NOTA TÉCNICA Nº 111/2021-SRT-SGI-SRD-SRG-SFE-SFG/ANEEL

Em 26 de novembro de 2021.

Processo: 48500.000027/2020-40

Assunto: **Análise das contribuições recebidas na 2ª Fase da Consulta Pública nº 007/2021, com intuito de coletar subsídios para a regulamentação sobre a segurança cibernética no Setor Elétrico Brasileiro.**

I - DO OBJETIVO

1. Analisar as contribuições recebidas na 2ª Fase da Consulta Pública nº 007/2021, que submeteu ao processo de participação social a minuta de Resolução Normativa (REN) responsável por dispor sobre as políticas de segurança cibernética a serem adotadas pelos agentes no Setor Elétrico Brasileiro.

II - DOS FATOS

2. O Decreto nº 9.637, de 26 de dezembro de 2018, instituiu a Política Nacional de Segurança da Informação (PNSI).

3. O Decreto nº 10.222, de 5 de fevereiro de 2020, aprovou a Estratégia Nacional de Segurança Cibernética.

4. Em 18 de maio de 2020, foi elaborada a Nota Técnica nº 50/2020-SRT-SGI-SRD-SRG/ANEEL[1], com objetivo de abertura de Tomada de Subsídios para obter contribuições sobre regulação cibernética no setor elétrico. Por meio do Aviso de Tomada de Subsídio nº 007/2020[2], foi aberto o período de contribuições de 25/5/2020 a 24/7/2020.

5. Em 9 de outubro de 2020, o Diretor Sandoval de Araújo Feitosa Neto foi sorteado como relator do Processo nº 48500.000027/2020-40.

6. O Decreto nº 10.569, de 9 de dezembro de 2020, aprovou a Estratégia Nacional de Segurança de Infraestruturas Críticas.

[1] SicNet nº 48552.000419/2020
SicNet nº 48542.001396/2020

7. Em 5 de março de 2021, a SRT concluiu a versão pré-participação pública do Relatório de Análise de Impacto Regulatório (AIR) nº 2/2021-SRT-SGI-SRD-SRG/ANEEL[3] sobre segurança cibernética no Setor Elétrico Brasileiro.

8. Por meio da Nota Técnica nº 20/2021-SRT-SGI-SRD-SRG/ANEEL[4], de 5 de março de 2021, foi recomendada a abertura de Consulta Pública visando coletar subsídios para Análise de Impacto Regulatório (AIR) sobre a segurança cibernética.

9. Na 7ª Reunião Pública Ordinária, realizada no dia 9 de março de 2021, a Diretoria Colegiada da ANEEL decidiu instaurar a 1ª Fase da Consulta Pública nº 007/2021, por meio de formulário eletrônico disponível no site da ANEEL no período de 11/3/2021 a 26/4/2021, com o objetivo de receber subsídios a respeito do Relatório de AIR sobre segurança cibernética.

10. O Decreto nº 10.748, de 16 de julho de 2021, instituiu a Rede Federal de Gestão de Incidentes Cibernéticos.

11. Por meio da Nota Técnica nº 77/2021-SRT-SGI-SRD-SRG-SFE-SFG/ANEEL[5], de 18 de agosto de 2021, foi recomendada a abertura de Consulta Pública visando coletar subsídios para a minuta de ato normativo da regulamentação sobre segurança cibernética no setor elétrico.

12. Na 32ª Reunião Pública Ordinária, realizada no dia 31 de agosto de 2021, a Diretoria Colegiada da ANEEL decidiu instaurar a 2ª Fase da Consulta Pública nº 007/2021, por meio de formulário eletrônico disponível no site da ANEEL no período de 1/9/2021 a 15/10/2021, com o objetivo de receber subsídios a respeito da minuta de REN sobre segurança cibernética no Setor Elétrico Brasileiro.

13. A Resolução do Conselho Nacional de Política Energética - CNPE nº 24, de 20 de outubro de 2021, aprovou as Diretrizes sobre Segurança Cibernética para o setor elétrico.

