Portaria CNEN-PR nº 004, de 09 de Janeiro de 2015

O PRESIDENTE DA COMISSÃO NACIONAL DE ENERGIA NUCLEAR *- CNEN, no uso das atribuições que lhe confere o inciso I, do artigo 14, do anexo I ao Decreto nº 5.667, publicado no Diário Oficial da União de 11 de janeiro de 2006 e, tendo em vista o disposto no Art. 5º, inciso VII, da Instrução Normativa GSI/PR Nº 1, de 13 de junho de 2008,*

resolve:

Art. 1º *Aprovar a Política de Segurança da Informação e Comunicações da Comissão Nacional de Energia Nuclear (PoSIC/CNEN), nos termos do Anexo a esta Portaria.*

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

Angelo Fernando Padilha
Presidente

Política de Segurança da Informação e Comunicações

PoSIC/CNEN

CNEN
Comissão Nacional
de Energia Nuclear

"Se você acredita que a tecnologia pode resolver seus problemas de segurança, então você não conhece os problemas e nem a tecnologia."

Bruce Schneier

Política de Segurança da Informação e Comunicações
PoSIC/CNEN

Sumário

1. Apresentação

A Política de Segurança da Informação e Comunicações (PoSIC/CNEN) é resultado da convergência de variadas iniciativas no âmbito governamental, dentro de uma perspectiva multidisciplinar que engloba questões de tecnologia da informação e comunicações (TIC), de administração de processos, de comportamento humano, entre outras.

Tais iniciativas tiveram como ponto de partida a necessidade de atendimento do Acórdão TCU 1.603/2008 – Plenário, o qual recomendou ao Gabinete de Segurança Institucional da Presidência da República - GSI/PR a orientar aos órgãos/entidades da Administração Pública Federal sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante orientação normativa, ações com o objetivo de estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso.

Visando atender essas recomendações o Gabinete de Segurança Institucional da Presidência da República publicou a Instrução Normativa GSI/PR Nº 01/2008 e normas complementares disciplinando a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, as quais constituem a estrutura normativa fundamental para a elaboração e implementação da PoSIC/CNEN.

Acredita-se que a publicação e implementação desta PoSIC/CNEN se constitui em um passo significativo para a melhoria da gestão da segurança da informação e comunicações no âmbito da CNEN e um instrumento capaz de apoiar de forma efetiva o alcance dos objetivos institucionais.

Esta PoSIC/CNEN tem a finalidade de estabelecer princípios, diretrizes, competências e responsabilidades relativas à Segurança da Informação e Comunicações (SIC) no âmbito da CNEN e, para tanto, foi estruturada em conformidade com a Norma Complementar no 03, de 30 de junho de 2009, publicada pelo Departamento de Segurança da Informação e Comunicações (DSIC/GSIPR).

2. Escopo

Esta Política de Segurança da Informação e Comunicações (PoSIC/CNEN) é um documento que estabelece e formaliza os compromissos institucionais para proteção das informações de propriedade e sob custódia da CNEN.

3. Objetivo

A PoSIC/CNEN tem por objetivo estabelecer princípios, diretrizes, competências e responsabilidades relativas à Segurança da Informação e Comunicações (SIC) no âmbito da CNEN, visando garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que suportam os objetivos institucionais.

4. Abrangência

4.1. Esta PoSIC/CNEN abrange todas as Unidades da CNEN, devendo ser adotada pelos servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e por outros que tenham acesso às instalações físicas e/ou aos ambientes computacionais da CNEN.

4.2. Os contratos, convênios, acordos e outros instrumentos congêneres, celebrados pela CNEN com órgãos e entidades públicas ou privadas, devem atender a esta PoSIC/CNEN e documentos complementares.

5. Conceitos e Definições

Para os fins desta PoSIC/CNEN, considera-se:

5.1. Ativos de Informação: elementos considerados essenciais para o cumprimento da missão institucional, os quais englobam os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.

5.2. Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

5.3. Avaliação de Conformidade em Segurança da Informação e Comunicações: exame sistemático do grau de atendimento dos requisitos relativos à SIC com as legislações específicas.

5.4. Comitê de Segurança da Informação e Comunicações (CSIC/CNEN): grupo de pessoas com a responsabilidade de assessorar a implementação das ações de SIC no âmbito da CNEN.

5.5. Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

5.6. Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

5.7. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais da CNEN (ETIR/CNEN): grupo de pessoas com a responsabilidade de receber, registrar, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

5.8. Gestão de Continuidade: processo abrangente de gestão que identifica ameaças potenciais para a CNEN e os possíveis impactos no funcionamento de seus serviços e atividades, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das

partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado.

5.9. Gestão de Risco: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, permitindo equilibrá-los com os custos operacionais e financeiros envolvidos.

