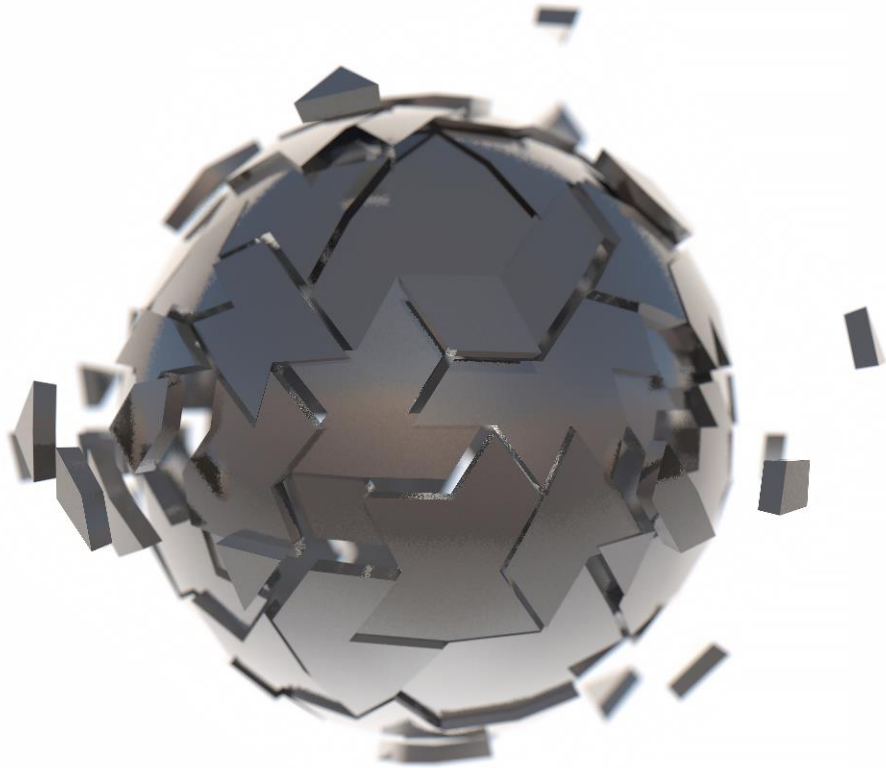
Deloitte.



Governança em Gestão de Riscos & Controles internos

A integração das 3 linhas de defesa

Contexto

Pesquisa de Governança em empresas estatais

Desafios e estratégias para adequação aos requerimentos da Lei nº 13.303/16

Pesquisa 2018

Metodologia e amostra da pesquisa

Objetivo da pesquisa: explorar como as empresas estão se estruturando para responder aos novos requerimentos de governança.

.

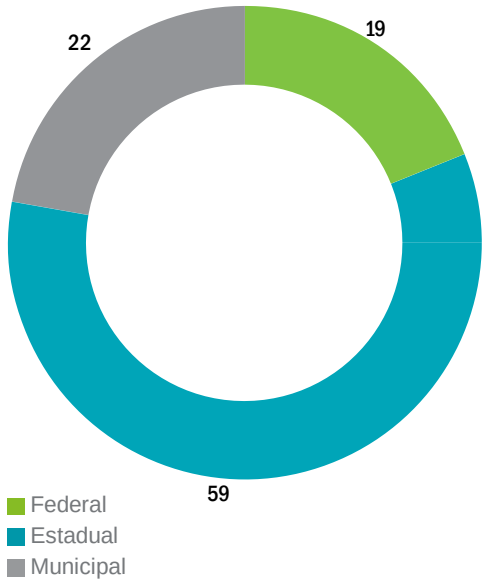
77 empresas participantes

Principais setores de atividade

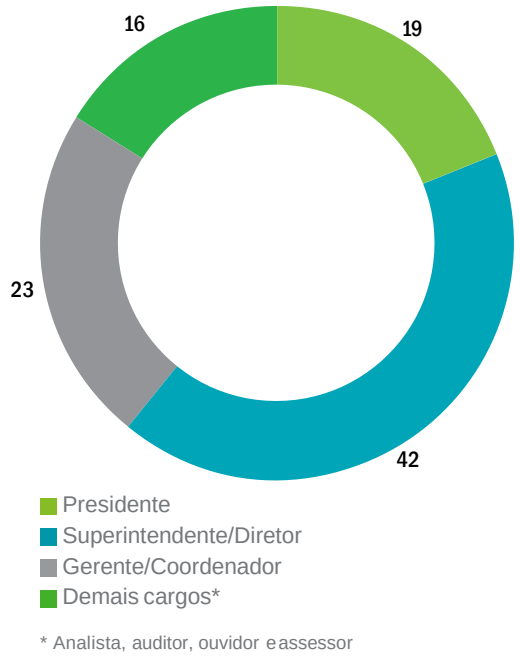
1. Energia/Petróleo e derivados
2. Setor financeiro e securitização
3. Saneamento/Habitação
4. Transporte/Portuário
5. Desenvolvimento regional

Nota: Percentuais de respondentes para cada uma das alternativas respondidas

Esfera de atuação (em %)



Cargo do respondente (em %)



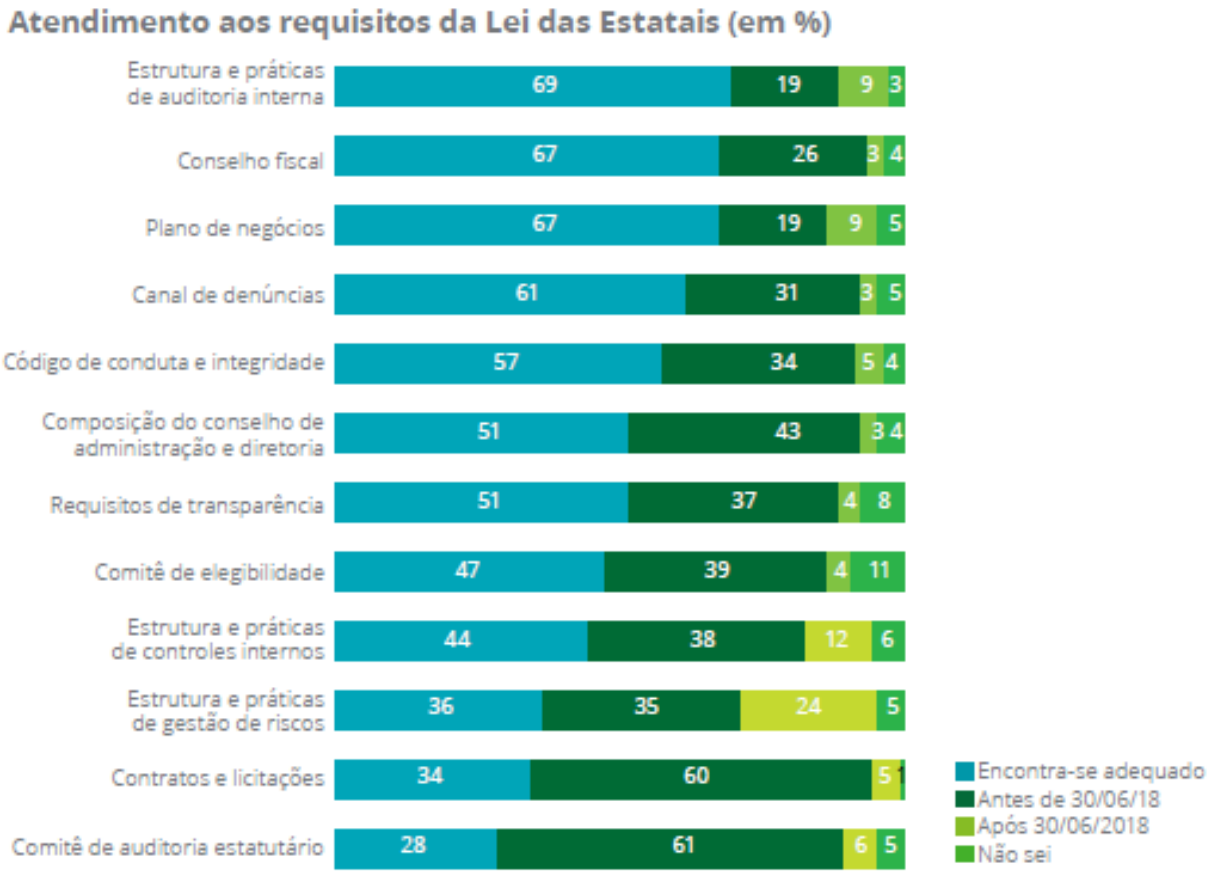
* Analista, auditor, ouvidor e assessor

A pesquisa teve como base respostas coletadas por meio de questionário eletrônico entre dezembro de 2017 e abril de 2018.

