# Como otimizar os investimentos feitos em privacidade de dados

## Estudo referencial de privacidade de dados

cisco

# Resumo executivo

**O EU General Data Protection Regulation (GRPR, Regulamento Geral de Proteção de Dados da UE) tornou-se obrigatório em 25 de maio de 2018, e as leis e regulamentos de privacidade em todo o mundo continuam mudando e se expandido.**

*Os clientes estão fazendo cada vez mais perguntas durante o ciclo de compra, sobre como seus dados são coletados, usados, transferidos, compartilhados, armazenados e destruídos.*

A maioria das empresas investiu e continua investindo em pessoas, processos, tecnologia e políticas para atender aos requisitos de privacidade do cliente e evitar multas pesadas e outras penalidades. Além disso, as violações de dados continuam expondo as informações pessoais de milhões de pessoas, e as empresas estão preocupadas com os produtos que elas compram, os serviços que usam, as pessoas que empregam e com quem firmam parcerias e fazem negócios em geral. Como resultado, os clientes estão fazendo cada vez mais perguntas durante o ciclo de compra, sobre como seus dados são coletados, usados, transferidos, compartilhados, armazenados e destruídos. No estudo do ano passado (Estudo referencial de eficiência da privacidade da Cisco 2018), a Cisco apresentou dados e insights relacionados a como essas preocupações de privacidade prejudicavam o ciclo de compras e os cronogramas. Este ano, a pesquisa atualiza essas descobertas e explora os benefícios associados ao investimento em privacidade.

O Estudo de referência de privacidade de dados da Cisco utiliza dados do Estudo de referência anual de segurança digital da Cisco, uma pesquisa duplo-cega realizada com mais de 3.200 profissionais de segurança, em 18 países, e em todos os principais setores e regiões. Muitas das perguntas específicas de privacidade foram feitas a mais de 2.900 entrevistados familiarizados com os processos de privacidade em suas empresas. Os participantes responderam se estão preparados para o GDPR, para possíveis atrasos no ciclo de vendas devido a preocupações com a privacidade de dados do cliente, para perdas por violações de dados e sobre suas práticas atuais relacionadas à otimização do valor de seus dados.

**Os resultados deste estudo fornecem fortes evidências de que as empresas, além de estarem em conformidade, estão se beneficiando dos investimentos feitos em privacidade.** As empresas em conformidade com o GDPR enfrentam atrasos menores no ciclo de vendas relacionados às preocupações com a privacidade de dados dos clientes em comparação às empresas que não estão conformidade. As empresas em conformidade com o GDPR também tiveram menos violações, e mesmo que tenham ocorrido, apresentaram menos impacto nos registros e menos tempo de inatividade do sistema. Como resultado, o custo total de violações de dados foi menor para empresas em conformidade com o GDPR. Embora as empresas tenham concentrado seus esforços no cumprimento dos regulamentos e requisitos de privacidade, quase todas dizem que estão recebendo outros benefícios corporativos desses investimentos, além da conformidade. Esses benefícios relacionados à privacidade estão proporcionando vantagens competitivas para as empresas, e esse estudo pode ajudar a orientar as decisões de investimento, pois as empresas se esforçam para tornar seus processos de privacidade mais eficientes.

> **“A privacidade é um ingrediente essencial ao sucesso organizacional, tanto para proteger os dados quanto para incentivar a inovação .”**
>
> **John N. Stewart, vice-presidente sênior e chefe de segurança e confiança, Cisco**

**“Esta pesquisa fornece evidências de algo que os profissionais de privacidade há muito entenderam: que as organizações estão se beneficiando de seus investimentos em privacidade, além da conformidade. O estudo da Cisco demonstra que uma conformidade sólida com a privacidade diminui o ciclo de vendas e aumenta a confiança do cliente”.**

**Peter Lefkowitz, diretor de riscos digitais, Citrix Systems e presidente do conselho de 2018 da International Association of Privacy Professionals (IAPP)**

