POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO LNCC			
CÓDIGO	**VERSÃO**	**TIPO DE ACESSO**	**NÍVEL DE ACESSO**
02-PSI	2.0	Externo	Público
CONTROLES DA ABNT NBR ISO/IEC 27001:2013		**PUBLICADO EM**	**PAGINAÇÃO**
A.5.1 - Orientação da Direção para segurança da informação		16/04/2024	1/10

SUMÁRIO

1 OBJETIVO

1.1. Por intermédio deste documento, fica instituída a Política de Segurança da Informação (PSI), no âmbito do LNCC, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

1.2. Este documento é uma declaração formal do LNCC a respeito do seu compromisso com a proteção dos ativos de informação de sua propriedade e sua guarda.

1.3. Esta política representa o comprometimento do LNCC 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. Esta política inclui o compromisso do LNCC com o processo da melhoria contínua do Sistema de Gestão da Segurança da Informação.

1.4. Este documento é uma declaração formal do comprometimento da alta administração, do LNCC com vistas a prover diretrizes estratégicas, responsabilidades, competências e apoio para implementar a gestão da segurança da informação em sua organização.

1.5. Esta política foi elaborada pelo LNCC, com base:

a) nas normas técnicas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013;
b) na legislação vigente;
c) na realidade; e
d) nos requisitos de negócio da entidade.

1.6. "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.".

1.7. Na preparação desta política e demais instrumentos relacionados a segurança da informação deve levar em consideração a natureza e a finalidade LNCC. Todos os normativos de segurança da informação devem estar alinhados ao seu planejamento estratégico.

1.8. 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.

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

1.10. A metodologia de gestão da segurança da informação do LNCC deve seguir as orientações previstas na legislação vigente. A metodologia baseia-se no processo de melhoria contínua, considerando o ciclo "PDCA" (*Plan-Do-Check-Act*), referenciado pela norma ABNT NBR ISO/IEC 27001.

1.11. O LNCC deve adotar os controles de segurança da informação estabelecidos pelo Gabinete de Segurança Institucional da Presidência da República.

1.12. A autoridade máxima 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.

1.13. O Gestor de Segurança da Informação deve 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 LNCC.

1.14. 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.

1.15. Para os fins do disposto nesta política, a segurança da informação abrange:

a) a segurança cibernética;
b) a defesa cibernética;
c) a segurança física;
d) a proteção de dados organizacionais; e
e) as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

1.16. São objetivos desta política:

a) Estabelecer e difundir as diretrizes de segurança da informação no âmbito do LNCC, de seus projetos e cooperações;
b) 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;
c) Fortalecer a cultura da segurança da informação na sociedade;
d) Orientar ações relacionadas a:
   i. segurança dos dados custodiados pela instituição;
   ii. segurança da informação das infraestruturas críticas;
   iii. proteção das informações das pessoas físicas que possam ter sua segurança ou a segurança das suas atividades afetada, observada a legislação específica;
   iv. tratamento das informações com restrição de acesso;
   v. uso adequado das informações e recursos de tecnologia da informação suportados pela instituição evitando impactos prejudiciais às atividades de negócio da instituição.
e) 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.

2 CAMPO DE APLICAÇÃO

2.1 Esta política se aplica a todas as unidades organizacionais do LNCC atuantes nos processos que fazem parte do escopo certificado em conformidade à ABNT NBR ISO/IEC 27001.

2.2 Esta política aplica-se a todos os ativos no escopo do Sistema de Gestão de Segurança da Informação (SGSI) do Supercomputador Santos Dumont (SSD) e do CPD do LNCC que estão conectados ao SSD.

2.3 Esta política considera a abrangência da segurança da informação nos aspectos físico, lógico, comportamental, de pessoas, processos e tecnologias, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

2.4 A política aplica-se a todas as formas intelectuais e físicas de ativos de informação, sejam próprios, utilizados ou custodiados no LNCC e relacionadas ao Supercomputador Santos Dumont. Estas formas incluem hardware, redes, software e dados, sejam armazenadas e processadas em computadores, transmitidas através de redes, impressas ou escritas 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, sociais redes, chats ou wikis.

2.5 Esta política 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 da instituição.

2.6 Esta política também se aplica, no que couber, ao relacionamento do LNCC com outros órgãos e entidades públicos ou privados.

2.7 Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo LNCC devem:

a) atender, no que couber, a esta política e demais normas relacionadas.
b) conter a previsão de termo específico de responsabilidade e sigilo, quando a natureza de seu objeto ou condições específicas assim o exigirem.
c) 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.

3 RESPONSABILIDADE

3.1 A responsabilidade pela elaboração, revisão e publicação desta norma é do Comitê de Segurança da Informação e Comunicação do LNCC.

