AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA - ANEEL

PORTARIA Nº 82, DE 15 DE JULHO DE 2004

O DIRETOR-GERAL DA AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA – ANEEL, no uso das atribuições regimentais, com base no disposto no Art. 7º, incisos I, IX e X e no art. 9º do Regimento Interno da ANEEL e em conformidade com deliberação da Diretoria, resolve:

Art. 1° Aprovar a Norma Organizacional nº 14, que estabelece as Normas Gerais para Administradores de Serviço, em atendimento à Política de Segurança da Informação da ANEEL.

Art. 2º Esta Portaria entra em vigor na data de sua publicação.

JOSÉ MÁRIO MIRANDA ABDO

Publicado no Boletim Administrativo de 15.07.2004, v. 7, n. 8.

Este texto não substitui o publicado no Boletim Administrativo de 15.07.2004.

(Revogada pela PRT ANEEL 3.522 de 22.05.2015)

NORMA ORGANIZACIONAL ANEEL Nº 14

DE 15 DE JULHO DE 2004

TÍTULO I
DAS DISPOSIÇÕES GERAIS

CAPÍTULO I
DO OBJETIVO

Art. 1.º Dispor sobre as Normas Gerais para Administradores de Serviço, determinando critérios para acesso privilegiado aos ativos, em atendimento à Política de Segurança da Informação da ANEEL.

CAPÍTULO II
DO ESCOPO

Art. 2.º Contempla todos os Colaboradores que, por força de suas atividades, necessitem de acessos privilegiados para configuração e utilização de softwares, hardwares, sistemas de informação e demais ativos pertinentes.

CAPÍTULO III
DA RESPONSABILIDADE

Art. 3.º Tendo como público alvo todos os Administradores de Serviço, deverão ser aplicadas as responsabilidades pertinentes, identificadas na Norma Diretrizes Básicas da Política de Segurança da Informação.

TITULO II
DA CONCEITUAÇÃO

I - acesso privilegiado – é aquele em que permite ao Colaborador sobrepor controles do sistema de informação e somente devem ser concedidos àqueles que o necessitam para a condução de suas atividades;

II - Administrador de Serviço – Colaborador que possui privilégios para a utilização e disponibilização, por força de suas funções, de recursos restritos de Tecnologia da Informação. Poderá, dependendo de suas atividades, ser classificado em:

a. Administrador de Banco de Dados - especialista na análise e configuração técnicas de armazenamento, acesso e classificação de registros;

b. Administrador de Correio Eletrônico - especialista responsável pela definição e atualização do esquema do banco de dados; e, pela definição da estrutura de armazenamento e a estratégia (ou método) de acesso aos dados; concessão de autorização para acesso a dados;

c. Administrador de Rede de Dados - especialista na análise e configuração técnicas dos recursos de conectividade e comunicação de dados;

d. Administrador de Segurança da Informação – especialista na análise e configuração técnicas de segurança da informação em ativos;

e. Administrador de WEB - especialista na análise e configuração técnicas de recursos relacionados à Internet, intranet, extranet;

f. Analista de Sistemas – especialista responsável pelo levantamento das necessidades da Unidades Organizacionais e elaboração do modelo conceitual do sistema a ser desenvolvido, bem como pela automação dos processos daí decorrentes; e

g. Técnico de Suporte – especialista na instalação e configuração de software e hardware, que realiza os apoios necessários aos Colaboradores no uso de ativos, na eliminação de dúvidas e na resolução de problemas.

III - ativo - tudo que manipula a informação (inclusive ela própria). São exemplos de ativos associados à tecnologia de informação: 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 (roteadores, fax, modens etc.), no-breaks e outros;

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

V - Central de Atendimento - Subprocesso da Superintendência de Gestão Técnica da Informação – SGI, responsável pelo atendimento e suporte técnico aos ativos;

VI - 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;

VII - confidencialidade - garantia do acesso autorizado a informações, de acordo com o nível de proteção. Sua classificação será alvo de normatização específica;

VIII - conta – recurso pelo qual o Colaborador é autenticado na rede ou em sistemas de informação, por meio da utilização do nome combinado com uma senha;

IX - direito autoral - direito exercido pelo autor ou por seus descendentes sobre suas obras, no tocante à publicação, tradução, venda e reprodução;

X - disponibilidade – garantia de que os Colaboradores possam ter acesso a informações segundo sua demanda e em conformidade com a Política de Segurança da Informação;

XI - dispositivo de identificação – instrumento que permite o reconhecimento do Colaborador de recursos de Tecnologia da Informação, como por exemplo, senha e crachá;

XII - hotfix – seqüência de instruções apresentadas , pelos fornecedores, para a correção de problemas relacionados ao funcionamento de ativos;

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

XIV - log - registro de informações que permite determinar se o uso de um ativo está ocorrendo de acordo com as regras de segurança estabelecidas;

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

XVI - patente - título de propriedade temporária sobre uma invenção ou modelo de utilidade, outorgado pelo Estado aos inventores ou autores ou outras pessoas físicas ou jurídicas detentoras de direitos sobre a criação;