Síntese dos resultados da pesquisa Deloitte/IIA Brasil

Expectativas de atendimento aos requisitos

- A aderência do conselho de administração tende a ser cumprida (assembleias ocorrem tipicamente no mês de abril).
- Cerca de 90% estarão adequados em relação à formalização de um plano de negócios (prazo definido como 31/12/2017).
- Principais benefícios esperados: maior alinhamento entre níveis operacionais e executivos e manutenção das diretrizes estratégicas (em caso de mudanças na gestão).
- Cerca de 90 % estarão adequados na adoção de um Canal de Denúncias (facilidade de implementação e custos envolvidos).
- Iniciativas mais complexas ou que envolvem mudanças estruturais têm níveis inferiores de adoção (ex.: estrutura para controles internos e gestão de riscos, comitê de elegibilidade).

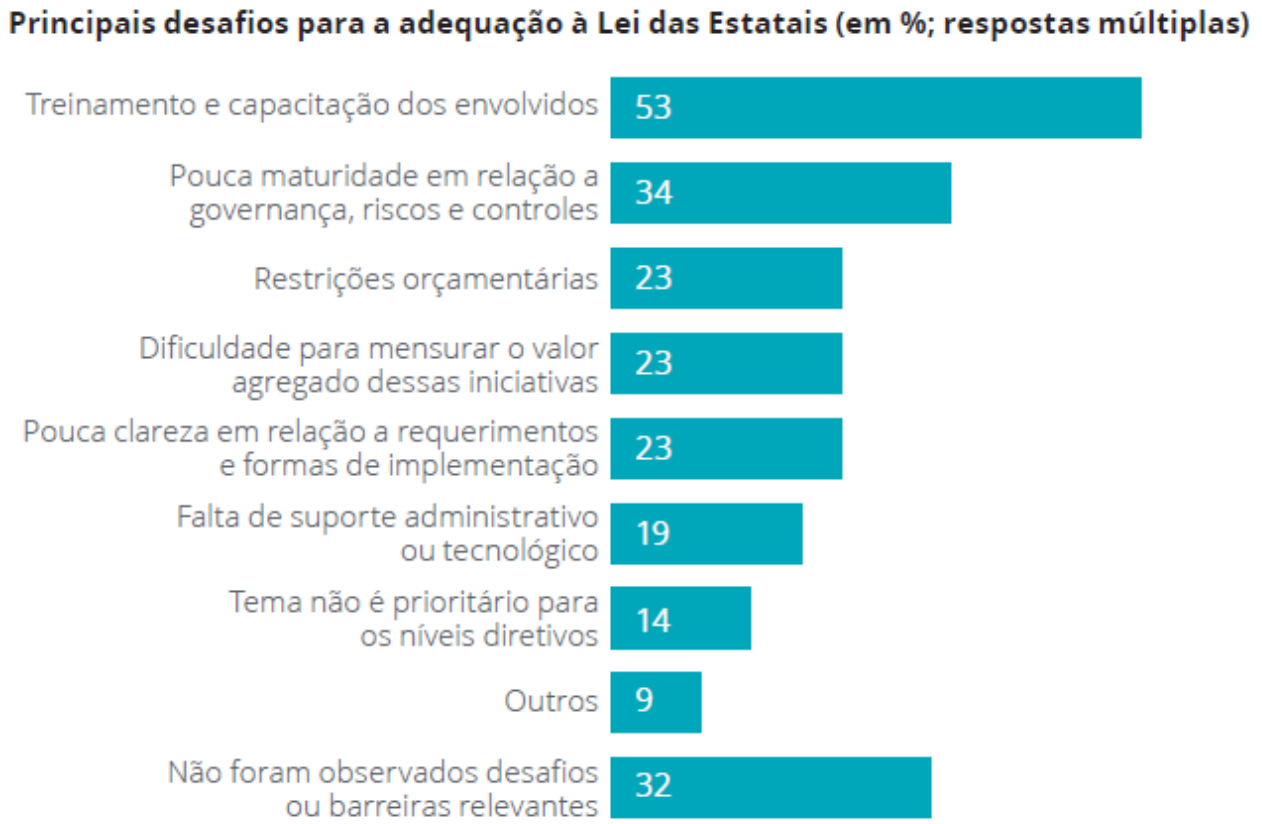


Nota: Percentuais de respondentes para cada uma das alternativas respondidas

Síntese dos resultados da pesquisa Deloitte/IIA Brasil

Principais desafios enfrentados

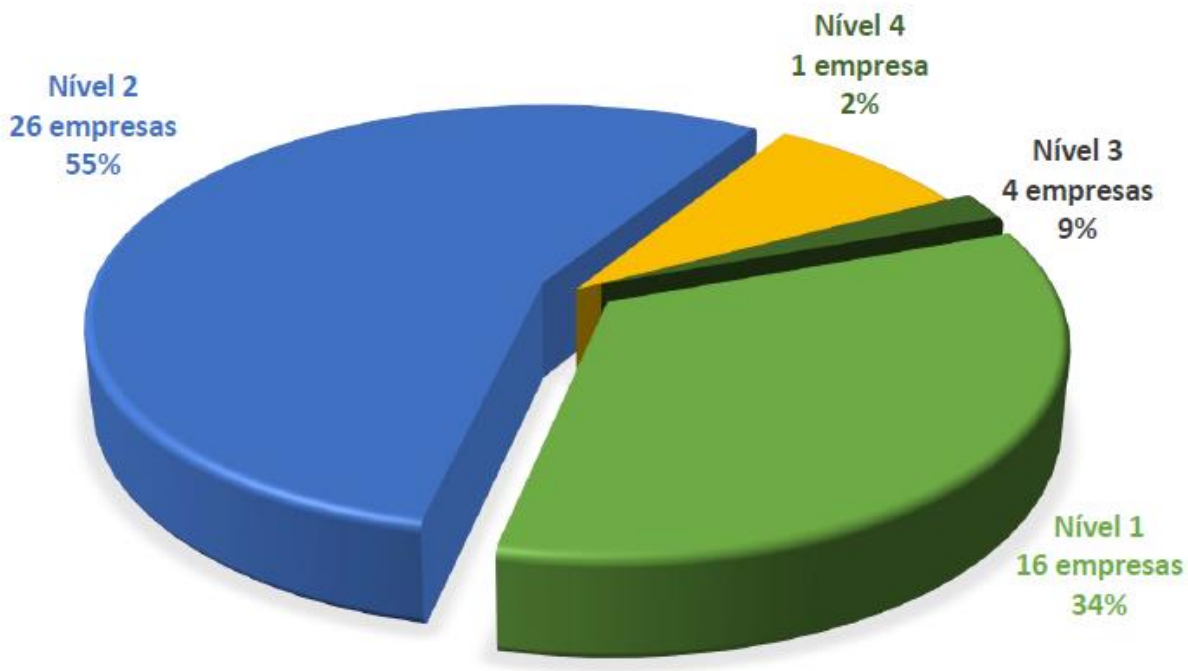
- Treinamento e capacitação dos envolvidos são, com destaque, o principal desafio apresentado por mais da metade das empresas respondentes do estudo.
- Menos de um terço indicou a pouca maturidade da empresa em relação aos temas governança, riscos e controles como entrave.
- Alto percentual (32%) de organizações que declararam não observar desafios ou barreiras relevantes (fator positivo, dada a magnitude das mudanças previstas).



