Será este o momento da verdade para a integridade corporativa?

Relatório de Integridade 2021
Portugal

Quanto melhor a pergunta. Melhor a resposta.
Melhor trabalha o Mundo.

EY
Building a better working world

Enquadramento

A pandemia global da COVID-19 teve um impacto significativo a nível mundial, com consequências sobre as famílias, organizações e a sociedade em geral. No meio desta crise, as organizações e os governos foram confrontados com a necessidade de tomar decisões difíceis, que afetaram a sua operação e viabilidade.

As organizações têm que decidir a melhor forma de proteger os seus colaboradores e clientes, enquanto detentores de um papel ativo na sociedade. Os Conselhos de Administração que têm de avaliar como remunerar os seus acionistas e que procuram apoio financeiro por parte do Estado, enfrentam novos desafios ao nível da integridade das suas organizações. Fazer o que está certo nunca foi tão difícil, uma vez que o nível de escrutínio dos negócios por parte da sociedade intensificou-se. As decisões tomadas pelas organizações e governos em contexto de crise, no auge da pandemia, serão avaliadas nos próximos anos. Agir com integridade é agora mais importante do que nunca.

O estudo realizado pela EY revela um conjunto de desafios éticos enfrentados pelas organizações, tanto no período que antecedeu a crise da COVID-19, como no auge da mesma. Durante o mês de março de 2021, 103 participantes responderam a este estudo de forma anónima, o qual utilizou uma metodologia que excluiu respostas inválidas. Os participantes deste estudo representam diferentes posições hierárquicas, nomeadamente membros de Conselhos de Administração, posições de gestão e outros colaboradores em *ranks* juniores.

A nível global, 90% considera que os efeitos da COVID-19 poderão aumentar os riscos de comportamentos antiéticos na sua organização. Apesar de ser pequena a percentagem de colaboradores que assume a disponibilidade para agir de forma antiética, para ganho pessoal, a pandemia agrava o risco de comportamentos irregulares. Observa-se, também, uma disparidade quanto às perceções de ética comportamental nos diferentes níveis hierárquicos dentro das organizações. Os colaboradores juniores confiam na integridade dos seus líderes. E os membros de Conselhos de Administração confiam no cumprimento das regras de integridade nas suas organizações. A generalidade dos inquiridos, considera que deve agir com integridade na vida interna da sua organização e na relação com terceiros, adotando medidas que minimizem o risco e cumprindo as disposições legais e regulatórias, em vigor.

> “Atualmente, organizações de todos os setores passam por desafios críticos para a sustentabilidade dos seus negócios e para a sua integridade. A COVID-19 veio acentuar esses desafios. Acresce que a curto prazo, em Portugal, as organizações terão de alinhar-se com novos requisitos legais, que decorrerão da recém aprovada Estratégia Nacional de Anticorrupção e da Diretiva Europeia de "Whistleblowing".

Pedro Subtil
Forensic & Integrity Services Leader
Portugal, Angola e Moçambique

Este relatório vem na sequência do anterior *Global Fraud Survey* e destaca quatro *call-to-action* críticas para as organizações priorizarem, nas suas agendas de integridade, bem como insights sobre os desafios éticos amplificados pela crise: conduta pessoal, *whistleblowing* (canais utilizados para reportar irregularidades), conduta de terceiros e integridade de dados.

1 **Ação 1** | *página 6*
Incorpore a integridade corporativa para se proteger contra a conduta antiética

2 **Ação 2** | *página 10*
Whistleblowing: Implemente canais de reporte de irregularidades anónimos e confidenciais

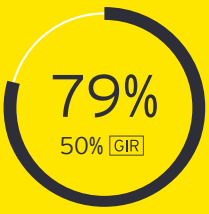
3 **Ação 3** | *página 12*
Construa uma relação de confiança com terceiros baseada na integridade

Key findings

Demonstrar integridade

Fazer o que está correto significa mais do que evitar penalizações financeiras.

Atrair novos clientes

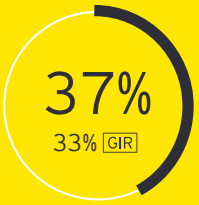


Ter uma reputação corporativa mais forte

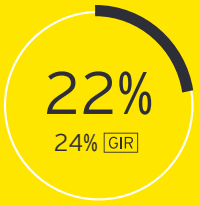
Minimizar os riscos de ações regulatórias/legais

COVID-19

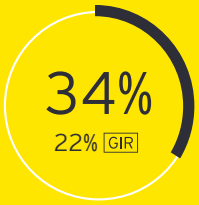
Para além do agravamento das condições de mercado, os inquiridos acreditam que os maiores riscos resultantes da Covid-19 à conduta ética são:



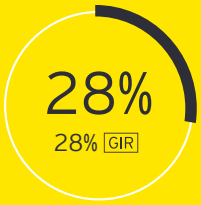
Interferência nos modelos de trabalho tradicionais



Redução dos benefícios e remuneração dos funcionários



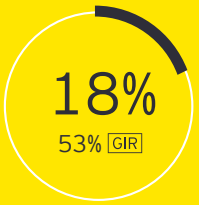
Deterioração das condições de mercado



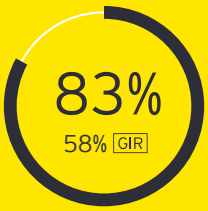
Declínio do desempenho financeiro da sua organização

Conduta Pessoal

Colaboradores juniores nem sempre acreditam na integridade dos seus líderes



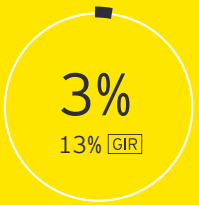
dos colaboradores juniores não estão inteiramente confiantes de que a Gestão da organização obedeça às leis relevantes, códigos de conduta e regulações do setor



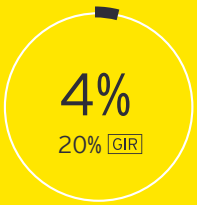
dos membros do Conselho de Administração entrevistados acreditam que a Gestão da organização atua de acordo com as regras

Conduta de Terceiros

Os gestores em cargos seniores estão preparados para ignorar más condutas de terceiros



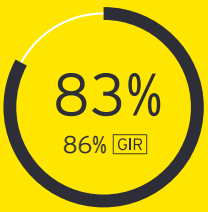
dos inquiridos estariam dispostos a ignorar comportamentos antiéticos por parte de terceiros a fim de melhorar a sua progressão de carreira ou remuneração



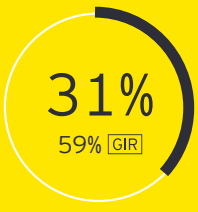
dos membros do Conselho de Administração, que responderam a este questionário, estariam dispostos a ignorar comportamentos antiéticos por parte de terceiros a fim de melhorar a sua progressão de carreira ou remuneração

Integridade dos Dados

As organizações estão com excesso de confiança sobre a proteção de dados



dos inquiridos dizem que estão bastante ou muito confiantes de que a sua organização está a fazer de tudo para proteger a privacidade dos dados do cliente



das organizações não forma os seus funcionários em obrigações regulamentares de privacidade de dados, tal como o Regulamento Geral de Proteção de Dados (RGPD)

4

Ação 4 | *página 16*
Proteja os dados de forma ética salvaguardando o seu valor

GIR

Nota: Ao longo deste relatório, todos os gráficos incluem a comparação com valores do 'Global Integrity Report' (**GIR**), estando este valor sempre ao lado do ícone criado.

