Gestão de Riscos de Terceiros: Tendências e Boas Práticas

Resultados da pesquisa EY Global Third-Party Risk Management 2023

Dezembro 2023

EY
Building a better working world

João Herculano

Sócio-líder de Consultoria de Riscos de Tecnologia e Gestão de Riscos de Terceiros na **EY**

Fernando Leitão

Director - Advisors Client Services, Cybersecurity da **Mastercard**

Márcia Bolesina

Sócia de Cybersecurity da **EY**

Marcio Kauffmann

Sócio de Consulting na **EY**

EY

Building a better working world

1

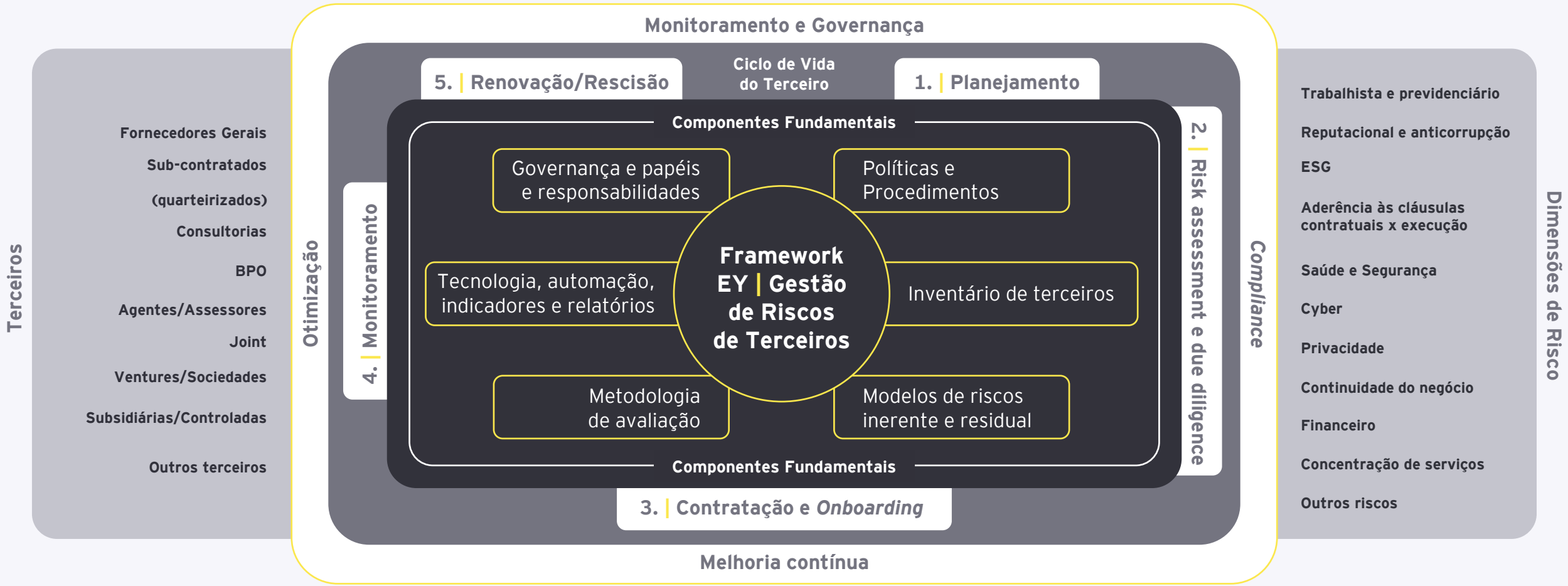
O que é **Gestão de Riscos de Terceiros (TPRM)?**

O **ecossistema das organizações** se tornou **complexo** e envolve **diversos fornecedores e parceiros** que desempenham **funções críticas de negócio** que precisam ser **gerenciadas**

Principais motivadores *(Pain Points)* para Gestão de Riscos de Terceiros (TPRM)

O que é Gestão de Riscos de Terceiros (TPRM)?

TPRM provê uma função para **identificar**, **avaliar**, **monitorar** e **gerenciar os riscos** associados com terceiros ***(ex: fornecedores, parceiros de negócio, quarteirizados)***



Entendendo o espectro de riscos de terceiros:

Diversos tipos de **riscos podem impactar uma organização** por meio de terceiros.

