Contribuição para a Consulta Pública 7/2021

OBTER SUBSÍDIOS PARA A ANÁLISE DE IMPACTO REGULATÓRIO (AIR) SOBRE A SEGURANÇA CIBERNÉTICA NO SETOR ELÉTRICO BRASILEIRO

1 INTRODUÇÃO

Este documento apresenta as contribuições do Instituto Acende Brasil para a Consulta Pública 7/2021 da Aneel, cujo objetivo é "OBTER SUBSÍDIOS PARA A ANÁLISE DE IMPACTO REGULATÓRIO (AIR) SOBRE A SEGURANÇA CIBERNÉTICA NO SETOR ELÉTRICO BRASILEIRO."

Os principais documentos oficiais que embasam esta contribuição são:
- Nota Técnica nº 20/2021-SRT-SGI-SRD-SRG/ANEEL; e
- Relatório de Análise de Impacto Regulatório nº 2/2021-SRT- SGI-SRD-SRG/ANEEL.

Dada a crescente relevância do tema em função do aumento de ocorrências de ataques cibernéticos que ameaçam a segurança dos ativos e operações do setor elétrico brasileiro, acreditamos que esta iniciativa da Aneel é fundamental para a definição tempestiva de política pública, legislação e regulação que promovam incentivos adequados – incluindo reconhecimento tarifário – para que autoridades e empresas do setor façam os investimentos e estruturem suas operações buscando:
- reduzir a probabilidade e o impacto destes eventos;
- diminuir a vulnerabilidade dos ativos e operações do setor;
- garantir a segurança nacional e a integridade de dados e de oferta de energia; e
- aumentar nossa capacidade de reação em caso de incidentes.

2 RESPOSTAS AO QUESTIONÁRIO DA CONSULTA PÚBLICA 7/2021

1. Nome ou Razão Social. *Requer resposta. Texto de linha única.*

R: Instituto Acende Brasil

2. E-mail para contato. *Requer resposta. Texto de linha única.*

R: eduardo.monteiro@acendebrasil.com.br

3. Atividade da empresa. *Requer resposta. Opção única.*

- ○ Geração
- ○ Transmissão
- ○ Distribuição
- ○ Consumidor livre
- ○ Associação
- ○ Órgão público
- ○ Fornecedor de serviços de TI
- ◉ Outros

4. O problema regulatório foi estabelecido como risco de ocorrência de incidentes de segurança cibernética no setor elétrico. O problema identificado representa efetivamente a situação que se deseja enfrentar no setor elétrico?

Requer resposta. Opção única.

- (●) Sim
- ( ) Não
- ( ) Parcialmente

5. Em caso negativo, quais são os aperfeiçoamentos sugeridos?

Texto Multilinha.

R: Sem sugestões

6. As causas identificadas foram:

• Atuação de agentes maliciosos e cibercriminosos: são os agentes responsáveis por efetuar os ataques cibernéticos que resultam em algum tipo de incidente. Os hackers são indivíduos que elaboram e modificam softwares e hardwares de computadores, seja desenvolvendo funcionalidades novas ou adaptando as antigas. Já os crackers são pessoas que praticam a quebra de um sistema de segurança. Não há consenso sobre a intenção da atuação de cada um deles, mas os dois tipos têm capacidades de invasão de sistemas.

• Falta de segurança adequada: a vulnerabilidade dos sistemas do setor elétrico pode facilitar a atuação dos hackers ou crackers. Embora haja agentes bem-preparados e com política de segurança cibernética bem desenvolvida, nem todos estão no mesmo nível de maturidade, o que pode expor parte ou mesmo todo sistema aos incidentes.

• Conectividade dos sistemas: os sistemas estão cada vez mais conectados, o que aumenta sua eficiência, seu monitoramento, a capacidade de integração e de análise de dados. A consequência, contudo, é o potencial aumento da abrangência de um ataque.

• Carência de recursos humanos especializados: uma vez que a importância desse problema cresceu recentemente, ainda faltam especializações nessa área, bem como uma cultura de segurança cibernética nas empresas do setor, cujo interesse, acompanhando a tendência da importância do problema, aumentou nos últimos anos.

