# INFORME DE BENCHMARKING DE TECNOLOGÍA ANTIFRAUDE 2024

ACFE
Association of Certified Fraud Examiners

sas

# ÍNDICE

Nueve de cada 10 organizaciones (91%) utiliza

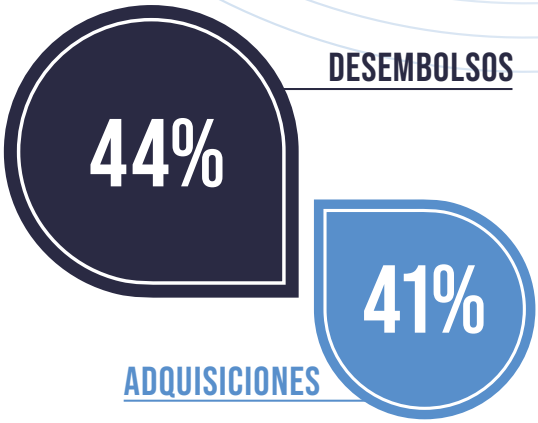
**TÉCNICAS DE ANÁLISIS DE DATOS**

como parte de sus programas antifraude.



**DATOS ESTRUCTURADOS INTERNAMENTE**

son la fuente más común para el análisis, y el 77% de las organizaciones confían en ese enfoque tradicional.



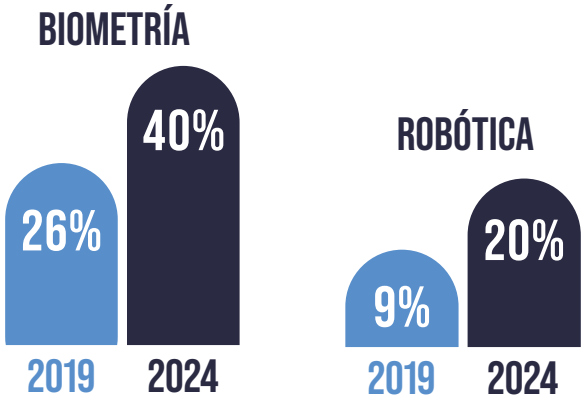

Las áreas de riesgo más comunes monitoreadas por la analítica de datos son

**DESEMBOLSOS (44%) y ADQUISICIONES (41%).**

El uso de

**BIOMETRÍA y ROBÓTICA**

en los programas antifraude ha aumentado constantemente durante los últimos años.




**Dos de cada cinco organizaciones (40%)** usa actualmente

**BIOMETRÍA FÍSICA**

como parte de su programa antifraude y **otro 17% espera adoptar esta tecnología** en los próximos dos años.

## EL USO DE INTELIGENCIA ARTIFICIAL (IA) y MACHINE LEARNING

**en programas antifraude,** aproximadamente

# TRIPLIQUE

durante los próximos dos años.

# 83%

de las organizaciones espera implementar

## IA GENERATIVA

como parte de sus programas antifraude durante los próximos dos años.

La mayoría de las organizaciones **(61%)** contribuyen actualmente o están dispuestas a **contribuir en consorcios de datos** para ayudar en sus esfuerzos antifraude.

**61%**
DE LAS ORGANIZACIONES

Tres de cada cinco organizaciones **(59%)** espera **aumentar sus presupuestos para tecnología antifraude** durante los próximos dos años.

**59%**
DE LAS ORGANIZACIONES

**82%**

## RESTRICCIONES PRESUPUESTARIAS O FINANCIERAS

son una de las principales preocupaciones al implementar nuevas tecnologías antifraude, lo cual representa un desafío importante o moderado para el **82%** de las organizaciones.

# MÁS DEL 50%

## DE LOS PROGRAMAS ANTIFRAUDE

utiliza actualmente o espera adoptar análisis de computer vision, robótica y biometría del comportamiento en algún momento en el futuro.

# INTRODUCCIÓN

En 2024, utilizar la tecnología como parte de un programa antifraude es una necesidad. Los perpetradores de fraudes buscan continuamente formas de explotar los avances tecnológicos y las debilidades humanas para llevar a cabo sus planes. Las organizaciones deben hacer uso de las herramientas más efectivas para protegerse de esas amenazas y eso, a menudo, significa implementar nuevos programas y capacitar a sus colaboradores para utilizarlos efectivamente.

Para comprender el modo como las organizaciones están abordando esa misión, el ACFE y SAS se han asociado para realizar una serie de estudios sobre el uso de tecnologías antifraude por organizaciones alrededor del mundo. Como continuidad de nuestros dos primeros informes publicados en 2019 y 2022, nuestro más reciente informe explora las tendencias en la adopción actual y esperada de la analítica tradicional, inteligencia artificial (IA) e IA generativa, herramientas de gestión de casos, biometría y una serie de otras tecnologías que pueden utilizarse para combatir los fraudes. Esperamos que los profesionales antifraude, la gestión organizacional y otros encuentren la información aquí disponible benéfica para comparar y evaluar la efectividad de su conjunto de herramientas antifraude y planificar futuros presupuestos y recursos relacionados con la tecnología.

# METODOLOGÍA

En octubre de 2023, enviamos una encuesta de 22 preguntas a 80,426 miembros de ACFE. Se les solicitó a los encuestados que proporcionaran información sobre el uso de diversas tecnologías por parte de sus organizaciones, y de sus iniciativas antifraude. Las respuestas de la encuesta se colectaron anónimamente. Recibimos 1,187 respuestas que se pudieron utilizar para los propósitos de este informe. Este informe proporciona un resumen de las respuestas de los encuestados a las preguntas de la encuesta, así como comentarios seleccionados indicados por los encuestados con relación a ciertos temas de la encuesta. (Para más información sobre los datos demográficos de los participantes, incluida la región geográfica y la industria, consulte la sección Datos Demográficos de los Encuestados en la página 29.)

El Informe de Benchmarking de Tecnología Antifraude 2024 se desarrolló en colaboración con SAS. Como parte de su apoyo a este proyecto, SAS ofrece acceso gratuito a un informe de SAS Visual Analytics, en el que usted puede explorar más a fondo los resultados de la encuesta con gráficos interactivos basados en varias categorías demográficas, incluyendo la industria y la región geográfica. Vea el informe de SAS Visual Analytics en **SAS.com/fraudsurvey**.

# COMO AS ORGANIZAÇÕES ESTÃO UTILIZANDO A ANÁLISE DE DADOS EM SUAS INICIATIVAS ANTIFRAUDE?

# QUAIS TÉCNICAS DE ANÁLISE DE DADOS AS ORGANIZAÇÕES UTILIZAM PARA COMBATER A FRAUDE?

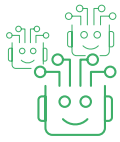
A capacidade de analisar eficazmente os dados em busca de sinais de alerta de fraude é crucial no kit de ferramentas de combate a fraude de uma organização. Mais de 90% das organizações em nosso estudo utilizam alguma forma de análise de dados como parte de seu programa antifraude. Conforme observado na Figura 1, as utilizações mais comuns da análise de fraudes são relatórios de exceções e detecção de anomalias (57% das organizações) e sinais de alerta automatizados e monitoramento de regras de negócios (54% das organizações).

Além disso, espera-se que todas as técnicas sobre as quais perguntamos sejam adotadas por mais organizações nos próximos um ou dois anos. A inteligência artificial (IA) e o machine learning têm a maior taxa de adoção prevista, com quase um terço das organizações que não usam a tecnologia atualmente esperando adicioná-la ao seu programa antifraude no futuro próximo. Isso significa que, até 2026, metade de todas as organizações espera utilizar IA e machine learning como parte de suas iniciativas de análise de fraude. Além disso, a taxa de adoção esperada de IA e machine learning aumentou desde o nosso estudo anterior, o que mostra um impulso crescente em torno dessas ferramentas; em 2022, 26% das organizações esperavam adotar essa tecnologia nos próximos dois anos, enquanto 32% das organizações em nosso estudo atual planejam implementar IA e machine learning nos próximos anos. A utilização de análise preditiva e modelagem também deve aumentar consideravelmente, com 22% das organizações planejando adotar essa tecnologia nos próximos dois anos.

Entretanto, apesar do aumento esperado na utilização de todas as técnicas de análise de dados, as taxas de adoção relatadas mostraram pouco crescimento desde 2019, destacando o ritmo lento com que as organizações conseguem implementar novas tecnologias.

**A UTILIZAÇÃO DE INTELIGÊNCIA ARTIFICIAL e MACHINE LEARNING**

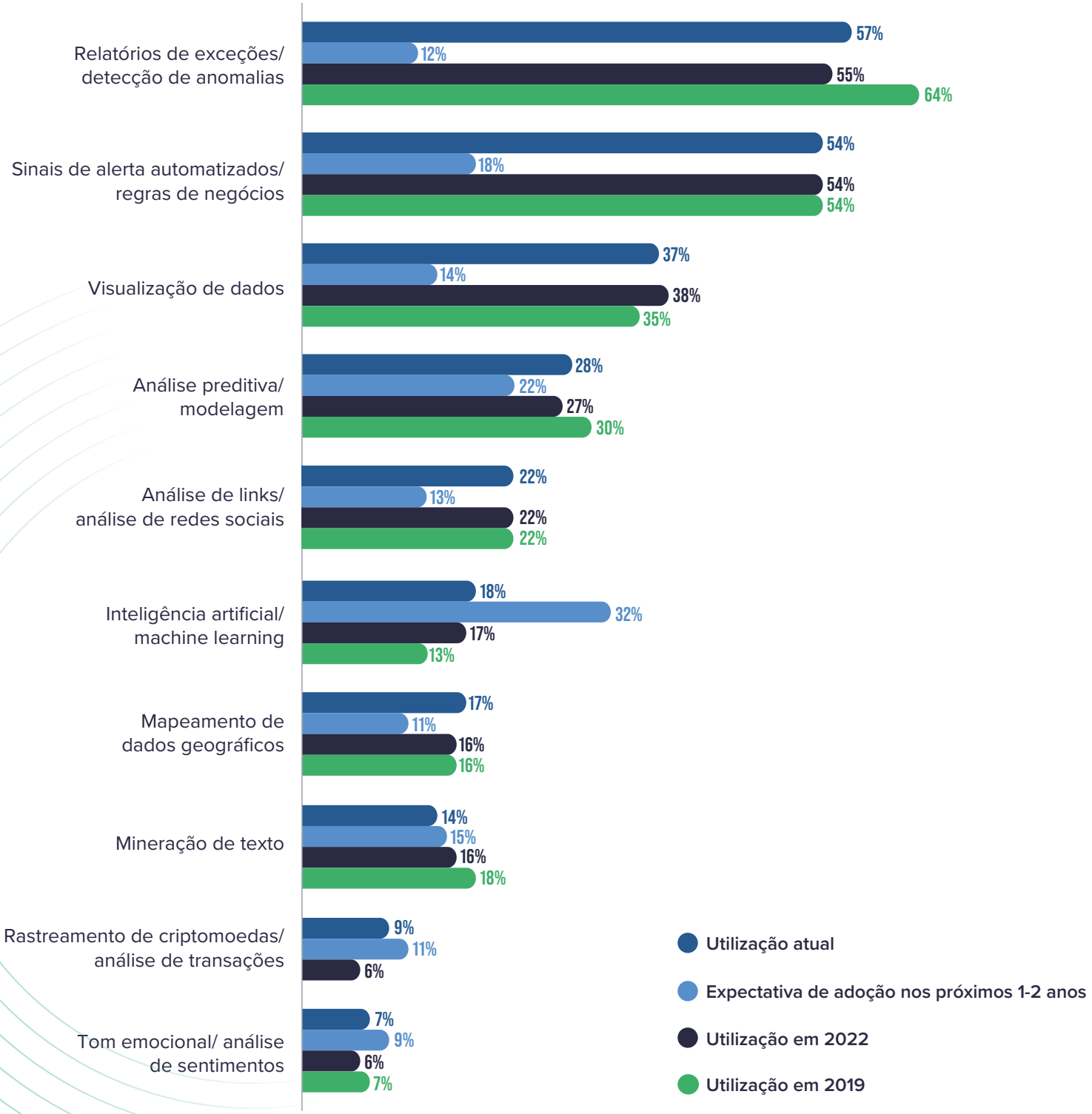
em programas antifraude deverá quase **TRIPLICAR** nos próximos dois anos.