III - DA ANÁLISE

[3] SicNet nº 48552.000156/2021
[4] SicNet nº 48552.000155/2021
SicNet nº 48552.001036/2021

14. A 2ª Fase da CP nº 007/2021 recebeu 226 contribuições, com a participação dos 27 contribuintes abaixo:

ABDIB - Associação Brasileira da Infraestrutura e Indústrias de Base
ABRADEE
ABRAGE - Associação Brasileira das Empresas Geradoras de Energia Elétrica
Associação Brasileira das Empresas de Transmissão de Energia Elétrica
Associação Brasileira dos Comercializadores de Energia (Abraceel)
Centrais Elétricas Brasileiras S.A - ELETROBRAS
Centrais Elétricas do Norte do Brasil S.A. - Eletronorte
Companhia Energética de Minas Gerais
Conselho de Consumidores da Copel Distribuição
COPEL
CTEEP - COMPANHIA DE TRANSMISSÃO DE ENERGIA ELÉTRICA PAULISTA
Enel Brasil (Enel Cien, Enel SP, Enel CE, Enel GO e Enel RJ)
ENGIE Brasil Energia S.A.
Equatorial Energia
FIESP - FEDERAÇÃO DAS INDÚSTRIAS DO ESTADO DE SÃO PAULO
Furnas Centrais Elétricas SA
Grupo CPFL Energia
Instituto de Engenharia do Paraná
Lemon
Marcos Ohlweiler da Silva
Neoenergia S.A.
ONS - Operador Nacional do Sistema Elétrico
Siemens Energy
Siemens Infraestrutura e Indústria Ltda.
Sonda
TI SAFE SEGURANÇA CIBERNÉTICA INDUSTRIAL LTDA
Transmissora Aliança de Energia Elétrica S.A. (TAESA)

15. As contribuições foram feitas por meio de formulário eletrônico e destinadas à minuta de Resolução Normativa que dispõe sobre as políticas de segurança cibernética a serem adotadas pelos agentes do Setor Elétrico Brasileiro.

16. A maior parte das contribuições recebidas foi destinada ao art. 4º da minuta, representando mais de 27% do total. A Figura 1 ilustra a quantidade de contribuições recebidas para cada dispositivo.

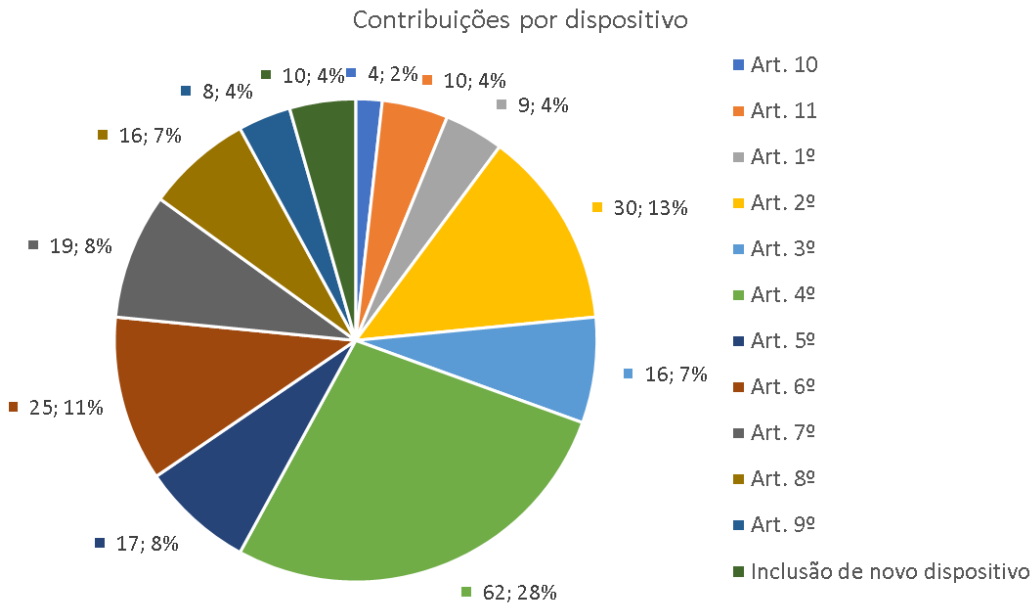

Figura 1 – Quantidade de contribuições para cada dispositivo no âmbito da 2ª Fase da CP nº 007/2021

III.1 - Art. 1º

17. O art. 1º recebeu contribuições diversificadas, com a maior parte focada em seu caput. Os contribuintes alertaram que a política proposta pela minuta de REN deveria abranger não somente a segurança cibernética, mas também a segurança da informação, deixando a cargo do agente a escolha do nome da política.

