Laboratório Nacional de Computação Científica
UNIDADE DE PESQUISA DO MCTI

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES

PÁTRIA AMADA BRASIL GOVERNO FEDERAL

Sistema de Gestão de Segurança da Informação

Política de Segurança da Informação do LNCC

Controle Interno	02-PSI
Classificação	Nível de Acesso: (**X**) Público () Restrito ( ) Sigiloso Tipo de Acesso: ( ) Interno (**X**) Externo
Grupo Responsável	CSI – Comitê de Segurança da Informação
Autor(es)	Luís Rodrigo de O. Gonçalves
Versão	1.0
Data do Documento	18 de março de 2022
Número de Páginas	19
Controles da ISO	5.2
Tipo do Documento	Política de Segurança

Diretor
Fábio Borges de Oliveira

Coordenação de Gestão e Administração – COGEA
Sérgio Ferreira de Figueiredo

Coordenação de Tecnologia da Informação e Comunicação – COTIC
Wagner Vieira Léo

Gestão de Segurança da Informação - GSI
Luís Rodrigo de Oliveira Gonçalves

Histórico de Versões

Versão	Data	Descrição	Revisor(es)
2019	30/07/2019	Portaria nº 81/2019/SEI-LNCC de 30 de julho de 2019	Comitê de Segurança Luís Rodrigo de O. Goncalves
1.0	18/03/2022	Revisão do conteúdo da política; adequação do conteúdo a PNSI, a PSI do MCTI, a IN01/GSI/PR, a IN02/GSI/PR e a IN03/GSI/PR	Comitê de Segurança Luís Rodrigo de O. Goncalves

Sumário

CAPÍTULO I - DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política de Segurança da Informação (PSI), no âmbito do Laboratório Nacional de Computação Científica (LNCC), com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Art. 2º Na preparação desta política e demais instrumentos relacionados a segurança da informação deve levar em consideração a natureza e a finalidade do Laboratório Nacional de Computação Científica (LNCC), e devem estar alinhados ao seu planejamento estratégico.

Art. 3º Este documento é uma declaração formal do Laboratório Nacional de Computação Científica (LNCC) a respeito do seu compromisso com a proteção dos ativos de informação de sua propriedade e sua guarda.

Art. 4º Esta política representa o comprometimento do Laboratório Nacional de Computação Científica em satisfazer os requisitos aplicáveis relacionados à segurança da informação, como: a ABNT NBR ISO/IEC 27001, requisitos definidos em contratos, as leis, os decretos e demais normativas governamentais. A política inclui o compromisso com o processo da melhoria contínua do Sistema de Gestão da Segurança da Informação.

Art. 5º A metodologia de gestão da segurança da informação do LNCC seguirá as orientações previstas na legislação vigente, ela será baseia em processo de melhoria contínua, considerando o "PDCA" (*Plan-Do-Check-Act*), referenciado pela norma ABNT NBR ISO/IEC 27001.

Art. 6º Este documento é uma declaração formal do comprometo da alta administração, do Laboratório Nacional de Computação Científica (LNCC) com vistas a prover diretrizes estratégicas, responsabilidades, competências e apoio para implementar a gestão da segurança da informação em sua organização.

Art. 7º Cabe ao Laboratório Nacional de Computação Científica (LNCC) adotar os controles de segurança da informação estabelecidos pelo Gabinete de Segurança Institucional da Presidência da República.

Art. 8º A autoridade máxima do Laboratório Nacional de Computação Científica (LNCC) é responsável por garantir os recursos necessários para a execução da Política de Segurança da Informação e da Gestão da Segurança da Informação no âmbito da organização.

Art. 9º Cabe ao Gestor de Segurança da Informação promover, com apoio da alta administração, a ampla divulgação da política, das normas internas de segurança da informação e de suas atualizações para toda comunidade de servidores públicos, agentes públicos, usuários e demais colaboradores do Laboratório Nacional de Computação Científica (LNCC).

