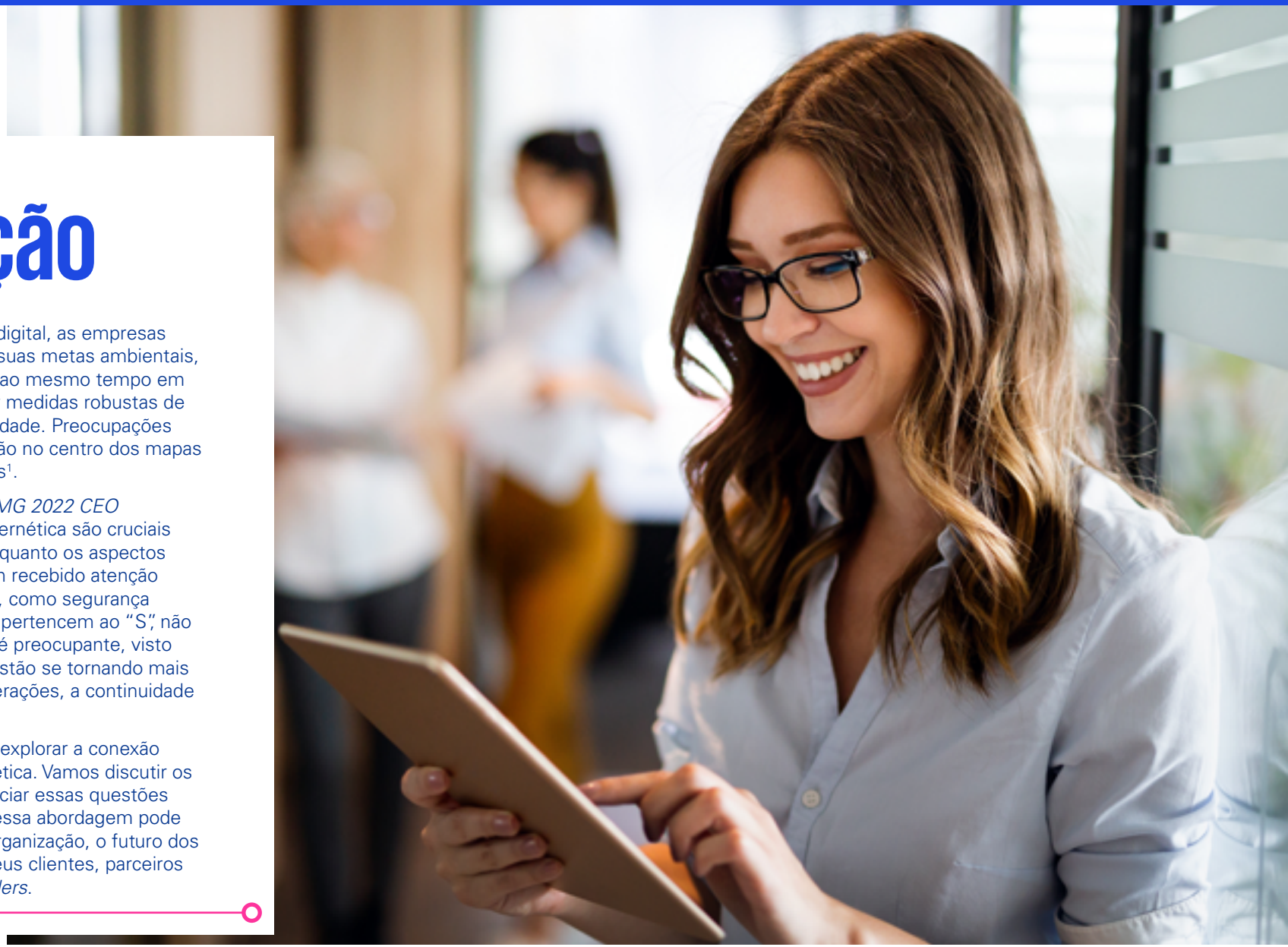
Segurança Cibernética em ESG

É hora de entender a conexão entre os temas ESG e a segurança cibernética

KPMG
Outubro de 2023

Conteúdo



Introdução

No atual cenário de economia digital, as empresas enfrentam desafios ao buscar suas metas ambientais, sociais e de governança (ESG) ao mesmo tempo em que se empenham em garantir medidas robustas de segurança cibernética e privacidade. Preocupações relacionadas a essas áreas estão no centro dos mapas globais de riscos há vários anos[1].