18. Outras contribuições recebidas tiveram como objetivo deixar clara a possibilidade de que os agentes podem contar com mais de uma política de segurança cibernética, trazendo a pluralidade para o termo utilizado na minuta.

19. Em relação ao nome da política, ficará a cargo do agente a escolha, porém, é importante esclarecer que a regulamentação da Segurança da Informação foge da competência da ANEEL. Assim, a resolução proposta refere-se à Segurança Cibernética.

20. Sobre haver mais de uma política de segurança cibernética, como se trata de um documento complexo e os agentes podem construir em várias partes, concordamos em deixar o texto no plural, conforme descrito na minuta de REN proposta.

III.2 - Art. 2º

21. O art. 2º recebeu contribuições com o intuito de incluir a segurança das vidas humanas e do meio ambiente como um comprometimento direto da ocorrência de um incidente cibernético. Além disso, algumas colaborações tinham como temática a definição do impacto de um incidente cibernético, com os contribuintes argumentando sobre o momento da definição e quais critérios para tal.

22. Porém, as contribuições foram predominantemente direcionadas para a definição de informações sensíveis. Os contribuintes sugeriram a troca do termo “sensíveis” por “críticas”, visando evitar conflito de conceito com o que é descrito pela Lei Geral de Proteção dos Dados (LGPD), Lei nº 13.709, de 2018.

23. Ademais, os participantes apontaram também a importância da definição de termos como “Rede de Informação” e “Rede de Operação”, propondo a inclusão de novos incisos no art. 2º.

24. Uma vez que a LGPD já define o termo “dados sensíveis” com conotação diversa daquela adotada nesta Resolução, concordamos em mudar o termo para “informações críticas”, conforme descrito na minuta de REN.

25. Além disso, foi acrescentada a definição de “rede de informação” para melhor esclarecimento dos termos empregados nesta Resolução. “Rede de operação” também é um termo já empregado no setor elétrico com conotação diversa da adotada na Resolução, assim, retiramos essa expressão.

III.3 - Art. 3º

26. O art. 3º recebeu manifestações dos contribuintes no sentido de especificar quais normas internacionais deveriam ser utilizadas pelos agentes em suas estruturas críticas no âmbito da cibersegurança. Por outro lado, outros participantes lembraram da importância de se levar em consideração as especificidades de cada ambiente tecnológico na aplicação da política de segurança cibernética.

27. A massiva contribuição, porém, foi direcionada para a necessidade da confidencialidade das informações sensíveis. Os participantes lembraram que a cooperação entre agentes deve prever tal aspecto, além de considerar o anonimato das empresas.

28. Uma vez que muitas contribuições trouxeram termos mais adequados e/ou mais abrangentes, incorporamos essas contribuições conforme descrito na minuta de REN.

29. Em relação ao anonimato das empresas, já tínhamos previsto isso no art. 7º, sobre compartilhamento de informações. Porém, dado que a confidencialidade das informações é muito importante para a segurança cibernética, trouxemos também para o art. 3º, sobre as diretrizes, para estender essa prática para toda a Resolução.

III.4 - Art. 4º

30. Por descrever quais itens a política de segurança cibernética dos agentes deve contemplar, o art. 4º foi o dispositivo que mais recebeu contribuições. As sugestões foram diversificadas, algumas apresentando um caráter mais prescritivo.

31. Entre as contribuições que sugeriam maiores detalhamentos, os participantes optaram por recomendações por parte da ANEEL para aplicação de modelos de maturidade. Além disso, outros sugeriram também uma forma mais específica de classificar dados e informações.

