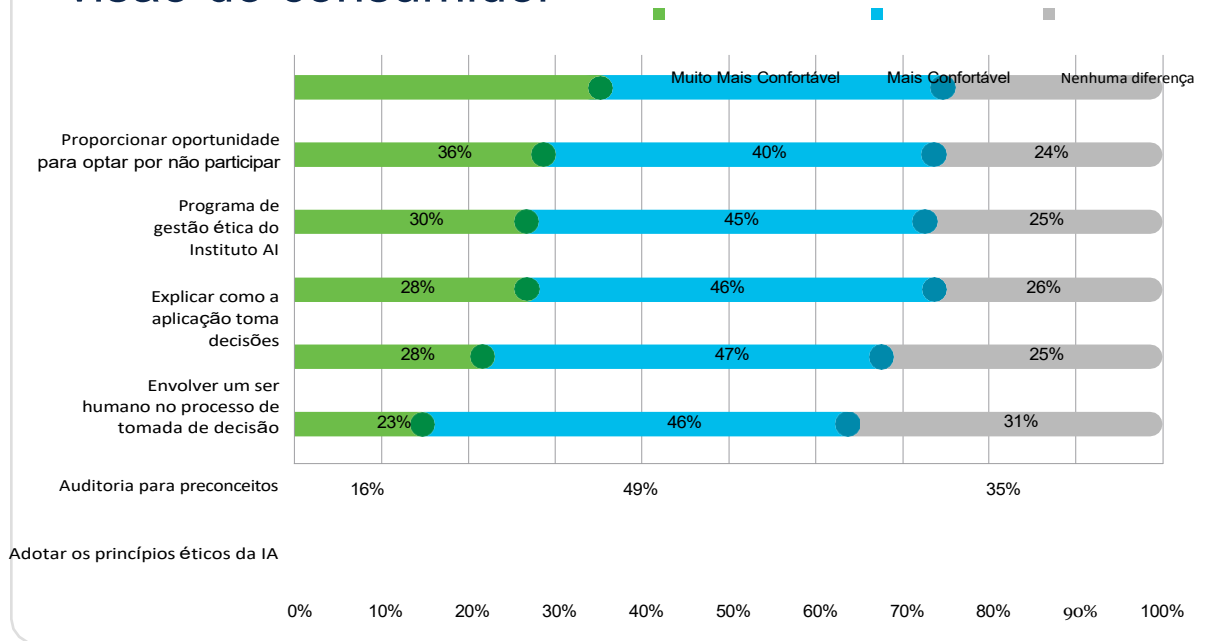
Figura 12: Porcentagem concordando que sua organização precisa fazer mais para assegurar aos clientes que seus dados estão sendo usados apenas para fins legítimos



Fonte: Cisco 2023 Data Privacy Benchmark Study

O que as organizações podem fazer? A principal abordagem para tornar os consumidores muito mais confortáveis seria oferecer oportunidades para que eles optassem por não participar da solução na qual a IA é aplicada ou utilizada, citada por 36% dos entrevistados da pesquisa de opinião dos consumidores. Ver Figura 13.

Figura 13: Abordagens para tornar os consumidores mais confortáveis com a IA, visão do consumidor



