GRUPO DE ESTUDO DE ASPECTOS EMPRESARIAIS E DE GESTÃO CORPORATIVA E DA INOVAÇÃO E DA EDUCAÇÃO E DE REGULAÇÃO DO SETOR ELÉTRICO - GEC

AVALIAÇÃO DE IMPACTO REGULATÓRIO SOBRE SEGURANÇA CIBERNÉTICA NO SETOR ELÉTRICO BRASILEIRO – UMA PROPOSTA DE ATUAÇÃO REGULATÓRIA

BRUNO DANIEL MAZETO (1); THELMA MARIA MELO PINHEIRO (1); SIDNEY MATOS (1); LEONARDO MENDONÇA OLIVEIRA DE QUEIROZ (1); RENATO ABDALLA AFONSO (1); MATEUS SOUSA PINHEIRO (1); VICTOR MATHEUS PASSAMANI OLIVEIRA (1); SANDOVAL FEITOSA (1)
AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA – ANEEL (1)

RESUMO

A cibersegurança é uma temática que vem ganhando interesse em esferas diversas. Com o crescimento de ciberataques, além de decretos publicados pelo Governo Federal para minimizar os riscos, a Agência Nacional de Energia Elétrica (ANEEL) elaborou Análise de Impacto Regulatório (AIR) sobre segurança cibernética do Setor Elétrico Brasileiro (SEB). O objetivo deste Informe Técnico é descrever o processo adotado pela Agência para a elaboração dessa análise, baseado principalmente em técnicas de *Design Thinking*, trazendo alternativas de ação para enfrentamento do problema regulatório. Como resultado, foi escolhida a alternativa de regulamentar os itens da política de cibersegurança dos agentes.

PALAVRAS-CHAVE

ANEEL, Segurança Cibernética, Análise de Impacto Regulatório, Regulação, Setor Elétrico Brasileiro.

1.0 INTRODUÇÃO

As discussões acerca de segurança cibernética vêm aumentando consideravelmente devido à sua importância em diversos setores. No setor elétrico, o aumento da conectividade digital promovido principalmente pela integração entre sistemas de Tecnologia da Informação (TI) e Tecnologia Operacional (TO), além da evolução das ferramentas utilizadas por cibercriminosos, contribuem para a exposição dos sistemas elétricos a ataques cibernéticos.

No Brasil, a publicação dos Decretos nº 9.637/2018, nº 10.122/2020 e nº 10.748/2021 teve o intuito de estabelecer mecanismos legais para incentivar a adoção de práticas mais robustas para minimizar o risco de ataques cibernéticos ou para identificar mais rapidamente e solucionar o problema. Além disso, mais especificamente no setor elétrico, o crescimento expressivo de casos que afetaram empresas tornou essencial a discussão sobre essa temática de cibersegurança.

A regulação é o instrumento por meio do qual o Estado intervém no comportamento dos agentes, de modo a promover aumento da eficiência, da segurança, do crescimento econômico e dos ganhos de bem-estar social. Tendo isso em vista, a Análise de Impacto Regulatório (AIR) objetiva avaliar a necessidade e as consequências de uma possível nova regulação ou melhoria na regulação existente, verificando se os potenciais benefícios são maiores que os custos estimados e se, dentre todas as alternativas para alcançar o objetivo, a ação escolhida é a mais benéfica para a sociedade.

A regulação do setor elétrico nacional é competência da Agência Nacional de Energia Elétrica (ANEEL), autarquia em regime especial vinculada ao Ministério de Minas e Energia (MME), que tem como principais atribuições, além da regulação, as atividades de: fiscalização, estabelecimento de tarifas, outorgas de concessão, mediação e ouvidoria.

Os agentes do setor elétrico são essenciais para a operação do Sistema Interligado Nacional (SIN), além de possuírem informações críticas, sejam financeiras ou operacionais para planejamento do setor. Logo, é necessário que a ANEEL avalie a necessidade de intervenção regulatória para incentivar esses agentes a implementarem soluções que minimizem o risco de ataques cibernéticos e que permitam rápida identificação e recuperação de eventuais incidentes.

Nesse diapasão, a ANEEL desenvolveu a Análise de Impacto Regulatório (AIR) sobre segurança cibernética no Setor Elétrico Brasileiro (1). Essa análise teve como objetivo apresentar o problema identificado em termos de segurança

cibernética no setor e uma metodologia para elaboração e comparação de possíveis intervenções regulatórias para tratamento do referido problema.

2.0 EXPERIÊNCIA NACIONAL E INTERNACIONAL

2.1 Experiência nacional

No Brasil, como citado, recentemente foram emitidos decretos específicos sobre segurança cibernética. Destacam-se os Decretos nº 9.637/2018, que instituiu a Política Nacional de Segurança da Informação, e nº 10.122/2020, que aprovou a Estratégia Nacional de Segurança Cibernética. Esse último, entre outros pontos de destaque, visa a proporcionar às infraestruturas críticas maior resiliência. Isto é obtido por meio da interação entre as agências reguladoras e por meio do incentivo às organizações para que implementem políticas de cibersegurança que contemplem métricas, mecanismos de avaliação e revisão periódica.

