Fortalecendo a privacidade e a confiança em um mundo baseado em dados

Principais conclusões da Global State of Information Security® Survey 2018

pwc

Apresentação

Como as empresas podem gerenciar melhor os riscos crescentes para a privacidade e a segurança dos seus dados? Essa é uma questão cada vez mais importante em uma sociedade extremamente conectada e que avança com base em inovações como *big data*, *data analytics*, inteligência artificial e aprendizagem de máquina.

Segundo a nossa *Global State of Information Security® Survey* 2018, muitas organizações em todo o mundo precisam de um gerenciamento de risco de privacidade mais forte e mais bem integrado à segurança cibernética para proteger o futuro dos seus próprios negócios.

Nas próximas páginas, apresentamos algumas conclusões do nosso estudo em relação a esse tema e destacamos nove *insights* para os líderes de negócios sobre como fortalecer a privacidade e a confiança em uma organização em um mundo baseado em dados.

Insights *da PwC sobre privacidade e confiança de dados*

O desafio para os CEOs está em passar da consciência à ação.

Comprometer-se com o gerenciamento de riscos na transformação digital é uma questão de sobrevivência.

As expectativas de privacidade se concentram não só na confidencialidade, mas também no uso de dados.

A tecnologia de autenticação avançada contribuirá para a geração de confiança.

Mesmo os gigantes da indústria devem ampliar o envolvimento da alta administração, do conselho e dos comitês.

Violações maciças de dados e a constante coleta de informações pessoais estimulam o debate sobre o fim da privacidade na era digital. Estamos em um mundo pós-privacidade? Sob vários aspectos, essa é a pergunta errada. Privacidade, segurança e confiança – todas em crescente risco – são cada vez mais vitais e interligadas em nossa sociedade baseada em dados.

Mais empresas devem avaliar a contratação de um Chief Privacy Officer (CPO).

Empresas retardatárias na Europa e no Oriente Médio têm mais trabalho a fazer.

A balcanização da Internet vai mudar a forma como as empresas fazem negócios.

O "bolso" pesará na escolha do consumidor pela inovação responsável e pelo uso consciente de dados.

Próximos passos para líderes de negócios globais.

Muitas organizações no mundo inteiro estão deixando de fazer tudo o que poderiam para proteger a privacidade, segundo informa a nossa *Global State of Information Security® Survey* 2018. É preciso fortalecer o gerenciamento de riscos de privacidade e integrá-lo melhor com a segurança cibernética. Consumidores e reguladores esperam por isso. Para CEOs e conselhos de administração, a questão principal é menos o futuro da privacidade e mais o futuro de suas próprias organizações: minha empresa conseguirá reunir a vontade e a imaginação necessárias para reagir ao choque e colocar em prática o gerenciamento de riscos de privacidade? Ela aproveitará esse impulso para integrar a segurança cibernética, esforçando-se para se tornar uma marca confiável e responsável em termos de inovação e uso de dados? Ou cederá seu lugar no mercado a concorrentes mais comprometidos?

Com base nas principais revelações da GSISS 2018, destacamos neste relatório nove *insights* sobre como fortalecer a privacidade e a confiança em uma organização em um mundo baseado em dados. Para encerrar, apresentamos quais são os próximos passos para os líderes empresariais globais.

1. O desafio para os CEOs está em passar da consciência à ação

87%
dos CEOs globais afirmam que estão investindo em segurança cibernética para desenvolver a confiança na relação com os clientes.

Altos executivos reconhecem os riscos crescentes da insegurança cibernética. Isso fica claro tanto na GSISS 2018 como na nossa *21ª Pesquisa Anual Global com CEOs*.[1] Na segunda, inclusive, os CEOs de todo o mundo apontam as ameaças cibernéticas como um dos maiores riscos para seus negócios. Nos Estados Unidos, os participantes vão além, classificando as ameaças cibernéticas como sua maior preocupação geral, à frente do excesso de regulamentação, da incerteza geopolítica e do terrorismo. O *Relatório de Riscos Globais* 2018 do Fórum Econômico Mundial classifica tanto os ataques cibernéticos em larga escala quanto as grandes violações de dados ou fraudes entre os cinco principais riscos mais prováveis na próxima década.[2]

