Brasília, 24 de julho de 2020.

Contribuições à Tomada de Subsídios 07/2020
Segurança Cibernética no SEB

A Associação Brasileira dos Comercializadores de Energia (Abraceel) apresenta contribuição à Tomada de Subsídios 07/2020 da Aneel, que visa obter subsídios para avaliar a necessidade de intervenção regulatória para a segurança cibernética do Sistema Elétrico Brasileiro.

3. Qual a sua relação com a segurança cibernética no setor elétrico?

(X) Agente prestador de serviço de energia elétrica

4. Quais as políticas e as práticas de segurança cibernética a empresa adota no Brasil? Qual legislação nacional e quais normas brasileiras a empresa segue como referência?

Inicialmente, reforçamos que o segmento de comercialização entende como muito pertinente a discussão sobre a segurança cibernética no setor elétrico brasileiro. Até pela sua própria característica, os comercializadores de energia – classe que por vezes transaciona o maior volume de energia no mercado – têm a questão da segurança da informação como uma de suas prioridades, parabenizando o regulador pela preocupação e disposição em discutir tema tão relevante.

Nessa linha, entendemos que o segmento de comercialização de energia não se enquadra como uma "infraestrutura crítica", conforme definido no Decreto 9.573/2018, visto que sua interrupção ou destruição não provocaria danos físicos, como impactos ambientais, econômicos ou à segurança do estado e da sociedade. Cada comercializadora possui sua própria política de segurança da informação, com a adoção de práticas internas adequadas às suas próprias necessidades, sendo essa questão, inclusive, um diferencial competitivo entre as empresas.

Comercializadoras cuja estrutura faz parte de bancos, por exemplo, tendem a seguir a regulamentação específica para instituições financeiras. Em comercializadoras integradas a grupos de geração e distribuição, onde a comercializadora poderia ser uma porta de entrada para ataques cibernéticos, há a adoção de políticas e práticas mais rigorosas de segurança da informação com vistas a mitigar riscos em eventuais infraestruturas críticas.

Assim, dada a variedade de empresas dentro do segmento de comercialização, que conta com empresas de pequeno porte, associadas a grandes grupos, integradas a outros segmentos, com controle externo internacional, etc., cada uma adota práticas internas de segurança individuais, sendo fundamental preservar essa individualidade em eventual regulamentação com vistas a incentivar a constante inovação tecnológica e não prejudicar a competição.

6. 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?

- Prescritiva: que consideram requisitos detalhados, a exemplo dos padrões CIP/Nerc;

- Autorregulação: em que um grupo organizado regula o comportamento de seus membros, elaborando e monitorando as normas, ações ou códigos que disciplinam suas atividades;

- Corregulação ou regulação compartilhada: quando a indústria desenvolve e administra seus próprios padrões, mas o governo fornece o apoio legal para permitir que eles sejam aplicados.

Considerando que ainda não há nenhuma norma específica sobre segurança da informação para o setor elétrico brasileiro, julgamos que neste primeiro momento a regulação deveria ser orientativa, tal como adotado na União Europeia e Estados Unidos. Assim, as empresas teriam margem para se adaptar em como implementar novos requisitos, considerando suas características próprias do negócio, também tendo incentivos para buscar maior diferencial competitivo.

Ainda não está claro até que ponto as políticas e sistemas em uso são capazes de endereçar o problema e quais seriam os custos para implementar sistemas com maior proteção, tampouco a facilidade de acesso à essas novas ferramentas. Dessa forma, a regulação não deve criar barreiras de entrada para novos e pequenos agentes, tampouco burocracias que prejudiquem a eficiência do negócio. Além disso, uma regulação muito específica tende a sofrer muitas alterações, devido ao rápido avanço tecnológico, prejudicando a estabilidade regulatória.

Como medidas orientativas, consideramos que poderia ser sugerido: (i) a conscientização dos colaboradores sobre segurança, dado que o usuário é o elo mais frágil, mas também pode ser o elo mais forte de uma estruturada política de segurança da informação, (ii) a autenticação de senhas e credenciais fortes, com mais de uma camada de proteção, (iii) a gestão de vulnerabilidades, como o hacker ético que objetiva mapear as falhas de segurança, (iv) o uso de sistemas de detecção de ameaças, entre outras.