Também foi instituída a Rede Federal de Gestão de Incidentes Cibernéticos por meio do Decreto nº 10.748/2021. De acordo com esse decreto, todos os órgãos e as entidades da administração pública federal direta, autárquica e fundacional estão obrigados a participar dessa Rede, que tem como objetivo divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos, compartilhar alertas sobre ameaças e vulnerabilidades, além de informações sobre ataques.

No cenário regulatório, o Banco Central emitiu a Resolução CMN nº 4.893, de 26 de fevereiro de 2021, que determinou, entre outros pontos, que as instituições financeiras desenvolvam uma política de segurança cibernética, além de um plano de ação de respostas a incidentes (2). Além disso, no setor de telecomunicações, a Anatel publicou a Resolução Anatel n° 740, de 21 de dezembro de 2020, que, apontou a necessidade do compartilhamento de informações sobre incidentes e do estabelecimento de requisitos de gestão da segurança cibernética às prestadoras. Tanto o Banco Central quanto a Anatel tendem a manter resoluções de caráter mais orientativo, com indicação dos requisitos mínimos a serem observados, de forma não prescritiva (3).

No âmbito do setor elétrico, durante a 7ª Reunião Pública Ordinária, em 9 de março de 2021, a Diretoria da ANEEL recomendou que o Operador Nacional do Sistema Elétrico (ONS) estabelecesse um documento operativo com as orientações e/ou critérios para definir a política de segurança e os recursos tecnológicos para proteção contra ataques cibernéticos na Rede de Supervisão e controle dos centros de operação (ARCiber). Assim, em julho de 2021, entrou em vigência a Rotina Operacional – Controles mínimos de segurança cibernética para o Ambiente Regulado Cibernético (RO-CB.BR.01), que aborda temas como arquitetura tecnológica, governança de segurança da informação, inventário de ativos, gestão de vulnerabilidades e de acessos, monitoramento de resposta a incidentes, entre outros.

2.2 Experiência internacional

No cenário internacional, as principais referências em segurança cibernética para o setor elétrico são as regras estadunidenses *Critical Infrastructure Protection* (CIP) da *North American Electric Reliability Corporation* (NERC), além do framework do *National Institute of Standards and Technology* (NIST) que, em geral, servem como recomendação para os agentes e para agências como a *Federal Energy Regulatory Commission* (FERC). Essa regulação abrange grandes geradores e transmissoras de energia, mas sistemas de transmissão e de distribuição local são de competência dos estados. Logo, não há uma regra geral para esses sistemas nos EUA.

Além dos Estados Unidos, outros países desenvolvidos em regulação como Austrália, Canadá e Nova Zelândia seguem as regras do NIST e NERC. Ademais, o México também está sujeito à regulamentação do NIST e NERC nas interligações com os EUA.

Os padrões CIP trazem obrigações relativas à segurança cibernética com temáticas acerca da categorização dos sistemas cibernéticos, treinamento de pessoal, segurança física dos sistemas cibernéticos, proteção da informação, plano de resposta a incidentes, entre outros. A Europa, embora não sujeita ao NIST e NERC, usa diretamente os textos da CIP em sua regulamentação.

Na União Europeia, a *European Network and Information Security Agency* (Enisa) é o órgão que propõe a regulamentação para a segurança cibernética. Esse órgão publicou, em 2016, a Diretiva *Network and Information Security* (NIS), composta por três partes: capacidades nacionais, apontando a necessidade das preparações individuais das nações para defesa cibernética; colaboração transfronteiriça e supervisão nacional de setores críticos, como o setor de energia, transporte, financeiro e serviços críticos digitais. Assim, apesar da Diretiva NIS não ser específica para o setor elétrico, ela fornece princípios orientativos e estratégia de alto nível de segurança de redes e sistemas de informação para os países membros, exigindo, por exemplo, que os operadores relatem incidentes que afetem segurança, fornecimento, confidencialidade e integridade do serviço.

3.0 METODOLOGIA DE DESIGN THINKING APLICADA À ANÁLISE DE IMPACTO REGULATÓRIO

Com o objetivo de tratar a questão de maneira sistêmica, a Análise de Impacto Regulatório (AIR) foi realizada colaborativamente por meio da metodologia de *Design Thinking*, já utilizada pioneiramente no âmbito das agências reguladoras pela Agência Nacional de Vigilância Sanitária (ANVISA).

O *Design Thinking* é uma abordagem que combina um conjunto de princípios, ferramentas e processos extraídos da prática do *Design* Industrial para permitir que pessoas consigam desenvolver soluções inovadoras e efetivas para problemas complexos. As etapas típicas propostas por essa abordagem são o entendimento e definição do problema, ideação e implementação.

Na fase de entendimento do problema ocorre a sua definição, posteriormente os objetivos e resultados esperados, bem como o mapeamento dos atores afetados. Na ideação, são construídas eventuais soluções e alternativas para o tratamento do problema, as vantagens e desvantagens de cada alternativa e, posteriormente, na fase de convergência, a escolha daquela proposta que se mostra mais vantajosa. Finalmente, ocorre a submissão da AIR e da minuta de ato normativo à Consulta Pública.