**3x**

> **“Sinais de alerta automatizados, machine learning e análise preditiva podem ser úteis atualmente devido ao alto volume de ataques cibernéticos e ao aumento do uso de tecnologia por criminosos.”**
>
> – Entrevistado

## FIG. 1 Quais técnicas de análise de dados as organizações utilizam para combater a fraude?



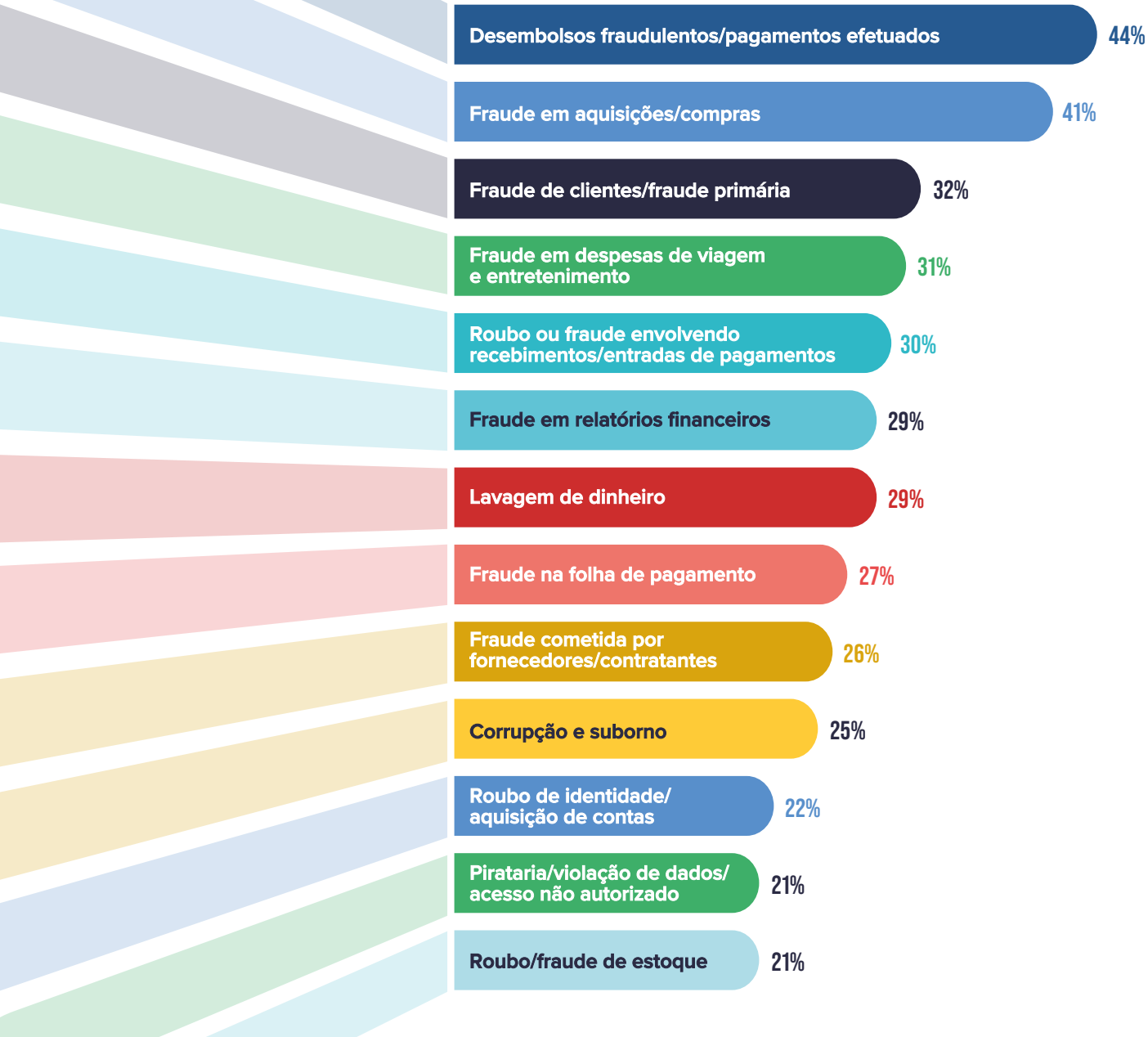
À medida que as organizações implementam e aprimoram seus programas de análise, pode ser útil ver quais ferramentas outras empresas estão utilizando para diversas finalidades. A Figura 2 mostra os programas mais comuns para cada uma das técnicas de análise em nosso estudo. Em todas as categorias, uma parte significativa dos entrevistados observou que sua organização utiliza uma plataforma interna proprietária para executar a técnica de análise mencionada.

## FIG. 2 Quais são os programas mais utilizados para cada técnica analítica?

# EM QUAIS ÁREAS DE RISCO AS ORGANIZAÇÕES UTILIZAM A ANÁLISE DE DADOS PARA MONITORAR FRAUDES?

Para garantir que a análise de dados seja utilizada da forma mais eficaz e eficiente possível, muitas organizações aplicam uma abordagem baseada em riscos, concentrando suas iniciativas de análise na detecção de possíveis fraudes em áreas de risco específicas da empresa. A Figura 3 mostra que os pagamentos e desembolsos de saída são a área mais comumente monitorada com a utilização da análise (44% das organizações), seguida de perto pela função de aquisição e compras (41% das organizações).

**FIG. 3** Em quais áreas de risco as organizações utilizam a análise de dados para monitorar fraudes?



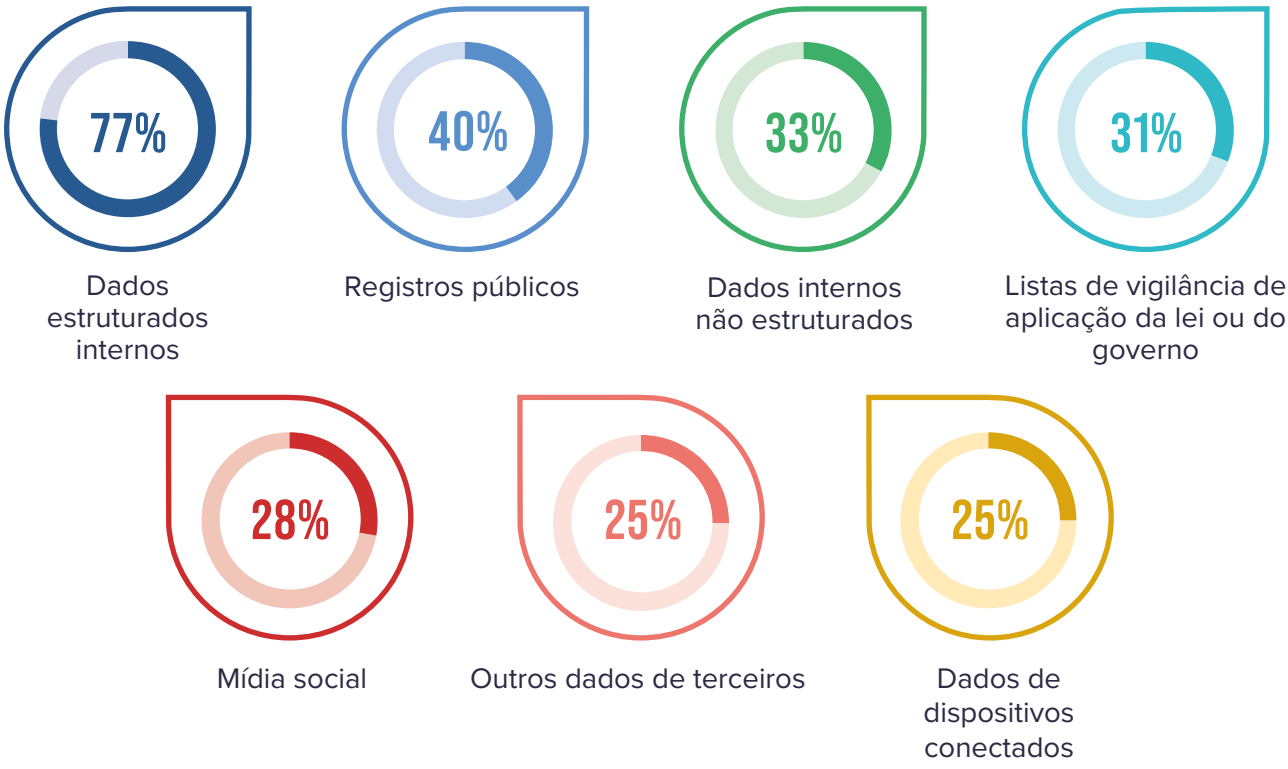
# QUAIS SÃO AS FONTES DE DADOS UTILIZADAS PELAS ORGANIZAÇÕES EM SUAS INICIATIVAS DE ANÁLISE DE DADOS ANTIFRAUDE?