3.2 A responsabilidade pela aprovação e cancelamento desta norma é do diretor do LNCC.

3.3 Este documento é elaborado com o apoio do Gestor de Segurança da Informação.

4 DOCUMENTOS DE REFERÊNCIA

Os documentos a seguir, no todo ou em parte, são referenciados neste documento e fornecem requisitos, diretrizes ou orientações que são indispensáveis à sua aplicação. Para referências datadas, aplicam-se somente as edições citadas. Para referências não datadas, aplicam-se as edições mais recentes do documento, incluindo emendas.

ISO/IEC 27000:2018	Information technology — Security techniques — Information security management systems — Overview and vocabulary
ABNT NBR ISO/IEC 27001:2013	Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos
ABNT NBR ISO/IEC 27002:2013	Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Aprova o Glossário de Segurança da Informação (https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370)
Lei nº 8.112, de 11 de dezembro de 1990	dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais
Lei nº 8.159, de 8 de janeiro de 1991	dispõe sobre a Política Nacional de Arquivos Públicos e privados
Lei nº 8.745, de 9 de dezembro de 1993	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
Lei nº 9.962, de 22 de fevereiro de 2000	disciplina o regime de emprego público do pessoal da administração federal direta, autárquica e fundacional
Lei n° 9.983, de 14 de julho de 2000	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
Lei nº 12.527, de 18 de novembro de 2011	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
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
Decreto nº 4.073, de 3 de janeiro de 2002	regulamenta a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados
Decreto nº 6.029, de 1º de fevereiro de 2007	institui o Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências
Decreto nº 7.724, de 16 de maio de 2012	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
Decreto nº 7.845, de 14 de novembro de 2012	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
Decreto nº 9.637, de 26 de dezembro de 2018	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
Decreto nº 10.222, de 5 de fevereiro de 2020	aprova a Estratégia Nacional de Segurança Cibernética
Portaria interministerial MCT/MPOG nº 140, de 16 de março de 2006	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
Decreto nº 11.529, de 16 de maio de 2023	dispõe sobre o Sistema de Integridade, Transparência e Acesso à Informação da Administração Pública Federal; e a Política de Transparência e Acesso à Informação da Administração Pública Federal

continua...

Portaria GSI/PR nº 93, de 18 de outubro de 2021	aprova o Glossário de Segurança da Informação
Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021	dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da Administração Pública Federal
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
Portaria LNCC/MCTI nº 420, de 28 de março de 2024	constitui o Comitê de Privacidade e Segurança do LNCC

4.1 Devem ser utilizadas, ainda, as instruções normativas e normas complementares relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República.

5 DOCUMENTOS COMPLEMENTARES

Os documentos a seguir serão utilizados, no todo ou em parte, para viabilizar a aplicação das informações documentadas do SGSI, devendo estar citados no corpo do texto normativo e disponíveis para uso.

6 SIGLAS

CPD	Centro de Processamento de Dados
CPSI	Comitê de Privacidade e Segurança da Informação
CSI	Comitê de Segurança da Informação IN GSI/PR Nº 3, de 28 de maio de 2021.
CTIR GOV	Centro de Tratamento e Resposta de Incidentes Cibernéticos do Governo
ETIR	Equipe de Tratamento e Resposta a Incidentes Cibernéticos
LNCC	Laboratório Nacional de Computação Científica
PSI	Política de Segurança da Informação
SGSI	Sistema de Gestão de Segurança da Informação
SSD	Supercomputador Santos Dumont
TIC	Tecnologia da Informação e Comunicações

Nota - As siglas das UO do LNCC podem ser acessadas no Regimento Interno do Laboratório Nacional de Computação Científica.

7 TERMOS E DEFINIÇÕES

Colaboradores	No contexto deste documento, entende-se como colaborador quaisquer agente público, estagiário, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações da instituição.

Para os efeitos deste documento, aplicam-se os termos e definições a seguir, baseados nas normas de referência, Portaria GSI/PR nº 93/2021, ISO/IEC 27000:2018, que devem ser interpretados somando-se as descrições. Em caso de divergência, prevalecem o termo e a definição estabelecidos na Portaria GSI/PR nº 93/2021

8 PRINCÍPIOS

8.1 As ações de Segurança da Informação no LNCC devem ser norteadas pelos seguintes princípios:

a) 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;
b) Visão abrangente e sistêmica da segurança da informação;
c) Responsabilidade do LNCC na coordenação de esforços e no estabelecimento de políticas, estratégias e diretrizes relacionadas à segurança da informação;
d) Educação como alicerce fundamental para o fomento da cultura em segurança da informação;
e) Orientação à gestão de riscos e à gestão da segurança da informação;
f) Prevenção e tratamento de incidentes de segurança da informação;
g) 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;
h) *Need to know* (necessidade de conhecer) para o acesso à informação sigilosa, nos termos da legislação;
i) Consentimento do proprietário da informação sigilosa recebida de outros países, nos casos dos acordos internacionais;
j) Cooperação entre os órgãos de investigação e os órgãos e as entidades públicos no processo de credenciamento de pessoas para acesso às informações sigilosas;
k) Integração e cooperação entre o Poder Público, o setor empresarial, a sociedade e as instituições acadêmicas;
l) Deve haver um alinhamento entre a Política de Segurança da com a missão institucional e seu planejamento estratégico;

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

8.2 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.