3.1 Problema regulatório, causas e consequências, atores afetados, objetivos e resultados esperados

Inicialmente, por meio de discussões interativas entre os responsáveis pelo desenvolvimento da AIR, o problema regulatório foi definido como o "Risco de ocorrência de incidentes de segurança cibernética no setor elétrico".

Depois, foram identificadas as causas raízes desse problema e suas respectivas consequências. A Figura 1 aponta o Diagrama do Problema Regulatório, relacionando-o com suas causas e consequências.

FIGURA 1 – Diagrama do Problema Regulatório: causas raízes e consequências

Entre as causas raízes apontadas, a conectividade dos sistemas pode ser verificada principalmente na integração entre TI e TO. TI pode ser definido como um conjunto de atividades que envolvem diferentes dispositivos, como banco de dados e redes, com o intuito de produzir, armazenar, e gerenciar informações geralmente utilizados na parte não operacional das empresas. Por sua vez, TO são *hardwares* e *softwares* usualmente designados para fazer tarefas específicas, como monitorar performance mecânica ou ativar dispositivos de emergência, no setor elétrico é o cerne da operação do sistema. Com esses sistemas cada vez mais interligados há o aumento da eficiência e integração. A consequência, contudo, é o potencial aumento da abrangência de um ataque cibernético.

Com relação aos atores e grupos afetados pelo problema regulatório, destacam-se os agentes detentores de infraestruturas do setor elétrico, tais como fornecedores de serviço de geração, transmissão, distribuição e comercializadores de energia elétrica; os consumidores; fornecedores de tecnologia; o ONS; além de outros órgãos do setor, como MME, ANEEL, Câmara Comercializadora de Energia Elétrica (CCEE), Empresa de Pesquisa Energética (EPE) e o governo em geral.

Tendo mapeados o problema em questão, suas causas e consequências, além dos responsáveis afetados, foi necessário então determinar os objetivos no enfrentamento desse problema. Logo, o objetivo principal apontado foi "Minimizar os impactos dos incidentes de segurança cibernética".

Após a definição do objetivo principal e analisando de forma mais detalhada as causas raízes, os objetivos específicos foram estabelecidos. Além disso, foram definidos os resultados esperados para cada consequência do problema identificado. Assim, conforme ilustra a Figura 2, há um relacionamento entre os objetivos específicos, listados nas colunas da esquerda, e os resultados esperados, nas colunas da direita.

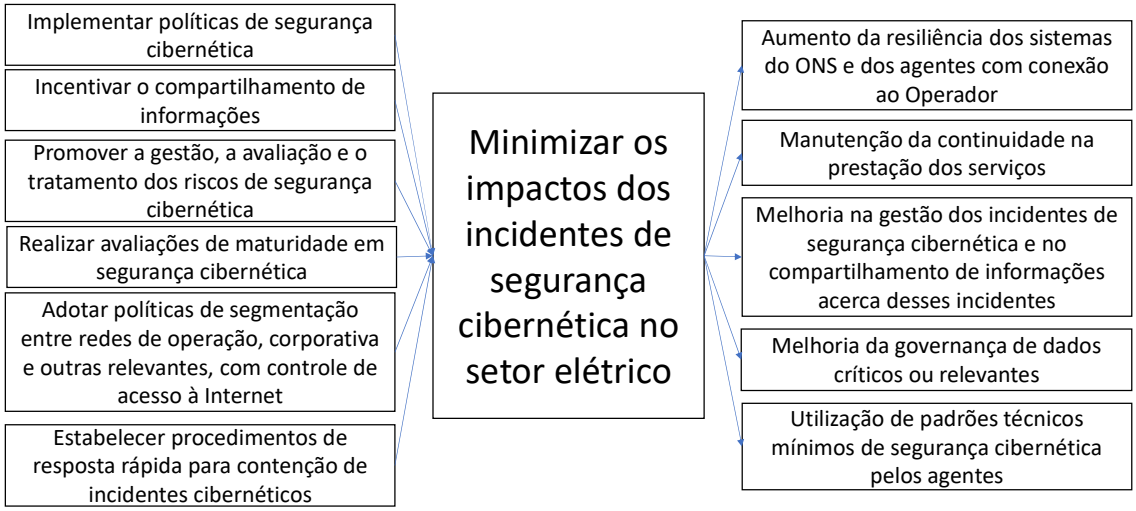

FIGURA 2 – Objetivo principal, objetivos específicos e resultados esperados

Destacam-se entre os objetivos específicos o incentivo ao compartilhamento de informações para que os agentes estejam mais preparados para evitar um incidente ou identificar e recuperar os sistemas no caso de uma ocorrência, além da realização de avaliações de maturidade em segurança cibernética, visando identificar os pontos de fragilidade na cibersegurança. Além disso, tanto o objetivo principal quanto os objetivos específicos devem estar em conformidade com o Decreto nº 10.222/2020.

3.2 Alternativas de solução, vantagens e desvantagens

Com os objetivos específicos estabelecidos, foram realizadas dinâmicas entre os participantes responsáveis pelo desenvolvimento da AIR no intuito de propor uma série de soluções normativas e não normativas capazes de atingir os resultados esperados. Logo após, houve o agrupamento em quatro alternativas, descritas a seguir.

