Modernizando a avaliação dos riscos para a integridade no Brasil

RUMO A UMA ABORDAGEM COMPORTAMENTAL E ORIENTADA POR DADOS



OCDE

Modernizando a avaliação dos riscos para a integridade no Brasil

RUMO A UMA ABORDAGEM COMPORTAMENTAL E ORIENTADA POR DADOS

OCDE
POLÍTICAS MELHORES
PARA UMA VIDA MELHOR

Este documento e qualquer mapa aqui incluído foi elaborado sem prejuízo do status ou soberania de qualquer território, da delimitação de limites e fronteiras internacionais e do nome do território, cidade ou área.

Por favor, cite esta publicação como:
OECD (2022), *Modernizando a avaliação dos riscos para a integridade no Brasil: Rumo a uma abordagem comportamental e orientada por dados*, OECD Publishing, Paris, https://doi.org/10.1787/61d7fc60-pt.

ISBN 978-92-64-45848-2 (pdf)
ISBN 978-92-64-54897-8 (HTML)
ISBN 978-92-64-80315-2 (epub)

Fotografias: Capa © Marcello Casal Jr - Agência Brasil, Brasília-DF

As erratas das publicações da OCDE podem ser acessadas online em: www.oecd.org/about/publishing/corrigenda.htm.

© OCDE 2022

O uso do conteúdo do presente trabalho, tanto em formato digital quanto impresso, é regido pelos termos e condições seguintes: https://www.oecd.org/termsandconditions.

Prefácio

Para que as políticas de integridade sejam relevantes, eficientes e eficazes, os riscos para a integridade necessitam ser adequadamente identificados, avaliados e minimizados. De acordo com a *Recomendação da OCDE sobre Integridade Pública*, os riscos para a integridade pública incluem não somente corrupção e fraude, mas também práticas que, embora não íntegras, podem não ser ilegais. Não obstante a importância da gestão dos riscos para a integridade, muitos países enfrentam consideráveis desafios à implementação de uma cultura de gestão de riscos para a integridade em suas administrações públicas. De fato, os gestores públicos nem sempre estão suficientemente cientes do valor da gestão de riscos.

A compreensão sobre a importância da gestão de riscos requer um claro entendimento dos valores e objetivos da função pública exercida. Tal entendimento pode ser difícil de alcançar se não houver objetivos claros, uma cultura de resultados ou suficiente prestação de contas, sobretudo em vista da dificuldade de quantificar o impacto e a produtividade do setor público. Além disso, os administradores muitas vezes carecem da capacidade, conhecimento e apoio necessários à efetiva gestão dos riscos para a integridade.

Muitos desses desafios se aplicam ao Brasil, país que, por meio de sua Controladoria-Geral da União (CGU), tem procurado fortalecer políticas, métodos e instituições no sentido de promover a integridade no Executivo Federal. O presente relatório é parte de um projeto de apoio da OCDE aos esforços da CGU, instância que lidera as políticas de integridade em nível federal. O projeto possui três componentes: uma revisão da metodologia de avaliação de riscos para a integridade; a aplicação de lições de ciência comportamental à integridade pública; e o fortalecimento das Unidades de Gestão de Integridade (UGI) no âmbito do Sistema de Integridade Pública do Poder Executivo Federal (SIPEF).

Este relatório contribui para o trabalho da OCDE no apoio aos países para a implementação efetiva da *Recomendação da OCDE sobre Integridade Pública*. Ele oferece uma análise e um conjunto de recomendações concretas para a melhoria da implementação da gestão de riscos para a integridade no Executivo Federal brasileiro. O presente documento também fornece subsídios para a *Revisão da OCDE sobre Integridade no Brasil*.

A revisão foi aprovada pelo Grupo de Trabalho de Altos Funcionários sobre Integridade Pública da OCDE (SPIO) em 13 de abril de 2022 e tornada pública pelo Comitê de Governança Pública em 5 de maio de 2022.

Agradecimentos

Este relatório foi elaborado pela Divisão de Integridade no Setor Público, da Diretoria de Governança Pública da OCDE, sob a liderança de Elsa Pilichowski, Diretora de Governança Pública da OCDE, e Julio Bacio Terracino, Chefe da Divisão de Integridade no Setor Público. O relatório foi coordenado e redigido por Frédéric Boehm e Camila Gomes Gomes. Gavin Ugale ofereceu inestimáveis orientações, apoio e subsídios para a análise e as recomendações. Estela Souto apoiou a pesquisa preliminar contextual e o desenho do questionário. Meral Gedik forneceu assistência editorial e administrativa. A tradução do relatório para o português foi realizada por Angela Martinazzo e revisado por Carolina Souto Carballido.

A OCDE agradece ao Ministro da Controladoria-Geral da União (CGU), Wagner de Campos Rosário, assim como à sua equipe, em particular à Secretaria de Transparência e Prevenção da Corrupção (STPC), representada por Roberto Cesar de Oliveira Viegas e Claudia Taya, e à Diretoria de Promoção da Integridade (DPI), representada por Pedro Ruske Freitas, Carolina Souto Carballido e Allison Roberto Mazzuchelli Rodrigues, pelo apoio na organização da averiguação virtual e pelas várias e frutíferas discussões sobre os achados preliminares e recomendações ao longo do projeto.

A OCDE também gostaria de agradecer aos indivíduos e organizações que contribuíram no processo e ofereceram valiosas informações para a elaboração do relatório. Em particular, a OCDE é grata pelas devolutivas e informações compartilhadas pela Ouvidoria-Geral da União, pela Secretaria Federal de Controle Interno da CGU e pelas Unidades de Gestão da Integridade das seguintes entidades federais que participaram do Grupo Focal e das entrevistas bilaterais: Agência Nacional de Telecomunicações; Departamento Nacional de Infraestrutura de Transportes; Ministério da Cidadania; Ministério da Mulher, da Família e dos Direitos Humanos; Ministério da Agricultura, Pecuária e Abastecimento; Ministério da Educação; Fundação Universidade Federal do Maranhão; Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina; Agência Nacional do Cinema; Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis; Ministério da Infraestrutura; Ministério do Turismo; Secretaria-Geral da Presidência da República; Fundação Nacional de Saúde; Superintendência de Desenvolvimento do Centro-Oeste; Ministério da Economia; e Controladoria-Geral da União. Finalmente, a OCDE agradece às 30 Unidades de Gestão da Integridade que responderam ao questionário enviado em 2020.

Sumário

Prefácio 3

Agradecimentos 4

Sumário executivo 7

1 Gestão de riscos para a integridade no Executivo Federal brasileiro 9
Gestão de riscos para a integridade: a base para políticas eficientes de integridade 10
Gestão de riscos para a integridade no Poder Executivo Federal brasileiro 11

2 Os três caminhos para fortalecer as avaliações de riscos para a integridade no Executivo Federal brasileiro 18
Desmistificar e simplificar as avaliações qualitativas de riscos para a integridade 19
Avançar na gestão de riscos para a integridade por meio do uso de dados e de ferramentas analíticas 24
Fortalecer o apoio organizacional para a gestão de riscos para a integridade e capacitar os gestores públicos 29

Referências 31

FIGURAS

Figura 2.1. Os três passos da gestão de riscos para a integridade 19
Figura 2.2. A teoria da mudança em uma interface de gestão de riscos para a integridade 24
Figura 2.3. O papel da CGU, das UGIs e dos líderes em integridade na promoção de culturas de gestão de riscos para a integridade no Executivo Federal brasileiro 30

TABELAS

Tabela 1.1. Matriz de riscos para a integridade com 4x4 níveis 14

Acompanhe as publicações da OCDE por:





http://twitter.com/OECD_Pubs



http://www.facebook.com/OECDPublications



http://www.linkedin.com/groups/OECD-Publications-4645871



http://www.youtube.com/oecdilibrary



http://www.oecd.org/oecddirect/

Sumário executivo

A gestão de riscos está no cerne de qualquer estratégia ou abordagem que vise assegurar e promover a integridade pública. No setor público, as estruturas normativas e as políticas de gestão de riscos geralmente se encontram alinhadas aos padrões internacionais; todavia, a efetiva incorporação de marcos de gestão de risco à prática cotidiana muitas vezes demora a ocorrer. A gestão dos riscos para a integridade pode representar um desafio ainda maior e mais complicado, uma vez que corrupção e fraude são tópicos sensíveis e complexos.

No Executivo Federal brasileiro, a gestão dos riscos para a integridade tornou-se obrigatória para todas as entidades públicas em 2017. A gestão dos riscos para a integridade é um dos elementos centrais dos Programas de Integridade e dos Planos de Integridade estabelecidos desde 2017 em todos as 186 órgãos e entidades da Administração Federal direta, autárquica e fundacional. Desde 2021, o Sistema de Integridade Pública do Poder Executivo Federal (SIPEF) avança na institucionalização e consolidação dos Programas de Integridade, incluindo a exigência de assegurar uma efetiva gestão dos riscos para a integridade. Este relatório revisa a metodologia utilizada para identificar e avaliar riscos para a integridade no Brasil e oferece recomendações concretas para o fortalecimento da atual abordagem.

Principais achados

Em 2018, a Controladoria-Geral da União (CGU), órgão central do SIPEF, lançou o *Guia Prático de Gestão de Riscos para a Integridade*, destinado a orientar as entidades federais. O documento reforça a importância da gestão dos riscos para a integridade e fornece diretrizes para sua implementação, incluindo passo a passos concretos, assim como análises de situações e exemplos de riscos para a integridade transversais. No âmbito das entidades federais, as Unidades de Gestão da Integridade (UGI) têm um papel fundamental em coordenar e apoiar a gestão de riscos para a integridade, atuando como uma “segunda linha de defesa”.

Apesar da existência desse sólido arcabouço sobre gestão de riscos para a integridade, o Brasil ainda enfrenta significativos desafios para a sua implementação:

- Embora algumas instituições públicas estejam mais adiantadas que outras, a maioria das instituições públicas do Executivo Federal brasileiro ainda se encontra em um estágio inicial no que se refere à incorporação da gestão de riscos para a integridade.
- Um dos principais desafios se constitui na consolidação de uma cultura de integridade pública que va além da abordagem tradicional, baseada na conformidade, para incluir uma abordagem dependente do contexto e baseada em riscos.
- A falta de apoio da alta administração foi identificada como uma das principais dificuldades enfrentadas pelas UGIs. Além disso, apenas uma pequena parte do trabalho das UGIs está voltada à orientação e treinamento de servidores em temas de integridade, embora haja uma significante necessidade de ampliar a capacitação nesses assuntos. Também faltam recursos públicos especialmente destinados à gestão de riscos para a integridade, o que impede o

adequado investimento em capacitações e a ampliação de atividades relacionadas à integridade pública.

- As ferramentas de TI poderiam auxiliar as instituições públicas a gerir adequadamente os riscos para a integridade; entretanto, atualmente apenas uma pequena parte delas usaas ferramentas disponíveis. Além disso, na maioria das vezes, essas ferramentas somente são usadas de modo *ad hoc* para fins de detecção e investigação, ao passo que poderiam ser sistematicamente empregadas para antecipar eventos críticos e fortalecer a integridade pública.

Principais recomendações

De modo geral, os desafios identificados reforçam a necessidade de continuar aprimorando a gestão dos riscos para a integridade na administração federal brasileira. O país poderia considerar o fortalecimento da atual metodologia de identificação e avaliação dos riscos para a integridade, por meio do trabalho em três áreas, que se complementam e se estruturam umas sobre as outras.

- Em primeiro lugar, a aplicação de lições de ciência comportamental amplia a percepção de vieses cognitivos no julgamento e auxilia os gestores públicos a melhor entender, identificar e avaliar os riscos para a integridade. Em essência, a ideia é tornar a gestão dos riscos para a integridade menos sensível, mais intuitiva e menos complexa. O Brasil poderia incorporar esses conceitos comportamentais a uma ferramenta de TI, para auxiliar os gestores públicos a melhorar sua tomada de decisões.
- Em segundo lugar, o país poderia se beneficiar dos avanços, realizados em anos recentes, por ferramentas de análise de dados como o “Alice” ou o “Faro”, no sentido de ir além da simples detecção e investigação e desenvolver soluções que apoiem a gestão de riscos para a integridade em instituições federais, com base em modelos preditivos. Para tanto, a CGU poderia desenvolver uma estratégia e um plano de ação para usar esses dados e aperfeiçoar as análises.
- Em terceiro lugar, é essencial continuar a desenvolver capacidades para a gestão de riscos para a integridade. Isso inclui garantir o apoio organizacional, o treinamento de equipes, o compartilhamento de boas práticas e o fornecimento de orientação ad hoc em áreas como riscos transversais para a integridade, metodologias de avaliação de riscos e letramento em dados e TI. Esse objetivo pode ser melhor alcançado por meio do trabalho da UGI e do treinamento de gestores públicos selecionados para liderar uma mudança rumo a uma cultura de gestão de riscos para a integridade.

