A evolução do setor elétrico diante das ameaças cibernéticas nos ambientes de missão crítica

pwc

Introdução

Poucas indústrias começaram 2020 com tão boas perspectivas como a de energia, com oportunidades consistentes para crescimento de investimentos nacionais e internacionais, especialmente relacionados às fontes de energias renováveis, como solar, eólica e biomassa. Em nosso estudo global *Digital Trust Insights 2020*,[1] 15% dos respondentes de empresas do setor no mundo esperavam um aumento de receita em 2020, mesmo com os impactos causados pela pandemia de Covid-19.

Apesar de o setor já ter superado diversas crises e contar com estrutura institucional e empresas robustas que asseguraram a prestação do serviço essencial durante a pandemia, o choque profundo na demanda impactou toda a cadeia. O segmento, no entanto, se reinventou rapidamente. Desde o início do isolamento, as concessionárias adotaram o trabalho remoto para a equipe de atendimento ao cliente, aperfeiçoaram os serviços por meio de novos canais digitais, aceleraram suas capacitações de *data analytics* e direcionaram esforços na geração de ganhos com a melhoria dos índices de qualidade, redução de custos e otimização da cadeia de suprimentos.

Em poucas semanas, foram anos de avanços na digitalização do atendimento. Um caminho sem volta para as empresas, mas que precisa ser acompanhado por um plano de segurança cibernética ágil e estruturado.

[1] PwC. Disponível em: https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/pwc-covid-19-ciso-pulse-survey.html. Acesso em: 7/1/2021

O setor elétrico no Brasil e sua cadeia produtiva

A cadeia produtiva do setor elétrico é dividida em três segmentos:

Transmissão

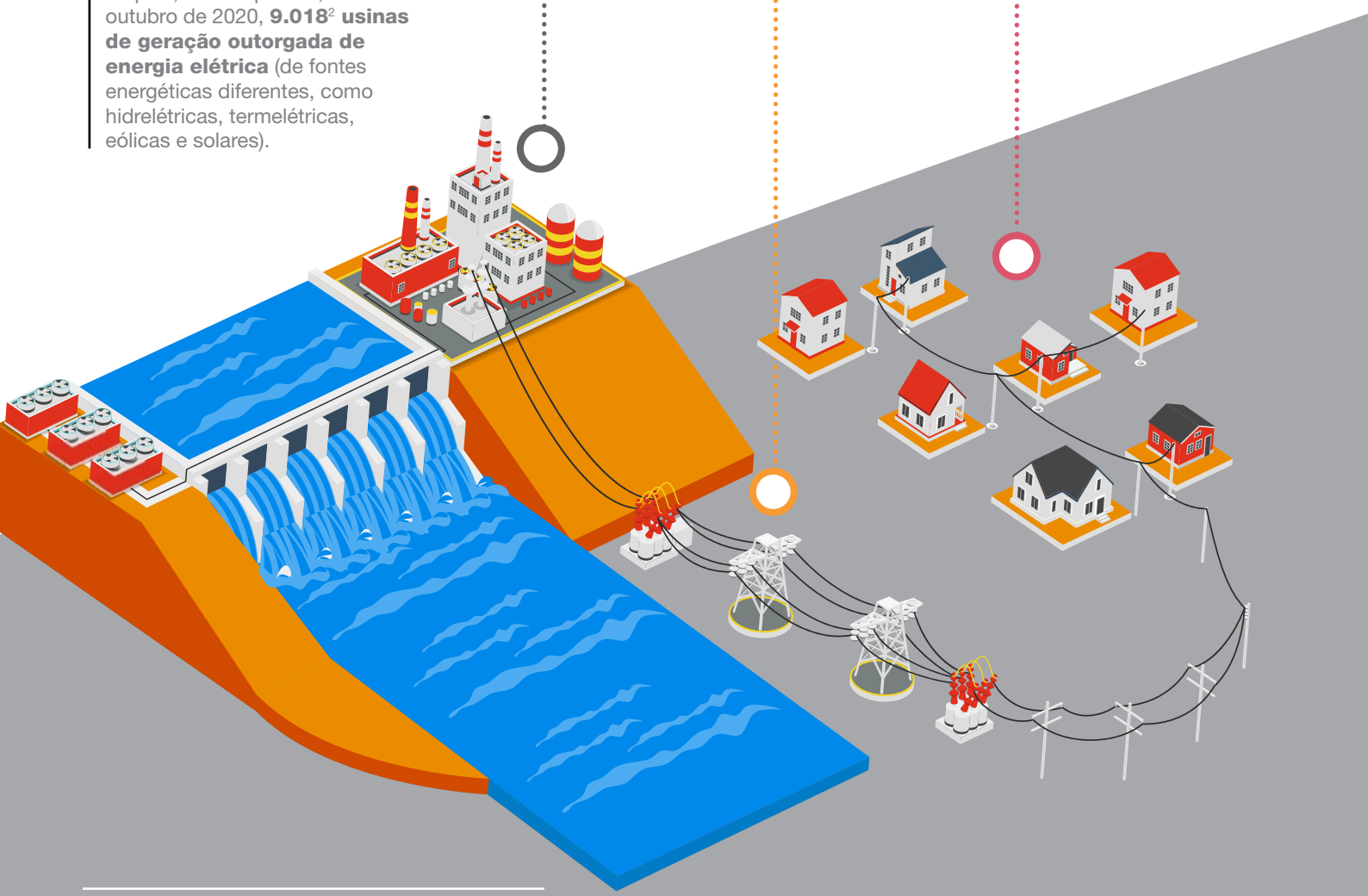
Encarrega-se de transportar energia proveniente das usinas geradoras até as distribuidoras. No Brasil, esse segmento contava com **157 agentes e 251 concessões em dezembro de 2020.**[3]