Art. 10º Para os fins do disposto nesta política, a segurança da informação abrange:

i. a segurança cibernética;
ii. a defesa cibernética;
iii. a segurança física;
iv. a proteção de dados organizacionais; e

v. as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Art. 11º Esta política define as diretrizes, competências e responsabilidades relativas ao uso e compartilhamento de dados, informações e documentos em conformidade com a legislação vigente, as normas técnicas pertinentes, os valores éticos e as melhores práticas de segurança da informação e comunicações.

Art. 12º Esta política foi elaborada pelo LNCC, com base: (i) nas normas técnicas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002, (ii) na legislação vigente, (iii) na realidade e (iv) requisitos de negócio da entidade.

> "A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos."

Art. 13º Integram também a esta política os documentos que a complementam, os quais destinam à proteção da informação e à disciplina de sua utilização.

Art. 14º O Glossário de Segurança da Informação, aprovado pelo Gabinete de Segurança Institucional da Presidência da República, deve ser utilizado, como referência, na elaboração de normativos internos afetos à segurança da informação e de trabalhos correlatos.

Seção I - Escopo

Art. 15º Este documento aplica-se a todos os ativos da informação do LNCC. Ele considera a abrangência da segurança da informação nos aspectos físico, lógico, comportamental, pessoas, processos e tecnologias preservando a confidencialidade, integridade, disponibilidade e autenticidade das informações do LNCC ou sob sua salvaguarda.

Art. 16º A política se aplica a todas as formas intelectuais e físicas de ativos de informação, sejam próprios, utilizados ou custodiados no LNCC. Estas formas incluem *hardware*, redes, *software* e dados, sejam armazenadas e processadas em computadores, transmitida através de redes, impressos ou escritos em papel, enviada por fax, armazenados em meios legíveis por máquina (por exemplo, CD-ROM, fitas, *tokens* USB) ou falada em conversas e por telefone ou postada na Internet por exemplo, em mídia social redes, *chats* ou *wikis*.

Seção II - Abrangência e Público-alvo

Art. 17º Esta Política de Segurança da Informação se aplica a todos os colaboradores do LNCC, quais sejam: funcionários servidores ou comissionados, estagiários, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações deste órgão.

Art. 18º Todos os colaboradores são responsáveis e devem estar comprometidos com a segurança da informação e comunicações do LNCC.

Art. 19º Esta Política também se aplica, no que couber, ao relacionamento do LNCC com outros órgãos e entidades públicos ou privados.

§ 1º Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo LNCC devem atender, no que couber, a esta política e demais normas relacionadas.

§ 2º Os contratos, convênios, acordos e instrumentos congêneres devem conter a previsão de termo específico de responsabilidade e sigilo, quando a natureza de seu objeto ou condições específicas assim o exigirem.

§ 3º Os contratos, convênios, acordos e instrumentos congêneres devem prever a obrigação de divulgação desta política e suas normas complementares aos empregados envolvidos em atividades do contrato, por meio da assinatura de termo de ciência, quando a natureza de seu objeto ou condições específicas assim o exigirem.

Art. 20º Os colaboradores do LNCC envolvidos no espoco definido anteriormente devem ser informados a certa desta política de segurança.

CAPÍTULO II - DOS PRINCÍPIOS

Art. 21º As ações de Segurança da Informação no Laboratório Nacional de Computação Científica (LNCC) devem ser norteadas pelos seguintes princípios:

I. Respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação;

II. Visão abrangente e sistêmica da segurança da informação;

III. Responsabilidade do LNCC na coordenação de esforços e no estabelecimento de políticas, estratégias e diretrizes relacionadas à segurança da informação;

IV. Educação como alicerce fundamental para o fomento da cultura em segurança da informação;

V. Orientação à gestão de riscos e à gestão da segurança da informação;

VI. Prevenção e tratamento de incidentes de segurança da informação;

VII. Articulação entre as ações de segurança cibernética, de defesa cibernética e de proteção de dados e ativos da informação;

VIII. Dever da entidade, dos agentes públicos e demais colaboradores de garantir o sigilo das informações imprescindíveis à segurança da sociedade e do Estado e a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas;