Em algumas das perguntas por diferença de dados específicos da geografia Portuguesa, não foi possível observar a comparação com o Global Integrity Report.

O caso para integridade nos negócios

O desenvolvimento de um programa de integridade não protege apenas as organizações, evitando multas e penalizações. Esta ação pode também ajudá-los a prosperar financeiramente e a proporcionar valor a longo prazo para os seus acionistas. Por exemplo, o estudo da Ethisphere identificou que as organizações mais éticas a nível mundial superaram o Large Cap Index dos EUA em 13,5% durante um período de cinco anos.

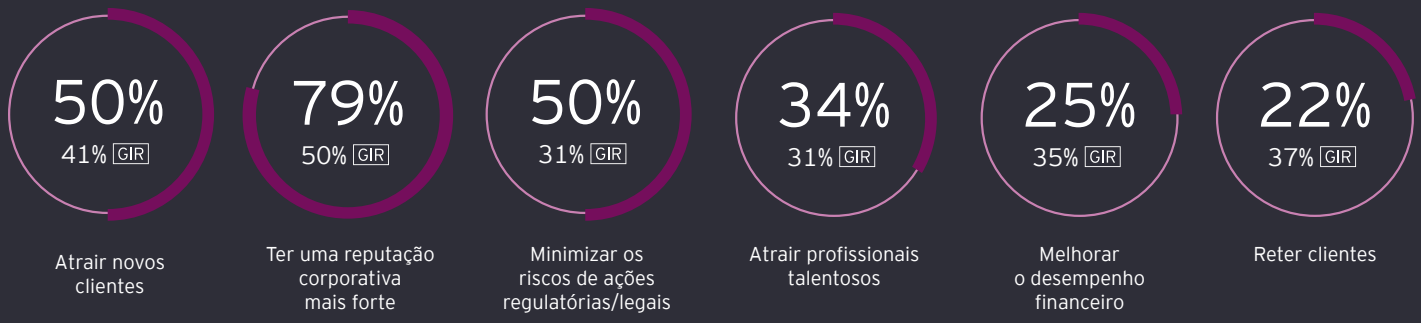
Todos os entrevistados acreditam que é importante demonstrarem que trabalham com integridade e 97% concordam que isso traz benefícios à sua organização.

Pela experiência que a EY tem vindo a adquirir, as organizações orientadas por objetivos que colocam a integridade no centro de tudo o que fazem, são mais resilientes e estarão em melhor posição para enfrentar os desafios organizaçãoriais acelerados pela pandemia COVID-19.

As organizações que promovem parcerias fortes com as principais partes interessadas (como os seus fornecedores, colaboradores, investidores, comunidades que atendem, reguladores e governos) baseadas na confiança têm operações mais robustas e ágeis que se podem adaptar rapidamente, à medida do desenrolar dos acontecimentos.

Os primeiros sinais já são visíveis em mais de 70% dos fundos ESG. Todas as classes de ativos tiveram um melhor desempenho do que os seus homólogos durante os primeiros quatro meses de 2020.

Os benefícios mais importantes de operar com integridade são:



Pergunta: Entre os possíveis benefícios de operar com integridade, quais são os três mais importantes para a sua organização?

Características de integridade

Quando se trata de operar com integridade, ligeiramente mais de metade (53%) dos entrevistados acreditam que a característica mais importante da integridade é cumprir as regras, leis e regulamentos. Esta foi a definição mais popular, seguida de respeito pelos valores da organização (45%), tolerância zero em relação a más condutas (40%) e transparência nas atividades desenvolvidas (40%).

Na EY, acreditamos que a integridade corporativa significa fazer o que nos propomos, com um elevado grau de compromisso. Trata-se de fazer o que está certo, porque é o correto a fazer e não apenas porque um código de conduta o descreve. A integridade gera confiança, orienta as organizações a gerirem bem os dados e protege contra a tentação de procurar ganhos de curto prazo em detrimento do comportamento ético.

Neste estudo, examinaram-se quatro áreas críticas do programa de integridade: conduta ética a nível pessoal e organizacional, *whistleblowing*, gestão de terceiros e proteção de dados. O impacto da pandemia COVID-19 tem ramificações importantes para as quatro áreas, pois os colaboradores, as cadeias de abastecimento e a segurança dos sistemas de informação estão sujeitos a novos riscos e tensões.

Um programa de integridade eficaz pode proteger as organizações de ameaças emergentes, ajudando-as a sobreviver e prosperar.

A crise pandémica é um momento importante para a Integridade Corporativa?

Os participantes neste inquérito são unanimes: a pandemia de COVID-19 acentuou os desafios à integridade e conduta ética empresarial. Consequentemente, o comportamento organizacional estará sob escrutínio, como nunca. Neste contexto, a fim de preservar a sua integridade durante e enquanto a crise pandémica perdurar, as organizações devem adotar quatro ações críticas.

A primeira (1) respeita à necessidade de incorporar a integridade corporativa no ADN da organização, passando da palavras à ação: a adoção de mecanismo efetivos de *compliance* é essencial. Agir com integridade é um dever de todos os intervenientes na vida da organização, desde o CEO e membros do Conselho de Administração, a gestores e colaboradores juniores, passando pelos parceiros de negócios, fornecedores e outros *stakeholders* – a conduta destes agentes reflete os valores organizacionais, e vice-versa.

A segunda (2) ação consiste em dotar as organizações com mecanismos de denúncia e reporte eficientes, a fim de detetar irregularidades e comportamentos antiéticos.

A terceira (3) ação crítica diz respeito à relação com terceiros, baseada na integridade. À medida que crescem e amplificam o seu âmbito de atuação, as organizações criam interdependência com terceiros que as representam ou agem em seu nome, numa variedade de mercados. A nossa experiência revela que parcerias de confiança com partes terceiras conferem às organizações maior resiliência e poder negocial nas cadeias de abastecimento, e uma maior fidelização de clientes, sobretudo na comparação com as organizações que operam apenas através de relações transacionais.

Finalmente, a quarta (4) ação crítica que propomos passa pela proteção de dados, gerindo-os de forma ética. A transformação digital tem permitido às organizações a otimização de operações e o tratamento, gestão e proteção de enormes quantidades de dados. Esta nova realidade traz desafios emergentes e reclama avaliações de risco adequadas, formação dos colaboradores e incorporação de regulamentações e quadros normativos.

