Empresas de tecnologia demandam segurança cibernética para crescer e ganhar confiança

Cultura e tecnologia são cruciais para uma estratégia cibernética resiliente

Junho de 2022

kpmg.com.br

Introdução

Os líderes das empresas de tecnologia apontam riscos cibernéticos como principal ameaça e prioridade operacional. Em resposta, eles estão investindo em habilidades, cultura e tecnologia para construir resiliência cibernética, acelerar a transformação digital e do modelo de negócios e promover a confiança dos *stakeholders*.

As empresas de tecnologia continuam fornecendo os produtos e serviços que impulsionaram a transformação digital durante a pandemia da covid-19 e permitiram que as rodas da indústria global continuassem girando. No entanto, essa aceleração digital também causou uma explosão no número de possíveis pontos de vulnerabilidade cibernética, pela imediata adoção do trabalho virtual e do armazenamento de dados em nuvem, pela necessidade de repensar/reorganizar agilmente as cadeias de suprimentos e pelo estabelecimento de novas parcerias de negócios. A rápida integração de novas tecnologias também criou uma avalanche de dados a serem armazenados e protegidos.

Embora algumas dessas tendências já estivessem em curso, a pandemia as acelerou drasticamente. As empresas de tecnologia foram forçadas a dar respostas rápidas. Nessa nova realidade, os CEOs das empresas de tecnologia classificam o risco cibernético como a maior ameaça ao crescimento de suas organizações nos próximos três anos; maior do que a interrupção das cadeias de suprimentos, as mudanças climáticas ou o risco de talentos[1].

Eles também citam a resiliência da segurança cibernética como sua prioridade operacional mais importante.1 Pesquisas adicionais indicam que o custo médio de uma violação de dados envolvendo um milhão de registros comprometidos é de US$ 52 milhões, e o custo aumenta a partir daí. Quando mais de 50 milhões de registros são comprometidos, o custo médio da violação é de US$ 401 milhões[2].

No entanto, os líderes de empresas de tecnologia também reconhecem a existência de oportunidades. Uma estratégia cibernética sólida permite que uma empresa maximize todos os benefícios da transformação digital para ampliar seus negócios rapidamente, sabendo que os riscos são gerenciados. A segurança da informação como uma vantagem competitiva é apontada por 61% dos respondentes. Mais da metade (57%) dos pesquisados afirma que sua estratégia cibernética está integrada à sua estratégia de crescimento[3].

A maioria (77%) dos CEOs de tecnologia acredita que uma estratégia cibernética sólida é fundamental para gerar a confiança das partes interessadas.1 Uma estratégia cibernética forte incorpora pessoas e tecnologia. A escassez contínua de talentos cibernéticos determina que todos os funcionários em todas as funções melhorem sua proficiência cibernética. Os Diretores de Segurança da Informação (CISOs) também estão intensificando sua participação — ampliando o seu papel para aumentar a colaboração e sua influência com outros líderes de unidades de negócios. Do ponto de vista tecnológico, os líderes das empresas estão aumentando seus investimentos em diversas soluções para aprimorar as proteções organizacionais.

A segurança cibernética cresceu além do foco tradicional de gerenciamento de riscos e *compliance* para se tornar uma vantagem competitiva que possibilita a confiança das partes interessadas e promove a resiliência organizacional. Essa não é mais uma questão exclusiva da área de TI — é uma prioridade estratégica que precisa ser incorporada em toda a cultura, tecnologia e operações de uma organização.

[1]. KPMG. *KPMG CEO Outlook 2021*. 2021.
[2]. IBM. *Cost of a Data Breach report 2021*. 2021.
[3]. KPMG. *KPMG Technology Industry Survey 2021*. 2021.