1 Gestão de riscos para a integridade no Executivo Federal brasileiro

A gestão de riscos auxilia as instituições públicas a cumprirem seus mandatos e alcançarem uma ampla gama de metas e objetivos políticos. A gestão dos riscos para a integridade, em particular, está no cerne da garantia e da promoção eficiente e eficaz da integridade pública. No Brasil, a Controladoria-Geral da União (CGU) lidera a gestão de riscos para a integridade e oferece apoio e orientação metodológica às instituições públicas do Executivo Federal. Em geral, a abordagem de gestão de riscos para a integridade da CGU está alinhada com os parâmetros internacionais. Todavia, a implementação dessa estrutura é heterogênea em toda a administração, com níveis variados de maturidade, e ainda há muitos desafios para a promoção de uma cultura de gestão de riscos.

Gestão de riscos para a integridade: a base para políticas eficientes de integridade

A gestão de riscos auxilia as instituições públicas a cumprirem seus mandatos e alcançarem uma ampla gama de metas e objetivos políticos (OECD, 2020[1]). Os riscos precisam ser identificados, analisados e adequadamente geridos. Entre os vários riscos passíveis de afetar uma entidade pública, a corrupção, a fraude e outras práticas não íntegras podem minar a integridade pública e ameaçar o alcance de metas e objetivos das políticas públicas. Elas impedem, ainda, o uso eficiente dos recursos públicos e contribuem para a redução da confiança nas instituições públicas.

À luz desses fatos, a *Recomendação da OCDE sobre Integridade Pública* coloca a gestão de riscos no centro de qualquer estratégia ou abordagem que vise garantir e promover a integridade pública. A Recomendação incentiva os participantes a "instituir uma estrutura de controle interno e de gestão de riscos para garantir a integridade em organizações do setor público" (OECD, 2017[2]), em consonância com diversos parâmetros e orientações internacionais. Por exemplo, várias organizações desenvolveram marcos ou diretrizes internacionais para a gestão de riscos no setor público, tais como o Comitê das Organizações Patrocinadoras da Comissão Treadway (COSO), a Organização Internacional das Instituições Superiores de Auditoria (INTOSAI), o Instituto dos Auditores Internos (IIA) e a Organização Internacional de Padronização (ISO), entre outros.

Em particular, os países devem ter como meta a criação de um ambiente de controle com objetivos claros, que demonstre o comprometimento dos gestores com a integridade e com os valores do serviço público, e que propicie um razoável nível de segurança acerca da eficiência e desempenho de uma instituição, assim como a sua observância a leis e práticas. Também se deve buscar uma abordagem estratégica à gestão de riscos, que inclua a avaliação de riscos para a integridade pública, de modo a abordar fragilidades de controle (incluindo o estabelecimento de sinais de alerta para processos críticos), estabelecendo um mecanismo eficiente de monitoramento e de garantia de qualidade para o sistema de gestão de riscos e fortalecendo efetivamente a prevenção das violações à integridade.

No setor público, as estruturas normativas e políticas para a gestão de riscos estão muitas vezes alinhadas com diretrizes internacionais; no entanto, é comum persistirem os desafios para a sua implementação. Idealmente, os gestores públicos devem identificar e gerir os riscos inerentes aos processos e áreas de sua responsabilidade. O adequado entendimento e assimilação da gestão de riscos permite à administração o uso contínuo da informação sobre os riscos no processo de tomada de decisão. Ademais, os mecanismos de avaliação de risco necessitam ser incorporados em um processo cíclico, em que não apenas os riscos, mas também questões metodológicas sejam revisadas e atualizadas mediante a incorporação de novas evidências empíricas (OECD, 2018[3]).

Todavia, a importância da gestão de riscos nem sempre é bem assimilada pelos gestores públicos. Em primeiro lugar, é necessário compreender que a gestão de riscos exige um claro entendimento sobre os valores e objetivos da função pública exercida. A ausência de objetivos nítidos e de uma cultura de desempenho, muitas vezes observada no setor público, juntamente com a falta de transparência e a dificuldade de quantificar tanto o impacto quanto a produtividade do setor público, podem prejudicar tal compreensão. Quando um gestor público não é responsabilizado pelo alcance de objetivos, ou quando esses objetivos não são claramente definidos, pode não haver pressão para o cumprimento de metas e, assim, para identificar e gerir os riscos passíveis de impedir tais conquistas. Além dos objetivos muitas vezes imprecisos, os administradores públicos não raro carecem das habilidades e conhecimentos necessários à gestão de riscos e/ou não contam com o apoio de sua organização.

Na América Latina, assim como em outras regiões, um relatório da OCDE identificou três obstáculos principais para alcançar um sistema efetivo de gestão de riscos (OECD, 2019[4]):

- Os gestores públicos desconhecem ou negligenciam os parâmetros, políticas ou diretrizes sobre gestão de riscos.
- Os gestores públicos não possuem um claro entendimento sobre o conceito de "risco" e sobre os processos e a utilidade da gestão de riscos.
- Os gestores públicos acreditam que a gestão de riscos é uma função a ser assumida por terceiros e não a consideram como tarefa inerente à sua própria função gerencial.

Esses desafios, embora se apliquem à gestão de riscos em geral, são particularmente relevantes para a gestão de riscos para a integridade, em que os desafios podem se afigurar ainda mais severos por se tratar de um tema sensível e complexo. Por um lado, certas práticas não íntegras podem ser racionalizadas por agentes públicos como legítimas ou normais ("é assim que as coisas funcionam aqui"), ou nem serem mais percebidas como um problema. Por outro lado, os agentes públicos podem ter dificuldade em identificar alguns riscos de fraude se não tiverem suficiente compreensão do funcionamento de esquemas complexos de corrupção, ou se simplesmente desconhecerem as muitas práticas diferentes ligadas à corrupção. Os agentes públicos também podem apresentar relutância em falar sobre riscos de fraude e corrupção se igualarem os riscos a ocorrências reais, ou sentirem que estão "falando mal" de sua unidade ou de si mesmos.

Este relatório revisa a atual metodologia de avaliação de riscos para a integridade no Executivo Federal brasileiro e oferece caminhos para modernizar e fortalecer a atual abordagem. O restante do presente capítulo apresenta o arcabouço da gestão de riscos para a integridade e os desafios relacionados à sua implementação. Enquanto a estrutura normativa e a orientação para a gestão de riscos para a integridade serão analisadas em detalhe na próxima *Revisão de Integridade da OCDE no Brasil* (OECD, em preparo[5]), O Capítulo 2 enfoca os três caminhos concretos para fortalecer e modernizar a atual metodologia, ou seja: reconhecer e enfrentar as barreiras sociais e cognitivas para uma efetiva gestão de riscos para a integridade; alavancar esforços contínuos para melhorar o uso de dados e de ferramentas analíticas, a fim de prevenir violações à integridade; e, finalmente, fortalecer o apoio organizacional à gestão de riscos para a integridade nas instituições públicas do Executivo Federal.

Gestão de riscos para a integridade no Poder Executivo Federal brasileiro

O Brasil possui uma sólida abordagem de gestão de riscos para a integridade, alinhada aos mais relevantes padrões internacionais, e proporciona orientação aos gestores públicos

No Executivo Federal Brasileiro, a Instrução Normativa Conjunta nº 01/2016 estabelece a criação e a melhoria dos controles internos da gestão, governança e gestão de risco. No ano seguinte, a gestão de riscos para a integridade tornou-se obrigatória para as instituições públicas federais, mediante o Decreto nº 9.203/2017. A gestão dos riscos para a integridade é um elemento central dos Programas de Integridade e dos Planos de Integridade estabelecidos desde 2017 nas 186 instituições do Executivo Federal para a prevenção, detecção, punição e remediação de atos de fraude, corrupção e outras práticas antiéticas. Em 2021, a criação do Sistema de Integridade Pública do Poder Executivo Federal (SIPEF), por meio do Decreto nº 10.756/2021, avançou na institucionalização e consolidação dos Programas de Integridade, incluindo a exigência de assegurar uma efetiva gestão de riscos para a integridade (Box 1.1).

Box 1.1. O Sistema de Integridade Pública (SIPEF) no Executivo Federal brasileiro

A Controladoria-Geral da União (CGU) é o órgão de controle interno do Governo Federal e, desde sua criação, em 2011, tem sido um elemento crucial na estratégia governamental para aumentar a integridade e prevenir a corrupção no Brasil (OECD, 2012[6]).

Em particular, a CGU é responsável por coordenar a implementação dos Programas de Integridade destinados a prevenir, detectar, punir e remediar casos de corrupção, fraude, atos ilícitos e violações dos padrões de conduta em todas as entidades públicas do Executivo Federal (Decreto nº 9.203/2017, posteriormente regulado pelas Portarias nºs 1089/2018 e 57/2019).

Os Programas de Integridade devem ser estruturados com base nos seguintes eixos:

- Comprometimento e apoio da alta administração.
- Existência de uma unidade responsável pela implementação no órgão ou entidade.
- Análise, avaliação e gestão dos riscos associados ao tema da integridade.
- Monitoramento dos atributos do Programa de Integridade.

Os Programas de Integridade visam assegurar que, em cada instituição federal, todas as unidades internas responsáveis por atividades e áreas ligadas à integridade trabalhem articulada e conjuntamente para garantir a integridade e minimizar os riscos para a integridade. As Unidades de Gestão da Integridade (UGIs) são responsáveis, em cada instituição, por coordenar a elaboração do Plano de Integridade, assim como sua subsequente implementação, monitoramento e avaliação. A alta gestão deve aprovar esses Planos de Integridade, os quais estabelecem medidas de integridade e um plano de ação para sua implementação.

O Sistema de Integridade Pública do Poder Executivo Federal (SIPEF), estabelecido em julho de 2021, pelo Decreto nº 10.756/2021, avança na formalização e fortalecimento da base normativa dos Programas de Integridade e das UGIs, tendo a CGU como seu órgão central (OECD, 2021[7]). O SIPEF institui as UGIs como as unidades setoriais responsáveis pelo sistema, expandindo suas funções e responsabilidades. Essas responsabilidades podem ser resumidas na articulação dos diferentes esforços para o alcance da integridade dentro da instituição, mas também incluem o fornecimento de orientações, treinamento e apoio em questões relacionadas à integridade pública e à gestão dos riscos para a integridade.

Fonte: (OECD, 2012[6]) e (OECD, 2021[7]).

A Controladoria Geral da União (CGU) inicialmente definiu o risco para a integridade como uma "vulnerabilidade que pode favorecer ou facilitar a ocorrência de práticas de corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, podendo comprometer os objetivos da instituição" (Portaria CGU nº 57/2019). Recentemente, com o SIPEF, a definição de risco para a integridade foi revista como a "possibilidade de ocorrência de evento de corrupção, fraude, irregularidade ou desvio ético ou de conduta que venha a impactar o cumprimento dos objetivos institucionais" (Decreto nº 10.756/2021). A CGU enfatiza que a gestão dos riscos para a integridade permeia todo o governo federal, abrangendo diferentes funções (por ex., gestão de recursos humanos, gestão de recursos públicos, gestão de riscos e controle interno e aquisições públicas) e setores (por ex., infraestrutura, habitação, saúde, educação, tributação e sistema alfandegário).

Em 2018, a CGU lançou o *Guia Prático de Gestão de Riscos para a Integridade* para apoiar as entidades federais (CGU, 2018[8]). O documento amplia a conscientização e oferece orientações sobre a gestão de riscos para a integridade, com passo a passos concretos para sua implementação. O guia também reforça

a noção de que a gestão dos riscos para a integridade é de responsabilidade dos gestores públicos, enquanto donos dos riscos. Especificamente, o documento determina que os gestores estabeleçam, monitorem e aperfeiçoem a gestão de riscos e os sistemas de controle interno. Isso inclui a identificação, avaliação, mitigação e monitoramento dos riscos para a integridade passíveis de afetar o alcance dos objetivos relativos ao cumprimento da missão institucional das instituições públicas.