Fonte: Cisco 2023 Data Privacy Benchmark Study



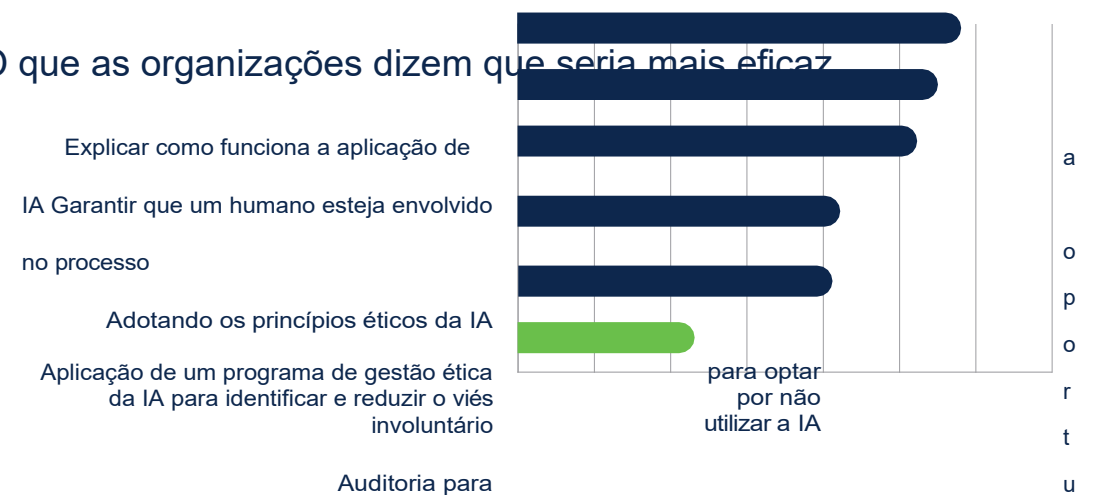
No entanto, que ações as organizações realmente implementaram e o que elas acham que mais tranquilizaria o cliente? Para estas duas perguntas, a oferta de oportunidades de opt-out foi a menos selecionada entre as seis opções. Sessenta e três por cento (63%) das organizações estão garantindo que um ser humano esteja envolvido no processo de tomada de decisão, 60% proporcionam maior transparência e 55% adotaram os princípios éticos da IA em suas operações. Apenas 21% disseram que dão aos clientes a oportunidade de optar pela não participação. As respostas são bastante semelhantes ao que as organizações acreditam ser a abordagem mais eficaz. A maioria das opções foi selecionada por 41% a 58% dos entrevistados, e apenas 22% selecionaram "dar aos clientes a oportunidade de optar por não participar", como mostrado na Figura 14.

Figura 14: Abordagens para tornar os consumidores mais confortáveis com a IA, visão organizacional

O que as organizações têm feito



O que as organizações dizem que seria mais eficaz



0% 10% 20% 30% 40% 50% 60% 70%

Fonte: Cisco 2023 Data Privacy Benchmark Study

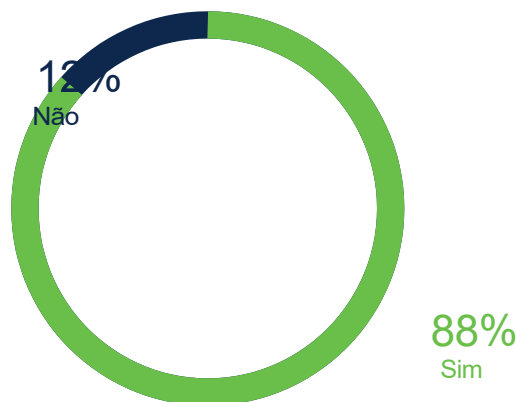
4: Apesar do desejo de localização de dados, os fornecedores globais são vistos como mais seguros do que os fornecedores locais.

Muitos governos e organizações estão estabelecendo requisitos de localização de dados, que forcem a manutenção de dados dentro de um país ou região. Para muitos, estes requisitos parecem uma boa idéia no início, mas nossa pesquisa indica que esta visão não se sustenta uma vez considerados os custos, a segurança, a privacidade e outras compensações. Na Pesquisa de Privacidade do Consumidor Cisco 2022, por exemplo, 78% dos consumidores disseram inicialmente que achavam que a localização de dados era uma boa idéia, mas o suporte caiu para 41% ao incluir o custo adicional de bens e serviços. De acordo com 89% dos consumidores das organizações na pesquisa deste ano, a localização de dados acrescenta um custo significativo às suas operações.