# Os resultados

## Conformidade com o GDPR

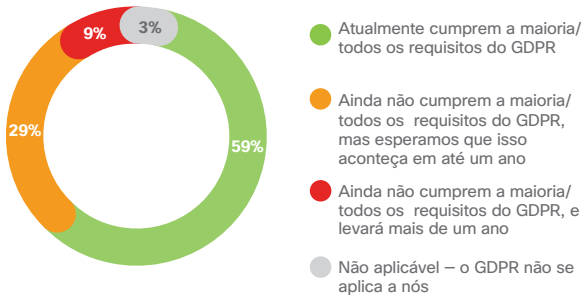
Entre todos os entrevistados no Estudo referencial de privacidade de dados, 59% indicaram que atualmente estão cumprindo todos ou a maioria dos requisitos do GDPR. (Consulte a Figura 1) Cerca de 29% disseram que esperam estar em conformidade com o GDPR em um ano, e outros 9% afirmaram que levará mais de um ano para alcançar a conformidade. Embora o GDPR seja aplicado às empresas localizadas na UE ou ao processamento de dados pessoais coletados sobre os entrevistados localizados na UE, é interessante que somente 3% da nossa pesquisa global indicaram que não acreditavam no GDPR aplicado à empresa.

Por país, o nível de conformidade com o GDPR variou de 42% a 76%. (Consulte a Figura 2) Conforme esperado, os países europeus que participaram da pesquisa (Espanha, Itália, Reino Unido, França, Alemanha) apresentaram os maiores percentuais de conformidade.

*Somente 3% dos entrevistados em nossa pesquisa global indicaram que não acreditavam no GDPR aplicado à empresa.*

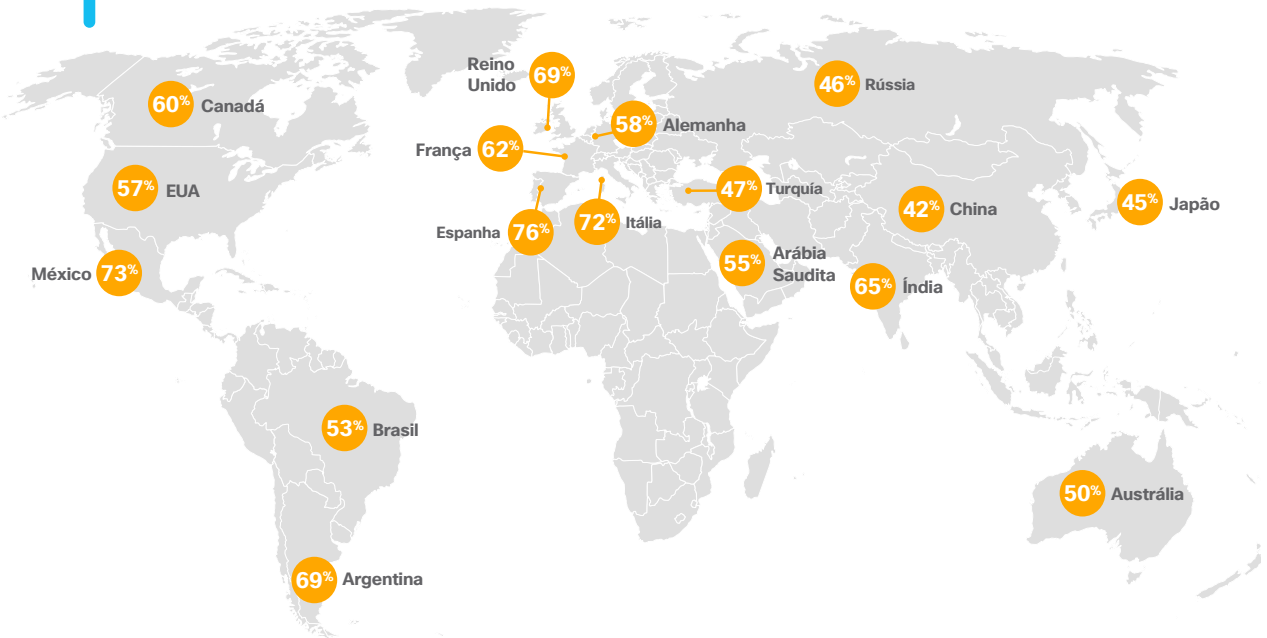
**59% das relataram cumprindo todos ou a maioria dos requisitos do GDPR atualmente, com outros 29% esperando cumprir em um ano. Os principais desafios para se preparar para o GDPR foram identificados como: segurança de dados, treinamento do funcionário e atualização em relação às regulamentações em evolução.**