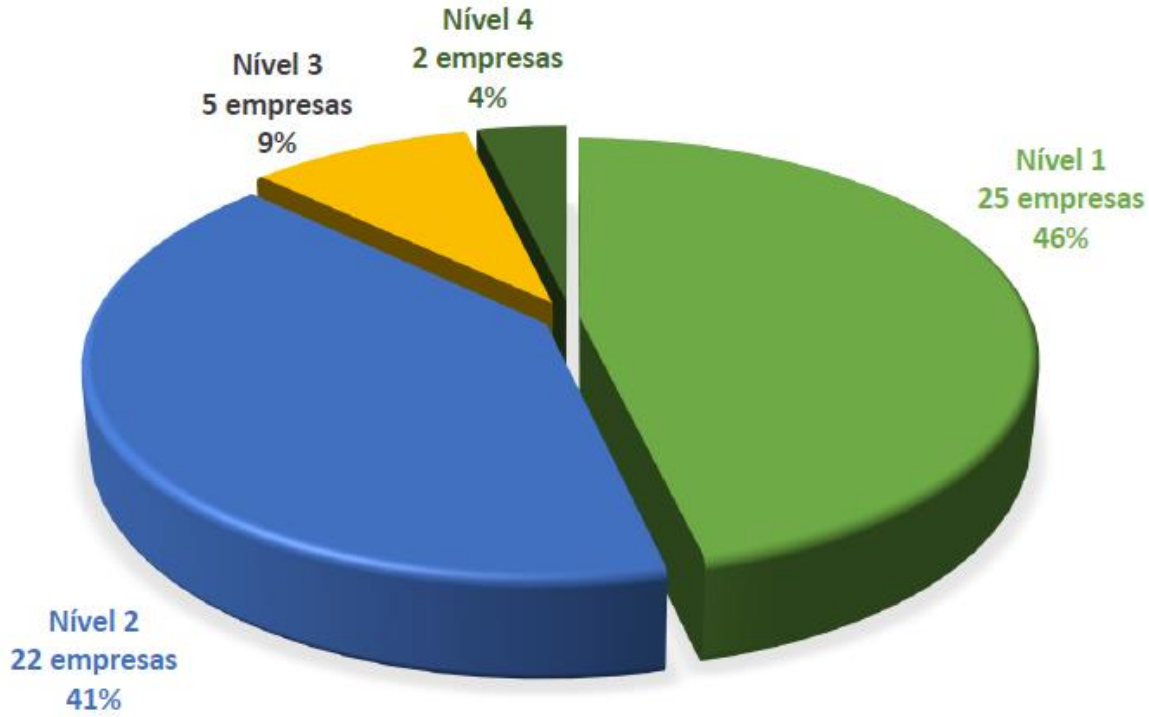
Nota: Percentuais de respondentes para cada uma das alternativas respondidas

IGSEST NÍVEL 1 IGSEST NÍVEL 2 IGSEST NÍVEL 3 IGSEST NÍVEL 4

2º Ciclo



3º Ciclo



As três linhas de defesa das organizações no gerenciamento de riscos e controles

Três Linhas de Defesa das organizações no gerenciamento de riscos e controles

Definição do modelo

Na figura a seguir*, o **modelo das Três Linhas de Defesa** pode ser identificado a partir das responsabilidades e coordenação delegadas a cada ator de uma organização:

(*)Adaptação da Declaração de Posicionamento do IIA: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles. IIA (2013)

Exigência na capacitação de Diretores e Conselheiros

Capacitação de Diretores e Conselheiros

Treinamentos em temas de governança

A lei traz novos parâmetros e exigências quanto à capacitação de Diretores e Conselheiros, os quais devem, anualmente ou após suas nomeações, realizar treinamentos em temas de governança, contemplando:

- ❑ Lei Anticorrupção;
- ❑ Gerenciamento de Riscos;
- ❑ Controles Internos;
- ❑ Legislação Societária e Mercado de Capitais;
- ❑ Divulgação de Informações;
- ❑ Atividades de empresas de públicas e de sociedade de economia mista;
- ❑ Código de Conduta da Companhia

O treinamento pode ser realizado de forma presencial ou por meio de plataformas de ensino à distância (EAD), trazendo maior flexibilidade e aproveitamento para os executivos.

Riscos

O que é Risco?

Definição

Risco é a **possibilidade de ocorrência de um evento** que poderá ter um **impacto no cumprimento dos objetivos** da organização, e que muitas vezes envolve um **elemento de incerteza** relacionado a uma atividade

"Incertezas inerentes a um conjunto de possíveis consequências (ganhos e perdas) que resultam de decisões tomadas diariamente por uma organização."

Fonte: metodologia Deloitte.

Gestão de Riscos

Evitar “versus” gerenciar

<u>Evitar</u> um risco é uma <u>decisão:</u>

- Avaliar a situação e desistir.
- Abandonar um determinado mercado.

<u>Gerenciar</u> um risco é uma <u>atividade contínua:</u>

- Entender os riscos.
- Desenvolver um plano para mitigar a exposição.
- Executar o plano.
- Monitorar a efetividade das ações desse plano.

Dicionário de Riscos

ESTRATÉGICO

Governança			Modelo de Negócios				Político e Econômico
1. Compliance	3. Reputação e Imagem	5. Estrutura Organizacional	6. Planejamento e orçamento	8. Investimento em projetos	10. Continuidade dos negócios	12. Parcerias	13. Cenário Político e Econômico
2. Conduta antiética/ Fraude	4. Relacionamento com Acionistas		7. Inovação e Tecnologia	9. Satisfação do Cliente	11. Mercado e Concorrência		

FINANCEIRO

Crédito	Mercado	Liquidez
14. Inadimplência	16. Taxa de Juros	18. Fluxo de Caixa
15. Concentração	17. Câmbio	

OPERACIONAL

Processo		Pessoal	Informação e Tecnologia	Meio Ambiente
19. Obrigações Contratuais e Terceirização	21. Fornecimento	23. Capacitação	25. Segurança da Informação	28. Licenciamento, Resíduos, Emissões e Efluentes
20. Capacidade e Eficiência	22. Perda e/ou Obsolescência	24. Retenção de talentos	26. Disponibilidade / Infraestrutura	29. Saúde e Segurança
			27. Integridade das Informações	

LEGAL

30. Trabalhista
31. Tributário
32. Civil
33. Regulamentar

Gestão de Riscos

Definição – Gerenciamento de Risco

Gerenciamento de Riscos:

***Exceto se a operação, atividade ou negócio que o risco está relacionado deixarem de existir.**

Evitar um risco é uma decisão. Já o gerenciamento de um risco é uma atividade contínua que compreende o entendimento da abrangência dos riscos, o desenvolvimento de um plano de mitigação da exposição ao risco, execução do plano e o monitoramento da efetividade das ações implementadas.

Gestão de Riscos

Definição – Avaliação de riscos

Identificação e Avaliação de riscos:

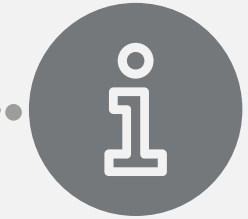
Para a identificação e avaliação dos riscos de um processo, deve-se executar as seguintes atividades:

Identificar:

Identificação do **fluxo, regras, políticas, procedimentos** e **responsabilidades** do processo

Avaliar:

Avaliação da **eficácia** da estrutura de **controles existente**, e identificação de riscos que podem resultar em **perdas** ou **custos de oportunidade**.