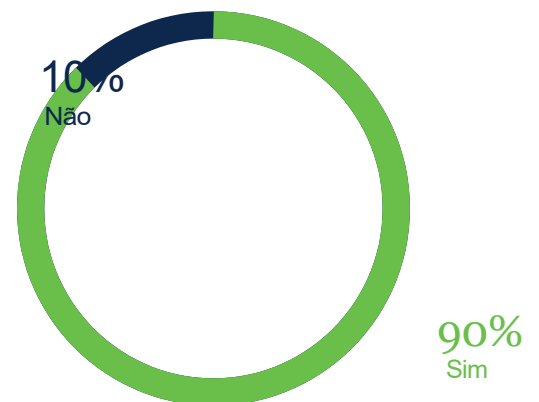
Os resultados deste estudo atual mostram que a grande maioria (88%) dos entrevistados acredita que seus dados seriam intrinsecamente mais seguros se fossem armazenados apenas dentro de seu país ou região. Notavelmente, um número ainda maior (90%) também disse que um fornecedor global, operando em escala, pode proteger melhor os dados em comparação com fornecedores locais. Ao ver estas duas afirmações juntas, parece que, embora as organizações preferissem manter seus dados locais, elas ainda preferem e confiam em um fornecedor global em vez de um fornecedor local. Naturalmente, sua solução ideal seria obter ambos - uma instância local que retém os dados criados localmente por um provedor global. Veja a Figura 15 abaixo.

Figura 15: Localização de dados

Os dados seriam intrinsecamente mais seguros se pudessem ser armazenados dentro de nosso país ou região



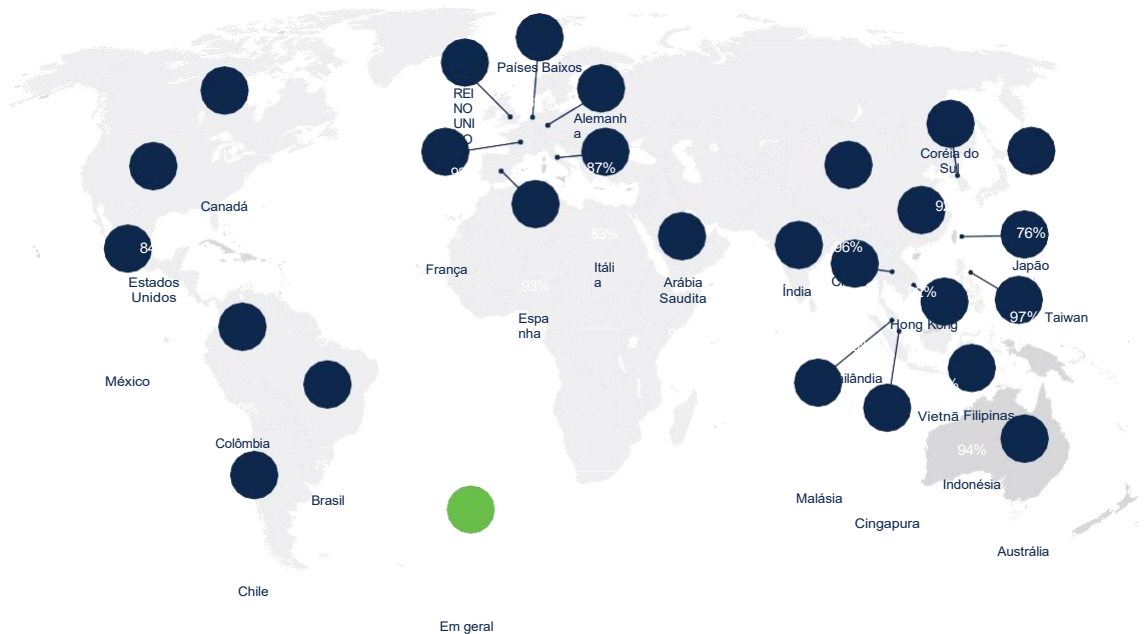
Os fornecedores globais podem proteger melhor nossos dados em comparação com os fornecedores locais



Fonte: Cisco 2023 Data Privacy Benchmark Study

Embora a localização de dados seja freqüentemente impulsionada por leis e atitudes nacionais, não houve variação substancial entre os entrevistados em diferentes geografias. A porcentagem de entrevistados dizendo que "um fornecedor global pode proteger melhor os dados em comparação com um fornecedor local" estava entre 75% e 100% em todas as 26 geografias dos entrevistados. Ver Figura 16.