Principais constatações

A KPMG coletou opiniões sobre questões de segurança cibernética de CEOs e executivos seniores de empresas de tecnologia em dois estudos globais separados: o *Technology Industry Survey* e o *CEO Outlook*. Os principais resultados incluem o seguinte:

#1 **O risco de segurança cibernética é a principal ameaça ao crescimento.**

74% **afirmam estar preparados para um futuro ataque cibernético.**

#1 **A resiliência cibernética, com ênfase nas habilidades e na cultura cibernética, é a principal prioridade operacional.**

61% **consideram que a segurança da informação é uma função estratégica e uma vantagem competitiva potencial.**

87% **consideram que construir uma cultura de segurança cibernética é tão importante quanto construir controles tecnológicos.**

57% **acreditam que sua estratégia de segurança cibernética está integrada à sua estratégia de crescimento.**

Fontes:

KPMG. *KPMG CEO Outlook 2021*. 2021.

KPMG. *KPMG Technology Industry Survey 2021*. 2021.

Investindo em habilidades e tecnologia

Construindo um *firewall* humano

Os CEOs de tecnologia reconhecem que o ambiente de ameaças muda constantemente e soluções sofisticadas podem ser a base de um programa de segurança cibernética. No entanto, a tecnologia não consegue proteger tudo. Ela precisa ser reforçada pelo comportamento humano.

Muitos estudos mostram que uma grande porcentagem das violações reportadas inclui algum elemento de erro humano. Isso torna fundamental que as empresas desenvolvam e mantenham uma estratégia de segurança cibernética abrangente e que incorpore a qualificação da força de trabalho.

Firewalls humanos permitem que as empresas extrapolem a conscientização cibernética e construam uma abordagem integrada e holística para a comunicação e o treinamento dos funcionários acerca desse tema, elevando o comportamento dos funcionários de uma escolha consciente para um hábito arraigado. Os CEOs de tecnologia reconhecem isso e mencionam as habilidades e a cultura como as principais ações que estão realizando para desenvolver resiliência cibernética e digital nos próximos três anos.

As principais etapas que as empresas de tecnologia planejam realizar para construir resiliência digital nos próximos três anos.

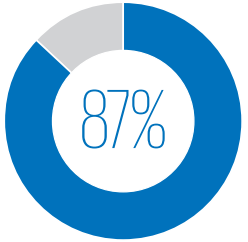
1 empate	**Focar a melhoria das habilidades em segurança cibernética e outras áreas de risco tecnológico**
1 empate	**Estabelecer uma forte cultura de risco digital e cibernético defendida pelos líderes seniores**
2	**Fortalecer a governança em torno da resiliência operacional e a capacidade de se recuperar de um grande incidente**
3	**Investir em uma infraestrutura baseada em nuvem segura e resiliente**

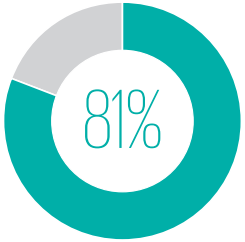
Fonte: KPMG. *KPMG CEO Outlook 2021*. 2021.

As empresas de tecnologia também fazem parte de um ecossistema complexo de fornecedores e parceiros, unidos por meio de dados e serviços compartilhados. Contratos tradicionais e modelos de responsabilidade parecem inadequados para essa cadeia de suprimentos em rápida transformação. A educação cibernética, o comportamento cibernético e a cultura cibernética desses aliados também devem mudar para proporcionar segurança a todas as partes.

Os CEOs de tecnologia reportaram uma alta concordância com as afirmações a seguir, reforçando que as habilidades cibernéticas e a cultura cibernética proficientes são requisitos fundamentais. Eles também reconhecem que as empresas devem trabalhar com seus parceiros e ecossistemas para criar um plano de defesa verdadeiramente holístico.

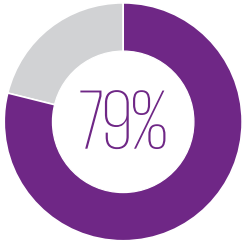
Construir uma cultura de segurança cibernética é tão importante quanto construir controles tecnológicos.