Alternativa 1 - Não regular: consiste em manter a estrutura regulatória atual sobre segurança cibernética, como por exemplo os comandos existentes nos Procedimentos de Rede e a estrutura de incentivos regulatórios e penalidades atualmente existentes. Por não envolver ação complementar à estrutura regulatória em vigor, essa alternativa se caracteriza por não existir um agente específico responsável pela sua implantação.

Alternativa 2 - Orientar e divulgar as melhores práticas de segurança cibernética para os agentes setoriais: consiste em criar canais de comunicação, implementar rotinas de *workshops*, criar fóruns de debates e de ideias, entre outras ações dessa natureza. Essa alternativa tem como foco dar acesso a informações importantes sobre segurança cibernética aos agentes do setor elétrico e estimular a adoção voluntária de medidas que atinjam o objetivo pretendido. Inicialmente, a ANEEL seria responsável pela execução das ações, mas esperar-se-ia que em seguida ações semelhantes seriam estimuladas pelos agentes do setor elétrico de forma voluntária.

Entre as ações a serem implementadas contidas nessa alternativa, destacam-se a disponibilização de modelos ou informações sobre as melhores práticas em segurança cibernética pela ANEEL em seu site; a elaboração de um guia orientativo com o escopo mínimo a ser compreendido na política de cibersegurança das empresas, além de métodos para avaliar a maturidade cibernética; incentivo à participação dos agentes em exercícios cibernéticos.

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. Primeiramente, essa alternativa seria implantada por meio de processo normativo padrão e, posteriormente, seriam elaboradas e implantadas as políticas de segurança cibernética pelas empresas e agentes.

As propostas de ação dessa alternativa consistem no estabelecimento em resolução da necessidade de implementação de políticas de segurança cibernética pela empresa compatíveis com o seu porte; da obrigação dos agentes do setor elétrico em informar ao regulador os eventos ocorridos em relação à segurança cibernética; da

obrigatoriedade de a empresa escolher e aplicar periodicamente uma metodologia de avaliação de maturidade regulatória; em exigir das organizações um Plano de Resposta e Recuperação de Incidentes, entre outros.

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, atuando de forma mais detalhada. Primeiramente, essa alternativa seria implantada por meio de processo normativo padrão e, posteriormente seriam elaboradas e implantadas as políticas de segurança cibernética pelas empresas e agentes.

Para essa alternativa, seriam previstas ações mais prescritivas como a obrigatoriedade de separar TI e TO; o estabelecimento de uma metodologia padrão para avaliação de maturidade e definição de um nível a ser atingido em um prazo específico; o estabelecimento de uma entidade coordenadora para a gestão de incidentes cibernéticos.

Após definição das alternativas, foi realizado o levantamento de seus impactos positivos e negativos. Para tal, essa etapa foi dividida em duas partes: para a primeira, foi utilizada como técnica o *Role-Playing Game* (RPG) *Brainwriting*, que consiste em uma discussão baseada na contribuição de ideias com cada participante da reunião interpretando o papel de um ator afetado pelo problema regulatório. Na segunda fase, houve o agrupamento de ideias semelhantes, objetivando assim uma visão geral, ou seja, os impactos comuns a todos os atores envolvidos.

Dessa forma, a Alternativa 1 teria impactos positivos como uma maior liberdade dos agentes para implementação de política de cibersegurança e ausência de custos regulatórios adicionais. Por outro lado, o incentivo à inércia dos agentes e a ausência de diretrizes seriam impactos negativos, podendo até aumentar os riscos de ataques.

A Alternativa 2 seria positiva no sentido de orientar os agentes para a melhor escolha de políticas de cibersegurança, além de não possuir uma carga regulatória associada. Os impactos negativos ficariam por conta da possível ineficiente busca de soluções por parte dos agentes, além de não haver previsibilidade acerca dos custos.

Os impactos positivos da Alternativa 3 seriam o aumento de eficiência na busca de soluções e um melhor direcionamento de atitudes aos agentes, levando em consideração o porte de cada um. Porém, os custos de adaptação aos itens da política de segurança cibernética se mostra como um dos impactos negativos.

Por fim, a Alternativa 4 teria o estabelecimento de um padrão mínimo de riscos de segurança cibernética, além do aumento da previsibilidade regulatória como pontos fortes. Entretanto, a baixa ou nenhuma flexibilização de tecnologias e metodologias de acordo com o porte dos agentes, além de maiores custos de adaptação seriam aspectos negativos.

3.3 Análise de alternativas

Para a avaliação dos impactos e comparação das alternativas foi utilizada a metodologia de Análise de Risco. Essa metodologia é prevista no Decreto nº 10.411/2020 , que regulamenta a Análise de Impacto Regulatório, e deve ser utilizada quando o problema regulatório é do tipo risco, de acordo com o documento das Diretrizes Gerais e Guia Orientativo para Elaboração de AIR, da Casa Civil (4).

Além das referências citadas, a Nota de Orientação do Governo Australiano traz recomendações sobre como os reguladores podem abordar a Análise de Risco. De acordo com essa nota, o tamanho de um risco é definido pela probabilidade de ocorrência de um evento e suas respectivas consequências, já citadas anteriormente para o problema regulatório em questão (5).