O **nível de exposição a esses riscos** é baseado na **natureza interconectada** entre as entidades dentro do **ecossistema de terceiros** de uma organização.

Geopolítico
Risco de fazer negócios em um país específico, inclui considerações legais, regulatórias, políticas e socioeconômicas

Qualidade e desempenho
Risco de que um terceiro não consiga atender às necessidades organizacionais sob a perspectiva de desempenho ou qualidade devido a deficiências nas operações do terceiro

Financeiro
Risco de que o terceiro não possa continuar a operar como uma entidade financeiramente viável

Digital
Risco associado aos processos de negócios digitais de terceiros

Continuidade de negócios
Risco de falha de terceiros na continuação do business as usual para a organização

Operacional
Risco de que um terceiro não consiga atender às necessidades organizacionais sob a perspectiva de entrega de serviços ou produtos devido a deficiências nas operações do terceiro

Concentração
Risco de que uma organização dependa de um fornecedor para realizar várias atividades críticas e/ou de alto risco para suas operações, ou risco de que os fornecedores estejam concentrados em determonadas localizações geográficas

Privacidade
Risco de que os dados de uma organização sejam perdidos ou comprometidos devido a deficiências nos controles de privacidade de terceiros (LGPD)

Regulamentação e conformidade
Risco de que um terceiro não cumpra uma regulamentação exigida, fazendo com que a organização fique fora de conformidade

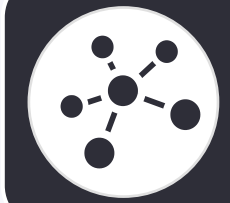
Quarteirização
Risco trabalhista e previdenciário para a organização devido à terceirização dentro dos terceiros da companhia

ESG
O risco de um terceiro não criar e aderir a uma estratégia de sustentabilidade ou não cumprir as normas ambientais

Segurança cibernética
Risco de que a segurança de uma organização seja comprometida devido a deficiências nos controles de segurança cibernética de terceiros

Third Party Cyber Risk Management (TPCRM)

Direcionadores



Crescente **interconexão com terceiros** (fornecedores, parceiros de negócios) e falta de centralização/supervisão

Obrigações regulatórias

Aumento das **ameaças cibernéticas** em termos de frequência, escala e sofisticação

O que é TPCRM

Supervisionar a **identificação**, **avaliação**, **monitoramento** e **tratamento de riscos associados a terceiros** (fornecedores, parceiros de negócios, joint ventures etc) e contratos relacionados, com foco específico em riscos cibernéticos.

Benefícios

Cumprimento de restrições regulatórias

Controle de riscos provenientes de novas tecnologias/modelos de negócios (por exemplo, vazamentos de dados e interrupções)

Visão holística dos riscos de terceiros, para apoiar a tomada de decisão e garantir a manutenção da confiança do mercado e dos clientes

Controle e mitigação de riscos cibernéticos, com foco na atualização dos padrões de segurança para reduzir a superfície de ataque

2

Pesquisa EY de **Gestão de Riscos de Terceiros** (TPRM)

Visão geral da pesquisa

A **EY**, em colaboração com a ***Oxford Economics***, buscou entender como as organizações lidam com a **gestão de riscos de terceiros** (TPRM) hoje.

As principais perguntas feitas nesta pesquisa incluíram:

- **Quais foram as principais mudanças na gestão de riscos de terceiros nos últimos três anos?**
- **Como os diferentes setores estão lidando com a necessidade constante de monitorar e antecipar riscos de terceiros?**
- **Quais são as melhores práticas para gerenciar riscos de terceiros?**

Dados demográficos dos entrevistados

- **N=500**; pesquisa com executivos que lideram ou auxiliam o programa de gestão de riscos de terceiros de suas organizações
- **$250m**+ de receita
- **17%** estão listados na Fortune 500
- Sediados nos EUA, Canadá, Reino Unido, França, Alemanha, Espanha, Itália, Países Nórdicos, Índia, China, Cingapura, Japão ou Austrália

Dados demográficos | Localização

- Onde é a matriz de sua organização?
- Qual a sua localização?

3

Principais mensagens

Uma infinidade de riscos - incluindo **sanções econômicas**, **reputacionais**, **cibernéticos** – impulsionam o **foco** e o **investimento**.