XVII - Plano de Contingência – descreve as ações que uma organização deve tomar para assegurar a continuidade das operações em caso de falha de ativos, incluindo a ativação de processos manuais, duplicidade de recursos e acionamento de fornecedores;

XVIII - Princípios da Segurança da Informação - são princípios que regem a segurança da informação, em acordo com o artigo 3° do Decreto n° 3.505, de 13 de junho de 2000, quais sejam: confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio;

XIX - senha – código composto no mínimo por 8 caracteres, sendo representado por números, letras e caracteres especiais que possibilitam o acesso do Colaborador à rede de dados;

XX - service pack – pacote de serviço utilizado, pelos fornecedores, para a atualização de software;

XXI - software - qualquer programa ou conjunto de programas de um computador;

XXII - termo de responsabilidade - acordo de confidencialidade e não divulgação de informações que atribui responsabilidades ao Colaborador e Administrador de Serviço quanto ao sigilo e a correta utilização dos ativos de propriedade ou custodiados pela ANEEL; e

XXIII - vulnerabilidade – ponto de fragilidade de um ativo que se explorado pode comprometer pelo menos um dos princípios de segurança da informação.

TÍTULO III
DO USO SEGURO DA INFORMAÇÃO

CAPÍTULO I
DA IDENTIFICAÇÃO

Art 4.° São considerados Administradores de Serviço:

I - Administrador de Banco de Dados;

II - Administrador de Correio Eletrônico;

III - Administrador de Rede de Dados;

IV - Administrador de Segurança da Informação;

V - Administrador de WEB;

VI - Analista de Sistemas; e

VII - Técnico de Suporte.

Parágrafo único. As atribuições específicas e os processos referentes aos tipos de Administradores de Serviço mencionados estarão descritos nos procedimentos em vigor.

Art 5.° Os dispositivos de identificação são únicos, pessoais e intransferíveis, não podendo ser compartilhados, conforme orientação dos procedimentos em vigor.

§ 1º. Os Administradores de Serviço devem possuir duas contas de identificação distintas; uma, exclusivamente, para atividades como Administrador de Serviço e a outra para suas tarefas como Colaborador.

§ 2º. Qualquer Colaborador poderá ter, desde que autorizado, acesso privilegiado aos ativos que se mostrarem necessários para a consecução de suas tarefas, utilizando-se de sua conta única de identificação, conforme procedimentos em vigor.

Art 6.° A SGI deverá manter atualizado o registro de todos os Colaboradores que possuam acesso privilegiado aos ativos.

CAPÍTULO II
DO ACESSO PRIVILEGIADO

Art 7.º Os Administradores de Serviço deverão fazer uso dos acessos privilegiados aos ativos disponibilizados, de acordo com os procedimentos em vigor.

§ 1º. Os Administradores de Serviço terão acesso privilegiado unicamente aos ativos que forem indispensáveis à realização de suas atividades, cabendo à SGI a administração destas concessões.

§ 2°. É vedada a utilização do acesso privilegiado pelos Administradores de Serviço para fins diferentes àqueles que justificaram sua concessão.

§ 3°. A utilização indevida dos privilégios a que se refere este artigo é de responsabilidade do Administrador de Serviço, como também são as conseqüências dela decorridas.

CAPÍTULO III
DA PROTEÇÃO DOS RECURSOS DE TECNOLOGIA

Art. 8.ºOs Administradores de Serviço assinarão um termo de responsabilidade, que terá características especiais em vista do acesso privilegiado concedido, garantindo a confidencialidade e a não-divulgação das informações a que tiverem acesso, bem como a correta utilização dos ativos.

§ 1° Os Colaboradores que, por força de suas funções, necessitarem de acesso privilegiado aos recursos de Tecnologia da Informação, também deverão assinar o termo mencionado no caput.

§ 2° O termo de responsabilidade a que se refere este artigo será elaborado de acordo com o modelo constante do Anexo I desta Norma e, depois de devidamente assinado, ficará sob a guarda da SGI.

Art 9.º A utilização de ativos deve respeitar a legislação em vigor referente aos direitos autorais e patentes.

Art 10. Implementações, alterações e atualizações de ativos devem ser homologadas pela SGI.

Art. 11. O compartilhamento de ativos deve preservar a confidencialidade, a integridade e a disponibilidade dos ativos.

Art. 12. Os Administradores de Serviço deverão estabelecer cópias de segurança dos ativos sob sua responsabilidade, de acordo com os procedimentos pertinentes em vigor.

TÍTULO IV
DAS ATRIBUIÇÕES

CAPÍTULO I
DO USO DO AMBIENTE TECNOLÓGICO

Art. 13. A utilização de ferramentas para administração de ativos deve ser realizada de forma controlada e que não comprometa a segurança das informações e dos ambientes.

Parágrafo único. Para a administração da rede de dados, dos sistemas, dos bancos de dados e dos ativos de segurança da informação, do correio eletrônico e da WEB tais ferramentas devem ser de uso exclusivo dos Administradores dos respectivos serviços.

