

COMISSÃO NACIONAL DE ENERGIA NUCLEAR**PORTARIA PR/CNEN Nº 11/2021**

Aprova a Política de Segurança da Informação e Comunicação no Âmbito da CNEN e dá outras providências.

O PRESIDENTE DA COMISSÃO NACIONAL DE ENERGIA NUCLEAR (CNEN), no uso das atribuições que lhe foram conferidas pelo art. 15, incisos I e V, do Anexo I, ao Decreto nº 8.886, publicado no Diário Oficial da União de 25 de outubro de 2016, e

CONSIDERANDO o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

CONSIDERANDO a Instrução Normativa GSI/PR nº 1, de 27 de Maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

CONSIDERANDO o Decreto nº 10.222, de 05 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

CONSIDERANDO a Portaria CNEN-PR nº 012, de 23 de Março de 2018, que aprova a Política de Segurança Institucional (PSI) e o Plano de Segurança Institucional (PLSI) da CNEN;

CONSIDERANDO o Decreto nº 8.777, de 11 de maio de 2016, que institui a Política de Dados Abertos do Poder Executivo Federal;

CONSIDERANDO a Lei nº 12.527, de 18 de Novembro de 2011, que dispõem sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir 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](#).

CONSIDERANDO a Lei nº 13.709/2018, de 14 de Agosto de 2018, que dispõe sobre a Proteção de Dados Pessoais;

CONSIDERANDO o constante dos autos do processo nº 01341.002010/2020-33;

RESOLVE:

Art. 1º Aprovar, na forma do anexo, a Política de Segurança da Informação e Comunicação da CNEN - POSIC.

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

Art. 3º Fica revogada a portaria CNEN-PR Nº 004, de 09 de Janeiro de 2015.

Paulo Roberto Pertusi
Presidente



Documento assinado eletronicamente por **Paulo Roberto Pertusi, Presidente**, em 19/02/2021, às 16:07, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#) e no §1º do art. 7º da Portaria PR/CNEN nº 80, de 28 de dezembro de 2018.



A autenticidade deste documento pode ser conferida no site http://sei.cnem.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0777200** e o código CRC **354D0E8A**.

ANEXO I

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (POSIC) DA CNEN

SEÇÃO I

DA FINALIDADE

Art. 1º A Política de Segurança da Informação e Comunicação estabelece e define diretrizes, normas, responsabilidades e competências para a gestão da segurança da informação e comunicação na CNEN.

SEÇÃO II

DOS FUNDAMENTOS

Art. 2º A gestão da segurança da informação e comunicação na CNEN deve seguir a legislação aplicável à matéria e, complementarmente:

- I - Estar alinhada com a missão da Autarquia;
- II - Buscar a sensibilização e o comprometimento de todo o efetivo da organização; e
- III - Estar continuamente atualizada, para assegurar a sua pertinência, adequação e eficácia.

SEÇÃO III

DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para fins da Política de Segurança da Informação e Comunicação considera-se:

- i. Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;
- ii. Agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

iii. Ameaça: causa potencial de um incidente que pode resultar em danos a um sistema ou organização; indivíduo ou grupo de indivíduos com intenção, motivação e capacidade (recursos técnicos,

tecnológicos, financeiros, materiais e humanos) para cometer um ato danoso;

iv. Aplicação: um programa de computador que tem por objetivo ajudar o seu usuário a desempenhar uma tarefa específica, em geral ligada a processamento de dados;

v. Ativo: tudo que tenha ou gere valor para a organização;

vi. Ativo de informação: todo elemento que agregue valor ao negócio, podendo ser uma informação digital ou física, pessoa ou ambiente físico, cuja quebra da confidencialidade, integridade ou disponibilidade traga prejuízo. E justamente por ser fundamental ao negócio, deve ser adequadamente protegido;

vii. Colaborador: toda pessoa que se vincula à CNEN, por meio de empresa prestadora de serviço ou por meio de contrato, convênio, acordo, ajuste ou outros instrumentos congêneres, tendo por finalidade a execução de atividades inerentes à Autarquia;

viii. Evento: incidente ou ocorrência, a partir de fontes internas ou externas a uma entidade, capaz de afetar a realização dos seus objetivos;

ix. Gestão da segurança da informação e comunicação: ações e métodos que visam à integração das atividades de gestão de riscos e de continuidade de negociação, tratamento de incidentes e da informação, conformidade, credenciamento, segurança cibernética, física, lógica, orgânica e organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação e Comunicação;

x. Gestor de Segurança da Informação: Área responsável designada pelo Presidente da CNEN pela governança da segurança da informação nos meios de TIC no âmbito da CNEN;

xi. Gestor da Informação e Comunicação: Área responsável designada pelo Presidente da CNEN pela governança da informação e comunicação no âmbito da CNEN;