**Figura 1** Conformidade com o GDPR
Porcentagem de entrevistados, N= 3.206




*Fonte: Estudo referencial de privacidade de dados da Cisco 2019, n = 3.206*

**Figura 2** Preparação para o GDPR por país
Porcentagem de entrevistados, N = 3.206




*Fonte: Estudo referencial de privacidade de dados da Cisco 2019*

Os entrevistados foram solicitados a identificar os desafios mais significativos que as suas empresas enfrentaram ao se prepararem para o GDPR. As principais respostas foram segurança de dados, treinamento interno, regulamentações em mudança e requisitos de Privacidade por projeto. (Veja a Figura 3)

**Figura 3** Desafios mais significativos para se prepararem para o GDPR
Porcentagem de entrevistados, N = 3.098

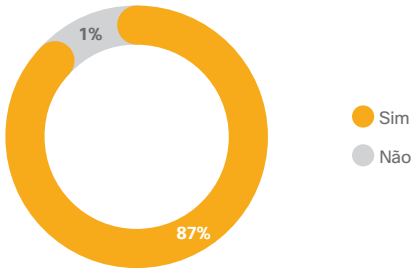
| | |
|---|---|
| **42%** | Cumprimento dos requisitos de segurança de dados |
| **39%** | Treinamento interno |
| **35%** | Ficar a par dos desenvolvimentos em constante mudança à medida que o regulamento se torna mais eficiente |
| **34%** | Cumprimento dos requisitos de Privacidade por projeto |
| **34%** | Cumprimento das solicitações de acesso dos titulares dos dados |
| **31%** | Catalogação e inventário dos nossos dados |
| **30%** | Permissão de solicitações de exclusão de dados |
| **29%** | Contratação/identificação dos diretores de proteção de dados de cada geografia relevante |
| **28%** | Gerenciamento de fornecedor |

*Fonte: Estudo referencial de privacidade de dados da Cisco 2019*

## Atraso das vendas devido à privacidade

Os entrevistados foram questionados se tiveram atrasos nos ciclos de vendas devido a preocupações sobre a privacidade de dados dos clientes 87% dos entrevistados disseram que têm atrasos nas vendas, seja de clientes atuais ou potenciais. (Veja a Figura 4) Isso é significativamente mais alto do que os 66% dos entrevistados que relataram atrasos de vendas na pesquisa do ano passado e, provavelmente, devido à maior conscientização sobre a importância da privacidade de dados, tornando o GDPR aplicável, e o surgimento de outras leis de privacidade e requisitos. A privacidade de dados tornou-se um problema de nível de diretoria para muitas empresas, e os clientes garantem que seus fornecedores e parceiros de negócios tenham respostas adequadas às suas preocupações com a privacidade, antes de fecharem negócios.

**Figura 4** Os entrevistados tiveram atrasos nos ciclos de vendas devido a preocupações sobre a privacidade de dados dos clientes
Porcentagem de entrevistados, N= 2.064




*Fonte: Estudo referencial de privacidade de dados da Cisco 2019*

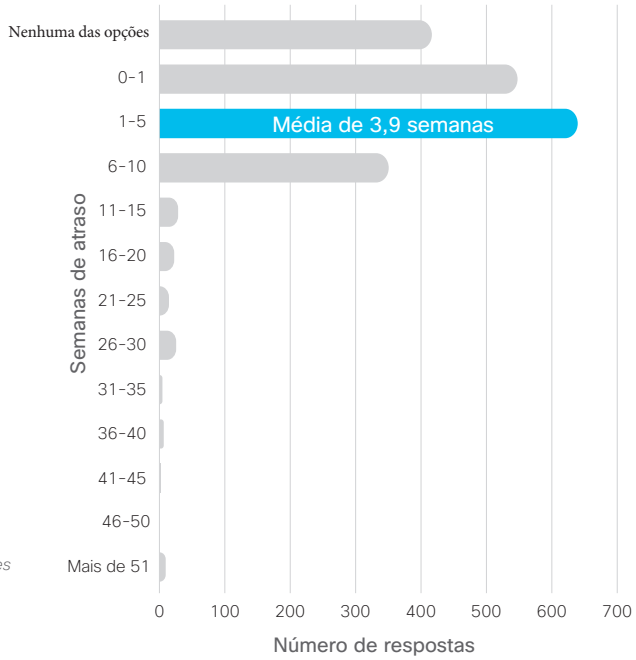
Quando questionados sobre a duração do atraso, as estimativas variaram muito. O atraso médio de vendas para clientes existentes foi de 3,9 semanas e mais de 94% das empresas relataram atrasos entre 0 e 10 semanas. Mesmo assim, algumas empresas relataram atrasos de até 25 a 50 semanas ou mais. (Veja a Figura 5) Observe que o atraso médio das vendas para clientes potenciais foi de 4,7 semanas, talvez refletindo os prazos mais longos necessários para lidar adequadamente com as preocupações de privacidade em um novo relacionamento com o cliente potencial.