Figura 16: Porcentagem concordando que um fornecedor global pode proteger os dados melhor do que um fornecedor local



Fonte: Cisco 2023 Data Privacy Benchmark Study

Conclusão e recomendações

Esta pesquisa destaca a importância da privacidade para as organizações e o crescente valor econômico dos investimentos em privacidade. Mesmo que a privacidade esteja mais integrada às prioridades e processos organizacionais, será importante para as organizações atender mais às expectativas dos consumidores com relação à transparência e ao uso de informações pessoais na tomada de decisão orientada pela inteligência artificial.

Fazer isso ajudará a melhorar a postura de privacidade de uma organização, demonstrará confiabilidade e maximizará os benefícios dos investimentos em privacidade. Os resultados desta pesquisa apontam para estas recomendações específicas:

1. Continue a investir na privacidade e construa capacidades de privacidade em toda a sua organização, especialmente entre os profissionais de segurança e TI e aqueles que estão envolvidos diretamente com o processamento e proteção de dados pessoais.
2. Seja mais transparente com seus clientes sobre como seus dados pessoais estão sendo utilizados pelas soluções e serviços que sua organização oferece. Enquanto as organizações precisam cumprir a lei, o cumprimento por si só não é suficiente; a transparência é a chave para a confiança.
3. Ao usar a IA em suas soluções, projete com os princípios éticos da IA em mente, forneça opções preferenciais de gerenciamento para tranquilizar os clientes, forneça maior transparência à decisão automatizada e garanta que um humano esteja envolvido no processo quando a decisão é conseqüente para uma pessoa.
4. Considere os custos e conseqüências da localização de dados e reconheça que os provedores locais podem ser mais caros e degradar a funcionalidade, privacidade e segurança de seus dados do que os provedores globais que operam em escala.

Satisfazendo o padrão de confiança de nossos clientes

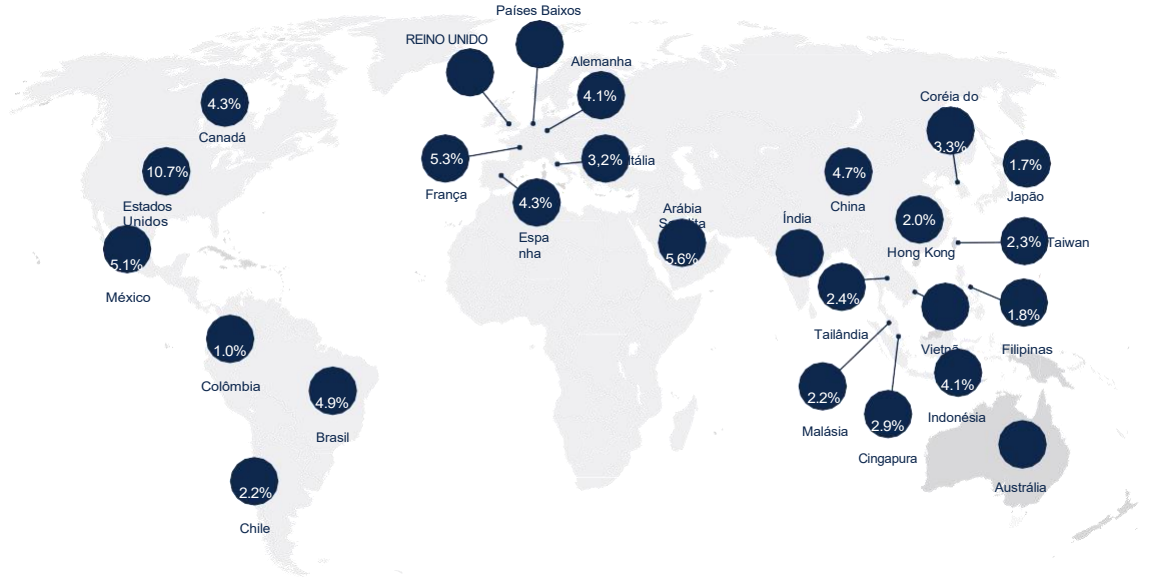
Embora as organizações sempre tenham precisado de segurança e privacidade para ganhar e construir a confiança do cliente, o ambiente de negócios de hoje as tornou de missão crítica. À medida que os clientes estabelecem seu padrão de confiança, a Cisco continua a ouvir, aprender e evoluir para atender às suas necessidades. Nossa abordagem holística da segurança e privacidade - priorizando a confiabilidade, a transparência e a responsabilidade - nos diferencia.