Os dados que contêm sinais de alerta ou evidências de fraude podem estar em vários lugares, tanto dentro quanto fora da organização. Perguntamos aos participantes da pesquisa quais dos vários tipos de dados eles utilizam como fontes de dados para suas análises antifraude. Conforme mostrado na Figura 4, a fonte de dados mais comum são os dados estruturados internos (77% das organizações), que são dados formatados em estruturas reconhecíveis e previsíveis, como os encontrados em bancos de dados e planilhas. Em contrapartida, os dados internos não-estruturados - dados encontrados fora de formatos, como documentos de texto, e-mails e arquivos de imagem - são utilizados por apenas 33% das organizações e os dados de dispositivos conectados à rede da organização são utilizados por apenas 25%. Os registros públicos são a forma mais comum de dados externos utilizados (40% das organizações), seguida por listas de vigilância do governo (31% das organizações).

Além disso, a análise de dados de várias fontes pode fornecer percepções e evidências valiosas que podem não ser reconhecidas com a análise de apenas uma fonte de dados. Das organizações em nosso estudo, 62% utilizam atualmente dados de mais de uma fonte como parte de sua análise antifraude e 51% incorporam dados de fontes internas e externas.

> **Trabalhamos com dados não estruturados, que representam 75% do universo de dados, para entender o comportamento humano e prever a intenção de cometer fraudes e outros atos antiéticos."**
>
> – Entrevistado da pesquisa

**FIG. 4** Quais fontes de dados as organizações utilizam em suas iniciativas de análise de dados antifraude?



# QUAL É A VANTAGEM DA ANÁLISE DE DADOS PARA DIFERENTES ÁREAS DAS INICIATIVAS ANTIFRAUDE DAS ORGANIZAÇÕES?

Com mais de 90% das organizações utilizando alguma forma de análise de dados como parte de seus programas antifraude, fica claro que o valor geral dessas iniciativas é amplamente aceito. Para fornecer mais informações sobre os benefícios específicos proporcionados pela análise de fraudes, perguntamos aos participantes da pesquisa como seus esforços de análise de dados afetavam quatro áreas específicas:

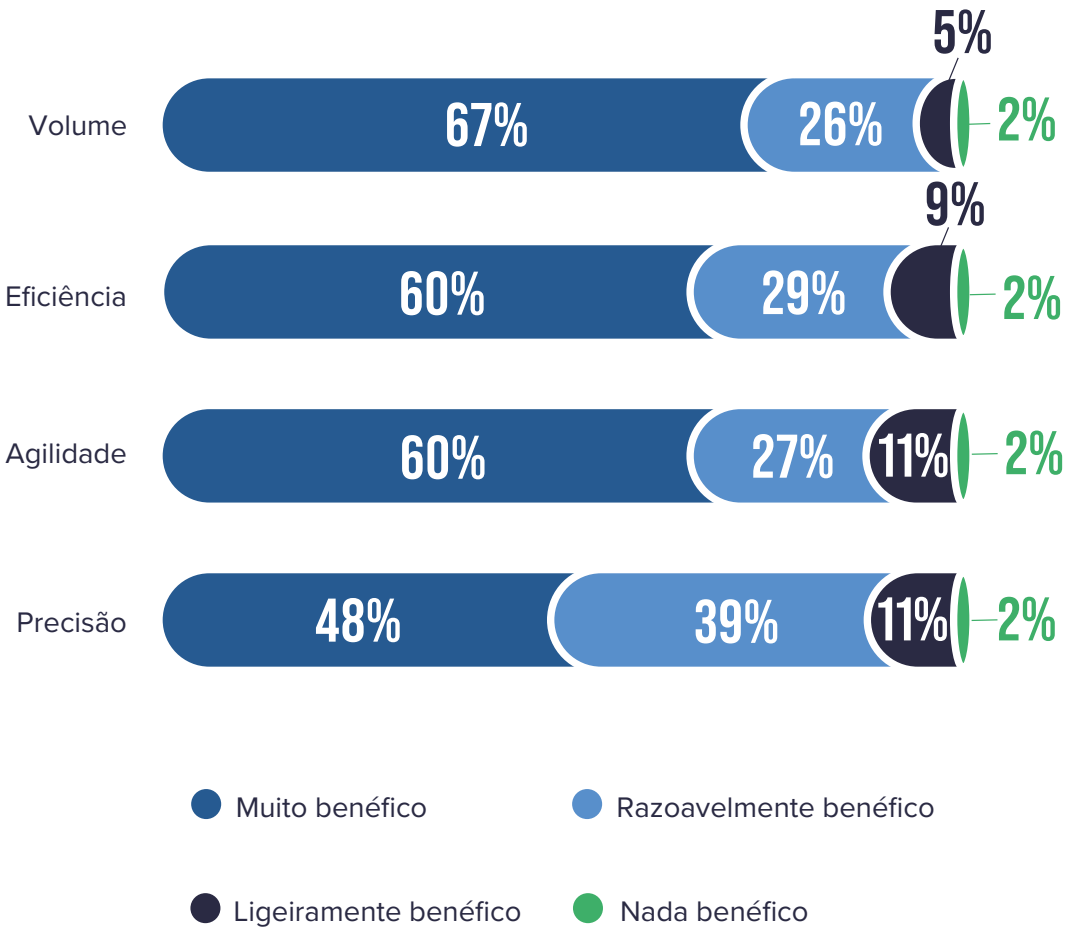
- **Volume**, ou a capacidade de analisar mais transações ou identificar mais casos de suspeita de fraude
- **Agilidade**, ou a capacidade de detectar anomalias mais rapidamente
- **Eficiência**, ou a capacidade de automatizar tarefas que consomem muito tempo
- **Precisão**, ou a capacidade de reduzir as taxas de falsos positivos

A Figura 5 mostra que o aumento no volume de transações analisadas e possíveis fraudes detectadas é o benefício mais percebido, com 93% dos entrevistados indicando que isso é muito ou razoavelmente benéfico. Da mesma forma, 89% observaram o aumento da eficiência como muito ou razoavelmente benéfico, e 87% disseram que a tempestividade adicional é muito ou razoavelmente benéfica para sua organização.

> **A análise de dados ajuda a enriquecer os resultados / relatórios antifraude. Ela não apenas reduz o tempo de resposta, mas também ajuda os investigadores a se concentrarem em aspectos muito importantes da investigação."**
>
> – Entrevistado da pesquisa

> **Os dados são tão bons quanto o que é inserido. Muitas vezes, a fraude está relacionada ao que não é inserido no sistema (dados ausentes)."**
>
> – Entrevistado

**FIG. 5** Qual é a vantagem da análise de dados para as diferentes áreas das iniciativas antifraude das organizações?



# QUE OUTRAS TECNOLOGIAS AS ORGANIZAÇÕES ESTÃO UTILIZANDO EM SUAS INICIATIVAS ANTIFRAUDE?

# AS ORGANIZAÇÕES ESTÃO UTILIZANDO SOFTWARE DE GERENCIAMENTO?

Ao avaliar ou investigar possíveis fraudes, o software de gerenciamento de casos pode tornar mais eficaz e eficiente a documentação da resposta e a organização das informações relacionadas. Entretanto, 57% dos entrevistados em nossa pesquisa indicaram que suas organizações não utilizam esse tipo de ferramenta como parte de seus programas antifraude. Entre os 43% das organizações que de fato utilizam um sistema de gerenciamento de casos, as plataformas internas ou proprietárias são o tipo mais comum de software utilizado.

**FIG. 6** As organizações estão utilizando software de gerenciamento de casos?

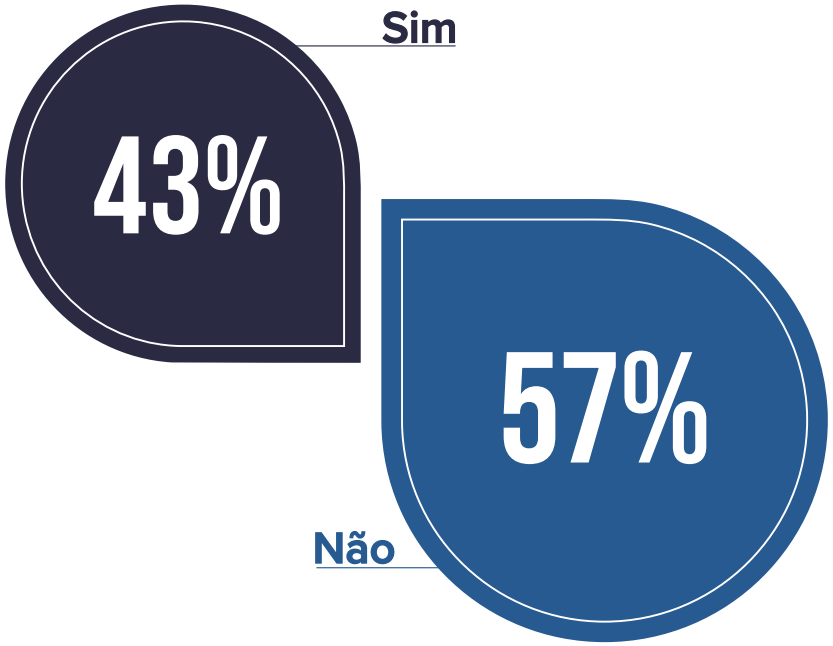



**FIG. 7** Quais são os programas de software de gerenciamento de casos mais comuns?*


*O tamanho do texto é relativo à frequência das respostas (ou seja, um texto maior indica mais respostas, e um texto menor indica menos respostas)

# AS ORGANIZAÇÕES ESTÃO UTILIZANDO SOFTWARE FORENSE DIGITAL/ DESCOBERTA ELETRÔNICA(E-DISCOVERY)?

As formas eletrônicas de evidência, incluindo arquivos e dados digitais, podem desempenhar um papel significativo nas investigações de fraudes. A utilização de programas de software forense digital e de descoberta eletrônica pode proporcionar numerosos benefícios na obtenção e no gerenciamento desse tipo de evidência. Entretanto, mais de 70% dos entrevistados indicaram que os programas antifraude de suas organizações não incluem a utilização de nenhuma plataforma formal de software forense digital ou de descoberta eletrônica. Para os 29% dos entrevistados cujas organizações utilizam esse tipo de software, o programa mais comumente utilizado é o EnCase, seguido pelo Cellebrite e pelo Relativity.