**Atrasos de vendas devido a preocupações de privacidade de dados do cliente continuam**

**87% relataram que tinham na venda para clientes existentes ou potenciais, um aumento significativo desde o último ano.**

Esses atrasos médios para os clientes atuais e potenciais são significativamente mais curtos do que a média de 7,8 semanas relatada na pesquisa do ano passado, talvez refletindo o fato de que as empresas estão mais bem preparadas, em relação ao último ano, para responderem às preocupações de privacidade do cliente.

**Figura 5** Atrasos na resposta às preocupações com privacidade de dados dos clientes
Porcentagem de entrevistados, N= 2.081




*Fonte: Estudo referencial de privacidade de dados da Cisco 2019*

*As principais razões para atrasos de vendas relacionados à privacidade:*

- *investigação das solicitações do cliente*
- *tradução das informações de privacidade para o idioma do cliente*
- *orientação do cliente sobre as práticas e processos de privacidade da empresa*
- *levando a um novo projeto do produto para atender aos requisitos de privacidade do cliente*

Por país, a distribuição de atrasos de vendas para clientes existentes variou de 2,2 semanas a 5,5 semanas. Atrasos mais longos geralmente podem ser encontrados onde os requisitos de privacidade são altos ou em um estado de transição, à medida que as empresas trabalham para se adaptar às preocupações relatadas por seus clientes. (Veja a Figura 6).

**Figura 6** Detalhamento de atrasos da distribuição de vendas por país
Porcentagem de entrevistados, N= 2.081

| País | Média de atraso (semanas) |
|---|---|
| Alemanha | 3.1 |
| Arábia Saudita | 4.8 |
| Argentina | 3.9 |
| Australia | 3.9 |
| Brasil | 5.2 |
| Canadá | 5.1 |
| China | 3.5 |
| Espanha | 5.5 |
| Estados Unidos | 3.7 |
| França | 4.2 |
| Índia | 4.9 |
| Itália | 2.6 |
| Japão | 4.1 |
| México | 2.9 |
| Reino Unido | 4.9 |
| Rússia | 2.5 |
| Turquia | 2.2 |
| Resumo | 3.9 |

*Fonte: Estudo referencial de privacidade de dados da Cisco 2019*

Os atrasos de vendas, no mínimo, fazem com que a receita seja adiada por algum período. Isso pode levar ao não cumprimento das metas de receita, afetando a remuneração, as decisões de financiamento e as relações com o investidor. Além disso, as vendas atrasadas podem se transformar em vendas perdidas, por exemplo, quando atrasos fazem com que um cliente potencial compre um produto do concorrente ou não compre o produto ou serviço.

Os entrevistados também foram solicitados a identificar os motivos de qualquer atraso na venda relacionada à privacidade das empresas. As principais respostas incluíam a necessidade de investigar solicitações específicas de clientes, traduzir informações de privacidade para o idioma do cliente, orientar o cliente sobre as práticas ou processos de privacidade da empresa ou reprojetar o produto para atender aos requisitos de privacidade do cliente. (Veja a Figura 7).

