*Por Rodrigo Leal de Siqueira**

NOVO

Capítulo I

A digitalização: o sistema elétrico está seguro?

Atualmente estamos vivenciando um dos momentos mais fascinantes e singular da história da humanidade. Neste exato momento em que está lendo este artigo, um novo mundo está sendo construído a partir dos ciclos de inovação cada vez mais curtos. As mudanças estão cada vez mais rápidas e em alguns setores disruptivos, de modo que o que é moderno hoje amanhã pode estar obsoleto. A velocidade, a amplitude e o impacto com que essas mudanças estão ocorrendo estão modificando os nossos comportamentos, o nosso trabalho e nossas vidas.

Somos testemunhas de toda evolução e mudanças em todos os setores, com surgimento de novos modelos de negócio e transformação de cadeias inteiras. Alguns modelos de negócio que pareciam sólidos e estabelecidos são ultrapassados em velocidade exponencial.

A pandemia nos mostra, claramente, que a tecnologia está cada vez mais presente em nossas vidas, transformando nosso modo de vida e nosso modo de trabalho, trazendo benefícios enormes em vários segmentos, inclusive no setor elétrico.

Esse momento revolucionário que estamos vivendo está levando a mudanças de paradigmas, sem precedentes, na economia, nos negócios, na sociedade em geral. O setor elétrico no Brasil e no mundo está passando por grandes mudanças e trazendo enormes desafios para as empresas e agências do setor. Com a ruptura do modelo tradicional provocada pela necessidade de avanço tecnológico no setor, o processo de digitalização tomou forma trazendo consigo novas tecnologias e soluções visando atender as nossas dores.

A digitalização está mudando a forma como vivemos, trabalhamos e nos relacionamos e não poderia ser diferente quando falamos sobre o setor de energia, nas áreas de geração, transmissão e distribuição.

A digitalização, assim como a descentralização e a descarbonização, está interligada com a transição energética, que é um conceito amplo. É um processo que consiste em uma mudança na matriz energética com foco nas fontes de energia renováveis e estando atreladas a modificações significativas na forma de produzir, distribuir e consumir energia, trazendo novidades em relação a tecnologias de conversão, modelos de negócios, segmentos industriais e relações internacionais.

Hoje a transformação do setor elétrico está centrada nestes pilares conhecidos como os 3Ds da transição energética.

A digitalização é a base para o desenvolvimento dos outros dois pilares, pois através das novas tecnologias estamos conseguindo conectar e capilarizar o sistema elétrico. Embora não seja um processo específico do setor de energia, é a espinha dorsal da Indústria 4.0 (IoT, big data, machine learning), responsável também por contribuir com soluções para o setor elétrico.

O processo de digitalização de instalações do setor elétrico é cada vez mais relevante e é uma tendência irreversível, uma vez que traz ganhos em qualidade e desempenho. No cenário atual, os dados e a informação que eles fornecem são considerados o "novo petróleo".

Hoje, no Brasil, estamos enfrentando grandes desafios no setor que podem ser transformados em oportunidades por meio da utilização inteligente de grandes quantidades de dados que as novas tecnologias nos disponibilizam, permitindo assim maior controle, planejamento e redução dos custos com maior eficiência.

Um exemplo é a evolução dos dispositivos inteligentes e sua penetração no setor industrial e de missão crítica.

Na transmissão, por exemplo, de acordo com a Associação Brasileira das Empresas de Transmissão de Energia Elétrica (Abrate), dezenas de milhares de equipamentos deverão ser trocados até 2023 pelo fim da vida útil regulatória. Com a adoção de dispositivos inteligentes nas redes e subestações de transmissão, podemos aumentar sensivelmente a vida útil dos equipamentos instalados. A revolução digital não deixa de fora o segmento de distribuição de energia que sofre constantemente com perdas técnicas e não técnicas.

Com as tecnologias apresentadas pela Indústria 4.0 é possível também fazermos a gestão da saúde dos ativos de forma mais preditiva, minimizando os custos, possibilitando ganhos de eficiência, melhoria na prestação do serviço, maior disponibilidade operacional e menor tempo de resposta para solicitações de clientes e demandas do mercado.

Em suma, essa é uma viagem sem volta, a digitalização está mudando o mundo como o conhecemos. Neste ambiente de mudanças revolucionárias, nos cabe monitorar os riscos e oportunidades, investindo em novas soluções e demandas.

