KPMG

Da reorganização geopolítica à construção da resiliência

Expostas a inúmeros desafios, incluindo a guerra entre Rússia e Ucrânia, as empresas de energia e serviços públicos são desafiadas a lidar com o redesenho do mapa global de energia, riscos cibernéticos ascendentes, questões de ESG e muito mais

Por Anderson Dutra*

Agosto de 2022

KPMG

Sumário

01

Introdução

As empresas de energia e serviços públicos lidam hoje com desafios sem precedentes. Neste artigo, vamos analisar aspectos como os riscos geopolíticos e seus impactos sobre as cadeias de suprimentos; de que maneira a guerra entre Rússia e Ucrânia vem reescrevendo o mapa global de energia; os riscos cibernéticos crescentes e sua relação com a agenda ESG (*environmental, social, and governance*) e a importância de se construir uma cultura de resiliência.

Os *insights* a seguir foram extraídos de artigos veiculados originalmente na revista *Plugged In*, uma publicação da KPMG.

02

Da globalização à segurança nacional

A guerra na Ucrânia alterou drasticamente as percepções sobre segurança energética e acelerou a agenda de descarbonização de muitos países.

Como a União Europeia (UE) prometeu cortar o fornecimento de gás da Rússia em dois terços até o final de 2022 e concordou com uma proibição parcial do petróleo russo, foi necessário buscar alternativas. Uma delas foi a aquisição de Gás Natural Liquefeito (GNL) dos Estados Unidos; mas isso não basta para suprir as necessidades dos países europeus; por isso, a UE está focada em acelerar drasticamente sua ambição de zero líquido, como exemplificado por seu plano **RePower EU**.

Vale ressaltar que, antes da guerra, os setores de energia e serviços públicos já passavam por dificuldades na Europa. Pressões de grupos ambientalistas e a própria ânsia da sociedade por energias mais limpas já vinham impulsionando as mudanças.

03

Riscos na cadeia de suprimentos

O mundo pode estar caminhando para um redesenho de fluxos comerciais e de suprimentos. Esse movimento se intensificou a partir da pandemia da covid-19, quando ficaram ressaltados os riscos da dependência de poucos países ou regiões para o abastecimento de determinados recursos.

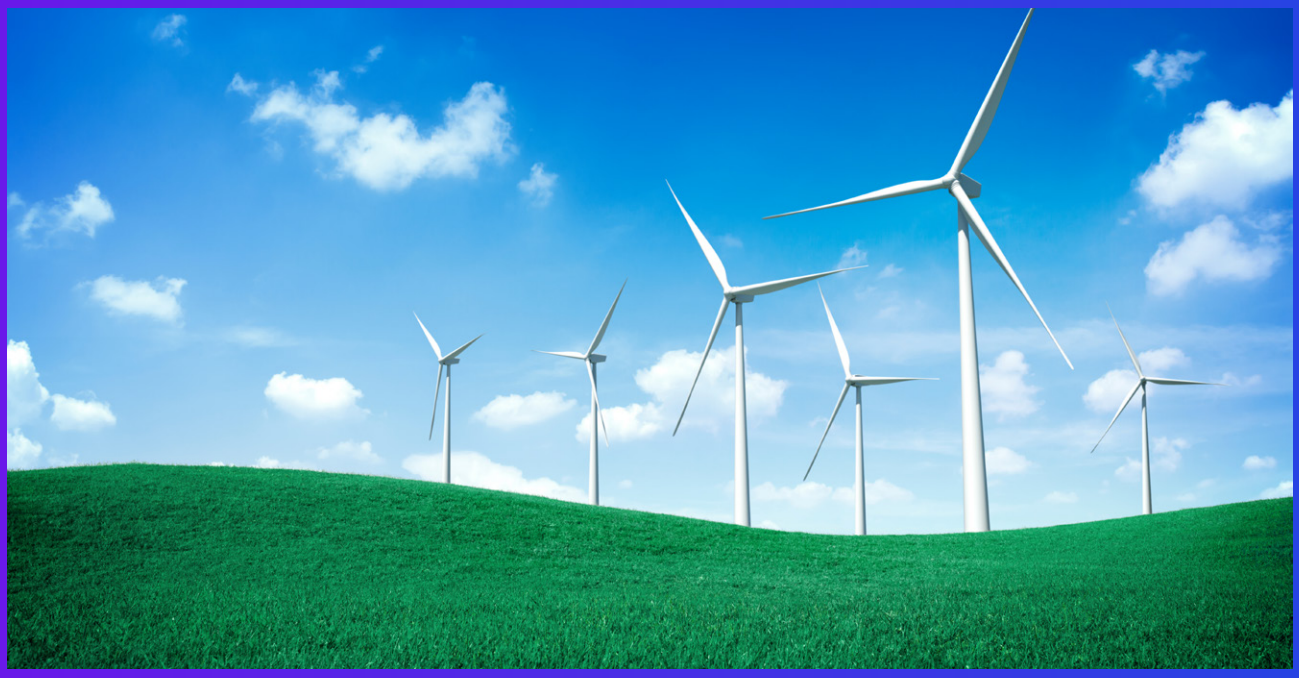
Essas mudanças afetam também o mapa global de energia.