**Figura 7** Motivos para atrasos de vendas
Porcentagem de entrevistados, N= 1.812

| | |
|---|---|
| **49%** | Precisamos investigar requisitos específico /incomuns para o cliente/cliente potencial, antes que eles se sintam confortáveis com nossas práticas de privacidade. |
| **42%** | Precisamos traduzir informações sobre nossas políticas/processos de privacidade para o idioma do cliente/cliente potencial. |
| **39%** | O cliente/cliente potencial precisa se informar mais sobre as nossas políticas ou processos. |
| **38%** | Nosso produto ou serviço precisa ser reformulado para atender aos requisitos de privacidade do cliente/cliente potencial. |
| **33%** | Não podemos ou não queremos atender aos requisitos de privacidade do cliente/cliente potencial (por exemplo, políticas de violação de dados, requisitos de exclusão de dados). |
| **28%** | Leva tempo para encontrar a pessoa certa ou a equipe para responder às perguntas do cliente/ cliente potencial. |
| **17%** | Temos que resolver questões sobre qual parte é responsável pelos dados. |
| **5%** | Temos que envolver nossos advogados para esclarecer a incerteza em relação à lei. |

*Fonte: Estudo referencial de privacidade de dados da Cisco 2019*

## Benefícios corporativos dos investimentos em privacidade

As empresas que investiram na preparação para o GDPR tinham como objetivo principal evitar as multas significativas e outras penalidades associadas ao não cumprimento do regulamento. No entanto, conforme indicado pela pesquisa, há outros benefícios comerciais associados a esses investimentos de privacidade.

Ao observar os atrasos nas vendas devido a problemas de privacidade, o atraso médio de vendas para clientes existentes era de 3,9 semanas. No entanto, as empresas que informaram o cumprimento de todos ou quase todos os requisitos do GDPR tiveram um atraso médio de vendas de 3,4 semanas, comparado a 4,5 semanas para empresas que ainda não estão preparadas, mas esperam estar dentro de um ano, e 5,4 semanas para as empresas que estão mais de um ano longe de estarem preparadas para o GDPR. Portanto, as empresas menos preparadas têm atrasos médios que são quase 60% maiores do que aqueles que estão mais preparados. (Veja a Figura 8).

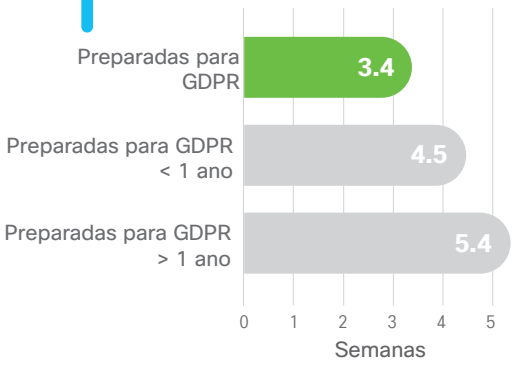
**Embora uma maior parte tenha relatado violações no ano passado, uma porcentagem menor (74%) de empresas preparadas para o GDPR foi afetada, se comparada a 80% das empresas com menos de um ano para se prepararem para o GDPR e 89% das com mais tempo para se prepararem para o GDPR.**

## Resumo dos resultados principais

As empresas prontas para GDPR estão se beneficiando de seus investimentos em privacidade, além da conformidade, de várias maneiras tangíveis. Elas tiveram atrasos de vendas mais curtos devido às preocupações de privacidade do cliente (3,4 semanas versus 5,4 semanas). Elas tinham uma probabilidade menor de ter experimentado uma violação no último ano (74% versus 89%), e quando uma violação ocorreu, menos registros de dados foram afetados (79 mil versus 212 mil registros), além disso o tempo de inatividade foi mais curto (6,4 horas versus 9,4 horas). Como resultado, os custos gerais associados a essas violações foram menores; somente 37% das empresas preparadas para GDPR tiveram uma perda de US $ 500.000 no último ano, em comparação a 64% da empresa menos preparada para o GDPR.

Esses resultados destacam que a eficiência da privacidade se tornou uma importante vantagem competitiva para muitas empresas. As empresas devem se esforçar para maximizar os benefícios comerciais de seus investimentos em privacidade, que podem ir além do requisitos de qualquer regulamentação de privacidade em particular.