Uma abordagem envolvendo todo o setor será necessária para enfrentar adequadamente o problema das demandas de *ransomware*

Proteger o ecossistema de parceiros e a cadeia de suprimentos é tão importante quanto construir as defesas cibernéticas da própria organização.



Fonte: KPMG. *KPMG CEO Outlook 2021*. 2021.

Investindo em habilidades e tecnologia (continuação)

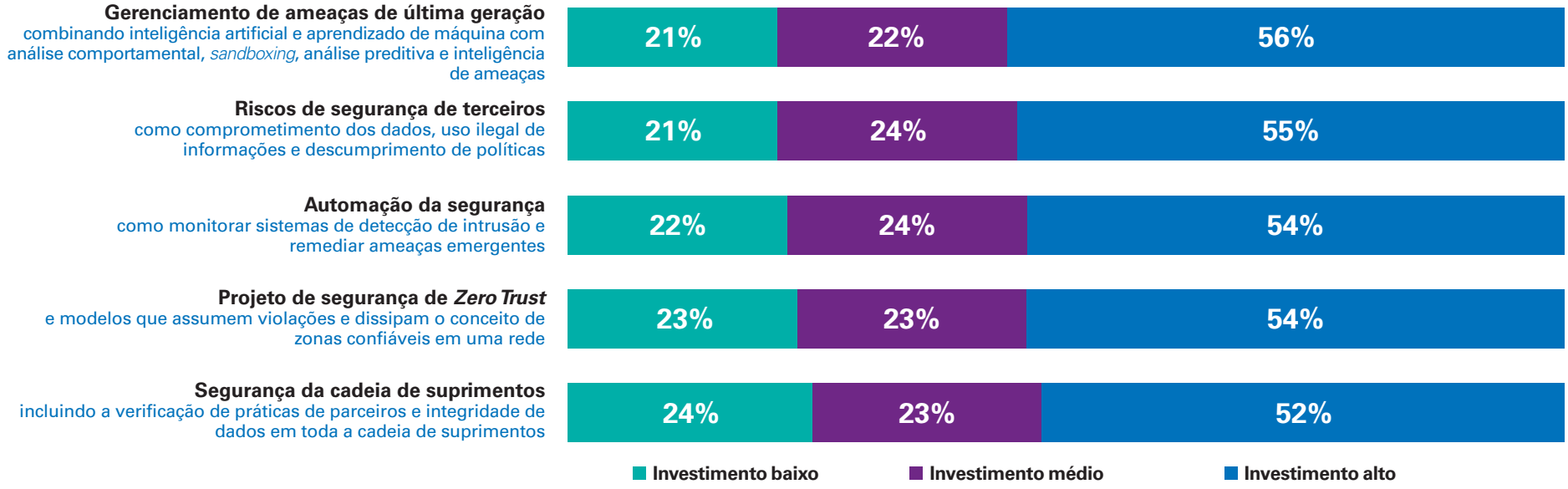
A segurança cibernética requer uma aldeia tecnológica

As empresas há muito reconhecem que uma tecnologia ou processo é incapaz de mitigar o risco cibernético por si só. É necessário investir de maneira contínua e ampla para identificar ameaças emergentes, melhorar os recursos de resposta da organização e aumentar a eficiência na segurança de todas as unidades de negócios. Os líderes de tecnologia também sentem que, embora as ferramentas cibernéticas sejam necessárias para possibilitar o sucesso da empresa, elas não podem ser intrusivas a ponto de afetar a eficiência operacional ou o crescimento.

Quando questionados sobre investimentos específicos em segurança, os executivos das empresas de tecnologia confirmaram que planejam realizar altos investimentos em várias áreas nos próximos três anos. O investimento em automação, especificamente, pode reduzir a carga de trabalho manual, diminuir a escassez de habilidades, promover maior eficiência e ajudar a atender aos requisitos crescentes de *compliance* de maneira consistente e reproduzível. Ele também pode ajudar a incorporar segurança e melhorar a experiência do usuário, além de reduzir o tempo de resposta a um grande incidente cibernético.