Visando analisar o tamanho e impacto potencial do risco de ocorrência de incidentes de segurança cibernética no setor elétrico, foi elaborada uma Matriz de Riscos. A Matriz de Riscos é uma ferramenta de gerenciamento de riscos que permite, de forma visual, identificar quais são os que devem receber mais atenção. Ela consiste em uma tabela orientada por duas dimensões: probabilidade e impacto.

Assim, foi elaborado um formulário com perguntas aos especialistas de unidades organizacionais da ANEEL responsáveis pelo desenvolvimento da AIR. Esse questionário objetivou analisar o provável comportamento de cada alternativa com relação à redução do tamanho do risco, à probabilidade de ocorrência do risco e com relação ao impacto em cada consequência do problema regulatório.

Em relação à redução do tamanho do risco, a maioria dos respondentes indicou que as Alternativas 2, 3 e 4 reduziriam o tamanho do risco, mas que nenhuma delas removeria o risco por completo. Foi indicado também que no caso das Alternativas 1, 2 e 3 não haveria transferência de risco, ao contrário da Alternativa 4, em que poderia haver. Para o caso da transferência do risco, levou-se em consideração nas respostas que quanto mais prescritivas fossem as soluções adotadas, as responsabilidades sobre cibersegurança passariam cada vez mais dos empreendedores para os órgãos responsáveis por estabelecer os comandos regulatórios, como ANEEL e ONS.

Além disso, foram obtidas as matrizes de risco para cada uma das consequências e para o risco analisado de acordo com as respostas dos participantes, assim como ilustram as Figuras 3, 4 e 5.

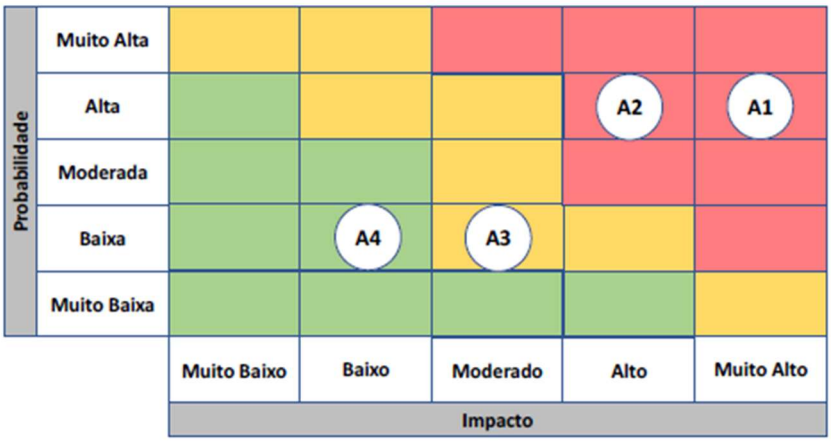

FIGURA 3 – Matriz de risco para a consequência “Interrupção no suprimento”

De acordo com a Figura 3, para a consequência da interrupção no suprimento, verifica-se que a alternativa que apresentou melhor desempenho quanto à avaliação da criticidade foi a Alternativa 4. As Alternativas 1 e 2 mantiveram o risco associado a essa consequência em níveis de criticidade alta.

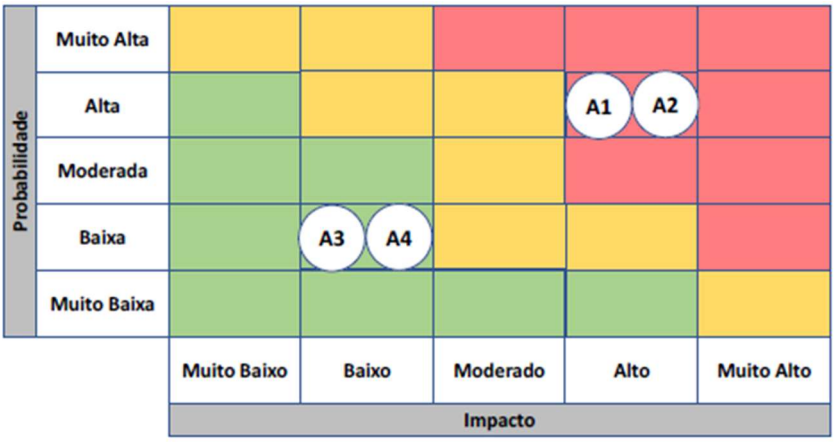

FIGURA 4 – Matriz de risco para a consequência “Impossibilidade de realizar operações técnicas, comerciais ou de faturamento”

Para a consequência da impossibilidade de realizar operações técnicas, comerciais ou de faturamento, conforme Figura 4, observa-se que as Alternativas 3 e 4 apresentaram os melhores desempenhos em relação à criticidade. As Alternativas 1 e 2 também mantiveram o risco associado a essa consequência em níveis de criticidade alta.