Responder:

Identificação e análise de **oportunidades de melhoria** do processo e respectivas **recomendações sistêmicas**, **mudanças de processos**, e **indicadores de riscos.**

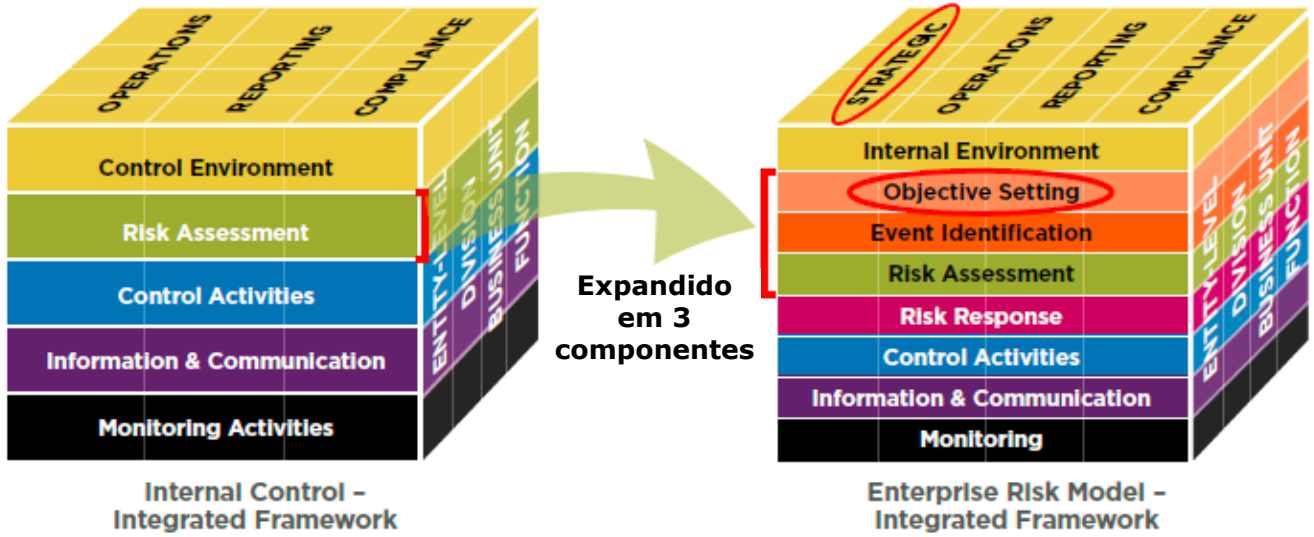
Gestão de Riscos e Controles

Implementação de uma estrutura de gestão de risco - Padrões internacionais de combate à fraude

Quais são eles?

COSO®ERM

Em 1992, o ***Committee of Sponsoring Organizations of the Treadway Commission*** **(COSO®)** publicou o seu **estudo sobre controle interno** (*Internal Control – Integrated Framework)* que foi aceito globalmente como sendo a **estrutura adequada** para ser aplicada nas organizações de forma a **conduzir o processo de controles internos de forma eficiente e eficaz**.



Internal Control – Integrated Framework

Enterprise Risk Model – Integrated Framework

Após alguns anos, o **COSO®** revisou esta estrutura e , com o objetivo de **endereçar as subestruturas no ambiente de negócios**, que são globais e muito mais complexos.

O **COSO®ERM** busca incorporar e atender as necessidades de **controle interno** em seu conteúdo quanto para adotar um processo completo de **gerenciamento de riscos**.

Gestão de Riscos e Controles

Implementação de uma estrutura de gestão de risco - Padrões internacionais de combate à fraude

Para a gestão de riscos, o COSO®ERM expandiu seus componentes, incluindo: Fixação de Objetivos; Identificação de Eventos; Resposta aos riscos estratégia, conforme figura abaixo:

Governança e Cultura

A governança dá o tom da organização, reforçando a importância e instituindo responsabilidades de supervisão sobre o gerenciamento de riscos corporativos. A cultura diz respeito a valores éticos, a comportamentos esperados e ao entendimento do risco em toda a entidade

Estratégia e definição de objetivos

Gerenciamento de riscos corporativos, estratégia e definição de objetivos atuam juntos no processo de planejamento estratégico. O apetite a risco é estabelecido e alinhado com a estratégia; os objetivos de negócio colocam a estratégia em prática e, ao mesmo tempo, servem como base para identificar, avaliar e responder riscos.

Performance

os riscos que podem impactar a realização da estratégia e dos objetivos de negócios precisam ser identificados e avaliados. Os riscos são priorizados com base no grau de severidade, no contexto do apetite a risco. A organização determina as respostas aos riscos e o total dos riscos assumidos.

Análise e Revisão

ao analisar a sua performance, a organização tem a oportunidade de refletir sobre até que ponto os componentes do gerenciamento de riscos corporativos estão funcionando bem ao longo do tempo e no contexto de mudanças relevantes, e quais correções são necessárias

