PORTARIA CNEN-PR Nº 012, DE 23 DE MARÇO DE 2018.

*O **PRESIDENTE DA COMISSÃO NACIONAL DE ENERGIA NUCLEAR (CNEN),** no uso das atribuições que lhe confere o artigo 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, tendo em vista o relatório apresentado pelo Grupo de Trabalho instituído pela Portaria CNEN-PR nº 41, de 25/09/2017, com a finalidade de elaborar a Política de Segurança Institucional e o Plano de Segurança Institucional, e;*

Considerando a relevância da segurança institucional para o exercício das funções legais da CNEN;

Considerando a necessidade de desenvolver a cultura de segurança que englobe a proteção e salvaguarda das pessoas, do material, das áreas e instalações, e da informação;

Considerando a necessidade de instituir uma política uniforme e um sistema nacional de segurança institucional com o estabelecimento de diretrizes gerais e mecanismos capazes de garantir as condições necessárias para o pleno exercício das atividades da instituição e de seus integrantes,

R E S O L V E:

Art. 1º Aprovar a Política de Segurança Institucional (PSI) e o Plano de Segurança Institucional (PLSI) da CNEN, constantes nos Anexos I e II desta Portaria.

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

PAULO ROBERTO PERTUSI
Presidente

ANEXO 1
POLÍTICA DE SEGURANÇA INSTITUCIONAL DA CNEN

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1° Ficam instituídas a Política de Segurança Institucional da Comissão Nacional de Energia Nuclear – PSI/CNEN e o Sistema de Segurança Institucional da CNEN – SSI/CNEN com a finalidade de integrar as ações de planejamento e de execução das atividades de segurança institucional no âmbito da Comissão Nacional de Energia Nuclear e garantir o pleno exercício de suas atividades.

§1° A PSI/CNEN constitui as diretrizes gerais que orientará o Plano de Segurança Institucional, visando à segurança das pessoas, materiais, áreas, instalações e informações da CNEN.

§2° O SSI/CNEN será coordenado pela Assessoria da Presidência da CNEN, por meio do Comitê Gestor de Segurança Institucional da CNEN – CGSI/CNEN e pelos Comitês Executivos de Segurança Institucional de cada unidade da CNEN - CESI, com o objetivo de articular a proteção integral de cada unidade.

CAPÍTULO II
DA ATIVIDADE DE SEGURANÇA INSTITUCIONAL
Seção I
Dos Princípios

Art. 2° A política de segurança institucional será desenvolvida no âmbito da CNEN com a observância, entre outros, dos seguintes princípios:

I – proteção aos direitos fundamentais e respeito aos princípios constitucionais reitores da atividade administrativa;

II – orientação de suas práticas pela ética profissional, cultuando os valores fundamentais do Estado Democrático de Direito;

III – atuação preventiva e proativa, de modo a possibilitar a estimativa das ameaças, visando à antecipação e neutralização de atos mal-intencionados;

IV – profissionalização da atividade, inclusive, com estreita conexão com outras áreas internas para proteção integral da Instituição e de seus integrantes;

V – integração da CNEN com outros órgãos essenciais à atividade de segurança institucional;

VI – orientação da atividade no que tange aos efeitos de acidentes naturais;

VII – capacitação dos recursos humanos com vistas à proteção de seus ativos, mormente, materiais, áreas, instalações e informações, bem como, os segmentos de tecnologia sensível;

VIII – reavaliação e atualização permanente de normas e procedimentos estabelecidos a partir da Política;

IX – implementação de ações em caráter permanente com o objetivo de desenvolver uma cultura de segurança institucional; e

X - observância à legislação pertinente, inclusive às normas da CNEN quando aplicáveis.

Seção II
Das Medidas de Segurança Institucional

Art. 3° A segurança institucional compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações de qualquer natureza que constituam ameaça à salvaguarda da Instituição e de seus integrantes, inclusive no que tange à sua imagem e reputação.

§1º As medidas a que se reporta o caput compreendem a segurança orgânica e a segurança ativa.

§2º A segurança orgânica é composta pelos seguintes grupos de medidas:

I – segurança de recursos humanos;

II – segurança de material;

III – segurança de áreas e instalações;

IV – segurança da informação.

§3º A segurança ativa compreende ações de caráter proativo e englobam, no âmbito da CNEN, medidas de contrassabotagem, de contraespionagem, de contra crime organizado, de contrapropaganda, de contra vazamentos não-intencionais e de contra sinistros de qualquer natureza.

Subseção I
Da Segurança de Recursos Humanos

Art. 4° A segurança de recursos humanos compreende o conjunto de medidas voltadas a proteger a integridade física de servidores e colaboradores em face dos riscos, concretos ou potenciais, decorrentes do desempenho das funções institucionais.

Subseção II
Da Segurança de Material

Art. 5° A segurança de material compreende o conjunto de medidas voltadas a proteger o patrimônio físico, bens móveis e imóveis, materiais radioativos e nucleares, pertencentes à CNEN ou sob sua responsabilidade.

Subseção III
Da Segurança de Áreas e Instalações

Art. 6° A segurança de áreas e instalações compreende o conjunto de medidas voltadas a proteger o espaço físico onde se realizam atividades da CNEN ou aqueles sob sua responsabilidade.

Subseção IV
Da Segurança da Informação

Art. 7° A segurança da informação compreende o conjunto de medidas voltadas a proteger dados e informações sensíveis ou sigilosos, cujo acesso ou divulgação não autorizados possa acarretar prejuízos de qualquer natureza à CNEN ou proporcionar vantagem a atores antagônicos.

§1º A segurança da informação visa garantir a integridade, o sigilo, a autenticidade, a disponibilidade, o não repúdio e a atualidade do dado, informação ou conhecimento.

§2º A segurança da informação, pela sua relevância e complexidade, desdobra-se nos subgrupos de: segurança da informação nos meios de tecnologia da informação; segurança da informação nos recursos humanos; segurança da informação na documentação; e segurança da informação nas áreas e instalações.

Subseção V
Das Medidas de Segurança Ativa

Art. 8° A contrassabotagem compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações intencionais contra materiais, áreas ou instalações da Instituição que possam causar interrupção de suas atividades e/ou impacto físico e psicológico sobre seus integrantes.

Art. 9° A contraespionagem compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações adversas e dissimuladas de busca de dados e informações sensíveis ou sigilosos.

Art. 10° O contra crime organizado compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações adversas de qualquer natureza contra a Instituição e seus integrantes, oriundas de organizações criminosas.

Art. 11 A contrapropaganda compreende o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar abusos, desinformações e publicidade enganosa de qualquer natureza contra a Instituição.

Art. 12 As medidas contra vazamentos não-intencionais compreendem ações para impedir a difusão de assuntos sensíveis ou sigilosos originada de ações não intencionais.

Art. 13 As medidas contra sinistros compreendem ações com o intuito de impedir a destruição ou dano, total ou parcial, de informações sensíveis e sigilosas provocada por forças da natureza ou qualquer outro agente externo ou interno de forma não intencional.

Seção III
Da Gestão de Risco

Art. 14 A Instituição deverá adotar as medidas necessárias para que os riscos a que está submetida sejam identificados, analisados, avaliados, tratados e monitorados de modo dinâmico, permanente, profissional e proativo, em consonância com a Política de Gestão de Risco da CNEN.

Subseção I
Do Planejamento de Contingência, do Controle de Danos e da Gestão de Continuidade de Negócios

Art. 15 A CNEN implementará e manterá um plano de contingência, controle de danos e gestão de continuidade de negócios no âmbito de suas instalações.

§1º O planejamento de contingência compreende a previsão de técnicas, inclusive de recuperação, e procedimentos alternativos a serem adotados para efetivar processos que tenham sido interrompidos ou que tenham perdido sua eficácia.

§2º O controle de danos compreende uma série de medidas que visem avaliar a profundidade de um dano decorrente de um incidente, o comprometimento dos ativos da Instituição e as suas consequências para esta, inclusive no que se refere à imagem institucional.

§3º A gestão de continuidade de negócios compreende a identificação de ameaças potenciais e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem, com o objetivo de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da CNEN e suas atividades de valor agregado.