67% das organizações relataram uma **visibilidade crescente do TPRM** pelos executivos e conselhos.

50% tiveram pelo menos uma **interrupção causada por terceiros**.

90% das empresas estão investindo na **melhoria da eficácia de seu programa TPRM**.

As organizações esperam um aumento de **13 vezes** no uso de **dados de risco e *analytics*** até 2024.

71% das solicitações de avaliações de TPRM ainda são **tratadas por e-mail**.

Fonte: EY Global TPRM Survey, 2023

As empresas estão enfrentando um **conjunto de fatores de risco** de terceiros muito amplo.

Externo

- Aumento da dependência de terceiros, quarteirizados ou mais;
- Aumento dos ataques cibernéticos por meio de terceiros;
- Cenário regulatório em evolução (por exemplo, LGPD);
- Sustentabilidade e cidadania corporativa (por exemplo, ESG);
- Mídias digitais e sociais (por exemplo, influenciadores);
- Interrupções imprevistas (por exemplo, pandemia, terremoto);
- Pressões de custo e rentabilidade;
- Globalização.

Interno

- Evolução dos modelos operacionais e de negócios;
- Canais novos e mais complexos;
- Violações de dados/*ransomware;*
- Resiliência da cadeia de suprimentos e riscos reputacionais;
- Aumento dos custos com gestão de risco e conformidade;
- Apontamentos de auditoria ou de reguladores.

Centralização, **níveis de risco**, **tecnologia** e **apoio externo** são tentativas de **fortalecer o TPRM**.

90% das organizações estão migrando para o **gerenciamento centralizado de riscos**.

54% das organizações utilizam **gestão centralizada de riscos** e

36% utilizam uma **abordagem híbrida**.

As organizações de **serviços financeiros** são mais propensas a **utilizar uma estrutura de programa centralizada de TPRM** (**62%** em comparação com **46%** dos **serviços não financeiros**).

As organizações com **estruturas TPRM centralizadas** gerenciam quase **o dobro de terceiros de forma eficaz** do que suas contra-partes com **estruturas TPRM híbridas**.

Fonte: EY Global TPRM Survey, 2023

As organizações contam com **níveis de risco e tecnologia** para compreender melhor a **postura de risco de terceiros**.

À medida que as empresas se concentram na **sua própria resiliência**, a **resiliência dos seus terceiros** é uma **prioridade alta**.

Quase **metade** (**48%**) das organizações tem **estratégias de saída ou planos de contingência** para **terceiros de alto risco**. Isso significa que **mais da metade não está preparada**.

63% das organizações **planejam integrar provedores de dados externos e automação** para gerenciar melhor as **avaliações de riscos inerentes**.

A gestão de riscos de terceiros **aumenta a resiliência** e tem potencial para se tornar **uma ferramenta estratégica de negócios**.

Fonte: EY Global TPRM Survey, 2023

Dados demográficos | Responsabilidade pela TPRM

34% dos programas de TPRM continua a reportar para **Enterprise Risk Management**

27% das organizações tem a **função de TPRM** gerida por **áreas de Segurança da Informação** ou **Segurança Cibernética ou de Resiliência**.

Isso acontece porque a **segurança cibernética**, com **61%**, e o **risco digital**, com **43%**, são os domínios considerados **mais importantes nos relatórios de TPRM**.

Além do risco de privacidade aparecendo como o quinto domínio mais relevante com **39%**, já que **37%** das organizações definem terceiros como críticos com base na sensibilidade dos dados envolvidos.

Fonte: EY Global TPRM Survey, 2023

Riscos de Cibersegurança e Privacidade são frequentemente considerados ao **monitorar subcontratados** e **Terceiros Não Tradicionais**

As organizações levam em consideração o **risco cibernético** em **46%** dos casos, bem como o **risco de privacidade** é considerado em **38%**.

54% mencionam que **identificam**, **avaliam** e **monitoram** as **relações com subcontratados** por meio de **diligência de terceiros** (incluindo a validação de seu programa de TPRM e avaliação de risco ou controle de sua população de terceiros).

Fonte: EY Global TPRM Survey, 2023

A **tecnologia** e os **recursos digitais** estão sendo cada vez mais utilizados para **habilitar** e **automatizar** as **atividades de TPRM** em todas as organizações.