**FIG. 8** As organizações estão utilizando software forense digital/descoberta eletrônica?

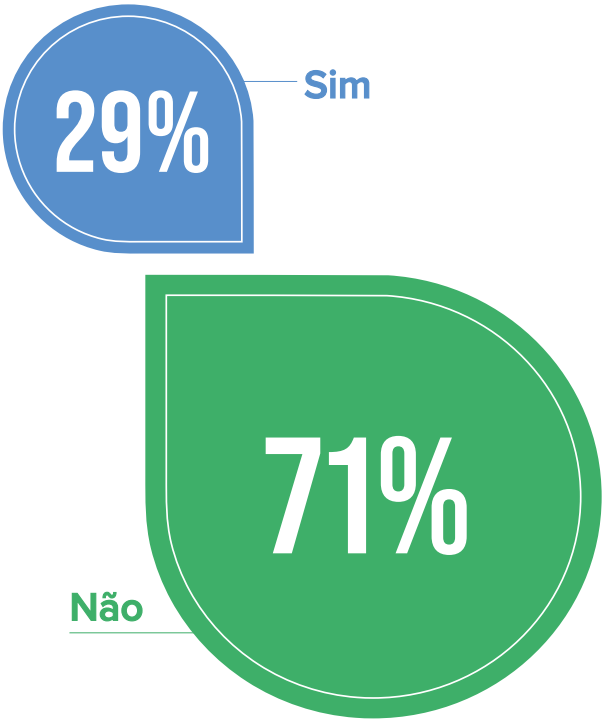
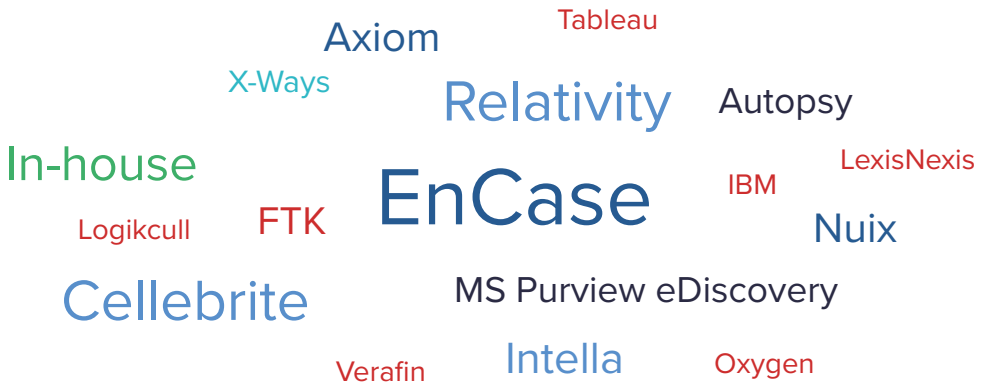



**FIG. 9** Quais são os programas de software forense digital/descoberta eletrônica mais comuns?*




* O tamanho do texto é relativo à frequência das respostas (ou seja, um texto maior indica mais respostas, e um texto menor indica menos respostas).

# AS ORGANIZAÇÕES ESTÃO UTILIZANDO SOFTWARE DE CAPTURA DE EVIDÊNCIAS ON-LINE?

As evidências digitais relevantes para as investigações de fraude também são obtidas regularmente de fontes online e as organizações podem empregar software de captura de evidências online para coletar e preservar essas evidências. Conforme mostrado na Figura 10, mais de dois terços das organizações dos entrevistados não incorporam atualmente software de captura de evidências online em seus programas antifraude. Dos 33% das organizações que possuem esse tipo de software, os programas internos ou proprietários são os mais comumente utilizados por uma margem significativa.

**FIG. 10** As organizações estão utilizando software de captura de evidências online?

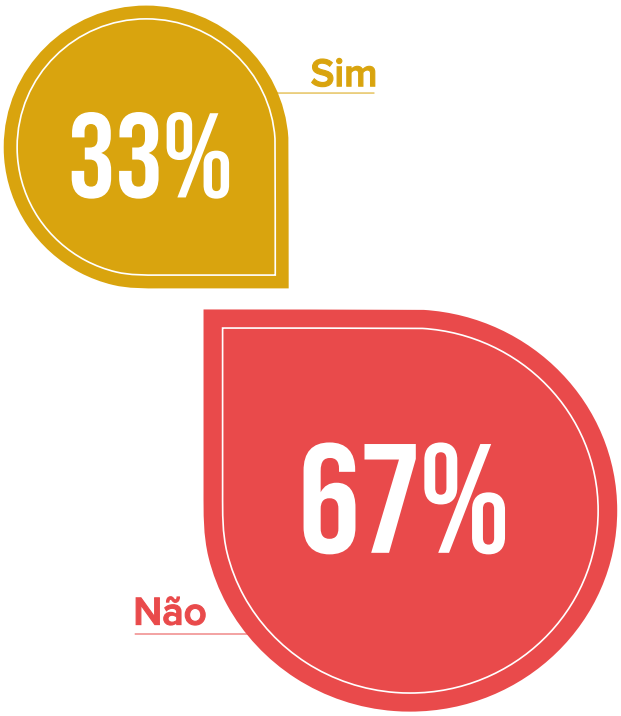
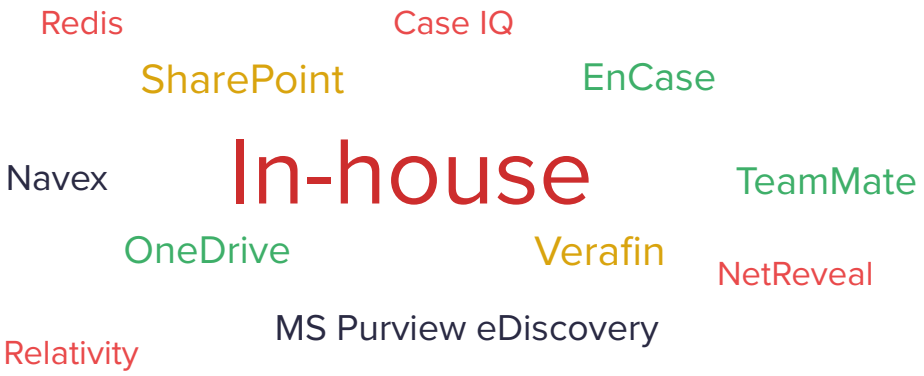



**FIG. 11** Quais são os programas de software de captura de evidências online mais comuns?*




* O tamanho do texto é relativo à frequência das respostas (ou seja, um texto maior indica mais respostas, e um texto menor indica menos respostas).

# QUAIS TECNOLOGIAS EMERGENTES AS ORGANIZAÇÕES ESTÃO UTILIZANDO PARA COMBATER A FRAUDE?

À medida que surgem novas classes de tecnologia que apoiam a investigação, a detecção e a prevenção de fraudes, muitas organizações avaliam os possíveis benefícios que essas tecnologias podem proporcionar a seus programas antifraude. Perguntamos aos participantes da pesquisa quais categorias de tecnologias emergentes eles utilizam atualmente em seu programa antifraude ou esperam incorporar no futuro.

Conforme ilustrado na Figura 12, a tecnologia emergente utilizada atualmente pela maioria das organizações é a biometria física, que é utilizada para identificar indivíduos com base em atributos físicos, como impressões digitais e características faciais ou vocais; 40% dos entrevistados observaram que sua organização emprega atualmente a biometria física e outros 17% esperam adotar essa tecnologia em um futuro próximo. Embora a utilização atual da biometria física seja duas vezes mais comum do que a análise de visão computacional (20%), robótica (20%) e biometria comportamental (20%), todas essas quatro tecnologias estão em utilização atualmente ou deverão ser utilizadas por mais de 50% das organizações entrevistadas em algum momento no futuro. Por outro lado, mais da metade dos entrevistados indicou que não espera que suas organizações utilizem a tecnologia blockchain/registro distribuído ou realidade virtual/aumentada como parte de seus programas antifraude.

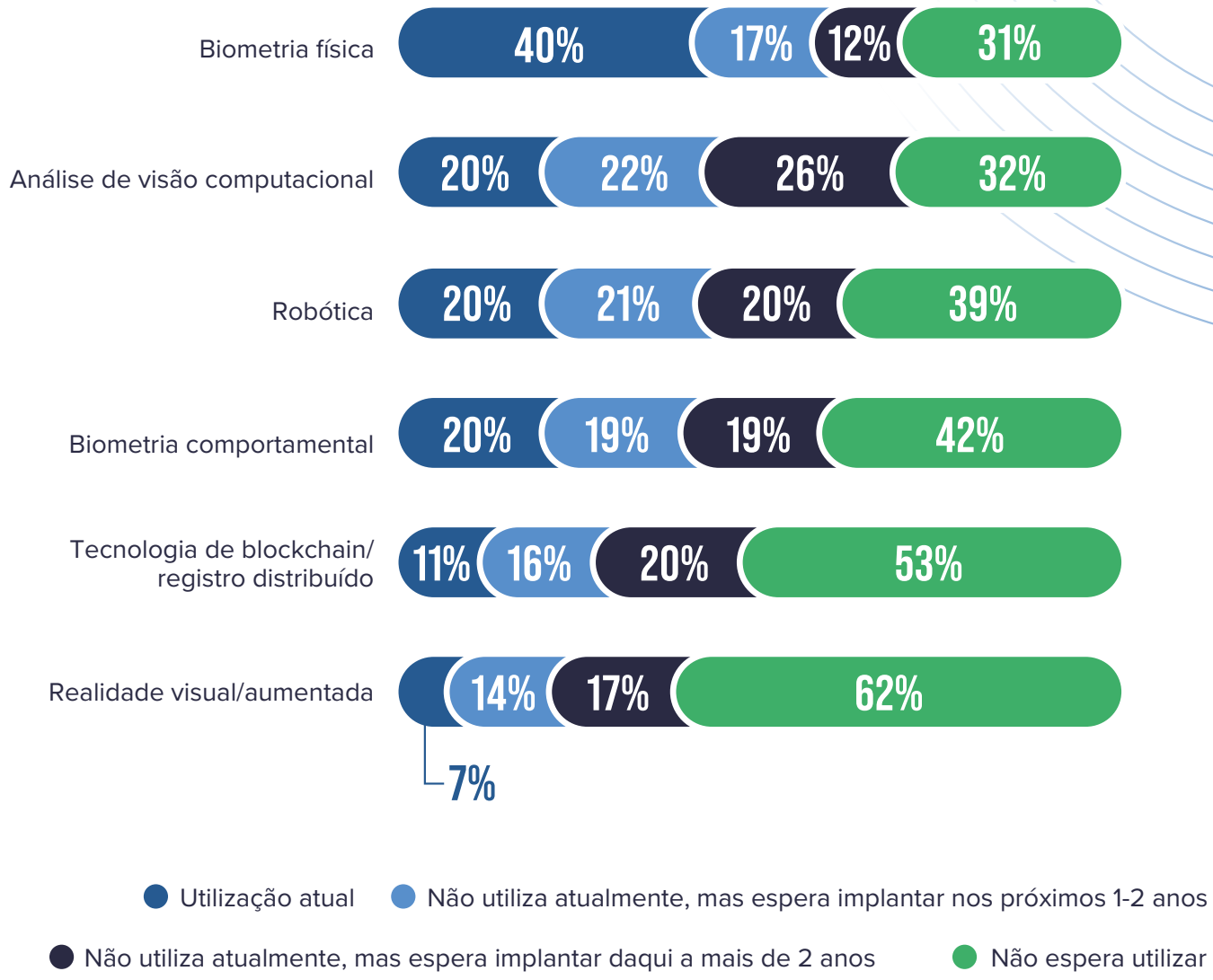
Além disso, nosso estudo mostrou um aumento constante no uso da biometria e da robótica como parte dos programas antifraude nos últimos anos. Em 2019, apenas 26% das organizações estavam utilizando qualquer forma de biometria em seus programas, enquanto 40% das organizações em nosso estudo atual utilizam apenas a biometria física. Da mesma forma, a utilização da robótica para combater a fraude cresceu de 9% das organizações em 2019 para 20% no estudo deste ano.