IX. *Need to know* (Necessidade de Conhecer) para o acesso à informação sigilosa, nos termos da legislação;

X. Consentimento do proprietário da informação sigilosa recebida de outros países, nos casos dos acordos internacionais;

XI. Cooperação entre os órgãos de investigação e os órgãos e as entidades públicos no

processo de credenciamento de pessoas para acesso às informações sigilosas;

XII. Integração e cooperação entre o Poder Público, o setor empresarial, a sociedade e as instituições acadêmicas;

XIII. Cooperação internacional, no campo da segurança da informação;

XIV. Deve haver um alinhamento entre a Política de Segurança da com a missão institucional e seu planejamento estratégico;

XV. A elaboração Política de Segurança da Informação (PSI) deve levar em consideração a diversidade das atividades do LNCC, respeitando a natureza e finalidade da instituição;

XVI. Toda informação produzida ou armazenada no LNCC é de sua propriedade e não de seu colaborador, exceto os casos em que a Instituição atua como custodiante dessa informação;

XVII. A Segurança da Informação deve obedecer aos princípios do acesso, da disponibilidade, da integridade, da confidencialidade, da autenticidade, da legalidade, da privacidade, da auditabilidade e do não repúdio.

Art. 22º Deve-se utilizar o Glossário de Segurança da Informação, aprovado pelo Gabinete de Segurança Institucional da Presidência da República, como referência na elaboração de normativos internos afetos à segurança da informação e de trabalhos correlatos.

CAPÍTULO III - DOS OBJETIVOS

Art. 23º São objetivos desta política:

I. Estabelecer e difundir as diretrizes de segurança da informação no âmbito do Laboratório Nacional de Computação Científica (LNCC);

II. Contribuir para a segurança do indivíduo, da sociedade e da instituição, por meio da orientação das ações de segurança da informação, observados os direitos e as garantias fundamentais;

III. Fortalecer a cultura da segurança da informação na sociedade;

IV. Orientar ações relacionadas a:

a) segurança dos dados custodiados pela instituição;

b) segurança da informação das infraestruturas críticas;

c) proteção das informações das pessoas físicas que possam ter sua segurança ou a segurança das suas atividades afetada, observada a legislação específica;

d) tratamento das informações com restrição de acesso;

e) uso adequado das informações e recursos de tecnologia da informação suportados pela instituição evitando impactos prejudiciais às atividades de negócio da instituição.

V. Definir e padronizar o uso, tratamento, controle e proteção das informações que possam causar impactos no seu desempenho financeiro, na sua participação no mercado, na sua

imagem, agregando valor à operação e eficiência na prestação de serviços ou no seu relacionamento com as partes interessadas.

CAPÍTULO IV - DAS REFERÊNCIAS NORMATIVAS

Art. 24º As ações de segurança da informação no âmbito desta política deverão observar os seguintes requisitos legais e normativos:

I. Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

II. Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e privados;

III. Lei nº 8.745, de 9 de dezembro de 1993, que dispõe sobre a contratação por tempo determinado para atender a necessidade temporária de excepcional interesse público, nos termos do inciso IX do art. 37 da Constituição Federal;

IV. Lei nº 9.962, de 22 de fevereiro de 2000, que disciplina o regime de emprego público do pessoal da administração federal direta, autárquica e fundacional;

V. Lei n° 9.983, de 14 de julho de 2000, que dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

VI. Lei nº 12.527, de 18 de novembro de 2011 que regula 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;

VII. Lei nº 13.709, de 14 de agosto de 2018, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

VIII. Decreto nº 4.073, de 3 de janeiro de 2002, que regulamenta a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobrea Política Nacional de Arquivos Públicos e Privados;

IX. Decreto nº 5.482, de 30 de junho de 2005, que dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da administração pública federal, por meio da Rede Mundial de Computadores (Internet);

X. Decreto nº 6.029, de 1º de fevereiro de 2007, que institui o Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências;

XI. Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;

XII. Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

XIII. Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional;

XIV. Decreto nº 10.222, de 5 de fevereiro de 2020 que aprova a Estratégia Nacional de Segurança Cibernética;

XV. Portaria Interministerial MCT/MPOG nº 140, de 16 de março de 2006, que disciplina a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores (Internet) e dá outras providências;

XVI. Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação;

XVII. As instruções normativas e normas complementares relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República;

XVIII. Instrução Normativa Conjunta MP/CGU Nº 1, de 10 de maio de 2016, dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal.