Há algum aspecto que deveria ser acrescentado a essas causas do problema regulatório ou retirado daqueles inicialmente identificados?

Requer resposta. Opção única.

- (●) Sim
- ( ) Não
- ( ) Em parte

7. Quais os aperfeiçoamentos sugeridos?

Texto Multilinha.

R: Definição tempestiva de política pública, legislação e regulação que promovam incentivos adequados – incluindo reconhecimento tarifário – para que autoridades e empresas do setor tomem as ações, façam os investimentos e estruturem suas operações para reduzir a probabilidade e o impacto dos ataques cibernéticos.

8. As consequências identificadas foram:

• Interrupção no suprimento: uma das consequências mais imediatas de um incidente cibernético é a interrupção de energia elétrica. Essa consequência afeta tanto o consumidor, que terá seu fornecimento interrompido, quanto o gerador, transmissora ou distribuidora, que podem ficar sem condições de atenderem suas demandas.

• Impossibilidade de realizar operações técnicas, comerciais ou de faturamento: pode haver incidentes em centros de operação, tanto no ONS, nos centros dos fornecedores de serviço, quanto nos centros de operação de geradores, transmissores e distribuidoras. No curto prazo, esses agentes podem não operar o sistema adequadamente, resultando tanto na interrupção do serviço quanto na operação ineficiente do SIN, como por exemplo, danos nos sistemas de faturamento, nos dados sobre medição de energia ou na execução de outras atividades do sistema.

• Extravio de dados: a troca e o armazenamento de informações sensíveis e sigilosas teve um aumento drástico com a conectividade. O acesso indevido, furto de propriedade intelectual, uso e venda dos dados são umas das consequências mais comuns de ataques cibernéticos.

Há algum aspecto que deveria ser acrescentado a essas consequências do problema regulatório ou retirado daqueles inicialmente identificados?

Requer resposta. Opção única.

- ○ Sim
- ○ Não
- ◉ Em parte

9. Quais os aperfeiçoamentos sugeridos?

Texto Multilinha.

R: Além das consequências mencionadas, existem outros riscos que merecem a atenção do regulador, uma vez que não podem ser menosprezados os riscos de danos físicos aos ativos que compõem o Setor Elétrico, tanto no que se refere aos ativos primários (geradores, disjuntores, transformadores, turbinas etc.) quanto aos ativos secundários (Dispositivos Eletrônicos Inteligentes, computadores, relés de proteção e monitoramento, *switches* e etc.).

10. Os atores e grupos afetados pela ocorrência de incidentes de segurança cibernética no Setor Elétrico são os agentes detentores de infraestruturas do setor elétrico; os consumidores; e o ONS. Além deles, são também afetados os fornecedores de serviço de geração, transmissão, distribuição e comercializadores de energia elétrica; os órgãos do setor, como MME, ANEEL, ONS, CCEE, EPE; o governo em geral; cidadãos e fornecedores de tecnologia. Foram mapeados todos os atores afetados pelo tema regulatório? Algum ator mapeado no estudo deveria ser retirado?

Texto Multilinha.

R: Apesar de terem sido adequadamente mapeados todos os atores e grupos afetados no Setor Elétrico, é importante destacar que, em caso de algum ataque cibernético de grande magnitude nas instalações do Setor Elétrico Brasileiro, outros setores econômicos poderão ser criticamente afetados pelo comprometimento da oferta de energia elétrica, incluindo setores de infraestrutura básica que viabilizam serviços públicos essenciais como os de Saneamento Básico e de Telecomunicações.

Portanto, a análise talvez possa ser expandida para incluir atores e grupos de outros setores econômicos afetados por incidentes de segurança cibernética no Setor Elétrico.

11. O objetivo principal do problema regulatório é: minimizar os impactos dos incidentes de segurança cibernética no setor elétrico. A definição do objetivo principal abrange o que realmente se deve esperar da alternativa regulatória adotada?

Requer resposta. Opção única.

- ○ Sim
- ○ Não
- ◉ Em parte

12. Em caso negativo, quais são os aperfeiçoamentos sugeridos?

Texto Multilinha.