De acordo com a pesquisa *KPMG 2022 CEO Outlook*[2], ESG e segurança cibernética são cruciais para o sucesso corporativo. Enquanto os aspectos ambientais da agenda ESG têm recebido atenção significativa, outros elementos, como segurança cibernética e privacidade, que pertencem ao "S", não foram tão desenvolvidos. Isso é preocupante, visto que as ameaças cibernéticas estão se tornando mais frequentes, impactando as operações, a continuidade e a reputação dos negócios.

Este artigo tem como objetivo explorar a conexão entre ESG e segurança cibernética. Vamos discutir os benefícios esperados ao gerenciar essas questões de maneira integrada e como essa abordagem pode ajudar a proteger a saúde da organização, o futuro dos negócios e os interesses de seus clientes, parceiros comerciais e demais *stakeholders*.

1 WORLD ECONOMIC FORUM. *The Global Risks Report 2023 -18th Edition*. Disponível em: <www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf>. Acesso em: set. 2023.
2 KPMG. K*PMG 2022 CEO Outlook*. Disponível em: <https://kpmg.com/br/pt/home/insights/2022/11/resiliencia-fortalece-empresas-enfrentar-desafios-2022.html>. Acesso em: set. 2023.

Aspectos ambientais

Infraestrutura crítica enfrenta riscos significativos

O *link* entre ESG e cibersegurança não parece óbvio, mas está se tornando cada vez mais importante. Profissionais da KPMG estão começando a observar ataques cibernéticos que tentam atingir infraestruturas críticas, como usinas de energia e instalações de processamento de água. Além disso, esses ataques a sistemas de controle industrial podem causar mau funcionamento de equipamentos, danos ambientais e riscos. As organizações precisam de uma segurança cibernética robusta, sofisticada e interconectada , que proteja sua infraestrutura crítica das ameaças à sua tecnologia operacional. À medida que esses incidentes se tornam mais comuns, prevemos um maior foco regulatório.

Conectar a segurança à descarbonização, à redução de CO_2 e à economia circular

A maioria dos planos de descarbonização e redução de CO_2 depende da transformação digital e da aplicação de tecnologias inteligentes e de sistemas automatizados que monitorem e gerenciem a produção, a distribuição e o consumo de energia. No entanto, essas soluções podem abrir oportunidades para crimes cibernéticos, exigindo um alto nível de cibersegurança e proteção de dados. Da mesma forma, a introdução de soluções tecnológicas para apoiar a economia circular, quando esses sistemas envolvem transações financeiras significativas para incentivar comportamentos sustentáveis, pode suscitar preocupações com novos padrões de fraude.

Incorporar a segurança cibernética a todos esses programas pode ajudar a antecipar a ameaça cibernética e garantir operações seguras. Ao mesmo tempo, aderir a princípios de proteção de dados, como a minimização de informações sensíveis, pode reduzir o risco de violações de dados e garantir compliance regulatório.

A economia digital levou a um aumento no processamento de dados, resultando na construção de centros de dados em todo o mundo. Os criminosos encontraram oportunidades para explorar vulnerabilidades na segurança de centros de dados e serviços em nuvem para roubar recursos de computação, incluindo mineração de criptomoedas em grande escala. Infelizmente, o uso desses sistemas tem um impacto negativo no consumo de energia e na pegada de carbono. Por exemplo, implementar os controles cibernéticos necessários ou as melhores práticas, como ter um centro de dados secundário para melhor resiliência, pode levar a um maior uso de recursos e energia.

As organizações de hoje precisam considerar tanto os aspectos positivos quanto negativos da resiliência cibernética, equilibrando cibersegurança e metas de ESG.

Alem disso, as mudanças climaticas vao exigir adaptaçao das empresas e suas cadeias e isso vai exigir taambem novas tecnologias digitais. De acordo com a pesquisa KPMG de 2022, 64% das empresas reconhecem as mudanças climáticas como um risco para seus negócios[3].

[3] 'KPMG. *Grandes Mudanças, Pequenos Passos – Pesquisa Global de Relatórios de Sustentabilidade 2022.* Disponível em: <https://kpmg.com/br/pt/home/insights/2023/05/regulamentacoes-miram-dados-relatorios-sustentabilidade.html>. Acesso em: set. 2023

Aspectos sociais

Protegendo o capital digital da sociedade

Considerações sociais também são um aspecto crítico do ESG – afinal, o risco cibernético pode impactar significativamente a sociedade, e se tornam mais críticos à medida que os ataques cibernéticos se tornam mais frequentes em todo o mundo.