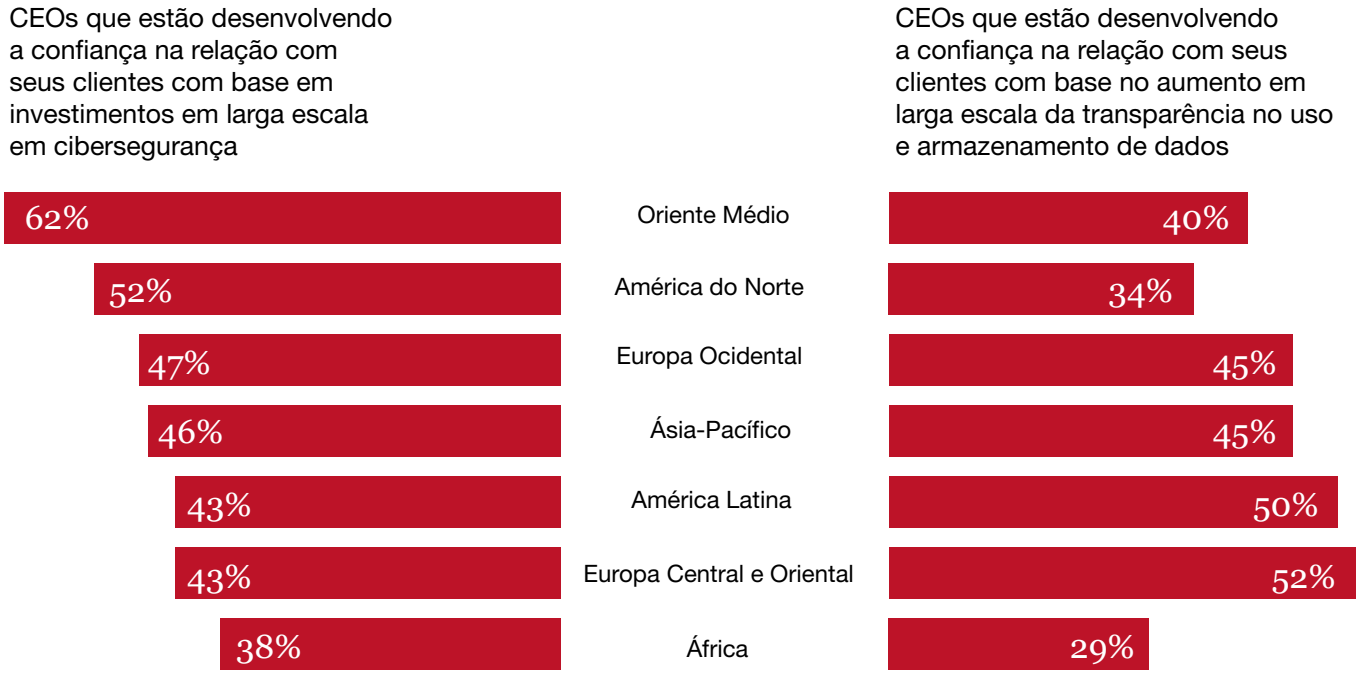
Mas há motivos para otimismo. Por exemplo, 87% dos CEOs globais afirmam que estão investindo em segurança cibernética para desenvolver a confiança na relação com os clientes. Quase o mesmo percentual (81%) diz que está dando mais transparência ao uso e armazenamento de dados. Será suficiente? Infelizmente, menos da metade dos CEOs diz estar adotando essas medidas "em larga escala".[3] Além disso, um terço dos CEOs africanos e quase um quarto dos CEOs norte-americanos (22%) dizem que "não estão" dando mais transparência ao uso e armazenamento de dados.

44% ***afirmam estar dando mais transparência ao uso e armazenamento de dados em larga escala.***

Fonte: PwC, "21ª Pesquisa Anual Global com CEOs", janeiro/2018.
Base: 1.293 participantes

[1] PwC, "21ª Pesquisa Anual Global com CEOs", janeiro/2018.
[2] World Economic Forum, "Relatório de Riscos Globais 2018", janeiro/2018.
[3] 47% dos CEOs globais afirmam estar investindo em cibersegurança em larga escala, enquanto 44% dizem estar dando mais transparência, em larga escala, ao uso e armazenamento de dados.

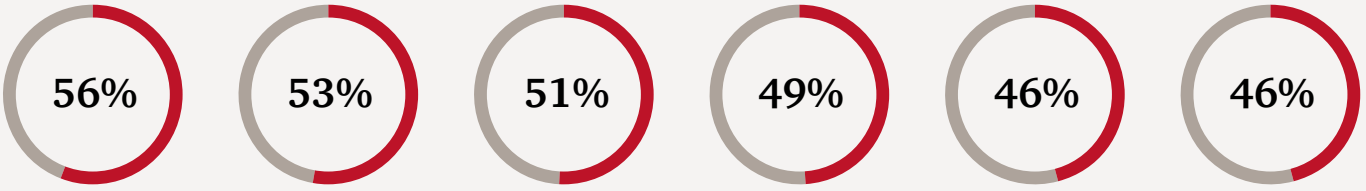
CEOs no mundo todo ainda têm como progredir em termos de cibersegurança e privacidade



Fonte: PwC, "21ª Pesquisa Anual Global com CEOs", janeiro/2018
Base: Oriente Médio (52), América do Norte (148), Europa Ocidental (274), Ásia-Pacífico (464), América Latina (136), Europa Central e Oriental (139) e África (80)

Muitas empresas estão apenas começando a adotar a governança no uso dos dados

Somente metade dos participantes já colocou em prática medidas essenciais



2. Comprometer-se com o gerenciamento de riscos na transformação digital é uma questão de sobrevivência

As tecnologias digitais estão mudando a maneira como a sociedade consome, transaciona, interage, se organiza e trabalha em uma escala que as métricas atuais não conseguem capturar completamente.[4] A quantidade estimada de dados que serão criados e copiados anualmente em 2025 é incalculável.[5] No entanto, os resultados da GSISS 2018, baseados nas respostas de 9.500 executivos de 122 países, mostram que muitas empresas ainda estão apenas começando a adotar a governança no uso de dados.

Reforçar a segurança cibernética "em todos os níveis – desde os que envolvem a coleta de dados até os que compreendem a transmissão, o processamento, o armazenamento e o uso – será crucial" para proteger os dados pessoais, de acordo com o Centro Europeu de Estratégia Política da Comissão Europeia.[6] No entanto, 44% dos participantes da GSISS 2018 dizem não ter uma estratégia geral de segurança da informação.[7] E os executivos estão preocupados com a escassez de competências em segurança cibernética e privacidade, como revela o nosso relatório da *Global Digital IQ® Survey 2017*.[8]

No mundo atual, o velho hábito de perseguir a inovação tecnológica antes de pensar nos problemas e riscos que ela traz pode ter consequências sem precedentes para as organizações. "Poucas empresas estão adotando corretamente o gerenciamento de riscos cibernéticos e de privacidade em sua transformação digital", diz Eduardo Batista, sócio de Segurança cibernética e privacidade de dados da PwC Brasil. "Os vencedores serão os que realizarem esse gerenciamento desde a fase da concepção até a produção. É uma oportunidade que define a marca."

"Poucas empresas estão adotando corretamente o gerenciamento de riscos cibernéticos e de privacidade em sua transformação digital", diz Eduardo Batista, sócio de Segurança cibernética e privacidade de dados da PwC Brasil.