Estas quatro ações-chave são impulsionadas pelos resultados do nosso estudo:

71%

30% GIR

Observa-se que 71% dos inquiridos responderam não estar dispostos a agir de forma antiética a fim de melhorar a sua progressão profissional ou pacote remuneratório. O nosso relatório mostra que este tipo de comportamento continua a acontecer e pode até difundir-se como resultado da pandemia visto que os colaboradores temem pelos seus empregos e salários. Os inquiridos acreditam que a interferência nos modelos tradicionais de trabalho (37%) e a deterioração das condições do mercado (34%) são dos riscos mais elevados para a conduta organizacional.

45%

58% GIR

Os colaboradores juniores referem que os colaboradores da sua empresa não podem relatar irregularidades sem medo de sofrerem consequências negativas. Em contraste, 100% dos membros dos Conselhos de Administração referem que é possível reportar um comportamento antiético sem sofrer represálias.

A equipa de gestão precisa de construir a confiança dos seus colaboradores através de uma comunicação clara de valores, do cumprimento transparente das regras e da possibilidade de garantir formas seguras de os trabalhadores denunciarem irregularidades.

23%

34% GIR

Dos inquiridos, apenas 23% apresentam-se muito confiantes sobre os seus terceiros demonstram integridade no trabalho que fazem. Como as organizações fazem o que é necessário para satisfazer as necessidades comerciais de curto prazo, novas terceiras partes de alto risco poderão ser contratadas, que não partilham a mesma cultura de integridade. O nosso estudo reforça esta mensagem, observando que 13% dos inquiridos referem que a rutura das cadeias de abastecimento é um dos maiores riscos para a conduta ética nos negócios.

41%

59% GIR

Dos respondentes, 41% consideram que as organizações onde trabalham não dão formação aos colaboradores, sobre privacidade de dados e regulamentação aplicável, tal como o RGPD (2016/679).

A COVID-19 acelerou os riscos para a segurança de dados, visto que a rápida mudança para o trabalho à distância abriu oportunidades aos ciber-criminosos para visar empregados que não estejam preparados para lidar com dados sensíveis e com a devida segurança.

Ação 1 2 3 4

Incorpore a integridade corporativa para se proteger contra a conduta antiética

1

Normalmente procura-se três características num colaborador: inteligência, energia e integridade. Se o colaborador não apresentar a última característica, não vale a pena preocuparmo-nos com as duas primeiras.

A integridade é hoje mais importante do que nunca. Ao mesmo tempo que as organizações respondem aos efeitos da COVID-19 e às eventuais mudanças de prioridades, antecipar o futuro é essencial, bem como capacitar as áreas de *compliance* para mitigar os riscos a que estão expostas.

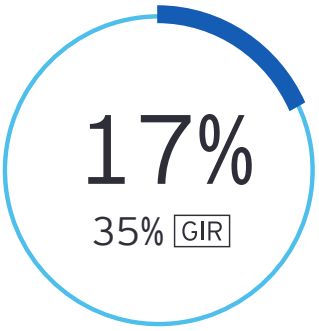
Em tempos de crise, a conduta pessoal pode ser o primeiro *standard* a ser negligenciado. Por exemplo, no auge da pandemia COVID-19, os colaboradores poderão ter identificado oportunidades para oferecer subornos ou outros tipos de pagamento ilícitos para obterem produtos de difícil aquisição.

As organizações não são máquinas. São sistemas complexos, constituídos por pessoas com instintos e comportamentos individuais, que são influenciados pelo meio.

Neste sentido, é crucial entender as pessoas que compõe a sua organização e o ambiente no qual operam, para haver uma proteção contra condutas antiéticas.

No nosso estudo, 17% dos entrevistados acreditam que o comportamento antiético da sua organização é frequentemente tolerado quando envolve colaboradores de cargos seniores ou colaboradores de desempenho elevado.

A mesma percentagem de gestores seniores respondeu de igual forma.



Acreditam que o comportamento antiético da sua organização é frequentemente tolerado, quando envolve colaboradores seniores ou funcionários de desempenho elevado.

Além disso, 21% dos entrevistados acreditam que existem cargos de chefia na sua organização que sacrificariam a integridade por ganhos financeiros a curto prazo. Este número aumenta para 30% se apenas tivermos em conta as respostas de colaboradores em cargos de gestão.

O nosso estudo demonstra que quanto mais sénior um colaborador é, maior é a probabilidade de ele ter comportamentos antiéticos. Os colaboradores seniores são mais propensos a justificarem comportamentos antiéticos, a ignorarem condutas antiéticas na sua equipa, a enganarem entidades externas como auditores ou reguladores e a oferecerem/aceitarem subornos de modo a impulsionarem a progressão das suas carreiras ou as suas remunerações. Estes dados são preocupantes uma vez que os gestores devem dar o exemplo, definindo os comportamentos para as suas organizações e ajudando os Conselhos de Administração a promover o *Tone at the Top*.

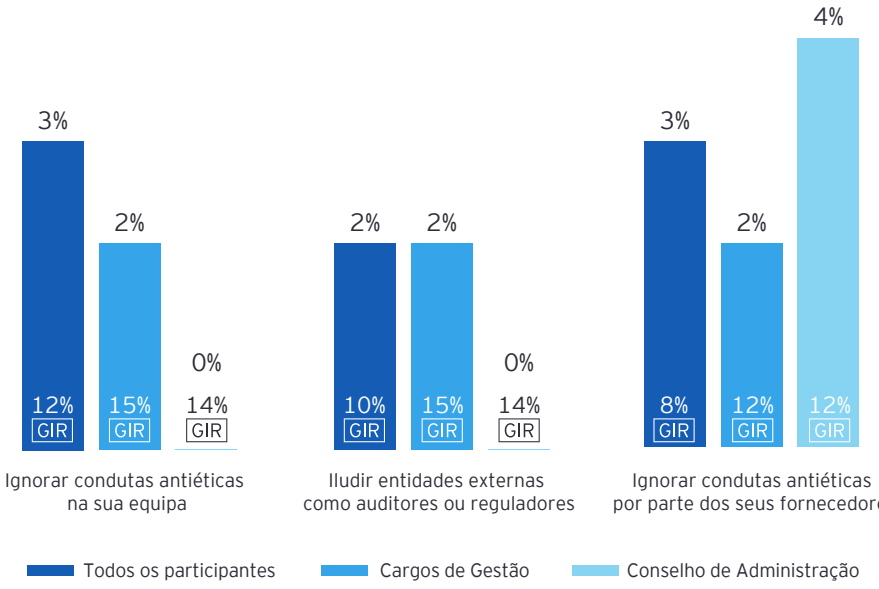
Os colaboradores que demonstram os mais elevados níveis de integridade, têm mais confiança na gestão. Com mais de metade (69%) de todos os inquiridos preocupados com a possibilidade das suas decisões no trabalho que realizem venham a ser alvo de escrutínio público, a COVID-19 e a crescente crise económica, veio indubitavelmente revelar comportamentos e ações pouco éticas. Isto deixa as organizações expostas a ameaças de dano reputacional, especialmente considerando o quão grande a pegada digital é atualmente como por exemplo em situações de decisões, declarações e publicações nas redes sociais.

