iapp KPMG

PR!VACY R!SK STUDY 2023

Sumário Executivo

Outubro de 2023

Prefácio

O estudo Privacy Risk Study 2023 é o trabalho mais abrangente já realizado sobre riscos de privacidade pela IAPP, em colaboração com a KPMG.

Desde 2015, a IAPP publica anualmente o estudo Privacy Risk Study para determinar as principais tendências em gestão de riscos de privacidade em diversas regiões.

Em 2017, as análises do Formulário 10-K – relatório anual exigido pela Comissão de Valores Mobiliários dos EUA – foram introduzidas no Estudo para destacar o impacto das divulgações de riscos de privacidade a proporção em que as organizações detalham publicamente suas atividades de tratamento de dados pessoais e conformidade com leis e regulamentos.

Este ano, além de apenas utilizar as divulgações públicas, nós perguntamos a líderes seniores de privacidade para explicar as suas práticas utilizadas de gestão de riscos. Também destacamos os resultados das entrevistas conduzidas com os líderes seniores por meio de *workshops* e reuniões.

Constantes mudanças regulatórias no mundo inteiro, novas tecnologias (incluindo inteligência artificial) e incerteza de novas tendências amplifica o cenário de riscos de privacidade para as organizações.

Este estudo explora alguns dos principais desafios de privacidade enfrentados pelas organizações, e o que estas organizações estão fazendo para gerenciar seus riscos de privacidade. Nós acreditamos que este estudo pode ajudar a desenvolver um *roadmap* de gerenciamento e mitigação dos riscos de privacidade identificados.

Saz Kanthasamy
Pesquisador-líder de Privacy Management da IAPP

Sylvia Klasovec Kingsmill
Sócia-líder global de Cyber Privacy da KPMG no Canadá

Escopo

Nossa análise utiliza três conjuntos de dados:

1. *Workshops* realizados com líderes seniores em 2022. Nós pedimos aos participantes para listar, ranquear, categorizar e descrever seus riscos de privacidade para o ano. A informação foi então coletada e analisada para determinar o tipo dos riscos que estão “no radar” para os profissionais seniores de privacidade.

2. Entrevistas com lideranças de privacidade de 14 organizações diferentes e de diversos tamanhos. Os participantes representaram 6 diferentes setores e 3 continentes, sendo questionados sobre 4 diferentes pilares de privacidade. As respostas foram inseridas em uma matriz padronizada onde foi possível entender as tendências entre as organizações participantes.

3. Relatórios anuais, Formulários 10-K e outras divulgações disponíveis ao público referentes a 2022 e 2023.

Sumário executivo

A complexidade, variedade e escala pode variar entre as organizações, mas todas que realizam tratamento de dados pessoais enfrentam riscos de privacidade.

As organizações precisam encontrar maneiras de identificar, avaliar e tratar os riscos de privacidade, enfrentando fatores como: incerteza na capacidade de entregar um programa de conformidade em privacidade devido às constantes mudanças regulatórias, o desafio em manter a conformidade com diversas e até conflitantes leis de privacidade pelo mundo inteiro, ou até pela incerteza devido a incapacidade de prever tendências para o futuro.

Dessa forma, as organizações estão cada vez mais precisando lidar com um ambiente complexo de riscos de privacidade e repleto de incertezas econômicas e regulatórias. É um ambiente que contém ameaças novas e em evolução através das novas tecnologias, mudando as expectativas dos consumidores sobre os requisitos de privacidade e aumentando o nível de averiguação nas iniciativas de negócios e tendências de mercado.
No relatório deste ano, os líderes de privacidade identificaram a instabilidade política, a velocidade de amadurecimento de tecnologias emergentes, falta de talentos disponíveis e aumento das expectativas dos acionistas e órgãos reguladores como alguns dos principais desafios, revelando preocupações sobre um mundo cada vez mais fragmentado e imprevisível.

Neste contexto, identificamos que as organizações estão tomando medidas para gerenciar os riscos de privacidade considerando sua identificação, avaliação e tratamento, através de requisitos como: definição de papéis e resposabilidades, metodologias, tecnologias, meios de comunicação e melhoria contínua.

Principais tópicos:

• Os 5 domínios de risco de privacidade com maior prioridade identificados pelos participantes foram: vazamento de dados, tratamento de dados por terceiros em não conformidade, implementações inefetivas de *Privacy by Design*, gestão de dados pessoais de forma inapropriada e treinamentos de privacidade insuficientes para os colaboradores.