Art. 14. O acesso físico aos ambientes tecnológicos da SGI, onde se desenvolvem projetos e se operacionalizam sistemas, será limitado aos Administradores de Serviço que necessitem desta permissão para realizar suas atividades.

CAPÍTULO II
DOS CONTROLES

Art. 15. Os Administradores de Serviço deverão manter controles que visem garantir a segurança e o funcionamento dos ativos, tais como:

I - aplicação de service packs e hotfixes nos ativos sob sua responsabilidade; e

II - registro em logs, quando da alteração das configurações específicas dos ativos sob sua responsabilidade.

CAPÍTULO III
DA MANUTENÇÃO

Art. 16. Os Administradores de Serviço deverão solicitar a presença de fornecedores, suporte e mantenedores de ativos, quando necessária a presença para resolução de problemas.

Art. 17. Os ativos devem ser atualizados sempre que for detectada alguma vulnerabilidade ou quando for implementada uma nova funcionalidade.

Art. 18. Os Administradores de Serviço são responsáveis por comunicar, aos Colaboradores envolvidos, quaisquer alterações de configurações, que impactem o funcionamento dos ativos.

Art. 19. A manutenção preventiva e a atualização dos ativos deve ser previamente agendado, preferencialmente, fora do horário normal de funcionamento.

CAPÍTULO IV
DA INTERRUPÇÃO E DA CONTINUIDADE DAS OPERAÇÕES

Art. 20. Todo Administrador de Serviço tem por obrigação possibilitar o acionamento do Plano de Contingências para as operações consideradas críticas, no caso de falhas dos recursos empregados, conforme procedimentos em vigor.

Art. 21. A paralisação de quaisquer serviços de Tecnologia da Informação ensejará a ação imediata do Administrador de Serviço responsável, no sentido de atenuar os impactos provenientes.

Parágrafo único. A paralisação aludida no caput será comunicada com antecedência aos Colaboradores, indicando os períodos de indisponibilidade dos serviços, sendo que no caso de paralisações fortuitas, a comunicação será feita após a estabilização da situação de emergência.

TÍTULO V
DAS DISPOSIÇÕES FINAIS
CAPÍTULO I
DA AVALIAÇÃO E DA REGULAMENTAÇÃO

Art. 22. O cumprimento desta norma será avaliado periodicamente, de acordo com os critérios do CSI.

Art. 23. Fica a SGI autorizada a regulamentar os procedimentos necessários para aplicação das disposições estabelecidas nesta Norma.

CAPÍTULO II
DAS PENALIDADES

Art. 24. Cabe à SGI, a qualquer tempo, suspender, em caráter preventivo, o acesso do Administrador de Serviço ao ativo quando evidenciados os riscos à segurança da informação, e informar o incidente ao CSI.

Art. 25. O descumprimento ou violação de um ou mais itens desta norma ensejarão na aplicação de sanções, conforme avaliação e orientação do CSI.

CAPÍTULO III
DA APLICAÇÃO E VIGÊNCIA

Art. 26. Esta norma é de aplicação interna, com vigência a partir da data de sua publicação, por prazo indeterminado.

ANEXO I

TERMO DE RESPONSABILIDADE PARA ADMINISTRADORES DE SERVIÇO

Pelo presente termo, declaro ter conhecimento da Política de Segurança da Informação da ANEEL, comprometendo-me, sob as possíveis penalidades previstas pela ANEEL, a realizar meu trabalho de forma íntegra, respeitando os preceitos fundamentais que pautam a missão, a visão e os valores da Agência, estando ciente das responsabilidades advindas do privilégio que estou recebendo.

Tenho consciência de que minhas ações serão monitoradas de acordo com a Política de Segurança da Informação da ANEEL, de que os sistemas a que tenho acesso poderão ser auditados e de que qualquer alteração feita sob minha identificação, advinda de minha autenticação, é de minha responsabilidade.
Para execução das minhas atividades na ANEEL e com autorização superior, estou recebendo uma conta com direito de administração de estações de trabalho, que deverá ser utilizada somente para execução das atividades necessárias e dependentes deste privilégio.
Nesta função receberei orientações sobre o uso e segurança dos recursos de tecnologia da informação da ANEEL da área competente (Superintendência de Gestão Técnica da Informação – SGI).
Estou ciente de que qualquer problema referente ao uso de computadores e demais recursos da rede corporativa da ANEEL terá que ser informado à SGI.
Tenho total responsabilidade pelo dano que possa causar pelo descumprimento da Política de Segurança da Informação da ANEEL e dos procedimentos acima citados, realizando uma ação de iniciativa própria de tentativa de modificação da configuração, física ou lógica, das estações de trabalho, sem a permissão da SGI.
Responsabilizo-me por qualquer conduta tomada de minha parte que possa prejudicar um outro colaborador ou a disponibilidade, integridade e sigilo das informações da ANEEL, que trafeguem ou fiquem armazenadas nos recursos de Tecnologia da Informação sob minha administração.

Brasília (DF), ___ de _____ de _____.

_____

Colaborador - Unidade Organizacional
CI/Órgão emissor:

_____

Líder da Unidade Organizacional

Testemunhas:

_____

_____