xii. Incidente de segurança da informação: um, apenas, ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações e ameaçar a segurança da informação;

xiii. Informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

xvi. Informação pessoal: informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;

xv. Política de Segurança da Informação e Comunicação (POSIC): documento aprovado pela CNEN com as diretrizes e critérios relativos à segurança da informação e comunicação;

xvi. Prestador de serviços: terceirizados contratados para execução de serviços específicos dentro das instalações da CNEN;

xvii. Proprietário da informação: indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela informação;

xviii. Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicação;

xix. Recursos de processamento da informação: qualquer sistema de processamento da informação, serviço, infraestrutura ou as instalações físicas que os abriguem;

xx. Segurança da informação e comunicação (SIC): ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

xxi. Servidor Público: todo aquele que mantém vínculo de trabalho profissional com órgãos e entidades governamentais;

xxii. Termo de responsabilidade: termo assinado pelo usuário concordando em adotar todas as medidas cabíveis para garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como em assumir responsabilidades decorrentes de tal acesso;

xxiii. Tratamento de Incidentes de Segurança em Redes Computacionais: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança da informação, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências; e

xxiv. - Usuários: agentes públicos e cidadãos com interesse nos serviços e/ou nas informações prestados pela CNEN.

SEÇÃO IV

DOS PRINCÍPIOS

Art. 4º A segurança da informação busca reduzir os riscos de vazamentos, fraudes, erros, uso indevido, sabotagens, paralisações, furto de informações ou qualquer outra ameaça que possa prejudicar os sistemas de informação, os recursos de processamento da informação ou os equipamentos de uma organização.

Art. 5º Para efeitos de aplicação desta Política, são considerados princípios da segurança da informação:

i. a disponibilidade: propriedade de que a informação esteja acessível e utilizável por uma pessoa física, sistema, órgão ou entidade;

ii. a confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados ou credenciados;

iii. a integridade: propriedade de que a informação não esteja modificada ou destruída de maneira não autorizada ou acidental;

iv. a autenticidade: propriedade que garante ter sido a informação produzida, expedida, modificada ou destruída por pessoa física, sistema, órgão ou entidade;

v. a confiabilidade: requer que os meios, nos quais a informação trafega e é armazenada, sejam preparados para promover e garantir eficientemente a recuperação dessa informação caso haja insucesso de mudança ou evento inesperado, com observância dos demais princípios de segurança;

vi. a responsabilidade: propriedade de que todo ativo possua um responsável que garanta sua correta utilização, além de monitorar o ativo de maneira que o uso indevido seja reportado e as ações cabíveis tomadas;

vii. a irretratabilidade: O princípio da irretratabilidade, mais conhecido como princípio do não repúdio, garante a autenticidade de algum documento quando utilizado por determinadas ferramentas, como no caso do Certificado Digital.

SEÇÃO V

DO OBJETO

Art. 6º As diretrizes de segurança da informação estabelecidas nesta POSIC aplicam-se às informações para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação da CNEN, e que devem ser seguidas pelos agentes públicos da instituição e por todos os usuários que tenham acesso às suas informações, incumbindo a todos a responsabilidade e o comprometimento com sua aplicação;

Parágrafo único. Seja qual for a forma ou o meio pelo qual a informação seja apresentada ou compartilhada, deverá ser sempre protegida adequadamente, de acordo com esta política;

Art. 7º Esta política estabelece responsabilidades e obrigações a todos os agentes públicos da CNEN e a todos os usuários que tenham acesso às suas informações;

Art. 8º O controle de acesso físico às instalações da CNEN, de acesso aos sistemas corporativos e às informações armazenadas, bem como o controle de circulação de pessoas e veículos devem também atender ao disposto em normas complementares a esta POSIC, tais como a Norma CNEN NE 2.01 – Proteção Física de Unidades Operacionais da Área Nuclear, e a Norma CNEN NN 2.06 – Proteção Física de Fontes Radioativas e Instalações Radiativas Associadas.

Art. 9º Esta POSIC deve ser difundida a todos os servidores, colaboradores, agentes públicos e cidadãos com interesse nos serviços prestados pela CNEN através de um processo permanente de conscientização em Segurança da Informação e Comunicação.

SEÇÃO VI

DAS DIRETRIZES GERAIS

Art. 10. Na CNEN, é permitido aos usuários o uso de recursos de processamento da informação disponibilizados pela Autarquia, de forma a garantir que os requisitos de segurança sejam atendidos.

Parágrafo único. Os chefes e os responsáveis pelas unidades organizacionais da CNEN devem autorizar os acessos aos recursos de processamento de informação.

Art. 11. Os usuários não podem, em qualquer tempo ou sob qualquer propósito, apropriar-se de informações para uso pessoal ou fora da competência de sua atuação.

