

AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA – ANEEL

RESOLUÇÃO NORMATIVA ANEEL Nº 964, DE 14 DE DEZEMBRO DE 2021

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

[Voto](#)

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, dispendo 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 afetadas, 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 em 1º de julho de 2022.

ANDRÉ PEPITONE DA NÓBREGA

Este texto não substitui o publicado no D.O. de 22.12.2021, seção 1, p. 287, v. 159, n. 240.