As próprias normas vigentes sobre o tema, como a Política Nacional de Segurança da Informação e a Lei Geral de Proteção de Dados Pessoais, são de caráter orientativo ao estabelecer diretrizes gerais, sendo essa também uma abordagem usualmente aplicada em outros setores da economia nacional. Em um segundo momento, ao evoluir nas práticas de segurança da informação as empresas poderiam partir para a autorregulação.

8. No âmbito do setor elétrico, o que deveria ser considerado como infraestrutura crítica? Quais critérios para classificação como infraestrutura crítica deveriam ser seguidos? Os critérios deveriam ser individualizados por segmento (geração, transmissão, distribuição, comercialização)? Caso afirmativo, quais seriam os critérios por segmento?

Tal como respondido na pergunta #4, entendemos que a comercialização de energia não se enquadra como infraestrutura crítica.

Entretanto, os critérios estabelecidos pelo Decreto 9.573/2018 para definir infraestruturas críticas podem eventualmente ser adaptados aos outros segmentos do setor elétrico cuja interrupção ou destruição do serviço, total ou parcial, poderia provocar sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade.

Em princípio, os critérios deveriam ser individualizados por segmento considerando a gravidade das consequências dos ataques a que estão suscetíveis, devendo ser ponderado também o porte do empreendimento e a sua localização.

9. Quais tipos de critérios de proporcionalidade podem ser levados em conta para diferenciação de requisitos obrigatórios entre empreendimentos? Deve haver alguma diferença por tipo de serviço (geradores, transmissores, distribuidoras concessionárias e distribuidoras permissionárias), por empreendimentos estruturantes ou por fonte de geração, entre outros, nos requisitos para os empreendimentos de energia elétrica?

O principal critério para diferenciar os requisitos que segmentos e empreendimentos devem seguir deve ser o potencial impacto que podem causar à sociedade.

10. 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?

Em relação ao segmento de comercialização, entendemos que o principal desafio está na proteção de dados e informações considerados confidenciais ou estratégicos, a maioria de caráter financeiro. Esse é um desafio que o segmento tem buscado endereçar de forma constante.

Além disso, no caso de comercializadoras integradas, conforme já mencionado, há o desafio adicional de proteger credenciais e sistemas compartilhados com as áreas de geração e distribuição, com vistas a mitigar impactos em possíveis infraestruturas críticas. Tal medida é possível com a adoção de políticas de segurança da informação bem desenvolvidas, que busquem segregar os acessos, dados e sistemas.

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

Regulamentos de caráter orientativo não criam barreiras nem custos para os agentes. Assim, a avaliação de uma empresa ao mudar de sistema ou escolher determinada ferramenta é balizada unicamente por sua eficiência, e não por imposições regulatórias. Além disso, caso se evolua para a autorregulação em um segundo momento, os agentes têm maior capacidade de acompanhar as atualizações tecnológicas do que o regulador, adaptando para a realidade comercial dessas empresas. Ainda, regulamentos muito específicos rapidamente se tornam defasados, o que impõe uma alta frequência de atualização para não impedir o uso de soluções mais tecnológicas.

14. Qual a forma mais adequada de realizar a prática de compartilhamento de informações sem comprometer a privacidade e o anonimato das empresas?

Os agentes poderiam firmar um acordo conjunto para o compartilhamento de informações com um sistema independente que busque preservar a privacidade e o anonimato das empresas sobre tentativas de ataque ou riscos detectados, alertando assim todos os outros. De toda forma, a participação do regulador é um ponto sensível, uma vez que seria preciso garantir que as informações compartilhadas não seriam usadas para fins de imposição de penalidades regulatórias.

15. Quais ações, envolvendo regulamento ou não, a ANEEL poderia realizar para subsidiar a cooperação de compartilhamento de informações entre as empresas?

Como a discussão do tema ainda é incipiente, sugerimos a realização de mais Workshops específicos sobre segurança cibernética do setor elétrico. Como resultado, a Aneel poderia produzir um documento de caráter informativo com os principais conceitos, riscos, ameaças, medidas de proteção e boas práticas internacionais para ampla divulgação e orientação às empresas.

Atenciosamente,

Yasmin de Oliveira
Assessora de Energia

Bernardo Sicsú
Diretor de Eletricidade e Gás

Alexandre Lopes
Vice-Presidente de Energia