AGÊNCIA NACIONAL DE ENERGIA ELETRICA – ANEEL

PORTARIA N° 6.143, DE 26 DE NOVEMBRO DE 2019

Aprova a Revisão 03 da Norma de Organização ANEEL n° 012, de 15 de julho de 2004, que estabelece as Diretrizes Básicas da Política de Segurança da Informação e Comunicações a serem observados no âmbito da Agência Nacional de Energia Elétrica - ANEEL.

Voto

O DIRETOR-GERAL DA AGÊNCIA NACIONAL DE ENERGIA ELETRICA – ANEEL, no uso de suas atribuições regimentais, de acordo com deliberação da Diretoria, tendo em vista o disposto no art. 7º, inciso IX, e no art. 9°, do Regimento Interno da ANEEL, aprovado pela Portaria n° 349, de 28 de novembro de 1997, do Ministério de Minas e Energia, considerando o que consta no Processo nº 48500.004225/2003-10 e a necessidade de revisão das normas relativas às ações de Segurança da Informação a serem executadas pela ANEEL, resolve:

Art. 1º Aprovar a Revisão 03 da Norma de Organização ANEEL nº 012, de 15 de julho de 2004, conforme o Anexo desta Portaria, estabelecendo as Diretrizes Básicas da Política de Segurança da Informação e Comunicações (PoSIC) da ANEEL.

Art. 2° Fica revogada a Portaria nº 3.522, de 28 de abril de 2015.

Art. 3° Esta Portaria entra em vigor na data de sua publicação.

ANDRÉ PEPITONE DA NÓBREGA

ANEXO À PORTARIA Nº 6143, DE 26 DE NOVEMBRO DE 2019

NORMA DE ORGANIZAÇÃO ANEEL Nº 012
REVISÃO 03

TÍTULO I
DAS DISPOSIÇÕES GERAIS

CAPÍTULO I DO OBJETIVO

Art. 1º Esta Norma dispõe sobre as Diretrizes Básicas da Política de Segurança da Informação e Comunicações (PoSIC), a serem cumpridas no âmbito da Agência Nacional de Energia Elétrica – ANEEL, referentes ao conjunto de medidas de proteção que, quando aplicado aos ativos de informações, possa proporcionar à ANEEL garantia aos Princípios de Segurança da Informação, consistindo estes nos princípios da confidencialidade, integridade, disponibilidade, autenticidade e não- repúdio.

CAPÍTULO II DOS PRÍNCIPIOS

Art. 2º A Agência atua em conformidade com os princípios estabelecidos no art. 1º nesta Norma, observando os princípios da legalidade, da impessoalidade, da moralidade, da publicidade, da eficiência, da finalidade, do interesse público e da motivação dos atos administrativos.

Art. 3º As Diretrizes Básicas da Política de Segurança da Informação e Comunicações da ANEEL referem-se:

I - aos aspectos estratégicos, estruturais e organizacionais, preparando a base para elaboração dos documentos normativos que as incorporarão; e

II - aos requisitos de segurança humana, física e lógica que dão sustentação aos procedimentos, dos processos de trabalho e dos ativos de informação que influirão diretamente nos produtos e serviços ofertados pela ANEEL.

CAPÍTULO III
DAS RESPONSABILIDADES

Art. 4º As responsabilidades para a gestão da segurança da informação e comunicações são atribuídas da seguinte forma:

I – Comissão Permanente de Avaliação de Documentos Sigilosos – CPADS: órgão colegiado, nomeado pela Diretoria da ANEEL, responsável pelo cumprimento das determinações legais pertinentes ao acesso a documentos de caráter sigiloso e pela análise periódica dos documentos

sob custódia da ANEEL, submetendo à Diretoria proposta motivada de classificação dos documentos a terem tratamento sigiloso, bem como dos procedimentos a serem adotados na sua tramitação e os prazos para sua desclassificação;

II – Comissão de Gestão da Informação - CGI: órgão colegiado, nomeado pela Diretoria da ANEEL, responsável por analisar e propor medidas para efetiva aplicação, disseminação e aprimoramento da Política de Segurança da Informação e Comunicações da ANEEL;