CAPÍTULO III
DO SISTEMA DE SEGURANÇA INSTITUCIONAL DA CNEN

Art. 16 O Sistema de Segurança Institucional da CNEN – SSI/CNEN é composto:
I – pelo Comitê Gestor de Segurança Institucional - CGSI; e
II – pelos Comitês Executivos de Segurança Institucional - CESI

§1º O CGSI é composto pela Assessoria da Presidência da CNEN, na função de coordenador, e por representantes das Diretorias de Pesquisa e Desenvolvimento, Radioproteção e Segurança Nuclear e Gestão Institucional.

§2º Ficam instituídos os CESI nas seguintes unidades da CNEN: Sede, IPEN, IRD, IEN, CDTN, CRCN-NE, CRCN-CO e LAPOC.

§3º O CESI de cada unidade será criado pelo seu dirigente máximo, ao qual ficará vinculado diretamente. Na Sede, o CESI deve ser criado e vinculado à DGI.

Art. 17 O Comitê Gestor de Segurança Institucional – CGSI, vinculado à Presidência da CNEN, como órgão consultivo, deliberativo e propositivo, tem a função de promover o direcionamento das ações de segurança institucional da CNEN, por meio de deliberações que promovam a uniformização, padronização e integração dos Planos de Segurança Orgânica - PLSO e de Ações de Segurança Institucional setoriais, competindo-lhe:

I – aprovar os Planos de Segurança Orgânica das unidades;

II – propor metas nacionais para atuação de segurança institucional no âmbito da CNEN;

III – incentivar a adoção de boas práticas em segurança institucional;

IV – propor critérios para orientar a aquisição de bens e serviços de segurança institucional na CNEN;

V – incentivar a utilização de padrões governamentais em segurança institucional;

VI – acompanhar, permanentemente, os cenários de interesse da CNEN no que se refere à segurança institucional, de modo a proporcionar suporte adequado ao desempenho das funções da instituição;

VII – propor programas de conscientização e capacitação de pessoas, necessários à preparação adequada dos integrantes da CNEN para o desempenho das atividades de segurança institucional e praticar outros atos necessários ao cumprimento do seu objetivo e compatíveis com suas atribuições.

Art. 18 Compete aos Comitês Executivos de Segurança Institucional – CESI o seguinte:

I – instituir planos de segurança orgânica e procedimentos necessários à execução de tais planos, inclusive com cronogramas específicos, tudo em consonância com as especificidades locais e com a presente Política e com o Plano de Segurança Institucional da CNEN;

II – desenvolver atitudes favoráveis ao cumprimento de normas de segurança no âmbito local, estimulando o comprometimento e o apoio explícito de todos os níveis de direção e chefia, sem prejuízo das medidas de responsabilização pelo descumprimento;

III – desenvolver e difundir uma mentalidade de segurança institucional, fazendo com que todos os integrantes da unidade compreendam as necessidades das medidas adotadas e incorporem o conceito de que cada um é responsável pela manutenção do nível de segurança adequado;

IV – elaborar programas de divulgação e capacitação de conteúdos de segurança para todos os integrantes da unidade;

V – intercambiar informações necessárias à produção de conhecimentos relacionados com as atividades de segurança institucional

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 19 As normas, procedimentos e técnicas de segurança devem ser exequíveis e a sua implementação acompanhada de um programa de capacitação e treinamento dos integrantes da CNEN.

Art. 20 Os casos omissos e as dúvidas suscitadas na aplicação da presente Política de Segurança Institucional serão dirimidos pelo Comitê Gestor de Segurança Institucional – GSI.

ANEXO 2

PLANO DE SEGURANÇA INSTITUCIONAL DA CNEN

CAPÍTULO I
APRESENTAÇÃO

O presente Plano de Segurança Institucional – PLSI tem por finalidade implantar atividades de segurança institucional no âmbito da Comissão Nacional de Energia Nuclear – CNEN e orientar a elaboração do Plano de Segurança Orgânica - PLSO de cada unidade, em conformidade com a Política de Segurança Institucional da CNEN – PSI/CNEN.

Segurança Institucional compreende o conjunto de medidas adotadas para prevenir, detectar, obstruir e neutralizar ações de qualquer natureza que constituam ameaça à salvaguarda da Instituição e de seus integrantes, inclusive no que tange à sua imagem e reputação.

A Segurança Institucional, no âmbito da CNEN, é estratificada em níveis de gestão administrativa e se estrutura por meio da Política de Segurança Institucional, do Plano de Segurança Institucional e do Plano de Segurança Orgânica de cada unidade.

A Política de Segurança Institucional refere-se ao nível de gestão política e estabelece as diretrizes gerais de segurança e áreas afins.

O Plano de Segurança Institucional abrange todos os grupos de medidas de segurança previstos na Política de Segurança Institucional e se refere ao nível de gestão estratégica, definindo as ações, projetos e programas necessários ao alcance dos objetivos específicos de Segurança Institucional. Aplica-se às unidades da CNEN e aos seus integrantes naquilo que se refere às práticas e aos procedimentos nas suas respectivas esferas de atribuições.

O Plano de Segurança Orgânica refere-se ao nível de gestão tática e se desdobra em normatização de rotinas e procedimentos específicos para cada unidade da Instituição, de acordo com suas características e peculiaridades, adequadas às necessidades de segurança locais e regionais.

CAPÍTULO II
ESTRUTURA ORGANIZACIONAL E ATRIBUIÇÕES

As funções de gestão de segurança institucional na CNEN serão desempenhadas pela Presidência da CNEN, no âmbito nacional e pelos Dirigentes máximos, no âmbito das respectivas unidades.

A coordenação técnica e operacional da atividade de segurança institucional será de responsabilidade da Assessoria da Presidência da CNEN, no âmbito institucional, por meio do Comitê Gestor de Segurança Institucional – CGSI e das respectivas Unidades de Segurança, no âmbito das unidades, por meio dos Comitês Executivos de Segurança Institucional – CESI.

2.1 Compete ao Comitê Gestor de Segurança Institucional – CGSI:

I - planejar, coordenar, orientar e supervisionar as atividades de segurança institucional no âmbito da CNEN e executar na unidade Sede;

II - propor a atualização e o aprimoramento periódico da Política de Segurança Institucional e do Plano de Segurança Institucional da CNEN;

III - subsidiar as unidades da CNEN na elaboração do Plano de Segurança Orgânica e aprovar os mesmos;

IV - assessorar a Presidência da CNEN na homologação dos Planos de Segurança Orgânica das unidades da CNEN e nos demais assuntos referentes à segurança institucional;

V - desenvolver a cultura de segurança institucional na CNEN;

VI – propor a elaboração ou a revisão de normas de segurança institucional para cada grupo de medidas previsto na Política de Segurança Institucional;

VII - desenvolver uma cultura de inovação para a área de segurança institucional da CNEN, inclusive promovendo estudos, avaliações e aplicações de novas tecnologias, táticas, técnicas e procedimentos de segurança;

VIII - propor programas de formação de recursos humanos ou treinamentos continuados na área de segurança institucional para os membros e servidores com funções de segurança;

IX - estabelecer os mecanismos e procedimentos necessários às comunicações e ao intercâmbio de informações e conhecimentos no âmbito da CNEN, observando as medidas necessárias para manutenção da segurança e sigilo, com base na legislação em vigor;

X - estabelecer um canal de comunicação com os CESI, de modo a compartilhar conhecimentos, dados e informações;

XI - propor instrumentos de cooperação técnica com órgãos de inteligência nacionais e internacionais e com outras instituições, no que se refere às questões de segurança institucional; e

XII - acompanhar, permanentemente, os cenários de interesse da CNEN, no que se refere à segurança institucional, de modo a proporcionar suporte adequado ao desempenho das funções.