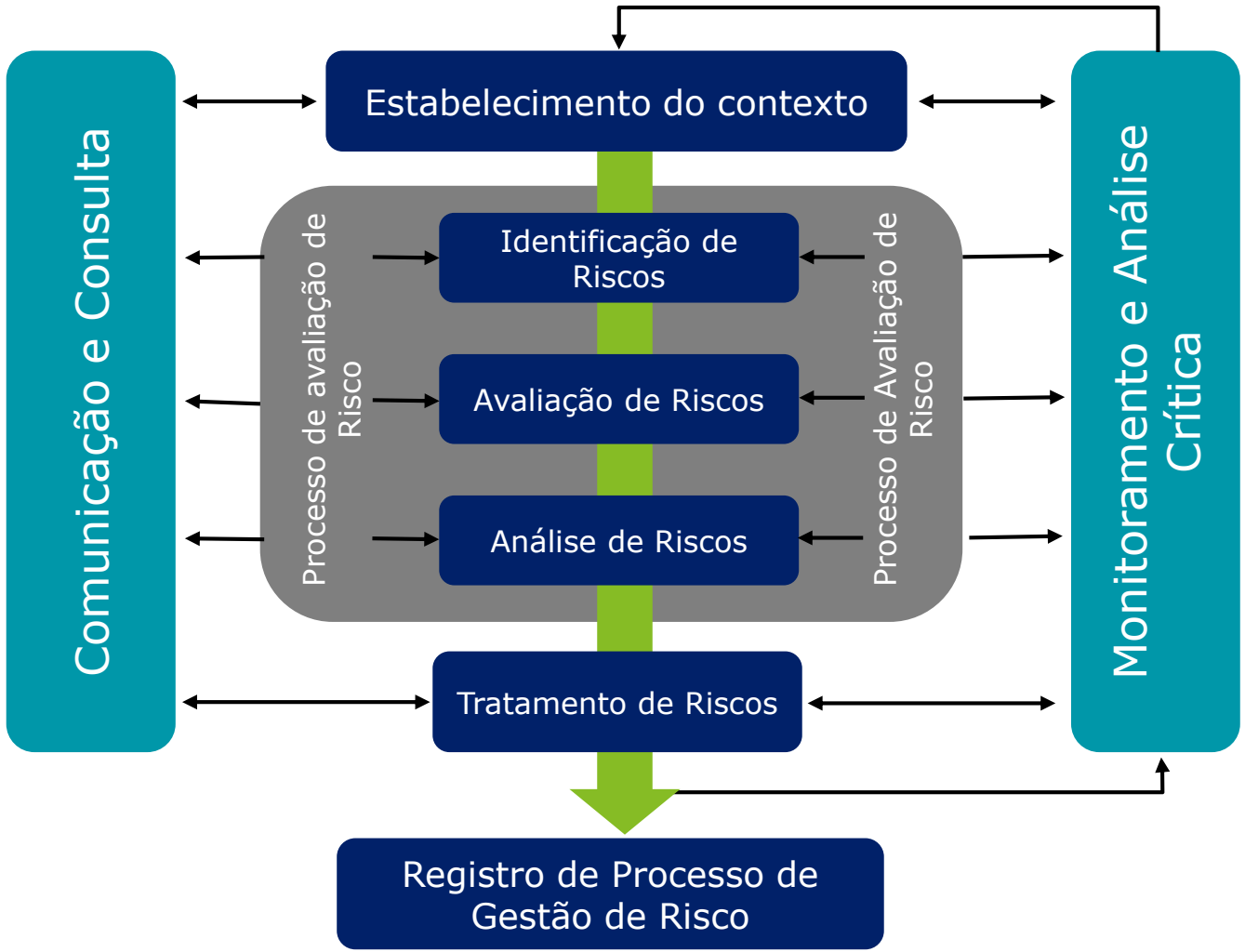
Informação, comunicação e divulgação

O gerenciamento de riscos corporativos demanda um processo contínuo de obtenção e compartilhamento de informações precisas, provenientes de fontes internas e externas, originadas das mais diversas camadas e processos de negócios da organização

Gestão de Riscos e Controles

Padrões Internacionais adotados pelo TCU

ISO 31000 (2015)



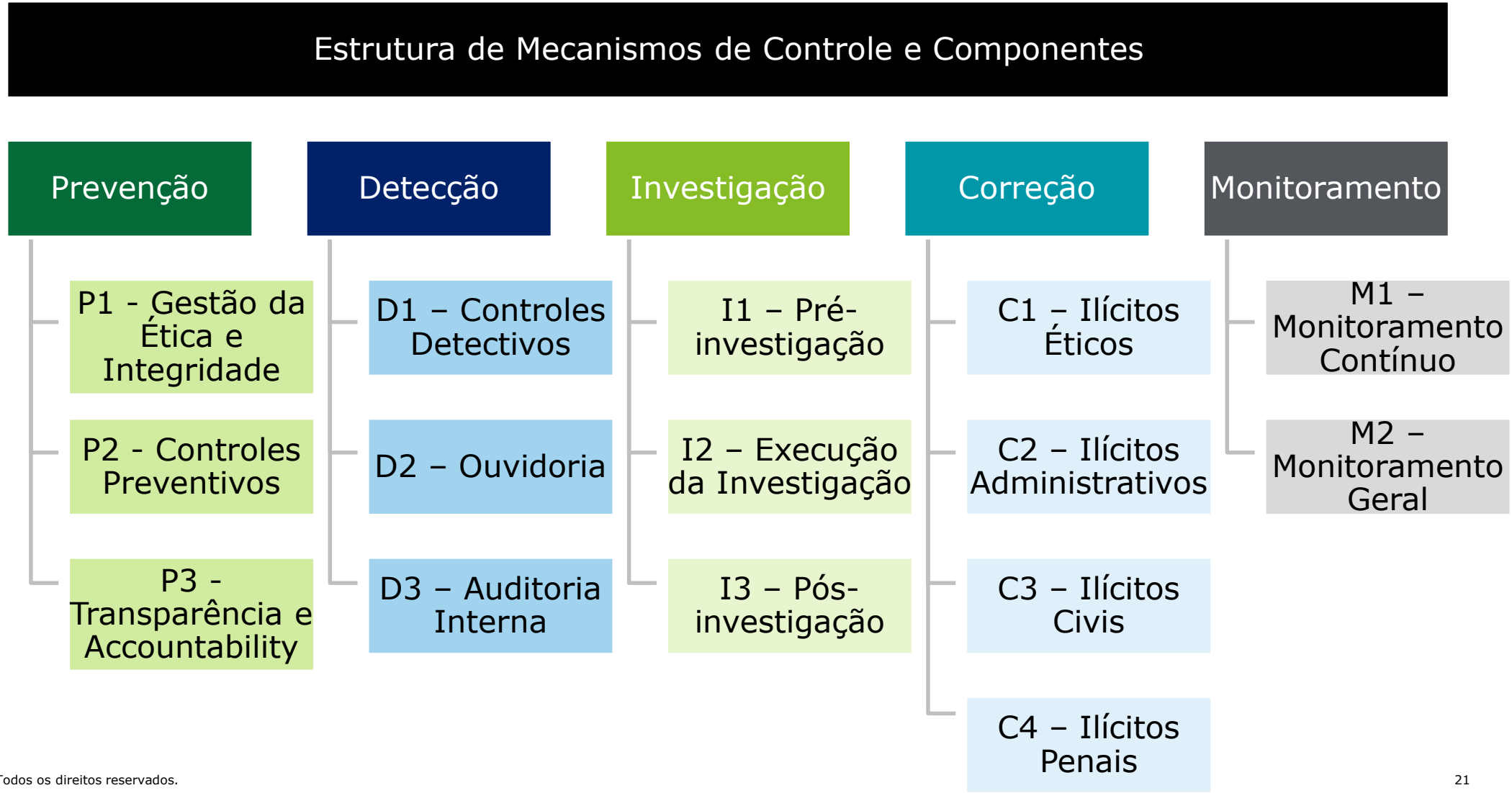
Fonte: Referencial de Combate à Fraude e à Corrupção - TCU