Em consonância com a *Recomendação da OCDE sobre Integridade Pública* (2017), o Guia da CGU altera o foco das políticas de integridade rumo a uma abordagem dependente do contexto, comportamental e baseada em riscos. Sua natureza geral permite às instituições públicas federais adaptar a metodologia a contextos específicos, ao tempo em que assegura uma base de coerência a toda a administração federal. Isso também significa, por exemplo, que se uma instituição pública já adotou uma metodologia de avaliação de riscos para outras áreas, ela poderá aplicar essa mesma metodologia à identificação de riscos para a integridade. Além disso, o Guia oferece flexibilidade para a melhoria contínua da metodologia, à medida em que a instituição amadurece sua implementação.

O Guia também convida as entidades a irem além da abordagem anticorrupção tradicional, baseada no cumprimento de regras, e reforça a relevância de promover uma mudança cultural efetiva na organização. Nesse sentido, a CGU enfatiza certos princípios e aspectos na gestão de riscos para a integridade, tais como o comprometimento da alta administração, o incentivo ao envolvimento de diferentes áreas da entidade e a capacitação no campo da integridade pública.

Adicionalmente, o Guia auxilia os gestores públicos a identificar riscos para a integridade ao apresentar uma lista genérica de potenciais eventos que podem prejudicar a realização dos objetivos institucionais (“riscos transversais para a integridade”) e ao fornecer ferramentas metodológicas. Sugere-se às instituições públicas empregar diferentes metodologias para coletar informações e identificar riscos para a integridade, tais como a análise de informações já existentes dentro da organização (Box 1.1), o aproveitamento da experiência e habilidades dos servidores públicos, o compartilhamento de experiências com organizações similares ou a análise de distintos cenários. A escolha da melhor abordagem dependerá da maturidade da organização e dos recursos humanos e financeiros disponíveis. Por exemplo, como uma possível ferramenta entre muitas, o Guia sugere o uso de reuniões de *brainstorming* para estimular os participantes a contribuir com pontos de vista para facilitar a identificação de riscos.

Box 1.2. O uso de dados de procedimentos disciplinares anteriores na identificação de riscos para a integridade pela

A avaliação de riscos para a integridade feita pela Corregedoria-Geral da União em processos disciplinares da Polícia Federal brasileira ilustra uma das metodologias voltadas à identificação desses riscos por meio do uso de dados de casos anteriores. De fato, deu-se início a um procedimento de avaliação de riscos mediante a análise quantitativa de 2.384 Processos Administrativos Disciplinares (PADs) que levaram a demissões, destituição de cargos e cassação de aposentadorias. Os dados foram obtidos por meio do Sistema de Gestão de Processos Disciplinares (CGU-PAD). Em seguida, a Polícia Federal analisou apenas os PAD que impuseram sanções e selecionaram uma amostra, excluindo os processos associados com sanções não expulsivas (por ex., advertências) e os que não envolveram nenhum ato de corrupção, totalizando 40 PADs. Durante esse procedimento, foram identificados riscos transversais, como enriquecimento ilícito, oferta de propina para a obtenção de informações privilegiadas, acesso indevido aos sistemas de consulta e fraude. Os riscos para a integridade resultantes foram classificados em quatro tipos principais de eventos: obtenção de vantagem pessoal, vazamento de informações, negociação de serviços privilegiados e fraude. Conquanto nesse caso tenha-se adotado uma metodologia baseada em processos disciplinares anteriores, a CGU enfatiza que as entidades não devem se concentrar somente em eventos passados (CGU, 2018[9]).

Fonte: OCDE, com base em informações fornecidas pela CGU.

Como ponto principal, o Guia da CGU apresenta a metodologia para a avaliação de riscos para a integridade; para tanto, utiliza a abordagem padrão de classificação de um risco de acordo com sua probabilidade e enfatiza diversas maneiras para estimar e apresentar ambas as dimensões de um risco, dependendo de sua precisão e complexidade. Em particular, o Guia da CGU estimula cada instituição a adotar escalas de classificação de impacto e probabilidade para construir um mapa de calor, a depender da complexidade calculada. As instituições com atividades de gestão de riscos para a integridade menos maduras, por exemplo, podem adotar metodologias básicas, como uma matriz 4x4 (quatro níveis de probabilidade e quatro níveis de impacto), conforme ilustrado na Tabela 1.1 a seguir. Consequentemente, para cada risco para a integridade catalogado, a organização deve indicar a possibilidade de sua ocorrência (probabilidade) e a gravidade das possíveis consequências (impacto). Esse processo define a base de análise das medidas mais adequadas para abordar os riscos, de acordo com sua gravidade.

Tabela 1.1. Matriz de riscos para a integridade com 4x4 níveis

Risco	Probabilidade	Impacto
1 – Muito baixo	O evento tem muito pouca probabilidade de ocorrer	Consequências insignificantes
2 – Baixo	O evento raramente ocorre	Consequências menores em processos e atividades secundárias
3 – Médio	O evento já ocorreu algumas vezes e pode ocorrer novamente	Consequências relevantes em processos e atividades secundárias ou consequências menores em processos e atividades prioritárias
4 – Alto	O evento tem ocorrido repetidamente e provavelmente ocorrerá muitas vezes mais	Consequências relevantes em processos e atividades prioritárias

Fonte: (CGU, 2018[8]).

Além de identificar, descrever e classificar os riscos, o Guia também determina que as organizações apontem as causas e as consequências mais significativas associadas a um potencial evento. A identificação das causas possibilita compreender as razões ou circunstâncias com maior probabilidade de estimular, causar ou permitir qualquer conduta que viole a integridade pública. O mapeamento das consequências, por sua vez, favorece um melhor entendimento de como os riscos para a integridade podem afetar os objetivos da organização (CGU, 2018[9]).

Finalmente, o Guia da CGU fornece orientações sobre como usar a informação obtida por meio da avaliação de riscos e do mapa de calor para introduzir medidas eficientes e eficazes de redução desses riscos. No desenvolvimento dos planos de integridade, o Guia recomenda que as instituições públicas se concentrem nos riscos para a integridade mais relevantes a serem geridos, ou seja, aqueles com o impacto mais significativo e maior probabilidade de ocorrência dentro de um nível de risco previamente definido pela alta administração. As organizações públicas devem priorizar os riscos para a integridade que excedam a sua tolerância ao risco ("apetite a riscos"). De acordo com o guia, os programas de integridade, então, devem identificar e promover a implementação de medidas para evitar, minimizar ou transferir os riscos para a integridade mais relevantes e prioritários, garantindo respostas apropriadas e tempestivas. Com base nas prioridades estabelecidas no mapa de calor e no nível de tolerância ao risco, a entidade deve verificar as medidas já existentes e avaliar a necessidade de aperfeiçoar ou estabelecer novas estratégias. A capacitação de equipes, a promoção da transparência, o controle social e a redução do nível de discricionariedade em processos decisórios sensíveis são algumas das medidas recomendadas pelo Guia da CGU para abordar os riscos para a integridade (CGU, 2018[8]). Muitas outras ações podem ser adotadas, dependendo dos riscos específicos de cada organização e da disponibilidade de recursos. O Guia também enfatiza que é essencial adaptar as medidas às reais necessidades da organização para auxiliar o alcance dos seus objetivos, ao invés de gerar burocracia desnecessária e retardar os processos.

A identificação, avaliação e minimização dos riscos para a integridade é um passo essencial para a aprovação do plano de integridade. Como apontado pela CGU, a identificação e avaliação de riscos realizada previamente à implementação do programa de integridade auxilia a reconhecer os processos e as áreas mais suscetíveis à corrupção, capacitando a entidade a agir tempestivamente e a se ajustar a novos riscos ao longo do tempo (CGU, 2018[9]).

Institucionalmente, no âmbito das instituições federais, as Unidades de Gestão da Integridade (UGIs) desempenham um papel crucial na coordenação e no apoio à gestão de riscos para a integridade, atuando como uma segunda linha de defesa. As UGIs são de estabelecimento obrigatório em todas as entidades do Executivo Federal. Elas coordenam a elaboração do Plano de Integridade da instituição e sua subsequente implementação, monitoramento e avaliação. O Sistema de Integridade Pública do Poder Executivo Federal (SIPEF) representa uma oportunidade de fortalecer ainda mais as UGIs para que elas possam cumprir seu relevante papel como unidades setoriais do SIPEF (OECD, 2021[7]).

Apesar de sua abordagem relativamente sólida da gestão dos riscos para a integridade, o Brasil ainda enfrenta significativos desafios à sua implementação

No Brasil, a capacidade de gestão de riscos sempre representou um desafio para o governo. Em 2014, o Tribunal de Contas da União (TCU) conduziu uma pesquisa em parceria com o Instituto Rui Barbosa, a Associação dos Membros dos Tribunais de Contas do Brasil (ATRICON) e 28 entidades de auditoria regionais, que destacou uma necessidade sistêmica de melhoria da gestão e mitigação de riscos no âmbito governamental. Especificamente, a pesquisa avaliou a maturidade da gestão de riscos com base em um conjunto específico de critérios e identificou ineficiências na gestão de riscos em entidades do setor público. Das 380 entidades públicas pesquisadas, 304 (80%) foram consideradas, à época, em um estágio incipiente de gestão de riscos (ou seja, capacidade inexistente ou insuficiente) (TCU, 2014[10]). A garantia da efetiva implementação permanece como um dos principais entraves enfrentados pelo governo

brasileiro no que se refere à gestão de riscos para a integridade, e, em geral, para assegurar a efetiva prestação de contas.

Como anteriormente observado, a implementação da gestão de riscos no setor público constitui um desafio, mas a implementação de riscos para a integridade talvez seja um desafio ainda maior (OECD, 2019[4]). Muitos países envidam grandes esforços para aplicar marcos conceituais à prática cotidiana e promover uma cultura de gestão de riscos para a integridade nas organizações públicas. O Brasil não é exceção. Um questionário de averiguação da OCDE e um grupo focal *on-line* realizado com as UGIs e a CGU, assim como diversas entrevistas com agentes públicos, evidenciaram que, a despeito do arcabouço normativo e das diretrizes disponíveis, a gestão de riscos para a integridade ainda se encontra em um estágio inicial. Embora exista um grau de heterogeneidade em relação ao amadurecimento da gestão de riscos para a integridade na administração federal, em que algumas instituições públicas se encontram em etapas mais avançadas que outras, há um amplo reconhecimento de que ainda persistem importantes desafios de implementação na maioria das entidades públicas do Executivo Federal brasileiro.

Um dos maiores desafios relacionados ao fortalecimento da gestão de riscos para a integridade no Brasil diz respeito à dificuldade de consolidar uma cultura de integridade pública, que se estenda para além da visão legalista tradicional e comece a incluir uma abordagem dependente do contexto e baseada em riscos. Os resultados obtidos a partir do grupo focal conduzido pela OCDE demonstram que a cultura da conformidade ainda é largamente difundida entre as entidades públicas federais e que há uma forte resistência à mudança por parte dos servidores públicos.

Além disso, é essencial contar com o apoio da alta administração e investir em treinamento de servidores. Na prática, entretanto, as respostas ao questionário da OCDE indicam que a falta de apoio dos altos gestores é uma das principais dificuldades enfrentadas pelas UGIs no desenvolvimento do seu trabalho e na implementação da avaliação dos riscos para a integridade. Ademais, não obstante a relevância de investir em capacitações, os resultados da averiguação realizada pela OCDE revelam que, atualmente, apenas uma pequena parte do trabalho das UGIs está voltada a aconselhar e treinar equipes em questões de integridade. Também se constata uma forte necessidade de intensificar o treinamento em temas específicos de integridade pública para as áreas que desenvolvem atividades relacionadas a essas questões.

Outros desafios dizem respeito aos obstáculos que têm dificultado a efetiva institucionalização da gestão de riscos para a integridade no Executivo Federal brasileiro. Em primeiro lugar, há uma falta de recursos públicos destinados especificamente a essa finalidade, o que acaba impedindo o adequado investimento no treinamento de equipes e na expansão das atividades relacionadas à integridade pública. De acordo com os resultados do questionário da OCDE, 93% (28) das UGIs que participaram da pesquisa não possuíam orçamento próprio à época. Isso significa que as atividades ligadas à integridade ficam muitas vezes sujeitas à disponibilidade de recursos alocados a outras atividades das UGIs, não relacionadas à integridade. Em segundo lugar, verifica-se uma insuficiência de força de trabalho qualificada e dedicada integralmente à gestão dos riscos para a integridade. A esse respeito, o grupo focal da OCDE chamou atenção para o fato de que os gestores públicos responsáveis pela gestão de riscos muitas vezes trabalham no limite de suas capacidades, tendo que realizar outras funções. Por sua vez, as UGIs estão aptas a oferecer apoio aos gestores públicos, mas, em geral, não possuem uma equipe em regime de dedicação exclusiva e adequadamente treinada para lidar com a gestão de riscos para a integridade (OECD, 2021[7]). Tais questões explicam por que a gestão de riscos para a integridade ainda não foi largamente implementada nas instituições governamentais federais, o que dá lugar a planos de integridade incompletos, análises de riscos inacabadas e dificuldades em estabelecer sistemas de detecção eficazes.