CAPÍTULO V - DAS COMPETÊNCIAS

Art. 25º As atribuições, referente gestão, coordenação e operação da segurança da informação, serão determinadas mediante portarias internas do LNCC e poderão complementar as competências descritas nesta política.

Seção I - Gestor de Segurança da Informação - GSI

Art. 26º O gestor de segurança da informação deve ser designado dentre os servidores públicos civis ocupantes de cargo efetivo e militares de carreira do órgão ou entidade, com formação ou capacitação técnica compatível às suas atribuições.

Art. 27º Compete ao gestor de segurança da informação:

I. Coordenar o Comitê de Segurança da Informação e a Equipe de Tratamento e Resposta a Incidentes Cibernéticos;

II. Coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

III. Assessorar a alta administração na implementação da Política de Segurança da Informação;

IV. Estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

V. Promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no

Laboratório Nacional de Computação Científica;

VI. Promover a cultura de segurança da informação;

VII. Realizar, incentivar e acompanhar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

VIII. Propor recursos necessários às ações de segurança da informação;

IX. Verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X. Acompanhar as investigações e as avaliações dos dados decorrentes de quebras de segurança;

XI. Acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

XII. Manter contato direto com o Departamento de Segurança da Informação (DSI) do Gabinete de Segurança Institucional (GSI) da Presidência da República (PR) em assuntos relativos à segurança da informação.

Seção II - Comitê de Segurança da Informação - CSI

Art. 28º O Comitê de Segurança da Informação (CSI), de natureza consultiva, vinculado à diretoria do LNCC, tem a finalidade de tratar sobre políticas, diretrizes, planejamento e demais ações relativas à Segurança da Informação no âmbito das unidades constantes da estrutura organizacional do LNCC.

Art. 29º O Comitê de Segurança da Informação possui as seguintes atribuições:

I. Assessorar a implementação das ações de segurança da informação;

II. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III. Participar da elaboração, assim como propor alterações da Política de Segurança da Informação, das diretrizes, das normas e procedimentos relativos à segurança da informação; em conformidade com as legislações existentes sobre o tema, bem como suas alterações, e submetê-la ao diretor da instituição para apreciação, pronunciamento e aprovação;

IV. Exercer outros atos de assessoramento e de proposição afetos à matéria de segurança da informação e comunicações.

Seção III - Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR

Art. 30º A Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) tem a finalidade de facilitar, coordenar e executar as atividades de tratamento e resposta a incidentes em redes computacionais no ambiente do LNCC.

Art. 31º A ETIR do LNCC tem como objetivos básicos:

I. monitorar as redes computacionais;

II. detectar e analisar ataques e intrusões;

III. tratar incidentes de segurança da informação;

IV. identificar vulnerabilidades e artefatos maliciosos;

V. recuperar sistemas de informação; e

VI. promover a cooperação com outras equipes, bem como participar de fóruns e redes nacionais e internacionais relativos à Segurança da Informação.

Art. 32º A equipe será composta, por servidores públicos civis ocupantes de cargo efetivo ou militares de carreira, com capacitação técnica compatível com as atividades dessa equipe.

Art. 33º A atuação da Equipe será regida por normativos, padrões e procedimentos técnicos exarados pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos do Governo (CTIR GOV), sem prejuízo das demais metodologias e padrões conhecidos.

Art. 34º As notificações enviadas pela Equipe ao Centro de Tratamento e Resposta à Incidentes Cibernéticos de Governo, bem como a troca de informações entre as Equipes existentes, devem seguir os formatos e os procedimentos que serão estabelecidos pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos do Governo.