Práticas de Governança
Setor Público

Práticas de Governança

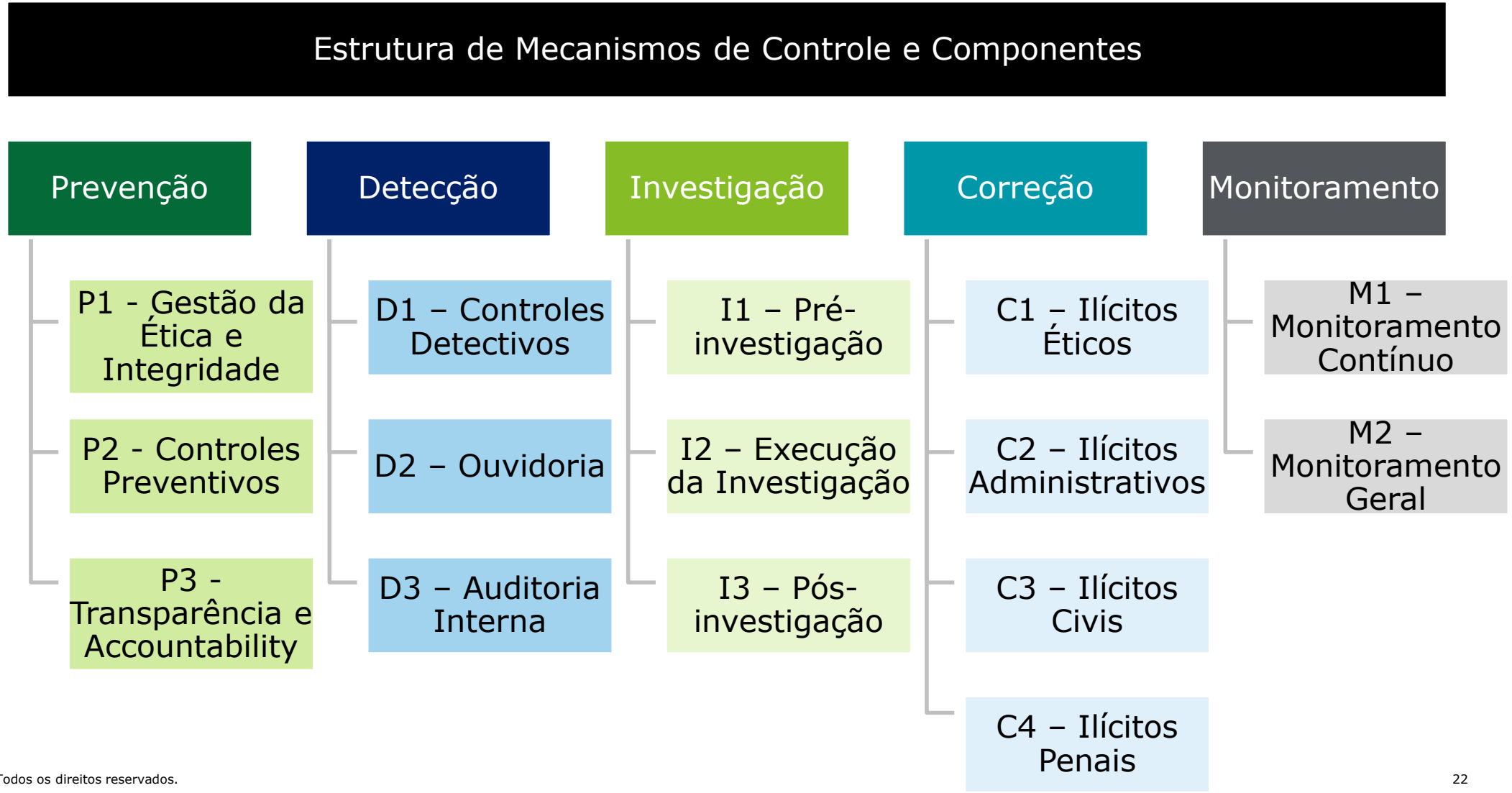
Dos mecanismos de controle

O TCU elaborou uma estrutura de mecanismos de controles e os seus componentes, conforme imagem ao lado, a fim de orientar os órgãos a se estruturar conforme melhores práticas utilizadas pelos Governos.



Práticas de Governança

Dos mecanismos de controle



Práticas de Governança

Prevenção

Prevenção

- P1 - Gestão da Ética e Integridade
- P2 - Controles Preventivos
- P3 - Transparência e Accountability*

A prevenção **evita a ocorrência de fraude e corrupção** e, usualmente, é **mais barata** que medidas corretivas.

A **mais eficiente e proativa atitude** para preservar os recursos públicos é prevenir que sejam desviados dos seus propósitos.

O risco de fraude e corrupção deve ser **considerado já nas etapas iniciais** de elaboração de políticas, programas, atividades ou processos públicos, para que medidas preventivas sejam concebidas desde a origem.

**Accountability* refere-se à obrigação que têm as pessoas ou entidades às quais se tenham confiado recursos, incluídas as empresas e organizações públicas, de assumir as responsabilidades de ordem fiscal.

Práticas de Governança

Prevenção

*Controle social é a **integração da sociedade com a administração pública com a finalidade de solucionar problemas** e as deficiências sociais com mais eficiência e empenho.*

FONTE: Cartilha de Orientação de Controle Social, Controladoria-Geral da União (CGU).

Práticas de Governança

Detecção

- Detecção
  - D1 – Controles Detectivos
  - D2 – Ouvidoria
  - D3 – Auditoria Interna

Um forte fator de dissuasão da fraude e corrupção é a consciência em todos de que **mecanismos detectivos estão em vigor**, o que acaba tendo o efeito de prevenção. Entretanto, enquanto na prevenção as medidas são aparentes, na detecção as medidas são, por natureza, ocultas, ou seja, as partes interessadas não sabem.

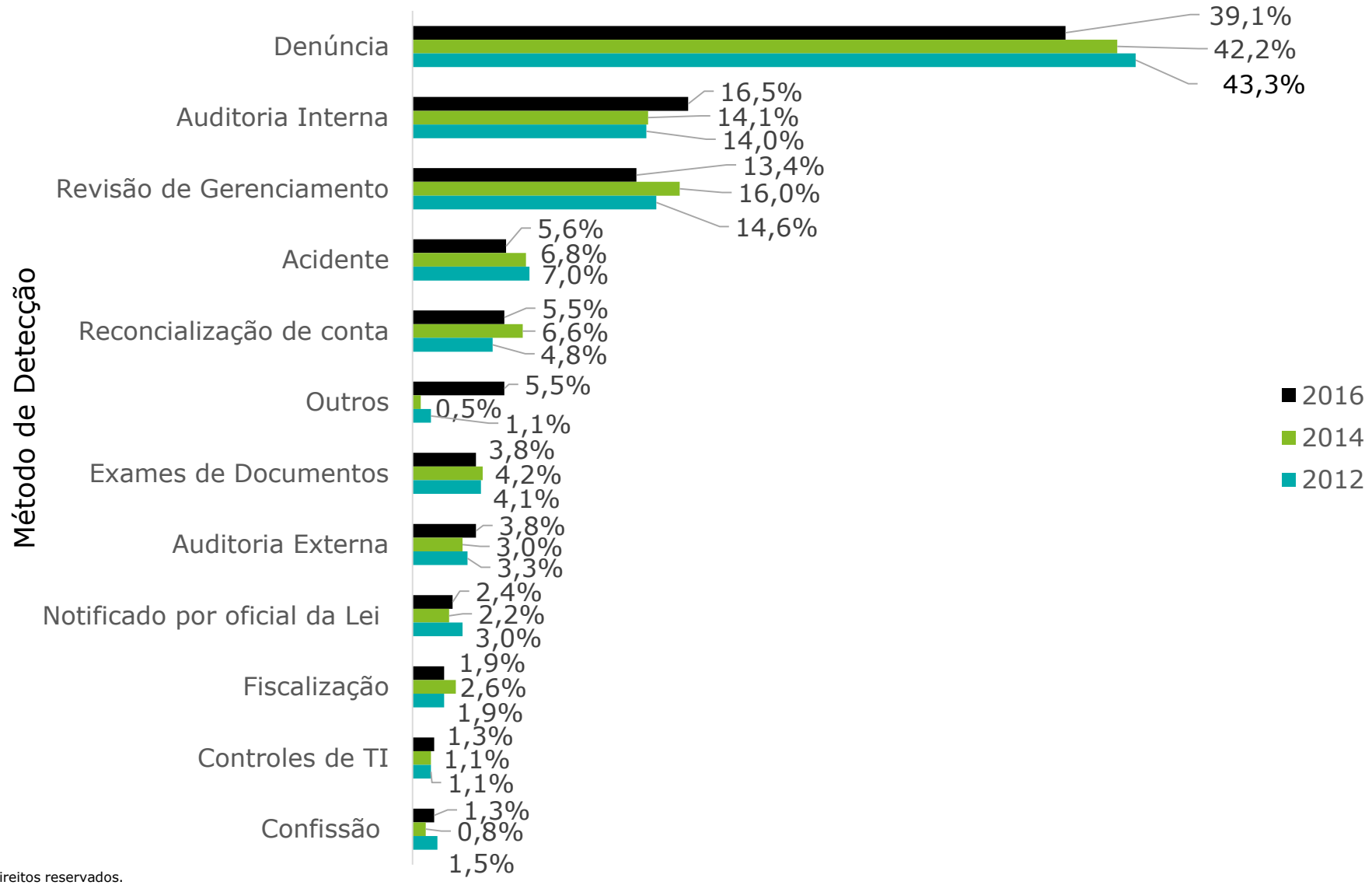
Identificação e Prevenção à Fraude

ACFE 2016 Report to the Nation on Occupational Fraud & Abuse

- ✓ **81,7% das empresas fraudadas** apresentam Auditoria Externa, contudo a detecção de fraude por esse controle foi de **4% dos casos analisados**.
- ✓ **Denúncia é o método mais comum para detecção da fraude (39,1%)**, mas apenas 60,1% das empresas possuem "hotline" (ex.canal de ouvidoria) e 12% oferecem algum tipo de benefício para o denunciante.
- ✓ Empresas proativas com **"monitoramento de informação" (ex. Indicadores, data mining, etc)** são mais efetivas na prevenção:
  - ✓ Redução de 54% em perdas com fraude.
  - ✓ 50% menos duradoura.