2.2 Compete aos Comitês Executivos de Segurança Institucional - CESI:

I - planejar, coordenar, executar, orientar e supervisionar as atividades de segurança institucional no âmbito da respectiva unidade da CNEN;

II - assessorar o Dirigente da unidade nas questões relativas à segurança institucional;

III - elaborar e implantar o Plano de Segurança Orgânica da respectiva unidade da CNEN e normas de segurança para cada grupo de medida previsto na Política de Segurança Institucional observando as recomendações do CGSI;

IV - acompanhar os cenários regionais e locais de interesse da CNEN, no que se refere à segurança, a fim de proporcionar suporte ao desempenho das funções institucionais;

V - seguir as recomendações e orientações técnicas do CGSI e com ele compartilhar conhecimentos, dados e informações, sem prejuízo da subordinação administrativa à respectiva unidade da CNEN;

VI - promover a conscientização dos integrantes da unidade quanto à importância da segurança institucional; e

VII - planejar e executar ações de capacitação de recursos humanos nas atividades de segurança institucional.

CAPÍTULO III
DO PLANO DE SEGURANÇA ORGÂNICA

O Plano de Segurança Orgânica das unidades da CNEN – PLSO, composto por rotinas e procedimentos de segurança, deve ser orientado para as necessidades e especificidades locais.

O PLSO será integrado por procedimentos de segurança e anexos que regulamentem ações de proteção relativos a cada grupo de medidas de segurança.

Cada unidade da CNEN, por meio do CESI, será responsável por elaborar e executar seu PLSO com o apoio técnico (modelo de plano, capacitação e revisão) do CGSI.

CAPÍTULO IV
SEGURANÇA INSTITUCIONAL

4.1 Medidas de Segurança

A Segurança Institucional compreende o conjunto de medidas de segurança orgânica e de segurança ativa.

4.1.1 A segurança orgânica é composta pelos seguintes grupos de medidas:

I - segurança de recursos humanos;

II - segurança de materiais;

III - segurança das áreas e instalações; e

IV - segurança da informação.

4.1.2 A segurança ativa é composta pelos seguintes grupos de medidas:

I -contrassabotagem;

II - contraespionagem;
III - contra crime organizado;
IV - contra propaganda;
V - contra vazamentos não-intencionais;
VI - contra sinistros de qualquer natureza.

4.1.3 Na implementação das medidas de segurança, além das normas constitucionais e legislação infraconstitucional, deverão ser observados a Política de Segurança Institucional, o Plano de Segurança Institucional, os Planos de Segurança Orgânica e os atos normativos da CNEN aplicáveis.

4.2 Segurança de Recursos Humanos

A segurança de recursos humanos compreende o conjunto de medidas voltadas a proteger a integridade física de servidores e colaboradores em face dos riscos, concretos ou potenciais, decorrentes do desempenho das funções institucionais.

Pela especificidade e circunstância do trabalho, é fundamental que os integrantes da CNEN tenham uma cultura de conscientização e sensibilização quanto às prováveis ameaças, seguindo procedimentos de proteção e preservação de sua integridade física.

4.2.1 Segurança da Integridade Física

As unidades da CNEN devem seguir as seguintes orientações:

I - Deverão ser elaborados procedimentos específicos para otimizar as ações de proteção pessoal no PLSO de cada unidade;

II – Os servidores e colaboradores devem ser orientados a respeito das normas de segurança institucional da CNEN;

III – Devem ser elaborados programas de capacitação e treinamento voltados para aspectos de segurança institucional, em coordenação com o CESI, com a finalidade de se buscar uma atitude de segurança adequada.

4.2.2 Segurança do Processo Seletivo, do Ingresso e do Desligamento

I - Os concursos de admissão para os servidores da CNEN devem conter medidas e procedimentos em seus respectivos editais que contemplem ações para evitar o ingresso de pessoas com características ou antecedentes que possam comprometer a segurança da Instituição. Procedimento similar será executado para contratação de pessoas em cargos comissionados;

II - Os novos integrantes da CNEN devem ser submetidos a um curso de ingresso ou adaptação, com conteúdo relativo às funções a serem exercidas e à segurança institucional;

III - Em situações de desligamento de servidores devem ser adotadas medidas de segurança, tais como: entrevista com o desligado, orientando-o sobre a necessidade de manter discrição sobre os assuntos institucionais; verificação de entrega de material ou equipamento acautelado com o desligado; verificação da existência de pendências de

ordem individual nas áreas de recursos humanos; e verificação da existência de pendências em projetos, serviços ou trabalhos realizados pelo desligado.

4.3 Segurança de Materiais

A segurança de material compreende o conjunto de medidas voltadas a proteger o patrimônio físico, bens móveis e imóveis, materiais radioativos e nucleares, pertencentes à CNEN ou sob sua responsabilidade.

Os registros de incidente de segurança devem ser controlados em cada unidade da CNEN para levantar e analisar a situação e as circunstâncias em que o fato ocorreu, com a finalidade de estabelecer medidas corretivas e preventivas.

Além dos procedimentos de controle patrimonial previstos em ato normativo específico da CNEN, devem ser adotadas as seguintes medidas:

I - A produção (quando for o caso), o recebimento, a distribuição, o manuseio, o armazenamento e o acondicionamento de materiais devem seguir as normas técnicas próprias;

II - Os materiais sensíveis ou de alto valor devem ser armazenados ou acondicionados em condições especiais de proteção, de acordo com a sua necessidade. O acesso às áreas ou locais de armazenamento ou acondicionamento de tais materiais deve ser restrito, com a devida sinalização;

III - As áreas de segurança das unidades da CNEN devem expedir orientação para servidores e colaboradores a respeito de medidas adicionais de segurança a serem atendidas em face das características técnicas de cada material;

IV - Os materiais em trânsito, conforme a necessidade e de acordo com suas características, devem receber medidas adicionais de segurança para sua proteção;

V - A saída de material das unidades da CNEN deve atender normas administrativas e constar em registro, mantido pelas áreas de segurança das unidades, em conjunto com os demais setores;

VI - Equipamentos e outros materiais portáteis, em viagens, devem ser conduzidos como bagagem de mão;

VII - O material a ser descartado ou doado contendo dados e informações institucionais deve ter o seu conteúdo destruído pela área competente de forma segura antes da sua eliminação ou entrega;

VIII - Todo incidente de segurança envolvendo material deve ser informado às áreas de segurança das unidades da CNEN;

IX - O descarte de material que exige medidas especiais para recolhimento ou eliminação, quando inservível, deve ser feito de acordo com as normas do respectivo órgão regulador;

X - O armazenamento ou o acondicionamento de materiais que exijam condições especiais deve seguir o constante em normas técnicas específicas;

XI - Os equipamentos e outros materiais da CNEN devem ser instalados de forma a: reduzir riscos ambientais em caso de um incidente de segurança; reduzir acessos

desnecessários às áreas de trabalho; permitir a sua utilização de forma segura; e atender parecer técnico da área específica;

XII - Todos os equipamentos ou outros materiais que exijam cuidados de manutenção devem ser incluídos em planejamentos de manutenção coordenados pelas respectivas áreas responsáveis;

XIII - Os equipamentos e outros materiais que exijam capacitação técnica para sua operação somente podem ser utilizados por pessoa capacitada;

XIV - As atividades de operação e manuseio de equipamentos e outros materiais nas unidades da CNEN devem estar em conformidade com as normas de segurança no trabalho;

XV - As bibliotecas das unidades da CNEN devem possuir sistemas de controle do acervo;

XVI - Em caso excepcional de aquisição de material externo ou de recebimento de bens em doação ou cessão, tais como equipamentos de informática e telefonia, as unidades da CNEN devem efetuar análise técnica com o intuito de verificar a existência de alguma anormalidade. Em caso de identificação de conteúdo não utilizado ou autorizado pela Instituição, a respectiva área técnica deve proceder à sua exclusão.

4.4 Segurança de Áreas e Instalações

A Segurança de Áreas e Instalações constitui-se em um grupo de medidas orientadas para proteger o espaço físico sob responsabilidade da CNEN.

Os sistemas de segurança devem ser integrados e complementares, aumentando o espectro de proteção.