5.10. Gestor de Segurança da Informação e Comunicações: é responsável pelas ações de SIC no âmbito da CNEN.

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

5.12. Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

5.13. Política de Segurança da Informação e Comunicações (PoSIC/CNEN): documento aprovado pela Alta Administração, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da SIC.

5.14. Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações.

5.15. Recursos Computacionais: equipamentos (computadores e seus periféricos, impressoras, scanners, projetores, etc), instalações físicas, aplicativos (*softwares*), bancos de dados e serviços relacionados ao processamento, armazenamento e à transmissão digital de dados (correio eletrônico, acesso à Internet, Intranet, backup, etc), entre outros.

5.16. Redes de Computadores: sistema de comunicação de dados constituído através da interligação de computadores e outros dispositivos, com a finalidade de trocar informações e partilhar recursos.

5.17. Sistemas de Informação: conjunto de elementos que, relacionados entre si, armazenam, tratam e fornecem informações, com o objetivo de apoiar as funções ou processos de uma organização, funcionando como suporte às ações e decisões humanas.

5.18. Tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

5.19. Unidades Técnico-Científica – UTC: são as Unidades da CNEN que recebem a designação de Institutos, Centros ou Laboratório.

5.20. Usuário: servidores, fornecedores, prestadores de serviço, colaboradores, bolsistas, estagiários, visitantes e alunos que obtiveram autorização do responsável pela área interessada para acesso aos ativos de informação da CNEN.

6. Referências Legais e Normativas

Esta PoSIC/CNEN foi elaborada considerando os seguintes marcos legais e normativos.

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

II. Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

III. Norma Complementar nº 01/IN01/DSIC/GSI/PR, de 13 de outubro de 2008, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta;

IV. Norma Complementar nº 02/IN01/DSIC/GSI/PR, de 13 de outubro de 2008, que define a metodologia de Gestão de Segurança da Informação e Comunicações utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta;

V. Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações (PoSIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta;

VI. Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta;

VII. Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 14 de agosto de 2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) nos órgãos e entidades da Administração Pública Federal, direta e indireta;

VIII. Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 11 de novembro de 2009, que estabelece diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta;

IX. Norma Complementar nº 07/IN01/DSIC/GSI/PR, de 15 de julho de 2014, que estabelece diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta;

X. Norma Complementar nº 08/IN01/DSIC/GSI/PR, de 19 de agosto de 2010, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta;

XI. Norma Complementar nº 11/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta; e

XII. Norma Complementar nº 20/IN01/DSIC/GSIPR, de 15 de julho de 2014, que estabelece diretrizes de Segurança da Informação e Comunicações para instituição do processo de tratamento da informação, envolvendo todas as etapas do ciclo de vida da informação, no âmbito da Administração Pública Federal, direta e indireta.

7. Princípios

As ações relacionadas com a Segurança da Informação e Comunicações no âmbito da CNEN são norteadas pelos seguintes princípios:

7.1. **Conhecimento**: todos devem conhecer e estar comprometidos com as normas de Segurança da Informação e Comunicações da CNEN.

7.2. **Ética**: os direitos individuais devem ser preservados, com respeito às leis, aos costumes e à dignidade da pessoa humana, sem comprometimento da Segurança da Informação e Comunicações da CNEN.

7.3. **Clareza**: as regras de segurança da informação e comunicações devem ser precisas, concisas e de fácil entendimento.

7.4. **Celeridade**: as ações de segurança da informação e comunicações devem oferecer respostas rápidas aos incidentes e falhas.

7.5. **Publicidade**: as normas de segurança da informação devem ser divulgadas e de fácil acesso.

7.6. **Propriedade**: os ativos de informação da CNEN não podem ser interpretados como de propriedade individual.

8. Diretrizes Gerais

São diretrizes gerais da PoSIC/CNEN:

I. estabelecer medidas e procedimentos de tratamento da informação e gestão dos seus ativos, com o objetivo de viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

II. manter equipe de tratamento e resposta a incidentes em redes computacionais, com objetivo de registrar, analisar e tratar incidentes de SIC por meio da coleta de evidências, investigação de ataques, provimento de assistência local e remota e intermediação da comunicação entre as partes envolvidas;

III. elaborar e implementar plano de gestão de riscos, com o objetivo de reduzir as vulnerabilidades, evitar ameaças, minimizar a exposição aos riscos e atenuar os impactos associados aos ativos de informação da CNEN;

IV. elaborar e implementar plano de gestão de continuidade, com o objetivo de identificar ameaças e possíveis impactos na continuidade dos processos, e responder e salvaguardar os interesses, a reputação, a marca e as atividades de valor agregado da CNEN;

V. elaborar e implementar mecanismos de auditoria e conformidade, com o objetivo de garantir a exatidão dos registros de acesso aos ativos de informação e avaliar sua conformidade com as normas de SIC em vigor;

VI. implementar controle de acesso lógico aos sistemas de informação e às redes de computadores e controle de acesso físico às instalações internas, com o objetivo de preservar os ativos de informação da CNEN; e

VII. definir regras claras e precisas para uso dos recursos computacionais da CNEN, com o objetivo de evitar a utilização para fins particulares, com abuso de direito ou violação à imagem institucional.