Com essa tendência, veremos uma profunda transformação na dinâmica das cadeias de suprimentos globais, com os fornecedores de energia e serviços públicos buscando fontes alternativas imediatas, inclusive GNL dos EUA e de outras regiões, para satisfazer a demanda doméstica dos consumidores e suprir as indústrias – sobretudo aquelas que demandam altíssimo uso de energia, como as siderúrgicas.

As cadeias de suprimentos de componentes para os setores de energia nuclear, hidrogênio e energia renovável, especialmente urânio, baterias, energia solar e eólica,

> **"O ponto positivo é que existem diversas ferramentas tecnológicas com capacidade de avaliar o nível de risco dos provedores."**

Emerson Melo
Sócio-líder de Forensic & Litigation da KPMG no Brasil e na América do Sul



provavelmente sofrerão uma pressão mais significativa à medida que a corrida por alternativas se intensificar.

A vulnerabilidade das cadeias de suprimentos e sua interdependência global são cada vez mais evidentes. Para o futuro, será imperativo e urgente encontrar fontes novas e confiáveis.

Esse cenário não difere no mercado local. Durante a pandemia, constatamos a centralização de algumas matérias-primas em um número reduzido de provedores no Brasil. A situação chamou a atenção sobre as necessidade da revisão e diversificação das cadeias de suprimentos.

A avaliação da cadeia é realizada por meio de um mapeamento completo de toda a cadeia de fornecedores *end to end*, entendendo todas as camadas de interação dos fornecedores atuais com as demais camadas (*tiers*) de fornecimento.

Dessa forma, não basta monitorar somente o fornecedor principal. É necessário ter visibilidade de toda a cadeia de suprimentos, entendendo as suas interconexões e as origens das matérias-primas que compõem o produto final.

Outro fator importante consiste na construção de um *Should Cost Model*, no qual é possível ter uma visão detalhada da composição dos custos dos materiais adquiridos, compreendendo os fatores que podem causar aumentos significativos no custo dos produtos adquiridos e minimizando os riscos operacionais e o posicionamento de preço no mercado.