Estamos caminhando para um futuro hiperconectado, no qual a Internet das Coisas (IoT) e as redes 5G aumentarão massivamente a eficiência e permitirão modelos de negócios radicalmente diferentes. Porém, isso também coloca, na perspectiva das organizações, novos vetores de ataque e questões de privacidade — exigindo a adesão a novos modelos de segurança, preferencialmente centrados em dados, como o confiança zero (*zero trust*). Outro estudo da KPMG, intitulado O imperativo dos dados, – concluiu que 44% dos entrevistados acreditam que uma estratégia de dados eficaz teria um alto impacto na melhoria da segurança cibernética.

Nível esperado de investimento das empresas de tecnologia nos próximos três anos.

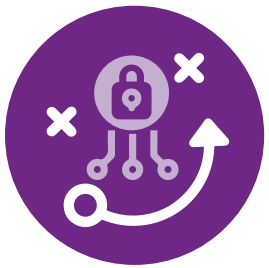


Fonte: KPMG. *KPMG Technology Industry Survey 2021*. 2021. Obs.: as porcentagens podem não totalizar 100% devido a arredondamentos

O investimento cibernético gera otimismo

De maneira geral, os líderes de empresas de tecnologia estão otimistas sobre a situação da sua função de segurança da informação, bem como sobre o grau de integração com seus esforços mais amplos de gerenciamento de risco, parcerias com terceiros e liderança de unidades de negócios. Quase três quartos (74%) dos CEOs de tecnologia afirmam estar preparados para um futuro ataque cibernético, em comparação com 58% em todos os setores[4].

Eles acreditam que seus maiores investimentos e foco renderam recursos empresariais suficientes para mitigar amplamente os riscos cibernéticos. Essa confiança e o investimento necessário para alcançá-la são necessários, pois 77% dos CEOs de tecnologia também acreditam que uma estratégia cibernética sólida é fundamental para gerar confiança junto aos principais *stakeholders*[4].



74% dos CEOs de tecnologia afirmam que estão preparados para um ataque cibernético futuro[4].

Executivos de empresas de tecnologia que concordam com as afirmações a seguir:

Minha empresa enxerga a segurança da informação como uma função estratégica e uma vantagem competitiva potencial. **61%**

Os riscos de segurança cibernética da minha empresa são incorporados ao planejamento geral de riscos corporativos. **60%**

Minha empresa está preparada para gerenciar os riscos de terceiros de fornecedores que prestam serviços críticos e/ou têm acesso a dados confidenciais. **58%**

A estratégia de segurança cibernética da minha empresa está integrada à sua estratégia de crescimento. **57%**

Fonte: KPMG. *KPMG Technology Industry Survey 2021*. 2021.

4. KPMG. *KPMG CEO Outlook 2021*. 2021

O CISO redefinido

Com as empresas de tecnologia combinando trabalhadores locais e remotos, dispositivos de IoT, parceiros terceirizados e provedores de serviços em equipes e ecossistemas dinâmicos, o CISO está assumindo um papel mais amplo não apenas na manutenção da segurança cibernética, mas também na resiliência organizacional geral.

Conforme as ameaças e expectativas regulatórias evoluem, os CISOs estão assumindo responsabilidades cada vez maiores e construindo relacionamentos com uma ampla gama de funções e líderes de unidades de negócios. A função do CISO vai além de "proteger e detectar": ela é estratégica e fundamental para que a empresa volte a funcionar com a máxima rapidez após um incidente e para que o CEO mantenha a confiança de clientes, fornecedores, reguladores e outras partes interessadas.

