AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA - ANEEL

PORTARIA Nº 581, DE 17 DE ABRIL DE 2007.

Aprova a Revisão 01 da Norma de Organização ANEEL nº 012, de 15 de julho de 2004, que estabelece as Diretrizes Básicas da Política de Segurança da Informação a serem observados no âmbito da Agência Nacional de Energia Elétrica – ANEEL.

Relatório

Voto

O DIRETOR-GERAL DA AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA – ANEEL, no uso de suas atribuições regimentais, de acordo com deliberação da Diretoria, tendo em vista o disposto no arts. 7º, inciso IX, e 9º, do Regimento Interno da ANEEL, aprovado pela Portaria nº 349, de 28 de novembro de 1997, do Ministério de Minas e Energia, e considerando a necessidade de revisar as ações de Segurança da Informação a serem executadas pela ANEEL, resolve:

Art. 1º Aprovar a Revisão 01 da Norma de Organização ANEEL nº 012, de 15 de julho de 2004, conforme o Anexo desta Portaria, que estabelece as Diretrizes Básicas da Política de Segurança da Informação da ANEEL.

Art. 2º Revogar a Portaria nº 080, de 15 de julho de 2004.

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

JERSON KELMAN

Este texto não substitui o publicado no Boletim Administrativo de 04.05.2007, v. 10, n. 8.

(Revogada pela PRT ANEEL 3.522 de 22.05.2015)

ANEXO À PORTARIA Nº 581, DE 17 DE ABRIL DE 2007.

NORMA DE ORGANIZAÇÃO ANEEL Nº 012

REVISÃO 01

TÍTULO I
DAS DISPOSIÇÕES GERAIS

CAPÍTULO I
DO OBJETIVO

Art. 1º Esta Norma dispõe sobre as Diretrizes Básicas da Política de Segurança da Informação, 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 procedimentos estabelecidos 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.

CAPÍTULO III
DO ESCOPO

Art. 3º As Diretrizes Básicas da Política de Segurança da Informação 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 IV
DAS RESPONSABILIDADES

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

I – Comissão Permanente de Avaliação de Documentos Sigilosos – CPADS: órgão colegiado, nomeado pela Diretoria da ANEEL, responsável pelo do 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;

III – Superintendência de Gestão Técnica da Informação – SGI: recomendar e regulamentar a operacionalização dos normativos provenientes da Política de Segurança 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 aquelas referentes a recursos humanos que interajam com os processos de ativos de informação;

VI – Assessoria de Comunicação e Imprensa – ACI: executar as atividades relacionadas à comunicação institucional, divulgando e disseminando as orientações emanadas pela Política de Segurança da Informação;

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 o Subprocesso da SGI Central de Atendimento aos Usuários de Informática; e

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.

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: tudo que manipula a informação, inclusive ela própria, tais como base de dados e arquivos, documentação do sistema, manuais, material de treinamento, procedimentos de suporte ou operação, planos de continuidade, procedimentos de recuperação, informações armazenadas, softwares, sistemas, ferramentas de desenvolvimento e utilitários, estações de trabalho, servidores, equipamentos de comunicação, no-breaks e outros;

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

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

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

IX - 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;

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

XI – plano de contingência: 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;

XII – política de segurança da informação: 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;

XIII – princípios da segurança da informação: 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;

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

XV – TCP/IP (Transmission Control Protocol/Internet Protocol): conjunto de padrões de comunicação em uma rede de dados, tais como Internet, intranet, que orienta o tráfego de informações e define o endereçamento e o envio de dados; e

XVI – termo de responsabilidade: acordo de confidencialidade para não divulgação 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 devem atender às seguintes normas:

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 - o Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades de Administração Pública Federal;

III - o Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal;

IV - a NBR/ISO/IEC 27001:2005 da ABNT, que trata do Código de Prática para o Sistema de Gestão de Segurança da Informação;

V - a NBR/ISO/IEC 17799:2005 da ABNT, que trata do Código de Prática para a Gestão da Segurança da Informação - Técnicas de Segurança;

VI - outras Normas de Organização ANEEL; e

VII - outras normas pertinentes em vigor.

CAPÍTULO II
DA CAPACITAÇÃO E DO APERFEIÇOAMENTO

Art. 8º As Diretrizes Básicas da Política de Segurança da Informação 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, 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 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 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.

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 confidencialidade e o sigilo das informações.

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

CAPÍTULO IV
DA UTILIZAÇÃO DOS RECURSOS

Art. 17. Os recursos disponibilizados são fornecidos com o propósito único de garantir o desempenho das atividades da ANEEL, sendo vedado aos colaboradores o uso desses recursos 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 dados da ANEEL 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.

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 é alvo de controle e monitoração.

Parágrafo único. A Política de Segurança da Informação prevê mecanismos que visem a garantir e proteger a informação quanto à autenticação.

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, 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 – avaliação em regime emergencial das conseqüências de desastres, falhas de segurança e perda de serviços;

II - contingência e recuperação do funcionamento normal dentro de períodos de tempos determinados; e

III - recuperação tempestiva das operações consideradas vitais.

CAPÍTULO IX
DA CONFORMIDADE

Art. 23. Devem ser adotados procedimentos apropriados para garantir a conformidade com as restrições 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.

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.

TÍTULO IV
DAS DISPOSIÇÕES FINAIS

CAPÍTULO I
DA AVALIAÇÃO E DA REGULAMENTAÇÃO

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

Art. 27. Fica a SGI autorizada a regulamentar, e submeter à Diretoria da ANEEL para aprovação, 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 poderá resultar na aplicação das sanções previstas na legislação vigente, conforme avaliação e orientação da CGI.

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 ANEEL ou que não tenha sido previamente autorizada pela CGI.

CAPÍTULO III
DA APLICAÇÃO E VIGÊNCIA

Art. 31. A Política de Segurança da Informação deve ser revisada e atualizada periodicamente, ou 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.