Art. 12. Quaisquer recursos de processamento da informação devem ser testados em ambiente de homologação antes de serem colocados em produção.

Art. 13. Os servidores e colaboradores da CNEN estão sujeitos à POSIC – Política de Segurança da Informação e Comunicação e têm o dever de observar integralmente o nela disposto. A inobservância dessa Política poderá acarretar sanções previstas no âmbito penal, civil e administrativo, na forma da legislação vigente.

Art. 14. É condição para acesso aos ativos de informação da CNEN a adesão formal aos termos desta Política.

Art. 15. O agente público da CNEN é responsável pela segurança dos ativos de informação e processos que estejam sob sua responsabilidade.

Parágrafo único. Ativos de tecnologia da informação e comunicação que necessitem de proteção adicional devido à sua criticidade e importância devem ser isolados e com controle restrito de acesso físico e lógico. A CNEN deve adotar ações de caráter preventivo para a contínua segurança e disponibilidade desses ativos de tecnologia da informação e comunicação;

Art. 16. Os contratos firmados pela CNEN devem conter cláusulas que determinem a observância desta política e das normas dela derivadas.

Parágrafo único. A CNEN deverá, em seus relacionamentos contratuais com terceiros, definir, especificamente, quais serviços e atividades serão autorizados para acesso e manuseio por terceiros. Deverá ser considerado, sempre, o menor perfil de privilégio aplicável ao caso para acesso às informações da Autarquia;

Art. 17. Os recursos de Tecnologia da Informação e Comunicação (TIC) disponibilizados pela CNEN devem ser utilizados estritamente para seu propósito.

Parágrafo único. É vedado a qualquer colaborador e agente público da CNEN o uso dos recursos de TIC para fins pessoais (próprios ou de terceiros), entretenimento, veiculação de opiniões político-partidárias ou religiosas, bem como para realizar ações que, de qualquer modo, possam constranger, assediar, ofender, caluniar, ameaçar, violar direito ou causar prejuízos a qualquer pessoa física ou jurídica, bem como ações que atentem contra a moral e a ética.

SEÇÃO VII

PROPRIEDADE DA INFORMAÇÃO

Art. 18. Informação é patrimônio - Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela CNEN é considerada parte do seu patrimônio e deve ser protegida quanto aos aspectos de confidencialidade, autenticidade, integridade e disponibilidade:

i. toda informação criada ou custodiada que for manuseada, armazenada, transportada ou descartada pelo colaborador e agente público da CNEN, no exercício de suas atividades, é de propriedade desta entidade e será protegida segundo estas diretrizes e nas regulamentações em vigor, conforme a classificação das informações, sem prejuízo da autoria, conforme definido em lei e de acordo com as diretrizes de Classificação da Informação da CNEN;

ii. quando da obtenção de informação de terceiros com direitos de uso restrito, o gestor da informação deve providenciar, junto ao concedente, a documentação formal atinente aos direitos de acesso, antes de seu uso;

iii. na cessão de bases de dados custodiadas ou de informação de propriedade da CNEN a terceiros, o gestor da informação deve providenciar a documentação formal relativa à autorização de acesso às informações, conforme as diretrizes de Classificação da Informação da CNEN;

iv. deve-se estabelecer procedimentos apropriados para garantir a conformidade dos requisitos legislativos, regulamentares e contratuais no uso de material, em relação aos quais pode haver direitos de propriedade intelectual e o uso de produtos de softwares proprietários de acordo com as diretrizes de aquisição, desenvolvimento e manutenção de sistemas;

v. deve-se estabelecer procedimentos de privacidade e a proteção de dados que estejam em conformidade com as exigências das legislações relevantes, regulamentações e cláusulas contratuais de acordo com as diretrizes de proteção de dados pessoais da CNEN.

Parágrafo único: Os dados privados, pessoais e ou sensíveis do titular, de crianças e adolescentes devem ser processados de forma legal, justa e transparente em relação aos seus titulares.

Art. 19. A CNEN, por meio do seu Gabinete da Presidência, deve avaliar o estabelecimento de procedimentos a serem seguidos para o cumprimento desta seção.

SEÇÃO VIII

CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

Art. 20. A classificação e o tratamento da informação devem observar os seguintes requisitos e critérios:

- i. o valor, requisitos legais, sensibilidade e criticidade da informação para a CNEN;
- ii. conjunto apropriado de procedimentos para rotulação e tratamento da informação que deve ser definido e implementado de acordo com o critério de classificação adotado pela CNEN;
- iii. toda informação criada, manuseada, armazenada, transportada ou descartada da CNEN deve ser classificada quanto aos aspectos de confidencialidade, integridade e disponibilidade.