> “As tecnologias emergentes em iniciativas antifraude fornecerão às organizações os recursos e as ferramentas necessárias para identificar tendências e indícios de fraude com mais eficiência e eficácia.”
>
> – Entrevistado da pesquisa

> Nem tudo é relevante para todas as organizações. É importante saber qual é a melhor e mais relevante tecnologia para a organização."
>
> – Entrevistado da pesquisa

> “Embora ainda haja algum refinamento a ser efetuado com relação à aplicabilidade de tecnologias emergentes em iniciativas antifraude, os investigadores não podem se dar ao luxo de ignorar a sua importância.”
>
> – Entrevistado da pesquisa

**FIG. 12** Quais tecnologias emergentes as organizações estão utilizando para combater a fraude?



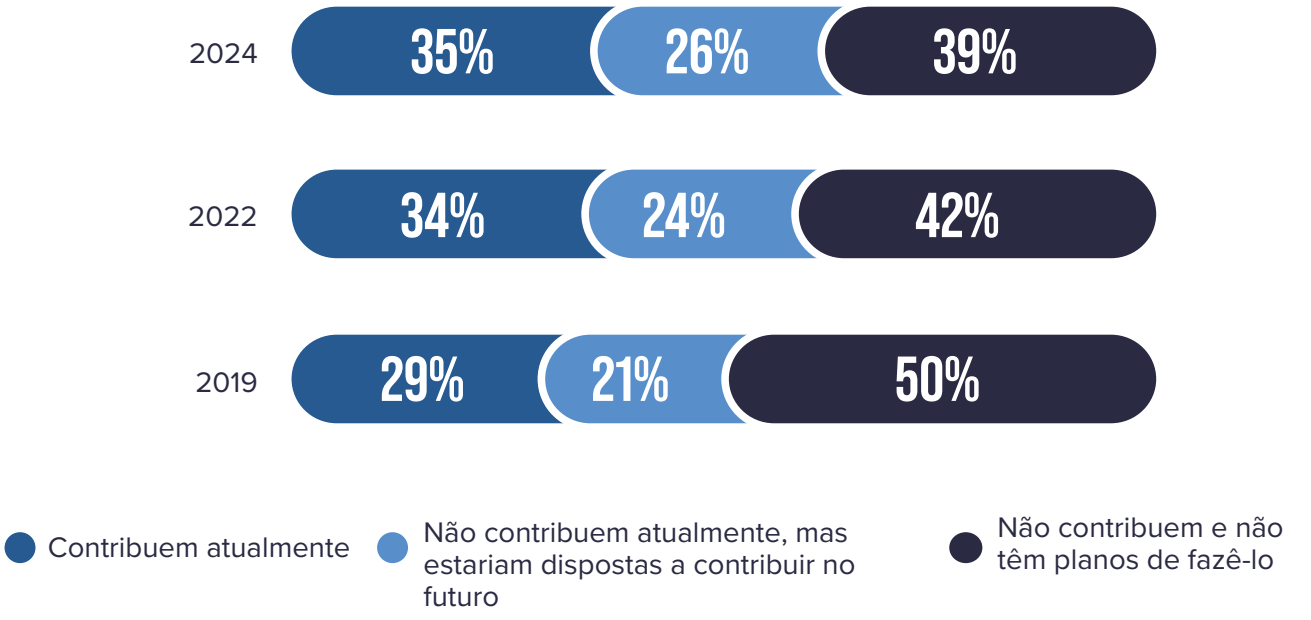
# AS ORGANIZAÇÕES ESTÃO CONTRIBUINDO COM CONSÓRCIOS DE COMPARTILHAMENTO DE DADOS PARA AJUDAR A PREVENIR OU DETECTAR FRAUDES?

Embora muitas organizações obtenham percepções de seus próprios dados que podem reforçar seus esforços de prevenção ou detecção de fraudes, essas percepções podem ser limitadas pelo escopo dos dados internos disponíveis. Os consórcios de compartilhamento de dados reúnem informações de várias organizações, geralmente do mesmo setor, para serem analisados quanto a tendências e padrões relacionados a possíveis atividades fraudulentas que podem ser aproveitadas nos programas antifraude das organizações participantes. A capacidade de acessar dados de organizações semelhantes pode melhorar os resultados de análise e monitoramento devido ao tamanho maior da amostra.

Conforme mostrado na Figura 13, 61% das organizações entrevistadas indicaram que atualmente contribuem para um consórcio de compartilhamento de dados (35%) ou que estariam dispostas a fazê-lo no futuro (26%). Adicionalmente, a porcentagem de organizações que não planejam participar de um consórcio tem caído constantemente nos últimos anos, ilustrando um maior reconhecimento do valor da colaboração e do compartilhamento de dados como parte da luta contra a fraude.

**61%** das organizações contribuem atualmente ou estão dispostas a contribuir com consórcios de dados para ajudar em seus esforços antifraude.

**FIG. 13** As organizações estão contribuindo com consórcios de compartilhamento de dados para ajudar a prevenir ou detectar fraudes?



# QUAIS DESAFIOS AS ORGANIZAÇÕES ENFRENTAM NA IMPLEMENTAÇÃO DE NOVAS TECNOLOGIAS ANTIFRAUDE?

A implementação de uma nova tecnologia não está isenta de desafios que podem afetar a eficácia da tecnologia para aplicativos antifraude. Perguntamos aos entrevistados sobre vários fatores que podem complicar a integração de novas soluções tecnológicas para determinar o grau de desafio que cada um representa. Cada um dos oito fatores apresenta pelo menos um desafio menor para 80% ou mais das organizações entrevistadas. As restrições orçamentárias/financeiras são a barreira mais significativa, representando um desafio importante ou moderado para 82% dos entrevistados. Outros desafios citados incluem baixa qualidade ou integração de dados e limitações de pessoal e habilidades internas relevantes para a tecnologia.

> Silos organizacionais com várias equipes de fraude tentando encontrar soluções - isso está melhorando, e a centralização da estratégia de fraude está em andamento, mas é um grande desafio.
> A integração de novas tecnologias em tempo hábil para ficar à frente da fraude é um desafio."
>
> – Entrevistado da pesquisa

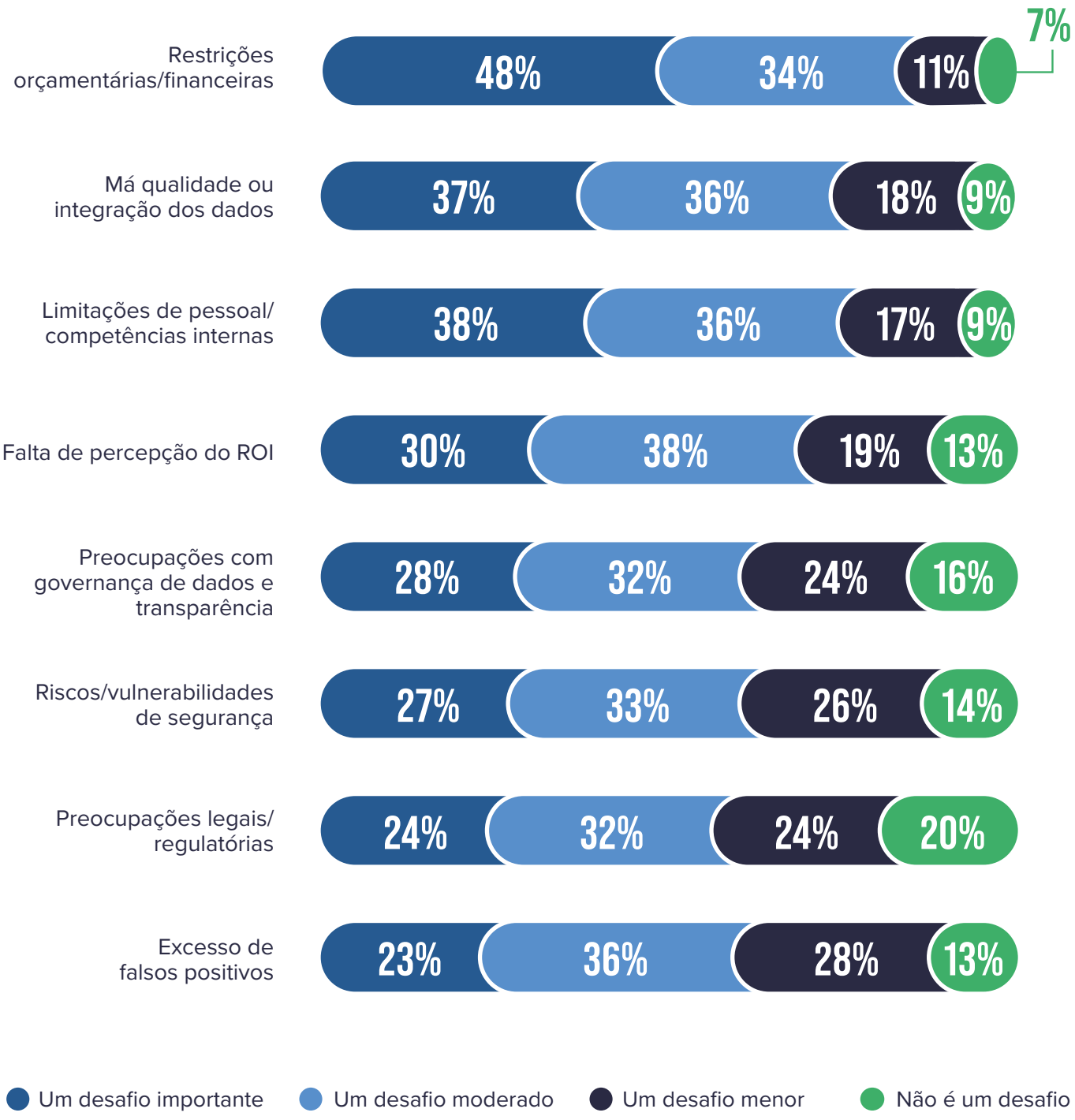
> Outro desafio da implementação de uma nova tecnologia antifraude em uma organização é garantir que haja um esforço colaborativo que maximize os recursos e o ROI."
>
> – Entrevistado

**82%**

## RESTRIÇÕES ORÇAMENTÁRIAS OU FINANCEIRAS

representam uma das principais preocupações ao implementar uma nova tecnologia antifraude, pois representam um desafio importante ou moderado para **82%** das organizações.