[4] Departamento de Comércio dos EUA, "First Report of the Digital Economy Board of Advisors", dezembro/2016.
[5] The Economist, "Data is giving rise to a new economy", 6/5/2017. O artigo contém uma previsão de uma entidade de pesquisa de mercado (IDC) segundo a qual os dados criados e copiados anualmente alcançarão 180 zettabytes (180 seguido de 21 zeros) em 2025.
[6] European Political Strategy Centre, "Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level", maio/2017.
[7] PwC, "Strengthening digital society against cyber shocks", 18/10/2017.
[8] PwC, "2017 Global Digital IQ® Survey", fevereiro/2017.

3. As expectativas de privacidade se concentram não só na confidencialidade, mas também no uso de dados

Com as ameaças crescentes à confidencialidade, a privacidade de dados está mais focada em controlar como os dados são usados, enquanto a segurança cibernética se concentra mais na prevenção da manipulação e destruição de dados que poderiam minar os sistemas confiáveis.[9] A iniciativa *Sheltered Harbor*, por exemplo, desenvolveu padrões para ajudar os bancos a recuperar e restaurar os dados de contas no caso de um grande ataque cibernético.[10]

Os consumidores, no entanto, confiam relativamente pouco que as empresas usarão dados pessoais de forma responsável. Na pesquisa *Consumer Intelligence* 2017 da PwC, apenas 25% dos consumidores disseram acreditar que a maioria das empresas lida com dados pessoais de forma responsável.[11] O risco de uso indevido de dados pessoais é a maior preocupação dos europeus em relação aos serviços bancários *on-line* e ao *e-commerce*, segundo uma pesquisa de opinião sobre segurança cibernética realizada na União Europeia em 2017.[12]

As metas do Instituto Nacional de Padrões e Tecnologia dos EUA para a engenharia de privacidade – um ramo novo da engenharia de sistemas focado no desenvolvimento de soluções de privacidade – incluíam inicialmente a confidencialidade.[13] Mas essa meta logo mudou para "dissociabilidade" – permitir transações não associadas à identidade de uma pessoa – o que está relacionado à criptografia e ao princípio da minimização de dados.[14] A Regulação Geral de Proteção de Dados (GDPR, na sigla em inglês) da União Europeia exige privacidade desde a concepção, incluindo a minimização de dados, e diz que as empresas podem usar pseudônimos ou criptografar dados pessoais. Tudo isso reafirma a necessidade da governança corporativa na gestão, na proteção e no uso de dados.

Na pesquisa* Consumer Intelligence 2017 *da PwC, apenas

25%

dos consumidores disseram acreditar que a maioria das empresas lida com dados pessoais de forma responsável.

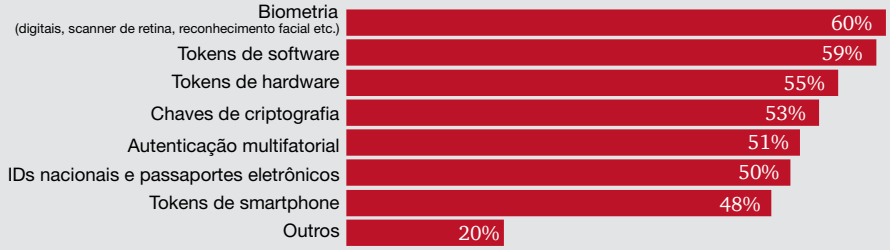
[9] Dan Geer, palestra de encerramento da SOURCE, Boston, 27/4/2017. Na palestra, ele afirma: "Da tríade clássica de confidencialidade, integridade e disponibilidade, até agora, nós priorizamos a confidencialidade, especialmente no setor militar. Não será assim daqui para frente. No setor civil, a integridade substituirá a confidencialidade como o principal objetivo da segurança cibernética. No setor militar, as armas contra a integridade já superam as armas contra a confidencialidade".
[10] PwC, "Strengthening digital society against cyber shocks", 18/10/2017.
[11] PwC, "Consumer Intelligence Series: Protect.me", novembro/2017.
[12] Comissão Europeia, "Special Eurobarometer 464a: Europeans' attitudes towards cyber security", setembro/2017.
[13] Inside Cybersecurity, "NIST's draft privacy-engineering concepts avoid defining privacy", 3/10/2014.
[14] NIST Interagency/Internal Report (NISTIR) - 8062, "An Introduction to Privacy Engineering and Risk Management in Federal Information Systems", janeiro/2017. As duas outras metas são previsibilidade e gerenciabilidade.

4. A tecnologia de autenticação avançada contribuirá para promover a confiança

Na GSISS 2018, metade dos entrevistados afirmou que o uso de autenticação avançada melhorou a confiança dos clientes e parceiros de negócios nos recursos de segurança e privacidade das informações da organização.

Em julho de 2017, a cúpula do G20 enfatizou a necessidade de "confiança nas tecnologias digitais".[15] Esperamos que melhorias que estão sendo feitas na tecnologia de autenticação, incluindo a biometria e a criptografia, ajudem cada vez mais os líderes empresariais a construir redes confiáveis. Na GSISS 2018, metade dos entrevistados afirmou que o uso de autenticação avançada melhorou a confiança dos clientes e parceiros de negócios nos recursos de segurança e privacidade das informações da organização. Além disso, 48% dizem que a autenticação avançada ajudou a reduzir fraudes, enquanto 41% afirmam que melhorou a experiência do cliente. Além disso, 46% planejam aumentar o investimento em biometria e autenticação avançada este ano. O simples uso da biometria, no entanto, cria uma autoexposição à regulamentação da privacidade e à preocupação dos cidadãos com o rastreamento de informações biométricas. E confiar na autenticação baseada em informações – quando os usuários fornecem o nome de solteira de uma mãe, por exemplo – pode deixar uma organização vulnerável a ataques, caso as informações sejam roubadas em uma violação separada.[16]

Empresas estão adotando tecnologias de autenticação avançadas



Fonte: PwC, CIO e CSO. "Global State of Information Security® Survey (GSISS) 2018"
Base: 9.500 participantes

Também esperamos uma pressão crescente sobre a indústria para criptografar dados como forma de protegê-los, o que impulsionará investimentos relacionados. Entre os participantes do setor financeiro, 46% dizem que planejam aumentar investimentos em criptografia este ano.