Ademais, embora as ferramentas de TI sejam passíveis de auxiliar as instituições públicas na identificação e avaliação dos riscos para a integridade, além de apoiá-las nos processos de tomada de decisão, tais instrumentos são atualmente usados apenas por uma minoria das instituições públicas. Ainda assim,

essas ferramentas são quase sempre usadas para fins de detecção e investigação, ao invés de serem empregadas para a antecipação de eventos críticos e o fortalecimento da integridade pública. Como exemplos dessas ferramentas, mencionam-se o Alice (Analisador de Licitações, Contratos e Editais) e o Faro (Ferramenta de Análise de Riscos em Ouvidoria). A CGU e, no caso do Alice, também o TCU, usam esses instrumentos para apoiar a investigação de eventos suspeitos. O Alice tem por foco as aquisições públicas, e o Faro auxilia a análise das denúncias dirigidas à Ouvidoria-Geral da União. O Capítulo 2 analisará mais detalhadamente essas ferramentas de TI e como o Brasil poderia se valer delas para fortalecer a gestão dos riscos para a integridade.

O Agatha, um instrumento desenvolvido pelo extinto Ministério do Planejamento, Desenvolvimento e Gestão (MP), objetiva facilitar a gestão de riscos e os sistemas de controle interno. Essa ferramenta foi projetada para auxiliar os gestores a avaliar as forças, fraquezas, oportunidades e ameaças (análise FOFA), tanto internas quanto externas, e a identificar, avaliar e orientar análises críticas de riscos a fim de impactar positivamente o alcance dos objetivos institucionais das entidades públicas, conforme dispõe o Decreto nº 9.203/17. Todavia, na prática, essa ferramenta não foi amplamente adotada, a despeito de sua gratuidade. Por exemplo, entre as UGIs que responderam ao questionário da OCDE, somente 10% (3) usam atualmente o Agatha, e uma delas está considerando a sua utilização. Outras poucas unidades estão no processo de implementação desse instrumento e algumas apontaram uma urgente necessidade de treinamento e orientações mais claras sobre como utilizar o Agatha. Entrevistas realizadas pela OCDE para entender as razões pelas quais o Agatha não é usado de modo mais sistemático indicaram que a ferramenta é de difícil utilização e limitada em termos de suporte analítico, oferecendo apenas um mapa de calor para facilitar as análises.

De modo geral, os pontos anteriormente levantados reforçam a necessidade de continuar a aperfeiçoar e amadurecer a gestão de riscos para a integridade na administração federal brasileira. Não menos importante, a pandemia de Covid-19 impôs diversos desafios adicionais aos países, incluindo o Brasil, elevando os gastos públicos, agravando a situação financeira nacional, conturbando os processos decisórios e obstruindo o controle social. Conforme relatado na averiguação, as entidades públicas brasileiras experimentaram uma série de dificuldades para desenvolver seu trabalho sob essas novas circunstâncias. Foi também mencionado que, em decorrência da crise, a agenda da integridade pública perdeu importância entre algumas entidades públicas, o que se refletiu na piora das limitações orçamentárias para tratar dessa questão.

Infelizmente, uma pesquisa recente sobre ética e corrupção no serviço público federal brasileiro revelou que, durante a crise da Covid-19, houve um aumento na percepção dos gestores públicos acerca da ocorrência de atos de corrupção, tais como interferência política na tomada de decisões e falta de transparência e responsabilidade em decisões concernentes às aquisições e contratações públicas (Ortega Nieto et al., 2021[11]). Portanto, em um contexto de crise, a gestão de riscos para a integridade se torna ainda mais relevante para guiar políticas de integridade efetivas e eficazes.

Não obstante, cabe ressaltar que, a despeito dos desafios experimentados por algumas entidades públicas durante a atual crise, o estabelecimento do SIPEF, em 2021, representa um marco indicativo de que o país está no rumo certo para concretizar a agenda da integridade no Executivo Federal. Todavia, esse novo sistema ainda necessita ser consolidado para atingir o objetivo de promover culturas de gestão de riscos para a integridade no âmbito da administração federal (OECD, 2021[7]). Com base na análise da situação atual, o capítulo seguinte apresenta caminhos concretos para continuar fortalecendo a cultura de integridade pública e de gestão de riscos para a integridade. As recomendações apresentadas no próximo capítulo serão complementadas pela *Revisão de Integridade da OCDE no Brasil* (OECD, em preparo[5]), que fornecerá uma análise mais sistêmica da gestão de riscos para a integridade e da sua prevenção no Brasil.

2 Os três caminhos para fortalecer as avaliações de riscos para a integridade no Executivo Federal brasileiro

Este capítulo apresenta três caminhos concretos para fortalecer e modernizar a abordagem de identificação e avaliação de riscos para a integridade no Executivo Federal brasileiro. Primeiramente, recomenda-se reconhecer e enfrentar barreiras sociais e cognitivas, a fim de melhorar a precisão do julgamento humano e promover uma cultura de gestão de riscos para a integridade. Em segundo lugar, os esforços contínuos para melhorar o uso de dados e de ferramentas analíticas podem ser alavancados no sentido de auxiliar a gestão de riscos para a integridade. Finalmente, o Sistema de Integridade Pública do Poder Executivo Federal (SIPEF) oferece uma oportunidade para promover a liderança e reforçar o apoio institucional à gestão de riscos para a integridade nas instituições públicas, por meio das Unidades de Gestão da Integridade (UGIs).

O Capítulo 1 descreveu e analisou os principais desafios enfrentados pelo Brasil para garantir a efetiva implementação da atual abordagem da gestão doa riscos para a integridade, e, em particular, para promover uma cultura de gestão de riscos em todo o Executivo Federal. Ao mesmo tempo, a gestão de riscos para a integridade se torna ainda mais crucial em tempos de crise, visto que assegura políticas de integridade não apenas efetivas, mas também eficientes e, portanto, econômicas.

Nesse sentido, o país poderia considerar o fortalecimento da atual metodologia e abordagem, trabalhando ao longo de três caminhos principais que complementam e se estruturam uns sobre os outros:

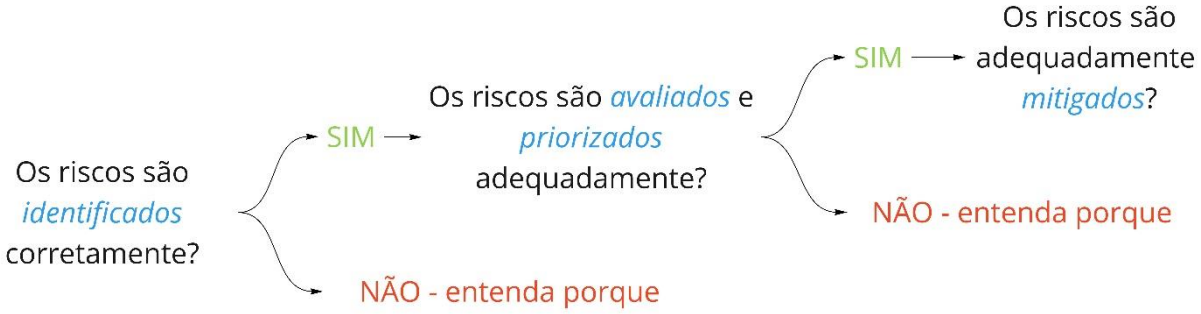
1. Desmistificar e simplificar as avaliações qualitativas de riscos para a integridade.
2. Avançar na gestão de riscos para a integridade por meio do uso de dados e de ferramentas analíticas.
3. Fortalecer o apoio institucional para a gestão de riscos para a integridade e capacitar os gestores públicos.

Desmistificar e simplificar as avaliações qualitativas de riscos para a integridade

Barreiras comportamentais e vieses na gestão de riscos para a integridade

A abordagem baseada em riscos é fundamental para a *Recomendação da OCDE sobre Integridade Pública*. A ideia pode ser encontrada ao longo de toda a Recomendação, a qual enfatiza que as análises de riscos devem orientar as medidas adotadas para mitigar esses riscos para a integridade, a fim de que essas medidas sejam proporcionais, eficientes e eficazes. No entanto, é necessário lembrar que o alcance desses objetivos depende, entre outros, de três passos fundamentais: da identificação precisa, da avaliação e mitigação dos riscos que podem afetar o cumprimento do mandato e dos objetivos de uma instituição pública (Figura 2.1). Além disso, a gestão de riscos para a integridade deve ser claramente comunicada, monitorada e avaliada para garantir uma efetiva implementação e aprendizado ao longo do tempo. Cada um desses passos necessita ser eficaz para alcançar o objetivo geral da gestão de riscos para a integridade, sendo crucial identificar e compreender os potenciais desafios e problemas.

Figura 2.1. Os três passos da gestão de riscos para a integridade



Embora o Guia da CGU descrito no Capítulo 1 apresente informações sobre esses três passos e enfatize a necessidade de promover culturas de gestão de riscos para a integridade nas instituições públicas, as orientações sobre como esses aspectos podem ser concretamente alcançados são limitadas. Naturalmente, existe uma ampla variedade de aspectos relacionados, por exemplo, com as estruturas normativas ou as capacidades disponíveis, que constituem elementos fundamentais para a consolidação de uma efetiva gestão dos riscos para a integridade. Esses aspectos serão analisados com mais detalhe na próxima *Revisão de Integridade da OCDE no Brasil* (OECD, em preparo[5]). A presente seção examina algumas barreiras comportamentais e vieses que podem prejudicar a gestão dos riscos para a integridade

em cada um dos três passos ilustrados na Figura 2.1, para os quais o discernimento e a experiência humana continuam e continuarão a contribuir com informações relevantes. De fato, o Guia da CGU atualmente carece de uma análise dessas dimensões comportamentais.

A aplicação de lições de ciência comportamental pode ajudar a revelar esses vises cognitivos e erros sistemáticos de julgamento, subsidiando, assim, estratégias de apoio aos gestores públicos (os responsáveis pelos riscos) a fim de melhorar sua compreensão, identificação e avaliação dos riscos. Isso, por sua vez, pode ensejar medidas de integridade melhor direcionadas e um sistema de controle interno mais resiliente à fraude e à corrupção e, finalmente, contribuir para estabelecer uma cultura de gestão de riscos para a integridade nas entidades públicas.

De fato, os seres humanos estão sujeitos a diversos vieses que dificultam a identificação e a avaliação da probabilidade da ocorrência e do potencial impacto de um determinado evento de risco. Apesar do uso de metodologias que simulam avaliações objetivas, a identificação e a avaliação dos riscos sempre terão um componente subjetivo (Slovic, 1999[12]). Os seguintes aspectos podem afetar o julgamento dos agentes públicos que participam de avaliações de riscos para a integridade, particularmente as avaliações qualitativas de riscos, como aquelas exemplificadas no Guia da CGU:

