Contribuições do Instituto Acende Brasil à Tomada de Subsídio Aneel 007/2020

AVALIAÇÃO DA NECESSIDADE DE INTERVENÇÃO REGULATÓRIA PARA A SEGURANÇA CIBERNÉTICA DO SISTEMA ELÉTRICO BRASILEIRO

24/JUL/2020

TOMADAS DE SUBSÍDIOS ANEEL 007/2020

"Avaliação da necessidade de intervenção regulatória para a segurança cibernética do Sistema Elétrico Brasileiro".

QUESTÕES:

4. Qual a abordagem mais adequada de eventual regulação (prescritiva, orientativa, voltada para autorregulação do mercado, entre outras) para que os objetivos de segurança cibernética sejam plenamente alcançados? Por quê?

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 tornam os sistemas um alvo de *malware* e *hackers*, aumentando a vulnerabilidade a ataques e acessos às informações e operações de dispositivos do sistema.

Assim, é necessário incentivar a construção de mecanismos regulatórios que – sempre tendo em mente a minimização de impactos tarifários – mitiguem o risco e promovam maior proteção das infraestruturas críticas do setor elétrico contra ataques cibernéticos.

Nos Estados Unidos, a adoção do NERC-CIP (*North American Reliability Corporation – Critical Infrastructure Protection)* estabelece que instalações no setor elétrico devem possuir projeto e equipamentos de acordo com este padrão.

A adoção de medidas para segurança cibernética deve passar por discussões e análises sobre os riscos ao setor elétrico adotando-se as seguintes abordagens regulatórias:

a) prescritiva, para garantir um padrão mínimo a ser seguido e maior segurança no médio e longo prazo; e

b) orientativa, para apontar uma direção a ser seguida e permitir mais flexibilidade aos agentes.

Em relação à abordagem prescritiva, a aplicação de padrões como ISA/IEC 62443, ISO 27000 e NERC-CIP aos segmentos de geração, transmissão e distribuição de energia elétrica poderá garantir níveis de uniformidade e padronização, respeitando as devidas particularidades. A definição de padrões mínimos uniformes é importante para assegurar concorrência isonômica nos Leilões de Transmissão e de Energia e para garantir compatibilidade mínima entre as instalações do Sistema Interligado Nacional. Entretanto, o que é "prescritivo" deve ser mínimo para evitar engessamento do setor.

Já a abordagem orientativa permite mais flexibilidade quanto às formas específicas encontradas pelos agentes para proteção contra ataques cibernéticos. É importante incentivar a inovação e desenvolvimento tecnológico e assegurar que haja concorrência entre os agentes para que o processo seja eficiente.

Pensando na evolução futura da segurança cibernética, cabe à Aneel promover discussões e atuar como um facilitador para identificar consensos quanto à direção de inovações e de padrões futuros.

Isto pode ajudar fornecedores e agentes do setor no planejamento e desenvolvimento de novas soluções.

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. Portanto, o que for prescritivo deve dispor de previsão de cobertura tarifária. Isto implica que a adoção de novos padrões deve ser anunciada com a antecedência para possibilitar a sua implementação de forma planejada e eficiente nos ritos regulatório-tarifários.

Assim, se a adoção de novos padrões de segurança cibernética exigir grandes aportes de investimentos, eventuais acomodações tarifárias podem ser necessárias. No caso da distribuição, tais custos tendem a ser incorporados nas revisões tarifárias periódicas por meio de ajustes na Base de Remuneração Regulatória ou na Base de Anuidade Regulatória (Módulo 2.3 do PRORET – Procedimentos de Regulação Tarifária), mas se houver uma mudança brusca de padrões que exija grandes investimentos, revisões extraordinárias podem vir a ser necessárias (Módulo 2.9 do PRORET). No caso da transmissão, pode ser que investimentos requeridos para atender a novas exigências tenham que ser autorizados no “Plano de Modernização de Instalações”, elaborado pelo Operador Nacional do Sistema Elétrico (ONS), ou na “Consolidação de Obras”, compilada pelo Ministério de Minas e Energia (e expressos no PRORET 9.7). No caso das concessionárias de geração, não há previsão de ampliação da receita tarifária para tais investimentos. Se houver mudanças que exijam investimentos muito relevantes para assegurar a confiabilidade cibernética, ajustes na regulamentação terão que ser implementados (PRORET 12.4).

5. Como a certificação relacionada com a segurança cibernética pode ser utilizada para propiciar a conformidade dos agentes em relação aos produtos, serviços, processos e profissionais especializados? Como eventual regulamentação poderia incentivar as empresas a obter essas certificações?

O desenvolvimento de procedimentos para mitigar os riscos e a definição de parâmetros de compatibilidade a serem atendidos pelas empresas de energia elétrica contribui para a segurança cibernética. Assim, a adoção de certificações, melhores práticas e requisitos mínimos de segurança deve ser incentivada.

No entanto, tais eventuais certificações não devem implicar transferência de responsabilidade. No cenário atual, é necessário estabelecer mecanismos para melhorar a articulação entre os representantes das infraestruturas críticas.

O incentivo regulatório aos agentes do setor pode ser promovido por meio do reconhecimento de melhorias na infraestrutura – e, portanto, de reconhecimento dos respectivos ativos incorporados às Bases de Remuneração Regulatória – e de requisitos de segurança a serem definidos em diretrizes e editais de novas licitações.

Em relação ao reconhecimento de ativos voltados à segurança cibernética, é provável que seja necessária a revisão dos seguintes manuais para dar segurança e clareza regulatória a tais investimentos:

a) Manual de Contabilidade do Setor Elétrico; e

b) Manual de Controle Patrimonial do Setor Elétrico.

8. Em relação à segurança cibernética, quais os desafios de cada segmento do setor elétrico (geração, transmissão, distribuição, comercialização)? Quais temas ou áreas da prestação do serviço por cada segmento merecem atenção em relação à segurança cibernética?

A tendência nas infraestruturas críticas de energia saírem do padrão eletromecânico para o digital nos segmentos do setor elétrico ressalta as demandas em segurança cibernética, dando destaque a uma série de desafios envolvendo dificuldades de certificação, capacitação de recursos humanos, compartilhamento de informações, entre outros.

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

Tal capacitação pode ser realizada com treinamentos de curta duração voltada a certificações de segurança e disponibilização de ferramentas computacionais e sistemas adequados.

9. Como devem ser consideradas as soluções regulatórias para que não sejam criadas barreiras à evolução tecnológica?

Uma vez reconhecida a importância da segurança cibernética no setor elétrico, é necessário dar o passo inicial para melhorar o ambiente regulatório.

O foco das medidas regulatórias deve ser mantido em princípios para evitar a criação de processos burocráticos e novos custos atrelados a tais burocracias.

Assim, a 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 deve ser compartilhado.