Art. 21. Classificação e tratamento de informação serão:

i. norteadas pela legislação específica que disponha 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 (APF), em especial a Lei nº 12.527/2011 e o Decreto nº 7845/2012;

ii. implementados e mantidos, em conformidade com a legislação vigente, visando a estabelecer os controles de segurança necessários a cada informação custodiada ou de propriedade da CNEN, ao longo do seu ciclo de vida; e

iii. realizados de acordo as diretrizes específicas de classificação da informação da CNEN.

Art. 22. As informações sob gestão da CNEN terão segurança de maneira a serem adequadamente protegidas quanto ao acesso e uso, sendo que para as consideradas de alta criticidade, serão necessárias medidas especiais de tratamento de acordo com as diretrizes de classificação da informação da CNEN.

Art. 23. A CNEN, por meio do seu Gabinete da Presidência, deve avaliar o estabelecimento de procedimentos a serem seguidos para cumprimento do quanto disposto desta seção.

SEÇÃO IX

DA GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E REDE

Art. 24. A gestão de incidentes de segurança da informação e rede seguirá os seguintes critérios e procedimentos:

i. os incidentes de segurança da informação devem ser relatados por meio dos canais apropriados da Instituição, o mais rápido possível;

ii. cada unidade gestora da CNEN deve divulgar internamente seu canal para relato dos incidentes de segurança da informação;

iii. as unidades gestoras da CNEN devem imediatamente relatar/encaminhar a notificação à área Gestora de Segurança da Informação em sua unidade;

iv. os agentes públicos, usuários de sistemas e serviços de informação devem ser instruídos a registrar e notificar qualquer observação ou suspeita de fragilidade de segurança em sistemas ou serviços;

v. devem ser observados os procedimentos de segurança da informação e comunicação, cada um com seu responsável, para assegurar respostas rápidas, efetivas e ordenadas;

vi. deverão ser observados os procedimentos de gestão de incidentes de rede, cada um com seu responsável, para assegurar respostas rápidas, efetivas e ordenadas;

Art. 25. Soluções de contorno aplicadas para minimizar a ocorrência de incidentes de segurança devem ser temporárias e imediatamente submetidas às áreas gestoras da segurança da informação com definição do prazo para que a solução definitiva do problema seja implementada.

Art. 26. As evidências dos incidentes de segurança devem ser coletadas, armazenadas e apresentadas em conformidade com as normas instituídas pelo órgão competente, nos casos em que um processo contra uma pessoa ou organização, após um incidente de segurança da informação tenha ocorrido.

Art. 27. A CNEN, por meio da Coordenação-Geral de Ciência e Tecnologia da Informação da Diretoria de Gestão Institucional, deve avaliar o estabelecimento de procedimentos a serem seguidos para cumprimento desta seção.

SEÇÃO XI

GERENCIAMENTO DE RISCOS

Art. 28. As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação e Comunicação – GRSIC devem considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura da CNEN.

Art. 29. A abordagem de gestão de riscos deve estar alinhada à Política de Gestão de Riscos, que estabelece a Gestão de Riscos na Comissão Nacional de Energia Nuclear - CNEN.

Art. 30. O processo de gestão de riscos em SIC possibilitará a seleção e a priorização dos ativos a serem protegidos.

Art. 31. A CNEN, por meio da Coordenação-Geral de Planejamento e Avaliação ligada à Presidência, deve avaliar o estabelecimento de procedimentos a serem seguidos para cumprimento desta seção.

SEÇÃO XII

GESTÃO DA CONTINUIDADE DAS ATIVIDADES INSTITUCIONAIS

Art. 32 A CNEN deve estabelecer procedimentos a serem seguidos para minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

Art. 33. A informação institucional, classificada como crítica ou essencial, deve ser mantida em local que a salvguarde adequadamente.

Art. 34. A elaboração dos Planos de Continuidade das Atividades, quando necessários, deve ser realizada, preferencialmente, por uma equipe multidisciplinar, visando que os planos sejam desenvolvidos com foco nas atividades institucionais da CNEN.

Art. 35. A CNEN, por meio da Coordenação-Geral de Planejamento e Avaliação ligada a Presidência, deve avaliar o estabelecimento de procedimentos a serem seguidos para cumprimento desta seção.

SEÇÃO XIII

MONITORAMENTO, AUDITORIA E CONFORMIDADE

Art. 36. A avaliação técnica de conformidade em Segurança da Informação e Comunicação deve considerar a POSIC com suas normas e os requisitos legais pertinentes.

Art. 37. A avaliação de conformidade em SIC deve ser aplicada de forma contínua, visando contribuir para a Gestão da Segurança da Informação e Comunicação.

i. o uso dos recursos de TIC disponibilizados pela CNEN é passível de monitoramento e auditoria e devem ser implementados e mantidos, sempre que possível, mecanismos que permitam a sua rastreabilidade; e

ii. a entrada e a saída de ativos de informação da CNEN, inclusive sua publicação e disponibilização, devem ser registradas e autorizadas por autoridade competente mediante procedimento formal.