4.4.1 A Segurança das Áreas e Instalações engloba:

I - Sistema Físico: composto por guardas que executam serviços de vigilância, de controle de acesso e de resposta a incidentes;

II - Sistema Eletrônico: composto por equipamentos eletrônicos de segurança, como sensores, circuito fechado de televisão (CFTV), alarmes, fechaduras eletrônicas, sistemas de registro, catracas, cancelas, sistema de controle de acesso etc; e

III - Sistema de Barreiras: envolve as diversas barreiras para segurança dos perímetros.

4.4.2 Barreiras Físicas

As unidades da CNEN devem seguir as seguintes orientações:

I - Devem-se instalar barreiras físicas para retardar o acesso às áreas de segurança das unidades da CNEN, possibilitando a detecção e a ação da força de segurança em tempo hábil;

II - Os perímetros das unidades da CNEN devem possuir barreiras dispostas de acordo com avaliação de risco do local, que se estendem do perímetro externo e chegam até as salas e gabinetes, passando pelas portarias, constituindo-se em linhas de proteção;

III - Os perímetros externos devem ser cercados por muros ou cercas. Em áreas de alto risco de invasão, as cercas ou muros podem conter concertinas ou cercas elétricas

nas suas extremidades. Nos casos onde houver cercas eletrificadas, devem ser afixados avisos de advertência ao longo de todo perímetro, alertando sobre sua existência;

IV - As guaritas de vigilância devem possuir um campo de visada que possibilite vigiar as áreas externas e/ou internas das unidades da CNEN;

V - Os prédios e instalações principais devem possuir serviço de portaria com equipamentos, computadores, telefone e sistema para cadastro de pessoal;

VI - Os locais de entrada nos perímetros externos e internos devem, preferencialmente, possuir portões ou portas de acesso com mecanismos que permitam o seu chaveamento;

VII - A iluminação de áreas externas e estacionamentos deve ser suficiente e adequada para possibilitar a vigilância, detecção e certificação de intrusão;

VIII - Os muros e cercas dos perímetros devem estar livres de vegetação ou outros obstáculos, de forma a possibilitar a visualização e inspeção visual pelos integrantes da força de segurança;

IX - O cabeamento da rede elétrica e do sistema de CFTV, quando houver, deve ser protegido, em particular nas áreas externas. Nas áreas internas, os quadros de energia elétrica devem ser de fácil acesso, livre de obstáculos;

X - O cabeamento da rede lógica deve ser protegido. Os quadros e racks devem possuir sistemas de fechadura com chave ou sistema de controle de acesso, a fim de impedir o acesso indevido;

XI - O cabeamento de energia elétrica deve ser instalado separadamente do cabeamento da rede lógica;

XII – As portas, janelas, cercas, portões, dutos de ventilação e entradas de ar-condicionado devem possuir proteção com características de resistência mecânica compatíveis e balanceadas que impeça o acesso indevido, quando necessário;

XIII - As áreas destinadas à circulação do público externo devem ser dispostas em locais favoráveis ao controle do fluxo de visitantes. Respeitando-se a arquitetura das edificações, as áreas de atendimento ao público, cantina, restaurante, setor de comunicação social, sala do Plano Médico, serviço de saúde e outras repartições de uso similar devem ser dispostas em locais que evitem o trânsito de visitantes por instalações sensíveis;

XIV - As unidades da CNEN que possuam postos de atendimento avançado de agências bancárias e caixas eletrônicos em suas dependências devem cumprir a legislação específica relacionada à segurança do local;

XV - As unidades da CNEN devem regular em seus respectivos Planos de Segurança Orgânica as rotinas e horários para abastecimento de valores nos caixas eletrônicos existentes em suas dependências; e

XVI - As salas onde se guardam materiais de alto custo e/ou sensíveis devem possuir teto com laje, grades em suas janelas, portas, sistema de alarme e, se necessário, posto armado, além de controle específico de chaves, CFTV e fechadura eletrônica.

4.4.3 Controle de Acesso

As unidades da CNEN devem seguir as seguintes orientações:

I - As entradas dos prédios ou instalações devem possuir um serviço de portaria, por vigilância 24 horas, destinado à segurança do local;

II - As portarias de acesso devem ter um serviço de recepcionistas, para realizar o registro de visitantes que entram no prédio. Os registros devem conter dados pessoais de identificação (inclusive CPF), data e hora do acesso, locais a que se dirigem, órgão de origem (quando cabível) e telefones para contato. Tais registros devem ser realizados, preferencialmente, por meio de sistemas informatizados que permitam fotografar os visitantes ou digitalizar documentos de identificação. Antes do acesso do visitante à área desejada, deve ser feito contato com uma pessoa do setor de destino para a devida autorização. A unidade deverá adotar as providências necessárias para o controle do deslocamento do visitante nas dependências internas, inclusive, quando possível, com a utilização de sistemas informatizados e barreiras que permitam, tão somente, o acesso ao setor de destino;

III - As portarias das unidades devem possuir um sistema de catracas com leitores de cartão (ou similar) para registros de servidores, estagiários, prestadores de serviço, terceirizados e visitantes;

IV - É obrigatório o uso de crachá de identificação para acesso às áreas e instalações das unidades da CNEN e permanência em seu interior;

V - Em locais onde houver detectores de metais, os portadores de marca passo não serão a eles submetidos, mas devem apresentar documentação que identifique sua situação, submetendo- se a outros meios de vistoria;

VI – As portarias das unidades devem possuir um procedimento de detecção de radiação, a ser definido no PLSO de cada unidade;

VII - As portas devem possuir dispositivos de fechadura com chave. As janelas devem possuir dispositivos de fechadura com trancamento interno. Locais que exigem maior controle de acesso devem possuir fechadura eletrônica controlada por equipamento de controle de acesso e os relatórios de acesso devem ser auditados periodicamente pelo CESI;

VIII - A entrada de servidores em dias e horários sem expediente ou após o expediente deve ser regulada e controlada. Os dados de acesso devem constar em registro específico. Terceirizados não devem acessar as áreas e instalações das unidades da CNEN nos dias e horários sem expediente, exceto em situações de prestação de serviços devidamente autorizados e monitorados;

IX - O estacionamento das unidades da CNEN deve ter o seu procedimento de controle de acesso regulado por norma específica. A entrada e a saída de veículos devem ser registradas em controle específico;

X - O claviculário deve estar localizado em área segura e possuir registro. Os terceirizados não devem ter acesso direto ao claviculário, que ficará sob a responsabilidade da respectiva Unidade de Segurança. Quando for necessário tal acesso, este deve ser feito por vigilantes e com controle de registro. Os relatórios de acesso a claviculários devem ser auditados periodicamente pelo CESI;

XI - Os registros de retirada e entrega de chaves devem possuir itens de controle que permitam auditorias posteriores;

XII - As áreas que abriguem instalações sensíveis e que sejam de acesso restrito devem ser sinalizadas com placas indicativas desta situação;

XIII - Nos casos necessários, o acesso a determinadas áreas será condicionado à credencial de segurança compatível com o grau de sigilo do local;

XIV - A presença de terceirizados de limpeza, serviço de copa, recepcionistas, mensageiros e outros serviços (incluindo manutenção de qualquer tipo) nas salas onde há dados ou informações sigilosas, deve ser supervisionada por servidor;

XV - A presença de fornecedores nas unidades da CNEN deve ser sempre acompanhada de um servidor ou vigilante previamente designado;

XVI - O material do patrimônio somente poderá sair de uma unidade com autorização da área competente, devendo ser registrado na portaria;

XVII - Não será permitido o ingresso de pessoas nas unidades da CNEN portando arma de qualquer natureza, ressalvados os seguintes casos: policiais Federais, Civis e Militares; profissionais de segurança de empresas de escolta de cargas e valores e vigilantes da segurança contratada, quando em serviço; e outros profissionais de segurança, participantes de solenidades ou eventos promovidos pela CNEN, desde que previamente autorizados;

XVIII - Os profissionais de segurança de empresas de escolta de cargas e valores deverão ser acompanhados por vigilante, sendo proibida a transferência de valores entre caminhões caixa-forte nas dependências da CNEN. Os profissionais deverão ser orientados quanto ao horário de realização do serviço e o itinerário a ser percorrido nas unidades da CNEN, evitando ao máximo a circulação em horários de grande deslocamento ou aglomeração de servidores;