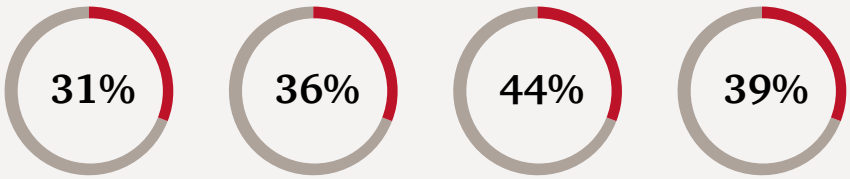
[15] Declaração dos líderes do G20, "Shaping an interconnected world", julho/2017.
[16] PwC, "2018 Global Economic Crime and Fraud Survey", fevereiro/2018. Prevê que o cibercrime será a fraude mais perturbadora para as organizações nos próximos 24 meses.

5. Mesmo os gigantes da indústria devem ampliar o envolvimento da alta administração, do conselho e dos comitês

Organizações de todos os tamanhos devem aumentar o engajamento da alta administração e dos conselhos e comitês corporativos na supervisão do gerenciamento de riscos cibernéticos e de privacidade. Menos de um terço dos participantes da GSISS 2018 afirma que a alta administração participa diretamente de uma avaliação dos riscos atuais de segurança e privacidade. Para organizações com valor superior a US$ 25 bilhões, esse percentual é apenas um pouco maior. Sem uma sólida compreensão dos riscos, os conselhos não estarão bem posicionados para exercer suas responsabilidades de supervisão dos temas de proteção de dados e privacidade.

Além disso, a maioria dos conselheiros de administração dos EUA não confia muito que o programa de privacidade e segurança de dados de suas empresas seja abrangente e que a empresa tenha identificado seus ativos digitais mais valiosos e sensíveis, segundo nossa 2017 *Annual Corporate Directors Survey*.[17]

Envolvimento do conselho tem muito espaço para crescer



afirmam que o conselho de administração participa diretamente da avaliação dos riscos atuais de segurança e privacidade*	das organizações com valor acima de US$ 25 bilhões dizem que seu conselho de administração participa diretamente da avaliação dos riscos atuais de segurança e privacidade**	dos conselheiros confiam muito que suas organizações têm um programa abrangente para questões de segurança de dados e privacidade***	confiam muito que suas organizações tenham identificado seus ativos digitais mais valiosos e sensíveis***

* Fonte: PwC, CIO e CSO. "Global State of Information Security® Survey (GSISS) 2018"
Base: 9.500 participantes
** Base: 435 participantes
*** Fonte: PwC, "2017 Annual Corporate Directors Survey"
Base: 842-849 participantes

[17] PwC, "2017 Annual Corporate Directors Survey", outubro/2017.

6. Mais empresas devem avaliar a contratação de um Chief Privacy Officer (CPO)

2/3

dos participantes dizem que suas organizações contrataram um diretor de Privacidade (CPO) ou executivo similar responsável pelo tema.

Fonte: PwC, CIO e CSO, "The Global State of Information Security® Survey 2018", 18/10/2017
Base: 9.500 participantes

Cerca de dois terços dos participantes em todo o mundo dizem que suas organizações contrataram um diretor de Privacidade (CPO) ou executivo similar responsável pelo tema.

Isso é ainda mais comum entre as organizações maiores. Entre as instituições avaliadas em mais de US$ 10 bilhões, pelo menos 79% dos participantes dizem que suas organizações têm esse cargo executivo. Para organizações com valor entre US$ 15 bilhões e US$ 25 bilhões, o percentual é de 81%.

As organizações com valor acima de US$ 25 bilhões parecem apresentar desempenho superior às outras em relação a: adoção de limites na coleta, retenção e acesso de dados; manutenção de um inventário de dados preciso; exigência de treinamento em políticas e práticas de privacidade; realização de auditorias de conformidade de terceiros; e exigência de que terceiros cumpram as políticas de privacidade. No entanto, um terço dos participantes das organizações com mais recursos afirma que ainda precisa realizar essas ações importantes.

Empresas com valor acima de US$ 25 bilhões estão à frente na governança do uso de dados

Mas um terço dessas gigantes ainda não adotou medidas essenciais.

*Fonte: PwC, CIO e CSO. "Global State of Information Security® Survey (GSISS) 2018"
Base: 9.500 participantes

7. Empresas retardatárias na Europa e no Oriente Médio têm mais trabalho a fazer

As empresas da Europa e do Oriente Médio, no geral, estão aquém das de Ásia, América do Norte e América do Sul no desenvolvimento de uma estratégia geral de segurança da informação e na implementação de práticas de governança de uso de dados, de acordo com a GSISS 2018.[18] Os dados confirmam a conclusão do European Political Strategy Centre de que a Europa está "insuficientemente preparada" para os riscos cibernéticos[19] e uma revelação anterior da PwC de que as empresas do Oriente Médio geralmente têm uma "falsa sensação" de segurança cibernética.[20]

Rankings regionais mostram que Ásia e América do Norte lideram em práticas essenciais

Fonte: PwC, CIO e CSO. "Global State of Information Security® Survey (GSISS) 2018"
Base: América do Norte (3.175), América do Sul (1.261), Europa (2.416), Ásia (1.581), Oriente Médio (94).