SEÇÃO XIV

CONTROLE, ACESSO E USO DE SENHAS

Art. 38. O controle de acesso e uso de senhas visa contribuir para a garantia da integridade, disponibilidade, confidencialidade e autenticidade das informações da CNEN e deve observar o seguinte:

i. Criar mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

Parágrafo único: Os agentes públicos da CNEN que utilizam os recursos de TIC terão uma conta específica de acesso, pessoal e intransferível, cuja concessão será regulamentada em norma

complementar (a área de tecnologia da informação é responsável pela disponibilização do serviço).

ii. A CNEN deve conter ferramentas de proteção contra acesso não autorizado aos ativos de informação, que favoreça, preferencialmente, a administração de forma centralizada pelas unidades administrativas da CNEN;

iii. A CNEN deve seguir o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação;

iv. A autorização, o acesso, o uso da informação e dos recursos de TIC serão controlados e limitados ao cumprimento das atribuições de cada agente público da CNEN, e qualquer outra forma de uso necessita de prévia autorização formal do gestor de cada setor ou unidade organizacional;

v. Sempre que houver mudanças nas atribuições de determinado agente público da CNEN, é de responsabilidade da chefia imediata solicitar a adequação imediata dos privilégios de acesso às informações e dos recursos de TIC;

vi. Os servidores e os colaboradores devem ser orientados a respeito dos procedimentos de segurança acerca do procedimento formal de registro, suspensão e bloqueio de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços;

vii. No caso de desvinculação temporária ou definitiva do agente público, as áreas de Recursos Humanos e os Gestores de contratos de apoio terceirizado administrativo ou técnico, conforme o caso, devem notificar às áreas de TI sobre a desvinculação para que os privilégios de acesso sejam suspensos ou cancelados;

viii. Os servidores e os colaboradores devem ser orientados, de forma regular e periódica, a seguir as boas práticas de segurança da informação na seleção e uso de senhas conforme a norma de responsabilidades dos usuários;

ix. Os equipamentos de TIC devem ser utilizados única e exclusivamente por agentes públicos habilitados na rede de TIC da CNEN;

x. Os servidores e os colaboradores serão orientados a adotar uma política de “mesa limpa” e de “tela protegida” para reduzir os riscos de acesso não autorizado, perda e dano à informação, durante e fora do horário de trabalho;

xi. Os usuários devem ter acesso somente a serviços que tenham sido especificamente autorizados a usar pela chefia imediata ou área responsável requisitante;

xii. Os métodos de autenticação de usuários nos sistemas são por autenticação segura;

xiii. Nas conexões advindas de localizações e equipamentos específicos devem ser implementadas identificações automáticas entre equipamentos como um meio de autenticar as conexões;

xiv. Todo procedimento de *logon* nas estações de trabalho, servidores de rede, ativos de rede e sistemas de informação deve ser configurado com o intuito de garantir autenticação por meio de protocolos de segurança que sigam as boas práticas vigentes em TIC;

xv. Os sistemas operacionais e aplicações disponibilizadas deverão ser configurados de forma que os usuários tenham permissão para alterar suas próprias senhas de logon, impreterivelmente, no primeiro acesso;

xvi. Programas utilitários que possuam a capacidade de sobrepor os controles dos sistemas e aplicações serão de uso restrito e controlado.

Art. 39. A CNEN, por meio da Coordenação-Geral de Ciência e Tecnologia da Informação da Diretoria de Gestão Institucional, deve avaliar o estabelecimento de procedimentos a serem seguidos para o cumprimento desta seção.

SEÇÃO XV

ACESSO À INTERNET, USO DO E-MAIL E OUTROS RECURSOS

Art. 40. O acesso à internet, uso de e-mail e outros recursos devem obedecer ao seguinte:

- i. As informações e os recursos de TI para acesso à rede da CNEN devem ser disponibilizados única e exclusivamente àqueles que os utilizam para o exercício de suas funções;
- ii. Todos os dispositivos utilizados para a proteção, manutenção da integridade, disponibilidade e confidencialidade das informações devem ser considerados sigilosos, sendo, portanto, proibida a sua divulgação a pessoas não autorizadas;
- iii. Norma complementar de administração de rede e internet que discipline o uso do recurso de acesso à internet, e-mail ou qualquer outro recurso deverá ser elaborada e apresentada pela Coordenação-Geral de Ciência e Tecnologia da Informação da Diretoria de Gestão Institucional.