Aplicações e sistemas digitais estão agora integrados em todos os aspectos de nossas vidas, desde os dispositivos pessoais em que confiamos e as redes sociais com as quais interagimos até as plataformas automatizadas e os sistemas sofisticados que sustentam ambientes de trabalho e estilos de vida digitais.

A proteção de dados é essencial

Essa integração pode aumentar a vulnerabilidade a riscos cibernéticos, como o roubo de informações pessoais e sensíveis, resultando em roubo de identidade, fraude financeira e outros danos. Os ataques cibernéticos também podem interromper serviços críticos de saúde, transporte e emergência. Para lidar com esses riscos, as organizações precisam de medidas consistentes de privacidade e segurança cibernética, que efetivamente protejam seus dados. Além disso, devem ter planos robustos de resposta a incidentes para minimizar o impacto de um ataque cibernético a serviços críticos.

Aumento dos ataques de *ransomware*

Os lucrativos ataques de *ransomware* continuam a aumentar globalmente e podem até paralisar as operações e a reputação de uma organização. Diante das graves consequências trazidas por esse tipo de crime, muitas organizações ficam propensas a pagar o resgate. Infelizmente, os pagamentos de *ransomware* apenas incentivam mais crimes e criam um ciclo custoso. Para combater os ataques de ransomware, medidas modernas de segurança cibernética devem ser implementadas para minimizar seu impacto social e financeiro e manter a resiliência das Empresas.

Ameaças à liberdade de expressão

A privacidade e a segurança cibernética também desempenham papéis vitais na proteção da liberdade de expressão e na segurança dos canais de comunicação digital que estão se proliferando hoje. Proteções legais, promoção da alfabetização digital e midiática e apoio à diversidade e à inclusão em espaços online também são medidas importantes

Tecnologias de criptografia podem garantir que apenas os destinatários pretendidos possam acessar informações, sem medo de escutas ou espionagem. A cibersegurança também pode ajudar a mitigar os efeitos de ataques disruptivos direcionados a sites e plataformas online que facilitam a liberdade de expressão.

Proteger informações de clientes

Controles de privacidade desempenham papel fundamental em limitar a exploração e o uso indevido de informações pessoais sem autorização ou conhecimento prévios. Isso é vital para manter a confiança pública e dos clientes nas organizações.

Antes de regulamentações como a Lei Geral de Proteção de Dados, muitas organizações acreditavam que tinham propriedade sobre os dados pessoais do público. Isso mudou com a introdução dessas regulamentações. Indivíduos agora têm o direito de decidir como seus dados pessoais podem ser usados, incluindo o direito de saber quais dados uma empresa detém e o direito de fazer com que sejam excluídos.

Novas preocupações sobre ética em IA e sua relação com dados

O uso de ferramentas de inteligência artificial (IA) pode acelerar a coleta de dados, mas levanta questões sobre o uso ético desses dados por algoritmos.

Organizações podem impactar positiva ou negativamente a sociedade com base em como avaliam riscos e protegem os dados que processam, especialmente com a velocidade e escala que IA permite. Novas regulamentações, como o Regulamento de IA da UE e novas regulações no Brasil visam garantir que a IA seja usada de maneira que não cause danos.

Aumento da conscientização e do "letramento" cibernético

Muitas empresas reconhecem que têm um papel a desempenhar na promoção da conscientização e do "letramento" em segurança cibernética, seja em sua base de clientes ou no ecossistema de fornecedores.

Essas ações podem ajudar a prevenir fraudes, incentivar a fidelidade à marca e reduzir a exposição da cadeia de suprimentos a possíveis ataques. Algumas organizações também buscam aumentar a conscientização social sobre ameaças cibernéticas, ajudar a desenvolver habilidades e promover a cibersegurança, ao mesmo tempo em que apoiam organizações que podem não ter a capacidade e a habilidade para proteger totalmente seus próprios sistemas.

Outubro é o Mês de Conscientização em Segurança Cibernética, uma campanha anual com o objetivo de aumentar a conscientização sobre cibersegurança e disponibilizar recursos para que indivíduos e organizações melhorem suas práticas de segurança cibernética. A KPMG, entre outras organizações, participa ativamente dessa campanha para aprimorar a segurança para todos.

Aspectos de governança

Foco nas regulamentações em um cenário de mudanças

Os riscos cibernéticos podem ter implicações significativas em governança, o "G" de ESG. Existem diversas regulamentações cibernéticas específicas para setores ou para o mercado que precisam ser implementadas e acompanhadas pelos órgãos de decisão da empresa.