[18] No entanto, 64% dos participantes do Reino Unido dizem ter uma estratégia geral de segurança da informação. Além disso, entre os participantes britânicos, os percentuais de adoção de medidas de governança de uso de dados se comparam favoravelmente aos resultados de organizações em todo o mundo. Por exemplo, 60% dos participantes do Reino Unido dizem ter um inventário de dados preciso.
[19] European Political Strategy Centre, "Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level", maio/2017.
[20] PwC, "A false sense of security? Cybersecurity in the Middle East", março/2016. A GDPR da União Europeia, aplicável a qualquer organização que atue na UE, entrou em vigor em 25 de maio de 2018.

A GDPR, aplicável a qualquer organização que atue na UE, entrou em vigor em 25 de maio de 2018. Alguns participantes da GSISS 2018 diziam estar se preparando para a GDPR desde maio de 2017. Cerca de um terço deles, por exemplo, iniciou uma avaliação para a GDPR. O número foi um pouco maior na Ásia (37%) do que em outros continentes. Em nossa mais recente edição da *GDPR Pulse Survey*, realizada com 300 executivos de empresas dos EUA, Reino Unido e Japão, a maioria dos participantes disse que os preparativos para a GDPR estavam ainda nas fases de avaliação e operacionalização, o que sugere poucos progressos nessas regiões.[21]

A Diretiva da UE sobre Segurança de Redes e Sistemas de Informação (diretiva NIS), que visa aumentar a resiliência cibernética, também entrou em vigor em maio de 2018. Empresas identificadas pelos estados membros da UE como operadoras de serviços essenciais (infraestrutura crítica) e provedoras de serviços digitais (mecanismos de busca, serviços de computação em nuvem e mercados *on-line*) precisam cumprir novos requisitos relacionados à diretiva de segurança e relatar incidentes às autoridades nacionais.

Assim como ocorre com a GDPR, as empresas podem enfrentar sérias consequências por não conformidade.[22] "Os CEOs devem ver a GDPR e a diretiva NIS não como exercícios de conformidade, mas como oportunidades estratégicas para promover o sucesso dos seus negócios em um mundo orientado por dados", diz Edgar D'Andrea, sócio e líder de Segurança Cibernética e Privacidade da PwC Brasil. "Além disso, as empresas devem procurar os reguladores para desenvolver relacionamentos e canais de comunicação antes do encerramento dos prazos de conformidade".

32%

afirmam ter iniciado uma avaliação para a GDPR em maio de 2017.

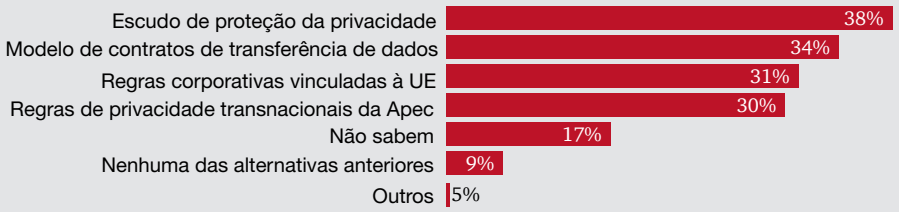
Fonte: PwC, CIO e CSO, "The Global State of Information Security® Survey 2018", 18/10/2017
Base: 9.500 participantes

[21] PwC, "Corporate GDPR preparations to stretch past May 2018", fevereiro/2018.
[22] Press release do governo do Reino Unido, "Government acts to protect essential services from cyber attack: Britain's most critical industries are being warned to boost cyber security or face hefty fines", janeiro/2018.

8. A balcanização da Internet vai mudar a forma como as empresas fazem negócios

A maneira como as empresas lidam com a GDPR e outras regulamentações, como a nova Lei de Segurança Cibernética da China e a Lei de Privacidade da Rússia, pode ter implicações de longo prazo. Segundo uma recente previsão do US National Intelligence Council, a crescente dependência mundial de dados "exigirá a fixação de limites e padrões claros sobre propriedade, proteção e privacidade de dados, fluxos de dados transnacionais e segurança cibernética que podem se tornar aspectos cada vez mais importantes de conflitos políticos domésticos e internacionais".[23] E o aumento da regulamentação nessa área é mais do que provável.

Quais abordagens as organizações estão adotando para o fluxo transnacional de dados



Fonte: PwC, CIO e CSO. "Global State of Information Security® Survey (GSISS) 2018"
Base: 9.500 participantes

Países como a China começaram a exigir que as empresas mantenham software de dados e aplicativos dentro dos limites geográficos em que estão operando.[24] A balcanização da Internet mudará a forma como as empresas fazem negócios. Isso provavelmente reduzirá a eficiência e, de modo mais amplo, terá algum efeito na economia global. Novas abordagens para os fluxos de dados transnacionais, novas regras de privacidade e a ampliação da regulamentação sobre o uso de dados em todo o mundo se somam para criar um caminho cada vez mais desafiador para as empresas alcançarem o sucesso na economia digital global.

"As empresas devem observar não apenas as leis que estão surgindo, mas também as diretrizes de implementação a elas relacionadas, que podem diferir de maneiras importantes", diz Maressa Juricic, líder de Privacidade de dados da PwC. "Por exemplo, as orientações preliminares (abril de 2017) sobre o fluxo transnacional de dados relacionadas à Lei de Cibersegurança da China incluíam chamadas em novos em idiomas como uma exigência para todas as operadoras de rede".

[23] US National Intelligence Council, "Global Trends: Paradox of Progress", janeiro/2017. Também segundo a publicação, "pressões conflitantes para equilibrar a privacidade com interesses de segurança terão consequências de longo alcance para a governança, a competitividade econômica e a coesão social".
[24] PwC, "Top Policy Trends of 2018", janeiro/2018.