**Figura 8** Média de semanas de atraso (existentes)
Porcentagem de entrevistados, N= 2.081



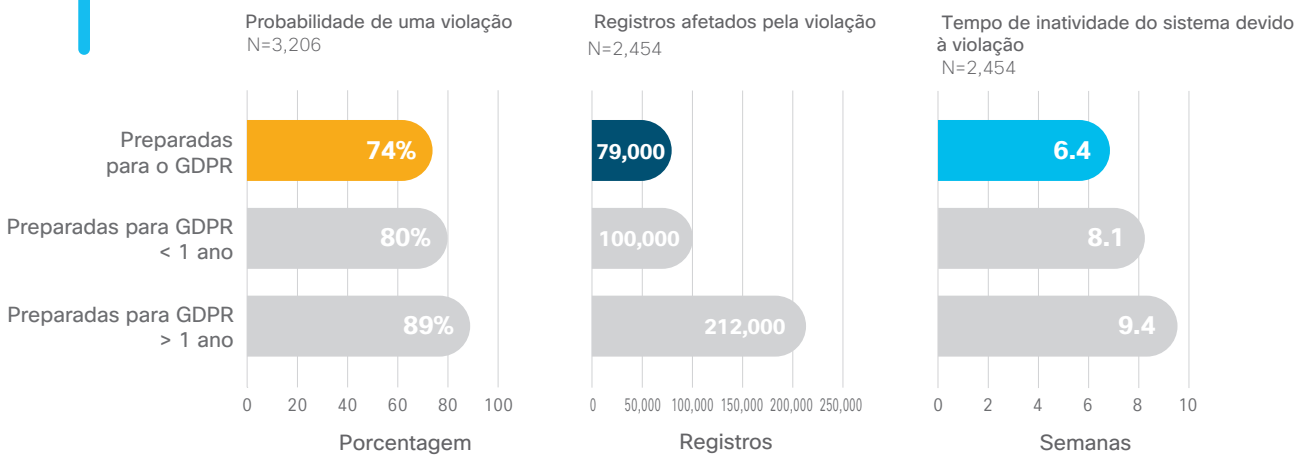

*Fonte: Estudo referencial de privacidade de dados da Cisco 2019*

Outra vantagem real da preparação para o GDPR é que ela parece reduzir a frequência e o impacto das violações de dados. O GDPR exige que as empresas saibam onde estão localizadas as informações pessoalmente identificáveis (PII) e forneçam proteções apropriadas para esses dados. Esses esforços podem ter ajudado as empresas a entender melhor seus dados, os riscos associados a seus dados e a estabelecer ou fortalecer proteções para eles.

> **"As empresas têm um longo caminho a percorrer para maximizar o valor de seus investimentos em privacidade. Nossa pesquisa mostra que o mercado está pronto e pronto para aqueles dispostos a investir em ativos de dados e privacidade chegar lá".**
>
> **Michelle Dennedy, diretora de privacidade, Cisco**

Embora muitas empresas relataram violações de dados no último ano, uma porcentagem menor (74%) das empresas preparadas para o GDPR foi afetada, se comparada a 80% das empresas com menos de um ano para se prepararem para o GDPR e 89% das com mais tempo para se prepararem para o GDPR. (Veja a Figura 9).

**Figura 9** Benefícios corporativos dos investimentos em privacidade




*Fonte: Estudo referencial de privacidade de dados da Cisco 2019*

**Com menos registros afetados e tempos de inatividade menores, não é de surpreender que as empresas prontas para GDPR tenham custos gerais menores associados a violações de dados.**

Além disso, depois de ocorrida a violação, as empresas preparadas para GDPR tiveram um impacto menor. O número médio de registros afetados foi de 79.000 para essas empresas em comparação com 212.000 para as que estão menos preparadas para o GDPR (consulte a Figura 9).

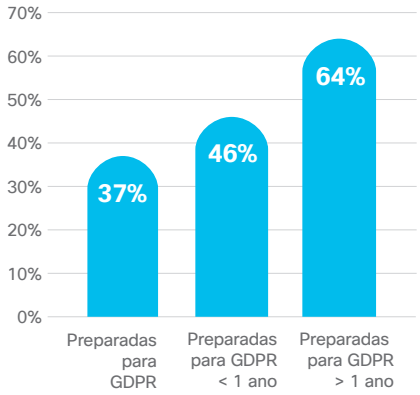
As empresas preparadas para GDPR também passaram por interrupções mais curtas do sistema associadas à violação, talvez por estarem relacionadas a um melhor gerenciamento de seus ativos de dados.