Os CISOs estão interagindo mais com CEOs e Conselhos, fornecendo atualizações consistentes sobre ameaças emergentes e esforços de mitigação, enquanto mantêm seus relacionamentos tradicionais com os Diretores de Tecnologia (CTOs) e Diretores de TI (CIOs). Eles estão ajudando a integrar a segurança nos processos de governança e gestão, educação e conscientização, além de estabelecerem a combinação correta de incentivos corporativos e pessoais para fazer a coisa certa.

Os CISOs têm aproveitado essa oportunidade para aumentar a resiliência organizacional, trabalhando para incorporar princípios de projeto focados em segurança e privacidade em todas as infraestruturas digitais de suas empresas. Esse escopo ampliado permite que as organizações melhorem sua capacidade de mitigar os riscos cibernéticos, regulatórios e de negócios.

Sete etapas que os CISOs devem considerar para melhorar seu papel.

1. Falar a linguagem do Conselho, pensando em termos de clientes, receita, custos e retorno sobre o investimento.

2. Concentrar-se na resiliência operacional: como manter as atividades e voltar ao normal rapidamente após uma crise.

3. Investir tempo na construção de uma rede na sua organização, visitando diferentes funções, aprendendo de que maneira elas funcionam e conquistando maior confiança.

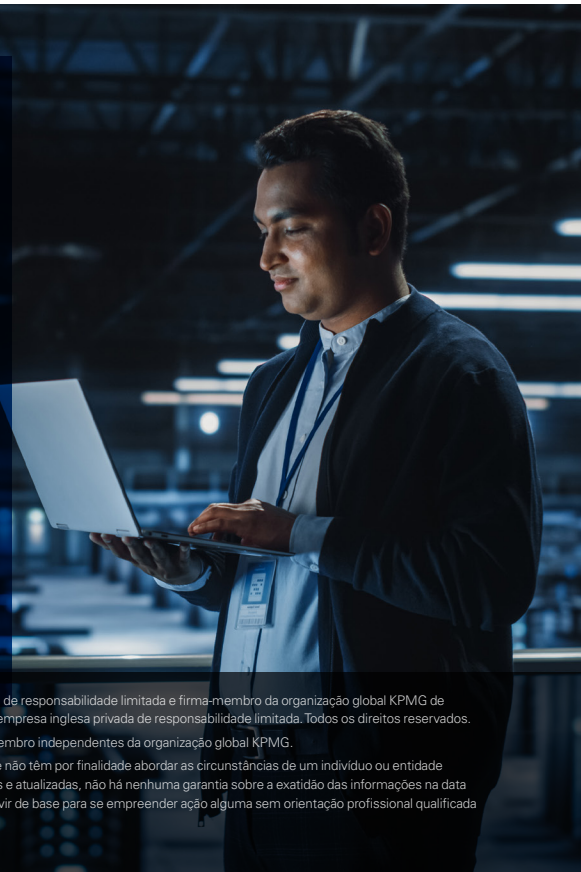
4. Refletir sobre como moldar a força de trabalho para as necessidades cibernéticas do negócio, em oposição a funções e estruturas permanentes. Considerar a proporção de funcionários e subcontratados e trabalhadores temporários.

5. Criar um caso de negócios para a automação, refletindo as eficiências que ele traz e o valor agregado dos trabalhadores que são liberados para tarefas de nível superior.

6. Descobrir o que a confiança zero significa para o seu negócio e enxergá-la como uma filosofia contínua em vez de um programa episódico.

7. Encontrar maneiras de se relacionar com seus pares no seu setor, ingressando em órgãos setoriais existentes ou formando grupos menos formais.

Leia mais sobre a evolução do papel do CISO aqui.



Principais considerações para os líderes de empresas em 2022

Ampliar a conversa sobre segurança estratégica

Mudar prioridades: a segurança eficaz passa a ser mais importante do que custo e velocidade, de modo a oferecer um maior valor de negócio e proporcionar uma experiência aprimorada ao usuário.