9. O "bolso" pesará na escolha do consumidor pela inovação responsável e pelo uso consciente de dados

Os dados estão impulsionando a economia global de maneiras extraordinárias, capazes de transformar a sociedade e expandir a prosperidade. A tecnologia é parte da vida cotidiana e considerada útil por muitas pessoas. Em nossa pesquisa *US Consumer Intelligence Series de 2017*, os participantes identificaram os cenários futuros que considerariam mais aceitáveis. No topo da lista está o uso da tecnologia de GPS para permitir que os consumidores localizem dispositivos perdidos ou roubados. Em seguida, vem o uso de registros de saúde abrangentes para identificar uma enfermidade antes que os sintomas surjam e o uso da tecnologia da casa inteligente para controlar a temperatura e os sistemas elétricos a fim de economizar dinheiro e recursos na ausência dos moradores.

Os consumidores atribuem um valor monetário à privacidade – mas o contexto é importante. Pode parecer paradoxal que os consumidores demonstrem preocupação com a privacidade e continuem fornecendo dados *on-line*, mas isso não significa que eles não valorizem a privacidade, como observou Alessandro Acquisti, professor de Tecnologia da Informação e Políticas Públicas do H. John Heinz III College da Carnegie Mellon University, Privacy Retreat da PwC, realizado em 2017.[25] Segundo ele, a pesquisa sugere que as preferências de privacidade são moldadas pelo contexto, não são absolutas.

Em nossa pesquisa, os consumidores disseram que, entre as maiores ameaças à proteção da privacidade, estão os hackers e novas tecnologias como a inteligência artificial, a aprendizagem de máquina e a Internet das Coisas (IoT, na sigla em inglês).[26]

A PwC acredita que, em 2018, as organizações enfrentarão pressão crescente dos usuários finais e dos órgãos reguladores para implantar recursos de inteligência artificial (IA) que tomem decisões de maneira inteligível, transparente e matematicamente demonstrável.[27] Governança sólida e um novo modelo operacional podem ajudar a IA a atingir seu pleno potencial.[28] "A adoção de soluções de inteligência artificial pelo mercado dependerá do quanto o usuário final confiará que são eles mesmos – e não as máquinas – que controlam suas informações e suas escolhas de vida", afirma Eduardo Batista, sócio de Segurança cibernética e privacidade de dados da PwC.

Também acreditamos que os consumidores pagarão mais pelos produtos tecnológicos projetados com base em segurança e privacidade. Em uma pesquisa de opinião realizada em 2017 na União Europeia, a maioria dos participantes (61%) disse levar em conta os recursos de segurança e privacidade ao escolher um produto de tecnologia da informação, enquanto mais de um quarto deles (27%) afirmou que está disposto a pagar mais por melhores recursos de segurança e privacidade.[29] Os resultados exibidos para a última afirmação são muito mais elevados em alguns países da UE, segundo a pesquisa.[30] O interesse do consumidor na privacidade de dados está crescendo na China.[31] Além disso, em uma pesquisa da PwC de 2017, 75% dos consumidores dos EUA disseram estar dispostos a pagar mais por segurança adicional nos dispositivos para a casa inteligente – se tivessem escolha.[32] Entretanto, os consumidores geralmente não têm essa opção, porque muitos dispositivos IoT são produzidos de maneira barata, com praticamente nenhuma proteção de segurança ou privacidade. Isso precisa mudar.

[25] PwC, "What CEOs need to know about privacy ethics, economics and risks", 2018.
[26] PwC, "Consumer Intelligence Series: Protect.me", novembro/2017.
[27] PwC, "2018 AI predictions", janeiro/2018.
[28] PwC, "Accelerating innovation: How to build trust and confidence in AI", 2017.
[29] Comissão Europeia, Special Eurobarometer 460, "Attitudes towards the impact of digitisation and automation on daily life", maio/2017.
[30] A porcentagem que diz que pagaria mais é ainda maior na Dinamarca (44%), Alemanha (43%), Irlanda e Chipre (ambos com 37%) e Reino Unido (36%), entre outros países da UE, segundo a mesmo pesquisa.
[31] The Economist, "In China, consumers are becoming more anxious about data privacy", janeiro/2018.
[32] PwC, "Smart home, seamless life: Unlocking a culture of convenience", janeiro/2017.

Próximos passos para os líderes de negócios globais

A diretoria executiva precisa gerenciar o risco digital: segurança cibernética, privacidade de dados e confiança na marca estão cada vez mais interligadas dentro e fora da organização. Os CEOs precisam liderar e não simplesmente delegar questões de proteção e privacidade de dados a terceiros que não são totalmente responsáveis por conduzir os negócios e definir o apetite a riscos. Para apoiar as decisões do CEO, o diretor de privacidade deve ser envolvido. Além disso, deve ser uma prioridade aumentar a comunicação com o conselho e seus comitês sobre essas questões. Os CEOs precisam liderar o desenvolvimento da resiliência necessária para manter as operações no caso de ataques cibernéticos disruptivos. A atualização das estratégias de continuidade de negócios, por exemplo, é importante para manter o acesso a dados precisos em uma crise. As organizações também devem se basear nos princípios de resiliência cibernética do Fórum Econômico Mundial.[33]

Envolva o conselho: os conselhos como um todo, não apenas seus membros individuais, precisam se municiar continuamente de conhecimentos melhores sobre os planos da diretoria executiva para abordar os novos riscos de proteção de dados e privacidade. Isso exige um comprometimento permanente com a educação do conselho. Nossas publicações *How your board can be effective in overseeing cyber risk* e *Five questions boards should ask about data privacy* podem ser um ponto de partida. Por exemplo, mais conselhos devem se perguntar se os planos de suas empresas para adoção de novas tecnologias e análise de dados estão em sintonia com os novos regulamentos globais de privacidade.