Identificação e Prevenção à Fraude

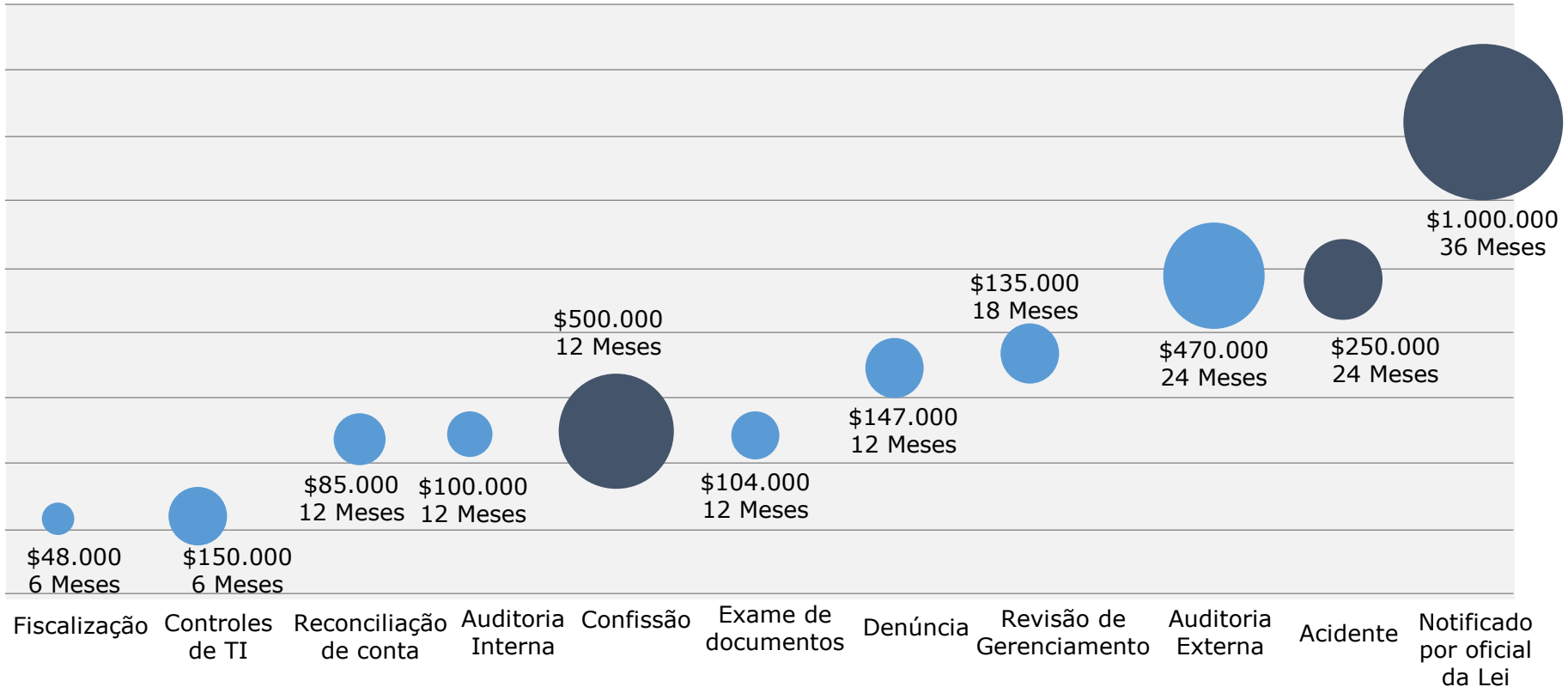
Método de Identificação da Fraude



Fonte: ACFE 2016 Report to the Nation on Occupational Fraud & Abuse

Identificação e Prevenção à Fraude

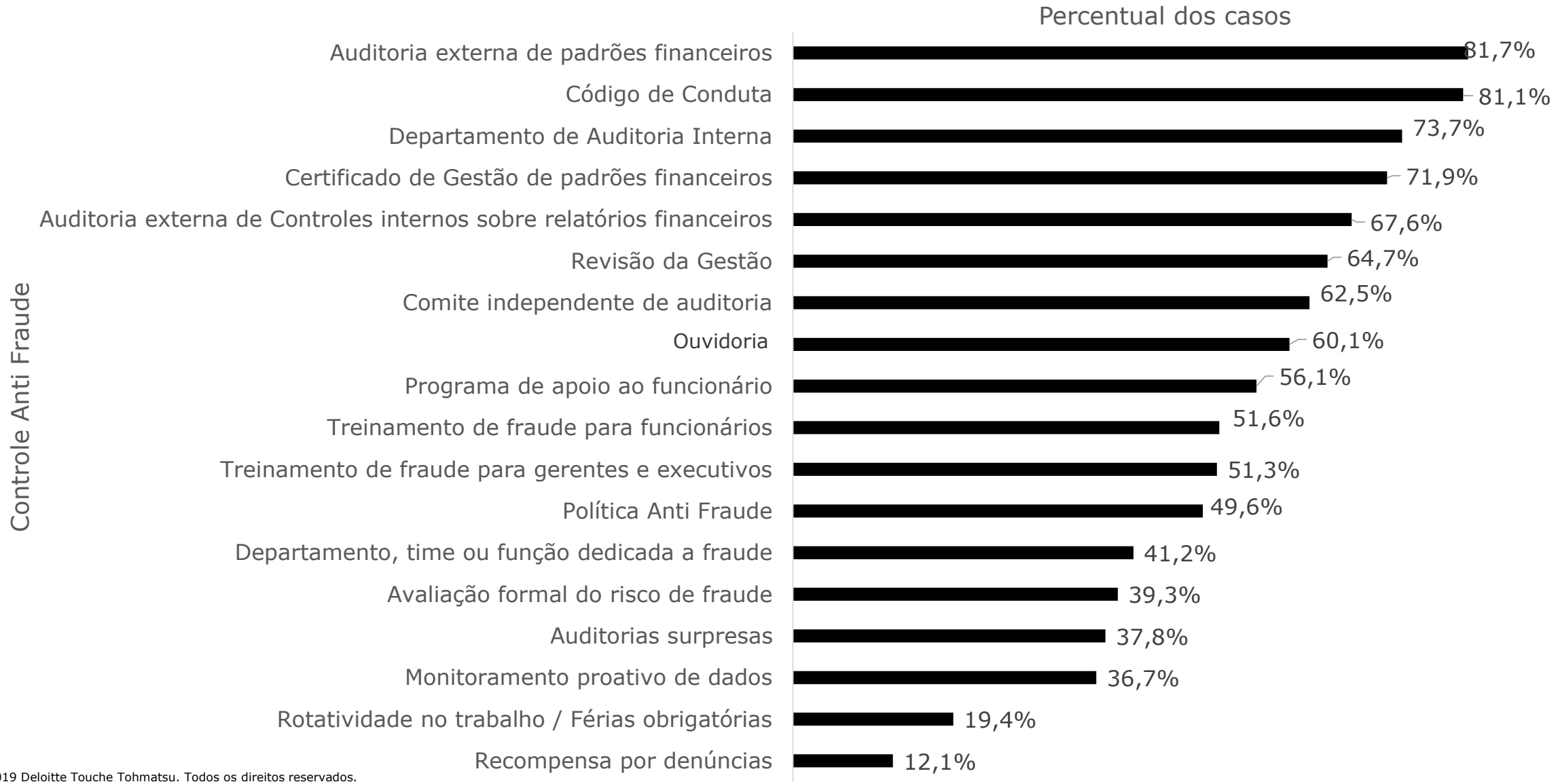
Método de Identificação Vs. Média de perda e duração da Fraude