Hoje, bilhões de dispositivos (sensores, câmeras, smartphones, TV, geladeira, veículos, etc.) estão conectados, aumentando a superfície de contato, ou seja, o perímetro, ocasionando um aumento da exposição diária a ataques cibernéticos maliciosos, colocando nossas vidas e a estabilidade da nossa sociedade em risco. Segundo estudos, a expectativa é que até 2025 existam 60 bilhões de dispositivos conectados, para uma população abaixo de 8 bilhões.

Neste contexto, a segurança cibernética tem se tornado um tema cada mais relevante na sociedade em geral.

Segurança cibernética tem se tornado assunto frequente no setor elétrico ao longo dos últimos anos, pois no Brasil e no mundo temos usinas e subestações interligadas em grandes infraestruturas

de telecomunicação e tudo isso pode ser acessado remotamente. Contribuiu para que o tema ganhasse relevância durante a pandemia o fato de que grande parte da força de trabalho das empresas que geram, transmitem e distribuem energia foi obrigada, em um curto espaço de tempo, a trabalhar de maneira remota. Empresas tiveram que se adaptar rapidamente e uma elevada conectividade nessas empresas foi necessária para manter o sistema elétrico brasileiro em operação e, ao mesmo tempo, garantir a saúde e segurança das pessoas. Esse cenário contribuiu para a explosão de incidentes cibernéticos.

De forma geral constata-se um aumento de ataques em todo o mundo e o Brasil foi o quinto país que mais sofreu ataques cibernéticos no ano passado. O ano de 2021 foi de consolidação das ameaças em relação a ataques cibernéticos, que nunca foram tão frequentes, impactantes e sofisticados. Houve vazamento de informações sigilosas, sequestro de dados, invasões de sistemas e muito dinheiro perdido. As interrupções afetam a produtividade, a receita e a segurança física e 9 a cada 10 organizações do setor industrial sofreram pelo menos uma intrusão no ano passado e 63% tiveram três ou mais invasões, o que é semelhante aos resultados em 2020.

No setor elétrico, na rede de geração, transmissão e distribuição, os ataques também vêm crescendo, principalmente a partir de 2015 com o ataque à Ucrânia, ocasionando um "apagão elétrico", atingindo 30 subestações e em torno de 230 mil pessoas por um período de seis horas, causado por um vírus de computador e se tornou o primeiro caso registrado dessa natureza.

Nos últimos dois anos tivemos vários casos de ataques cibernéticos no setor elétrico no Brasil, como os ocorridos com CPFL, Enel, Energisa, EDP, Light, Copel e Eletronuclear, todos veiculados na mídia.

O tema vem ganhando tanta relevância no setor elétrico, que faz parte da agenda regulatória da Agência Nacional de Energia Elétrica (Aneel) e do Operador Nacional do Sistema Elétrico (ONS).

Em um webinar realizado pelo Cigre-Brasil no ano passado, do qual fui o anfitrião, o diretor da Aneel, Sandoval Feitosa, abriu o webinar levantando a questão de a segurança cibernética ser uma temática que vem ganhando interesse em diversos setores de infraestrutura com abrangência nacional e internacional. No setor elétrico, o aumento da conectividade entre sistemas, além de propiciar a ampliação de incidentes sofridos pelas organizações, também contribui para a sofisticação dos ataques promovidos por cibercriminosos. Nessa conjuntura, ele apresentou que a Agência vem desenvolvendo proposta de atuação regulatória sobre segurança cibernética do Setor Elétrico Brasileiro (SEB), tendo como objetivo a definição do problema regulatório até a escolha da melhor alternativa de ação regulatória.

A atuação regulatória da agência trouxe no final do ano passado como resultado a emissão da Resolução Normativa Aneel Nº 964, de 14 de dezembro de 2021, que dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica.

A existência de uma regulamentação nacional para o setor elétrico é base para que um país tenha infraestruturas críticas de energia menos expostas e vulneráveis, garantindo a segurança nacional e capacidade de reação em caso de incidentes.

Pelo ONS, até o momento existia um item nos Procedimentos de Rede que tratava do assunto, mas de forma abrangente. Após receber contribuições dos agentes, o Operador Nacional do Sistema Elétrico divulgou, em 1º de julho de 2021, a Rotina Operacional RO-CB.BR.01 - Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético. O documento, que estabelece os controles de segurança cibernética a serem implementados nos centros de operação dos agentes e nos equipamentos de infraestrutura, está em vigor desde 9 de julho de 2021. Desde então, os agentes e o Operador devem adotar a rotina e o seu conjunto de requisitos e critérios, de acordo com os prazos estabelecidos.