III – Superintendência de Gestão Técnica da Informação – SGI: recomendar e regulamentar a operacionalização dos normativos provenientes da Política de Segurança da Informação e Comunicações, por meio da elaboração de normas e procedimentos complementares no âmbito da Tecnologia da Informação;

IV - Superintendência de Administração e Finanças – SAF: executar as atividades pertinentes à segurança física do ambiente e patrimonial dos ativos de informação;

V – Superintendência de Recursos Humanos – SRH: executar as ações de Treinamento e Desenvolvimento – T&D referentes à segurança da informação, bem como àquelas referentes a recursos humanos que interajam com os processos de ativos de informação;

VI – Assessoria Institucional da Diretoria – AID: executar as atividades relacionadas à comunicação institucional, divulgando e disseminando as orientações emanadas pela Política de Segurança da Informação e Comunicações;

VII – demais Unidades Organizacionais: executar as ações necessárias sob suas responsabilidades que interajam com a Política de Segurança da Informação;

VIII – colaboradores: observar e acatar as recomendações para a utilização segura dos recursos dos ativos de informação e, em caso de dúvidas ou problemas, contatar a área da SGI de suporte técnico em informática aos colaboradores da ANEEL;

IX – administradores de serviço: observar e acatar as recomendações para utilização segura dos acessos privilegiados concedidos para a administração dos recursos da Tecnologia da Informação.

X – Gestor de Segurança da Informação e Comunicação: coordenar as ações de segurança da informação e comunicações necessárias para a garantia de cumprimento da Política de Segurança da Informação e Comunicações da Agência;

XI – Comitê de Segurança da Informação e Comunicação: assessorar na implementação das ações de segurança da informação e comunicações no âmbito da Agência.

Art. 5º As determinações contidas nas regras e diretrizes são obrigatórias e necessárias.

TÍTULO II
DA CONCEITUAÇÃO

Art. 6º Para fins de uniformidade dos procedimentos contidos nesta Norma, são adotados os conceitos a seguir:

I – acesso privilegiado: acesso que permite ao administrador de serviço sobrepor controles do sistema de informação e somente deve ser concedido àqueles que o necessitam para a condução de suas atividades;

II – administrador de serviços: colaborador que possui acesso privilegiado para a utilização e disponibilização, por força de suas funções, de recursos restritos de Tecnologia da Informação;

III – ativo de informação: compreende os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas a que eles têm acesso;

IV – autenticidade: garantia de que o dado ou informação é verdadeiro e fidedigno tanto na origem quanto no destino;

V – colaborador: agente público em exercício na ANEEL podendo ser titular de cargo efetivo ou em comissão, contratado por tempo determinado ou prestador de serviço terceirizado;

VI – computação em nuvem: modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (redes de computadores servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

VII – confidencialidade: garantia do acesso autorizado a informações, de acordo com o nível de proteção, devendo a ANEEL regular sua classificação;

VIII – disponibilidade: garantia de que os colaboradores possam ter acesso a informações segundo sua demanda e em conformidade com a Política de Segurança da Informação e Comunicações da Agência;

IX – gestão de riscos de segurança da informação e comunicações: conjunto de processos que permitem identificar as medidas de proteção necessárias para minimizar ou eliminar os riscos de segurança da informação e comunicações a que estão sujeitos os ativos de informação;

X – informação: dados, processados ou não, que podem ser utilizados para produção e transmissão do conhecimento, contidos em qualquer meio, suporte ou formato;

XI – informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

XII – infraestruturas críticas da informação: subconjunto dos ativos de informação que afetam diretamente a consecução e continuidade do cumprimento da Missão da Agência.