Nos Estados Unidos, temos: Regulação de Gerenciamento de Riscos Cibernéticos para Consultores de Investimento; Estratégia, Governança e Divulgação de Incidentes; Divulgação de Nomes de Empresas de Investimento; e a Regra de Diversidade do Conselho da Nasdaq (a bolsa de valores eletrônica norte-americana).

Na União Europeia, as regulamentações englobam o Regulamento Geral de Proteção de Dados (GDPR), a Lei de Resiliência Operacional Digital (DORA) e a Diretiva Revisada de Sistemas de Rede e Informação (NIS2).

No Brasil, temos diversas orientações sobre o tema publicadas pelo Banco Central do Brasil, SUSEP, CVM, além dos fatores de segurança requisitados pela Lei Geral de Proteção de Dados.

Regulamentações relacionadas ao ESG incluem o Regulamento de Divulgação de Finanças Sustentáveis da União Europeia (SFDR) e a Diretiva de Relatório de Sustentabilidade Corporativa (CSR-D). Nos EUA, regulamentações de divulgação obrigatória incluem orientações da comissão sobre divulgações relacionadas a mudanças climáticas, aprimoramento e padronização de divulgações relacionadas a mudanças climáticas, alterações nas regras dos itens 101, 103, 105 do Regulamento S-K e divulgações aprimoradas por determinados consultores e empresas de investimento, sobre práticas de alocação de recursos em questões ambientais, sociais e de governança.

Todos esses dados são apresentados publicamente em formato digital e portanto correm risco de serem alterados por agentes relacionados com crimes digitais.

A medição da eficácia das práticas de privacidade, segurança cibernética e gerenciamento de dados de uma organização pode ajudar a garantir a qualidade da empresa na governança dos dados que ela processa e compartilha internamente e externamente.

Os dados e relatórios ESG exigem precisão

Os dados ESG provêm de quatro principais fontes: dados de terceiros; dados reportados; dados derivados e funcionais; e dados brutos de propriedade da empresa. Esforços significativos estão sendo feitos em prol da elaboração e asseguração de relatórios ESG.

A segurança cibernética é um fator crítico para garantir relatórios ESG fidedignos. Ela existe para proteger os dados em suas fontes enquanto estão sendo coletados, em trânsito e após terem sido analisados e relatados. É vital que esses os processos que resultam nos dados a serem publicados não sejam manipulados para garantir relatórios precisos.

A segurança cibernética é relevante para as três dimensões do ESG. Portanto, organizações em qualquer estágio de sua jornada ESG devem considerar a divulgação de seu posicionamento cibernético como parte de seus relatórios ESG. Isso contribui para desenvolver e manter a confiança de todos os públicos de interesse que se relacionam com a empresa.

As normas internacionais reforçam a importância da transparência

As normas que definem os indicadores a serem relatados em relatórios de sustentabilidade e financeiros e visam aumentar a transparência e a comparabilidade nos relatórios corporativos, o que pode ajudar os investidores a tomar decisões com mais respaldo.

Um dos fatores de sustentabilidade abordados pelo SASB – uma norma americana sobre relatórios corporativos - é o risco cibernético, que se enquadra principalmente em tecnologia e comunicações, sendo também mencionado em muitos outros setores.

O risco cibernético é um fator que as empresas devem considerar divulgar em seus arquivos públicos e está incluído no tópico de divulgação de Segurança de Dados. Esse tópico abrange uma variedade de ameaças cibernéticas que poderiam comprometer informações sensíveis, além de oferecer orientações sobre o gerenciamento de riscos cibernéticos.

A Iniciativa Global de Relatórios (GRI) é amplamente usada globalmente para relatórios de sustentabilidade. As normas GRI incluem orientações sobre como as empresas devem divulgar sua gestão de questões de segurança cibernética e privacidade de dados.

Ao incluir o risco cibernético como um fator de sustentabilidade relevante, tanto o SASB quanto o GRI reconhecem que as ameaças cibernéticas podem impactar significativamente o desempenho financeiro, a reputação e a sustentabilidade de longo prazo de uma empresa. Empresas que divulgam suas práticas de gerenciamento de risco cibernético e fornecem informações sobre suas políticas e procedimentos de segurança de dados podem melhorar sua transparência e responsabilidade perante seus *stakeholders*, incluindo investidores, clientes e reguladores.