Seção IV - Do Agente Responsável pela ETIR

Art. 35º Compete ao Agente Responsável pela ETIR do MCTIC:

I. Estabelecer os procedimentos operacionais, gerenciar as atividades e distribuir tarefas para a ETIR;

II. Assistir o CTIR GOV com informações necessárias à atualização e manutenção das bases de dados de incidentes do Governo Federal.

Seção V - Conselhos, Coordenações, Serviços, Seções, Setores e Áreas

Art. 36º As atribuições, referente a Segurança da informação, atribuídas aos Conselhos, Coordenações, Serviços, Seções, Setores e Áreas identificadas no Regimento Interno do Laboratório Nacional de Computação Científica, serão determinadas mediante portarias internas da instituição.

Seção VI - Dos Colaboradores

Art. 37º Compete aos colaboradores do LNCC:

I. cumprir fielmente as políticas, as normas, os procedimentos e as orientações de segurança da informação e comunicações do LNCC;

II. buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;

III. assinar Termo de Responsabilidade, formalizando a ciência e o aceite da PSI do LNCC, bem

como assumindo responsabilidade por seu cumprimento;

IV. proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pelo LNCC;

V. assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo LNCC;

VI. comunicar imediatamente ao Comitê de Segurança da Informação (CSI) qualquer descumprimento ou violação desta Política ou de seus documentos complementares;

VII. participar dos treinamentos de segurança da informação e das atividades de conscientização sobre o mesmo tema;

VIII. implementar uma política de mesa limpa e tela limpa;

IX. ao se afastar, ele deve utilizar os recursos disponíveis para realizar o bloqueio de sua estação de trabalho;

X. não fornecer, divulgar ou compartilhar sua credencial de acesso a terceiros;

XI. utilizar apenas os serviços, recursos e demais ativos aos quais foi autorizado o acesso;

XII. não utilizar os ativos do LNCC para finalidades diferentes daqueles relacionados aos objetivos do projeto, atividade ou função ao qual está vinculado.

CAPÍTULO VI - DAS DIRETRIZES GERAIS

Art. 38º A segurança da informação tem como principal diretriz a proteção da informação, garantindo a continuidade do negócio, minimizando seus riscos, maximizando o retorno sobre os investimentos e as oportunidades pertinentes.

Art. 39º As diretrizes de segurança da informação devem considerar, prioritariamente, objetivos estratégicos, processos, requisitos legais e a estrutura do LNCC.

Art. 40º As diretrizes de segurança da informação e comunicações descritas nesta política devem ser observadas por todos os usuários que executem atividades vinculadas ao LNCC durante todas as etapas do tratamento da informação, a saber: produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Art. 41º O cumprimento desta Política, bem como dos normativos que a complementam deverá ser avaliado periodicamente por meio de verificações de conformidade, realizadas por grupo de trabalho formalmente instituído pelo Comitê de Segurança da Informação (CSI), buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

Art. 42º O LNCC deve observar as diretrizes estabelecidas nesta Política e deve se orientar pelas melhores práticas e procedimentos de segurança da informação e comunicações recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

Art. 43º Os contratos, convênios, acordos e instrumentos congêneres firmados pelo LNCC

devem conter cláusulas que determinem a observância desta Política e seus documentos complementares.

CAPÍTULO VII - DAS DIRETRIZES ESPECÍFICAS

Art. 44º Para cada uma das diretrizes constantes das seções deste capítulo deve ser observada a pertinência da elaboração de políticas, procedimentos, normas, orientações e/ou manuais que disciplinem ou facilitem o seu entendimento.

Seção I - Gestão da Segurança da Informação

Art. 45º A gestão de segurança da informação (GSI) deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de segurança da informação e comunicações.

Art. 46º A gestão de segurança da informação deve compreender ações e métodos que visem a estabelecer parâmetros adequados, relacionados à segurança da informação, para a disponibilização dos serviços, sistemas e infraestrutura que os apoiam, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais do LNCC.