SEÇÃO XVI

GESTÃO DE ATIVOS

Art. 41. Os ativos associados à informação e aos recursos de processamento da informação devem ser identificados, e um inventário destes ativos deve ser estruturado e mantido;

Art. 42. Todas as informações e ativos associados a recursos de processamento da informação devem ser controladas pela área que dispõe do recurso ou serviço;

- i. para cada ativo identificado, deve ser indicado um responsável (proprietário) e a classificação do ativo;
- ii. a unidade gestora deve designar uma pessoa ou uma equipe que será responsável por acompanhar a produção, o desenvolvimento, a manutenção, o uso e a segurança do ativo;
- iii. a eliminação de informações deve observar a norma de procedimentos internos e classificação, e também a temporalidade prevista na legislação (Conarq); e
- iv. os ativos de informação serão classificados de acordo com a classificação da informação armazenada, processada, manuseada ou protegida pelo ativo.

Art. 43. A CNEN, por meio da Coordenação-Geral de Ciência e Tecnologia da Informação da Diretoria de Gestão Institucional, deve avaliar o estabelecimento de procedimentos a serem seguidos para cumprimento desta seção.

SEÇÃO XVII

SEGURANÇA FÍSICA DOS EQUIPAMENTOS

Art. 44. A segurança física dos equipamentos deve obedecer ao seguinte:

- i. a área responsável pela segurança organizacional/corporativa da CNEN deve implementar perímetros de segurança a fim de garantir proteção e separação entre ambientes internos e externos;
- ii. as áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso;
- iii. os equipamentos que operam fora das dependências da CNEN estão sujeitos à norma complementar que trate de operações externas; e
- iv. as estações de trabalho de TIC da CNEN devem possuir proteção física mínima para acesso ao interior do equipamento, como cadeado ou tranca equivalente.

Art. 45 A CNEN, por meio da Coordenação-Geral de Apoio Logístico da Diretoria de Gestão Institucional, deve avaliar o estabelecimento de procedimentos a serem seguidos para cumprimento

desta seção.

SEÇÃO XVIII

SERVIÇOS TERCEIRIZADOS

Art. 46. Os serviços terceirizados seguirão ao seguinte:

- i. a CNEN deve, em seus relacionamentos contratuais com terceiros, definir, especificamente, quais serviços e atividades serão autorizados para acesso e manuseio por terceiros; e
- ii. todo acesso por terceiros às informações e ativos da CNEN deve ser autorizado somente após regular preenchimento de Termo de Responsabilidade pertinente, de acordo com modelo estabelecido na Política de Segurança da Informação e Comunicação (POSIC) da CNEN;
- iii. toda atualização da POSIC da CNEN, bem como de procedimentos, sistemas e processos envolvidos, devem ser repassados a terceiros contratados a fim de se manter alinhado o conhecimento e implementação de mudanças de segurança necessárias à Autarquia.

Art. 47 A CNEN, por meio da Coordenação-Geral de Apoio Logístico da Diretoria de Gestão Institucional, deve avaliar o estabelecimento de procedimentos a serem seguidos para cumprimento desta seção.

SEÇÃO XIX

PLANEJAMENTO E ACEITAÇÃO DE SISTEMAS

Art. 48. O planejamento e aceitação dos sistemas da CNEN devem seguir o seguinte:

- i. Devem ser estabelecidas as exigências acerca da segurança afeta às aplicações adquiridas;
- ii. Devem ser feitas projeções para necessidades de capacidade futura, para garantir o desempenho requerido do sistema;
- iii. Testes para aplicações devem ser implementados a fim de se comprovar que erros, falhas e vulnerabilidades foram, efetivamente, evitados dentro do ciclo de desenvolvimento dessas soluções;
- iv. Controles de detecção, prevenção e recuperação devem ser implementados para a proteção contra códigos maliciosos;
- v. a infraestrutura de rede deve ser adequadamente gerenciada e controlada, de forma a protegê-la contra ameaças, reduzir as vulnerabilidades e manter a segurança de sistemas e aplicações que utilizam essas redes, incluindo a informação em trânsito;
- vi. interconexões de sistemas externos de informação da CNEN devem ser implementadas em conformidade com as orientações, regras, padrões de interoperabilidade do Governo Federal;
- vii. a integridade das informações disponibilizadas nos sistemas da CNEN e publicamente acessíveis devem ser protegidas para prevenir modificações não autorizadas;
- viii. os registros (logs) devem ser protegidos contra a falsificação e acesso não autorizado;
- ix. os relógios de todos os sistemas de processamento da informação relevantes, dentro da CNEN ou do domínio de segurança, devem ser sincronizados;
- x. Com base em uma classificação do nível da informação, é obrigatória, ao conjunto crítico, a produção e manutenção, por período de tempo previamente determinado, de registros (logs) que possam ser usados como trilha de auditoria, contendo atividades dos usuários, exceções e outros eventos de segurança da informação para auxiliar em futuras investigações e monitoramento de controle de acesso.

