Título	**Segurança cibernética como prioridade no setor elétrico**
Veículo	**Revista Brasil Energia**
Data	**05 de Abril de 2021**
Autores	**Claudio J. D. Sales e Eduardo Müller Monteiro**

Claudio Sales

Claudio Sales é engenheiro e presidente do Instituto Acende Brasil. Escreve na Brasil Energia a cada dois meses.
Eduardo Müller Monteiro, coautor deste artigo, Diretor Executivo da entidade.

SEGURANÇA CIBERNÉTICA COMO PRIORIDADE NO SETOR ELÉTRICO

Com o avanço do uso de sistemas digitais na automação da rede elétrica, as infraestruturas estão cada vez mais interligadas, e o aumento de acesso e de comunicação entre dispositivos posicionam os sistemas operados por geradores, transmissores e distribuidores de eletricidade como alvos de malware e hackers, aumentando a vulnerabilidade a ataques e acessos às informações e operações de dispositivos.

Uma vez reconhecida a importância da segurança cibernética no setor elétrico, é necessário melhorar o ambiente regulatório, evitando a criação de processos burocráticos e custos ineficientes atrelados a tais burocracias.

É necessário incentivar a construção de mecanismos regulatórios que – sempre tendo em mente a minimização de impactos tarifários – reduzam o risco e promovam maior proteção das infraestruturas críticas do setor elétrico contra ataques cibernéticos. Além disso, a regulação deve levar em conta que investimentos para aumento dos padrões de segurança implicam custos que poderão impactar o equilíbrio econômico-financeiro das empresas.

A fim de ser uma solução e não um problema adicional, a regulação da segurança cibernética no setor elétrico deveria, sempre que possível, ser orientativa – e não prescritiva – e, portanto, caminhar tanto para promover o desenvolvimento de procedimentos de mitigação de riscos quanto para definir parâmetros de compatibilidade a serem atendidos pelas empresas de energia elétrica.

Assim, a adoção de certificações, de melhores práticas e de requisitos mínimos de segurança deve ser incentivada. No entanto, tais certificações não devem implicar transferência de responsabilidade, mas estabelecer mecanismos para melhorar a articulação entre os representantes das infraestruturas críticas.

Além disso, caso eventualmente sejam concebidos comandos prescritivos, os mesmos devem ser acompanhados de previsão de cobertura tarifária, com a adoção de novos padrões anunciada com antecedência, para possibilitar a sua implementação planejada e eficiente nos ritos regulatório-tarifários.

Tal regulamentação poderá ser discutida e implementada com base em "objetivos" e "fins", evitando amarras e reconhecendo a necessidade de adaptações flexíveis pelos próprios agentes ao longo dos estágios iniciais que, provavelmente, serão marcados por intenso aprendizado, que precisará ser compartilhado.

Por ser tema de fronteira do conhecimento, a segurança cibernética exigirá novos tipos de profissionais, e será essencial o tratamento regulatório adequado para abordar a capacitação de pessoas em segurança cibernética, tanto nos seus aspectos tecnológicos quanto nos de gestão e governança.

O potencial de mudança no setor elétrico decorrente da inserção de tecnologias digitais e a necessidade de acompanhamento dos impactos da digitalização no setor já havia sido originalmente abordado no Capítulo IV.7 do Plano Nacional de Energia 2050 (PNE 2050), mas o Ministério de Minas e Energia (MME) acabou acolhendo nossa contribuição na revisão final do PNE 2050 e incluiu o item "Desenvolver mecanismos regulatórios para desenvolvimento e inclusão de sistemas de proteção a ataques cibernéticos", mantendo inclusive a necessidade de equilíbrio entre, de um lado, das ações de "ampliação dos padrões de segurança da operação e manutenção de dados" e, de outro, da "preservação do equilíbrio econômico-financeiro das empresas e impacto tarifário para os consumidores".

A emergência das redes 5G multiplicará as probabilidades de ataque cibernético contra as infraestruturas críticas do setor elétrico, e o MME, a Aneel e o próprio Operador Nacional do Sistema Elétrico (ONS) acertam em colocar medidas de segurança cibernética nas suas listas de prioridades.