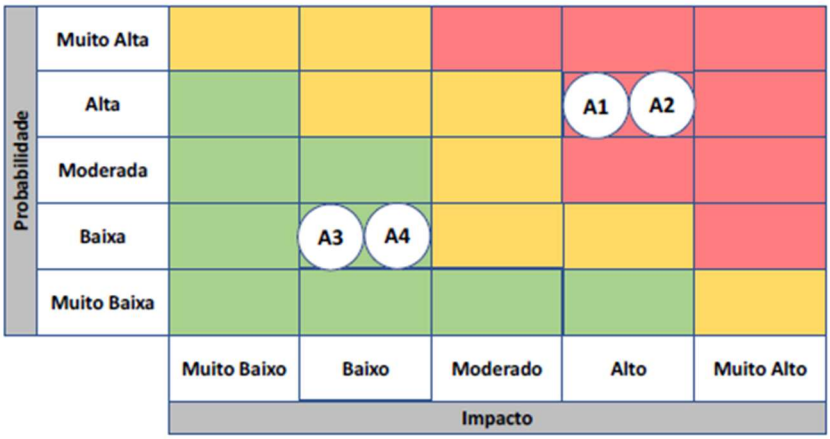

FIGURA 5 – Matriz de risco para a consequência “Extravio de dados”

Com relação à consequência do extravio de dados, de acordo com a Figura 5, verifica-se que as Alternativas 3 e 4 apresentaram resultados semelhantes e os melhores desempenhos em relação à criticidade. As Alternativas 1 e 2 também mantiveram o risco associado a essa consequência em níveis de criticidade alta.

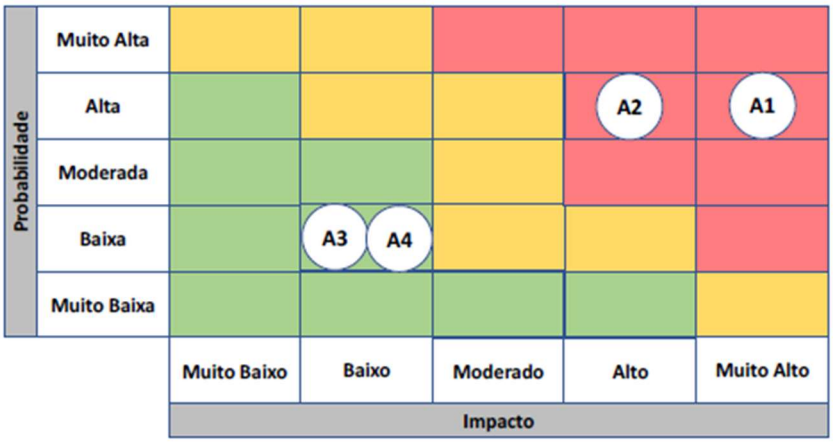

FIGURA 6 – Matriz de risco para o “Risco de ocorrência de incidentes de segurança cibernética no setor elétrico”

Na matriz de risco para o problema regulatório, na Figura 6, observa-se que as Alternativas 3 e 4 apresentaram os melhores desempenhos em relação à criticidade, enquanto as Alternativas 1 e 2 mantiveram o risco associado em níveis de criticidade alta.

Logo, de acordo com a Análise de Risco, pode-se afirmar que as Alternativas 3 e 4 são equivalentes e cumprem com o objetivo de minimizar os impactos dos incidentes de segurança cibernética no setor elétrico. Entretanto, uma das desvantagens da Análise de Risco citadas pelo Guia Orientativo para Elaboração de AIR, da Casa Civil, é que essa metodologia não leva em consideração os custos para a redução do risco, além de outros impactos potenciais. Assim, foi realizada uma avaliação complementar considerando critérios específicos.

Para tal, os participantes da equipe voltaram a representar os atores afetados pelo problema regulatório e avaliaram, com notas de 0 a 10, a performance das alternativas quanto aos critérios específicos. A Tabela 1 mostra quais critérios foram levados em consideração, a média simples das avaliações de cada um dos participantes e o somatório dessas médias, apontando assim o desempenho de cada alternativa.

TABELA 1 – Avaliação dos critérios para cada alternativa de ação regulatória.

Critérios	Alternativa 2	Alternativa 3	Alternativa 1	Alternativa 4
Tempo de implementação	8,8	7,3	10,0	4,9
Grau de esforço	8,2	7,5	10,0	5,4
Simplificação	8,5	7,5	9,1	5,5
Carga administrativa	8,2	7,8	8,8	5,6
Impacto regulatório	8,2	8,6	8,2	6,8

Aplicabilidade	7,1	7,5	6,2	7,5
Aceitação da sociedade	7,8	8,3	5,5	7,3
Aceitação política	7,4	8,6	3,8	7,7
Tecnologia disponível	8,5	8,6	7,4	7,6
Conhecimento disponível	8,4	8,3	7,5	6,7
Recursos disponíveis	8,4	7,8	8,0	6,0
Resultado	**89,5**	**88,0**	**84,5**	**70,9**

De acordo com a metodologia aplicada, a Alternativa 2 apresentou o melhor desempenho, com 89,5 pontos. Entretanto, ela não configurou entre as alternativas de melhor performance na Análise de Risco. Considerando apenas as Alternativas 3 e 4, que foram as de melhor desempenho na comparação por meio da Análise de Risco, verifica-se que a Alternativa 3 apresenta o resultado da avaliação dos critérios com maior pontuação (88 pontos) do que a Alternativa 4 (70,9 pontos).