Mais de metade (75%) dos inquiridos dizem ser um desafio para as organizações manterem os seus padrões de integridade em períodos de mudança rápida ou de difíceis condições de mercado. Quando observado este valor em mercados emergentes o mesmo continua acima de metade da amostra (63%).

Estas descobertas revelam um quadro negro, mesmo antes da COVID-19, uma vez que se observou 16% dos inquiridos que acreditam que a conduta ética diminuirá pelas consequências da pandemia COVID-19.

Agora que as organizações estão sob pressões externas para sobreviverem, as normas éticas podem ficar ainda mais perturbadas. Em tempos de dificuldade, é importante mais do que nunca, haver um profundo empenho em medir e controlar os padrões pessoais e a integridade corporativa.

É mais provável a gestão agir de forma pouco ética



> “É crucial entender as pessoas que compõe a sua organização e o ambiente no qual operam para haver uma proteção contra condutas antiéticas.

Pergunta: Quais (se é que alguma) das seguintes ações estaria disposto a realizar de forma a melhorar o seu próprio pacote de progressão ou remuneração de carreira (i.e. o seu salário ou qualquer bónus que possa receber)?

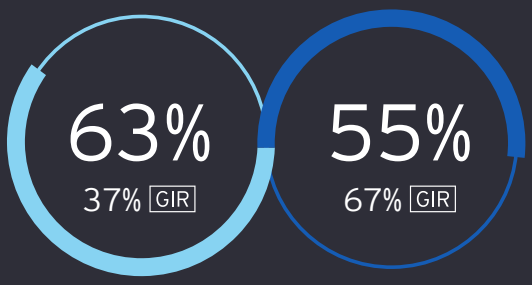
Quatro *insights* sobre a visão dos seus funcionários acerca da cultura organizacional

O nosso estudo identifica uma discrepância significativa entre a forma como a equipa de gestão e os colaboradores juniores percebem as ações de liderança e os valores da sua organização. Apenas porque os colaboradores juniores acreditam que algo está a acontecer, não significa que esteja realmente, no entanto esta perceção é importante de analisar a fim de compreender o real motivo da mesma.

Maneiras práticas de utilizar a integridade de forma a proteger-se contra más condutas éticas

- Avalie o seu enquadramento de conformidades. O mesmo é adequado à evolução de risco, influencia o comportamento dos colaboradores e possui os recursos adequados?
- Averigue as atitudes dos colaboradores sobre os riscos e pressões que sentem para transgredirem, e fortaleça os canais para que os colaboradores relatem casos de conduta imprópria sem medo de retaliações.
- Responsabilize-se pelas suas ações profissionais, quer sejam ou não examinadas. Os colaboradores seniores devem dar o exemplo para criar uma cultura de integridade.
- Analise as causas de comportamentos antiéticos. Em vez de tratar os sintomas, tente entender a dinâmica do ambiente social que molda o comportamento antiético.
- Desenvolva políticas e procedimentos que influenciem o comportamento individual a todos os níveis, e reforce as mesmas com formações e comunicações personalizadas.
- Use a *big data* para obter perceções mensuráveis sobre os comportamentos dentro da organização.

1

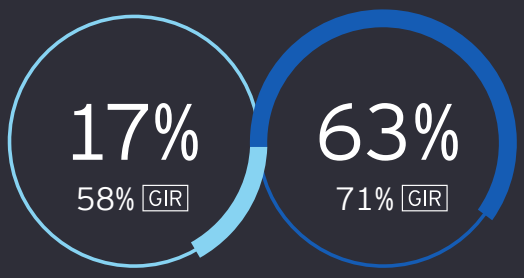


A equipa de gestão não fala o suficiente sobre integridade

Dois terços (63%) do Conselho de Administração pensa que a equipa de gestão fala frequentemente sobre a importância de comportamentos de integridade e 55% dos novos colaboradores pensam o mesmo. A equipa de gestão deve falar sobre integridade com toda a organização, comprometendo os colaboradores com o assunto.

Pergunta: Nos últimos dois anos com que frequência ouviu a equipa de gestão falar sobre a importância de ter um comportamento integro?

2

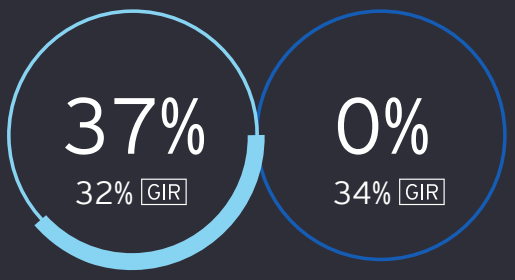


Os Colaboradores juniores duvidam que os padrões de integridade estejam a melhorar

Dos colaboradores juniores, 17% acreditam que o padrão de integridade dentro da organização se manteve igual ou piorou, mas 63% dos membros de Conselhos de Administração acredita que os padrões melhoraram. As organizações devem trabalhar para que as melhorias dos níveis de integridade sejam tangíveis e para que estas melhorias possam ser sentidas em toda a organização.

Pergunta: No geral, diria que os padrões de integridade têm melhorado, piorado ou se têm mantido iguais na organização nos últimos dois anos?

3

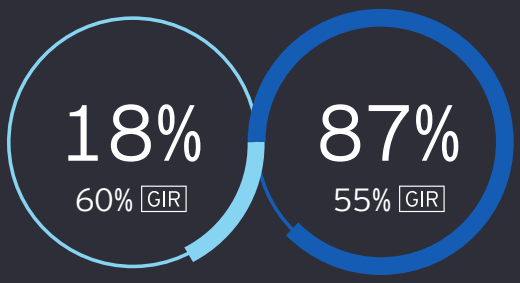


Acredita-se que os gestores permitem comportamentos antiéticos em cargos superiores

Um terço (37%) dos colaboradores juniores acreditam que comportamentos antiéticos são tolerados se os transgressores forem colaboradores com cargos elevados. Enquanto que nenhum (0%) dos membros do Conselho de Administração têm a mesma opinião. A má conduta não deve ser tolerada a qualquer nível.

Pergunta: Em que medida concorda ou discorda: os comportamentos antiéticos são frequentemente tolerados dentro da organização quando as pessoas envolvidas são seniores ou têm cargos importantes?

4



Os colaboradores juniores não acreditam que a equipa de gestão opera com integridade

Observamos que alguns dos colaboradores juniores (18%) não estão muito confiantes de que os seus gestores demonstrem integridade a nível profissional. De forma oposta, a maioria (87%) dos membros do Conselho de Administração acredita que isso acontece. A equipa de gestão deve sempre demonstrar integridade e ser um exemplo a seguir.

Pergunta: Acha que os gestores da organização demonstram integridade no trabalho que realizam?