Art. 47º Os conceitos relacionados à temática dessa política poderão ser consultados no glossário de segurança da informação, aprovado e atualizado por portaria do Gabinete de Segurança Institucional da Presidência da República.

Art. 48º Os processos relacionados à gestão de segurança da informação devem estar alinhados com os controles internos de gestão do órgão ou da entidade.

Art. 49º A gestão de segurança da informação deve ser mantida e implementada de forma contínua, buscando manter o alinhamento com a evolução da tecnologia e de seus riscos, identificando os fatores internos e externos que podem impactar no alcance dos objetivos do órgão ou da entidade.

Art. 50º Conforme definido na Instrução Normativa GSI/PR Nº 3, a gestão de segurança da informação será constituída pelos seguintes processos de realização obrigatória:

I. mapeamento de ativos de informação;

II. gestão de riscos de segurança da informação;

III. gestão de continuidade de negócios em segurança da informação;

IV. gestão de mudanças nos aspectos de segurança da informação; e

V. avaliação de conformidade de segurança da informação.

Art. 51º Os processos referentes a gestão da segurança da informação, indicados no artigo anterior, serão regulamentados por normas específicas.

Seção II - Tratamento da Informação

Art. 52º O LNCC deve criar, gerir e avaliar critérios de tratamento da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 53º É vedado comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo LNCC.

Art. 54º Quando documentos relacionados a segurança da informação, como as políticas, as normas e os procedimentos, forem distribuídos para fora da organização, deve-se assegurar a proteção de informações confidenciais ou restritas.

Seção III - Segurança em Recursos Humanos

Art. 55º Os colaboradores devem ter ciência:

I. das ameaças e preocupações relativas à segurança da informação e comunicações;

II. de suas responsabilidades e obrigações conforme estabelecidos nesta Política.

Art. 56º Todos os colaboradores devem difundir e exigir o cumprimento desta Política, de seus documentos complementares, das normas de segurança e da legislação vigente acerca do tema.

Art. 57º Os colaboradores são responsáveis pelos danos e ações causadas pelas aplicações instaladas nas suas estações de trabalho.

Art. 58º Serão estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os colaboradores do LNCC, de acordo com suas competências funcionais.

Seção IV - Gestão de Ativos da Informação

Art. 59º Segundo o Glossário de Segurança da Informação do GSI/PR:

> "Ativos de Informação são 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 os recursos humanos que a eles têm acesso."

Art. 60º Os ativos de informação devem:

I. ser inventariados e protegidos;

II. ter identificados, formalmente, o proprietário do ativo de informação e o custodiante do ativo de informação;

III. ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

IV. ter a sua entrada e saída nas dependências do LNCC autorizadas e registradas pelo proprietário do ativo de informação;

V. ter sua entrada, sua movimentação, e saída nas dependências do LNCC comunicadas, autorizadas e registradas ao setor de patrimônio do LNCC, quando o ativo for um bem patrimoniado;

VI. ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;

VII. ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 61º Os proprietários dos ativos de informação devem estabelecer regras e mecanismos que visem a proteção do ativo e a manutenção de uma base de conhecimento sobre a realização de atividades no LNCC, observadas as normas de segurança da informação e comunicações.

Art. 62º O custodiante do ativo de informação deve ser formalmente designado pelo proprietário do ativo de informação.

§ 1º A não designação pressupõe que o proprietário do ativo de informação é o próprio custodiante.

§ 2º Os proprietários dos ativos podem delegar tarefas de segurança da informação para outros. Todavia, eles permaneçam responsáveis e devem determinem se quaisquer tarefas delegadas tenham sido corretamente executadas.

Art. 63º As informações geradas, adquiridas ou custodiadas sob a responsabilidade do LNCC são consideradas parte do seu patrimônio intelectual não cabendo a seus criadores qualquer forma de direito autoral, salvo aqueles direitos garantidos no âmbito da Lei de Inovação e outros dispositivos legais, e devem ser protegidas segundo as diretrizes descritas nesta Política, em seus documentos complementares e demais regulamentações em vigor.