R: Tão importante quanto a minimização dos impactos de eventuais incidentes é o desenvolvimento de extenso trabalho voltado à prevenção de ocorrências e acidentes cibernéticos por meio do monitoramento do comportamento ofensivo de agentes maliciosos. A regulação não pode tratar apenas da mitigação dos efeitos causados por um eventual ataque, mas deverá ser igualmente eficiente para impedir que estes ataques ocorram.

O número de ataques cibernéticos aumentou consideravelmente entre 2019 e 2020, e podem ser observados em "duas ondas": entre março e junho de 2020 e entre outubro e dezembro de 2020. Não é uma coincidência que isso tenha acontecido no período em que as empresas adotaram o modelo *home office*, permitindo que seus funcionários acessem remotamente os sistemas. Na primeira onda os ataques foram mais direcionados, buscando navegar pelos sistemas e obter acessos restritos, sendo que quase 35% destes ataques envolveram códigos maliciosos. Já na segunda onda os ataques priorizaram o reconhecimento do ambiente para explorar eventuais vulnerabilidades das redes críticas monitoradas, visando a próximos ataques que podem ter magnitude maior por serem mais planejados. Após uma onda de ataques de reconhecimento, pode-se esperar que uma terceira onda de ataques direcionados esteja a caminho. (TI Safe, 2021)

13. Os objetivos específicos são:

a) implementar políticas de segurança cibernética: uma vez que os agentes do setor elétrico não têm controle direto sobre as motivações da atuação de agentes maliciosos e cibercriminosos.

b) incentivar o compartilhamento de informações: para que os agentes estejam mais preparados para evitar um incidente ou, no caso de uma ocorrência, identificá-la e recuperar o mais rapidamente os sistemas.

c) promover a gestão, a avaliação e o tratamento dos riscos de segurança cibernética, para solucionar de forma adequada a falta de segurança.

d) realizar avaliações de maturidade em segurança cibernética, também relacionada à falta de segurança adequada para mapear pontos de fragilidade e desenvolver um planejamento de ações.

e) adotar políticas de segmentação entre redes de operação, corporativa e outras relevantes, com controle de acesso à Internet, no intuito de solucionar potenciais problemas advindos do aumento de conectividade dos sistemas.

f) estabelecer procedimentos de resposta rápida para contenção de incidentes cibernéticos, relacionado à conectividade dos sistemas e à carência de recursos humanos especializados.

Há algum objetivo específico que deveria ter sido elencado ou algum que foi identificado, mas que não é compatível com o problema regulatório identificado?

Texto Multilinha.

R: Sem sugestões

14. Os resultados esperados são:

a) aumento da resiliência dos sistemas do ONS e dos agentes com conexão ao Operador, relacionado à interrupção no suprimento e à impossibilidade de realizar operações técnicas, comerciais ou de faturamento.

b) manutenção da continuidade na prestação dos serviços, devido à consequência interrupção no suprimento.

c) melhoria na gestão dos incidentes de segurança cibernética e no compartilhamento de informações acerca desses incidentes, assim como o resultado (a), relacionado à interrupção no suprimento e à impossibilidade de realizar operações técnicas, comerciais ou de faturamento.

d) utilização de padrões técnicos mínimos de segurança cibernética pelos agentes, por causa da interrupção no suprimento.

e) melhoria da governança de dados críticos ou relevantes, devido ao extravio de dados.

Há algum resultado esperado que deveria ter sido elencado ou algum que foi identificado, mas que não é compatível com o problema regulatório identificado?

Texto Multilinha.

R: Além dos importantes pontos mencionados no texto, recomendamos que alguns objetivos também sejam considerados:

- Estabelecimento de regulamentação nacional integrada e única para o setor elétrico brasileiro a fim de que as instalações críticas de energia estejam submetidas às mesmas regras em todo o território nacional.

- Adequação de instalações existentes, considerando o procedimento de requisitos mínimos de segurança cibernética.

- Revisão do Proret (Procedimentos de Regulação Tarifária da Aneel) a fim de promover o reconhecimento de investimentos em segurança cibernética, dando cobertura tarifária para ativos que ainda não são reconhecidos na Base de Remuneração Regulatória.