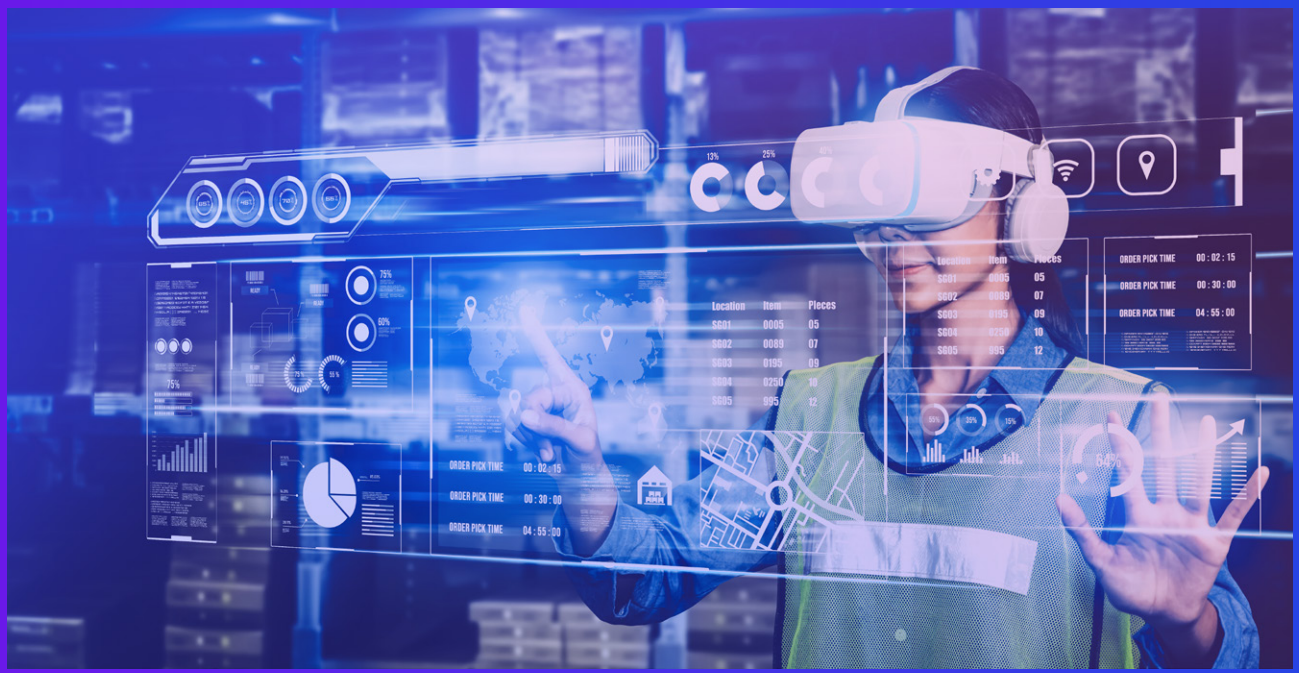
Nesse novo contexto, os fornecedores não podem mais ser tratados como apenas como provedores, mas sim como *business partners* (aliados de negócio), uma vez que é fundamental incrementar o nível de colaboração entre cliente e fornecedor, de forma a obter maior visibilidade dos estoques ao longo da cadeia de suprimentos em tempo real.

A adoção de torres de controle passa a ser fundamental para agir de forma antecipada e preditiva nos gargalos operacionais de transporte e armazenagem em toda a cadeia de fornecedores.

Para sanear esses desafios, as empresas têm investido em novas tecnologias para aumentar a precisão de seu planejamento e, assim, garantir níveis de estoque adequados para não gerar rupturas na cadeia de suprimentos.

Soluções robustas de inteligência de dados estão sendo construídas para traçar um modelo mais preditivo de demanda, e tecnologias como *machine learning* e inteligência artificial são fundamentais para interpretar os dados coletados na cadeia de suprimentos e transformá-los em *insights* estratégicos que possam direcionar o posicionamento de estoques na cadeia e a estratégia de abastecimento.

Para isso, a KPMG apoia organizações em sua revisão da matriz estratégica de compras, identificando os materiais críticos e estratégicos e desenhando estratégias de contingência para garantir o abastecimento desses itens e, consequentemente, reduzindo o risco de ruptura na cadeia e garantindo a sustentabilidade do negócio a curto, médio e longo prazo.



Outro ponto muito relevante é a avaliação da capacidade dos provedores atuais. Hoje, as empresas de todos os setores dependem cada vez mais de uma rede robusta de terceiros, tais como fornecedores, distribuidores, agentes, terceiros intermediários, *joint ventures*, alianças, subcontratados e prestadores de serviços, entre outros.

Essa rede é fundamental para manter uma presença global e um diferencial competitivo, além de concorrer com eficácia e eficiência no mercado.