As empresas preparadas para GDPR tiveram um tempo de inatividade médio do sistema de 6,4 horas em comparação com 9,4 horas para empresas menos preparadas para o GDPR. (Veja a Figura 9)

Com menos registros afetados e tempos de inatividade menores, não é de surpreender que as empresas prontas para GDPR tenham custos gerais menores associados a violações de dados. Somente 37% dessas empresas tiveram perdas causadas por violações de dados, totalizando, no mínimo, US$ 500.000, se comparadas a 64% dessas empresas menos preparadas para o GDPR (Consulte a Figura 10)

*Quase todas as empresas (97%) informam que estão recebendo benefícios auxiliares hoje de seus investimentos em privacidade, incluindo agilidade/inovação, vantagem competitiva, eficiência operacional, mitigação de perdas resultantes de violações, redução de atrasos de vendas e atração de investidores.*

**Figura 10** Probabilidade de violação de dados de US$ 500.000
Porcentagem de entrevistados, N= 3206




*Fonte: Estudo referencial de privacidade de dados da Cisco 2019*

## As empresas reconhecem os benefícios do investimento em privacidade

As duas seções anteriores deste estudo destacaram as correlações entre investimentos em privacidade e benefícios empresariais, tais como
Menores atrasos em vendas e menos custos com violações de dados. É interessante observar que a maioria dos entrevistados está reconhecendo muitos desses benefícios. Quando perguntado se o investimento em privacidade gerava benefícios (como maior agilidade e inovação, ganho de vantagem competitiva, eficiência operacional etc.), 75% de todos os entrevistados identificaram um ou mais desses benefícios e quase todas as empresas (97%) identificaram, no mínimo, um benefício. (Veja a Figura 11)

**Figura 11** Benefícios dos investimentos em privacidade
Porcentagem de entrevistados, N= 3259

| | |
|---|---|
| 42% | Proporcionam agilidade e inovação pelo controle dos dados apropriados. |
| 41% | Obtêm vantagem competitiva em comparação com outras empresas. |
| 41% | Alcançam a eficiência operacional devido aos dados organizados e catalogados. |
| 39% | Mitigam as perdas relacionadas a violações de dados. |
| 37% | Reduzem quaisquer atrasos de vendas devido a preocupações com a privacidade de clientes/ clientes potencial. |
| 36% | Atraem investidores. |
| 3% | Nenhuma das alternativas acima. |

*Fonte: Estudo referencial de privacidade de dados da Cisco 2019*

*As empresas que informaram que estão atendendo a todos ou a maioria dos requisitos de GDPR tiveram um atraso médio de vendas de 3 a 4 semanas*

## Maximização do valor dos dados

A privacidade de dados é um aspecto essencial do esforço geral de uma empresa para maximizar o valor de seus ativos sobre os dados aplicações. Como qualquer outro ativo, os dados devem ser eficientemente adquiridos, armazenados, protegidos, utilizados e arquivados/excluídos. As organizações que maximizam o valor de seus dados de maneiras apropriadas podem se beneficiar muito ao criar laços de confiança com os clientes e usar dados bem protegidos e selecionados para melhorar a experiência do cliente e agregar mais valor para todas as partes interessadas.

Os entrevistados nesta pesquisa foram questionados sobre uma variedade de comportamentos tipicamente encontrados em ambientes de dados eficientes, como ter um catálogo de dados completo, conectar dados a outros ativos, contratar um diretor de dados e monetizar os dados externamente. (Consulte a Figura 12). Menos da metade dos entrevistados da pesquisa exibiu cada uma dessas características, e essa será uma área para pesquisas futuras, visando entender melhor como as organizações estão maximizando o valor de seus ativos de dados.

## Implicações

Esses resultados destacam que o investimento em privacidade criou um valor corporativo multo além da conformidade e se tornou uma importante vantagem competitiva para muitas empresas. Portanto, as empresas devem trabalhar para entender as implicações de seus investimentos em privacidade, inclusive reduzindo atrasos em seu ciclo de vendas e reduzindo os riscos e custos associados a violações de dados, além de outros benefícios potenciais como agilidade/inovação, vantagem competitiva e eficiência operacional.