Tecnologia	Descrição	Capacidades
Tecnologia de governança, risco e conformidade (GRC)	Fornece uma visão holística do risco e da conformidade em toda a empresa, oferecendo suporte a vários recursos, incluindo gerenciamento de conformidade, gerenciamento de problemas, gerenciamento de riscos de terceiros, relatórios de risco e painéis de controle.	▸ Automatiza e padroniza as atividades de risco (por exemplo, gerenciamento de problemas, relatórios, avaliações) ▸ Serve como uma única "fonte de verdade" para informações de risco, controle e conformidade em toda a organização ▸ Permite a agregação e a comunicação de riscos em várias dimensões de risco (por exemplo, risco de terceiros, conformidade com políticas)
Automação robótica de processos (RPA)	Automação de tarefas frequentes, manuais e repetitivas por softwares configurados, a fim de reduzir custos, aumentar eficiências e reduzir erros humanos.	▸ Automatiza atividades de rotina (por exemplo, testes, revisões de evidências) ▸ Automatiza a revisão das respostas de terceiros a um questionário ou ao envio de evidências
Analytics e digital	Utilização de analytics para extrair e analisar dados a fim de identificar padrões e tendências; Uso de tecnologia para digitalizar atividades de risco e controle, inclusive melhorando a experiência do cliente.	▸ Permite a análise de grandes volumes de dados e riscos emergentes ▸ Facilita a tomada de decisões e a geração de relatórios ▸ Expande o acesso a insights de risco em toda a organização por meio de portais on-line
Fontes de dados externas	Fontes de dados fornecidas por fornecedores de fora do negócio para auxiliar na identificação, avaliação e monitoramento contínuo dos riscos dos fornecedores.	▸ Monitoramento contínuo de riscos como viabilidade financeira e riscos de segurança cibernética ▸ Integração com plataformas GRC (por exemplo, SAP Ariba) ▸ Identificar ameaças e tendências que as organizações enfrentam atualmente
Inteligência artificial (IA) e machine learning	Aprendizado de máquina que imita as capacidades cognitivas e de resolução de problemas humanos.	▸ Facilita o aprendizado não supervisionado em amplo acesso a dados

Perguntas sobre TPRM e pontos relevantes a serem considerados

1. Como identifico os contratos nos quais focar a avaliação de riscos?
2. Quem conduz o processo dentro da empresa?
3. Que tipo de processo é desencadeado caso um terceiro se recuse a aceitar contratualmente as medidas indicadas?
4. Até que ponto devo verificar meus terceiros?
5. Devo focar a análise nos serviços ou em terceiros?
6. Os terceiros estão preparados e estruturados para lidar com um modelo TPRM?
7. Posso contar apenas com a certificação como garantia de implementação dos requisitos necessários?
8. Por que e quando devo me munir de uma plataforma que automatize o processo TPRM?
9. Como devo gerenciar contratos ativos e novos contratos/renovações?
10. Qual é o valor acrescentado das ferramentas OSINT no contexto do TPRM?

Fonte: EY Global TPRM Survey, 2023

4

Q&A

EY

Construindo um mundo de trabalho melhor

Sobre a EY
A EY existe para construir um mundo de trabalho melhor, ajudando a criar valor de longo prazo para clientes, pessoas e sociedade e construir confiança no mercado de capitais.

Habilitadas por dados e tecnologia, diversas equipes da EY em mais de 150 países geram confiança por meio de garantias e ajudam os clientes a crescer, transformar e operar.

Trabalhando com garantia, consultoria, direito, estratégia, impostos e transações, as equipes da EY fazem perguntas melhores para encontrar novas respostas para os problemas complexos que o mundo enfrenta hoje.

EY refere-se à organização global, e pode referir-se a uma ou mais, das firmas-membro da Ernst & Young Global Limited, cada uma das quais é uma entidade legal separada. Ernst & Young Global Limited, uma empresa do Reino Unido limitada por garantia, não presta serviços a clientes. Informações sobre como a EY coleta e usa dados pessoais e uma descrição dos direitos que as pessoas têm sob a legislação de proteção de dados estão disponíveis através do ey.com/privacy. As firmas-membro da EY não exercem a advocacia quando proibidas pelas leis locais. Para mais informações sobre nossa organização, visite ey.com.

EYG nº 004253-23Gbl

ey.com