Ação 1 2 3 4

Whistleblowing: ferramentas de promoção de integridade e resposta a requisitos legais e normativos

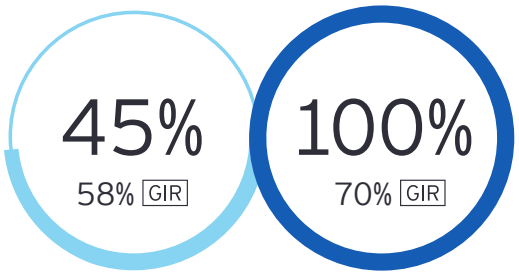
2

***Whistleblowing*: prevenir antes de remediar**

Os resultados do nosso estudo mostram de forma clara e evidente que existem pelo menos dois problemas importantes de refletir.

Em primeiro lugar, o facto de existir uma percentagem significativa de participantes que refere continuar a sentir medo de denunciar algum tipo de comportamento antiético.

Em segundo lugar, é importante observar a discrepância existente entre a perceção de colaboradores juniores e participantes que se encontram em cargos de administração. Esta diferença de perceção pode ser claramente explicada pelo não alinhamento e falha de comunicação ao nível transversal na organização, ou até mesmo pelo desconhecimento dos desafios dos colaboradores por parte dos membros do Conselho de Administração. Este desconhecimento poderá enviesar a comunicação e as mensagens do tone at the top que são disseminadas de forma infrutífera para com a organização e *stakeholders*.



Os colaboradores juniores temem consequências pessoais por relatarem irregularidades

Quase metade (45%) dos colaboradores juniores referem que os colaboradores da sua empresa não podem relatar irregularidades sem medo de sofrerem consequências negativas. Em contraste, 100% dos membros do Conselho de Administração referem que é possível reportar um comportamento antiético sem sofrer represálias. A equipa de gestão precisa construir a confiança dos seus colaboradores através de uma comunicação clara de valores, de um cumprimento transparente das regras e da possibilidade de garantir formas seguras de os trabalhadores denunciarem irregularidades.

Pergunta: Em que medida concorda ou discorda: os funcionários nesta organização podem reportar irregularidades no trabalho sem medo de consequências negativas?no trabalho sem medo de consequências negativas?

O momento de pensar e preparar a resposta aos requisitos legais e de cumprimento normativo em Portugal chegou

A Estratégia Nacional Anticorrupção, publicada recentemente, e a Diretiva Europeia relativa ao *Whistleblowing* que Portugal terá de adotar até ao final do ano, estão na ordem do dia a impulsionar as organizações em Portugal para se capacitarem a conseguir responder aos requisitos legais e de cumprimentos normativo que serão impostos.

Se antes a implementação de ferramentas como canais de denúncia já se observava crucial enquanto elemento de promoção da integridade, atualmente estas são também peças-chave para que as organizações respondam aos requisitos elencados e não sofram os impactos legais que estão pressupostos.

Impactos do não cumprimento da Estratégia Nacional Anticorrupção

Impedimento de acesso ao procedimento de contratação pública
Previsão de sanções, nomeadamente contraordenacionais, aplicáveis quer ao **setor público**, quer ao **setor privado**

> “A equipa de gestão precisa construir a confiança dos seus colaboradores através de uma comunicação clara de valores, de um cumprimento transparente das regras e da possibilidade de garantir formas seguras de os colaboradores denunciarem irregularidades de forma anónima.

Algumas das considerações que as organizações necessitam ter na implementação de um canal de denúncia passam por:

- Reflexão e definição do *Governance* do canal
- Capacitar uma equipa interna de apoio ao canal com formação avançada
- Garantir o anonimato, a confidencialidade e a possibilidade da comunicação bidirecional entre a pessoa autora do reporte e a equipa de gestão do canal
- Considerar diferentes geografias, culturas e idiomas caso exista operação em outros países
- Refletir uma eventual parceria com equipas externas para a gestão do canal a fim de garantir a independência, *expertise* e acelerar o processo de triagem
- Trabalhar a comunicação para disseminar mensagens que ativem cognitivamente todas as pessoas a sentirem que são agentes ativos de mudança na sua organização

Construa uma relação de confiança com terceiros baseada na integridade

3

É essencial que as organizações possam confiar totalmente nos terceiros com quem trabalham. Essa confiança precisa de ser cuidadosamente construída segundo um programa de triagem baseada no risco que é realizado de forma consistente e robusta.

A COVID-19 causou uma significativa perturbação nas cadeias de fornecimento, com 94% das organizações da Fortune 1000 a reportarem alterações nos seus fornecimentos regulares desde o início da crise[6], bem como a diversificação da existência de fornecimentos para novos parceiros, países, fontes e fornecedores.

O nosso estudo demonstra que a perturbação das cadeias de fornecimento é vista como uma das maiores ameaças à integridade dos negócios, com 13% dos participantes a dizerem que este é um dos maiores riscos relacionados com a conduta ética. As organizações ao estarem sob pressão, de modo a garantir a continuidade dos negócios, podem expor-se a níveis desconhecidos de risco, envolvendo parceiros com valores éticos questionáveis.

Mesmo antes da pandemia, as organizações enfrentavam questões de integridade em torno das práticas de terceiros, relacionadas com propriedade efetiva, escravidão moderna e sanções.

À medida que as organizações se começarem a regenerar, emergindo da pandemia para um clima económico mais difícil, podem ficar mais suscetíveis a ignorar comportamentos antiéticos de terceiros. Desde omitir fases dos processos e procedimentos, ou pensar conscientemente em comportamentos antiéticos ou ilegais para ajudar à sobrevivência financeira, os comportamentos desta índole podem promover graves consequências.

Muitas jurisdições afirmam que as organizações detêm responsabilidade sob as ações de terceiros. Na verdade, 90% da violação da lei de práticas de corrupção no exterior dos EUA (FCPA) são provenientes de terceiros.[7]

Embora a gestão da ética de terceiros seja sempre crucial para as organizações, os nossos dados demonstram que as organizações têm vindo a falhar relativamente a este aspeto. Menos de um terço (26%) dos participantes estão seguros de que as entidades terceiras com quem trabalham (fornecedores, parceiros e outros) cumprem as leis, códigos de conduta e regulamentos da indústria. Esta situação é preocupante e sugere uma falta de rigor na avaliação do risco.

É especialmente preocupante os resultados do estudo revelarem que a maior parte dos entrevistados apontaram como o principal comportamento antiético que poderiam cometer, ignorarem a má conduta de terceiros.

26%

34% GIR

dos participantes estão seguros de que as entidades terceiras com quem trabalham (fornecedores, parceiros e outros) cumprem as leis, códigos de conduta e regulamentos da indústria.

[6] Erik Sherman, "94% of the Fortune 1000 are seeing coronavirus supply chain disruptions: Report," Fortune 21 de fevereiro de 2020.
[7] "Foreign Corrupt Practices Act Clearinghouse" Standford Law School http://fcpa.stanford.edu/chart-intermediary.html

A monitorização ativa de um programa, pode ajudar a proteger contra a má conduta de terceiros, especialmente quando as cadeias de fornecimento estão a ser redefinidas.