Embora os terceiros sejam fundamentais para uma empresa atuar globalmente, os riscos associados a eles não podem ser terceirizados. Há muitos casos em que a falta de supervisão e monitoramento adequado dos fornecedores gerou graves consequências. Empresas globais já foram expostas a riscos significativos, afetando negativamente seu desempenho, imagem e reputação, além do impacto financeiro.

Adicionalmente, os órgãos regulatórios em todo o mundo esperam que as empresas realizem a supervisão e o monitoramento efetivo e eficiente de seus terceiros. Por isso, as empresas tiveram que priorizar e aprimorar seus esforços de *compliance* em consequência de ações de execução e multas em função de casos de suborno e corrupção, lavagem de dinheiro e violações à legislação. Na maioria dos casos reportados, houve suborno por meio de intermediários externos.

Diversos organismos internacionais publicaram regulamentações e boas práticas sobre o ciclo de vida de terceiros (identificação, avaliação de riscos, *due diligence*, integração, avaliação e monitoramento contínuo) relacionadas à eficácia dos programas de *compliance*.

O Departamento de Justiça (DOJ) e a Comissão de Valores Mobiliários (SEC) dos EUA elaboraram um guia conjunto, que estipulava como a *due diligence* baseada em riscos é particularmente importante com terceiros e que deve ser considerada ao se avaliar a efetividade do programa de *compliance* de uma empresa. Além disso, o DOJ forneceu orientações detalhadas recentemente sobre a avaliação de programas de *compliance* corporativo.

A supervisão e o monitoramento do ciclo de vida de terceiros evoluíram de uma abordagem reativa para uma de alinhamento aos programas globais de *compliance* corporativo. Para obter essa consistência, os programas de gerenciamento de riscos de terceiros (*Third Party Risk Management* - TPRM) ideais precisam ir além da função de compras e englobar outros *stakeholders* e departamentos da empresa.

Esses programas também ganharão maturidade por meio da automação, com a qual a organização se beneficia dos dados e entende os riscos por meio da tecnologia para aprimorar o gerenciamento de terceiros de maneira sustentável.

Embora as empresas continuem enfrentando riscos complexos em ambientes de negócios dinâmicos e os reguladores pressionem as empresas para que elas estejam em conformidade, continuará sendo essencial que os negócios mantenham uma abordagem sustentável para que qualquer programa de gerenciamento de riscos de terceiros seja bem-sucedido.

O KPMG Watch é uma plataforma tecnológica, desenvolvida pela KPMG, que permite diversos acessos simultâneos de fontes individuais de informação públicas e privadas e possibilita uma avaliação completa, eficiente e de alto valor agregado de terceiros.

04

Risco cibernético

Os ativos de energia e serviços públicos são vitais para a segurança nacional. Em um mundo abalado por guerras, é previsível que as práticas de *hacking, ransomware* e *malware* sejam adotadas como novas "armas" – isso sem falar dos criminosos cibernéticos e *hacktivistas*, que têm atentado contra a segurança cibernética de empresas e governos nos últimos anos.

Companhias de energia e prestadoras de serviços públicos possuem com uma quantidade gigantesca de dados e têm múltiplas frentes de atuação. Ou seja: suas superfícies de ataque são amplas. Um ataque *hacker* pode levar à inoperância de usinas, geradores e turbinas eólicas; à desconexão remota das redes, causando prejuízos imensos; e, no âmbito da Internet das Coisas (*Internet of Things* -IoT), acarretar panes a dispositivos e veículos elétricos, levando ao roubo de informações de clientes, fraude de faturamento e interrupção dos serviços.

Mais do que nunca, fornecedores de energia e serviços públicos devem revisar seus planos de continuidade dos negócios, avaliar as vulnerabilidades ao longo da cadeia de suprimentos e realizar simulações para identificar fragilidades e prever respostas aos possíveis ataques. Criar uma cultura cibernética ajuda a evitar a perspectiva de um ataque e a melhorar a comunicação de incidentes.

05

Mudanças climáticas e gestão de ativos

Milhares de quilômetros de gasodutos e linhas de energia elétrica. Basta uma pequena falha em qualquer um desses equipamento paras iniciar um incêndio florestal, por exemplo e, como consequência, a companhia responsável pelo incidente sofrerá perdas em diversos níveis, desde multas pesadíssimas até danos de imagem que demoram anos para serem revertidos.