**FIG. 14** Quais são os desafios que as organizações enfrentam ao implementar uma nova tecnologia antifraude?



# COMO A IA GENERATIVA ESTÁ AFETANDO OS PROGRAMAS ANTIFRAUDE DAS ORGANIZAÇÕES?

*IA Generativa* é o termo utilizado para descrever modelos de inteligência artificial de aprendizagem profunda utilizados para geração de imagens, vídeos, áudio ou textos de alta qualidade. Essa tecnologia ganhou destaque rapidamente e muitas organizações a estão experimentando e implementando formalmente para auxiliar suas operações em várias funções.

Como parte do nosso estudo, exploramos a implementação da IA generativa como parte dos programas antifraude das organizações. A maioria dos entrevistados (83%) indicou que suas organizações esperam adotar ferramentas de IA generativa como parte de seu kit de ferramentas antifraude nos próximos dois anos.

Ao avaliar como empregar essa tecnologia, as organizações devem considerar vários fatores. Conforme observado na Figura 15, 85% das organizações consideram a precisão dos resultados obtidos pela IA generativa como um fator muito importante ou importante nessa decisão, enquanto os riscos e as vulnerabilidades de segurança recebem o mesmo nível de consideração por 83% delas. Além disso, embora a facilidade de utilização seja frequentemente apontada como um dos principais benefícios da IA generativa, 77% das organizações ainda consideram a equipe e as habilidades internas relacionadas à tecnologia como um fator importante ou muito importante para determinar se a tecnologia será implementada.

**83%**

das organizações esperam implementar

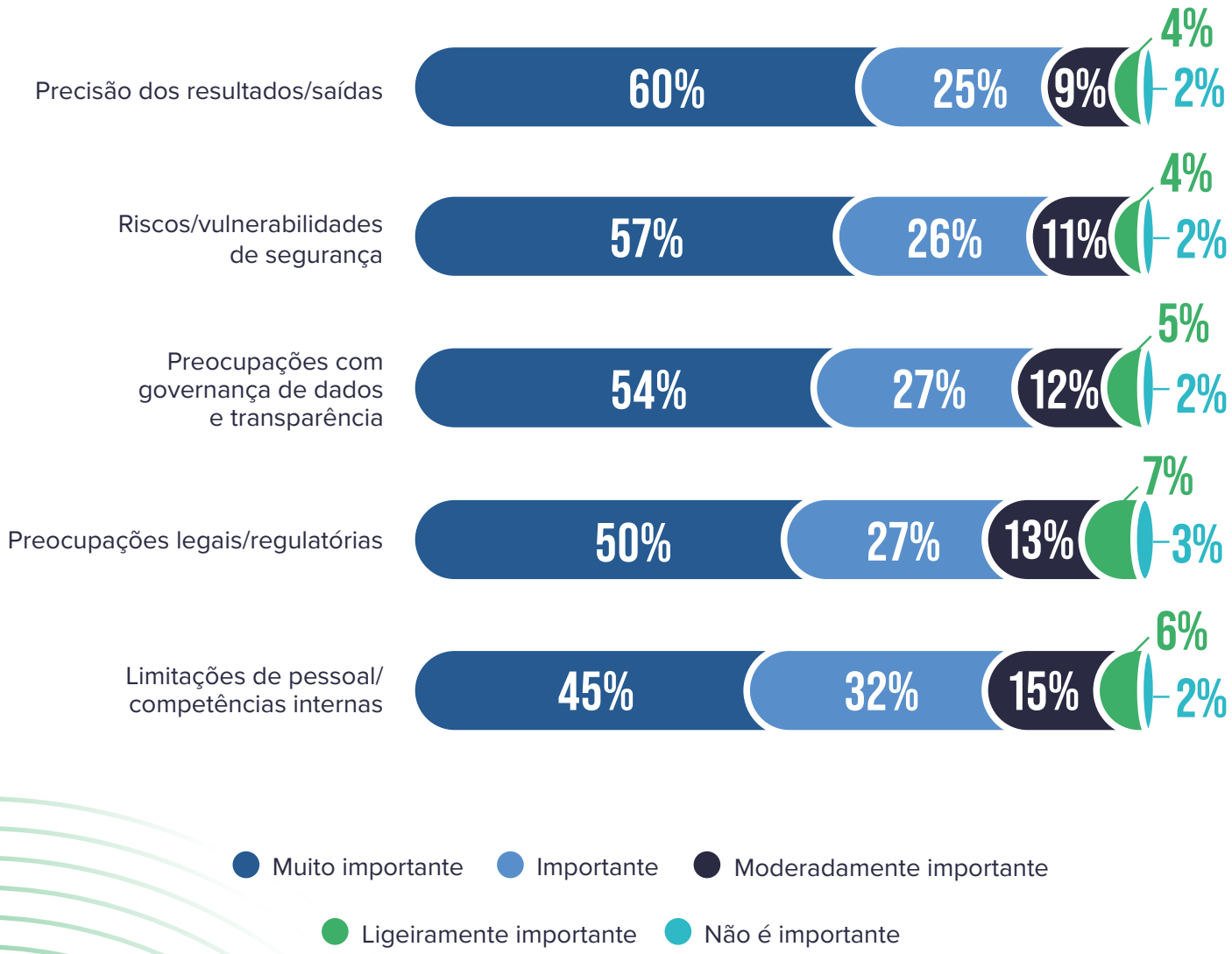
**IA GENERATIVA**

como parte de seus programas antifraude nos próximos dois anos.

> A utilização de IA generativa em outras iniciativas antifraude poderia desempenhar um papel significativo na identificação de anomalias, tendências e indicações em volumes maiores de dados com preocupações mínimas de recursos. No entanto, a organização precisará garantir que as diretrizes adequadas estejam em vigor para minimizar erros e tendenciosidades.”
>
> – Entrevistado da pesquisa

> **A precisão, na minha opinião, é o maior desafio para a IA generativa, pois os investigadores terão dificuldade em confiar ou em implantar uma tecnologia imprecisa. Isso ocorre porque a investigação deve ser uma ciência exata.”**
>
> – Entrevistado da pesquisa

**FIG. 15** Qual é a importância dos diferentes fatores ao decidir se a IA generativa deve ser implementada como parte de um programa antifraude?



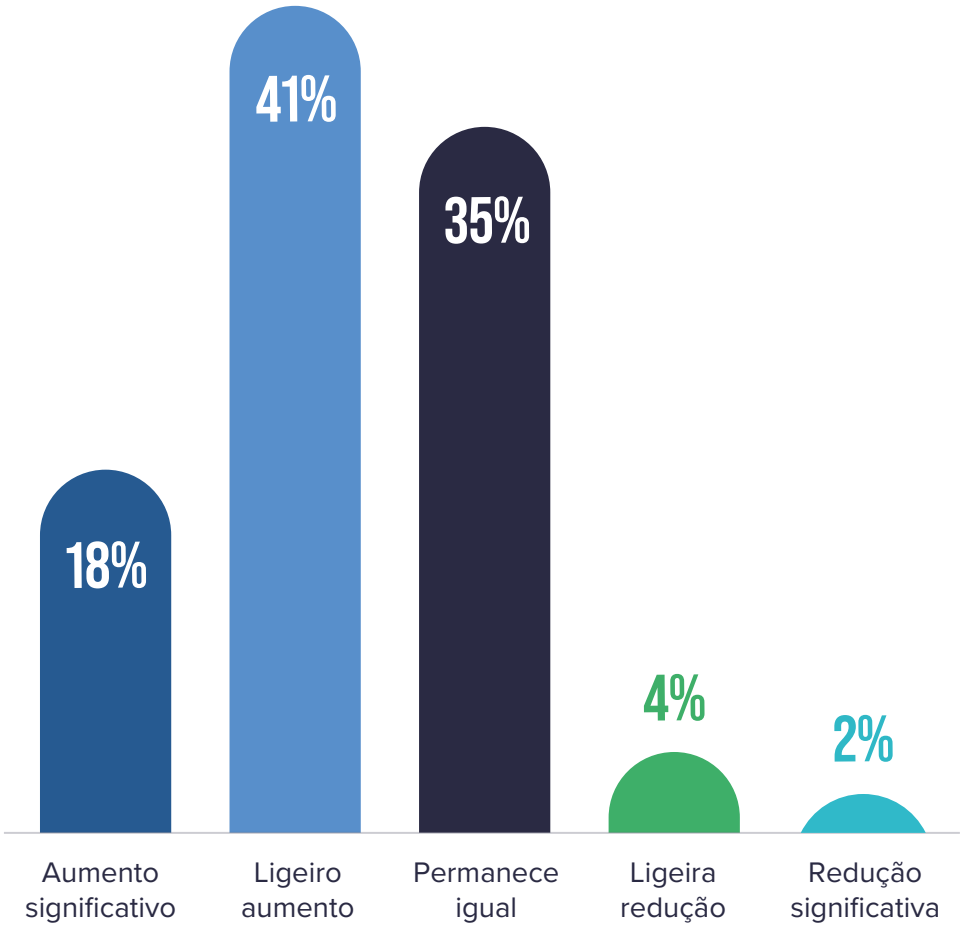
# COMO SE ESPERA QUE OS ORÇAMENTOS DE TECNOLOGIA ANTIFRAUDE DAS ORGANIZAÇÕES MUDEM NOS PRÓXIMOS DOIS ANOS?

Manter-se à frente dos fraudadores geralmente significa dedicar recursos para adquirir e implementar ferramentas adicionais para prevenir e detectar seus esquemas. Conforme observado na Figura 14, as restrições orçamentárias e financeiras representam um desafio importante ou moderado para a implementação de novas tecnologias antifraude pela maioria das organizações.

Mesmo assim, nosso estudo mostra que 59% das organizações esperam aumentar seus orçamentos para a tecnologia antifraude nos próximos dois anos (veja a Figura 16). Apenas 6% das organizações preveem cortes orçamentários nessa área, demonstrando o valor que a implantação de novas tecnologias pode trazer para o combate à fraude.

**59%** das organizações esperam **AUMENTAR SEUS ORÇAMENTOS** para tecnologia antifraude nos nos próximos dois anos.

FIG. 16 Como se espera que os orçamentos de tecnologia antifraude das organizações mudem nos próximos dois anos?