- O conceito de “risco” e de tolerância ao risco é muitas vezes mal compreendido ou difícil de definir ou comunicar, particularmente no contexto da gestão de riscos para a integridade, em que a retórica política promove a chamada “tolerância zero”. Ademais, a racionalização inconsciente de práticas antiéticas ou a suscetibilidade que acompanha as violações de integridade podem comprometer a identificação de eventos de risco relevantes. Por um lado, a tarefa de identificar os riscos para a integridade pode desencadear desconforto ou até receio. Os agentes públicos podem sentir que a identificação de riscos nos processos sob sua responsabilidade corresponde de fato a uma avaliação de sua própria integridade ou da integridade de suas equipes, confundindo o risco de violações da integridade com sua real ocorrência. Por outro lado, o valor agregado na identificação e gestão de riscos muitas vezes é menos valorizado pelos agentes públicos do que os riscos potenciais para si mesmos. Eles podem *não estar dispostos* a identificar riscos para a integridade, por perceberem tal exercício como indicativo de fraquezas em suas unidades e processos, com consequências potencialmente negativas. Por exemplo, os agentes públicos podem relutar em chamar a atenção da investigação ou de unidades de auditoria sobre sua área, no receio de atrair mais trabalho ou pressão.
- Para identificar riscos mais específicos para a integridade, é necessário um conhecimento detalhado do setor, de sua organização e dos seus processos. Esse conhecimento pode ser útil para estimular a participação dos gestores e dos servidores da linha de frente. Eles são diretamente responsáveis pelas operações e serviços em toda a organização e podem contribuir para a identificação de riscos, oferecendo diferentes perspectivas e validando os resultados do mapeamento de riscos (OECD, 2020[1]). Seguindo essa lógica, o Guia da CGU recomenda o uso de oficinas de riscos, similares a sessões de *brainstorming*, para identificar riscos e considerar diferentes perspectivas e experiências por meio do envolvimento dos servidores públicos (CGU, 2018[8]). Contudo, diversos conceitos comportamentais mostram que as reuniões de *brainstorming* estão sujeitas a dinâmicas sociais que podem comprometer a identificação dos riscos. Por exemplo, ao invés de corrigir erros cometidos pelos indivíduos de um grupo, o grupo pode amplificar esses erros. Os grupos também podem apenas seguir as ideias dos participantes que se manifestam primeiro, polarizar-se em torno de ideias extremistas ou continuar focando no que todos já sabem, ao invés de considerar informações cruciais de indivíduos que podem não querer externá-las (Sunstein and Hastie, 2014[13]).
- Finalmente, a avaliação de riscos identificados também pode sofrer vieses. Diversos estudos observaram que os seres humanos têm bastante dificuldade em pensar estatisticamente e, como tal, podem enfrentar problemas para avaliar corretamente a probabilidade de riscos (Kahneman and Tversky, 1982[14]; Kahneman and Tversky, 1972[15]). Para lidar com a incerteza e avaliar

probabilidades, as pessoas tendem a usar o pensamento heurístico (Tversky and Kahneman, 2007[16]). Embora a heurística seja econômica, muitas vezes ela acarreta julgamentos enviesados. Por exemplo, as pessoas tendem a confundir plausibilidade com probabilidade. Entretanto, um risco que parece mais plausível ou que tem uma narrativa mais coerente não é necessariamente o de ocorrência mais provável. Um fator típico de distorção de nossa estimativa de probabilidade é a falácia da taxa básica. Quando questionadas sobre violações à integridade em determinado procedimento, as pessoas imaginam ou recordam quantas vezes uma violação ocorreu, mas normalmente desconsideram quantas vezes o procedimento aconteceu sem nenhuma violação da integridade. Além disso, eventos de risco que tendem a nos afetar emocionalmente ou que vivenciamos diretamente no passado costumam desencadear sentimentos mais intensos e nos fazem acreditar que são mais prováveis (Loewenstein et al., 2001[17]). A disponibilidade de informação sobre um tópico ou a sua relevância também podem influenciar nossas estimativas. Uma ampla cobertura midiática sobre casos de corrupção, por exemplo, pode distorcer nossa percepção no sentido de superestimar a probabilidade de ocorrência de certos riscos para a integridade. Finalmente, diferentes crenças e visões de mundo podem ensejar classificações de risco muito díspares, resultando em pouco ou nenhum benefício da matriz de riscos para a gestão efetiva e racional destes (Ball and Watt, 2013[18]).

Mesmo quando os riscos para a integridade são adequadamente identificados e avaliados, por meio de técnicas qualitativas ou quantitativas, as preconcepções e as barreiras comportamentais podem dificultar a correta tomada de decisão em relação ao modo de lidar com esses riscos e, portanto, impedir uma efetiva mitigação desses riscos. De fato, os gestores públicos que necessitam agir com base nas informações disponíveis sobre os riscos muitas vezes se veem propensos tanto à inação como a uma reação exagerada.

- Por um lado, o excesso de confiança ou a cegueira em reação às vulnerabilidades pode levar a medidas preventivas que são muito fracas. A já mencionada racionalização de algumas práticas antiéticas e a susceptibilidade ligada aos riscos para a integridade, aliadas à incompreensão da probabilidade do risco *versus* a ocorrência do risco, podem levar os gestores públicos a preferir fechar os olhos para os riscos para a integridade ao invés de agir – por exemplo, para evitar estar no foco da atenção e atrair potencial estresse, estigma ou trabalho extra.
- Por outro lado, gestores públicos demasiadamente avessos a riscos, ou contextos em que os escândalos de corrupção são largamente cobertos pela mídia, despertando reações tanto dos cidadãos como dos partidos de oposição, podem levar a medidas muito estritas, que acabam indo "além do alvo". A aversão à perda é, de fato, um conceito comportamental amplamente pesquisado e estabelecido (Kahneman and Tversky, 1979[19]). Os custos do enfrentamento de um escândalo de corrupção em determinada entidade são muitas vezes considerados impeditivos para a alta administração e podem, assim, ensejar medidas extremas. No entanto, é importante ter em mente que as medidas anticorrupção também acarretam custos (Falk and Kosfeld, 2006[20]; OECD, 2018[21]; Schulze and Frank, 2003[22]). Esses custos estão ligados a *trade-offs* com flexibilidade e inovação, ao dano psicológico decorrente do sinal de desconfiança que é enviado aos servidores públicos e ao risco de afastar a motivação intrínseca à honestidade.

Para abordar os vieses comportamentais, a CGU poderia revisar a atual metodologia de avaliação de riscos para a integridade e oferecer apoio tecnológico para os gestores públicos ao longo do processo

Segundo enfatizado no Capítulo 1, há diversos desafios para implementar uma cultura de gestão de riscos para a integridade. Eles estão relacionados às restrições de capacidade (conhecimento sobre riscos ligados à integridade) e de tempo (prioridades concorrentes). Além disso, a seção prévia ressaltou que os vieses comportamentais podem exacerbar o desafio de estabelecer culturas de gestão de riscos para a

integridade. A CGU reconhece alguns desses entraves, mas não oferece orientações e apoio suficiente sobre como abordá-los concretamente. Nesse caso, a aplicação de conceitos comportamentais permite reconhecer e tratar os potenciais problemas identificados na seção anterior. Em resumo, a ideia é tornar a gestão de riscos para a integridade um tópico menos sensível, mais intuitivo e menos complexo.

Em particular, a CGU poderia considerar a aplicação de lições de ciência comportamental por meio das seguintes estratégias ou medidas:

- *Apoiar a identificação de riscos para a integridade, superando mal-entendidos e desmistificando os riscos ligados à integridade.* A predisposição em identificar riscos para a integridade, em primeiro lugar, é fundamental para os resultados da gestão desses riscos. A CGU e as UGIs, portanto, devem continuar e mesmo intensificar os esforços para esclarecer os conceitos de integridade e de risco. Essencialmente, é crucial que os gestores públicos compreendam que a gestão de riscos para a integridade visa examinar a integridade de funções e processos, não a sua própria integridade pessoal. Tanto quanto possível, a comunicação necessita dissociar a identificação de riscos de casos específicos. Uma estratégia seria começar com um experimento mental nos seguintes moldes: “Imagine que você está deixando seu cargo atual e deseja garantir que a pessoa que vier depois não possa abusar de sua posição e dos processos sob sua responsabilidade”. A comunicação também deve buscar “normalizar” a gestão de riscos para a integridade na medida do possível. Os administradores necessitam se conscientizar de que a gestão dos riscos para a integridade, em última instância, auxilia o alcance dos objetivos institucionais, porquanto favorece uma melhor tomada de decisões, uma alocação mais direcionada de recursos e a prevenção de danos à reputação.
- *Apoiar a identificação de riscos para a integridade, simplificando a metodologia e fornecendo orientações intuitivas*. Embora a atual abordagem de gestão de riscos para a integridade no Brasil corresponda a diretrizes e práticas internacionais, a averiguação realizada durante o presente trabalho evidenciou que essa gestão é percebida como algo complicado e que demanda habilidades específicas. Os detalhes são importantes, mas os riscos para a integridade são frequentemente bem conhecidos e podem ser tratados de uma forma mais genérica. Essencialmente, levando em consideração o atual nível de maturidade da gestão de riscos para a integridade no governo brasileiro, há benefícios em simplificar as abordagens, identificar pequenas conquistas e resistir ao apelo de metodologias excessivamente sofisticadas de avaliação de riscos para a integridade, atentando, ao mesmo tempo, para as preconcepções e armadilhas das avaliações quantitativas de riscos, conforme discutido.
- *Abordar dinâmicas de grupo problemáticas para evitar vieses na identificação e avaliação dos riscos para a integridade.* O reconhecimento dos problemas inerentes às sessões de brainstorming ajuda a contrabalançá-los na realização de trabalhos em grupo. Nesse sentido, a CGU pode adotar técnicas para evitar as armadilhas típicas da tempestade de ideias e do pensamento de grupo (Sunstein and Hastie, 2015[23]). Por exemplo, adaptando essas técnicas à identificação de riscos para a integridade, o Brasil poderia considerar uma metodologia desenvolvida no Reino Unido, em que os participantes, em silêncio (mas não de forma anônima), contribuem para um único documento on-line em uma mesma sessão (Box 2.1). De modo semelhante, um grupo poderia identificar riscos para a integridade trabalhando conjuntamente em um mesmo documento on-line. Quando as atividades se aperfeiçoarem, o país também pode explorar a incorporação de conceitos qualitativos e quantitativos para a triangulação de riscos em setores-chave e a validação das percepções dos gestores sobre a probabilidade e o impacto dos riscos, com base em dados históricos, quando disponíveis.
- *Apoiar uma avaliação mais adequada de riscos para a integridade e um melhor uso da informação obtida.* Ao longo do processo, lembretes ou “toques” poderiam ser usados para salientar pressuposições típicas em avaliações humanas de eventos de risco. Em resumo, a ideia é fazer com que os agentes públicos envolvidos em avaliações de risco adotem um uso mais reflexivo da

informação e estejam menos sujeitos aos vieses descritos na seção anterior. Não há dúvida de que mesmo simples lembretes sobre possíveis preconcepções podem levar os gestores públicos a abandonar um modo de pensar intuitivo ou geralmente inconsciente, que poupa esforços mas está sujeito a vieses ("pensar rápido", ou "sistema 1"), em favor de um processo mental mais racional e consciente ("pensar devagar", ou "sistema 2") (Kahneman, 2013[24]).

Box 2.1. Conceitos comportamentais para a capacitação de funcionários em nível coletivo no Reino Unido

No Reino Unido, a Equipe de Conceitos Comportamentais (BIT) desenvolveu um processo de pensamento em grupo ("*ThinkGroup*") em que os participantes, em silêncio, mas não anonimamente, contribuem para um único documento *on-line* ao mesmo tempo. A BIT instituiu essa ferramenta para possibilitar aos participantes tanto interagir uns com os outros como seguir sua própria linha de pensamento, a fim de tornar a tempestade de ideias mais eficaz (Hallsworth et al., 2018[25]).

No documento *on-line*, os colaboradores podem escolher as ideias às quais desejam responder ou desenvolver, com base nas contribuições de outros participantes. Essa metodologia representa uma alternativa ou complemento útil às tradicionais discussões presenciais de *brainstorming*. Em uma reunião tradicional de tempestade de ideias, a atenção do grupo se concentra em uma ideia por vez, impedindo que os indivíduos desenvolvam sua própria linha de pensamento sobre diferentes aspectos da discussão.

Tal ferramenta também pode contribuir para melhorar o grau de abertura de uma organização, permitindo que os funcionários compartilhem ideias e preocupações. Por ser uma forma de interação menos direta e com menor possibilidade de confronto, o uso de um documento *on-line* pode parecer menos intimidador e dar aos participantes tempo para expressar adequadamente seus pensamentos e inquietações.

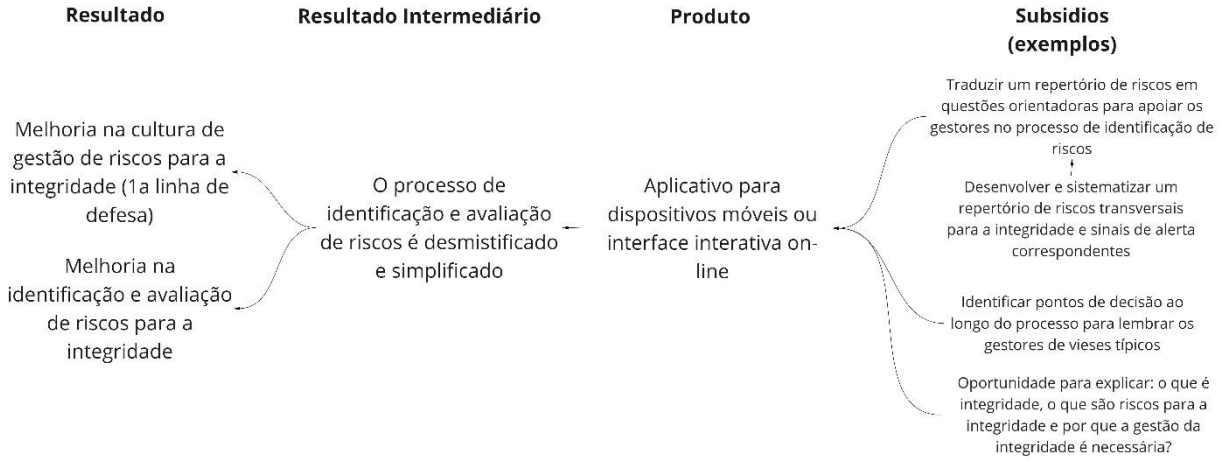
Fonte: (Hallsworth et al., 2018[25]).