Mas a verdade é que existe muita infraestrutura envelhecida que lida com uma quantidade gigantesca de dados e com múltiplas frentes de atuação, ou seja: suas superfícies de ataque são amplas. Um ataque hacker pode levar à inoperância de usinas, geradores e turbinas eólicas; à desconexão remota das redes, causando prejuízos imensos; e, no âmbito da Internet das Coisas (*Internet of Things* - IoT), acarretar panes a dispositivos e veículos elétricos, levando ao roubo de informações de clientes, fraude de faturamento e interrupção dos serviços. Há muita cobrança pela substituição dos ativos vulneráveis. Os perigos aumentam à medida ▸

Claudio Graeff
Sócio de Infraestrutura da KPMG no Brasil

Rodrigo Milo
Sócio de Cyber Security & Privacy da KPMG no Brasil

05

Mudanças climáticas e gestão de ativos (continuação)

que as mudanças climáticas se tornam uma realidade e acarretam, com frequência e intensidade cada vez maiores, tempestades com vendavais e mudanças bruscas de temperatura.

Para se tornarem mais resilientes, as empresas precisam adotar modelos de gestão de ativos baseados em gestão de riscos, de performance e de custos, a fim de avaliar seus ativos mais vulneráveis.

A utilização de tecnologias emergentes pode ser muito útil para as empresas, como *drones* de longo alcance para inspeções visuais e tecnologias de satélite para avaliar as mudanças no entorno de seus ativos, por exemplo. Com o exposto acima, a gestão de ativos, cada vez mais deve fazer parte da estratégia das empresas para garantir a continuidade de suas operações alinhada aos objetivos de longo prazo. A manutenção sozinha não é capaz de avaliar impactos, riscos e benefícios para manter, substituir ou descartar um ativo e, por isso, é importante a implantação do processo de gestão de ativos em seu mais amplo espectro, a fim de analisar a necessidade de investimentos e os riscos de um determinado período.

No Brasil, entrou em vigor desde julho de 2022 a resolução normativa nº 964, que dispõe sobre regras de segurança cibernética a serem adotadas pelos agentes do setor de energia elétrica. A resolução tem como objetivo ser o primeiro passo para a preparação das políticas de segurança cibernética pelas empresas, com classificação dos dados, registro e análise da causa e do impacto de possíveis incidentes que possam ocorrer. Para o mercado, isso representa uma evolução sobre o tratamento dos riscos cibernéticos e um passo adiante para a padronização da troca de informações entre empresas do setor e agências reguladoras.

Entretanto, o grande desafio das empresas é trabalhar com a avaliação dos riscos cibernéticos para os ambientes de tecnologia da informação (TI) e de operação (*operational technology* - OT) e avaliar se os padrões estabelecidos inicialmente na resolução permitem o efetivo aumento da maturidade cibernética das organizações.

Segundo dados do PDE 2031, quase 70% dos ativos de transmissão já estão com a sua vida útil regulatória expirada. Este cenário é desafiador, considerando o crescente volume de energias renováveis adicionados ao SIN (Sistema Integrado Nacional) e a grande onda de descentralização da geração.

06

ESG e segurança cibernética são dois lados da mesma moeda

Conforme já apontado, os países que têm forte dependência dos combustíveis russos estão lidando com uma emergência: encontrar alternativas em um cenário marcado pela guerra contra a Ucrânia, que acarretou sanções contra a Rússia.

A Alemanha é um desses países. E, na durante a Conferência das Nações Unidas sobre Mudanças Climáticas (COP26), realizada em Glasgow, na Escócia, em novembro de 2021, os alemães anunciaram a intenção de abandonar totalmente o carvão até 2030, oito anos antes de sua meta original. Agora, sua meta é extrair de fontes renováveis nada menos que 80% de sua eletricidade.

França, Áustria e Polônia, alguns dos maiores consumidores de carvão da Europa, caminham na mesma direção.