A publicação dessa rotina aprimora as orientações sobre o tema junto aos agentes, elevando o nível de segurança cibernética de toda a operação. A rotina operacional é focada na arquitetura, governança, inventário, gestão da vulnerabilidade, gestão de acessos e monitoramento e resposta a incidentes, conforme detalhado a seguir:

Fonte: ONS

Segurança cibernética deve ser analisada como um investimento. Um espaço cibernético seguro é um ambiente que evita indisponibilidade e permite ganhos operacionais por meio de tecnologias que viabilizam a operação remota segura e a coleta de dados que, combinados com soluções de inteligência artificial, ajudam na redução de custos com operação e manutenção. Ainda, novas

TRANSFORMANDO ENERGIA EM DESENVOLVIMENTO.

Imagens ilustrativas.

trael.com.br

Indústria e Assistência Técnica
Cuiabá-MT • Brasil
[65] 3611-6500

TRAEL TRANSFORMADORES ELÉTRICOS

ISO 9001

ISO 14001

CERTIFICADA PELA ISO 9001 E ISO 14001
DNV·GL
OCS 0010
OCA 0003

tecnologias que podem ser habilitadas por um espaço cibernético seguro apoiam no aprimoramento dos índices de qualidade dos serviços prestados à sociedade no que tange à geração, transmissão e distribuição de energia elétrica.

A segurança cibernética deve ser considerada como um processo de melhoria contínua ao longo do tempo, e três pilares devem ser considerados para o sucesso do investimento neste segmento. O pilar da tecnologia é, provavelmente, o que a maioria das pessoas pensa quando tratamos deste tema, no entanto, temos o pilar dos processos e o pilar das pessoas, que é o elo mais fraco.

Assim, é fundamental aplicar os recursos disponíveis na empresa em mudança de processos, com apoio da tecnologia, e com sensibilização e capacitação das pessoas.

Com relação às pessoas observa-se que profissionais ligados, em sua maioria, com trabalho com dados, cibersegurança e sistemas estão entre os 10 mais demandados, conforme pesquisa realizada pelo "LinkedIn Economic Graph", que analisou dados de empregos iniciados entre 2017 e 2021 e estão em alta em 2022.

Considerando que o ciberespaço é a nova arena de batalha e, finalizando este artigo, fica a pergunta para reflexão: a próxima pandemia será a Guerra Cibernética?

Sabemos que não existe "bala de prata" para tratar do tema de segurança cibernética e, por isso, pede uma abordagem holística e investimentos com o objetivo de proteger o perímetro das ameaças e mitigar a exposição ao risco.

Este é o primeiro capítulo de uma série sobre segurança cibernética, que iniciamos nesta edição e se estenderá ao longo do ano. Os oito capítulos deste fascículo abordarão diversos tópicos, entre os quais, destacam-se:

- Visão regulatória;
- O estado da arte;
- Arquitetura de rede eficiente;
- Gestão de riscos e vulnerabilidades;
- Gestão de processos;
- Conscientização e capacitação;
- Protegendo da ameaça;
- Segurança corporativa;
- Segurança operativa;
- Plano de resposta a incidentes;
- Centros de operação de segurança;
- O futuro.

Estamos selecionando líderes e especialistas para fazer parte da equipe que comporá os demais fascículos. Caso você se interesse será um prazer conversarmos. Entre em contato comigo pelo e-mail rodrigol@chesf.gov.br ou pelo LinkedIn www.linkedin.com/in/rodrigolealdesiqueira.

**Rodrigo Leal é graduado e mestre em engenharia elétrica. Possui MBA em Gestão de Projetos pela Fundação Getúlio Vargas (FGV) e curso de Gestão de Negócios da Era Digital pela Cesar School. Atualmente cursa MBA Executivo de Negócios do Setor Elétrico pela FGV. Desde 2006 atua na Chesf, tendo passado pelos cargos de Gerente do Departamento de Telecomunicações, Assessor da Superintendência de Telecomunicações, Proteção e Automação e atualmente como assessor do Diretor de Operação, coordenando vários processos da diretoria, incluindo os assuntos relativos à tecnologia operativa. Ocupa ainda a posição de Vice-Presidente do Conselho Diretor da UTC América Latina e Coordenador do Comitê de Tecnologia da Informação e Telecomunicações no Cigre-Brasil.*