Distribuição

Fornece a energia aos consumidores finais. Contemplava em janeiro de 2021 **105 agentes no Brasil, sendo 52 concessionárias, 52 permissionárias e 1 autorizada.**[4]

Geração

Responsável por produzir energia elétrica e inseri-la no SIN (Sistema Interligado Nacional). O segmento de geração é bastante pulverizado no país, contemplando, em outubro de 2020, **9.018**[2] **usinas de geração outorgada de energia elétrica** (de fontes energéticas diferentes, como hidrelétricas, termelétricas, eólicas e solares).



[2] http://antigo.mme.gov.br/documents/239673/1059011/10.Boletim+de+Monitoramento+do+Sistema+El%C3%A9trico+-+Out+-2020.pdf/75838dd3-5c59-7258-320c-ef4f70533adf
[3] http://www.ons.org.br/AcervoDigitalDocumentosEPublicacoes/SEAMSE_202012.pdf
[4] https://www.aneel.gov.br/distribuicao2

Os desafios do setor elétrico em cibersegurança

Cada grande revolução industrial trouxe uma ampla gama de novas tecnologias, transformando fundamentalmente a sociedade e a natureza do trabalho. Mas a quarta revolução, que a sociedade vive agora, evidencia o intenso uso de dados por meio de tecnologias como inteligência artificial (IA), robótica, *machine learning* e Internet das Coisas (IoT), entre outras, que alavancam a utilização de *big data*, migrando as atividades presenciais para o mundo digital.

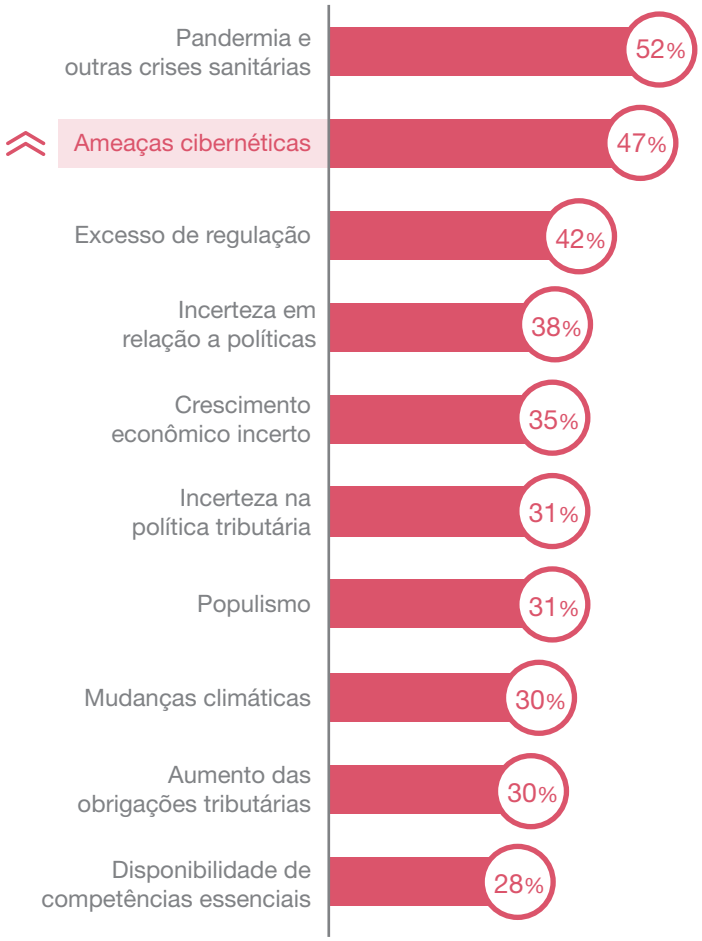
Essas tecnologias permitiram avanços no ambiente de automação, como a possibilidade de operar grandes instalações, plantas e subestações de forma remota e centralizada, mas também aumentaram drasticamente a exposição das empresas a ameaças e os riscos de segurança cibernética.