XIX - As portarias de acesso das unidades da CNEN devem possuir cofre com abertura digital ou, na sua ausência, artefato similar para guarda de armas, assim como uma caixa de descarga para ações de desmuniciamento do armamento, que deve ser instalada em local reservado;

XX - É vedado o ingresso nas dependências das unidades da CNEN de pessoas: para a prática de comércio e propagandas diversas ou angariação de donativos e congêneres, salvo as campanhas institucionais; para a prestação de serviços autônomos não vinculados a contrato ou convênio firmado com a CNEN; fazendo uso de trajes inadequados, incompatíveis com o decoro, ou de vestimenta que possa atentar contra a moralidade do serviço público, respeitadas as especificidades culturais; portando instrumentos sonoros, fogos de artifícios ou quaisquer objetos que por sua natureza representem risco à incolumidade física ou patrimonial e perturbem o andamento dos serviços; com qualquer espécie de animal, salvo cão-guia de pessoa portadora de deficiência visual, mediante apresentação da carteira de vacina atualizada do animal; e que sejam identificadas como possível ameaça à segurança, à ordem, à integridade patrimonial e física nas dependências da Instituição e cuja forma de apresentação ou atitudes forem consideradas suspeitas para os fins propostos, caso em que o responsável pela segurança na unidade será imediatamente acionado;

XXI - Sempre que as condições técnicas permitirem, os sistemas de registro de pessoas nas portarias das unidades da CNEN devem ser integrados a sistemas de identificação de pessoas e pesquisa de antecedentes;

XXII - Em situações de solenidades e eventos organizados nas unidades da CNEN, os integrantes de serviços de segurança armada de autoridades devem ser previamente identificados para eventuais autorizações de entrada e permanência com armamento;

XXIII - O ingresso de equipamentos de propriedade e de uso particular nas dependências da CNEN deverá ser precedido de registro nas portarias de acesso. A saída dos equipamentos particulares deverá ser autorizada somente mediante a apresentação do protocolo de registro ou documento comprobatório da propriedade do bem;

XXIV - Não é permitida a filmagem ou fotografia no interior das unidades da CNEN sem prévia autorização da autoridade competente, comunicada à respectiva área de segurança institucional;

XXV - A cobertura jornalística, filmagem e fotografia realizadas nas dependências da CNEN serão feitas por profissionais de imprensa previamente credenciados pelo setor de comunicação social da unidade, que deverá manter informada a respectiva área de segurança institucional;

4.4.4 Sistemas de Vigilância Eletrônica

As unidades da CNEN devem seguir as seguintes orientações:

I - As unidades da CNEN, em regra, devem possuir um sistema de Circuito Fechado de Televisão - CFTV com cobertura das áreas e locais sensíveis.

II - Os sistemas de CFTV devem ser monitorados em tempo real e possuir capacidade de armazenamento com qualidade. As salas destinadas aos equipamentos de CFTV devem ter o acesso restrito por sistema de controle de acesso;

III - As salas que abrigam instalações sensíveis devem possuir, sempre, sensores de presença ligados a central de alarme e sistema de controle de acesso, com suporte a registro dos acessos permitidos e das tentativas de acesso inválidas;

IV - Em caso de utilização de alarme, a central deve ser monitorada por vigilante durante 24 horas por dia, 7 dias por semana.

4.4.5 Serviço de Vigilância

As unidades da CNEN devem seguir as seguintes orientações:

I - Os perímetros das unidades da CNEN devem ser protegidos por um serviço de vigilância. A disposição dos respectivos postos deve ser distribuída em função da análise das ameaças e risco previstos para a unidade e registrada no PLSO;

II - Os Procedimentos Operacionais Padrão para cada posto de segurança devem conter os seguintes dados: composição do posto, discriminando o número de vigilantes; finalidade do posto; atribuições dos vigilantes, com detalhamento do que os vigilantes fazem no local; procedimentos comportamentais, em que são discriminados os procedimentos em relação ao tratamento com pessoas, apresentação individual e outros; e procedimentos operacionais, em que é detalhado o que fazer em diversas situações;

III - Nas unidades da CNEN deve-se prever no respectivo instrumento de contrato um supervisor ou líder para fiscalizar o serviço de vigilância e fazer cumprir as normas de segurança;

IV - Os postos de vigilância devem ser dotados de equipamentos redundantes de comunicação para uso dos vigilantes.

4.4.6 Emergência, Prevenção a Pânico e Prevenção e Combate a Incêndio

As unidades da CNEN devem seguir as seguintes orientações:

I - Todas as unidades da CNEN devem possuir um planejamento de prevenção e combate a incêndio em conformidade com a legislação e com as normas técnicas em vigor. Os planos devem ser simples, exequíveis, viabilizar ações com pessoal e material existentes e prever situações em dias e horários com e sem expediente;

II - A instalação dos equipamentos de combate a incêndio deve atender aos requisitos técnicos de utilização de cada dependência, considerando a quantidade de equipamentos existentes e de pessoal;

III - Cada unidade da CNEN deve possuir um serviço de Bombeiro Voluntário, com a participação de servidores e treinamento específico;

IV – O CESI de cada unidade da CNEN deve prever planejamento de capacitação para os integrantes da Brigada de Combate a Incêndio;

V - Devem ser realizados exercícios de evacuação das dependências, de acordo com as especificidades locais;

VI - As unidades da CNEN devem possuir iluminação auxiliar para situações de emergência, independente da rede de energia elétrica convencional;

VII - Os sistemas essenciais que constem na infraestrutura crítica das unidades da CNEN devem possuir alimentação elétrica suplementar em caso de falha ou intermitência no suprimento da rede elétrica comercial;

VIII - As unidades da CNEN devem possuir um planejamento para situações extraordinárias e de emergência, conforme disposto no PLSO.

4.4.7 Prescrições Diversas

As unidades da CNEN devem seguir as seguintes orientações:

I - As pessoas que trabalham em cantinas, restaurantes ou postos avançados de agência bancária nas dependências da unidade da CNEN devem ser registradas na respectiva área de segurança e possuir crachá de identificação;

II - As unidades da CNEN devem possuir um número de telefone destinado a emergências, que deverá ser amplamente divulgado entre os integrantes da unidade;

III - Os projetos de arquitetura para construções de unidades da CNEN devem prever *layouts* de ambientes internos que privilegiem os aspectos de segurança;

IV – O CESI deve disponibilizar apoio técnico às áreas de engenharia e arquitetura das unidades com a finalidade de prever medidas de segurança nas áreas e instalações de futuras unidades da CNEN, com a devida coordenação de ações entre os dois setores para a execução de projetos de construção, desde a sua primeira etapa;

V - As unidades da CNEN devem assegurar que as medidas de segurança de áreas e instalações atendam à legislação trabalhista e ambiental, às normas municipais

aplicáveis e às demais normas técnicas de prevenção e combate a incêndio e de edificações.

4.5 Segurança da Informação

A segurança da informação compreende o conjunto de medidas voltadas a proteger dados e informações sensíveis ou sigilosos, cujo acesso ou divulgação não autorizados possa acarretar prejuízos de qualquer natureza à CNEN ou proporcionar vantagem a atores antagônicos.

A segurança da informação, pela sua relevância e complexidade, desdobra-se nos subgrupos de: segurança da informação nos meios de tecnologia da informação; segurança da informação nos recursos humanos; segurança da informação na documentação; e segurança da informação nas áreas e instalações.

4.5.1 Segurança da Informação nos Meios de Tecnologia da Informação

A Segurança da Informação nos Meios de Tecnologia da Informação constitui um grupo de medidas para salvaguarda da informação, da integridade dos sistemas e dos meios de tecnologia da informação, da confidencialidade da informação nos meios de tecnologia da informação e da disponibilidade dos recursos de tecnologia da informação, englobando as áreas de Informática e Comunicações.

Ressalta-se que os recursos de tecnologia da informação disponíveis da CNEN destinam-se exclusivamente ao suporte das atividades desempenhadas pelos servidores, terceirizados, bolsistas e estagiários.

A seguir são relacionadas medidas de segurança da informação nos meios de tecnologia da informação.