Art. 64º Nos termos da Lei de Acesso à Informação, é vedada a divulgação e uso por terceiros de informações restritas ou classificadas por grau de sigilo, produzidas ou custodiadas pelo LNCC, salvo nos casos de autorização específica.

Seção V - Gestão de Riscos

Art. 65º As áreas responsáveis por ativos de informação devem implantar processos contínuos de gestão de riscos, os quais serão aplicados na implementação e operação da gestão da segurança da informação e comunicações.

Art. 66º A gestão de riscos de segurança da informação será regulamentada por norma específica.

Seção VI - Gestão do Uso dos Recursos Operacionais e de Comunicações

Art. 67º Cabe ao Comitê de Segurança da Informação e ao Gestor de Segurança sugerir modelos e arquiteturas de referência, que descrevam requisitos mínimos para a disponibilização de serviços, sistemas e infraestrutura, atendendo às necessidades operacionais e de segurança desta política.

Art. 68º Cabe a Coordenação de Tecnologia da Informação (COTIC) apoiar do Comitê de Segurança da Informação (CSI) e ao Gestor de segurança na sugestão de modelos, assim como deve implementar os modelos e arquiteturas de referência, que descrevam requisitos mínimos para a disponibilização de serviços, sistemas e infraestrutura, atendendo às necessidades operacionais e de segurança desta política.

Seção VII - Relação com Terceiros

Art. 69º Nos editais de licitação, nos contratos, contratos de gestão, convênios, acordos e instrumentos congêneres de cooperação técnica com entidades prestadoras de serviços para o LNCC deverá constar cláusula específica sobre a obrigatoriedade de observância a esta Política.

Art. 70º O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta Política, bem como suas normas e procedimentos complementares aos seus empregados e prepostos envolvidos em atividades no LNCC.

Seção VIII - Controles de Acesso

Art. 71º Deve-se implementar um procedimento formal de registro e cancelamento de usuário.

Art. 72º A concessão e uso de privilégios deve ser restrita e controlada.

Art. 73º A concessão de senhas deve ser controlada por meio de um processo de gerenciamento formal.

Art. 74º Para garantir disponibilidade de acesso a ativos críticos, o LNCC pode bloquear ou limitar temporariamente o acesso, de forma parcial ou completa, aos demais ativos.

Art. 75º As diretrizes de controle de acesso, complementares, serão regulamentadas por norma específica.

Seção IX - Gestão de Continuidade

Art. 76º Deve-se implementar controles evitar a interrupção das atividades críticas ao negócio e para proteger os processos contra efeitos de falhas.

Art. 77º A Gestão de continuidade será regulamentada por norma específica.

Seção X - Auditoria e Conformidade

Art. 78º O processo de auditoria deve ser definido segundo os objetivos estratégicos do LNCC.

Art. 79º Anualmente deve-se promover a execução de auditorias interna e externa de segurança da informação nos ativos do Supercomputador Santos Dumont e nos ativos hospedados no CPD do LNCC diretamente conectados ao supercomputador.

Art. 80º As diretrizes relacionadas a Auditoria e Conformidade serão regulamentadas por norma específica.

Seção XI - Segurança Física e do Ambiente

Art. 81º Deve-se implementar um perímetro de segurança para proteger as áreas que hospedam, processam, utilizam e transmitam informações críticas ao negócio.

Art. 82º As diretrizes relacionadas a Segurança Física e do Ambiente serão regulamentadas por norma específica.

Seção XII - Gestão de Incidentes em Segurança da Informação

Art. 83º Deve-se assegurar um enfoque consistente e efetivo à gestão de incidentes de segurança da informação.

Art. 84º A Gestão de incidentes em segurança da informação será regulamentada por norma específica.