Na *24ª CEO Survey* da PwC, publicada em março de 2021, 47% dos executivos entrevistados no mundo em todos os setores classificaram as ameaças cibernéticas como o segundo maior risco ao crescimento das empresas. No ano anterior, o percentual foi de 33%.

Incidentes de segurança cibernética de média ou grande proporção fazem parte da realidade das empresas em todos os setores. No entanto, observamos um aumento de incidentes de segurança no setor elétrico, o que pode causar grande impacto para a sociedade – devido às características dos serviços prestados –, gerar multas regulatórias e prejudicar significativamente a reputação das empresas, em virtude de possíveis paralisações parciais ou totais dos serviços.

10 principais ameaças de 2020

10 principais ameaças de 2021



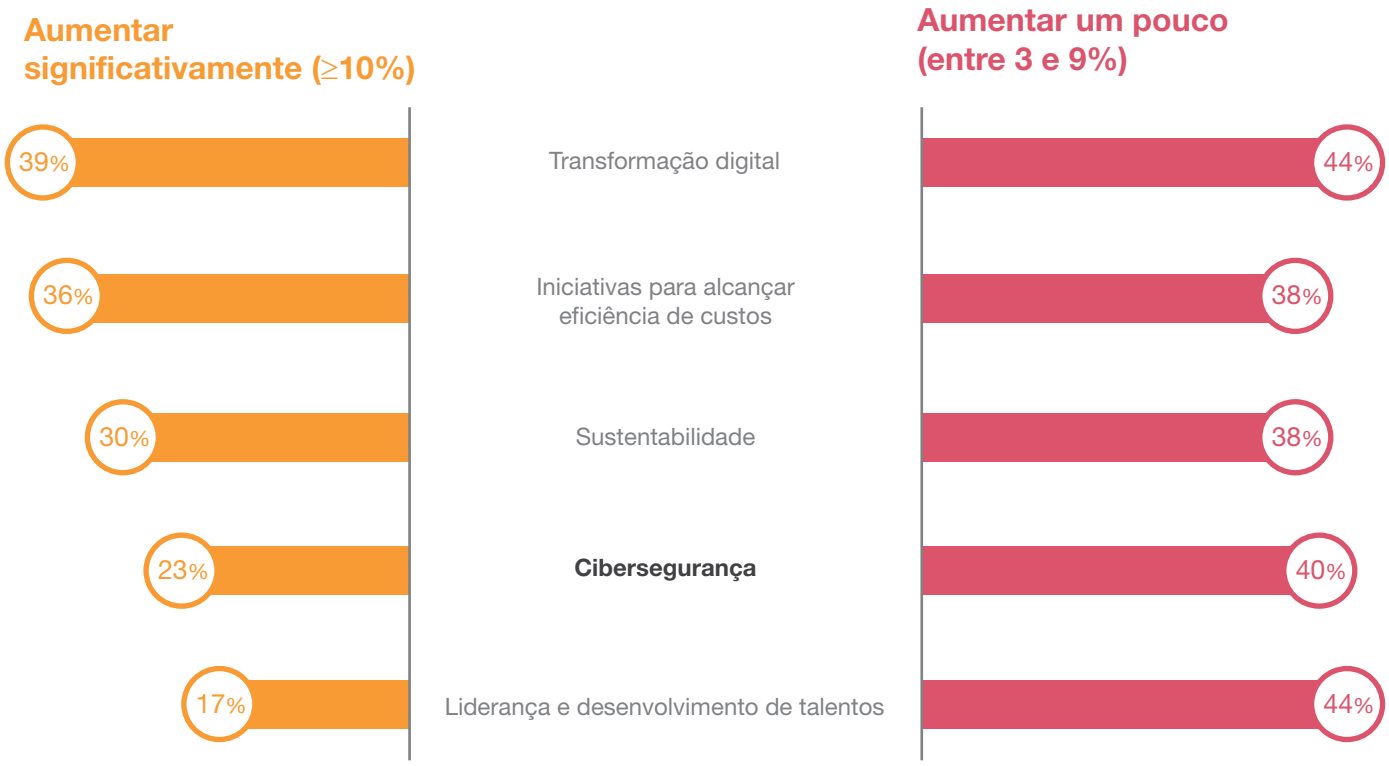
Fonte: *24ª CEO Survey*, PwC.