Saiba como a Cisco está priorizando estas recomendações em nossas operações, políticas, processos e nas soluções que oferecemos:

- [Cisco Trust Center: www.cisco.com/go/trust](http://www.cisco.com/go/trust)
- [Cisco 2022 Purpose Report - Poder: http://cs.co/9008MhQMp](http://cs.co/9008MhQMp)
- [Cisco ESG Reporting Hub - Integridade e Confiança: http://cs.co/9004JSD1O](http://cs.co/9004JSD1O)

A Cisco continuará a monitorar estas tendências e questões e compartilhará nossas conclusões. Para informações adicionais sobre a pesquisa de privacidade da Cisco, entre em contato com Robert Waitman, Diretor de Pesquisa de Privacidade e Economia da Cisco em rwaitman@cisco.com.

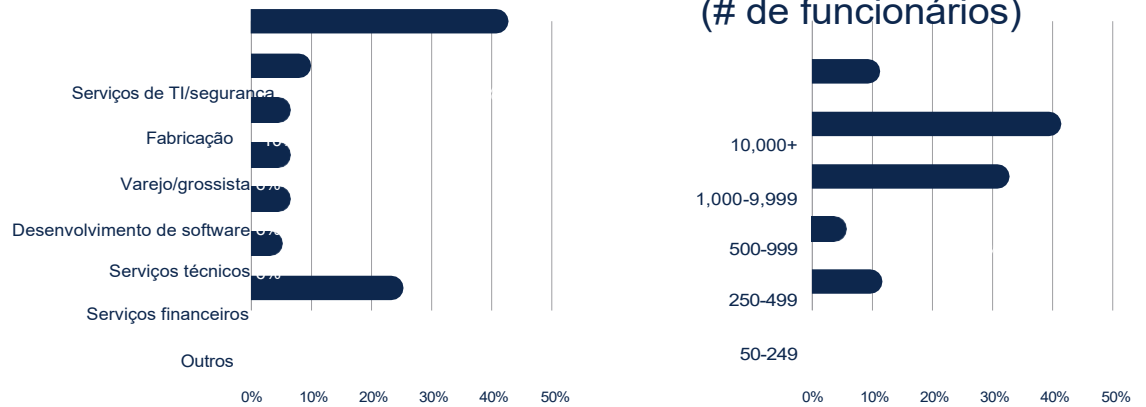
Apêndice A: Dados demográficos por geografia



Anexo B: Dados demográficos por indústria/tamanho

Por

indústria Por tamanho da empresa
(# de funcionários)



Fonte: Cisco 2023 Data Privacy Benchmark Study

Sobre a série de relatórios de ciber-segurança

Durante a última década, a Cisco publicou uma riqueza de informações de segurança e de inteligência de ameaças para profissionais de segurança interessados no estado de segurança cibernética global. Esses relatórios abrangentes forneceram relatos detalhados dos cenários de ameaça e seus efeitos sobre as organizações, bem como as melhores práticas para se defender contra os impactos adversos das violações de dados.

Em nossa nova abordagem de liderança do pensamento, a Cisco Security está publicando uma série de estudos baseados em pesquisa e baseados em dados. Expandimos o número de títulos para incluir diferentes relatórios para profissionais de segurança com diferentes interesses. Chamando a atenção para a profundidade e amplitude da experiência de pesquisadores e inovadores da indústria de segurança, os relatórios de cada série anual incluem o [Security Outcomes Report](#), [Threat Report e Blogs](#), e [Data Privacy Benchmark Study](#), e [Consumer Privacy Survey](#), com outros publicados ao longo de cada ano.





CISCO SECURE