32. Alguns contribuintes citaram a necessidade de possuir um Plano de Resposta a Incidentes Cibernéticos, além de uma política que exigisse gestão de ativos da rede, backup seguro, rastreabilidade de acessos e monitoramento contínuo de ativos do SIN.

33. Por outro lado, outras contribuições alertavam que uma política não deve obter mecanismos, registros, controles ou procedimentos, assim como descrito nos incisos do art. 4º, mas sim apenas diretrizes que orientem a elaboração destes.

34. Conforme a minuta de REN resultante, muitas contribuições para melhoria de texto ou trazendo expressões mais adequadas para o contexto de Segurança Cibernética foram incorporadas. No entanto, outras contribuições foram negadas seguindo-se a premissa para este trabalho de evitar um regulamento excessivamente detalhado e prescritivo.

III.5 - Art. 5º

35. Grande parte das contribuições destinadas ao art. 5º foi direcionada à classificação das instalações. Os contribuintes reforçaram a necessidade de classificar os ativos de acordo com a sua criticidade ao invés do seu porte.

36. Além disso, outras colaborações lembraram da importância de atualizar e revisar as políticas de segurança cibernética sempre que necessário, além da própria ação periódica proposta na minuta de REN.

37. Da mesma forma que os art. 3º e art. 4º, houve muitas contribuições para melhoria de texto e para trazer expressões e termos mais adequados. Essas contribuições foram incorporadas na Resolução conforme minuta de REN.

III.6 - Art. 6º

38. O art. 6º recebeu contribuições no sentido de dividir em etapas a notificação dos casos de incidentes cibernéticos de maior impacto. De acordo com os contribuintes, é necessário que uma primeira notificação seja encaminhada à ANEEL ou à equipe de coordenação setorial designada e, após um determinado período, um relatório é encaminhado incluindo análise da causa e do impacto e respectivas ações de mitigação adotadas.

39. Ademais, outras colaborações apontavam a necessidade da centralização das notificações e a adoção de um sistema específico para o recebimento destas.

40. Essas contribuições foram de grande valia, porém, esclarecemos que o procedimento de notificação de incidentes cibernéticos de maior impacto não será detalhado na Resolução. Ele será disponibilizado posteriormente à publicação da norma no site da ANEEL.

41. Esclarecemos que o texto do art. 6º foi atualizado para ficar compatível com o art. 13 do Decreto nº 10.748, de 16 de julho de 2021, uma vez que deverá ser instituída ou designada a equipe de coordenação setorial.

III.7 - Art. 7º

42. As contribuições destinadas ao art. 7º em sua maioria também tratam sobre a necessidade da criação de um ambiente solidificado e seguro para o compartilhamento de informações sobre incidentes cibernéticos de maior impacto.

43. Uma vez que o compartilhamento de informações sobre ameaças e outras informações relativas à segurança cibernética, diferentemente com o que ocorre com a notificação à ANEEL de incidentes cibernéticos de maior impacto, envolve soluções de caráter técnico, em ambiente seguro e no qual é facultado o anonimato, é esperado que os agentes construam essas soluções de forma mais eficiente e adequada.

III.8 - Art. 8º

44. O art. 8º recebeu contribuições direcionadas aos custos trazidos pela adequação por parte dos agentes ao que é determinado na Resolução Normativa. Os agentes exigiram ressarcimento desses custos, alegando investimentos de grande montante para tal adequação.

45. Além disso, outras contribuições foram recebidas e tinham como objetivo expandir o escopo da norma para outros órgãos e terceiros, não se limitando apenas aos agentes do setor elétrico.

46. As contribuições relativas a custo, da forma como inseridas pelos contribuintes, não foram acatadas, pois o art. 8º refere-se a gastos que os agentes poderão incorrer independentemente da forma ou possibilidade de reconhecimento. Destacamos que os gastos necessários para a operação ou prestação do serviço são tratados conforme a regulação vigente de cada segmento.

III.9 - Art. 9º

47. As contribuições direcionadas ao art. 9º foram relacionadas também com o compartilhamento de informações e à aplicação do modelo de maturidade. Os contribuintes questionaram como seria feito o envio destas informações e quais modelos de maturidade adotar.