Desenvolver talentos e conjuntos de habilidades críticos

Transformar a equipe de segurança cibernética de executora em influenciadora.

Adaptar a segurança para a nuvem

Aumentar a segurança da nuvem por meio da automação — da implementação, passando pelo monitoramento, à remediação.

Colocar a identidade no centro do modelo *Zero Trust*

Colocar o gerenciamento de identidades e de acesso e a confiança zero para funcionar no local de trabalho – lembrando que, hoje, esse "local de trabalho" é hiperconectado.

Explorar a automação da segurança

Obter vantagem competitiva por meio da implementação inteligente da automação da segurança.

Proteger a fronteira da privacidade

Migrar para uma abordagem multidisciplinar de gerenciamento de risco de privacidade que incorpore os conceitos de *privacy by design* e *security by design*

Proteger além das fronteiras

Proteger a organização ao incentivar a cadeia de suprimentos mais ampla a ter segurança cibernética

Reformular a conversa sobre resiliência cibernética

Ampliar a capacidade de manter as operações, recuperar-se rapidamente e mitigar as consequências quando um ataque cibernético ocorrer

Leia mais sobre essas considerações aqui.

Sobre os autores

Alex Holt é sócio-líder global de Tecnologia, Mídia e Telecomunicações da KPMG no EUA, e está baseado no Vale do Silício (Califórnia, EUA). Conta com mais de 20 anos de experiência internacional. Alex ingressou na KPMG em 2012 como diretor de operações no Reino Unido, assumindo a liderança do setor de TMT deste país em 2015. Mudou-se para os Estados Unidos, ingressando na KPMG nos EUA em 2018 como executivo de contas globais para várias empresas líderes de tecnologia com base no Vale do Silício. Em 2020, ele assumiu a prática global de TMT, liderando os profissionais da KPMG que atendem clientes em todo o setor com uma ampla gama de serviços de consultoria, impostos e auditoria. alexanderholt@kpmg.com

Mark Gibson é sócio-líder de Tecnologia, Mídia e Telecomunicações da KPMG nos EUA. Durante seus 30 anos de experiência em contabilidade e consultoria pública, ele atendeu clientes nos setores de tecnologia, produtos de consumo e varejo como sócio de auditoria e consultoria. Antes de sua função atual, Mark foi o sócio de gestão do escritório de Seattle (EUA). Ele atua como executivo de contas para grandes clientes no mercado norte-americano e trabalha com profissionais da KPMG de auditoria, tributação e consultoria em mais de 15 países. mgibson@kpmg.com

Vijay Jajoo é sócio-líder da prática de *Cyber Security Services* da KPMG nos EUA. Ele é tem mais de 20 anos de experiência especializada em estratégia de TI, arquitetura de segurança corporativa, implementação de soluções, gerenciamento de identidades e acesso, segurança na nuvem e governança corporativa, riscos e *compliance*. Vijay ajuda as empresas de tecnologia globais a se transformarem, estabelecendo confiança e incorporando segurança cibernética e privacidade em projetos de produtos e serviços. Ele impulsiona o alinhamento interfuncional para desenvolver soluções inovadoras com análises avançadas e correlaciona conjuntos de dados em grupos para fornecer *insights* para decisões eficazes de mitigação de riscos. vjajoo@kpmg.com

Colaboradores

Danny Le
Sócio-líder de Cyber Security Services
da KPMG nos EUA
dqle@kpmg.com

Rik Parker
Sócio-líder de Cyber Security Services
da KPMG nos EUA
rikparker@kpmg.com

Deepak Mathur
Diretor de Serviços de Cyber Security Services
da KPMG nos EUA
deepakmathur@kpmg.com

Austyn McLoughlin
Diretor de Serviços de Cyber Security Services
da KPMG nos EUA
austynmcloughlin@kpmg.com

Como a KPMG pode ajudar

As firmas da KPMG podem ajudar a criar um mundo digital resiliente e confiável — mesmo diante das ameaças. Os profissionais de segurança cibernética da KPMG podem oferecer uma visão multidisciplinar do risco, ajudando-o a implementar a segurança em toda a sua organização, para que você possa antecipar o futuro, mover-se com mais rapidez e obter vantagens com tecnologia segura e confiável.