• O risco de privacidade mais comum e mais emergente identificado pelos participantes foi a dificuldade em manter a conformidade com diversos regulamentos, e seus requisitos divergentes e/ou em constante evolução.

• Riscos emergentes adicionais incluídos foram: equilibrar os requisitos de localização de dados com as necessidades de negócios da UE, consequências não planejadas devido à imaturidade no gerenciamento dos riscos de privacidade que ocorrem devivo ao uso de Inteligência Artificial e riscos de privacidade resultantes dos esforços em monetizar dados.

• Conformidade regulatória, gestão de dados e governança são os 3 principais domínios de riscos identificados pelos participantes.

21%

Apenas de 21% das organizações capacitaram a terceira linha de defesa para realizar auditorias de privacidade.

30%

Quase 30% das organizações utilizam planilhas para ajudar a gerenciar seus esforços direcionados à risco de privacidade.

50%

Apenas 50% das organizações estabeleceram seus critérios de tolerância ao risco.

64%

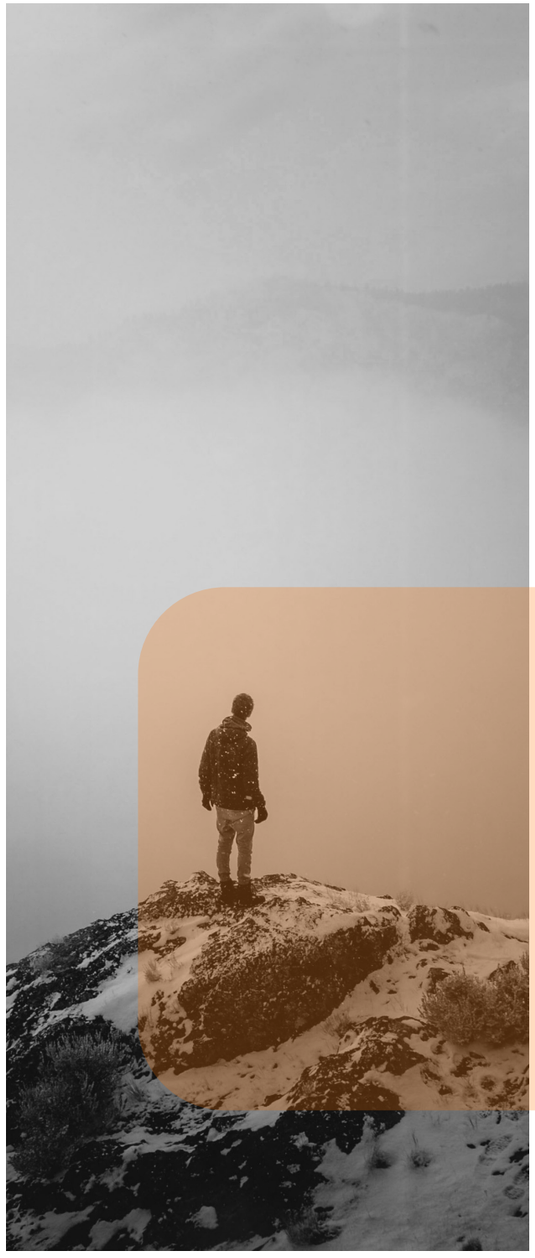
64% das organizações possuem um programa de gerenciamento de riscos de privacidade totalmente integrado ao seu programa de gerenciamento de riscos corporativos.

83%

83% das organizações reportam informações de risco de privacidade em seu relatório anual.

93%

Quase 93% das organizações indicaram que a privacidade é um dos 10 principais riscos organizacionais, e 36% classificaram entre os 5 principais riscos.



Fale com o nosso time

Leandro Augusto
Sócio-líder de Cyber Security & Privacy
da KPMG no Brasil e na América do Sul
lantonio@kpmg.com.br

Klaus Kiessling
Sócio de Cyber Security & Privacy
da KPMG no Brasil
kkiessling@kpmg.com.br

Marcos Fugita
Sócio-líder de Managed Risk e Security Services da
KPMG no Brasil
mfugita@kpmg.com.br

Thiago Labliuk Leme
Sócio-diretor de Managed Risk & Security Services
da KPMG no Brasil
tleme@kpmg.com.br

Follow the IAPP on social media

Published June 2023.