- Com a tendência da digitalização e a *Internet of Energy (IoE)*, os cuidados com segurança cibernética devem estar em constante aprimoramento, passando por frequentes avaliações e melhorias, tanto em processos, tecnologias e capacitação de profissionais. (WEF, 2019)

15. Em relação às experiências nacionais e internacionais em estudo, elas são pertinentes ao problema regulatório e aos objetivos identificados? Opção única.

- ○ Sim
- ○ Não
- ◉ Parcialmente

16. Há mais aspectos que podem ser acrescentados?

Texto Multilinha.

R: Recomendamos a adoção do "*Charter of Trust*", uma iniciativa criada por relevantes empresas internacionais que discutem as melhores práticas e compromissos para um futuro digital mais seguro e mais próspero.

1. Responsabilidade na Segurança Cibernética e de TI
2. Responsabilidade em toda a cadeia de suprimentos digital
3. Segurança por padrão
4. Centrado no usuário
5. Inovação e cocriação
6. Educação
7. Certificação e soluções para infraestruturas críticas
8. Transparência e respostas
9. Ambiente regulatório
10. Iniciativas conjuntas

Além dos itens mencionados acima, é necessário destacar a importância de demais princípios que devem ser seguidos para que o setor elétrico brasileiro consiga caminhar em direção ao que há de mais moderno sendo discutido no âmbito da segurança cibernética. É necessário que o desenho do setor seja marcado pela resiliência, a começar pela cultura empresarial. À medida que todo o setor caminha para a digitalização, é condição necessária que os agentes do setor incluam essa preocupação e a enxerguem como uma responsabilidade. Os planos de resiliência cibernética que abrangem todo o ecossistema do setor elétrico devem ser criados, testados e continuamente melhorados, incluindo a capacidade de resposta e recuperação, e, para isso, é necessária a mobilização de diversos agentes do setor. (WEF, 2019)

17. As Alternativas propostas são:

Alternativa 1: Não regular. Consiste em manter a estrutura regulatória atual sobre segurança cibernética, ou seja, manter por exemplo os comandos existentes nos Procedimentos de Rede do ONS sobre segurança cibernética e a estrutura de incentivos regulatórios e penalidades atualmente existentes.

Alternativa 2: Orientar e divulgar as melhores práticas para a segurança cibernética para os agentes setoriais. Consiste em criar canais de comunicação, por exemplo, no site da ANEEL, implementar rotinas de workshops, criar fóruns de debates e de ideias, entre outras ações dessa natureza. Algumas propostas de soluções (na forma de possíveis ações a serem implementadas) contidas nessa alternativa são: disponibilizar no site da ANEEL modelos ou informações sobre as melhores práticas em segurança cibernética; elaborar guia orientativo com o escopo mínimo a ser

compreendido na política de segurança cibernética das empresas; promover eventos para compartilhamento de informações sobre incidentes de segurança cibernética no setor elétrico; promover a adoção de fóruns ou plataformas que possam ser utilizadas para compartilhamento de informações; disponibilizar guias com métodos para avaliar a maturidade cibernética; etc.

Alternativa 3: Regulamentar os itens da política de segurança cibernética. Consiste em criar comandos regulatórios para estabelecer a obrigatoriedade de os agentes do setor estabelecerem suas políticas de segurança cibernética. Para essa alternativa, algumas das propostas de solução (na forma de possíveis ações a serem implementadas) são: restringir a contratação em leilões novos ou existentes de empresas que não possuam uma política de segurança cibernética compatível com seu porte; estabelecer em resolução a necessidade de implementação de políticas de segurança cibernética compatível com porte da empresa; definir a obrigatoriedade de a empresa seguir algum tipo de norma referente à segurança cibernética; estabelecer um fórum permanente coordenado por ONS de empresas de todos os segmentos; estabelecer em norma a obrigatoriedade de informar à Aneel casos de crise em segurança cibernética; etc.