Não importa em qual ponto da sua jornada de segurança cibernética você esteja, as firmas-membro da KPMG têm a experiência e os recursos em todo o espectro — da sala do conselho ao *data center*. Além de avaliar sua segurança cibernética e alinhá-la às suas prioridades de negócios, podemos ajudá-lo a desenvolver soluções avançadas, implementá-las, assessorá-lo no monitoramento dos riscos contínuos e ajudá-lo a responder a incidentes cibernéticos com eficácia.

As firmas da KPMG oferecem uma combinação exclusiva de especialização tecnológica, profundo conhecimento de negócios e profissionais criativos que são apaixonados em ajudá-lo a proteger e construir o seu negócio. Nós o ajudaremos a criar um mundo digital confiável, para que você possa ultrapassar os limites do que é possível. Saiba mais aqui.

Sobre as fontes de pesquisa

A *KPMG Technology Industry Survey* 2021, atualmente no seu nono ano, incluiu respostas de mais de 800 executivos globais no setor de tecnologia em 12 países. Doze países foram incluídos na pesquisa *on-line* e cerca de dois terços (65%) dos entrevistados eram executivos de alto nível. A coleta de dados para esta publicação foi concluída no terceiro trimestre de 2021.

A *KPMG CEO Outlook 2021* solicitou a 1.325 CEOs que apresentassem suas perspectivas sobre o cenário econômico e de negócios e sobre o impacto que a pandemia de covid-19 terá no futuro de suas organizações. A pesquisa foi realizada de 29 de junho a 6 de agosto de 2021 e incluiu líderes de 11 países e 11 setores. Um total de 120 respondentes de empresas de tecnologia participou.

Material relacionado

Firewall Humano: Superando o Fator de Risco Humano na Segurança Cibernética

Os *firewalls* humanos permitem que as empresas superem o fator de risco humano na segurança cibernética. Este relatório explora as cinco etapas que as organizações devem seguir para aumentar a conscientização e criar uma abordagem integrada e holística para a comunicação dos funcionários em torno da segurança cibernética — elevando o comportamento dos funcionários de uma escolha consciente para um hábito arraigado.

From Enforcer to Influencer

Os CISOs e as equipes de segurança cibernética atualmente são responsáveis por construir confiança e resiliência, forjando uma cultura de segurança pragmática e ajudando a incorporar o *design thinking* em cada aspecto da infraestrutura digital e de dados. Para fazer isso, eles devem se ver como habilitadores e facilitadores. Este relatório identifica sete ações que os CISOs devem tomar para ajudar a manter as organizações resilientes e competitivas.

Fatores-chave sobre Segurança Cibernética em 2022

Olhando além das mudanças digitais criadas pela pandemia, esse mundo hiperconectado provavelmente enfrentará riscos cibernéticos crescentes em várias frentes globais. Este relatório identifica oito fatores-chave que os líderes devem priorizar para ajudar a mitigar e minimizar o impacto dos ataques cibernéticos enquanto protegem os clientes, os dados e a sustentabilidade.

The Data Imperative

A transformação digital acelerou na maioria das empresas durante a COVID-19, resultando em enormes novas quantidades de dados que as empresas não estão utilizando plenamente. Este relatório descreve como as estratégias de dados devem ser priorizadas e reescritas para aproveitar os investimentos em transformação digital.

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

Felipe Catharino
Sócio-diretor líder do segmento de Tecnologia da KPMG no Brasil
felipecatharino@kpmg.com.br

Baixe o nosso APP

kpmg.com.br

/kpmgbrasil