Logo, de acordo com os resultados apresentados para a metodologia de Análise de Risco complementada pela avaliação de critérios, a Alternativa 3 – Regulamentar os itens da política de segurança cibernética se mostra mais adequada para alcançar os objetivos pretendidos.

4.0 PARTICIPAÇÃO SOCIAL E APRIMORAMENTOS DA ALTERNATIVA ESCOLHIDA

O resultado da comparação das alternativas e a configuração das soluções propostas para cada uma delas foram submetidas para contribuições da sociedade por meio da Consulta Pública nº 007/2021. De acordo com as manifestações recebidas, verificou-se a oportunidade de aprimoramento da Alternativa 3, sem que fosse alterada a sua essência.

Assim, a configuração final de soluções para a Alternativa 3 lista o estabelecimento em norma da obrigatoriedade, por parte dos agentes, de implementar políticas de segurança cibernética compatíveis com o porte da empresa, de informar à ANEEL casos de crise de cibersegurança, de compartilhar incidentes cibernéticos relevantes entre os agentes e entre os agentes e a ANEEL, de escolher e aplicar periodicamente uma metodologia de avaliação de maturidade regulatória, além de realizar a gestão, avaliação e o tratamento dos riscos de segurança cibernética. Além disso, a ANEEL deve estabelecer em regulamento que a política de segurança cibernética da empresa deve prever a segmentação de redes de operação da rede de TI e da Internet, além de prever procedimentos de resposta rápida para contenção de incidentes.

Foi levantado também na Consulta Pública nº 007/2021 a possibilidade de inclusão de algumas das soluções da Alternativa 2 no escopo da Alternativa 3. Tendo em vista o papel da fiscalização da ANEEL na educação e na orientação dos agentes do setor de energia elétrica, tais soluções foram incluídas, como ações de divulgação para participação dos agentes em exercícios cibernéticos, para melhores práticas de segurança cibernética, além da conscientização desses agentes da importância de reconhecer seu nível de maturidade cibernética.

5.0 MONITORAMENTO REGULATÓRIO

O monitoramento consiste na verificação de pontos de controle pré-definidos de uma intervenção regulatória. Ele gera evidências sobre as atividades e impactos de uma intervenção ao longo do tempo de maneira contínua e sistemática desde sua implementação, ajudando a identificar se uma intervenção regulatória está sendo aplicada e produzindo resultados conforme o esperado.

Tendo sido definidos osobjetivos da intervenção regulatória também podem ser estabelecidos os pontos de controle que permitem verificar ao longo do tempo os impactos do regulamento. Esses pontos serão monitorados em período pré-definido, permitindo que possíveis efeitos indesejados sejam identificados e corrigidos de forma mais rápida. Para isso, faz-se necessária a criação de indicadores, que vão dar a direção da efetividade da intervenção regulatória.

Considerando a dimensão dos processos em que o problema se localiza, a criação de apenas um indicador para medir o nível de maturidade das empresas quanto à segurança cibernética ou a quantidade de informações compartilhadas seria insuficiente para apontar de forma satisfatória se a intervenção foi ou não eficaz. Além disso, a dependência do porte dos agentes, das suas áreas de negócios e governança faz com que a avaliação não seja apenas quantitativa, mas tenha uma forte subjetividade atrelada.

Sugere-se também que possam ser estabelecidos mecanismos qualitativos para avaliação da intervenção regulatória dadas as características peculiares do problema regulatório. Esse tipo de monitoramento qualitativo compreenderia a percepção dos agentes do modelo como um todo, incluindo todos os subprocessos e suas melhorias.

6.0 CONCLUSÕES

A AIR tem como objetivo analisar previamente à edição de atos normativos, os possíveis efeitos e verificar a razoabilidade do impacto gerado, subsidiando assim a tomada de decisão. Considerando a importância da temática de segurança cibernética e o aumento da ocorrência de ataques cibernéticos sofridos pelos agentes do setor elétrico, torna-se necessário o estudo prévio da atuação da ANEEL no âmbito regulatório diante do problema identificado por meio do Relatório de AIR. Para esse fim, a aplicação da metodologia de *Design Thinking* mostra-se como uma ferramenta capaz de auxiliar o desenvolvimento da AIR de maneira interativa entre os participantes.

Conclui-se então que a Avaliação de Impacto Regulatório atingiu seus objetivos propostos inicialmente, desde a definição do problema regulatório até a melhor alternativa de solução.

7.0 REFERÊNCIAS BIBLIOGRÁFICAS

(1) ANEEL. Relatório de Análise de Impacto Regulatório (AIR) sobre segurança cibernética no Setor Elétrico Brasileiro. SICNET Processo nº 48500.000027/2020-40. Brasil.

(2) BACEN. Resolução CMN nº 4.893, de 26 de fevereiro de 2021. Brasil.

(3) ANATEL. Resolução Anatel nº 740, de 21 de dezembro de 2020. Brasil.

(4) GOVERNO FEDERAL. Diretrizes Gerais e Guia Orientativo para Elaboração de Análise de Impacto Regulatório - AIR. Brasil.

(5) AUSTRALIAN GOVERNMENT. Australian Government Guide to Regulation. Austrália.