48. Outros contribuintes apontaram também a importância de manter os registros das informações pedidas nos incisos I, II e III da minuta de REN.

49. Da mesma forma que o art. 6º, essas contribuições são válidas, porém, esclarecemos que o procedimento de envio de informações à ANEEL não será detalhado na Resolução. Ele será disponibilizado posteriormente à publicação da norma no site da ANEEL. Cabe ressaltar que é exigido manter registro dessas informações, assim incorporamos essas contribuições na minuta de norma.

III.10 - Art. 10 e Art. 11

50. O art. 10 recebeu contribuições no sentido de diminuir o prazo para desenvolvimento da Avaliação de Resultado Regulatório (ARR), tendo em vista a velocidade das mudanças tecnológicas e do risco de incidentes cibernéticos.

51. De acordo com os resultados do monitoramento da regulamentação, a ANEEL irá avaliar o comportamento dos indicadores. Portanto, caso necessário, o tempo para desenvolvimento da ARR será revisto.

52. Por definir o prazo da entrada em vigor da Resolução, o art. 11, de maneira geral, recebeu contribuições pedindo o aumento do prazo, com argumentos acerca da complexidade das adequações ao que foi disposto na minuta da REN, além dos prazos referentes à Rotina Operacional RO-CB.BR.01, estabelecida pelo ONS.

53. A resolução proposta traz as diretrizes gerais e conteúdo mínimos para as políticas de segurança cibernética, ambos baseados nas experiências e boas práticas verificadas no setor. Com base nas coletas de dados realizadas neste trabalho, consideramos que grande parte dos agentes já cumpre com as disposições do normativo. Adicionalmente, o assunto tem caráter urgente e é relevante para o setor elétrico, de forma tal que o prazo proposto para vigência da norma será mantido. Sobre a Rotina Operacional, ela diz respeito a outros itens operativos de âmbito exclusivo do ONS, portanto, não cabe necessariamente uma compatibilização de prazos.

54. O gráfico a seguir representa o aproveitamento das contribuições propostas pelos agentes no âmbito da 2ª Fase da CP nº 007/2021.

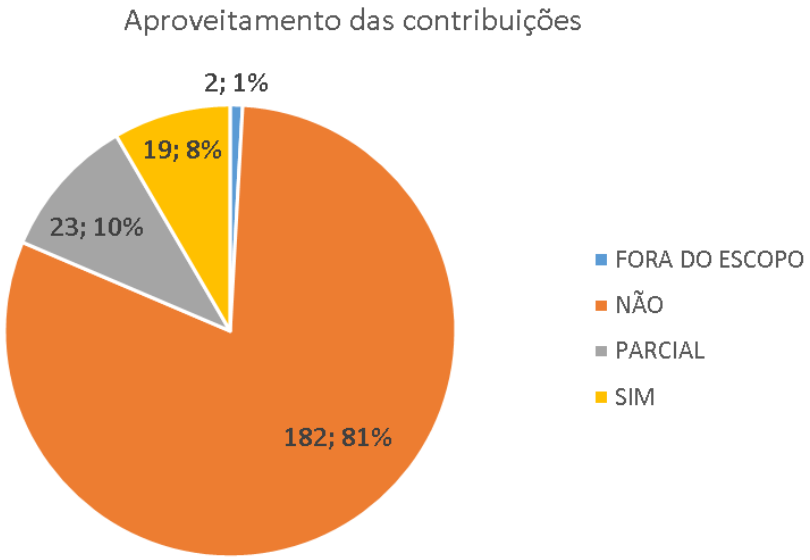

Figura 2 – Resultado do aproveitamento das contribuições da 2ª Fase da CP nº 007/2021

55. A Figura 2 demonstra que a maioria das contribuições recebidas no âmbito da CP nº 007/2021 não foram aproveitadas. Contudo, cabe ressaltar que houve grande concentração de contribuições semelhantes ou mesmo repetidas nos seguintes assuntos: detalhamento da notificação

sobre incidentes de maior impacto (art. 6º) e do envio de informações (art. 9º); reconhecimento de custos (art. 8º); menor prazo para elaboração da ARR (art. 10) e maior prazo para vigência do regulamento (art. 11); que foram negadas pelos motivos já explicados. Além disso, houve muitas contribuições sugerindo que fossem definidas diretrizes em vez de procedimentos (art. 4º), que também foram negadas, conforme o RAC em anexo.