De todos os entrevistados, pouco mais de 3 em cada 100 (3%) ignoraria a conduta antiética de terceiros, no entanto, estes valores sobem ligeiramente para 4 em cada 100 quando os entrevistados são membros do Conselho de Administração. Estes resultados irão afetar negativamente a confiança dos acionistas nos membros do Conselho de Administração e reforçar a necessidade de mudança.

Ignorar a má conduta de terceiros é um grande risco para as organizações. Por exemplo, os gigantes da tecnologia têm vindo a ser fortemente criticados pelas condições de trabalho impostas pelos seus fornecedores estrangeiros.

Na gestão de terceiros, revela-se mais importante do que nunca, haver um profundo comprometimento com programas de integridade pessoal e organizacional.

De forma a protegerem-se contra o risco, as organizações podem solicitar aos terceiros que apresentem os seus níveis de integridade. Isto pode ser conseguido adotando uma abordagem baseada no risco, de modo a conseguir envolver e gerir os terceiros.

Integridade e M&A

Os riscos provenientes de terceiros a que as organizações estão sujeitas não estão apenas relacionados com as cadeias de fornecimento. As organizações podem enfrentar vários riscos ao adquirirem, investirem e fazerem parcerias com outras organizações.

Observamos no nosso estudo que quase todos os participantes (96%) acreditam que os riscos relacionados com integridade são dos riscos mais significativos durante uma transação. Os nossos resultados demonstram ainda que o maior risco durante uma transação M&A, relaciona-se com a manipulação ou distorção da contabilidade (64%). Ao adquirir ou fazer parceria com outra organização, deve ter a certeza de que o terceiro segue rigorosamente as práticas de segurança e privacidade. Se não o confirmarem, a organização pode estar exposta ao risco.

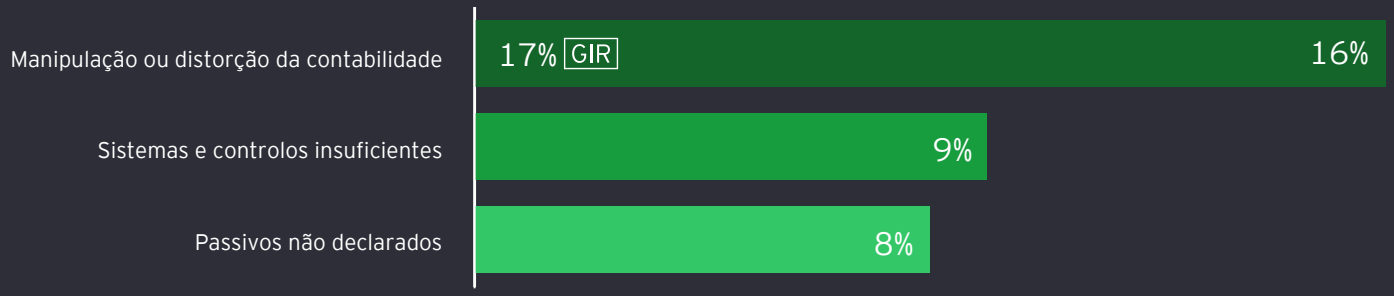
Outros importantes fatores de risco que as organizações enfrentam ao se envolverem em operações de M&A relacionam-se com limitações dos sistemas e controlos (36%) e Passivos não declarados (36%).

O escândalo da organização privada com sede no Dubai, Abraaj Capital Ltd., em 2018, e o seu consequente colapso, é visto pela indústria como um alerta, para que os investidores fortaleçam os seus procedimentos de *due diligence*, de modo a facilitar a descoberta de conflitos de interesse onde existem relacionamentos complexos.

À medida que os investidores começam a olhar novamente para os mercados emergentes em busca de maiores retornos, é importante lembrar que a integridade desempenha um papel significativo na *due diligence* de M&A- aproximadamente 1 em cada 10 (%) organizações dizem que a gestão da integridade numa organização está entre os maiores riscos associados à compra, investimento e parceria, entre organizações.

Ao reconhecer o impacto que o comportamento antiético pode ter, algumas organizações já iniciaram uma reflexão sobre novo clausulado a incluir por exemplo em certas transações de M&A, onde as partes necessitam declarar a sua boa conduta a nível ético a fim de prevenir riscos financeiros e reputacionais.

Riscos fundamentais de analisar durante operações de M&A



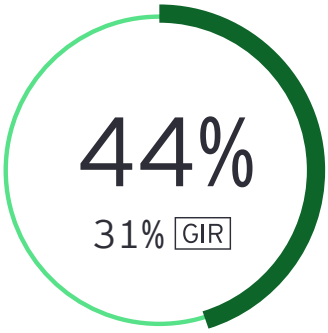
Pergunta: Dos seguintes riscos, quais os três que considera mais relevantes ao adquirir, criar parceria ou investir em outras organizações?

As organizações devem avaliar a integridade de todas as partes na atividade M&A, no entanto os nossos dados sugerem que tal não acontece o suficiente.

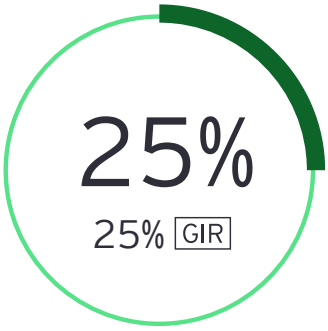
Só 44% das organizações realiza *due diligence* sobre reputação e integridade e apenas 24% implementa análises de suborno e corrupção.

À medida que os investidores emergem da pandemia e começam a avaliar as potenciais oportunidades que surgem diante deles, maior deve ser a cautela e cuidado a ter, para garantir que sua integridade não é comprometida pela conduta indevida de terceiros associados.

A maioria das organizações não avalia a integridade das partes integrantes das transações M&A



***Due diligence* ao nível da reputação e integridade**



Implementação de revisões *Anti-bribery Anti-Corruption* (ABAC)

Pergunta: Qual das seguintes opções a sua organização realiza ao adquirir outra organização?

Maneiras praticas de utilizar a integridade de forma a proteger-se contra a má conduta ética de terceiros:

- **Realizar a triagem de novos terceiros baseando-se no risco:** a confiança com terceiros é construída através de um nível consistente e robusto de triagem de risco. Isso deve identificar e avaliar possíveis riscos legais, de reputação e/ou financeiros.

- **Classifique o risco dos seus terceiros:** de acordo com o apetite de risco e o programa de integridade da sua organização. Determine o nível de risco que a sua organização está disposta a assumir.

- **Tome as ações adequadas para mitigar quaisquer sinais de alerta:** os riscos identificados durante a *due diligence* devem ser tratados antes de envolverem um terceiro, por exemplo, adicionando cláusulas contratuais específicas. Não deve avançar com o negócio se o risco não puder ser mitigado de forma adequada.