Alternativa 4: Regulamentar requisitos mais prescritivos para segurança cibernética. Consiste em criar comandos regulatórios para estabelecer requisitos mínimos de segurança cibernética a serem seguidos compulsoriamente pelos agentes do setor. Algumas das propostas de solução (na forma de possíveis ações a serem implementadas) são: estabelecer requisitos mínimos de segurança cibernética em regulamento; estabelecer uma entidade coordenadora, ou atribuir responsabilidade, para a gestão de incidentes cibernéticos relevantes; estabelecer uma metodologia padrão para avaliação de maturidade, estabelecer a necessidade de aplicação pelas empresas dessa metodologia e definir um nível de maturidade desejada em um prazo específico; estabelecer em norma a obrigatoriedade de separar TI e TO.

Existem aspectos de diferentes alternativas do estudo que poderiam ser combinados para formar uma nova alternativa?

Texto Multilinha.

R: A "Alternativa 4" poderia implicar uma série de custos e burocracias a serem arcados por diferentes agentes, agentes estes que possuem realidades muito distintas, tornando praticamente inviável a criação de uma série de obrigações iguais para todos.

A "Alternativa 3", considerada mais adequada pela Aneel, pode ser insuficiente em algumas dimensões. Mesmo criando normativas e obrigatoriedades para os agentes, a criação de requisitos mínimos para segurança cibernética faz-se necessária. É importante considerar que não estamos discutindo apenas um problema existente, mas sim uma questão que continuará a se agravar com o passar do tempo, afinal:

- o futuro do setor elétrico tende a ser cada vez mais digital e integrado; e
- a capacidade e o ferramental técnico dos agentes maliciosos se ampliam a cada dia.

Acreditamos que a melhor alternativa seria uma "Alternativa 3.5" que leve em consideração elementos presentes nas "Alternativas 3 e 4", combinando elementos e comandos regulatórios:
- prescritivos quanto aos fins (resultados) a serem obtidos (que devem ser os mesmos para todos os agentes);
- orientativos quantos aos meios (processos e tecnologias) que serão adotados para se chegar aos resultados, permitindo flexibilidade para que cada agentes faça as adaptações necessárias às diferentes realidades em que atuam e evitando a criação de amarras e burocracias ineficientes e custosas.

As políticas adotadas por cada agente podem ser diferentes, mas todas devem estar alinhadas a uma regulamentação nacional e abrangente sobre o tema.

18. Foram identificados os seguintes impactos positivos e negativos da:

Para a Alternativa 1: não regular

Positivos: Liberdade para escolha e implementação de políticas de segurança cibernética pelos agentes. Ausência de custos regulatórios adicionais. Menor atribuição à fiscalização. Sem necessidade de adaptação a nova regulação. Sem aumento tarifário devido à inexistência dos custos de adaptação.

Negativos: Ineficiência devido à busca de soluções de forma individualizada pelos agentes. Longo período de conscientização dos agentes. Responsabilização indireta da ANEEL pelas consequências de um ataque. Ausência de diretrizes e boas práticas recomendáveis acerca do tema para orientar os agentes. Incentivo à inércia dos agentes. Permanência ou aumento de riscos de incidentes cibernéticos.

Para a alternativa 2: orientar e divulgar as melhores práticas de segurança cibernética para os agentes setoriais

Positivos: Orientação e liberdade para escolha e implementação de políticas de segurança cibernética. Natureza informativa e indicativa que evita discordâncias regulatórias. Potencial educacional dos fóruns e eventos. Sem carga regulatória associada.

Negativos: Incentivo à inércia dos agentes. Ineficiência devido à busca de soluções de forma individualizada pelos agentes. Desincentivo devido ao sigilo de informações solicitadas nos fóruns e eventos. Falta de previsibilidade acerca dos custos de

investimento diante da alternativa não regulatória. Exposição da rede devido aos agentes com políticas de segurança mais simples.

Para a alternativa 3: regulamentar os itens da política de segurança cibernética

Positivos: Melhoria da percepção de riscos por parte dos agentes. Aumento de eficiência na busca de soluções. Flexibilização de tecnologias e metodologias de acordo com o porte dos agentes. Liberdade aos agentes para escolha da política de segurança. Menor risco de defasagem tecnológica dos procedimentos adotados pelas empresas. Melhor direcionamento de atitudes aos agentes. Aumento da previsibilidade regulatória. Maior segurança com os dados de consumidores.