DADOS BIOGRÁFICOS

(1) BRUNO DANIEL MAZETO
Possui graduação em Engenharia Elétrica - Ênfase em Telecomunicações pela Universidade de São Paulo (2007), graduação em Engenharia pela Ecole Centrale Paris (2006) e mestrado em Matemática pela Universidade de Brasília (2019). Atualmente é Especialista em Regulação da Agência Nacional de Energia Elétrica. Trabalhou de 2010 a 2011 como analista de infraestrutura no Ministério de Minas e Energia e de 2008 a 2010 na Peugeot Citroën Brasil.

(2) THELMA MARIA MELO PINHEIRO
Thelma Maria Melo Pinheiro, graduada em Engenharia Elétrica pela Universidade Federal do Ceará (1997) e mestrado em Engenharia Elétrica pela Universidade de Brasília (2012). Concluiu os cursos de especialização em Eficiência e Qualidade Energética (UFC, 2000), MBA em Gestão de Negócios em Energia Elétrica pela Fundação Getúlio Vargas (FGV, 2003) e MBA em Gestão Financeira e Controladoria (FGV, 2006). Atualmente é Especialista em Regulação da ANEEL e Coordenadora de Monitoramento e Procedimentos de Rede da Superintendência de Regulação dos Serviços de Transmissão. Tem experiência em Distribuição e Transmissão de Energia Elétrica, atuando na regulamentação e fiscalização da prestação dos serviços.

(3) MATEUS SOUSA PINHEIRO
Mateus Sousa Pinheiro, graduado em Gestão da Qualidade pela Unicesumar (2021) e graduando em Engenharia de Energia pela Universidade de Brasília. Atualmente é estagiário da Agência Nacional de Energia Elétrica (ANEEL), atuando na Coordenação de Monitoramento e Procedimentos de Rede da Superintendência de Regulação dos Serviços de Transmissão (SRT).

(4) SIDNEY MATOS
Sidney Matos da Silva, graduado em Engenharia Elétrica pela Universidade Veiga de Almeida (UVA, 2004), Pós-graduação lato sensu em Sistemas de Telecomunicações, por 16 anos é Especialista em Regulação da Agência Nacional de Energia Elétrica - ANEEL, tendo trabalhado na Superintendência de Gestão Tarifária, na Superintendência de Fiscalização Econômica e Financeira - SFF e atualmente na Superintendência de Regulação dos Serviços de Transmissão - SRT.

(5) LEONARDO MENDONÇA OLIVEIRA DE QUEIROZ
Engenheiro Eletricista graduado pela Universidade Federal de Goiás (UFG) em 2002, Mestre e Doutor pela Universidade de Campinas (Unicamp) em 2005 e 2010, respectivamente. Concluiu o curso Theory and Operation of

a Modern National Economy – Programa Minerva, pela George Washington University (2012) e Especialização em Análise de Impacto Regulatório (AIR) pela UnB (2017). Desde 2007 é especialista em regulação na ANEEL, tendo atuado na Superintendência de Regulação da Distribuição – SRD como coordenador da Qualidade da Energia, desde 2017 na Superintendência de Regulação dos Serviços de Transmissão como superintendente adjunto e, em 2018, como titular da unidade.

(6) VICTOR MATHEUS PASSAMANI OLIVEIRA
Graduando em Engenharia Elétrica pela Universidade de Brasília (UnB). Com conhecimentos na análise de casos concretos relativos à aplicação dos regulamentos do serviço de transmissão de energia elétrica, nas atividades de monitoramento e avaliação da regulamentação do serviço de transmissão e na área de energia solar fotovoltaica. Já estagiou na Superintendência de Regulação dos Serviços de Transmissão na Agência Nacional de Energia Elétrica (ANEEL).

(7) SANDOVAL FEITOSA
Servidor Público Federal da ANEEL desde 2005. Em 2014 ocupou o cargo de Assessor da Diretoria da ANEEL, em 2015, assumiu cargo de Superintendente de Regulação dos Serviços de Transmissão, em 2017 tornou-se superintendente de Fiscalização dos Serviços de Eletricidade, e em 2018, foi nomeado para o cargo de Diretor da ANEEL. Mestre em Engenharia Elétrica- Regulação Técnica e Econômica de Transmissão de Energia Elétrica pela UnB (2009), pós-graduado em Administração de Empresas com ênfase em Estratégia pela FGV (2017), e graduado em Engenharia Elétrica pela UFMA (2002). Antes de trabalhar na ANEEL, atuou na Cemar e também na Chesf.

(8) RENATO ABDALLA AFONSO
Engenheiro Eletricista e Mestre em Sistemas Elétricos de Potência, ambos pela Universidade de Brasília (UnB). É servidor público ocupante do cargo de especialista em regulação de serviços públicos de energia desde 2007. No período de 2007 a 2015, atuou na Superintendência de Fiscalização dos Serviços de Eletricidade como integrante da equipe de fiscalização dos serviços de transmissão de energia elétrica. Em 2015, assumiu a posição de coordenador substituto do Grupo de Instrução do Processo Decisório da SFE. De 2017 a junho de 2018, assumiu posição de coordenador desse mesmo grupo. É assessor da Diretoria da ANEEL desde junho de 2018.