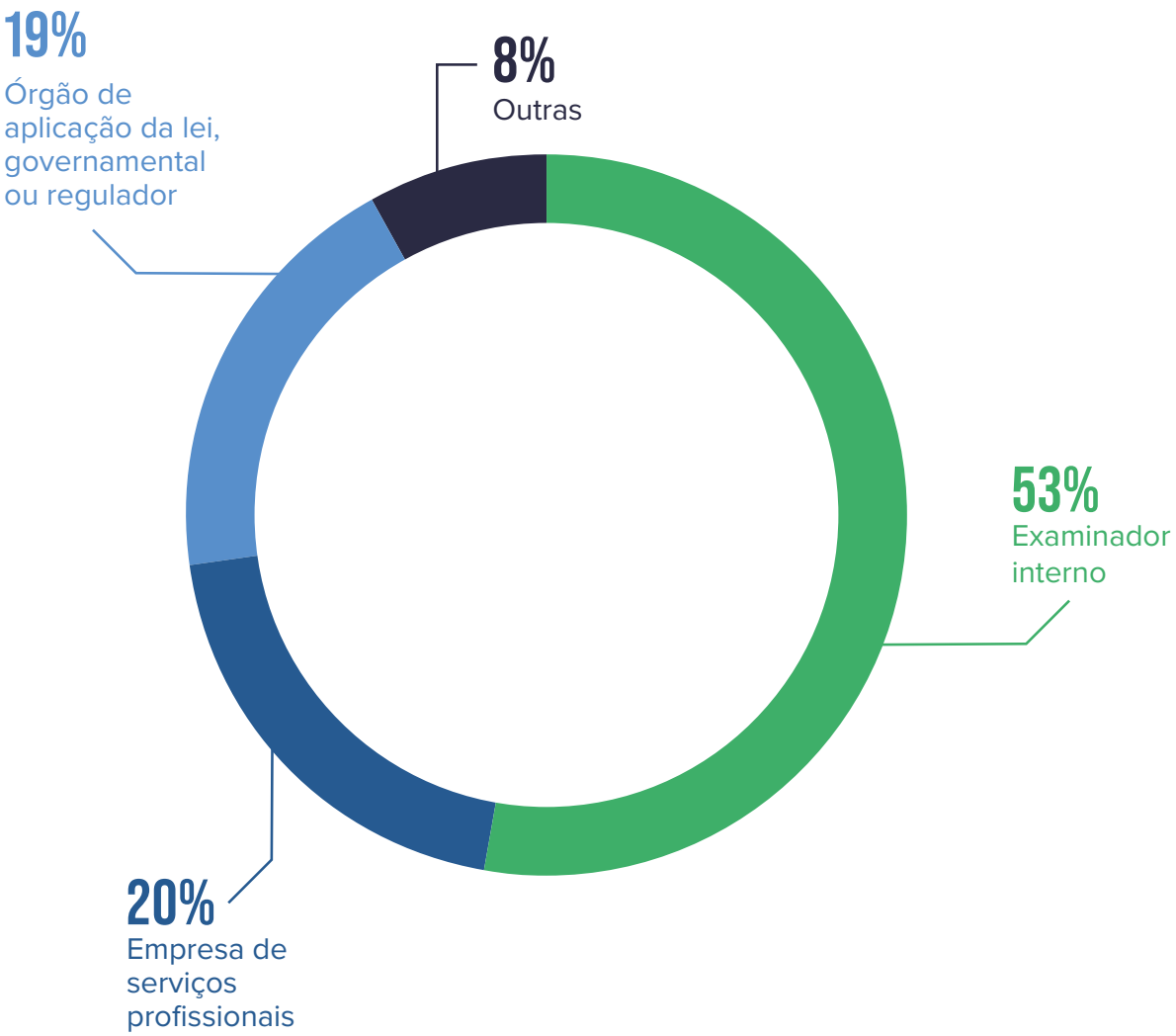
# DADOS DEMOGRÁFICOS DOS ENTREVISTADOS

Este relatório contém análises dos resultados de nossa pesquisa com base em todas as respostas recebidas em todas as categorias demográficas. Para obter subanálises baseadas em setores, regiões e tamanhos de organização específicos, acesse **SAS.com/fraudsurvey.**

# FUNÇÃO PROFISSIONAL DOS ENTREVISTADOS

Mais da metade (53%) dos indivíduos que participaram do nosso estudo trabalham internamente e realizam atividades antifraude em uma única organização. Outros 20% trabalham para empresas de serviços profissionais que realizam atividades antifraude ou compromissos em nome de outras organizações e 19% trabalham para um órgão de aplicação da lei, governamental ou regulador que realiza investigações de fraude ou outros compromissos envolvendo partes externas sob a autoridade de seu órgão.

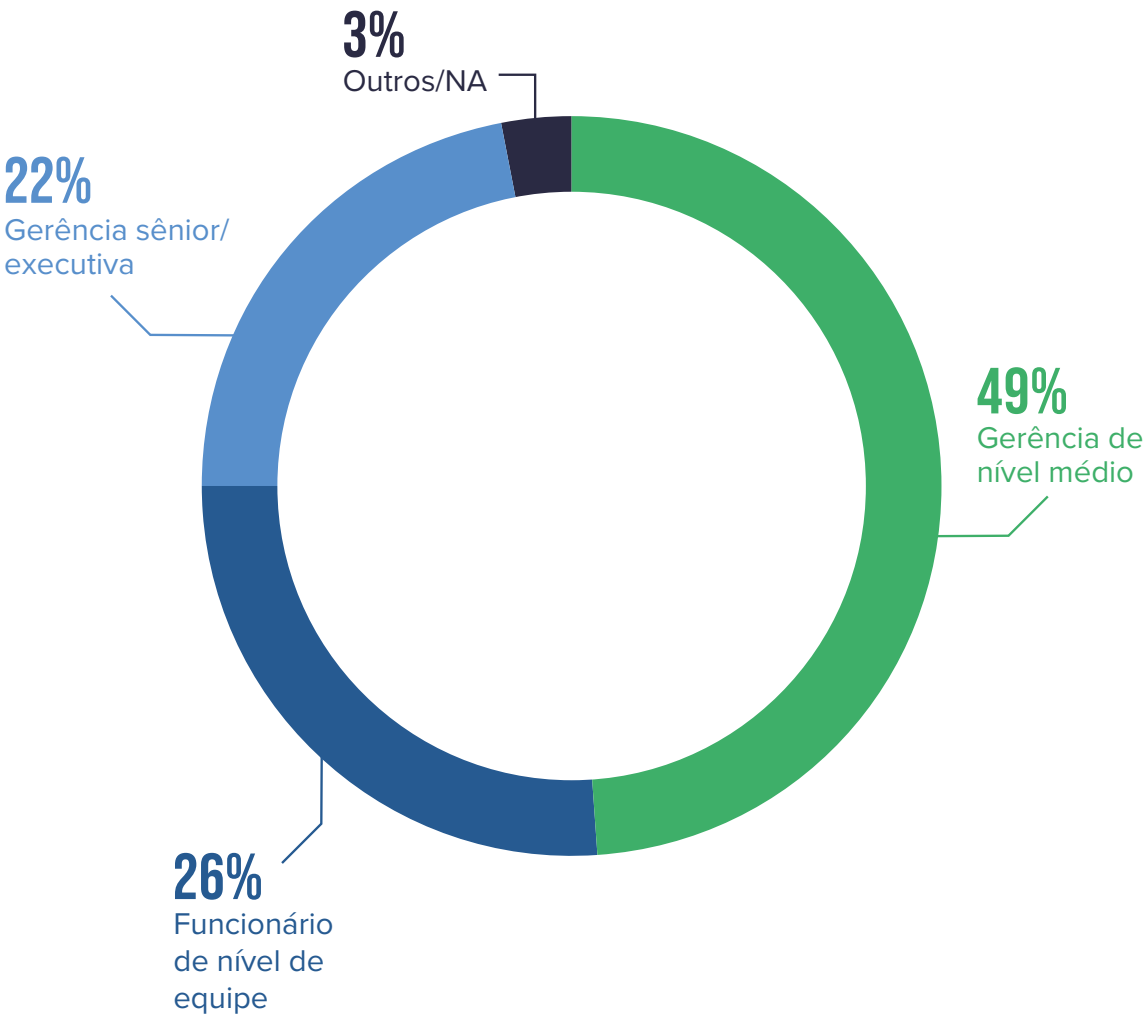
FIG. 17 Função profissional dos entrevistados



## CARGO DOS ENTREVISTADOS

Quase a metade dos participantes da pesquisa ocupa cargos de gerência de nível médio em suas organizações, enquanto 26% ocupam funções de nível de equipe (sem supervisão) e 22% estão no nível de gerência sênior ou executiva.

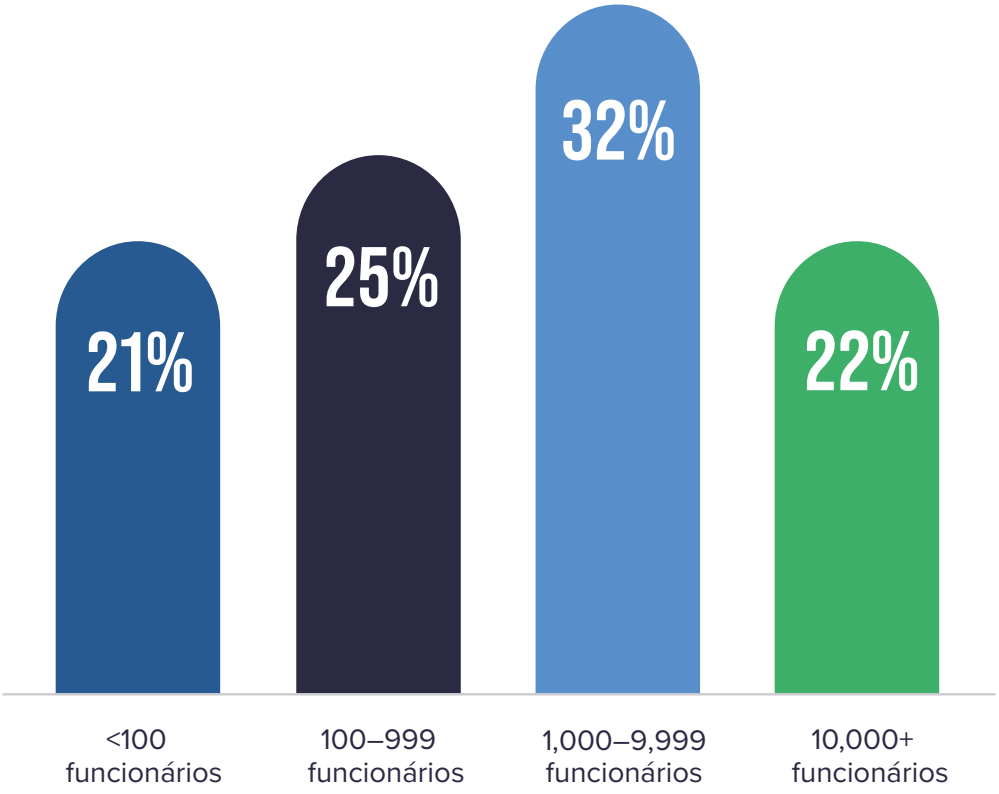
**FIG. 18** Cargo dos entrevistados



## TAMANHO DAS ORGANIZAÇÕES DOS ENTREVISTADOS

Os entrevistados da pesquisa representaram uma variedade de tamanhos de organizações. Conforme observado na Figura 19, quase um terço (32%) trabalha para organizações com 1.000 a 9.999 funcionários e um quarto trabalha para organizações com 100 a 999 funcionários.