Finalmente, as ferramentas de TI podem incorporar algumas dessas recomendações do campo comportamental e contribuir para o apoio aos gestores públicos ao longo do processo. Conforme mencionado no Capítulo 1, o Agatha atualmente não é um sistema suficientemente amigável e, por essa razão, não foi amplamente adotado na administração pública brasileira. Portanto, o Brasil poderia considerar uma revisão e uma simplificação do Agatha. Todavia, desenvolver um novo sistema do zero, em consonância com as orientações da CGU e os conceitos comportamentais, talvez represente uma solução mais fácil. O produto resultante poderia constituir uma interface de aplicativo para dispositivos móveis e/ou uma plataforma *on-line* para auxiliar os gestores públicos no processo de gestão dos riscos para a integridade. A ferramenta teria o objetivo de reduzir as contribuições dos gestores públicos a um mínimo estrito e, ao mesmo tempo, desempenhar a função pedagógica de esclarecer conceitos relacionados à integridade e à gestão de riscos. Para tanto, à CGU caberia elaborar, de forma prévia, orientações e informações automatizadas sobre os riscos para a integridade mais típicos e genéricos, para depois incorporá-los a essa interface. O Órgão já começou a trabalhar na sistematização de tais "riscos transversais para a integridade", que seriam usados como um ponto de partida. Esse trabalho poderia ser traduzido sob a forma de questões orientadoras para auxiliar os gestores e acompanhá-los ao longo do processo de identificação e avaliação de riscos para a integridade.

Essa interface, mais amigável e de simples utilização, poderia contribuir para desmistificar a gestão de riscos para a integridade e ajudar na superação dos receios e mal-entendidos recorrentes. Em última instância, tal interface proporcionaria a melhoria da qualidade das avaliações de riscos e a implementação

de culturas de gestão de riscos para a integridade nas instituições federais. A interface poderia ser promovida por meio das UGIs, a fim de garantir a participação de todas as instituições federais. Com o tempo, se um volume suficiente de participantes estiver usando a ferramenta, os dados coletados podem ser centralizados pela CGU, para subsidiar a elaboração de mapas de riscos setoriais ou regionais. A Figura 2.2 apresenta um panorama da teoria da mudança subjacente a tal ferramenta de TI para apoiar os gestores na gestão dos riscos para a integridade.

Figura 2.2. A teoria da mudança em uma interface de gestão de riscos para a integridade



Avançar na gestão de riscos para a integridade por meio do uso de dados e de ferramentas analíticas

O desenvolvimento dos Sistemas de Informação e Comunicação levou ao surgimento de um considerável volume de dados no setor público. Considerando a limitação humana para processar grandes quantidades de informação, os governos de todo o mundo começaram a adotar estratégias digitais para tirar proveito da miríade de dados que se multiplicaram nos últimos anos, criando novas oportunidades para melhorar a gestão de riscos para a integridade. Juntamente com os conceitos comportamentais discutidos na seção anterior, os dados e as ferramentas de análise podem facilitar ainda mais as futuras iniciativas da CGU na gestão e avaliação de riscos para a integridade (OECD, 2019[26]).

De fato, o uso de técnicas quantitativas e de análises de dados pode contribuir para a identificação de potenciais situações de fraude e corrupção em uma série de áreas nas quais os governos tendem a coletar dados confiáveis e válidos graças à emissão de sinais de alerta (OECD, 2021[27]). A inteligência artificial (IA), incluindo o aprendizado de máquina, possui um rico histórico de aplicações para a gestão de riscos, por exemplo, transformando dados estruturados e não estruturados em conceitos para a detecção e monitoramento de risco. Além de emitirem sinais de alerta, as ferramentas analíticas subsidiam a gestão de riscos para orientar a prevenção. Modelos preditivos podem fornecer dados para a tomada de decisão e ajudar os gestores a reagir aos riscos antes que estes se materializem (OECD, 2021[28]). Em geral, a qualidade das metodologias para avaliação de riscos baseadas em IA ou em análises estatísticas corresponde à qualidade dos dados disponíveis. Dados abertos e administrativos em áreas como infraestrutura pública, aquisições, folha de pagamento, serviços sociais, saúde e serviços de emprego costumam ter qualidade suficiente para seu uso e reuso.

O Brasil deu passos significativos para alavancar dados e ferramentas analíticas que podem ser usados para fins de integridade

A utilização de dados e ferramentas de análise para a integridade pública e redução de riscos é cada vez mais comum na América Latina. Colômbia e México são exemplos recentes dessa aplicação (OECD, 2021[28]; OECD, 2021[29]). O Brasil foi um dos primeiros países na região a adotar ferramentas de análise de dados e um pioneiro no seu uso para o controle e a transparência dos processos. Por exemplo, conforme mencionado no Capítulo 1, o Alice (Analisador de Licitações, Contratos e Editais) e o Faro (Ferramenta de Análise de Risco em Ouvidoria) destacam-se no contexto do apoio a auditorias e investigações. O Alice é uma ferramenta de Automação Robótica de Processos (RPA) que usa inteligência artificial (IA) para permitir a contínua auditoria de aquisições públicas e de processos de contratação. O Alice começou a ser implantado pela CGU em 2015 e, em 2016, pelo Tribunal de Contas da União (TCU). A ferramenta tem contribuído para o combate à corrupção em compras públicas. O Faro também é uma tecnologia baseada em IA, adotada em 2021 pela Ouvidoria-Geral da União (OGU, é uma das Secretarias da CGU) para automatizar a análise de denúncias enviadas pelos cidadãos por meio da plataforma *on-line* Fala.BR.

Alice

No Brasil, o alto volume de licitações representa um grande desafio analítico, considerando que, com base em informações fornecidas pelo país, são publicados em média 357 editais por dia. Além disso, muitas licitações permanecem abertas por apenas algumas semanas ou dias; por conseguinte, os auditores devem realizar avaliações de risco rapidamente, antes que os contratos sejam assinados, o que na prática é quase impossível. Com o objetivo de superar esse desafio, a CGU e o TCU iniciaram a implantação do Alice.

No TCU, por exemplo, essa ferramenta é programada para acessar diariamente o Comprasnet, o portal de compras do Governo Federal (https://www.gov.br/compras/pt-br), que registra dados sobre as aquisições públicas em âmbito federal. Na CGU, o Alice também é programado para recuperar dados do sistema Licitações-e e do Diário Oficial da União. O Licitações-e é o portal de aquisições do Banco do Brasil, também compartilhado com diversas empresas estatais e agências governamentais. A partir do Diário Oficial da União, o Alice extrai informações sobre licitações encerradas e não executadas. De acordo com informações atualizadas da CGU, o Alice baixa os documentos e dados de todos os editais e realiza correspondências de dados usando 223 bases de dados governamentais e 14 tipos de análises textuais para detectar sinais de má conduta e riscos nos documentos licitatórios, tais como manipulação de lances, restrições à concorrência, superfaturamento de preços e ausência de informações importantes no edital (Bemquerer Costa and Leitão Bastos, 2020[30]).

Por exemplo, o Alice analisa o “fator de materialidade”, que é uma estimativa de valor de riscos aplicada aos editais de licitação. Como os editais são salvos em PDF, o texto muitas vezes não é uniforme. O Alice aplica um algoritmo que obtém automaticamente os valores monetários das licitações a partir dos arquivos em PDF e organiza os dados aplicando o método de “floresta aleatória” (“*Random Forest*”) de classificação. Assim, segundo a CGU, um acordo atualmente em negociação com o Ministério da Economia permitirá que o Alice acesse diretamente o correto valor monetário dos editais. Para detectar irregularidades nas ofertas, o Alice também obtém informações relevantes a partir do Comprasnet e as salva em um repositório em formato computacionalmente legível para, mais tarde, cruzá-las com outros conjuntos de dados. Além disso, o TCU pactuou com a Receita Federal brasileira a obtenção de dados confidenciais relativos ao CNPJ dos proponentes como um identificador único para o cruzamento de referências das entidades ao longo de bases de dados e para a detecção de qualquer indício que possa constituir motivo de inelegibilidade durante a fase de ofertas.

O Alice vem gerando um impacto muito positivo no fortalecimento da prática de identificação de riscos no Brasil e no combate à corrupção em aquisições públicas no âmbito da administração federal. De acordo com informações fornecidas pela CGU, no primeiro ano de utilização do Alice, foram analisados mais de 100.000 editais e, entre dezembro de 2018 e novembro de 2019, oito licitações foram revogadas, totalizando um valor de aproximadamente R$ 3,2 bilhões. Além disso, foram suspensas 14 licitações devido a sinais de corrupção revelados pelo Alice, perfazendo um total de R$ 470 milhões. Em 2021, 139.566 licitações foram examinadas, 35.461 alertas de risco foram emitidos e 646 editais foram analisados por auditores, que abriram 70 processos de auditoria distintos. Segundo o relatório de atividades do TCU, em 2020, o montante decorrente das análises desenvolvidas por meio do sistema Alice totalizou mais de R$ 194 milhões (TCU, 2021[31]).

O Alice constitui um exemplo bem-sucedido de uso de dados e ferramentas analíticas para identificar sinais de alerta quanto a potenciais atos de corrupção e má conduta em aquisições, assim como para melhorar a eficiência do trabalho dos auditores. Podem-se apontar dois fatores subjacentes para o sucesso do instrumento:

- Um fator decisivo para a obtenção de resultados valiosos na identificação de riscos de corrupção em compras públicas foi o apoio da alta administração, o que é considerado um elemento fundamental para a consolidação de uma cultura de integridade. Por exemplo, o uso do Alice inovou a maneira como os auditores enfrentam as irregularidades que são descobertas. O fato de os auditores terem sido prontamente apoiados pelos Conselheiros do TCU, que concordaram em assinar uma Portaria validando o novo fluxo de trabalho, habilitou-os a agir da forma mais eficiente para abordar os riscos de corrupção identificados por essa tecnologia de inteligência artificial.
- Para evitar sobrecarregar os auditores com excesso de informações e compensar a dificuldade humana em lidar com grandes volumes de dados, tanto a CGU como o TCU adotaram duas estratégias para apoiar os auditores. Em primeiro lugar, o Alice envia e-mails diários com as informações mais importantes sobre as licitações e os alertas gerados pelo sistema, considerando as principais responsabilidades de cada área, capacitando os auditores, assim, a priorizar informações na condução de suas análises. Em segundo lugar, foi criado um painel para que permite aos auditores aplicar diferentes filtros para direcionar suas pesquisas, no qual podem ser encontradas informações mais detalhadas sobre a análises de editais conduzidas pelo Alice e as irregularidades resultantes.

Faro

No Brasil, a plataforma Fala.BR (https://falabr.cgu.gov.br/) foi criada para enfrentar o desafio de examinar as numerosas manifestações registradas pelos cidadãos por meio da internet. O Fala.BR é gerido pela CGU para substituir dois sistemas diferentes: o sistema de ouvidoria anteriormente denominado e-Ouv e o acesso ao sistema de informações antes conhecido como e-SIC. Trata-se de uma plataforma inovadora, que permite aos cidadãos não apenas requerer informações, mas também registrar reclamações ou alegações contra qualquer órgão federal, expressar satisfação ou insatisfação em relação a um serviço ou programa e oferecer sugestões para melhorar ou simplificar os serviços públicos (OECD, em preparo[32]). Na esfera federal, a Ouvidoria-Geral da União (OGU) é atualmente responsável por receber essas manifestações. A análise de aptidão é uma etapa-chave desse processo, durante a qual todos os materiais referentes às denúncias (seus textos e anexos) são examinados para verificar se cumprem os requisitos mínimos a serem aprofundados pelas áreas disciplinares ou pelas auditorias internas. Para conduzir essa análise, é necessário validar a informação indicada nos textos e complementá-las com outros dados externos.