4.5.1.1 Uso de Recursos de Tecnologia da Informação

As unidades da CNEN devem seguir as seguintes orientações:

I - Os recursos de informática e comunicações disponíveis para os usuários da CNEN somente poderão ser utilizados em atividades estritamente relacionadas às funções institucionais;

II - O usuário do recurso de tecnologia da informação é responsável pelo seu estado e funcionamento, devendo comunicar qualquer defeito ou comportamento anormal às áreas de tecnologia da informação das unidades da CNEN;

III - Os programas e sistemas somente poderão ser instalados: de forma automática pelo sistema, por acesso remoto ou presencialmente por profissional autorizado pela área de tecnologia da informação e comunicação de cada unidade da CNEN.

IV - É vedada a instalação e/ou execução de qualquer outro programa ou sistema, exceto em casos de comprovada necessidade do serviço, mediante anuência técnica das áreas de tecnologia da informação das unidades da CNEN e com a autorização da autoridade competente;

V - As áreas de tecnologia da informação das unidades da CNEN deverão prever rotinas de *backup* para as unidades de armazenamento de rede;

VI - A realização de cópias de segurança dos dados armazenados no disco rígido da estação de trabalho será de responsabilidade do usuário da estação;

VII - Os procedimentos e as operações realizados por intermédio das estações de trabalho conectadas à rede serão da responsabilidade dos usuários que nelas estiverem autenticados;

VIII - Ao afastar-se temporariamente da estação de trabalho, o usuário deverá desconectar-se da rede. Além disso, deverá ser implantada uma rotina automática de proteção de tela com senha;

IX - As estações de trabalho e seus periféricos somente poderão ser removidos dos locais de instalação, mesmo que provisoriamente, por servidores das áreas de patrimônio e das áreas de tecnologia da informação das unidades da CNEN.

4.5.1.2 Segurança de Rede e Internet

As unidades da CNEN devem seguir as seguintes orientações:

I - As áreas de armazenamento de dados disponibilizadas aos usuários deverão ser compartimentadas, podendo ser auditadas com a finalidade de identificar utilização irregular;

II - O armazenamento e a transmissão de dados e informações sensíveis ou sigilosas na CNEN nos meios de informática e telefonia serão realizados mediante a utilização de recursos (sobretudo criptografia), padronizados institucionalmente, que garantam a integridade e confidencialidade dos respectivos dados e informações. Para tanto, será elaborado ato normativo específico regulamentando o uso de tais recursos no âmbito da CNEN. A Coordenação Geral da Tecnologia da Informação - CGTI deverá elaborar estudos e prover os meios necessários para viabilizar tais providências;

III - A retirada de dados e informações sigilosos ou sensíveis da Rede Nacional da CNEN e das redes locais das respectivas unidades só poderá ser realizada mediante permissão da autoridade classificadora e por usuário com credencial de segurança com grau de sigilo compatível;

IV - Identificação do usuário e utilização de senha são condições indispensáveis para utilização dos recursos de tecnologia da informação da CNEN;

V - Por ocasião do login do usuário na rede, deverá ser apresentada uma mensagem informando que o acesso e o registro do tráfego na rede serão armazenados para fins de auditoria e responsabilização em caso de descumprimento das normas internas da instituição;

VI - A solicitação para uso dos recursos de tecnologia da informação deverá ser realizada formalmente pela chefia às unidades de TI da CNEN, informando o perfil de utilização.

VII - A remoção, o desligamento e afastamento da função deverão ser tempestivamente informados às unidades de TI da CNEN;

VIII - As senhas de acesso deverão ser individuais, sigilosas e intransferíveis. As unidades de TI da CNEN definirão as regras de formação de senhas e de suas reutilizações e período de validade;

IX - O acesso às redes institucionais e à Internet dar-se-á por meio disponibilizado e configurado pelas unidades de TI da CNEN. Para acesso a recursos computacionais

realizados a partir das redes institucionais serão gerados registros nos equipamentos de acesso e segurança de rede, para eventual ação de auditoria. O acesso aos registros somente será realizado mediante autorização de cada unidade de TI;

X - É vedado o acesso às páginas ou serviços que possuam características diversas das atividades institucionais da CNEN, salvo as previamente autorizadas pelas unidades de TI.

XI - O serviço de correio eletrônico destina-se a agilizar a comunicação interna e externa, e deverá ser utilizado para o envio e o recebimento de mensagens eletrônicas com conteúdo relacionado às funções desempenhadas pelo usuário. É vedado o uso dos recursos do correio eletrônico para a veiculação de mensagens desvinculadas do exercício das funções institucionais;

XII - As áreas de tecnologia da informação das unidades da CNEN poderão prover acesso sem fio às suas redes locais. Somente equipamentos autorizados e previamente homologados pelas áreas de tecnologia da informação das unidades poderão atuar como pontos de acesso sem fio às redes locais;

XIII - Os pontos de acesso sem fio às redes locais da CNEN deverão prover mecanismos de criptografia e autenticação das conexões de usuários;

XIV - Será de responsabilidade do usuário solicitante a verificação de conformidade dos equipamentos particulares com as características de conexão sem fio utilizadas nas unidades da CNEN;

XV - A configuração do dispositivo que irá realizar o acesso remoto será de responsabilidade do usuário solicitante, sob orientação da CGTI ou das áreas de tecnologia da informação das unidades da CNEN;

XVI - As salas onde se encontram instalados equipamentos de infraestrutura de rede de computadores deverão, sempre que possível, ter o seu interior monitorado por câmeras do sistema de CFTV e outros dispositivos de sensoriamento pertencentes ao sistema de segurança das unidades da CNEN.

4.5.1.3 Segurança de Mídias, Acesso Remoto e Auditoria

As unidades da CNEN devem seguir as seguintes orientações:

I - As mídias contendo dados e informações sigilosas devem ser protegidas durante o transporte externo às instalações das unidades da CNEN. A proteção deverá ser realizada mediante o uso de criptografia;

II - O acesso aos recursos de tecnologia da informação poderá ser realizado a partir de ambiente externo às dependências da CNEN. Os recursos de tecnologia da informação que serão homologados para acesso remoto, bem como os perfis de usuários autorizados, serão definidos pelas unidades de TI da CNEN. Para o acesso, a autenticação do usuário deverá utilizar identificação e senha, preferencialmente acompanhadas de mecanismos de segurança adequados ao nível de proteção requerido;

III - O acesso remoto deverá ser solicitado às unidades de TI da CNEN, sendo tal acesso de uso exclusivo do usuário solicitante;

IV - O uso dos recursos de tecnologia da informação, sempre que possível, deverá gerar informações que possam ser coletadas e transformadas em trilhas de auditoria, de

forma que pela análise ou visualização destas, sejam respondidas questões de autoria e temporalidade;

V - Para fins de verificação do cumprimento das normas de segurança ou por determinação de autoridade competente, a CGTI e as áreas de tecnologia da informação das unidades da CNEN poderão realizar auditoria nas trilhas de uso dos recursos de tecnologia da informação sob sua responsabilidade. As informações provenientes dessas auditorias receberão tratamento sigiloso;

VI - As auditorias e verificações de conteúdo das áreas de armazenamento das redes e estações de trabalho locais deverão ser realizadas sob prévia autorização da autoridade competente e de modo a não comprometer o sigilo de dados e informações assim classificados em razão do serviço. Tais atividades devem ser realizadas por servidores especificamente designados e de maneira a permitir a rastreabilidade das ações da auditoria. As informações provenientes dessas auditorias receberão tratamento sigiloso.