XIII – integridade: garantia de que as informações e métodos de processamento somente sejam alterados mediante ações planejadas e autorizadas;

XIV – medidas de proteção: medidas destinadas a garantir o sigilo, quando necessário, a inviolabilidade, a integridade, a autenticidade, a legitimidade e a disponibilidade de dados e informações, com o objetivo de prevenir, detectar, anular ou registrar ameaças reais ou potenciais a dados e informações;

XV – não-repúdio: garantia de que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação;

XVI – plano de continuidade: plano que descreve as ações que uma organização deve tomar para assegurar a continuidade dos processos críticos em caso de falhas nos sistemas, incluindo a ativação de processos manuais, duplicidade de recursos e acionamento de fornecedores;

XVII – Política de Segurança da Informação e Comunicações: recomendações com o propósito de estabelecer critérios para o adequado manuseio, armazenamento, transporte e descarte das informações através do desenvolvimento de Diretrizes, Normas, Procedimentos e Instruções destinadas, respectivamente, aos níveis estratégico, tático e operacional;

XVIII – princípios da segurança da informação e comunicações: princípios da confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio, que regem a segurança da informação, de acordo com o art. 3° do Decreto n° 3.505, de 13 de junho de 2000;

XIX – rede de comunicação de dados: conexão de dois ou mais computadores, ligados entre si através de um ou um conjunto de protocolo(s) de comunicação, permitindo a troca de informações e o compartilhamento de recursos;

XX – redes sociais: estruturas sociais digitais compostas por pessoas ou organizações conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.

XXI – termo de responsabilidade: acordo de confidencialidade para não divulgação ou uso indevido de informações, atribuindo responsabilidades ao colaborador e administrador de serviço quanto ao sigilo e a correta utilização dos ativos de propriedade ou custodiados pela ANEEL.

TÍTULO III DAS DIRETRIZES

CAPÍTULO I
DOS REQUISITOS

Art. 7º As Diretrizes Básicas da Política de Segurança da Informação e Comunicações da ANEEL devem atender às seguintes normas, além daquelas de caráter geral que disponham sobre a matéria:

I - a Lei nº 9.983, de 14 de julho de 2000, que dispõe sobre a responsabilidade civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

I - a Lei nº 9.983, de 14 de julho de 2000, que dispõe sobre a responsabilidade civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

II - a Lei 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal e dá outras providências;

III – a Lei 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para uso da Internet do Brasil;

IV - o Decreto 7.724, de 16 de maio de 2012, que regulamenta a Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição;

V - o Decreto 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

VI - a Lei 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014;

VII - o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam

comprometer a segurança nacional.

VIII - Instrução Normativa nº 01/DSIC/GSIPR, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, bem como às demais Normas Complementares a ela elaboradas pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança da Informação da Presidência da República;

IX - a NBR/ISO/IEC 27001:2013 da ABNT - Técnicas de Segurança - Sistemas de Gestão de Segurança da Informação – Requisitos; e

X - a NBR/ISO/IEC 27002:2013 da ABNT - Código de Prática para Controles de Segurança da Informação;

CAPÍTULO II
DA CAPACITAÇÃO E DO APERFEIÇOAMENTO

Art. 8º As Diretrizes Básicas da Política de Segurança da Informação e Comunicações devem ser divulgadas nas Unidades Organizacionais, garantindo que todos tenham consciência da política e a pratiquem na organização.

Parágrafo único. Todos os colaboradores devem obedecer ao disposto nas Diretrizes Básicas da Política de Segurança da Informação e Comunicações, recebendo as informações necessárias para o seu adequado cumprimento.

Art. 9º Os colaboradores devem ser continuamente capacitados para o uso dos ativos de informação quando da realização de suas atividades.

Art. 10. Programas de conscientização sobre segurança da informação e comunicações serão implementados através de treinamentos específicos, assegurando que todos os colaboradores sejam informados sobre os potenciais riscos de segurança e o tipo de exposição a que estão submetidos os sistemas de informações, as comunicações e operações da ANEEL e suas partes interessadas.

Art. 11. Os treinamentos a serem disponibilizados devem estar compatíveis com as tecnologias atualmente implementadas no ambiente informatizado, e pelas demais que porventura venham a ser adotadas.

CAPÍTULO III
DO ACESSO, PROTEÇÃO E GUARDA DA INFORMAÇÃO

Art. 12. A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade.

