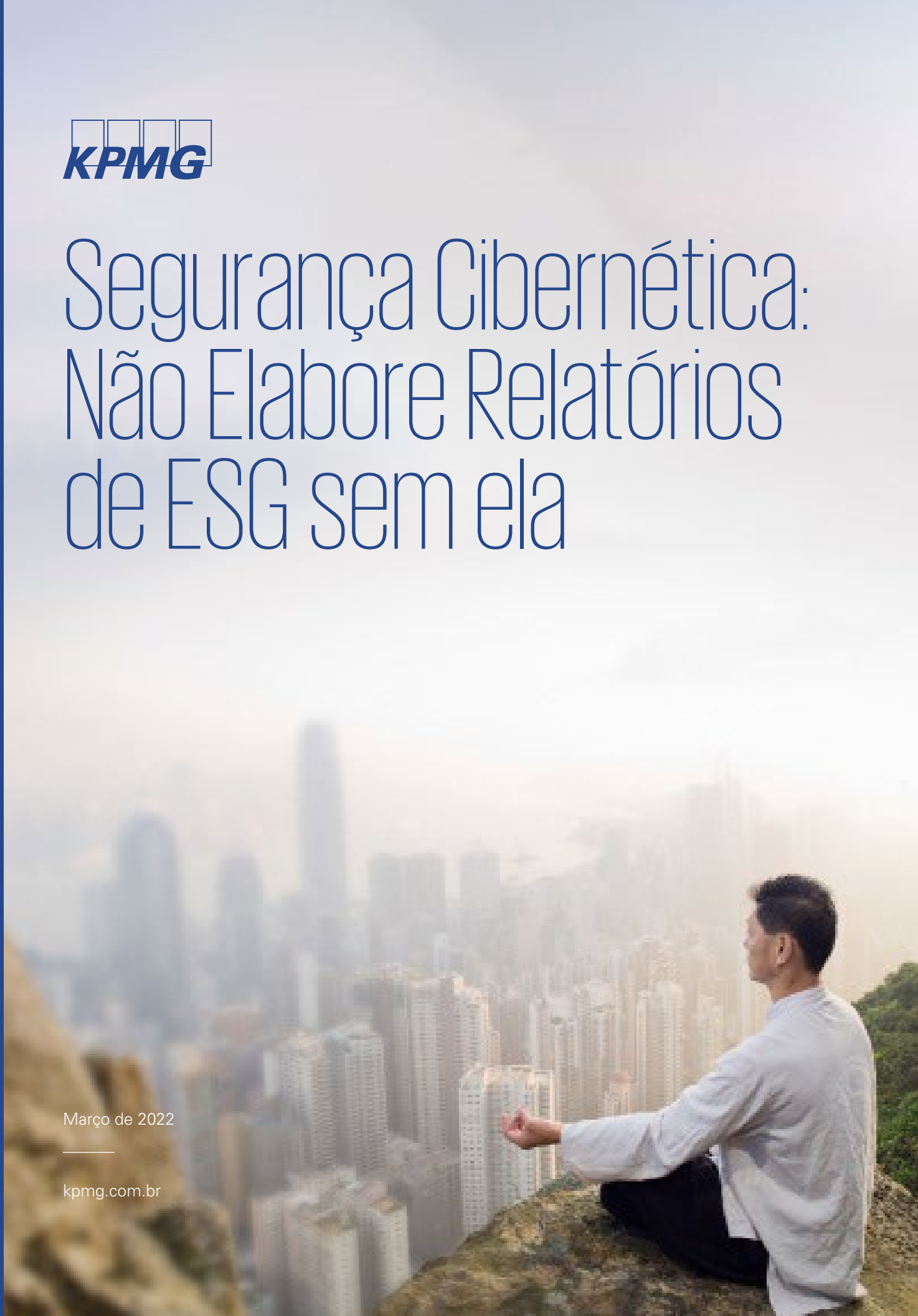
Segurança Cibernética: Não Elabore Relatórios de ESG sem ela



Março de 2022

kpmg.com.br

O elo entre segurança cibernética e ESG

Com base nas violações de segurança recentes (como, por exemplo, os ataques de *ransomware* a um oleoduto e a uma grande empresa de produção de carne ou a bancos e telefonia), os consumidores de todos os tipos estão se tornando cada vez mais esclarecidos sobre as vulnerabilidades cibernéticas nas organizações com as quais se conectam e compartilham dados. Como resultado disso, há uma demanda por transparência sobre como as organizações usam e protegem a confidencialidade e a integridade dos dados pessoais de seus clientes. As consequências de falhar na proteção desses dados podem variar de uma perda devastadora de ativos — passando pela corrosão da confiança entre a organização e seus consumidores, funcionários e terceiros — a danos irreparáveis à reputação, à marca e aos resultados financeiros da organização.