Tais ambições se alinham com os Objetivos de Desenvolvimento Estratégico (ODEs) da ONU. O mundo depende cada vez mais da eletricidade – inclusive para alimentar os meios de transporte –, mas as energias renováveis precisam passar no teste de confiança e demonstrar que podem oferecer a confiabilidade sem interrupções.

Um dos lados positivos das fontes renováveis – além, claro, de serem fundamentais para a descarbonização – é que elas geram energia perto do consumidor. As microrredes levam esse conceito um passo adiante, possibilitando que provedores menores e consumidores individuais produzam, armazenem e distribuam energia limpa.

No entanto, a multiplicidade de novos fornecedores de energia — inclusive residências particulares —, que atuam equipados com medidores inteligentes conectados a dispositivos móveis pessoais, amplia exponencialmente a complexidade das redes de distribuição. Além disso, há a crescente digitalização da tecnologia operacional (*Operational Technology* -OT) das usinas de energia, o que inclui inúmeros dispositivos IoT para rastrear o desempenho e a captura de carbono.

O resultado é um leque maior de pontos de ataque. Em sistemas cada vez mais interconectados, os *hackers* têm várias oportunidades de invadir a rede primária.

07

Construir e manter a confiança na descarbonização

A segurança cibernética robusta e a elaboração de relatórios demonstram para os *stakeholders* que as empresas de energia e serviços públicos têm operações seguras e resilientes, capazes de se precaver e se recuperar de ataques cibernéticos e físicos e de ameaças climáticas, como incêndios florestais, inundações, ventos e temperaturas extremas de calor e frio.

Para lidar com as ameaças cibernéticas crescentes, uma cultura de segurança cibernética e um protocolo robusto podem melhorar as defesas e a capacidade de resposta. A prioridade é proteger os ativos críticos que determinam se os clientes recebem energia, água e outros serviços públicos vitais.

Todas as empresas de energia e serviços públicos precisam de uma estrutura padrão para medir o risco cibernético e de procedimentos transparentes para restaurar o serviço após um ataque.

Há falta de consistência global quanto aos padrões e práticas de segurança cibernética e uma necessidade urgente de convergir e compartilhar informações para tornar todo o setor de energias renováveis mais resiliente, de modo a conquistar e a manter a confiança da sociedade – e, por consequência, acelerar a sua adoção.

Dado o papel excepcional da infraestrutura de energia e serviços públicos para todos os países e a natureza interconectada da energia, é provável que os governos se envolvam mais e colaborem com os agentes privados em toda a cadeia de suprimentos.

A agenda ESG, por sua vez, pode beneficiar o setor de energia e serviços públicos, delegando-lhes um papel essencial na consolidação de sociedades mais verdes, seguras e resilientes.

Elementos críticos

Governança:
Um executivo sênior deve ser o responsável pela gestão do risco de segurança cibernética.

Vulnerabilidades:
Deve-se conhecer as vulnerabilidades e acompanhar a evolução das potenciais ameaças.

Cultura:
É importante que todos os profissionais tenham treinamento abrangente em segurança cibernética.

Ativos:
É fundamental manter-se informado sobre todos os ativos que podem precisar de proteção cibernética.

Monitoramento:
Sistemas e ativos devem ser monitorados continuamente.

Relatórios:
É fundamental acompanhar e relatar a eficácia das defesas de segurança cibernética e a origem, o volume e a gravidade dos incidentes.

Conformidade de segurança
É essencial manter-se a par das normas e dos regulamentos do setor para a sua prática e divulgação.

A KPMG pode proporcionar uma abordagem prática para seus relatórios de segurança cibernética, de modo a promover a confiança digital na sua organização. Nossa firmas-membro oferecem uma variedade de serviços ideais para que sua organização crie uma mensagem digital confiável, incluindo:

01 Avaliações da maturidade cibernética (CMAs) para examinar o cenário atual de ameaças e riscos e a conformidade com os regulamentos do setor.

02 Desenvolvimento de um modelo operacional de destino e gerenciamento de mudanças para governar seu programa cibernético.

03 Associação com as principais plataformas de descoberta de IoT/TO para ajudar a identificar seus ativos operacionais e manter sua visibilidade.