Parágrafo único. Os ativos de informação e suas infraestruturas críticas a serem protegidos deverão ser priorizados e seus riscos deverão ser gerenciados por meio de adequado processo de gestão de riscos de segurança da informação e comunicação.

Art. 13. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela ANEEL é considerada seu patrimônio e deve ser protegida conforme estabelecido nesta Norma.

Parágrafo único. Qualquer falha na segurança da informação, identificada por qualquer colaborador, deve ser imediatamente comunicada ao seu superior imediato, que a encaminhará à CGI para avaliação e determinação das ações que se fizerem necessárias.

Art. 14. É vedado o controle exclusivo, por apenas um colaborador, de um processo de negócio ou recurso.

Art. 15. Todos os colaboradores que manipulem ou tenham acesso a informações sigilosas de propriedade da ANEEL devem assinar termo de responsabilidade, visando garantir a adequada confidencialidade delas.

Art. 16. As violações de segurança da informação e comunicações devem ser registradas e, esses registros, analisados periodicamente para os propósitos de caráter corretivo, legal e de auditoria.

CAPÍTULO IV
DA UTILIZAÇÃO DOS ATIVOS DE INFORMAÇÃO

Art. 17. Os ativos de informação disponibilizados são fornecidos com o propósito único de garantir o desempenho das atividades da ANEEL, sendo vedado aos colaboradores o uso desses ativos para constranger, assediar, ofender, caluniar, ameaçar ou causar prejuízos a qualquer pessoa física ou jurídica, veicular opiniões político-partidárias e quaisquer outras atividades que contrariem os objetivos institucionais da ANEEL.

Art. 18. Os acessos à rede de comunicação de dados da ANEEL, ou mesmo àquelas redes externas proporcionadas por meio desta, são gerenciados em todos os tipos de conexão, devendo os colaboradores ser identificados e ter acessos apenas às informações e aos recursos tecnológicos necessários ao desempenho de suas atividades.

Parágrafo único. A eventual possibilidade de o colaborador ou administrador de serviço acessar os ativos de informação que não sejam necessários ao desempenho de suas atividades não o isenta, de forma nenhuma, da responsabilidade pelo adequado uso destes, conforme disposto nesta ou em outras normas da Administração Pública Federal.

Art. 19. Todos os ativos de informação devem ser inventariados, com identificação patrimonial e de seus responsáveis, bem como a definição de suas configurações, manutenções e documentações pertinentes.

Parágrafo único. Todo o ativo de informação deve ser protegido e conservado, de forma a preservar os seus componentes internos e externos.

CAPÍTULO V
DA COMUNICAÇÃO ELETRÔNICA

Art. 20. Toda informação veiculada eletronicamente, utilizando a rede de comunicações de dados da ANEEL, está sujeita ao controle e à monitoração, eventual ou permanente.

§ 1° A Política de Segurança da Informação e Comunicações da ANEEL prevê mecanismos que visem a garantir e proteger a informação quanto à autenticidade e ao não-repúdio.

§ 2° Procedimentos complementares para o tratamento e resposta de incidentes de segurança da informação em redes de comunicações de dados devem ser mantidos, com o objetivo de evitar ou mitigar os impactos deles decorridos.

CAPÍTULO VI
DA SEGURANÇA FÍSICA E DO AMBIENTE E DE RECURSOS HUMANOS

Art. 21. Tendo em vista a necessidade de se garantir a segurança física e do ambiente, bem como a segurança de recursos humanos, a ANEEL estabelecerá controles, visando a:

I - prevenir o acesso físico indevido e sem autorização, bem como danos e interferências com as instalações e informações da ANEEL; e

II – assegurar que os colaboradores, fornecedores e terceiros entendam suas responsabilidades e assinem acordos sobre seus papéis e responsabilidades pela segurança da informação e comunicações, com a finalidade de reduzir os riscos de erros humanos, furto, roubo, apropriação indébita, fraude, ou uso indevido dos ativos de informações da ANEEL.