O ambiente de automação está sendo cada vez mais digitizado com o objetivo de reduzir custos e aumentar a eficiência operacional. As violações cibernéticas que visam especificamente esse ambiente estão em ascensão, com foco em protocolos proprietários e sistemas operacionais comuns, como Windows e Linux, nos quais são executados muitos sistemas SCADA (de supervisão e aquisição de dados).

Globalmente, o setor elétrico já foi vítima de grandes ataques cibernéticos que resultaram na queda das operações. Segundo o estudo *Digital Trust Insights,* 58% das empresas de energia e serviços públicos acreditavam que os serviços de nuvem sofreriam tentativas de ataques cibernéticos nos 12 meses seguintes à pesquisa, enquanto 57% temiam violações por *ransomware* — programa que bloqueia o acesso a dados e arquivos dos computadores.

Diante dessas ameaças, empresas de energia em todo mundo têm investido cada vez mais na segurança digital. Ainda segundo a pesquisa, 58% das empresas do setor pretendem aumentar o orçamento de cibersegurança em 2021 e investir em soluções com capacidade de identificar e evitar incidentes de *ransomware.*

O gráfico abaixo mostra a intenção de investimento das empresas do setor de Energia em todo mundo nos próximos 3 anos em consequência da crise da Covid-19.



Fonte: *24ª CEO Survey*, PwC.

Os governos também estão atentos à vulnerabilidade digital de serviços essenciais, como os de energia e serviços públicos. Os Estados Unidos são, hoje, o país mais regulamentado — com investimentos em segurança cibernética passando dos US$ 17 bilhões, segundo dados divulgados pela Casa Branca no final de 2020. Cabe à Agência de Cibersegurança e Infraestrutura determinar as regras mínimas e os *frameworks* que devem ser adotados por todo o setor. Na Europa, também existe um movimento avançado em defesa de uma regulamentação. A Agência da União Europeia para a Cibersegurança (Enisa) é a referência para segurança cibernética na comunidade.

No Brasil, ainda não há uma regulamentação específica sobre segurança cibernética para as infraestruturas do setor elétrico. O Operador Nacional do Sistema Elétrico (ONS), órgão que coordena e controla a operação das usinas de geração e das linhas de transmissão de energia elétrica no país, submeteu à Agência Nacional de Energia Elétrica (Aneel), em dezembro de 2019, uma proposta de procedimento de rede com critérios e requisitos mínimos para a operação segura do Sistema Interligado Nacional (SIN). Em maio de 2020, a Aneel abriu uma consulta pública visando obter contribuições para essa regulamentação na atividade nº 103 da Agenda Regulatória 2020/2021.

O que propõe o ONS

Todos os agentes puderam contribuir para a proposta do ONS, que visa estabelecer controles de segurança cibernética mínimos a serem implementados pelos agentes e pelo órgão, por instalações da rede de operação, centros de operação dos agentes e instalações da rede de supervisão diretamente conectadas ao ONS. Esses requisitos podem servir de referência também para todos os ambientes de missão crítica do setor elétrico brasileiro, ou seja, aqueles indispensáveis para o funcionamento dos serviços.

A PwC apoiou ativamente o ONS nessa iniciativa de proposição do novo procedimento de rede, com sua experiência em projetos de segurança cibernética no setor elétrico, domínio de *frameworks* e melhores práticas aplicáveis de segurança cibernética, além de *benchmark* de diretrizes de segurança cibernética reguladas em outros países da América Latina e ao redor do mundo.