Priorize a governança do uso de dados: o uso de dados de formas mais inovadoras leva a mais oportunidades e mais riscos. As empresas devem equilibrar o uso de dados com fortes controles de proteção e detecção. Compreender os riscos mais comuns – incluindo a falta de consciência sobre atividades de coleta e retenção de dados, por exemplo – é um ponto de partida para desenvolver uma estrutura de governança de uso de dados. Para mais informações, consulte *Monetizing data while respecting privacy, Responsibly leveraging data in the marketplace* e *Strategically managing emerging cyber risks*.

[33] WEF, "Advancing Cyber Resilience: Principles and Tools for Boards", 18/1/2017.

Encare a GDPR como uma oportunidade: Os líderes de negócios devem encarar a GDPR não apenas como uma exigência, mas também como uma oportunidade de promover o sucesso de suas organizações, de gerenciar riscos estrategicamente. As empresas devem tomar a iniciativa de se relacionar com os reguladores europeus e manter o foco nesse tema mesmo após o prazo de conformidade, porque a fiscalização talvez não atinja o seu auge este ano. É importante ter em mente também que escritórios de advocacia ambiciosos podem atuar como verdadeiros fiscalizadores ao perseguirem litígios relacionados à GDPR nos tribunais. Para mais informações, consulte nosso site.[34]

Avalie os riscos da regulamentação no exterior em um contexto estratégico: a balcanização da Internet pode levar mais empresas a sofrer pressões de governos estrangeiros para fornecerem acesso a ativos de propriedade intelectual sensíveis, como códigos-fonte. As decisões sobre como responder a essas pressões devem ser fundamentadas nos riscos cibernéticos, de privacidade e de confiança associados à divulgação dessas informações confidenciais a autoridades governamentais estrangeiras.

Defender a inovação responsável: a indústria deve apoiar e participar do desenvolvimento de novos padrões e dos esforços incipientes para estabelecer laços entre os profissionais de privacidade e tecnologia,[35] pois eles podem ajudar a colocar em prática os princípios de privacidade e fornecer aos consumidores dispositivos mais inteligentes projetados com base na segurança cibernética e na privacidade. Além disso, ao incorporar a gestão de riscos cibernéticos e de privacidade aos esforços de transformação digital, os líderes corporativos podem preparar melhor suas organizações para resistir a ameaças cibernéticas disruptivas, manter as operações, fortalecer a marca e os negócios, desenvolver a confiança dos consumidores e obter vantagem competitiva.

Acreditamos que as empresas que aproveitam essa oportunidade para gerenciar a proteção de dados e os riscos à privacidade estão mais bem posicionadas para prosperar na economia baseada em dados e desenvolver a resiliência da sociedade digital. Já as empresas que se apressam em se transformar digitalmente sem desenvolver a segurança e a privacidade estão no caminho da obsolescência. No próximo artigo sobre as principais conclusões da nossa *Global State of Information Security® Survey* 2018, abordaremos temas relacionados ao futuro da segurança cibernética.

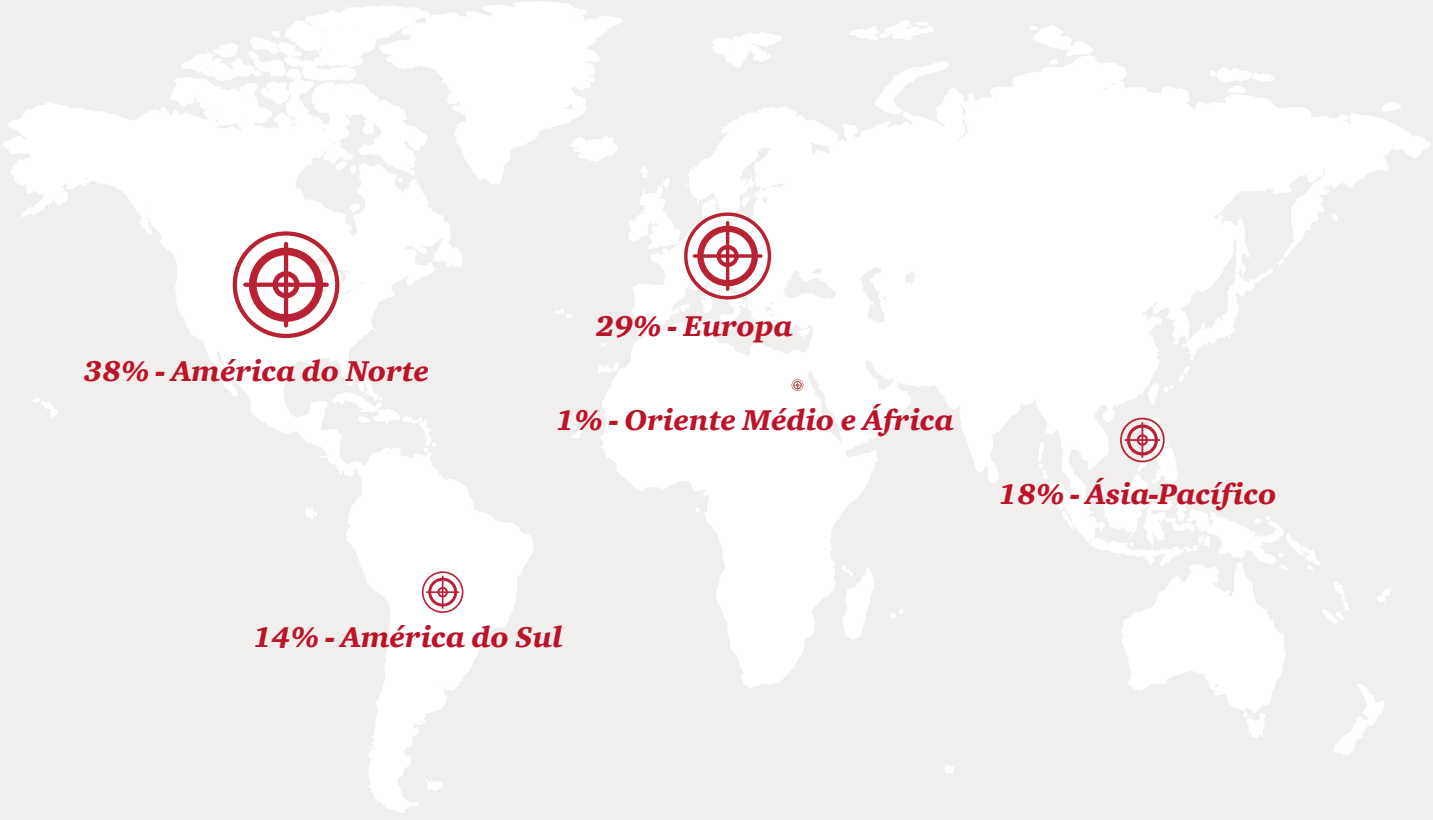
[34] https://www.pwc.com.br/pt/consultoria-negocios/tecnologia-da-informacao/general-data-protection-regulation.html
[35] NIST, "Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1", 5/12/2017. Inclui uma seção sobre engenharia de privacidade.