CAPÍTULO VII
DO PLANO DE CONTINUIDADE

Art. 22. Os procedimentos que garantam a continuidade e a recuperação do fluxo de informações devem ser mantidos, observando-se as classificações de disponibilidades requeridas, de forma a não permitir a interrupção das atividades de negócios e proteger os processos críticos contra falhas e danos, que atenderão aos seguintes objetivos:

I - implementação de medidas de proteção necessárias para minimizar ou eliminar os riscos de segurança da informação e comunicações identificados e avaliados a que estão sujeitos os ativos de informação e suas infraestruturas críticas;

II - avaliação em regime emergencial das consequências de desastres, falhas de segurança da informação e comunicações, perda de serviços e ativos de informação;

III - contingência e recuperação do funcionamento normal dentro de períodos de tempos determinados dos ativos de informações e infraestruturas críticas da informação; e

IV- recuperação tempestiva das operações consideradas vitais.

CAPÍTULO IX
DA CONFORMIDADE

Art. 23. Devem ser adotados procedimentos apropriados para garantir a conformidade com as reestrições legais quanto ao uso de materiais protegidos por leis de propriedade intelectual, direitos autorais, patentes e marcas registradas.

Art. 24. Os processos de aquisição de bens e serviços, especialmente dos ativos de informação, devem estar em conformidade com esta Norma.

§1º O uso de recursos de computação em nuvem para suprir demandas corporativas de transferência e armazenamento de arquivos, processamento de dados, aplicações e sistemas de informação deve atender às diretrizes desta norma e demais orientações governamentais e legislações em vigor, visando garantir a segurança das informações hospedadas na nuvem, em especial àquelas sob custódia e gerenciamento de um prestador de serviço terceirizado.

§2º O uso das redes sociais com o objetivo de prestar atendimento e serviços públicos de divulgação e compartilhamento de informações corporativas da ANEEL, deve atender às determinações desta norma e demais orientações governamentais e legislações em vigor.

Art. 25. Os sistemas de informações, além de disponibilizar os registros em prazos e formatos aceitáveis, devem protegê-los contra perda, destruição e falsificação, visando à salvaguarda dos dados.

Parágrafo Único. Boas práticas de segurança na obtenção e desenvolvimento de *software* deverão ser seguidas atendendo às diretrizes desta norma e demais orientações governamentais e legislações em vigor.

TÍTULO IV
DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

CAPÍTULO I
DA AVALIAÇÃO E DA REGULAMENTAÇÃO

Art. 26. O cumprimento desta Norma deve ser avaliado periodicamente, de acordo com os critérios

da CGI.

Parágrafo único. A avaliação do cumprimento desta Norma, por meio de verificações de conformidade, poderá inclusive ser realizada com o apoio de entidades externas e independentes.

Art. 27. Fica a SGI autorizada a regulamentar os procedimentos necessários para a aplicação das disposições estabelecidas nesta Norma.

CAPÍTULO II DAS PENALIDADES

Art. 28. O descumprimento ou violação da Política de Segurança da Informação e Comunicações poderá resultar na aplicação das sanções previstas na legislação vigente, conforme avaliação e orientação da CGI.

Parágrafo único. Por Proposição da SGI, a CGI poderá elaborar procedimentos complementares dispondo acerca das formas de apuração, bem como das sanções e penalidades resultantes das violações à Política de Segurança da Informação e Comunicações da Agência.

Art. 29. Os casos omissos serão analisados e deliberados pela CGI da ANEEL.

Art. 30. É vedada qualquer ação que não esteja explicitamente permitida na Política de Segurança da Informação e Comunicações da ANEEL ou que não tenha sido previamente autorizada pela CGI.

CAPÍTULO III
DA APLICAÇÃO E VIGÊNCIA

Art. 31. A Política de Segurança da Informação e Comunicações da ANEEL deve ser revisada e atualizada periodicamente, não excedendo o período máximo de 3 (três) anos ou, por proposição da CGI, sempre que ocorrer eventos ou fatores relevantes que exijam sua revisão imediata.

Art. 32. Esta Norma é de aplicação interna e entra em vigor na data de sua publicação.