A análise e os insights dessa pesquisa podem servir como estrutura e ponto de partida para cada empresa para maximizar o valor de seus investimentos em privacidade.

**Figura 12** Comportamentos normalmente encontrados em ambientes de dados eficientes.
Porcentagem de entrevistados, N= 3259

| | |
|---|---|
| 42% | Compreendemos o valor de quase/todos nossos ativos de dados. |
| 42% | Sabemos onde quase/todas as informações pessoalmente identificáveis (PII) estão localizadas e como elas são usadas. |
| 40% | Somos eficientes em conectar diferentes ativos de dados para criar mais valor para nossos clientes e para nós mesmos. |
| 37% | Temos um catálogo relativamente completo de nossos ativos de dados. |
| 32% | Temos um chefe de dados. |
| 32% | Nos consideramos uma empresa baseada em informações. |
| 30% | Somos capazes de monetizar ativos de dados selecionados vendendo-os (ou trocando-os) externamente. |
| 2% | Nenhuma das alternativas acima. |

*Fonte: Estudo referencial de privacidade de dados da Cisco 2019*

**As organizações que maximizam o valor de seus dados de maneiras apropriadas podem se beneficiar muito ao criar laços de confiança com os clientes e usar dados bem protegidos e selecionados para melhorar a experiência do cliente e agregar mais valor para todas as partes interessadas.**

> “Uma boa política de privacidade corporativa pode proteger as empresas contra os danos financeiros causados por uma violação de dados – oferecendo aos clientes transparência e controle sobre suas informações pessoais – enquanto uma política falha pode agravar os problemas causados por uma violação”.
>
> Harvard Business Review, “A Strong Privacy Policy Can Save Your Company Millions”, 15 de fevereiro de 2018

# Conclusão

*O investimento em privacidade criou um valor corporativo multo além da conformidade e se tornou uma importante vantagem competitiva para muitas empresas.*

Esta pesquisa quantificou vários benefícios de negócios relacionados à eficiência da privacidade. Muitos dos benefícios inicialmente identificados no relatório do ano passado foram confirmados e explorados de forma mais completa, incluindo a redução de atrasos de vendas relacionados à privacidade e a redução da frequência e do impacto das violações de dados. Em pesquisas futuras, exploraremos como esses benefícios estão mudando ao longo do tempo, especialmente à medida que as regulamentações de privacidade e as expectativas dos clientes continuam a evoluir em diferentes setores e diferentes regiões geográficas. A Cisco continuará a trabalhar com nossos clientes e outros líderes no setor de privacidade para fornecer uma melhor tomada de decisão de investimentos e aumentar a confiança com nossos clientes. Para obter mais informações, consulte:

Privacidade de dados: uma perspectiva corporativa

# Sobre a Serie de Relatórios de Cibersegurança

Ao longo da última década, a Cisco publicou uma série de informações sobre inteligência de ameaças para profissionais de segurança interessados no status global da segurança digital. Estes relatórios abrangentes forneciam detalhes dos cenários de ameaças e as implicações para as empresas, bem como as melhores práticas para se defenderem contra os impactos das violações de dados.

Na nova abordagem da nossa liderança de pensamento, a Cisco Security está publicando vários artigos baseados em pesquisas e orientados por dados no banner **Serie de Relatórios de Cibersegurança**. Ampliamos o número de títulos para incluir relatórios diferentes para profissionais de segurança com interesses diferentes. Apelando para a profundidade e amplitude da experiência de pesquisadores de ameaças e inovadores no setor de segurança, a coleção de relatórios da série 2019 inclui o Relatório de Privacidade de Dados, o Relatório de Ameaças e o Relatório de Referência do CISO, e outros ainda virão ao longo do ano.

Para obter mais informações, acesse www.cisco.com/br/securityreports.

**Sede - América**
Cisco Systems, Inc. San Jose, CA

**Sede na região da Ásia-Pacífico**
Cisco Systems (EUA) Pte. Ltd. Cingapura

**Sede na Europa**
Cisco Systems International BV Amsterdam,

A Cisco possui mais de 200 escritórios em todo o mundo. Os endereços, números de telefone e de fax estão disponíveis no site da Cisco: www.cisco.com/go/offices.

Publicação: janeiro de 2019 PRIV_01_0119_r1