Fonte: ACFE 2016 Report to the Nation on Occupational Fraud & Abuse

Identificação e Prevenção à Fraude

Controles usualmente utilizados pelas empresas



Fonte: ACFE 2016 Report to the Nation on Occupational Fraud & Abuse

Identificação e Prevenção à Fraude

O que não fazer


FOLHA DE S.PAULO

ENTRAR

Governo de SP processa servidores que denunciaram irregularidades na gestão

Estado não prevê proteção legal a funcionários que apontem problemas a órgãos investigativos

Práticas de Governança

Controles detectivos

Programas de denúncia tornam-se parte do DNA de conformidade
(Matéria: Whistleblowing Programs Become Part of Compliance DNA*)

A assistência e a informação de um denunciante que conhece possíveis violações da lei de valores mobiliários podem estar entre as **armas mais poderosas do arsenal de aplicação da lei da Securities and Exchange Commission**. Através do seu conhecimento das circunstâncias e dos indivíduos envolvidos, os denunciantes podem ajudar a Comissão a identificar possíveis fraudes e outras violações muito antes do que de outra forma poderia ser possível.

Isso permite que a Comissão minimize os danos para os investidores, preserve melhor a integridade dos mercados de capitais dos Estados Unidos e responsabilize mais rapidamente os responsáveis por conduta ilegal.

A Comissão está autorizada pelo Congresso a fornecer prêmios monetários a pessoas elegíveis que apresentam informações originais de alta qualidade que levam a uma ação de execução da Comissão em que são ordenadas mais de US $ 1.000.000 em sanções. O intervalo para prêmios é entre 10% e 30% do dinheiro arrecadado

Fonte: The Wall Street Journal – Risk & Compliance Journal

Práticas de Governança

Investigação

Investigação

I1 – Pré-investigação

- **Desenvolver plano de resposta à fraude e corrupção**
- **Realizar avaliação inicial do incidente**
- **Estabelecer equipe de investigação**
- **Estabelecer parcerias com outras organizações**

I2 – Execução da Investigação

- Desenvolver plano de investigação
- Estabelecer a confidencialidade da investigação
- Investigar os atos de fraude e corrupção
- Realizar entrevistas eficazes
- Examinar documentos

I3 – Pós-investigação

Elaboração do relatório de investigação.

Boa Prática: Revisar controles internos após a ocorrência de uma fraude e corrupção.

Práticas de Governança

Correção

Correção

- C1 – Ilícitos Éticos
  - Procedimento ético preliminar.
  - Processo de apuração ética e de integridade.
- C2 – Ilícitos Administrativos
- C3 – Ilícitos Civis
- C4 – Ilícitos Penais

Procedimento para averiguação dos fatos com objetivo de confirmar a existência da transgressão e identificar a sua suposta autoria.

Com base no relatório produzido, a comissão decidirá se:

- Arquiva o processo;
- Propõe um acordo de conduta com o investigado;
- Converte em um processo de apuração ética.

Práticas de Governança

Monitoramento

Monitoramento

- M1 – Monitoramento Contínuo
- M2 – Monitoramento Geral

Sobre a Deloitte.

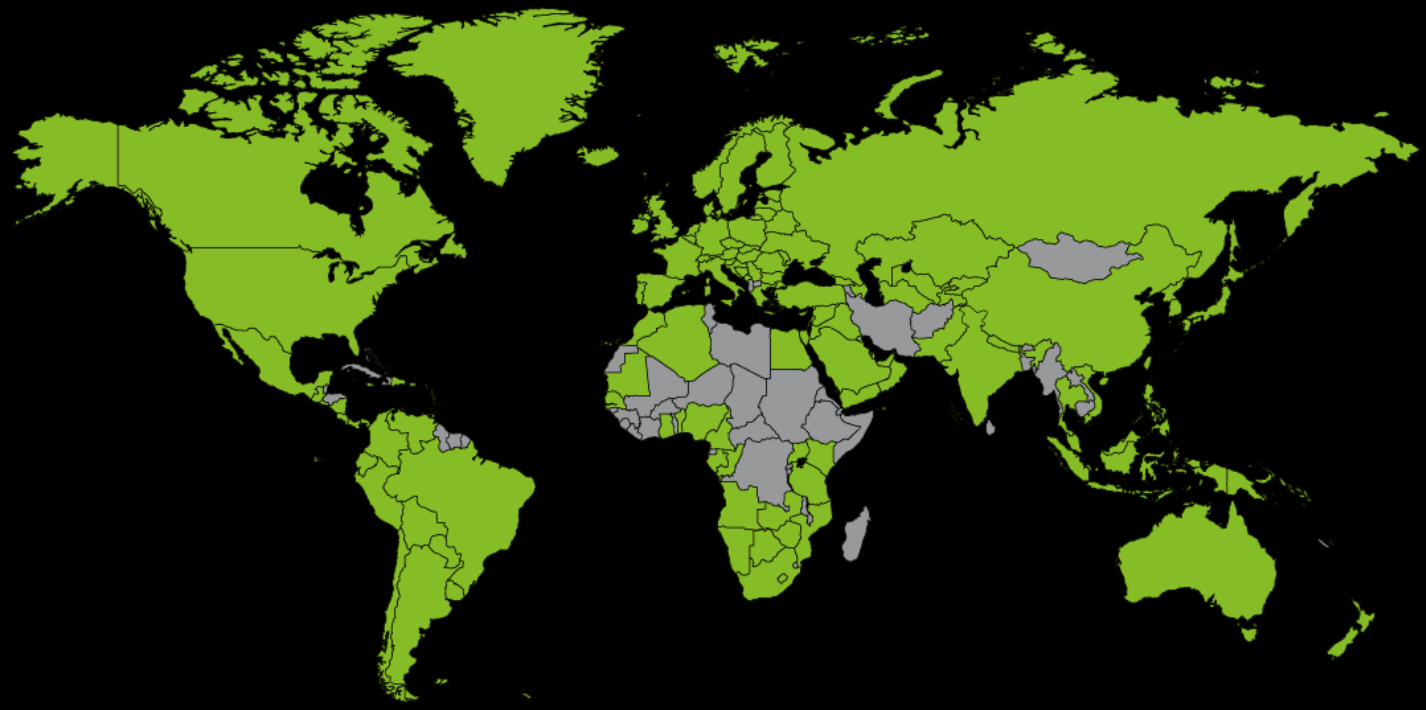
Institucional

Presença mundial

São 244 mil profissionais atuando em mais de 150 países, destacados em verde no mapa.

Faturamento global de US$36,8 bilhões no ano fiscal de 2016, com crescimento de 9,5% em relação a 2015.

Atendemos a 83% das 500 maiores empresas do mundo, de todos os setores econômicos que figuram na lista da “Global Fortune 500”.*



*Revista Global Fortune 2015.

Institucional

Presença nacional

No Brasil, são cerca de 5.500 profissionais, 170 sócios e 12 escritórios nos principais centros econômicos do País.*

Contamos com 3,5 mil clientes ativos, de todos os setores da economia e regiões do país.

*São Paulo, Brasília, Belo Horizonte, Campinas, Curitiba, Fortaleza, Joinville, Porto Alegre, Recife, Ribeirão Preto, Rio de Janeiro e Salvador.

Nossos Contatos

Edson Cedraz

Sócio – Consultoria
Fone: (81) 3464-8127
E-mail: ecedraz@deloitte.com

Diego Hudson

Gerente – Consultoria
Fone: (81) 3464-8127
Celular: (81) 99168-3101
E-mail: diehudson@deloitte.com

Deloitte.

© 2019 Deloitte Touche Tohmatsu. Todos os direitos reservados.