Negativos: Exposição da rede devido aos agentes com políticas de segurança mais simples. Falta de clareza acerca dos investimentos em segurança cibernética. Menor liberdade aos agentes para escolha da política de segurança, em relação às alternativas 1 e 2. Menor consideração da diferente realidade dos agentes, em relação às alternativas 1 e 2. Custos de adaptação aos itens da política de segurança cibernética.

Para a alternativa 4:

Positivos: Estabelecimento de padrão mínimo de riscos de segurança cibernética. Aumento da previsibilidade regulatória. Maior discussão sobre reconhecimento tarifário de investimentos específicos exigidos pela regulação. Menor custo de aprendizagem, ou seja, menor custo na escolha de requisitos a serem aplicados.

Negativos: Maior risco de defasagem tecnológica dos procedimentos adotados pelas empresas devido a exigências específicas da regulação. Baixa ou nenhuma flexibilização de tecnologias e metodologias de acordo com o porte dos agentes. Baixa liberdade aos agentes para escolha da política de segurança. Maior necessidade de fiscalização. Maiores custos de adaptação aos requisitos de segurança cibernética. Maiores custos de adaptação que desconsideram diferentes realidades dos agentes de geração.

Há pontos que não foram mapeados ou deveriam ser desconsiderados do mapeamento inicial?

Texto Multilinha.

R: Sem sugestões

19. Comente sobre a implementação na prática das alternativas elencadas, sobre eventuais limitações e dificuldades não consideradas ou sobre os aspectos vantajosos que favorecem a implementação das alternativas.

Texto Multilinha.

R: A fronteira de conhecimento, práticas e ativos voltados à Segurança Cibernética deveria ser tratada pela Aneel como um conjunto de alternativas que envolvem decisões regulatórias de investimentos no setor elétrico e que podem afetar o equilíbrio dinâmico entre CAPEX e OPEX.

Investimentos (CAPEX) em Segurança Cibernética podem implicar ganhos operacionais e redução de custos (OPEX) para todos os agentes (empresas e consumidores). Exemplos:
- tais investimentos viabilizam a operação remota e a coleta de dados que, quando combinadas com soluções de Inteligência Artificial, contribuem para a redução dos custos com manutenção; e
- tais investimentos impactam positivamente os índices de qualidade de prestação de serviço (DEC, FEC, DIC, FIC e DMIC).

20. A ANEEL identificou a alternativa 3 como mais adequada para alcançar os objetivos pretendidos, utilizando a metodologia de Análise de Riscos complementada pela avaliação de critérios. Existe algum aspecto que não foi considerado?

Requer resposta. Opção única.

- ○ Sim
- ○ Não
- ◉ Parcialmente

21.Quais são os aperfeiçoamentos sugeridos?

Texto Multilinha.

R: Vide resposta à questão 17

22.Na hipótese de a ANEEL caminhar para um estudo mais quantitativo, como quantificar impactos positivos e negativos de cada alternativa? Como conseguir dados que suportem argumentos associados a cada alternativa?

Texto Multilinha.

R: Sem sugestões

3 BIBLIOGRAFIA

TI Safe (2020). "O aumento dos ataques hackers contra empresas de energia no Brasil na pandemia." [Webinar]. TI Safe. Disponível em: https://www.youtube.com/watch?v=gX9PXSmYKLg

BAILEY, Tucker; MARUYAMA, Adam; WALLANCE, Daniel (2020). "The energy-sector threat: How to address cybersecurity vulnerabilities" McKinsey & Company

4 REFERÊNCIAS BIBLIOGRÁFICAS

TI Safe. "TI Safe ICS-SOC Retrospectiva de Ameaças de 2020", (Comunicação Pessoal, fevereiro de 2021)

World Economic Forum - Centre for Cybersecurity and Electricity Industry Community (2019). "Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards". World Economic Forum; Boston Consulting Group