Art. 49. A CNEN, por meio da Coordenação-Geral de Ciência e Tecnologia da Informação da Diretoria de Gestão Institucional, deve avaliar o estabelecimento de procedimentos a serem seguidos para cumprimento desta seção.

SEÇÃO XX

USO, AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

Art. 50. O uso, aquisição, desenvolvimento e manutenção de sistema de informação deverão observar ao seguinte:

- i. qualquer software que, por necessidade do serviço necessitar ser instalado, deve ser solicitado com antecedência à área de Tecnologia da Informação da CNEN em sua respectiva unidade;
- ii. fica permanentemente proibida a instalação de quaisquer softwares sem licença de uso;
- iii. a área de Tecnologia da Informação da CNEN fica autorizada a desinstalar todo e qualquer software sem licença de uso;
- iv. a área requisitante deve solicitar às áreas de TIC prévia aprovação técnica, a qual conterà regras de segurança a fim de se manter protegidas as informações veiculadas;
- v. os dados de entrada de aplicações devem ser validados de forma a garantir que são corretos e apropriados;
- vi. os dados de saída das aplicações devem ser validados para assegurar que o processamento das informações armazenadas esteja correto e apropriado às circunstâncias;
- vii. a implementação de mudanças deve ser controlada por meio de gerenciamento formal de mudanças;
- viii. o gerenciamento de mudanças deve garantir o retorno ao estado anterior quando ocorrer alguma falha no procedimento;
- ix. as aplicações críticas da CNEN devem ser analisadas criticamente e testadas quando sistemas operacionais forem alterados (novas versões ou instalação de patches), para garantir que não haverá impacto adverso nas operações da CNEN ou na segurança;
- x. as informações acerca das vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas em tempo hábil, avaliada a exposição da CNEN a essas vulnerabilidades, e tomadas as medidas apropriadas para lidar com os riscos associados;

Art. 51. Cabem às áreas de Tecnologia da Informação da CNEN e unidades, por meio de servidores designados, a supervisão e o monitoramento do desenvolvimento terceirizado de software de forma a garantir que critérios de segurança, qualidade, conformidade e desempenho sejam devidamente implementados;

Parágrafo único: Nos casos em que for impreterível ao usuário final possuir privilégios de administrador do computador, seja para desenvolvimento de softwares ou para softwares e atividades que assim o exijam, o usuário deverá preencher e assinar um termo de responsabilidade com justificativa e anuência formal de sua chefia imediata e aprovada pela área competente de TIC e pelo responsável da unidade administrativa, ou quem este último designar.

Art. 52. A CNEN, por meio da Coordenação-Geral de Ciência e Tecnologia da Informação da Diretoria de Gestão Institucional, deve avaliar o estabelecimento de procedimentos a serem seguidos para cumprimento desta seção.

SEÇÃO XXI

GESTÃO DA SEGURANÇA NA COMUNICAÇÃO

Art. 53. A gestão da segurança na comunicação seguirá às seguintes diretrizes:

i. a divulgação de informações nos meios de comunicação social, incluindo internet, estará de acordo com a Política de Segurança da Informação e Comunicação da CNEN e da Política de Segurança Institucional - PSI;

ii. nome, marcas e símbolos institucionais do órgão somente podem ser divulgados e publicados de acordo com regulamentação específica;

iii. o servidor que repassar, sem autorização, informações estratégicas, operacionais, de segurança e de inteligência da CNEN, estará sujeito às sanções administrativas, cíveis e penais cabíveis.

Art. 54. Divulgação de Imagens Sensíveis:

i. a divulgação de imagens (fotografias, vídeos, desenhos, dentre outros) associadas às instalações e atividades consideradas sensíveis, deve ser precedida de análise de risco, considerando a necessidade de preservação dos aspectos de segurança física das instalações, de ativos e do conhecimento produzido na instituição.

ii. a unidade deverá realizar o mapeamento das áreas e das informações consideradas sensíveis à divulgação de imagens, de maneira a não restringir a difusão do conhecimento científico e tecnológico, bem como a divulgação institucional, através de imagens não elencadas como sensíveis.

Art. 55. A CNEN, por meio da Coordenação de Comunicação ligada ao Gabinete da Presidência, deve avaliar o estabelecimento de procedimentos a serem seguidos para cumprimento desta seção.

SEÇÃO XXII

GESTÃO DE RECURSOS HUMANOS

Art. 56. A Gestão de Recursos Humanos deve observar as seguintes diretrizes:

i. Os Servidores, Colaboradores e prestadores de serviço da CNEN devem conhecer e cumprir a Política de Segurança da Informação e Comunicação (POSIC); e

ii. O estabelecimento de procedimento específico de segurança da informação na gestão de recursos humanos da CNEN deve ser avaliado, por meio da Coordenação-Geral de Recursos Humanos da Diretoria de Gestão Institucional.