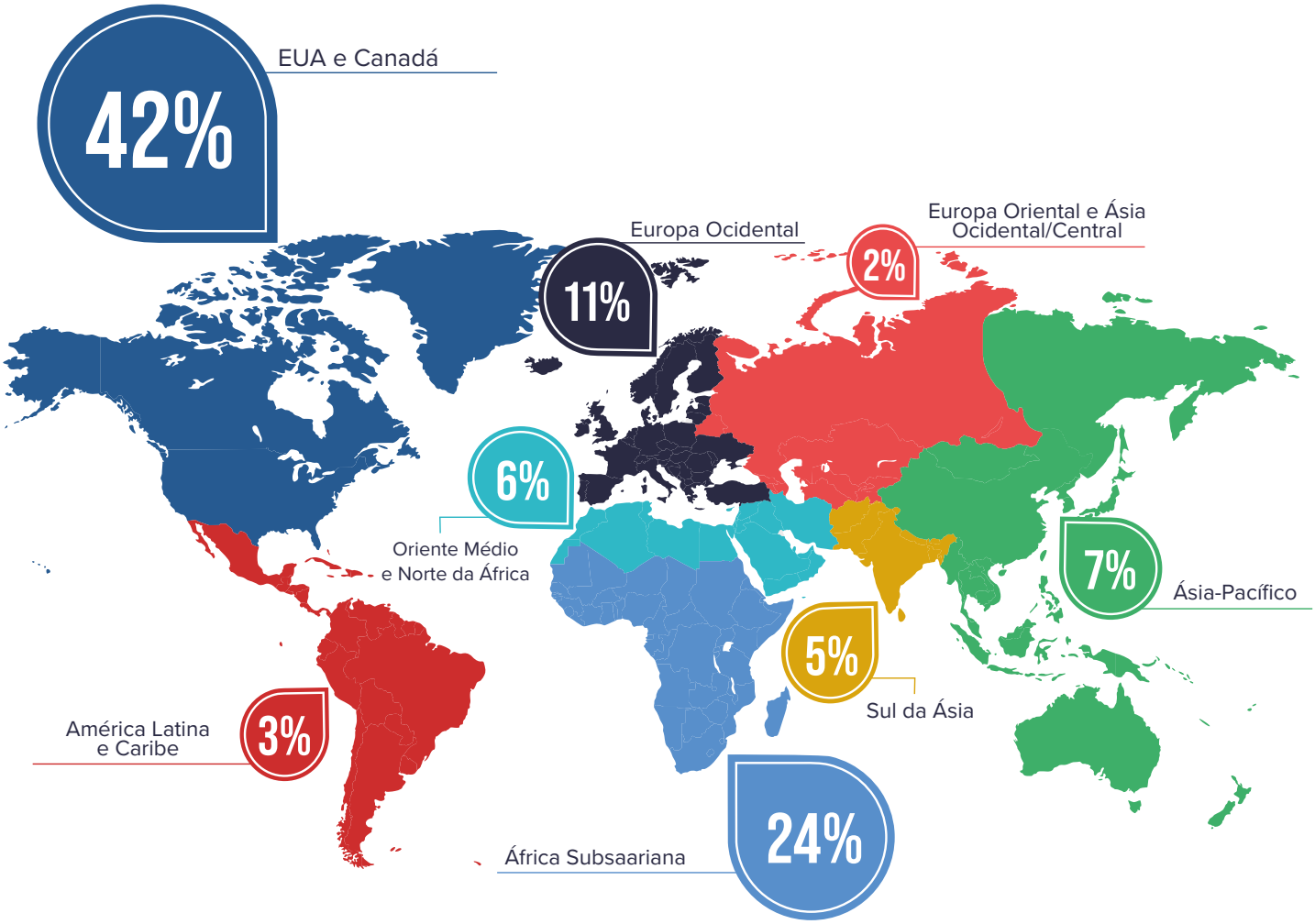
FIG. 19 Tamanho das organizações dos entrevistados



# REGIÃO DAS ORGANIZAÇÕES DOS ENTREVISTADOS

Os entrevistados da pesquisa representaram organizações de 111 países em todo o mundo, fornecendo uma visão global das tendências da tecnologia antifraude. A maior proporção de entrevistados (42%) é dos Estados Unidos e do Canadá, seguidos pela África Subsaariana (24%) e pela Europa Ocidental (11%).

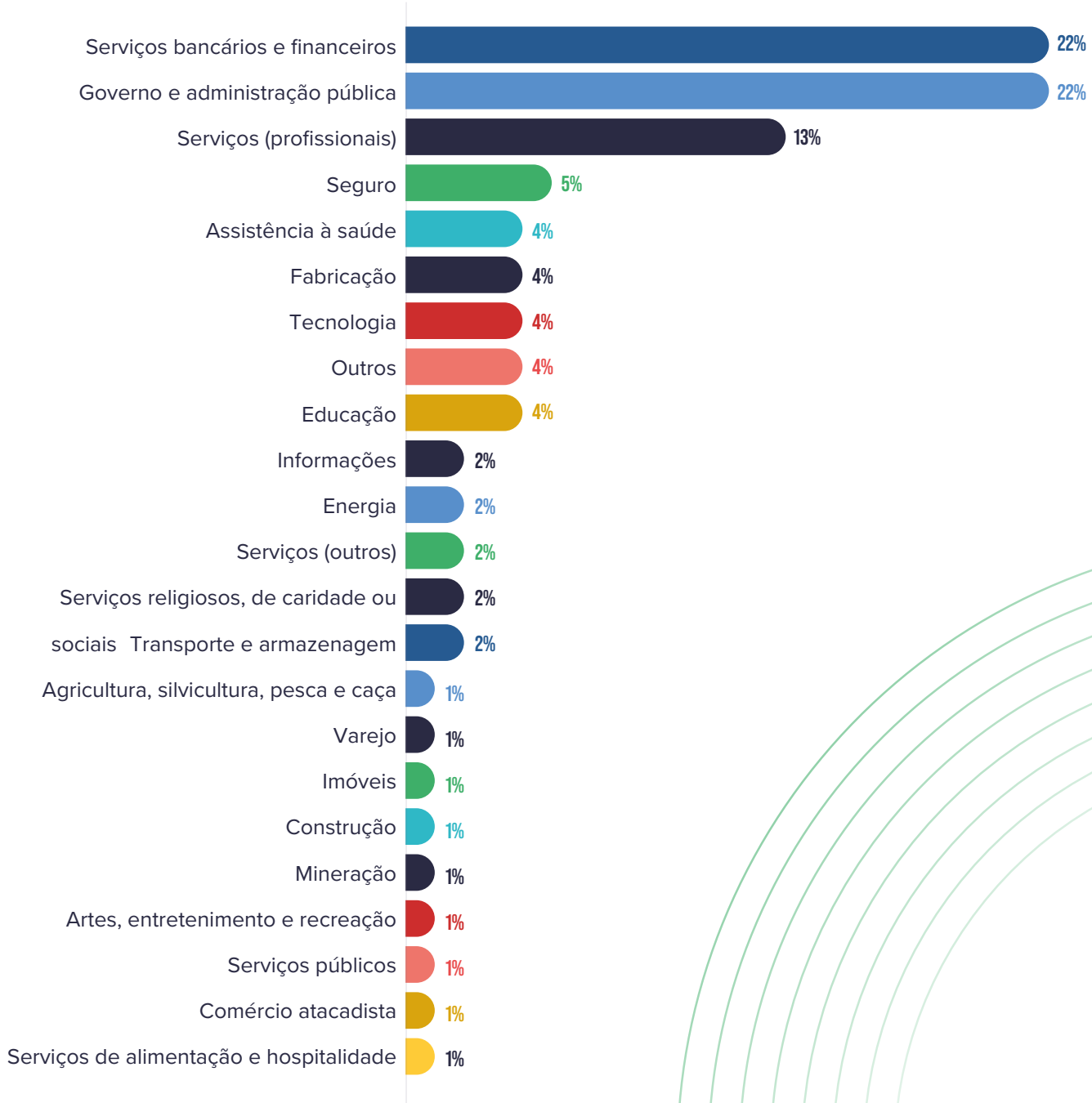
**FIG. 20** Região das organizações dos entrevistados



# SETOR DAS ORGANIZAÇÕES DOS ENTREVISTADOS

Os dois setores mais comuns representados em nosso estudo são serviços bancários e financeiros e governo e administração pública, cada um com 22% dos participantes da pesquisa. Outros setores com representação notável são o de serviços profissionais (13%) e o de seguros (5%), e o restante dos participantes está distribuído entre muitos outros setores.

**FIG. 21** Setor das organizações dos entrevistados



## SOBRE A ACFE

Fundada em 1988 pelo Dr. Joseph T. Wells, CFE, CPA, a Associação dos Investigadores de Fraude Certificados (ACFE) é a maior organização antifraude do mundo e a principal fornecedora de treinamento e educação antifraude. Juntamente com mais de 90.000 membros, a ACFE está reduzindo as fraudes comerciais em todo o mundo e inspirando a confiança do público na integridade e objetividade da profissão.

A ACFE une e apoia a comunidade global antifraude, fornecendo ferramentas educacionais e soluções práticas para profissionais por meio de eventos, publicações, redes e materiais educacionais para faculdades e universidades. A ACFE oferece a seus membros a oportunidade de obter certificação profissional. A credencial de Investigadores de Fraude Certificados (CFE) é a preferida por empresas e entidades governamentais em todo o mundo e indica experiência em prevenção e detecção de fraudes.

**Saiba mais em ACFE.com.**

## SOBRE O SAS

O SAS é o líder global em dados e IA. O SAS ajuda as organizações a transformar dados em decisões confiáveis mais rapidamente, fornecendo conhecimento nos momentos que importam. E em um mundo digital onde o combate à fraude e aos crimes financeiros se torna mais complexo a cada dia, o SAS oferece as mais poderosas soluções de inteligência contra fraude, lavagem de dinheiro e segurança para mantê-lo à frente. É por isso que 90% das empresas da Fortune 100 confiam no SAS para resolver seus desafios mais difíceis com maior velocidade, escala e eficiência. Desde 1976, o SAS tem oferecido aos clientes de todo o mundo THE POWER TO KNOW®. **Saiba mais sobre o SAS.**

ACFE®
Association of Certified Fraud Examiners

sas®



113901_G270570.0224