O grande número de denúncias registradas, juntamente com o extenso volume de documentos a serem analisados, sobrecarrega a OGU e impede a entidade de agir de modo tempestivo para investigar os casos e adotar as medidas cabíveis. Além disso, para um entendimento completo dos fatos apontados

pelos cidadãos, geralmente é necessário considerar outras informações não apresentadas no texto das denúncias. Portanto, para automatizar o processo de exame e imprimir mais eficiência à análise de aptidão, em 2021 a OGU iniciou o uso do Faro, uma ferramenta de IA que auxilia o processo decisório sobre se uma denúncia deve continuar a ser investigada ou não. Além de automatizar os processos de identificação e de extração de certas variáveis dos textos das denúncias, essa ferramenta também enriquece os subsídios fornecidos pelos cidadãos, correlacionando-os com dados de 57 bases de dados externas, e, portanto, identificando novos elementos associados às denúncias.

A metodologia aplicada pelo Faro para automatizar a avaliação das denúncias e determinar se elas devem ou não ser levadas adiante envolve cinco passos principais (Paiva and Pereira, 2021[33]).

- Em primeiro lugar, na etapa de conversão, essa tecnologia lê todos os materiais anexos às denúncias, que geralmente se encontram em diferentes formatos (por ex., imagens, planilhas, PDFs, apresentações etc.) e muitas vezes não são computacionalmente legíveis. Esses anexos são transformados em formato de texto e as informações relevantes são extraídas e vinculadas aos textos originais das denúncias.
- Em segundo lugar, o Faro extrai as informações mais importantes dos textos das denúncias, como o nome dos contribuintes e empresas por meio do Cadastro de Pessoas Físicas (CPF) e do Cadastro Nacional de Pessoas Jurídicas (CNPJ), os números dos contratos e acordos, os valores monetários, assim como palavras ou expressões consideradas relevantes no contexto de uma possível falha de conduta indicada nas denúncias (por ex., fraude, corrupção, superfaturamento). Uma vez identificados, todos esses elementos são armazenados em uma base central de dados para serem usados ao longo da investigação.
- Em terceiro lugar, o Faro realiza um processo de expansão, que consiste em encontrar, nas 57 bases de dados externas, novas informações sobre as entidades previamente identificadas, a fim de comprovar sua existência e descobrir novos elementos e conexões. Por exemplo, quando um CNPJ específico é identificado no texto de uma denúncia, essa variável é primeiramente cruzada com outas bases de dados para checar se o CNPJ é válido. Na sequência, outros elementos derivados desse CNPJ são buscados, tais como as pessoas listadas como membros da entidade.
- O quarto passo consiste em qualificar as entidades identificadas nas etapas prévias. Como exemplo, no caso de um CPF, é possível verificar se ele pertence a um servidor público ou mesmo se a pessoa recebe benefícios oriundos de programas sociais.
- Finalmente, o Faro realiza uma elaboração de dados na qual as informações obtidas nos passos anteriores são agregadas, criando uma base de dados centralizada que é usada para treinar o modelo. Cada denúncia é representada por um conjunto de dados estruturados obtidos a partir dos textos originais das denúncias (anexos incluídos), assim como de informações provenientes de outras fontes.

Dessa maneira, o Faro demonstrou um significativo potencial para obter e agregar informações que não fazem originalmente parte das denúncias, assim como para aumentar a eficiência da análise dessas denúncias. O sistema minimiza o esforço de consultar manualmente diversos documentos e sistemas para a avaliação da conveniência e factibilidade da investigação das denúncias direcionadas à OGU por meio da plataforma Fala.BR.

Segundo dados fornecidos pela OGU, desde o começo de sua operação, em janeiro de 2020, o Faro foi responsável pela análise de 5.361 denúncias; destas, 40% foram automaticamente classificadas pelo sistema como não aptas ao avanço da investigação (as que alcançaram menos de 30 pontos) e 8% foram automaticamente classificadas como tendo elementos suficientes para o início da investigação (as que obtiveram mais de 80 pontos). Assim, a equipe da OGU foi capaz de concentrar seus esforços sobre os 52% restantes das denúncias, já previamente pontuadas e qualificadas pelo Faro com base em dados de outras bases governamentais, para decidir se elas continham ou não os elementos necessários ao trabalho das unidades investigativas.

A CGU poderia desenvolver uma estratégia e um plano de ação para desbravar o potencial das atuais metodologias de análise de dados para prevenir violações de integridade

Não obstante os avanços do Brasil no uso de dados e de ferramentas analíticas e os benefícios alcançados até o momento, ainda restam alguns desafios cruciais obter o máximo proveito do uso das análises de dados na gestão de riscos para a integridade entre as organizações do Executivo Federal brasileiro. Para incorporar efetivamente a cultura da gestão de riscos para a integridade nas entidades públicas e promover uma abordagem preventiva, é necessário implementar estratégias que possam ir além da simples identificação de sinais de alerta e de finalidades meramente investigativas.

Por exemplo, embora o sistema Alice ajude a identificar riscos para a integridade no contexto das licitações públicas, essa tecnologia foi primordialmente implementada pela CGU e pelo TCU para aumentar a eficiência do trabalho dos auditores, capacitando-os a analisar uma quantidade muito maior de editais e identificar sinais de alerta de corrupção na etapa de ofertas. De fato, apesar do avanço de ambas as entidades no uso da ciência de dados, de sua excelente estrutura de TI, dos resultados positivos alcançados e da expansão do uso do Alice para outros tribunais locais de contas (Projeto Alice nacional), a ferramenta é atualmente limitada a atividades investigativas nas aquisições públicas (Bemquerer Costa and Leitão Bastos, 2020[30]). Além disso, embora as compras públicas representem uma área crucial no que se refere aos riscos para a integridade, ela não é a única; nesse sentido, o Brasil poderia aprofundar a aplicação das ferramentas analíticas em outros campos, como para as análises de concessões de bolsas e subsídios ou despesas com viagens, por exemplo.

Portanto, a CGU poderia se beneficiar das equipes técnicas e do amadurecimento já alcançado na aplicação da ciência de dados para desenvolver uma estrutura tecnológica que auxilie a gestão de riscos para a integridade nas entidades de todo o Executivo Federal e que seja baseada, fundamentalmente, em modelos preditivos. Para tanto, cabe à CGU desenvolver uma estratégia e um plano de ação para o uso de dados e análises que levem em consideração o contexto de integridade e anticorrupção específico da administração pública federal. Nesse exercício, a coordenação e o compartilhamento de informações entre a CGU e o TCU poderia ser considerado.

Essa estratégia e plano de ação poderiam ter como base os seguintes procedimentos:

- *Mapear as bases de dados relevantes para a avaliação dos riscos para a integridade.* Tal mapeamento inclui um inventário de todas as bases de dados potencialmente disponíveis para fortalecer a capacidade da CGU de avaliação de riscos para a integridade. O mapeamento pode se estruturar sobre o considerável trabalho já realizado pela CGU e não ser puramente descritivo, mas incluir uma análise da qualidade, acessibilidade e relevância dos dados para a avaliação de riscos para a integridade. Esse mapeamento também poderia incluir uma análise das bases de dados prioritárias para seguir aprimorando a estratégia de análise de dados no futuro.
- *Revisar e desenvolver uma análise comparativa da estratégia e capacidade das ferramentas analíticas*. O uso de dados e análises depende da existência de estratégias que tenham objetivos claramente articulados, assim como de uma série de pré-condições e capacidades técnicas. A CGU poderia examinar essas áreas, incluindo a governança, gestão e capacidade de dados disponíveis para avaliar os riscos para a integridade. Essa análise ofereceria um mapa situacional claro das áreas que necessitam de melhoria no desenvolvimento e implementação da estratégia e do plano de ação.
- *Desenvolver um modelo de avaliação de riscos para a integridade orientado por dados*. Esse modelo deve refletir a maturidade da CGU com base em diferentes fatores, incluindo a criação de uma plataforma que congregue diversas bases de dados relacionadas à integridade. O modelo deve ser ambicioso, atualizado e teoricamente sólido. Ampliando a experiência com o Faro, a CGU poderia empregar os mais recentes avanços em aprendizado de máquina e inteligência

artificial, como está sendo feito pela Espanha com o apoio da OCDE (OECD, 2021[27]). Outras técnicas poderiam incluir uma pontuação de riscos baseada em indicadores, por exemplo. O objetivo do modelo vai além do mero cruzamento de bases de dados e visa adotar ferramentas de IA que apoiem diretamente a gestão de riscos para a integridade, detectando padrões, realizando previsões e fornecendo ideias úteis.

- *Realização de capacitações*. A estratégia e o plano de ação devem identificar e incluir objetivos relacionados à oferta de treinamento e à realização de oficinas para apoiar a implementação do modelo de riscos e abordar alguns dos desafios identificados. Essas oficinas são uma oportunidade de reunir participantes de todo o Executivo Federal, conforme o caso, para promover o modelo e aperfeiçoar a identificação de riscos. A CGU pode apoiar as entidades públicas com o uso das informações obtida por meio das ferramentas analíticas (ver a seção seguinte). Isso ajudaria a fortalecer ainda mais o SIPEF e permitiria à CGU, enquanto órgão central do sistema, estender a gestão de riscos para a integridade em nível institucional em todo o Executivo Federal.

Fortalecer o apoio organizacional para a gestão de riscos para a integridade e capacitar os gestores públicos

Além de desmistificar e simplificar a gestão de riscos para a integridade, aplicando análises de dados para auxiliar os gestores públicos, é essencial continuar a desenvolver a capacidade de gestão dos riscos para a integridade em todo o Executivo Federal brasileiro. Isso inclui a promoção de apoio organizacional, o treinamento regular das equipes, o compartilhamento de boas práticas e a oferta de orientação *ad hoc*, entre outros, e abrange áreas como conceitos, riscos genéricos para a integridade e metodologias de avaliação de riscos, assim como letramento em dados e TI.

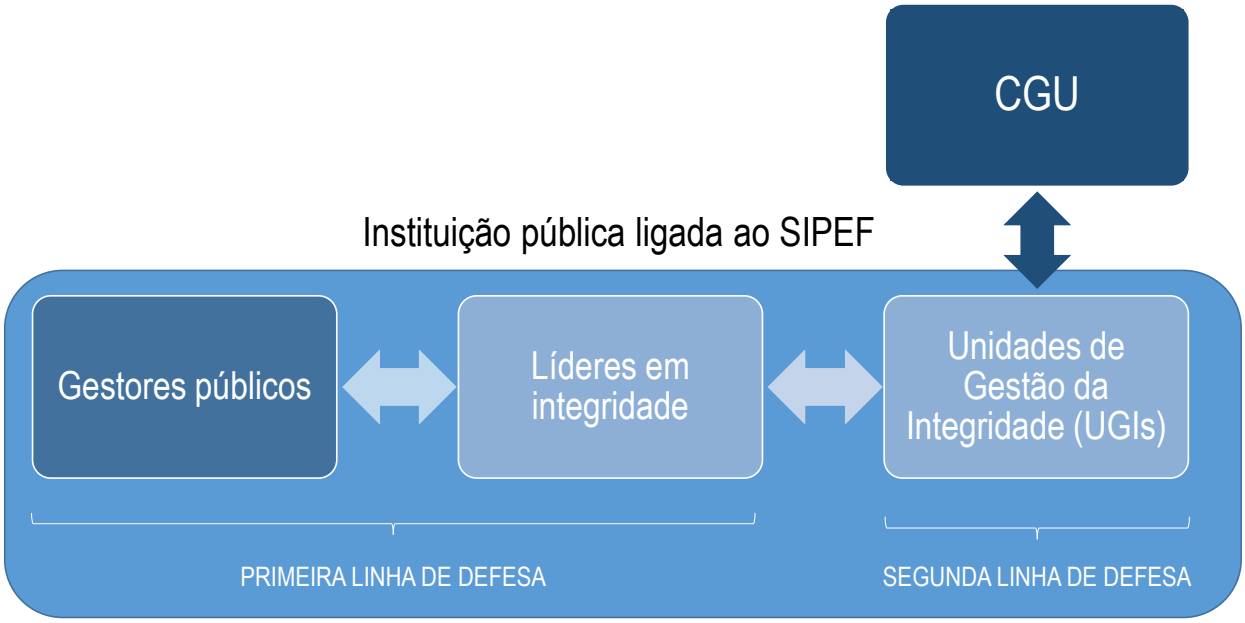
Para alcançar todas as áreas do Executivo Federal, as Unidades de Gestão da Integridade (UGIs) desempenham um papel fundamental no Sistema de Integridade Pública do Poder Executivo Federal (SIPEF). As UGIs são responsáveis por oferecer capacitações e prestar assistência às áreas responsáveis pela gestão de riscos para a integridade, incluindo orientações sobre o uso das ferramentas de análise de dados (OECD, 2021[7]). Concretamente, o Decreto nº 10.756/2021, que estabelece o SIPEF, dispõe que as UGIs devem coordenar a gestão de riscos para a integridade. Além disso, elas são responsáveis por conduzir a elaboração de um Plano de Integridade institucional, que deve ter por base uma análise de riscos para a integridade (CGU, 2018[9]; CGU, 2018[34]). Essa responsabilidade é crucial para a qualidade dos Planos de Integridade, e as medidas preventivas propostas dependem, sobretudo, da qualidade das avaliações de risco.