04 Suporte de serviços gerenciado para monitorar os alertas do IDS/IPS na tecnologia operacional.

05 Programas de gerenciamento de vulnerabilidades para garantir que seus sistemas permaneçam operacionais e protegidos.

06 Programas de treinamento e conscientização sobre segurança cibernética criados para ambientes e pessoal de OT.

07 Análise de dados avançada para avaliar a postura contínua do programa de segurança.

As emergências climáticas deveriam estar no topo das agendas governamentais de todos os países. Pelo menos, de todos aqueles que assumiram compromissos de redução drástica de emissões durante a COP26 (26ª Conferência do Clima da Organização das Nações Unidas).

O Brasil, por exemplo, assumiu uma nova meta climática na ocasião: antes, o País prometia reduzir **43%** de suas emissões até 2030; na COP26, prometeu uma redução de **50%** e neutralidade de carbono até 2050.

08

Da continuidade à resiliência

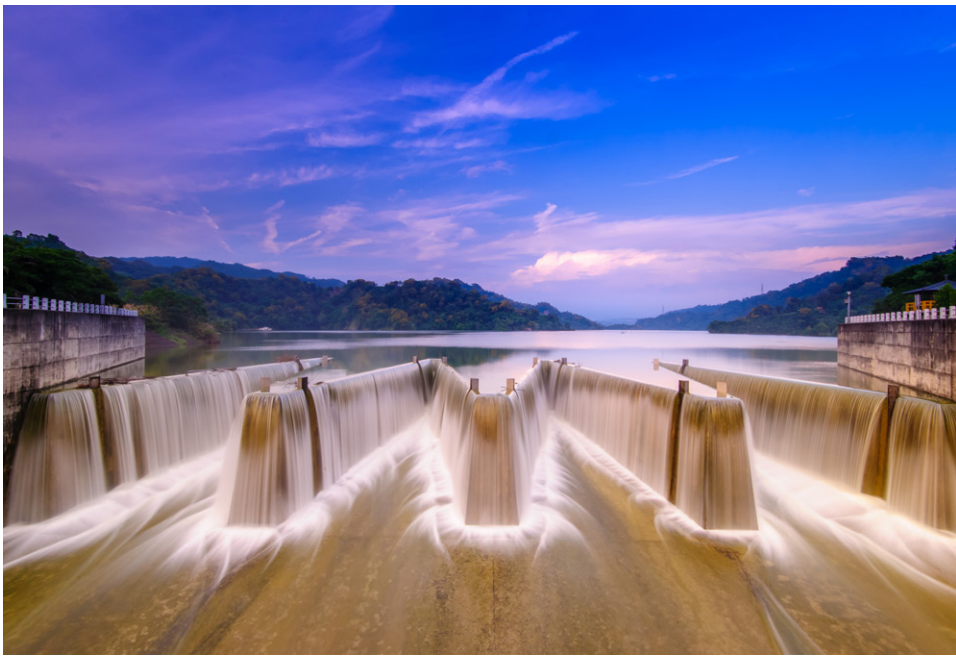
"*Too big to fail*" (em tradução livre para o português, "muito grande para falhar") é uma expressão muito usada em inglês, mas é relevante e apropriada no caso de energia e serviços públicos, essenciais à nossa existência.

Ao longo do tempo, empresas de energia e serviços públicos, estatais e privadas, sempre se concentraram em suprir as necessidades do consumidor de forma segura e sem interrupções.

Hoje, o setor enfrenta inúmeros desafios. As mudanças climáticas são uma preocupação grande e crescente para o setor. Tempestades, queimadas e incêndios florestais, inundações, ventos, calor e frio extremos e secas são cada vez mais recorrentes e causam prejuízos milionários.

Na Índia, em 2022, mais de um bilhão de cidadãos enfrentaram temperaturas acima de 40° Celsius. Foi a primavera mais quente registrada na história do país. Ficaram inviáveis atividades corriqueiras, como o trabalho ao ar livre; houve danos à agricultura, falta de água, racionamento imposto pelo Estado, cancelamento de trens e outros inconvenientes.