56. Contudo, reafirmamos a importância das contribuições aceitas, no sentido de construir um regulamento como termos mais precisos, abrangentes e adequados à segurança cibernética do Setor Elétrico Brasileiro. Assim, a 2ª fase da Consulta Pública nº 007/2021 foi de grande importância para construir um regulamento mais robusto.

IV - DO FUNDAMENTO LEGAL

57. Esta Nota Técnica está fundamentada no Decreto nº 9.637/2018; no Decreto nº 10.222/2020; e no Decreto nº 10.569/2020.

V - DA CONCLUSÃO

58. Foram analisadas as contribuições recebidas no âmbito da 2ª Fase da Consulta Pública nº 007/2021 acerca da minuta de Resolução Normativa sobre segurança cibernética no Setor Elétrico Brasileiro.

59. A análise detalhada das contribuições, Relatório de Análise de Contribuições (RAC), à 2ª Fase da Consulta Pública nº 007/2021 consta do Anexo Técnico I desta Nota Técnica.

60. Com base no disposto nesta Nota Técnica, propõe-se a emissão da Resolução Normativa, conforme Anexo II desta Nota Técnica.

VI - DA RECOMENDAÇÃO

61. Recomenda-se encaminhamento deste processo ao Diretor-relator para posterior deliberação da Diretoria sobre a emissão da Resolução Normativa sobre a segurança cibernética no setor elétrico.

(Assinado digitalmente)
BRUNO DANIEL MAZETO
Especialista em Regulação - SRT

MATEUS SOUSA PINHEIRO
Estagiário - SRT

(Assinado digitalmente)
SIDNEY MATOS DA SILVA
Especialista em Regulação -SRT

(Assinado digitalmente)
THELMA MARIA MELO PINHEIRO
Especialista em Regulação – SRT

(Assinado digitalmente)
RODRIGO VARGAS BEZERRA
Técnico em Administração – SGI

(Assinado digitalmente)
LUIZ HENRIQUE CAPELI
Especialista em Regulação – SRD

(Assinado digitalmente)
IGO RODRIGUES DE CASTRO
Analista Administrativo – SGI

(Assinado digitalmente)
ESILVAN CARDOSO DOS SANTOS
Especialista em Regulação – SFE

(Assinado digitalmente)
JAYME MILANEZI JUNIOR
Especialista em Regulação – SRG

(Assinado digitalmente)
IZUMI RENATA SANTOS TAKADA MARWELL
Especialista em Regulação – SRG

(Assinado digitalmente)
MARCELO PEREIRA MENDES
Especialista em Regulação – SFG

(Assinado digitalmente)
SÉRGIO RIBEIRO LEITE
Especialista em Regulação – SFG

(Assinado digitalmente)
SAULO RABELO DE MARTINS CUSTODIO
Especialista em Regulação – SFE

De acordo:

(Assinado digitalmente)
LEONARDO MENDONÇA OLIVEIRA DE QUEIROZ
Superintendente de Regulação dos Serviços de Transmissão – SRT

(Assinado digitalmente)
CARLOS ALBERTO CALIXTO MATTAR
Superintendente de Regulação dos Serviços de Distribuição – SRD

(Assinado digitalmente)
ALESSANDRO D'AFONSECA CANTARINO
Superintendente de Regulação dos Serviços de Geração – SRG

(Assinado digitalmente)
ISSAO HIRATA
Superintendente de Gestão Técnica da Informação – SGI

(Assinado digitalmente)
GIÁCOMO FRANCISCO BASSI ALMEIDA
Superintendente de Fiscalização dos Serviços de Eletricidade – SFE

(Assinado digitalmente)
GENTIL NOGUEIRA DE SÁ JUNIOR
Superintendente de Fiscalização dos Serviços de Geração – SFG

ANEEL
AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA

ANEXO II - MINUTA DE RESOLUÇÃO NORMATIVA

AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA – ANEEL

RESOLUÇÃO NORMATIVA ANEEL Nº , DE (DIA) DE (MÊS) DE (ANO)

Dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica.