4.5.1.4 Segurança das Comunicações

As unidades da CNEN devem seguir as seguintes orientações:

I - É vedado o uso de aparelhos de telefones sem fio, exceto aqueles originais das próprias centrais telefônicas, nas unidades da CNEN;

II - As instalações físicas destinadas à sala da central telefônica deverão ser dedicadas exclusivamente a este uso. Na impossibilidade, a central telefônica deve ser instalada em local que permita restringir o acesso, inclusive ser fechado com chave ou sistema similar. Preferencialmente, a instalação da central telefônica deve ser em racks com chave;

III - Não é autorizado acesso remoto à central telefônica, inclusive por empregados de empresa de manutenção, sem monitoramento da ação pelas áreas competentes da CNEN;

IV - Os computadores utilizados por telefonistas devem possuir acesso somente ao sistema de telefonia, sendo bloqueados os demais sistemas e serviços;

V - A sala de telefonistas e a sala da central telefônica são áreas restritas e devem ter acesso controlado, com a devida sinalização. As instalações físicas destinadas ao serviço de telefonistas e à central telefônica devem ser monitoradas por câmeras do sistema de CFTV ou possuírem sensores de presença ligados a alarmes;

VI - Os quadros de telefonia devem ser protegidos por sistemas de fechadura com chave ou similar, sem exibir a identificação dos ramais;

VII - As empresas e/ou as pessoas contratadas para a função de telefonista e serviço de manutenção devem ser capacitadas em aspectos de segurança da informação e assinar um termo de compromisso de confidencialidade.

4.5.1.5 Prescrições Diversas

As unidades da CNEN devem seguir as seguintes orientações:

I - Os equipamentos que forem destinados à doação, considerados inservíveis ou que tenham que sofrer manutenções corretivas em ambientes fora da CNEN, deverão ter

seus dados previamente eliminados de forma segura pelas áreas de tecnologia da informação das unidades;

II - As mídias inservíveis contendo dados e informações sigilosos ou sensíveis que por qualquer motivo devam ser destruídas, serão eliminadas de forma segura. As áreas de tecnologia da informação das unidades da CNEN deverão identificar os itens que requeiram descarte seguro. O descarte de itens desta natureza deverá ser registrado em controle com descrição de conteúdo, para permitir a realização de auditorias futuras;

III - O acesso aos recursos de tecnologia da informação por visitante, sempre que possível, deve exigir o cadastramento do usuário na área de tecnologia da informação;

IV - O ingresso e o uso de equipamentos de informática e periféricos particulares em unidades da CNEN devem ser controlados, de forma a restringir o acesso a informações institucionais.

4.5.2 – Segurança da Informação nos Recursos Humanos

A segurança da informação nos recursos humanos refere-se ao conjunto de medidas voltadas a estabelecer comportamentos adequados dos integrantes da CNEN que proporcionem a proteção da informação.

4.5.2.1 Segurança no Desligamento

As unidades da CNEN devem seguir as seguintes orientações:

I - O afastamento de função que trata de assuntos sigilosos deve ser realizado gradativa e paulatinamente, de forma a ocorrer uma desmobilização controlada, caso seja necessário;

II - Os membros e servidores que tenham acesso, por força de sua função, a sistemas ou serviços que tratem de assuntos sigilosos, devem ser excluídos do acesso por ocasião de seu desligamento da função;

III - Para efeito do item anterior, as chefias imediatas e os setores de recursos humanos devem informar aos gerentes de cada sistema ou serviço sobre o afastamento das funções por membros e servidores. Os gerentes de cada sistema ou serviço que trate de assuntos sigilosos devem avaliar periodicamente os seus respectivos sistemas ou serviços para identificar acessos indevidos.

4.5.2.2 Credencial de Segurança

A credencial de segurança é um documento que habilita o portador ao acesso a dados e informações classificados em qualquer grau de sigilo, em conformidade com a legislação específica em vigor.

A credencial será concedida pelas autoridades competentes, conforme definido em ato normativo específico.

As unidades da CNEN devem seguir as seguintes orientações:

I - Todos os integrantes da CNEN que possuam credencial de segurança serão submetidos periodicamente a treinamento específico para o trato com dados e informações classificados em qualquer grau de sigilo;

II - Os integrantes da CNEN que desempenham função com acesso a dados e informações classificados em qualquer grau de sigilo devem ser submetidos a avaliação periódica para renovação da credencial de segurança;

III - O acesso à informação classificada em qualquer grau de sigilo a pessoa não credenciada ou não autorizada por legislação poderá, excepcionalmente, ser permitido mediante assinatura de Termo de Compromisso de Manutenção de Sigilo - TCMS, pelo qual a pessoa se obrigará a manter o sigilo da informação, sob pena de responsabilidade penal, civil e administrativa, na forma da lei.

4.5.2.3 Termo de Compromisso de Confidencialidade

O Termo de Compromisso de Confidencialidade é um documento que representa o compromisso formal do signatário em manter confidencialidade a respeito de dados e informações a que tenha acesso por força de suas funções, conforme os casos previstos no presente PLSI.

As unidades da CNEN devem seguir as seguintes orientações:

I - Cada unidade deverá estabelecer um modelo próprio de Termo de Compromisso de Confidencialidade;

II - O Termo de Compromisso de Confidencialidade deve ser arquivado em local seguro e estar disponível para consulta e auditoria;

4.5.3 Segurança da Informação na Documentação

A Segurança da Informação na Documentação é um conjunto de medidas que visa à proteção da informação contida na documentação que é arquivada ou que tramita da CNEN. Inclui, ainda, medidas de segurança no ato de produzir, classificar, tramitar, arquivar e destruir a documentação.

É relevante que se proceda à gestão documental para documentos ostensivos e sigilosos de acordo com a legislação em vigor, implementando-se protocolos de documentos adequados a essa classificação.

A seguir são elencadas as medidas de segurança da informação na documentação.

4.5.3.1 Classificação e Segurança

As unidades da CNEN devem seguir as seguintes orientações:

I - A documentação produzida na CNEN deve ser classificada quando o seu conteúdo exigir grau de sigilo;

II - A classificação dos documentos ou informações sigilosos da CNEN e os seus respectivos trâmites e tratamentos observarão a legislação vigente, sem o prejuízo das demais hipóteses legais de sigilo e de segredo de justiça;

III - O acesso aos documentos ou informações sigilosos é restrito e condicionado à credencial de segurança e à necessidade (funcional) de conhecer;

IV - O princípio da compartimentação deve ser adotado no desenvolvimento das atividades de segurança da informação na documentação;

4.5.3.2 Gestão de Documentos Sigilosos

As unidades da CNEN devem seguir as seguintes orientações:

I - Os responsáveis pela guarda ou custódia de documentos sigilosos os transmitirão a seus substitutos, por meio de inventário devidamente conferido, quando da passagem ou transferência de responsabilidade;

II - A classificação de um grupo de documentos que formem um conjunto deve ser a mesma atribuída ao documento classificado com o mais alto grau de sigilo;

III - Os mapas, planos-relevo, cartas e fotocartas baseados em fotografias aéreas ou em seus negativos serão classificados em razão dos detalhes que revelem e não da classificação atribuída às fotografias ou negativos que lhes deram origem ou das diretrizes baixadas para obtê-las.

4.5.3.3 Documentos Controlados

As unidades da CNEN devem seguir as seguintes orientações:

I - Os Documentos Controlados - DCs são documentos sigilosos cujo conteúdo requer medidas extras de segurança, que incluem guarda e custódia;

II - A segurança do DC requer medidas adicionais de controle, tais como: identificação dos destinatários em protocolo e recibo próprios, quando da difusão; lavratura de termo de custódia e registro em protocolo específico; lavratura anual de termo de inventário, pelo órgão ou entidade expedidor e pelo órgão ou entidade receptor; e lavratura de termo de transferência de custódia ou guarda. O termo de inventário deverá conter, no mínimo, os seguintes elementos: numeração sequencial e data; órgãos produtor e custodiante do DC; rol de documentos controlados; e local e assinatura. O termo de transferência, por sua vez, deverá conter, no mínimo, os seguintes elementos: numeração sequencial e data; agentes públicos substituto e substituído; identificação dos documentos ou termos de inventário a serem transferidos; e local e assinatura.