Além de danificar a infraestrutura física, esses fenômenos também podem causar atrasos nas cadeias de suprimentos de peças e materiais vitais. Além disso, as empresas de energia e serviços públicos não têm que lidar apenas com os efeitos das mudanças climáticas em suas operações, mas também considerar o impacto de sua própria organização no meio ambiente e na sociedade, seja nas emissões de carbono, seja no tratamento dos funcionários.



09

Ameaças operacionais

As redes estão se tornando mais distribuídas, com faixas de fontes de energia menores e localizadas, criando uma mistura híbrida de energia convencional/nuclear e, cada vez mais, renovável, proveniente de pequenos geradores de energia hidroelétrica, de biomassa, de biogás, solar, eólica e geotérmica. É uma grande dor de cabeça orquestrar essa complexa rede de participantes para manter a integridade do sistema.

Ao mesmo tempo, a digitalização traz maior automação e sofisticação aos sistemas de controle, integrando operações e TI, com dependência cada vez maior de uma rede externa em nuvem e provedores *as-a-service*. Com esse *backbone* interconectado, uma única falha pode ter várias consequências e potencialmente desligar toda a instalação.

À medida que os fornecedores de energia e serviços públicos migram para empresas digitais, com todos os equipamentos interconectados, inclusive *hardware*, sensores de IoT e dispositivos pessoais e com o inevitável envolvimento de terceiros, aumenta drasticamente o risco de ataques cibernéticos.

A construção de uma **estrutura de resiliência integrada** envolve algumas etapas, listadas a seguir:

01 Definir o escopo e entender necessidades e requisitos dos *stakeholders*.

02 Avaliar riscos e identificar vulnerabilidades.

03 Desenvolver mitigações e alternativas de resiliência.

04 Adotar os 4 R's: Redundância, Resistência, Resposta e Recuperação.

05 Desenvolver portfólio de mitigação, respostas e recuperação.

06 Implementar e mensurar, por meio de relatórios pós-ação, métricas e indicadores-chave de desempenho (*Key Performance Indicators* – KPI's).

10

Ativos e força de trabalho envelhecem

Em um setor com muitos ativos, a substituição e a manutenção com boa relação custo-benefício são fatores constantes.

Sem as pessoas e habilidades certas, as redes de energia e serviços públicos entram em crise. Por isso, é vital atrair novos talentos para o setor e transmitir as décadas de experiência das gerações mais velhas.

É necessário ainda falar sobre a criação de uma estrutura e cultura de resiliência. No Reino Unido, foi criada uma Estratégia Nacional de Resiliência, que tem como atribuições lidar com clima extremo, terrorismo, pandemias, ataques cibernéticos, instabilidade geopolítica e acidentes.

Ou seja, à medida que se esforçam para construir organizações seguras e robustas que possam fornecer serviços ininterruptos, as empresas de energia e serviços públicos estão tratando a resiliência como um imperativo estratégico.

11

Conclusão

Os países que estão em estágio inicial de transição energética enfrentam escolhas difíceis, pois têm menos alternativas aos combustíveis fósseis e não querem arriscar apagões ou interrupções nas indústrias. No mundo inteiro, o cenário é semelhante: riscos ambientais e geopolíticos se somam à crise na cadeia de suprimentos – mais um dos problemas herdados da pandemia –, à escassez de recursos e de talentos, ao envelhecimento de ativos e aos desafios da crescente digitalização.

As empresas não podem perder tempo. É imperativo delinear suas estratégias de sobrevivência e, mais do que isso, de crescimento e de disrupção.

Isso envolve mapear riscos, monitorar eventos e planejar cenários que levem em consideração o maior número possível de variáveis – desde os resultados de eleições nacionais até a eclosão de novos conflitos bélicos. Construir uma cultura de resiliência é, basicamente, optar por se manter relevante e adequar-se ao novo mundo que se delineia.

Fale com o nosso time

Anderson Dutra
Sócio-líder de ENR
da KPMG no Brasil
adutra@kpmg.com.br

kpmg.com.br

/kpmgbrasil