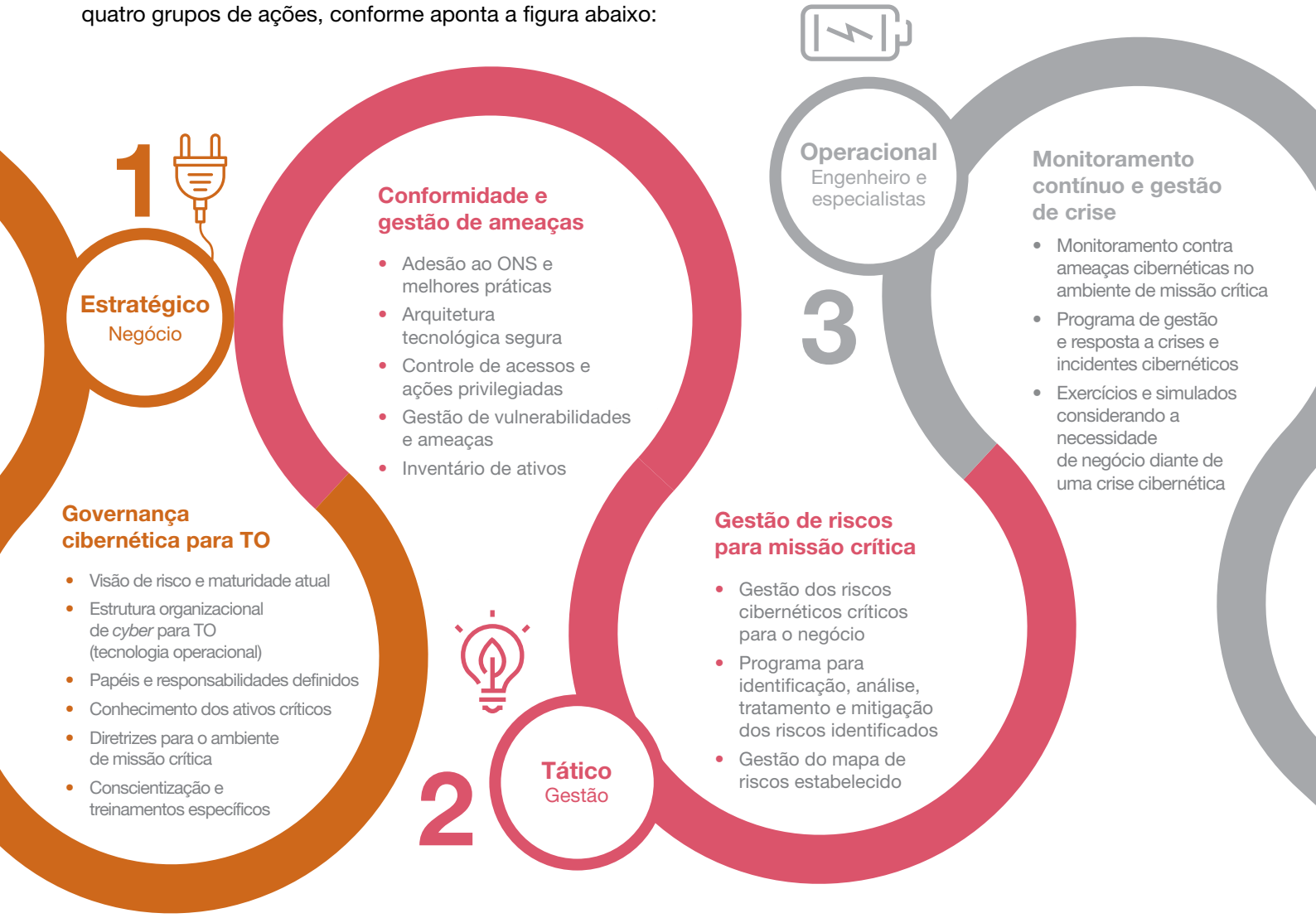
O procedimento de rede sugerido compreende requisitos para os principais domínios de segurança: arquitetura, gestão de acesso e de vulnerabilidades, inventário de ativos e resposta a incidentes cibernéticos.

Uma jornada para transformação do ambiente de missão crítica no setor elétrico

Para melhor detectar e responder a ataques cibernéticos, além de se preparar para as futuras obrigações regulatórias, empresas do setor elétrico devem se comprometer com o financiamento, desenvolvimento e melhoria de um programa proativo de segurança cibernética.