Portanto, em vista do papel central da gestão de riscos para a integridade, a fim de garantir a relevância, eficiência e eficácia das medidas de integridade implementadas nas instituições públicas federais, a CGU deve priorizar a qualificação das equipes das UGIs nessa área. As UGIs, por sua vez, podem consolidar seu papel como segunda linha de defesa para alcançar os gestores públicos, fornecendo-lhes orientações e apoio. Nesse sentido, o relatório da OCDE sobre o SIPEF já havia enfatizado que as UGIs, em particular, podem promover um melhor entendimento sobre a importância da gestão de riscos para a integridade entre os gestores públicos (OECD, 2021[7]). As UGIs devem ser capazes de comunicar claramente a base lógica da gestão de riscos para a integridade, contribuindo para desmistificar o conceito e reduzir os temores e mal-entendidos a ele relacionados. Ademais, as UGIs devem fornecer orientação e assistência aos gestores públicos. Para tanto, e com o auxílio da Coordenação-Geral de Integridade Pública da CGU, as UGIs necessitam desenvolver capacidades para a realização de avaliações de riscos para a integridade e oferecer apoio aos gestores públicos, se necessário.

Todavia, para promover uma cultura de gestão de riscos para a integridade nos níveis organizacionais, tais medidas são necessárias, mas talvez insuficientes. A fim de alcançar uma mudança cultural, além de intervir diretamente nas rotinas, políticas e procedimentos institucionais e de oferecer treinamento, os

conceitos comportamentais sugerem a importância de influenciar indivíduos específicos nessas organizações para garantir mudanças em toda a organização (OECD, 2020[35]). No relatório da OCDE sobre a integridade das lideranças no Brasil, destaca-se o papel dos líderes e dos gestores como exemplos para a promoção de culturas institucionais de integridade (OECD, em preparo[36]). O mesmo se aplica, naturalmente, à gestão de riscos para a integridade. Portanto, as UGIs poderiam iniciar a identificação de um conjunto de gestores públicos em suas entidades que já são líderes ou que mostram potencial para tanto, os quais se tornariam elementos de ligação com outros gestores públicos, uma fonte de conhecimento e informação, e, não menos importante, modelos a serem seguidos (Figura 2.3).

Figura 2.3. O papel da CGU, das UGIs e dos líderes em integridade na promoção de culturas de gestão de riscos para a integridade no Executivo Federal brasileiro



Finalmente, a CGU não está apenas na função de fornecer subsídios e realizar capacitações dentro do SIPEF. A gestão de riscos para a integridade também oferece à CGU uma oportunidade única de obter informações quantitativas e qualitativas sobre riscos para a integridade coletados no nível de cada entidade, além de receber devolutivas e catalogar boas práticas. Essas informações sobre riscos para a integridade e medidas de integridade adotadas podem ser analisadas de modo centralizado e comparativo pela Coordenação-Geral de Integridade Pública da CGU, a fim de se chegar a conclusões acerca de riscos emergentes e variáveis para a integridade, por exemplo, ou sobre o que funciona e por que na mitigação desses riscos. Para fins analíticos, essas informações oriundas de instituições públicas ligadas ao SIPEF podem ser agregadas em âmbito federal, ou de modo a representar setores, regiões ou processos específicos, tais como as aquisições públicas ou a gestão de recursos humanos, por exemplo.

Referências

Ball, D. and J. Watt (2013), “Further Thoughts on the Utility of Risk Matrices”, *Risk Analysis*, Vol. 33/11, pp. 2068-2078, https://doi.org/10.1111/risa.12057. [18]

Bemquerer Costa, M. and P. Leitão Bastos (2020), “Alice, Monica, Adele, Sofia, Carina e Ágata: o uso da inteligência artificial pelo Tribunal de Contas da União”, *Controle Externo: Revista do Tribunal de Contas do Estado de Goiás*, Vol. 2/3, pp. 11-34. [30]

CGU (2018), *Guia Prático das Unidades de Gestão de Integridade*, Controladoria-Geral da União (CGU), Brasilia, https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/unidades-de-gestao.pdf (accessed on 17 August 2021). [34]

CGU (2018), *Guia Prático de Gestão de Riscos para a Integridade: Orientações para a Administração Pública Federal direta, autárquica e fundacional*, Controladoria Geral da União (CGU), Brasilia, https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/manual-gestao-de-riscos.pdf (accessed on 4 August 2021). [8]

CGU (2018), *Guia Prático de Implementação de Programa de Integridade Pública*, Controladoria-Geral da União (CGU), Brasilia, https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/integridade-2018.pdf (accessed on 17 August 2021). [9]

Falk, A. and M. Kosfeld (2006), “The Hidden Costs of Control”, *American Economic Review*, Vol. 96/5, pp. 1611-1630. [20]

Hallsworth, M. et al. (2018), *Behavioural Government: Using behavioural science to improve how governments make decisions*, Behavioural Insights Team, London, https://www.bi.team/wp-content/uploads/2018/08/BIT-Behavioural-Government-Report-2018.pdf (accessed on 20 January 2022). [25]

Kahneman, D. (2013), *Thinking, fast and slow*, Farrar, Straus and Giroux. [24]

Kahneman, D. and A. Tversky (1982), “On the study of statistical intuitions”, *Cognition*, Vol. 11/2, pp. 123-141, https://doi.org/10.1016/0010-0277(82)90022-1. [14]

Kahneman, D. and A. Tversky (1979), “Prospect theory: An analysis of decision under risk”, *Econometrica*, Vol. 47/2, pp. 263-292, https://doi.org/10.2307/1914185. [19]

Kahneman, D. and A. Tversky (1972), “Subjective probability: A judgment of representativeness”, *Cognitive Psychology*, Vol. 3/3, pp. 430-454, https://doi.org/10.1016/0010-0285(72)90016-3. [15]

Loewenstein, G. et al. (2001), “Risk as feelings.”, *Psychological Bulletin*, Vol. 127/2, pp. 267-286, https://doi.org/10.1037/0033-2909.127.2.267. [17]

OECD (2021), *Countering Public Grant Fraud in Spain: Machine Learning for Assessing Risks and Targeting Control Activities*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/0ea22484-en. [27]

OECD (2021), *Preventive and Concomitant Control at Colombia’s Supreme Audit Institution: New Strategies for Modern Challenges*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/a2bdadf3-en. [28]

OECD (2021), *Progress report on the implementation of the Mexican Superior Audit of the Federation’s mandate: Increasing impact and contributing to good governance*, OECD, Paris, https://www.oecd.org/governance/ethics/progress-report-on-the-implementation-of%20the-Mexican-Superior-Audit-of-the-Federation-s-mandate.pdf (accessed on 27 January 2022). [29]

OECD (2021), *Strengthening Public Integrity in Brazil: Mainstreaming Integrity Policies in the Federal Executive Branch*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/a8cbb8fa-en. [7]

OECD (2020), *Behavioural Insights and Organisations: Fostering Safety Culture*, OECD Publishing, Paris, https://doi.org/10.1787/e6ef217d-en. [35]

OECD (2020), *OECD Public Integrity Handbook*, OECD Publishing, Paris, https://doi.org/10.1787/ac8ed8e8-en. [1]

OECD (2019), *Analytics for Integrity: Data-driven Approaches for Enhancing Corruption and Fraud Assessments*, OECD, Paris, http://www.oecd.org/gov/ethics/analytics-for-integrity.pdf. [26]

OECD (2019), *La Integridad Pública en América Latina y el Caribe 2018-2019: De Gobiernos reactivos a Estados proactivos*, OECD, Paris, https://www.oecd.org/gov/ethics/integridad-publica-america-latina-caribe-2018-2019.pdf. [4]

OECD (2018), *Behavioural Insights for Public Integrity: Harnessing the Human Factor to Counter Corruption*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/9789264297067-en. [21]

OECD (2018), *National Risk Assessments: A Cross Country Perspective*, OECD Publishing, Paris, https://doi.org/10.1787/9789264287532-en. [3]

OECD (2017), *Recommendation of the Council on Public Integrity*, OECD/LEGAL/0435, OECD, Paris, http://www.oecd.org/gov/ethics/Recommendation-Public-Integrity.pdf. [2]

OECD (2012), *OECD Integrity Review of Brazil: Managing Risks for a Cleaner Public Service*, OECD Public Governance Reviews, OECD Publishing, Paris, https://doi.org/10.1787/9789264119321-en. [6]

OECD (em preparo), *Behavioural Insights for Public Integrity: Strengthening integrity leadership in Brazil’s federal executive branch*, OECD Publishing, Paris. [36]

OECD (em preparo), *OECD Integrity Review of Brazil*, OECD Publishing, Paris. [5]

OECD (em preparo), *Open Government Review of Brazil*, OECD Publishing, Paris. [32]

Ortega Nieto, D. et al. (2021), *Ethics and Corruption in the Federal Public Service: Civil Servants' Perspectives (English)*, World Bank Group, Washington D.C., http://documents.worldbank.org/curated/en/559381639027580056/Ethics-and-Corruption-in-the-Federal-Public-Service-Civil-Servants-Perspectives (accessed on 10 January 2022). [11]

Paiva, E. and F. Pereira (2021), "Extraction and enrichment of features to improve complaint text classification performance", *Anais do Encontro Nacional de Inteligência Artificial e Computacional (ENIAC)*, pp. 338-349, https://doi.org/10.5753/ENIAC.2021.18265. [33]

Schulze, G. and B. Frank (2003), "Deterrence Versus Intrinsic Motivation: Experimental Evidence on the Determinants of Corruptibility", *Economics of Governance*, Vol. 4/2, pp. 143-160, https://doi.org/10.1007/s101010200059. [22]

Slovic, P. (1999), "Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield", *Risk Analysis*, Vol. 19/4, pp. 689-701, https://doi.org/10.1111/J.1539-6924.1999.TB00439.X. [12]

Sunstein, C. and R. Hastie (2015), *Wiser: Getting Beyond Groupthink to Make Groups Smarter*, Harvard Business Review Press, Cambridge. [23]

Sunstein, C. and R. Hastie (2014), *Making Dumb Groups Smarter*, Harvard Business Review, https://hbr.org/2014/12/making-dumb-groups-smarter (accessed on 20 January 2022). [13]

TCU (2021), *Relatório anual de atividades do TCU : 2020*, Secretaria-Geral da Presidência (Segepres), Brasilia, https://portal.tcu.gov.br/data/files/99/64/46/8E/7298871003178887E18818A8/relatorio_anual_atividades_TCU_2020.pdf (accessed on 10 January 2022). [31]

TCU (2014), *Survey of Risk Management in Public Governance, Gestão De Riscos Levantamento De Governança*, Tribunal de Contas da União (TCU), Brasilia, http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24E08D405014E0D42E95B3708 (accessed on 4 August 2021). [10]

Tversky, A. and D. Kahneman (2007), "Judgment under Uncertainty: Heuristics and Biases", *Science*, Vol. 185/4157, pp. 1124-1131. [16]

Modernizando a avaliação dos riscos para a integridade no Brasil

RUMO A UMA ABORDAGEM COMPORTAMENTAL E ORIENTADA POR DADOS

A Recomendação da OCDE sobre Integridade Pública coloca a gestão de riscos no centro de qualquer estratégia ou abordagem para garantir e promover a integridade pública. Este relatório analisa a metodologia atual de avaliação de riscos para a integridade no Poder Executivo federal brasileiro, sob a ótica de *insights* comportamentais e do uso de dados. Após apresentar a metodologia e analisar os desafios relacionados à sua implementação, o relatório fornece três caminhos concretos para o fortalecimento e modernização da abordagem atual: reconhecer e enfrentar barreiras cognitivas e sociais, alavancar esforços contínuos para melhorar o uso de dados e análises para fins preventivos e fortalecer o apoio organizacional à gestão dos riscos para a integridade, promovendo uma cultura de gestão de riscos nas instituições públicas do Poder Executivo federal.

PDF ISBN 978-92-64-45848-2

9 789264 458482