CAPÍTULO VIII - DOS DESVIOS E EXCEÇÕES

Art. 85º A não observância desta Política e/ou de seus documentos complementares, bem como a quebra de controles de segurança da informação e comunicações, poderá acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 86º Casos omissos e exceções a esta política devem ser tratadas pelo Gestor de Segurança da Informação e pelos membros do comitê de segurança e posteriormente encaminhadas para a direção.

CAPÍTULO IX - DA MANUTENÇÃO, DISTRIBUIÇÃO E VIGÊNCIA

Art. 87º A Política de Segurança da Informação, bem como o conjunto de instrumentos normativos relacionados a segurança da informação, devem ser analisados criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

Art. 88º O intervalo entre os processos de análise crítica desta política não deve exceder o período máximo de 2 (dois) anos.

Art. 89º O intervalo entre os processos de análise crítica das demais políticas, normas complementares, procedimentos e demais documentos relacionados a segurança da informação não deve exceder o período máximo de 1 (um) ano.

Art. 90º Os documentos relacionados a segurança da informação serão publicados e disponibilizados segundo os critérios de classificação e rotulação definidos pela instituição.

I. Os documentos públicos serão disponibilizados em site próprio (https://sec.lncc.br), assim como no site oficial da instituição (https://www.lncc.br);

II. Os manuais de processo e de operação serão publicados em um repositório definido pela equipe responsável.

Art. 91º A presente portaria entre em vigor na data de sua publicação, permanecendo válida até que seja revogada.

Anexo A: Conceitos e Definições

Este anexo relaciona e descreve os conceitos e definições a serem utilizados nesta política. O seu conteúdo tem como base o Glossário de Segurança da Informação, aprovado pelo Gabinete de Segurança Institucional da Presidência da República.

Agente Público[1]	:	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 APF, direta e indireta;
CENAPAD	:	Centro Nacional de Processamento de Alto Desempenho.
COGEA	:	Coordenação de Gestão e Administração.
Colaborador[2]	:	No contexto deste documento, entende-se como colaborador quais quer agente público, estagiário, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações do Laboratório Nacional de Computação Científica.
COMAC	:	Coordenação de Métodos Matemáticos e Computacionais.
COMOD	:	Coordenação de Modelagem Computacional.
COPGA	:	Coordenação de Pós-Graduação e Aperfeiçoamento.
COTIC	:	Coordenação de Tecnologia da Informação e Comunicação.
CSIC	:	Comitê de Segurança da Informação e Comunicações e de Segurança Física.
ISO	:	*International Organization for Standardization.*
LNCC	:	Laboratório Nacional de Computação Científica.
MSO	:	*Management System Overview.*
Necessidade de Conhecer	:	Ou "*Need to know*" é condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais.

[1] Glossário de Segurança da Informação - PORTARIA Nº 93, DE 26 DE SETEMBRO DE 2019 do Gabinete de Segurança Institucional da Presidência da República

[2] Vide glossário da Política da Segurança da Informação do LNCC

NUSTI	:	Núcleo de Governança de Tecnologia da Informação.
PAD	:	Processamento de Alto Desempenho.
Política de Segurança[2]	:	Conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação das entidades.
PSI[2]	:	Política de Segurança da Informação é o documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da SI (Este termo substituiu o termo Política de Segurança da Informação e Comunicações).
SDumont	:	Supercomputador Santos Dumont.
Segurança Cibernética[2]	:	Ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.
Segurança Corporativa[2]	:	Veja Segurança Orgânica.
Segurança da Informação[2]	:	Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.
Segurança Orgânica[2]	:	Conjunto de medidas passivas com o objetivo de prevenir e até mesmo obstruir as ações que visem ao comprometimento ou à quebra de segurança de uma organização. Inclui os processos relacionados às áreas: de pessoal, de documentação, das comunicações, da tecnologia da informação, dos materiais e das instalações de uma organização, dentre outros.
SGIS	:	Sistema de Gestão de Segurança da Informação.
SINAPAD	:	Sistema Nacional de Processamento de Alto Desempenho.
SSD	:	Supercomputador Santos Dumont.
TIC	:	Tecnologia da Informação e Comunicações.