SEÇÃO XXIII

PROTEÇÃO DE DADOS PESSOAIS

Art. 57. Os dados privados, pessoais e ou sensíveis do titular e dos seus dependentes devem ser processados de forma legal, justa e transparente em relação aos seus titulares e observará as seguintes diretrizes:

i. devem ser coletados para fins específicos, explícitos e legítimos e não processados posteriormente de maneira incompatível com esses objetivos;

ii. devem estar adequados, relevantes e limitados ao uso necessário e em relação aos fins para os quais são destinados e/ou processados;

iii. quando solicitado pelo titular e/ou quando necessário, os dados devem ser atualizados;

iv. Os dados pessoais poderão ser armazenados desde que sejam processados exclusivamente para arquivamento no interesse público, para fins de pesquisa científica ou histórica ou

para fins estatísticos sujeitos à implementação das medidas técnicas e organizacionais apropriadas exigidas pela Lei nº 13.709/2018;

v. Dados pessoais/privados sensíveis deverão ser tratados de forma diferenciada; e

vi. As atribuições e responsabilidades do profissional responsável (Encarregado de Dados Pessoais) pela proteção de dados pessoais/privados e informações sensíveis devem ser exercidas por servidor designado por intermédio de portaria do Presidente da CNEN para a unidade Sede (que inclui escritórios, distritos e CRCN-CO) e demais unidades da CNEN com CNPJ próprio.

Art. 58. A CNEN, por meio do Gabinete da Presidência, deve avaliar o estabelecimento de procedimentos a serem seguidos para o cumprimento desta seção.

SEÇÃO XXIV

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 59. A Gestão da Segurança da Informação e Comunicação da CNEN deverá estar alinhada a esta Política e à Política de Segurança Institucional da CNEN.

Art. 60. São competências da CNEN, no âmbito da POSIC:

i. aplicar ações corretivas e disciplinares cabíveis nos casos de quebra de segurança, por meio da Corregedoria da Instituição;

ii. nomear gestores específicos às seções desta POSIC;

iii. instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais.

Art 61. As competências do Comitê de Segurança Institucional - CSI estão descritas na Política de Segurança Institucional, que possui uma seção específica de Segurança da Informação e Comunicação. Compete ao Comitê, no escopo desta Política:

i. propor a revisão da POSIC e dos atos normativos dela decorrentes, sempre que julgado necessário para preservar a disponibilidade, a integridade e a confidencialidade das informações da CNEN;

ii. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicação;

iii. avaliar e dar parecer acerca dos planos de continuidade de operações e serviços, ou as atualizações, apresentados semestralmente pelas unidades operacionais da CNEN;

iv. propor alterações na Política de Segurança da Informação e Comunicação (POSIC);

v. propor normas e procedimentos internos relativos à segurança da informação e comunicação, em conformidade com as legislações existentes sobre o tema;

Art. 62. O Gestor de Segurança da Informação da CNEN será o titular do cargo de Coordenador-Geral de Ciência e Tecnologia da Informação da Diretoria de Gestão Institucional da CNEN, ou seu substituto nas situações de impedimento;

Art. 63 O Gestor da Informação e Comunicação da CNEN será o titular do cargo do Chefe de Gabinete da Presidência da CNEN, ou seu substituto nas situações de impedimento;

Art. 64. São atribuições do Gestor de Segurança da Informação e do Gestor da Informação e Comunicação da CNEN:

i. assessorar o Comitê de Segurança Institucional - CSI nos assuntos pertinentes à Segurança da Informação e Comunicação;

ii. promover a melhoria contínua dos processos de gestão da segurança da informação;

iii. acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

iv. propor recursos necessários às ações de segurança da informação e comunicação;

v. propor e receber propostas de ajustes corretivos e de melhoria a serem incluídos nas revisões da Política de Segurança da Informação e Comunicação da CNEN (POSIC).

Art. 65. São responsabilidades atribuídas aos usuários que utilizam os recursos de processamento pertencentes ou controlados pela CNEN:

i. conhecer e cumprir a POSIC - Política de Segurança da Informação e Comunicação;

ii. dentro das instalações da CNEN, portar crachá de identificação de maneira visível e/ou uniforme para os cargos que o exigirem;

iii. manter sob proteção e sigilo a sua senha pessoal, e trocá-la periodicamente;

iv. zelar pelas informações e equipamentos disponibilizados para a execução do seu serviço;

v. ao tomar conhecimento de qualquer incidente de segurança da informação, notificar o fato, imediatamente, ao Comitê de Segurança Institucional - CSI da CNEN; e

vi. participar de eventos promovidos pelo CSI relacionados à segurança de informação e comunicação.

Art. 66. Os casos omissos serão resolvidos pelo Presidente da CNEN.

FIM DO DOCUMENTO