Metodologia

A *Global State of Information Security® Survey* 2018 é um estudo global da PwC, da CIO e da CSO. Ela foi realizada *on-line* entre 24 de abril e 26 de maio de 2017. Leitores da CIO e da CSO e clientes da PwC em todo o mundo foram convidados a participar por e-mail.

Os resultados apresentados neste relatório se baseiam nas respostas de mais de 9,5 mil CEOs, CFOs, CIOs, CSOs, CISOs, VPs e diretores de TI e de práticas de segurança de mais de 122 países.

Do total, 38% dos participantes são da América do Norte, 29% da Europa, 18% da região Ásia-Pacífico, 14% da América do Sul e 1% do Oriente Médio e da África.



A margem de erro é inferior a 1%; os totais podem não somar 100% por questões de arredondamento. Todos os números e gráficos deste relatório têm como fonte os resultados da pesquisa.

Contatos da PwC Brasil para cibersegurança e privacidade

Edgar D'Andrea
Sócio e líder de
Segurança Cibernética e Privacidade
+55 (11) 3674 3826
edgar.dandrea@pwc.com

Eduardo Batista
Sócio de Segurança Cibernética
e Privacidade
+55 (11) 3674 3843
eduardo.batista@pwc.com

Escritórios

São Paulo - SP
Av. Francisco Matarazzo, 1400
Torre Torino, Água Branca
São Paulo, SP, 05001-903
T: +55 (11) 3674 2000

Barueri - SP
Al. Mamoré, 989, 21º, 22º e 23º
Cond. Edifício Crystal Tower
Barueri, SP, 06454-040
T: +55 (11) 3674 2000

Belo Horizonte - MG
Rua dos Inconfidentes, 911, 18º e 17º
Bairro Funcionários
Belo Horizonte, MG, 30140-128
T: +55 (31) 3269 1500

Brasília - DF
SHS, Quadra 6, Conj. A, Bl. C
Ed. Business Center Tower
Salas 801 a 811
Brasília, DF, 70322-915,
Caixa Postal 08850
T: +55 (61) 2196 1800

Campinas - SP
R. José Pires Neto, 314, 10º
Campinas, SP, 13025-170
T: +55 (19) 3794 5400

Cuiabá - MT
Av. Doutor Hélio Ribeiro, 525
Ed. Helbor Dual Business Office & Corporate
Salas 1510 a 1513, Alvorada
Cuiabá, MT, 78048-250
T: +55 (65) 3641 8979

Curitiba - PR
Al. Dr. Carlos de Carvalho, 417, 10º
Curitiba Trade Center
Curitiba, PR, 80410-180
T: +55 (41) 3883 1600

Florianópolis - SC
Av. Rio Branco, 847
Salas 401, 402, 403 e 409
Florianópolis, SC, 88015-205
T: +55 (48) 3212 0200

Goiânia - GO
Av. 136, 797, Setor Sul
Cond. New York Square
Business Evolution
Salas 1005, 1006, 1007 e 1008 A
Goiânia, GO, 74093-250
T: +55 (62) 3270 5900

Maringá - PR
Av. Pedro Taques, 294, 10º, Zona 3
Ed. Átrium, Centro Empresarial
Maringá, PR, 87030-000
T: +55 (44) 3472 2200

Porto Alegre - RS
R. Mostardeiro, 800, 8º e 9º
Ed. Madison Center
Porto Alegre, RS, 90430-000
T: +55 (51) 3378 1700

Recife - PE
R. Padre Carapuceiro, 733, 8º
Ed. Empresarial Center
Recife, PE, 51020-280
T: +55 (81) 3464 5000

Ribeirão Preto - SP
Av. Antônio Diederichsen, 400,
21º e 22º
Ed. Metropolitan Business Center
Ribeirão Preto, SP, 14020-250
T: +55 (16) 3516 6600

Rio de Janeiro - RJ
R. do Russel, 804, 6º e 7º
Ed. Manchete, Térreo
Rio de Janeiro, RJ, 22210-907
T: +55 (21) 3232 6112

Salvador - BA
Av. Tancredo Neves, 2539, 22º andar
Ed. CEO Salvador Shopping
Torre Nova Iorque
Salvador, BA, 41820-021
T: +55 (71) 3319-1900

São José dos Campos - SP
R. Carlos Maria Auricchio, 70, 14º
Ed. Royal Park
São José dos Campos, SP, 12246-876
T: +55 (12) 3519 3900

Sorocaba - SP
R. Eulália Silva, 454, 8º
Ed. Millenia, Cjs. 81 e 82
Sorocaba, SP, 18030-230
T: +55 (15) 3332 8080

PwC Brasil @PwCBrasil @PwCBrasil PwC Brasil PwC Brasil