- **Atualize o seu conhecimento acerca das entidades terceiras já existentes:** não é suficiente realizar a triagem apenas uma vez ao integrar novos terceiros. Deve ser feita uma *due diligence* contínua sobre os terceiros existentes de acordo com sua classificação de risco, para que quaisquer riscos novos ou emergentes sejam considerados.

- ***Due diligence* holística sobre a integridade da M&A:** isso deve ser feito preferencialmente antes da aquisição. Garantir que a conformidade é parte do processo de integração pós-negociação.

- **Integrar tecnologia digital e automação:** melhorar a eficiência e a tomada de decisões durante a integração, triagem e monitoramento de terceiros.

Ação 1 2 3 4

Proteja os dados de forma ética salvaguardando o seu valor

4

Um quinto dos entrevistados sofreu de uma grande violação de segurança cibernética no ano anterior. Os cibercriminosos não discriminam com base na geografia – os resultados obtidos foram semelhantes nos mercados desenvolvidos (19%) e nos emergentes (23%) - 21% de todos os entrevistados confirmam terem sofrido algum grande acontecimento de perda de dados, as organizações devem garantir que os dados são efetivamente protegidos.

Um aumento exponencial no volume de dados que as organizações armazenaram na última década impulsionou o surgimento de novos modelos de negócios que utilizam análise de dados, inteligência artificial (IA) e automação. A COVID-19 acelerou esta tendência, pois as organizações tiveram que adaptar-se às mudanças nos comportamentos dos consumidores de um dia para o outro e às rápidas transformações digitais necessárias para atender às exigências crescentes dos serviços e dos produtos orientados para dados.

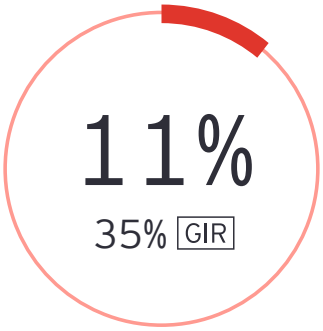
Embora as tecnologias avançadas como IA possam fornecer informações valiosas para a tomada de decisões corporativas e monitorização da integridade dos negócios, também representam riscos significativos. Por exemplo, os algoritmos de IA podem monitorizar o desempenho no trabalho analisando as publicações ou os e-mails de um colaborador nas redes sociais, mas esse tipo de uso pode violar as normas de privacidade e levantar questões éticas. A falha na proteção adequada dos dados, cria vulnerabilidades que podem entrar em conflito com os valores corporativos e com a rápida evolução da regulamentação sobre as obrigações de conformidade.

Onze por cento dos entrevistados acreditam que as atuais leis de proteção de dados são uma barreira para o sucesso nos negócios, enquanto 68% dizem que esperam que a aplicação dessas leis aumente no futuro.

Numa economia em rápida evolução, com crescentes requisitos regulatórios e de análise, as organizações precisam de ser mais cautelosas e preocupadas na forma como recolhem, mantêm e usam os dados, de forma a garantir a conformidade, sem comprometer as operações críticas de negócios. Também é relevante que as organizações estejam cientes das soluções alternativas ou atalhos operacionais que os colaboradores podem implementar para contornar barreiras.

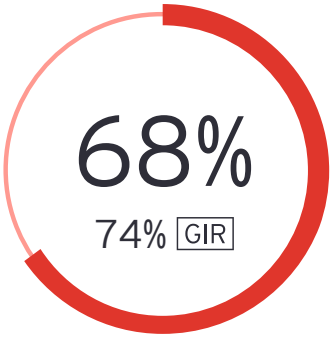
As organizações têm vindo a enfrentar ataques cada vez mais sofisticados de cibercriminosos que procuram roubar dados às organizações com o objetivo de expor falhas de segurança nesta área, lucrar com a venda dos dados ou através de pedidos de resgate às organizações após encriptarem os seus dados. A violação de dados pode paralisar as operações ou até mesmo colocar pequenas organizações fora do mercado. Na última década, as organizações que tiveram falhas na proteção dos dados dos seus clientes, quebraram a confiança pública e sofreram enormes danos resultado de multas regulatórias, litígios, perda de reputação e redução das receitas.

As organizações enfrentam desafios na privacidade de dados de navegação e regulamentos de proteção.



Acredita que as leis de proteção de dados atuais são uma barreira para o sucesso nos negócios

Pergunta: Até que ponto concorda ou discorda: a atual legislação sobre proteção de dados e privacidade são uma barreira para o sucesso nos negócios?



Espera um aumento na aplicação de leis de proteção de dados

Pergunta: Até que ponto concorda ou discorda: esperamos que o nível de atividade das autoridades em torno da aplicação da legislação de proteção de dados e privacidade aumente no futuro?

As organizações continuam preocupadas com a constante ameaça de ciberataques.

Acreditam que os ciberataques constituem um dos maiores riscos para a sua organização

Pergunta: Qual dos seguintes, se algum, pensa representar um maior risco para o sucesso a longo prazo da sua organização?

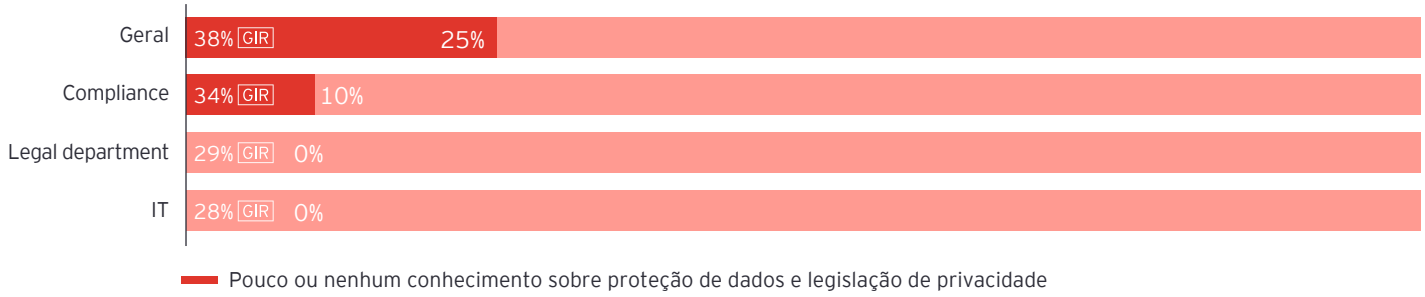
Fonte: Relatório de Integridade Global 2020 (2.948)

Os criminosos informáticos que tentam explorar os medos e incertezas em torno do vírus intensificaram os ataques de *phishing* e de *ransomware*, aumentando os riscos para as organizações que já lutavam para operar durante uma pandemia. A rápida mudança para trabalho remoto tornou a segurança cibernética num desafio ainda maior – um pelo qual as organizações pouco tempo tiveram para se preparar. Pudemos já ver estes ataques em vários setores, incluindo organizações de saúde.