4.5.3.4 Segurança na Autuação e Processamento Administrativo

As unidades da CNEN devem seguir as seguintes orientações:

I - Os documentos sigilosos encaminhados para autuação, além das diretrizes estabelecidas para os documentos ostensivos, devem estar classificados, conforme a legislação em vigor e os atos normativos regulamentares da CNEN, em sistema oficial de controle de documentação da CNEN;

II - Quando a autuação for realizada pela CNEN, não devem constar da capa do processo sigiloso os dados que possam acarretar qualquer risco à segurança das atividades ou comprometer o respectivo sigilo;

III - Quando da realização de juntada de documentos sigilosos deve ser considerada a mesma classificação atribuída ao documento classificado com o mais alto grau de sigilo;

IV - As páginas do processo sigiloso serão numeradas seguidamente, devendo cada uma conter, também, a indicação do total de páginas que compõem o documento.

4.5.3.5 Segurança na Expedição, Tramitação e Reprodução

As unidades da CNEN devem seguir as seguintes orientações:

I - Toda a documentação sigilosa deve tramitar em grau de urgência;

II - Os mesmos critérios de segurança aplicados no encaminhamento à CNEN de documentação classificada como sigilosa devem ser observados em seu trâmite interno e em sua devolução ao órgão de origem;

III - A documentação classificada como sigilosa, em sua tramitação interna, na expedição, condução, entrega e reprodução, obedecerá os procedimentos estabelecidos pelo CGSI;

IV - Os documentos sigilosos serão mantidos ou guardados em condições especiais de segurança, conforme o grau de sigilo.

4.5.3.6 Segurança na Publicação, Arquivamento e Acesso

As unidades da CNEN devem seguir as seguintes orientações:

I - A publicação dos atos sigilosos, quando necessário, limitar-se-á aos seus respectivos números, datas de expedição e ementas, redigidas de modo a não comprometer o sigilo;

II - Poderão ser elaborados extratos de documentos sigilosos, para sua divulgação ou execução, mediante autorização da autoridade classificadora ou autoridade superior competente para dispor sobre o assunto;

III - Os documentos sigilosos que forem objeto de desclassificação serão encaminhados ao Arquivo para fins de organização, preservação e acesso;

IV - Os documentos, enquanto classificados como sigilosos, não podem ser desfigurados ou destruídos, sob pena de responsabilidade penal, civil e administrativa, nos termos da legislação em vigor;

V - Quando da reconstituição de autos originais de processos extraviados ou destruídos, a mesma obedecerá a normatização legalmente estabelecida, preservando-se para a documentação sigilosa reconstituída o mesmo grau de sigilo do original; assim como, os procedimentos que vierem a instruir tais processos passarão a ter grau idêntico de sigilo;

VI - O acesso à documentação sigilosa é condicionado à emissão de credencial de segurança pela autoridade competente no correspondente grau de sigilo e à necessidade (funcional) de conhecer. Os demais casos serão solicitados e concedidos na forma da legislação vigente.

4.5.3.7 Segurança em contratos envolvendo sigilo

As unidades da CNEN devem seguir as seguintes orientações:

I - A celebração de contrato cujo objeto implique realização de ações sigilosas, ou a guarda, ou tratamento de dados ou informações (incluídos mapas, desenhos, cartas, modelos, plantas, fotografias, documentos, equipamentos, software, hardware ou outro tipo de material), de natureza sigilosa, deve condicionar o conhecimento do dado protegido à assinatura de Termo de Compromisso de Confidencialidade pelos interessados na contratação (pessoa jurídica e pessoa física);

II - Os contratos que envolvem sigilo devem apresentar cláusulas que estabeleçam a obrigação do contratado de adotar medidas de segurança adequadas à manutenção do sigilo e ao tratamento dos dados e informações sigilosos; de se submeter ao monitoramento e inspeção por parte da CNEN com o objetivo de verificar o nível de segurança em que estão sendo tratados os dados e informações sigilosos.

III - Em regra, é vedado o acesso da contratada a dados e informações sigilosos referentes à atividade institucional da CNEN. Situações excepcionais devem ser submetidas ao CESI. Em caso da exigência de realização de ensaios ou exercícios pilotos para operacionalização de sistemas ou serviços, devem ser utilizados dados ostensivos;

IV - A ação de alimentação de dados e informações sigilosos em bancos de dados deve, em regra, ser feita por servidor com credencial de segurança compatível com o grau de sigilo. Situações excepcionais devem ser submetidas ao CESI.

4.5.3.8 Prescrições Diversas

As unidades da CNEN devem seguir as seguintes orientações:

I - Os dados e informações sigilosos, constantes de documento produzido em meio eletrônico, serão assinados e criptografados mediante o uso de certificados digitais emitidos pela Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil;

II - Os equipamentos e sistemas utilizados para a produção de documentos no mais alto grau de sigilo só podem estar ligados a redes de computadores seguras, e que sejam logicamente isoladas de qualquer outra;

III - Os equipamentos e sistemas utilizados para a produção de documentos sigilosos só podem integrar redes de computadores quando a respectiva conexão possua controles de segurança adequados, visando à garantia da confidencialidade, da integridade e da disponibilidade das informações;

IV - Os documentos sigilosos submetidos à digitalização serão mantidos ou guardados em condições especiais de segurança, somente podendo ser manuseados por portadores de credencial compatível com o grau de sigilo.

4.5.4 – Segurança da Informação nas Áreas e Instalações

A Segurança da Informação nas Áreas e Instalações compreende um conjunto de medidas voltadas a proteger informações sensíveis armazenadas ou em trâmite no espaço físico sob a responsabilidade da Instituição ou no espaço físico onde estejam sendo realizadas atividades de interesse institucional.

As unidades da CNEN devem seguir as seguintes orientações:

I - As salas em que são tratados assuntos sigilosos ou que, pela sua sensibilidade, mereçam maior grau de segurança devem possuir, sempre que possível, isolamento

acústico. Esses locais devem, de acordo com a necessidade, ser submetidos à varredura eletrônica e à inspeção de ambiente;

II - As mesas de trabalho em que são tratados assuntos sigilosos devem ser protegidas da observação externa pelas janelas;

III - Os locais onde se processam dados e informações sigilosas, sempre que possível, devem ser separados fisicamente de locais onde trabalham terceirizados;

IV - O acesso aos itens de configurações do sistema de CFTV e às imagens gravadas deve ser controlado pelo responsável pela Unidade de Segurança ou servidor autorizado.

4.6 Gestão de Riscos

A Gestão de Riscos inclui a identificação, análise, avaliação e tratamento do risco, constituindo-se em atividade fundamental para proteção da CNEN, por ser um processo dinâmico e proativo de defesa da instituição.

O Planejamento de Contingência é a previsão de técnicas e procedimentos alternativos adotados para efetivar processos que venham a ser interrompidos ou a perder sua eficácia. Visa a minimizar o impacto e a restabelecer a continuidade desses processos, combinando ações preventivas e de recuperação. É fundamental para permitir o cumprimento das funções da CNEN, mesmo diante de um incidente que atente contra a realização de processos.

O Controle de Danos é a determinação de uma série de medidas que visem a avaliar a profundidade de um dano, o comprometimento dos ativos e as demais consequências para a CNEN decorrentes de um incidente, inclusive no que se refere à imagem institucional. Constitui-se em eficaz ferramenta de suporte para tomada de decisões em situações de crise, possuindo concepção complementar ao Planejamento de Contingência.

A gestão de continuidade negócios é uma abordagem integrada que envolve a mobilização de toda a instituição para gerenciar crises e recuperar as operações após a ocorrência de qualquer evento que cause uma ruptura operacional.

A análise de Gestão de Riscos relacionada com a segurança institucional, incluindo o planejamento de contingência, controle de danos e gestão de continuidade de negócios, devem ser orientados pelas diretrizes da Política de Gestão de Riscos da CNEN.

CAPÍTULO V
DISPOSIÇÕES FINAIS

O presente Plano de Segurança Institucional tem aplicação imediata e deverá ser periodicamente revisado a critério do CGSI. A execução do plano receberá tratamento prioritário no âmbito da Instituição, inclusive no que diz respeito à expedição dos atos

normativos que se revelem necessários ao cumprimento de todas as diretrizes e procedimentos nele previstos.

Em caso de divergências entre os requisitos de âmbito geral deste Plano e os de normas específicas, baixadas pela CNEN, aplicáveis a casos particulares de procedimentos, prevalecerão os requisitos das normas específicas.