O DIRETOR-GERAL DA AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA – ANEEL, no uso de suas atribuições regimentais, de acordo com a deliberação da Diretoria, tendo em vista o disposto no art. 6º da Lei nº 8.987, de 13 de fevereiro de 1995, na Lei nº 9.427, de 26 de dezembro de 1996, no Decreto nº 2.335, de 6 de outubro de 1997, no art. 13 da Lei nº 9.648, de 27 de maio de 1998, no art. 4º da Lei nº 10.848, de 15 de março de 2004, no Decreto nº 10.222, de 5 de fevereiro de 2020, no Decreto nº 10.748, de 16 de julho de 2021, e o no que consta do Processo nº 48500.000027/2020-40, resolve:

Art. 1º Estabelecer as diretrizes e o conteúdo mínimo das políticas de segurança cibernética a serem adotados pelos agentes do setor de energia elétrica.

Parágrafo único. Sujeitam-se ao disposto nesta Resolução:

I - os concessionários, os permissionários e os autorizados de serviços ou instalações de energia elétrica; e

II - as entidades responsáveis pela operação do sistema, pela comercialização de energia elétrica ou pela gestão de recursos provenientes de encargos setoriais.

DEFINIÇÕES

Art. 2º Para fins do disposto nesta Resolução, considera-se:

I - incidente cibernético: ocorrência que comprometa, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema, que poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que constitua violação de norma, política de segurança, procedimento de segurança ou política de uso;

II - incidente cibernético de maior impacto: é estabelecido com base na classificação de severidade que consta do processo de gestão de riscos de segurança da informação do agente;

III - informações críticas: são aquelas com potencial de impacto negativo na prestação de serviços à população, em caso de comprometimento; e

IV - rede de informação: rede corporativa de dados da empresa, composta por toda infraestrutura de telecomunicações própria e de terceiros destinada aos ativos de Tecnologia da Informação.

DIRETRIZES GERAIS

Art. 3º As diretrizes para a atuação em segurança cibernética são:

I - adotar normas, padrões e referências de boas práticas em segurança cibernética;

II - atuar com responsabilidade, zelo e transparência;

III - disseminar a cultura de segurança cibernética;

IV - buscar a utilização segura das redes e serviços de energia elétrica;

V - identificar, proteger, diagnosticar, responder e recuperar os incidentes cibernéticos;

VI - identificar, avaliar, classificar e tratar os riscos cibernéticos na estrutura estabelecida pelo agente; e

VII - buscar a cooperação entre os diversos agentes envolvidos com fins de mitigação dos riscos cibernéticos, respeitadas as regras de confidencialidade das informações definidas pelo agente.

POLÍTICAS DE SEGURANÇA CIBERNÉTICA

Art. 4º As políticas de segurança cibernética devem contemplar, no mínimo:

I - os objetivos de segurança cibernética, dispondo sobre a capacidade para prevenir, detectar, responder e reduzir a vulnerabilidade a incidentes cibernéticos;

II - a aplicação com periodicidade anual de pelo menos um modelo de maturidade em segurança cibernética;

III - a classificação dos dados e das informações quanto à relevância;

IV - os procedimentos e os controles para reduzir a vulnerabilidade a incidentes e atender aos demais objetivos de segurança cibernética;

V - as medidas técnicas, incluindo aquelas de rastreabilidade da informação, que busquem garantir a segurança das informações críticas;

VI - o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes de maior impacto para suas atividades, abrangendo inclusive informações recebidas de empresas prestadoras de serviços a terceiros;

VII - a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações críticas ou que sejam relevantes para a condução das atividades operacionais em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pelo próprio agente;

VIII - a definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes cibernéticos;
IX - os mecanismos para disseminação da cultura de segurança cibernética, incluindo:

a) a implementação de programas de capacitação e de avaliação periódica de pessoal;

b) o plano de ação com medidas para a conscientização e educação de seus usuários sobre aspectos de segurança cibernética; e

c) o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

X - as simulações de cenários e ameaças para testes de resiliência, de análise das ferramentas e da capacidade e tempo de resposta;

XI - os mecanismos para prevenir, mitigar e recuperar incidentes cibernéticos em sua Rede de Informação ou na rede das instalações, e para impedir que os incidentes afetem a operação; e

XII - os procedimentos para prevenção, tratamento e resposta a incidentes cibernéticos.