Essa jornada de transformação envolve considerações que vão além do monitoramento e do plano de resposta a incidentes e levam à criação de programas capazes de garantir uma conformidade sustentável e alinhamento estratégico com o negócio.

O processo de transformação para uma empresa segura no âmbito digital passa por três dimensões de análise e quatro grupos de ações, conforme aponta a figura abaixo:



Estratégico

Neste primeiro estágio de análise, é preciso entender a dimensão da sua estrutura atual de segurança e o quanto ela está alinhada ao plano de negócio da empresa. Aborda temas como visão de risco e estrutura organizacional de *cyber*, com a definição de papéis e responsabilidades. Com base nessa reflexão, é possível dar o primeiro passo na jornada de transformação, com o desenho de uma plano de governança cibernética para os ambientes de missão crítica.

Empresas de energia bem-sucedidas em sua governança não deixam dúvidas em relação a quem é responsável pela segurança cibernética. E, embora os programas de segurança cibernética sejam normalmente executados por um diretor de informações, CISO ou diretor de segurança, a liderança executiva da empresa precisa estar comprometida com o plano como um imperativo de negócios e buscando sinergia de proteção e controle cibernético entre as áreas de TO e TI.

Tático

Esta dimensão engloba de forma estruturada as ações que serão executadas e monitoradas para alavancar a estratégia definida no início da jornada. Ela leva em conta temas como gestão de ameaças e riscos para missão crítica, buscando alinhamento com as regulamentações e melhores práticas do setor.

Operacional

A análise operacional aponta o nível do monitoramento de ameaças e gestão dos riscos da empresa. Um bom monitoramento, em tempo real, consegue medir a frequência e o perigo de ameaças emergentes para construir uma base de inteligência (*threat intelligence*) e assim poder fazer uma avaliação precisa do risco cibernético e da realidade da empresa. Antecipar as ameaças por meio de processos MDR (*Managed Detect and Response*) bem estabelecidos permite um gerenciamento proativo dos incidentes e uma gestão efetiva do plano de resposta antes da materialização dos incidentes cibernéticos.

Considerações finais

As empresas do setor de energia estão desenvolvendo seus modelos de negócio baseados em tecnologias, buscando aprimorar os controles de segurança cibernética em seus ambientes de missão crítica de forma alinhada aos objetivos de negócio e à estratégia organizacional.

Com a evolução dos incidentes cibernéticos no setor e potenciais impactos para a operação e a prestação de serviços, muitas empresas ainda demonstram ter dificuldade em lidar com ameaças cada vez mais sofisticadas, que demandam novos modelos de resposta.

Regulamentações locais devem surgir para definir requisitos gerais para evolução da maturidade de segurança cibernética na indústria, ampliando a necessidade de preparação das empresas para adequações de segurança e evolução da capacidade de resposta aos incidentes.

Um bom programa de segurança cibernética, estruturado nas três dimensões de análises e alinhado aos objetivos do negócio, pode alavancar as capacidades de identificação, preparação e resiliência das organizações contra as ameaças cibernéticas no ambiente de missão crítica, bem como atender às novas regulamentações no setor.

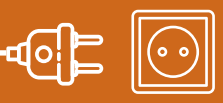
Contatos

Ronaldo Valiño
Sócio e líder da Indústria de Energia
ronaldo.valino@pwc.com

Eduardo Batista
Sócio e líder de *Cyber Security* no Brasil
eduardo.batista@pwc.com

Magnus Santos
Sócio de *Cyber Security* para a Indústria de Energia
magnus.santos@pwc.com

Larissa Escobar
Diretora de *Cyber Security* para a Indústria de Energia
larissa.escobar@pwc.com



Colaborou com esta produção:
Fábio Leandro.

Centro Avançado para Operações de Segurança Cibernética da PwC Brasil

Para abordar os desafios do setor e a constante exposição aos riscos cibernéticos que as organizações enfrentam, a PwC Brasil tem um Centro Avançado para Operações de Segurança Cibernética, que presta serviços para os ambientes de TI e TO, apoiado por capacidades de gestão de ameaças e vulnerabilidades e resposta a incidentes. Esse centro mantém alianças estratégicas e intercâmbio de inteligência com outros centros do Network PwC que fazem monitoramento de missão crítica no setor elétrico em Israel, Canadá e Estados Unidos.

Traga desafios. Leve confiança.
www.pwc.com.br

PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil PwC Brasil @PwCBrasil

pwc