9. Penalidades

9.1. Ações que violem as diretrizes desta PoSIC/CNEN ou quaisquer orientações internas e procedimentos decorrentes da mesma serão passíveis de sansões civis, penais e administrativas, conforme as regulamentações internas e a legislação em vigor, assegurados aos envolvidos o contraditório e a ampla defesa.

9.2. A resolução de casos de violação/transgressões omissos nas legislações correlatas será resolvida pelo Comitê de Segurança da Informação e Comunicações da CNEN.

10. Competências e Responsabilidades

10.1. A implementação, o acompanhamento e a avaliação de conformidade desta PoSIC/CNEN devem ser apoiados por uma estrutura de Gestão da Segurança da Informação que contemple no mínimo:

I. Gestor de Segurança da Informação e Comunicações;

II. Comitê de Segurança da Informação e Comunicações (CSIC/CNEN); e

III. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR/CNEN).

10.2. Ao Gestor de Segurança da Informação e Comunicações da CNEN, compete:

I. Promover a cultura de SIC;

II. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III. Propor recursos necessários às ações de SIC;

IV. Coordenar o Comitê de Segurança da Informação e Comunicações (CSIC/CNEN) e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR/CNEN);

V. Promover e coordenar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VI. Manter contato direto com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI/PR) para o trato de assuntos relativos à SIC; e

VII. Propor elaboração e alteração da PoSIC/CNEN e das orientações internas e procedimentos relativos à SIC no âmbito da CNEN;

10.3. Ao Comitê de Segurança da Informação e Comunicações (CSIC/CNEN), compete:

I. Assessorar na implementação das ações de SIC;

II. Constituir grupos de trabalho, em caráter permanente ou temporário, para tratar de temas específicos relacionados à SIC;

III. Propor alterações na PoSIC/CNEN;

IV. Propor Orientações Internas (OIs); e

V. Apoiar a implementação de programas destinados a conscientização e à capacitação de recursos humanos em SIC.

10.4. À Equipe de Tratamento e Resposta a Incidentes de Redes Computacionais (ETIR/CNEN), compete:

I. Elaborar estratégias, metodologia, orientações e procedimentos internos para o tratamento e resposta aos incidentes de segurança da informação;

II. Adotar procedimentos para tratamento e resposta aos incidentes, garantindo a preservação das evidências;

III. Analisar os incidentes e suas causas, indicando necessidades de controles aperfeiçoados ou adicionais para evitar a sua propagação ou recorrência;

IV. Monitorar os incidentes em sistemas e redes computacionais da CNEN;

V. Adotar procedimentos de *feedback* para assegurar que os usuários que comuniquem incidentes sejam informados dos procedimentos adotados; e

VI. Apoiar, incentivar e contribuir para a realização de eventos de informação ao usuário nos temas relacionados à SIC.

10.5. Aos servidores, terceirizados e demais pessoas alcançadas por esta PoSIC/CNEN, compete:

I. Cumprir fielmente as políticas, as orientações internas e os procedimentos de SIC da CNEN;

II. Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à SIC;

III. Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pela CNEN;

IV. Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela CNEN; e

V. Comunicar imediatamente ao Comitê de Segurança da Informação e Comunicações (CSIC/CNEN) qualquer descumprimento ou violação desta PoSIC/CNEN e/ou de documentos complementares.

11. Atualização

11.1. Esta PoSIC/CNEN será revisada e/ou atualizada de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de três anos.

12. Disposições Gerais

12.1. As Unidades Técnico-Científicas e a Sede da CNEN possuem autonomia para a Gestão da Segurança da Informação e Comunicações, desde que seja mantida a aderência à esta PoSIC/CNEN e demais orientações internas da CNEN.

12.2. As estruturas de Gestão da Segurança da Informação e Comunicações devem ser formalmente instituídas e estar presentes no Regimento Interno da CNEN.

12.3. Esta PoSIC/CNEN deve ser complementada por orientações internas, procedimentos e mecanismos que garantam o seu cumprimento e avaliação.

12.4. A implementação desta PoSIC/CNEN deve observar as melhores práticas de SIC recomendadas por órgãos e entidades públicas e privadas.

12.5. Os investimentos para implementação desta PoSIC/CNEN devem estar previstos no Planejamento Orçamentário Institucional.

12.6. A capacitação dos recursos humanos envolvidos nos assuntos de SIC e a conscientização interna devem estar previstas no Plano de Capacitação Institucional.

12.7. O CSIC/CNEN poderá receber e avaliar propostas de alterações na PoSIC/CNEN, devidamente justificadas, apresentadas por qualquer pessoa que esteja submetida à aplicação desta PoSIC/CNEN.