No entanto, menos da metade das empresas tem representação de nível de liderança para a sustentabilidade[4].

Os clientes esperam serviços confiáveis

Os clientes têm mais probabilidade de fazer negócios com uma empresa na qual confiem para proteger suas informações pessoais e financeiras. Isso é especialmente verdadeiro para clientes corporativos, que valorizam a proteção de seus dados confidenciais e propriedade intelectual. Muitos setores dispõem de requisitos regulatórios para segurança cibernética e as organizações que estejam em compliance com essas regulamentações normalmente são preferidas pelos stakeholders. A pesquisa da KPMG constatou que menos da metade das empresas divulga seus riscos de governança[5].

Tanto clientes privados quanto corporativos querem ter certeza de que os serviços que contratam atendem às suas expectativas em termos de ESG e segurança cibernética. O compromisso de uma empresa com ESG pode ser um impulsionador de vendas, melhorando sua reputação, estimulando a inovação, gerenciando riscos, garantindo conformidade e melhorando o acesso ao capital. Por isso, é importante levar em consideração a qualidade das práticas de privacidade e segurança cibernética de uma empresa ao fazer negócios.

Ao abordarem os riscos cibernéticos, as empresas protegem suas operações, seus clientes e sua reputação e ao mesmo tempo cumprem suas obrigações éticas, sociais e ambientais.

[4-5] KPMG. *Grandes Mudanças, Pequenos Passos – Pesquisa Global de Relatórios de Sustentabilidade 2022*. Disponível em: <https://kpmg.com/br/pt/home/insights/2023/05/regulamentacoes-miram-dados-relatorios-sustentabilidade.html>. Acesso em: set. 2023.

Conclusão: novas conexões entre ESG e segurança cibernética

As organizações podem se beneficiar enormemente entendendo a conexão entre ESG e riscos cibernéticos. Ambas as áreas têm foco na identificação e gestão de riscos e oportunidades, resultando em produtos e soluções aprimorados e na construção de uma sociedade que protege direitos individuais e coletivos.

Essa conexão está sendo cada vez mais reconhecida pelos públicos que se relacionam com as empresas que buscam maior transparência sobre como as organizações protegem as informações que elas usam para operar.

Para proteger sua infraestrutura crítica, sistemas de controle industrial e dados dos clientes, as empresas devem ter medidas sólidas de privacidade e segurança cibernética em vigor. A boa notícia é que muitas empresas já o fazem, o que deve impactar de maneira positiva seu desempenho, em geral e também em ESG.

Finalmente, as empresas devem ter estruturas de governança bem estabelecidas para supervisionar a gestão de riscos de privacidade e segurança cibernética e garantir a conformidade com requisitos legais e regulatórios. Ao abordar os riscos cibernéticos no contexto de ESG, as empresas podem proteger suas operações, clientes e reputação, ao mesmo tempo em que cumprem suas obrigações sociais e ambientais mais amplas.

Como a KPMG pode ajudar

As firmas-membro da KPMG têm experiência em todo o espectro relativo a essa questão da segurança cibernética.

Além de avaliar sua segurança cibernética e alinhá-la às prioridades do seu negócio, os profissionais da KPMG podem ajudar no desenvolvimento de soluções digitais avançadas, além de implementar e monitorar riscos contínuos, ajudando você a responder de maneira eficaz a incidentes cibernéticos.

Independentemente de como você se envolve, pode esperar trabalhar com pessoas que entendem o seu negócio e sua tecnologia. E quer você esteja ingressando em determinado mercado, lançando produtos e serviços ou interagindo com os clientes de uma nova maneira, o crescimento sustentável é a única forma de construir um negócio bem-sucedido e resiliente.

Os profissionais da KPMG estão comprometidos em trabalhar com você para aumentar a confiança, mitigar riscos e desbloquear valor à medida que você constrói um negócio resiliente.

Eles também podem ajudar você a antecipar o amanhã, agir com mais rapidez e obter uma vantagem com tecnologia segura e confiável.

Fale com o nosso time

Leandro Augusto
Sócio-líder de Cyber Security & Privacy
da KPMG no Brasil e na América do Sul
lantonio@kpmg.com.br

Nelmara Arbex
Sócia-líder de ESG da KPMG
no Brasil e na América do Sul
narbex@kpmg.com.br

Os serviços descritos neste material, no todo ou em parte, podem não ser permitidos a ser prestados a clientes de auditoria da KPMG e suas afiliadas ou entidades relacionadas.

kpmg.com.br

/kpmgbrasil