Como a segurança cibernética se alinha não apenas com o "G", mas também com o "S" e o "E" de ESG

Governança: os clientes querem saber se as empresas em que investem estão fazendo tudo o que podem para se proteger contra um ataque cibernético potencial e que contam com protocolos robustos de recuperação de desastres caso uma violação ocorra. Como o mundo ainda está no meio da recuperação e reconstrução da pandemia da covid-19, é fundamental demonstrar resiliência operacional e flexibilidade para se ajustar às mudanças nas condições. Quando se trata de investir, usar relatórios para demonstrar resiliência cibernética — ou a capacidade de continuar entregando produtos e serviços mesmo ao enfrentar problemas de segurança virtual — oferece aos investidores uma visão completa das capacidades operacionais de uma organização antes da avaliação das oportunidades de investimento.

Os relatórios sobre as métricas de risco cibernético podem apresentar o padrão do comportamento corporativo geral. Dessa forma, essas métricas devem seguir os mesmos princípios das classificações de ESG, ou seja, refletir o que os comportamentos dizem sobre uma corporação, como por exemplo o nível de resiliência a eventos cibernéticos futuros ou situações adversas de negócios futuros em geral. Além disso, há uma crença cada vez maior de que reportar os riscos de segurança cibernética e resiliência como parte das práticas de ESG pode em breve ser um requisito regulatório[1].

Social: à primeira vista, a segurança cibernética pode não parecer ter uma forte ligação com os aspectos sociais de ESG. No entanto, com violações de dados de grande visibilidade, o relacionamento de uma empresa com seus clientes pode ser gravemente prejudicado caso seus dados pessoais se tornem públicos.

> "O ESG oferece uma oportunidade única para as organizações fornecerem transparência aos investimentos significativos em segurança cibernética que estão sendo feitos para ganhar e manter a confiança dos *stakeholders*."
>
> **– Matthew P. Miller**
> Sócio de Cyber Security da KPMG nos EUA

[1] DEANER, Laura. *There is a C in ESG*. FS-ISAC. 2021.

Além disso, o público está cada vez mais preocupado com o que as organizações estão fazendo pela sociedade — do avanço da diversidade à redução de suas emissões de carbono. Da mesma forma, os clientes querem saber se a proteção das informações e dos direitos de privacidade individual são a prioridade de uma organização e se eles podem ter certeza de que seus dados não serão compartilhados ou vendidos para outras organizações. Para aumentar a confiança do cliente, as empresas devem determinar que o acesso aos dados confidenciais seja ajustado cuidadosamente, com base nas funções e responsabilidades dentro da organização.

Ambiental: uma vez que a política/impacto ambiental positivo de uma corporação pode potencialmente beneficiar aqueles que estão fora dos seus muros corporativos, considera-se um bem público contribuir para a limpeza do ar e da água. No mesmo sentido, a interconectividade do mundo atual significa que as métricas de política cibernética, *compliance* e risco de uma empresa podem ter impacto de longo alcance, capaz de se espalhar por toda a sociedade. As organizações com sólidos programas de segurança cibernética e relatórios que dão transparência aos *stakeholders* estão bem posicionadas para melhorar seus ecossistemas e proteger suas conexões com outras instituições em todo o mundo. As empresas devem determinar que podem articular claramente a efetividade dos seus modelos operacionais e processos de apoio em termos de promoção da segurança e conscientização sobre riscos, bem como gerar relatórios sobre programas de controles robustos que protejam os dados dos clientes.

Contando sua história de segurança cibernética

Em 2020, 66% dos diretores de serviços financeiros (16 pontos percentuais a mais do que em 2019) relataram que sua confiança na capacidade de sua organização de responder a um ataque cibernético estava crescendo[2]. No entanto, quando se trata de informar sobre segurança cibernética ao conselho, há espaço para melhorias — apenas 56% dos CEOs, 53% dos CIOs (*Chief Information Officer*) e 45% dos CISOs (*Chief Information Security Officer*) afirmaram que atualmente se reportam ao conselho sobre segurança cibernética, de acordo com um estudo recente. A necessidade de continuar melhorando as comunicações fica clara quando considera-se que os conselhos que têm três ou mais executivos seniores reportando sobre segurança cibernética afirmam que estão mais propensos a fornecer supervisão eficaz do que aqueles com menos executivos[3].