Parágrafo único. Os procedimentos e os controles devem ser aplicados, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas em suas atividades.

Art. 5º As políticas de segurança cibernética devem ser aderentes às diretrizes dispostas neste Regulamento, e ainda:

I - ser compatível com a relevância da instalação no contexto do SIN, a natureza e a complexidade dos serviços, atividades, processos e sistemas;

II - ser compatível com a sensibilidade dos dados e das informações sob sua responsabilidade;

III - ser disseminada aos profissionais e colaboradores das áreas afetas, em seus diversos níveis, papéis e responsabilidades, resguardando-se o compartilhamento de informações críticas apenas para as pessoas que exerçam diretamente atividades de planejamento e execução da política, no que couber;

IV - estabelecer responsabilidades pela aplicação da política, com a identificação de pessoas e áreas competentes, bem como ponto focal para contato em eventuais urgências;

V - designar dirigente responsável pela política de segurança cibernética, o qual pode desempenhar outras funções, desde que não haja conflito de interesses;

VI - ser aprovada pelo Conselho de Administração ou órgão de deliberação colegiado equivalente;

VII - ser revisada e atualizada periodicamente ou sempre que necessário; e

VIII - estar disponível à ANEEL sempre que solicitada, juntamente com os documentos complementares e os comprovantes de sua aprovação interna pelo órgão competente.

Parágrafo único. Caso a estrutura de governança da política de segurança cibernética seja única para o grupo econômico, deve ser identificado o agente responsável, em níveis e funções, quando aplicável.

NOTIFICAÇÃO DE INCIDENTES CIBERNÉTICOS

Art. 6º Os agentes devem notificar a equipe de coordenação setorial designada dos incidentes cibernéticos de maior impacto que afetem de maneira substancial a segurança das instalações, a operação ou os serviços aos usuários ou de dados.

§ 1º A notificação do incidente cibernético de maior impacto deve incluir análise da causa e do impacto, bem como ações de mitigação adotadas, conforme o caso.

§ 2º A notificação do incidente cibernético de maior impacto não exclui o atendimento de outras obrigações de comunicação previstas em leis, normas e regulamentos.

§3º A notificação deve ser realizada assim que o agente tiver ciência do incidente e de sua dimensão.

COMPARTILHAMENTO DE INFORMAÇÕES

Art. 7º Os agentes devem adotar procedimento de compartilhamento de informações sobre ameaças e outras informações relativas à segurança cibernética de forma sigilosa e não discriminatória, sendo facultado o anonimato.

§ 1º O compartilhamento de informações não pode ser restrito às empresas do mesmo grupo societário, caso exista.

§ 2º O compartilhamento de informações não compreende aquelas classificadas pelo agente como críticas ou que possam comprometer a sua própria segurança.

DISPOSIÇÕES GERAIS

Art. 8º A segurança das instalações e a continuidade na prestação do serviço é responsabilidade dos agentes do setor elétrico, sendo assim, a adoção e execução da política de segurança cibernética e demais condutas e procedimentos exigidos neste Regulamento são de ônus dos agentes.

Art. 9º Os agentes devem manter registros e enviar para a ANEEL ou para a equipe de coordenação setorial designada as seguintes informações sempre que solicitadas:

I - os resultados dos modelos de maturidade aplicados em formato a ser definido;

II - os riscos cibernéticos identificados, com a respectiva forma de tratamento; e

III - os dados das equipes de prevenção, tratamento e resposta a incidentes cibernéticos.

Art. 10. Esta Norma será objeto de Avaliação de Resultado Regulatório (ARR) decorridos 7 (sete) anos de vigência.

Art. 11. Esta Resolução entra em vigor 180 dias após a data da publicação.

ANDRÉ PEPITONE DA NÓBREGA