Indivíduos da linha da frente devem estar equipados com o conhecimento e a preparação certa para salvaguardar dados

É fundamental desenvolver e implementar um plano de resposta a incidentes de violação cibernética, juntamente com a preparação de colaboradores, considerando que a maioria dos ataques de *ransomware* ocorrem quando um colaborador clica num link ou anexo de e-mail fraudulento. No entanto, o nosso estudo mostra que 62% não possui esses planos em vigor, e menos de metade (49%) está preparado adequadamente. Um plano de resposta abrangente que é implementado rapidamente após um incidente demonstrou reduzir significativamente o impacto e o custo financeiro de uma violação.

Muitos funcionários desconhecem as responsabilidades de proteção de dados



Pergunta: No geral, quanto diria que sabe sobre cada um dos itens seguintes? – Proteção de dados e privacidade (p.ex. o Regulamento Geral de Proteção de Dados ou legislação local específica)

De forma preocupante, os entrevistados referem que as suas organizações falham em seguir muitas práticas recomendadas para a proteção de dados. Observamos que 39% refere que não perceciona que a sua organização prepara os seus colaboradores para as responsabilidades de privacidade de dados. Este défice de preparação é refletido na falta de conhecimento sobre integridade de dados, mesmo entre os muitos colaboradores que trabalham na área jurídica, conformidade e funções de IT.

Os utilizadores são os *gatekeepers* de dados e possuem as credenciais que os cibercriminosos visam atacar. Essa falta de conhecimento pode dar origem a violações de dados internos, onde colaboradores inconscientes são vítimas de ataques de engenharia social ou contornam as políticas de proteção de dados ao fazerem o *download* de dados confidenciais da organização para os seus dispositivos pessoais.

Muitos entrevistados também relataram uma falta de conhecimento sobre os procedimentos de segurança de dados da própria organização.

Um quarto da nossa amostra (25%) refere saber pouco ou nada acerca das políticas e procedimentos da sua organização no que toca a manter as suas instalações, equipamentos e redes seguras.

A mesma percentagem (25%) também admitiu saber pouco ou nada acerca das políticas e procedimentos de acesso dos colaboradores aos dados.

A falha na educação e formação dos colaboradores sobre a proteção de dados é surpreendente, considerando que os entrevistados nomearam os ciberataques como o maior risco para o sucesso a longo prazo das suas organizações. A realidade é que as organizações deveriam fazer mais para salvaguardar os dados uma vez que 2019 foi um ano recorde para violações, com mais de 15 bilhões de registos confidenciais expostos.

Maneiras práticas de ajudar a proteger os dados com integridade:

As tecnologias avançadas podem tanto ajudar como prejudicar a integridade do negócio

As organizações estão a adotar cada vez mais tecnologias de IA, análise e automação nos seus programas de conformidade. Essas ferramentas podem ajudar uma organização a operar de forma ética detetando e até mesmo prevendo instâncias de fraude, corrupção e roubo dentro da organização e entre terceiros. Ferramentas como *machine learning* também podem ser usadas para proteger os dados de forma mais eficaz, por exemplo, reduzindo o número de falsos positivos em alertas de segurança e bloqueando automaticamente situações de *malware*.

Mas o uso de tecnologias analíticas avançadas também pode trazer ramificações éticas e até legais. Por exemplo, revelar informações de identificação pessoal (PII) ao agregar elementos de dados que, de outra forma, estão livres de preocupações de PII.

As organizações devem avaliar cuidadosamente os riscos éticos da adoção de novas tecnologias e tomar medidas proporcionais para mitigá-los. Isso os posicionará bem no cumprimento de quaisquer regulamentações futuras e mudanças repentinas nas condições de trabalho.

> “Organizações comprometidas com a integridade devem examinar as novas tecnologias com atenção, implementá-las com cuidado e educar os funcionários para o seu uso ético.

- Promover uma cultura de integridade de dados que englobe a organização e a sua cadeia de abastecimento, fortalecida com comunicações e formações regulares.
- Atualizar a formação para ter em conta os novos ambientes de trabalho e regulamentações e distribuí-la pelos trabalhadores de todas as funções, cargos e níveis de antiguidade.
- Utilizar tecnologia avançada como parte de um programa de conformidade eficaz para monitorar atividades de negócios e sinalizar áreas de risco potencial – por exemplo, como parte de um plano de resposta de violação cibernética para detetar e quantificar dados que possam ter sido perdidos.
- Realizar uma avaliação de risco ao introduzir novas tecnologias avançadas que incorporam cenários éticos onde a integridade dos dados pode ser comprometida.

Conclusão

Fazer o que está certo, porque isso é a coisa certa a fazer.

> A integridade corporativa não deve ser tida como "greenwashing", ou ser vista como fazer a coisa certa apenas para a opinião pública. Integridade existe quando as organizações se comportam de forma a gerar valor a longo prazo para os *stakeholders* e para a sociedade.

Não há dúvida de que as organizações enfrentam um desafio único de uma geração. Mesmo antes da atual pandemia global, as organizações enfrentavam enormes desafios como por exemplo sanções, convulsões políticas, mudanças de visão da sociedade e guerras comerciais, entre outros. Atualmente enfrentam novas e significativas decisões que apresentam dilemas éticos, aos quais devem responder com rapidez e sob crescente escrutínio.

É essencial que as organizações coloquem a integridade no centro de suas operações. As organizações que o fazem são mais resilientes e estarão em melhor posição para enfrentar a pandemia e as consequências advindas da mesma.

As organizações que demonstram maior integridade surgem mais fortes do que os seus concorrentes, tendo mantido os seus melhores talentos e até atraíram novos clientes, mesmo em tempos difíceis.

A Integridade é mais do que uma declaração de missão e políticas escritas. É algo que todos devem desenvolver, desde o CEO e Conselho de Administração até aos colaboradores juniores, parceiros de negócios e terceiros. Pela nossa experiência, a melhor maneira de o fazer é abordar os quatro elementos principais das ações de integridade: cultura, governance, dados e controlos internos que alinham as ações e objetivos da organização.

Não é altura de reduzir ou reorganizar equipas de *compliance*, mas sim de manter a sua energia enquanto o ambiente em que operam se vai alterando.

Para minimizar o gap entre as intenções e a realidade, as organizações devem concentrar os seus esforços na melhoria dos seus programas de *Compliance Anti-Bribery Anti-Corruption*, reavaliando continuamente a gestão da integridade organizacional e aproveitando as novas tecnologias para um melhor tratamento dos dados.

Em última análise, a integridade dos negócios permite que as organizações de sucesso permaneçam fiéis às suas missões, cumpram as suas promessas, respeitem as leis e normas éticas, promovam a confiança pública e aumentem a resiliência em tempos de crise. Isso, por sua vez, permite que acumulem capital – tanto financeiro quanto reputacional.

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

© 2021 Ernst & Young, S.A.
All Rights Reserved.

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as legal, accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com