> “As organizações em qualquer etapa da sua jornada de ESG devem considerar informar sua postura de segurança cibernética para desenvolver e sustentar a confiança com seus seus clientes, funcionários e outros *stakeholders*.”
>
> **– Prasanna Govindankutty**
> Sócio de Cyber Security da KPMG nos EUA

[2] NACD. *2019–2020 NACD Public Company Governance Survey*. 2020.

[3] NACD. *2019–2020 NACD Public Company Governance Survey* . 2020.

Abaixo, seguem algumas áreas-chave que devem ser incluídas nos relatórios de segurança cibernética e exemplos de ações que as empresas podem realizar agora:

Subcategorias de divulgação e de relatórios de riscos cibernéticos	Diretrizes
Governança	Nomear e capacitar um executivo sênior responsável pelos riscos de segurança cibernética.
	Determinar a frequência apropriada de relatórios de risco cibernético para o Conselho de Administração.
	Determinar que o Conselho seja composto por profissionais com habilidades, conhecimentos e experiências suficientes em segurança cibernética.
Abordagem de conformidade de segurança	Acompanhar as atualizações das normas do setor para estruturas de controle e divulgação, levando em conta que as estruturas de divulgação do Fórum Econômico Mundial e da Força-Tarefa sobre Divulgações Financeiras Relacionadas ao Clima estão prestes a se tornar as normas futuras de divulgação e de relatórios externos.
	Considerar os requisitos regulatórios de segurança cibernética e privacidade no escopo da organização (por exemplo, setor de cartões de pagamento, Regulamento Geral de Proteção de Dados, Lei de Privacidade do Consumidor da Califórnia).
	Determinar se devem ser incluídas estruturas de continuidade de negócios nos relatórios.
	Avaliar e ajustar sua cobertura de seguro cibernético regularmente.
	Criar uma avaliação de riscos com periodicidade regular envolvendo terceiros.
Cultura	Trabalhar para garantir que todos (membros do conselho, funcionários e subcontratados) concluam os programas de treinamento obrigatórios e contínuos para garantir a confiança do investidor.
	Aumentar a porcentagem do orçamento de TI dedicado à segurança cibernética e iniciativas relacionadas.
	Compartilhar conhecimentos da área, principalmente com empresas conhecidas por protocolos de segurança cibernética maduros.
Relatórios de privacidade de dados	Informar sobre o número de incidentes de segurança relevantes envolvendo informações pessoalmente identificáveis ou o padrão revelado por esses dados.
	Quantificar o número de clientes/funcionários cujos dados são usados para fins secundários.
	Totalizar as perdas monetárias históricas associadas a violações de dados.
	Incluir uma política de privacidade ou proteção de dados divulgada publicamente em todos os relatórios.
	Determinar a postura de segurança da organização e desenvolver um programa de métricas que consolide dados diversos e muitas vezes inconsistentes.
	Determinar que os relatórios internos sejam abrangentes e incluam todos os tipos de risco.
	Adotar uma visão de médio a longo prazo não apenas para segurança cibernética, mas também para todas as questões de ESG, pois os efeitos podem se materializar muito mais tarde do que outros tipos de risco.
	Ter cuidado ao divulgar muitas informações sobre ferramentas e recursos utilizados para gerenciar o risco cibernético, a fim de não divulgar dados que possam ser úteis para invasores.

Conclusão

Já está bem estabelecido que ser transparente pode trazer vantagens competitivas, pois permite que consumidores, funcionários, investidores e outros *stakeholders* usem dados para a tomada de decisões específicas. Por isso, adotar uma abordagem de ESG para os relatórios de segurança cibernética pode promover a confiança digital na sua organização. As métricas de relatórios cibernéticos devem ser baseadas em dados que a sua organização já possui.

— **Nossa equipe cibernética oferece diversos serviços e soluções para permitir que a sua organização compartilhe sua história de segurança cibernética e de ESG, incluindo:**

Fale com o nosso time

Prasanna Govindankutty
Sócio
de Cyber Security
da KPMG nos EUA
pkgovindankutty@kpmg.com

Matthew P Miller
Sócio
de Cyber Security
da KPMG nos EUA
matthewpmiller@kpmg.com

Leandro Augusto
Sócio-líder
de Cyber Security
da KPMG no Brasil
lantonio@kpmg.com.br

A prestação de todos ou de alguns dos serviços aqui descritos pode não ser permitida para clientes de auditoria da KPMG e suas afiliadas ou entidades relacionadas.

#KPMGTransforma

Baixe o nosso APP

kpmg.com.br /kpmgbrasil