9 COMPETÊNCIAS

9.1 As atribuições, referentes a gestão, coordenação e operação da segurança da informação, serão determinadas mediante portarias internas do LNCC e poderão complementar as competências descritas nesta política.

9.2 Gestor de Segurança da Informação – GSI

9.2.1 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.

9.2.2 Compete ao gestor de segurança da informação:

a) Coordenar o Comitê de Segurança da Informação e a Equipe de Tratamento e Resposta a Incidentes Cibernéticos;
b) 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;
c) Assessorar a alta administração na implementação da Política de Segurança da Informação e das normas internas de segurança da informação;
d) Estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
e) 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 LNCC;
f) Promover a cultura de segurança da informação;
g) Realizar, incentivar e acompanhar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;
h) Propor recursos necessários às ações de segurança da informação;
i) Verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;
j) Acompanhar as investigações e as avaliações dos dados decorrentes de quebras de segurança;
k) Acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e
l) 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.

9.3 Comitê de Privacidade e Segurança da Informação

9.3.1 O Comitê de Privacidade e Segurança da Informação (CPSI), 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.

9.3.2 O Comitê possui as seguintes atribuições:

a) Assessorar a implementação das ações de privacidade e segurança da informação;
b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre privacidade e segurança da informação;
c) 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;
d) Exercer outros atos de assessoramento e de proposição afetos à matéria de segurança da informação e comunicações.

9.4 Equipe de Tratamento e Resposta a Incidentes Cibernéticos

9.4.1 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.

9.4.2 A ETIR do LNCC tem como objetivos:

a) monitorar as redes computacionais;
b) detectar e analisar ataques e intrusões;
c) tratar incidentes de segurança da informação;
d) identificar vulnerabilidades e artefatos maliciosos;
e) recuperar sistemas de informação; e
f) promover a cooperação com outras equipes, bem como participar de fóruns e redes nacionais e internacionais relativos à Segurança da Informação.

9.4.3 A equipe deve ser composta, por servidores públicos civis ocupantes de cargo efetivo ou militares de carreira, com capacitação técnica compatível com as atividades dessa equipe.

9.4.4 A atuação da Equipe deve ser 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.

9.4.5 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 CTIR GOV.

9.5 Do Agente Responsável pela ETIR

9.5.1 Compete ao Agente Responsável pela ETIR do LNCC:

a) Estabelecer os procedimentos operacionais, gerenciar as atividades e distribuir tarefas para a ETIR;
b) Assistir o CTIR GOV com informações necessárias à atualização e manutenção das bases de dados de incidentes do Governo Federal.

9.6 Conselhos, Coordenações, Serviços, Seções, Setores e Áreas

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

9.7 Colaboradores

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

9.7.2 Os colaboradores do LNCC envolvidos no escopo definido anteriormente devem ser informados acerca desta política de segurança.

9.7.3 Os colaboradores do LNCC devem:

a) cumprir fielmente as políticas, as normas, os procedimentos e as orientações de segurança da informação e comunicações do LNCC;
b) buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;
c) assinar Termo de Responsabilidade, formalizando a ciência e o aceite da PSI do LNCC, bem como assumindo responsabilidade por seu cumprimento;
d) proteger as informações da instituição contra acesso, modificação, destruição ou divulgação não-autorizados pelo LNCC;
e) assegurar que os recursos tecnológicos à sua disposição sejam utilizados conforme a política de uso aceitável;
f) comunicar imediatamente ao Comitê de Privacidade e Segurança da Informação (CPSI) qualquer descumprimento ou violação desta Política ou de seus documentos complementares;
g) participar dos treinamentos de segurança da informação e das atividades de conscientização sobre o mesmo tema;
h) utilizar apenas os serviços, recursos e demais ativos aos quais foi autorizado o acesso;
i) não utilizar os ativos do LNCC para finalidades diferentes daqueles relacionados aos objetivos do projeto, atividade ou função ao qual está vinculado.
j) implementar uma política de mesa limpa e tela limpa;
k) ao se afastar, deve utilizar os recursos disponíveis para realizar o bloqueio de sua estação de trabalho;
l) não fornecer, divulgar ou compartilhar credenciais de acesso.

10 DIRETRIZES GERAIS

10.1 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.

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

10.3 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.

10.4 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 instituido, buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

10.5 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.

10.6 Os contratos, convênios, acordos e instrumentos congêneres firmados pelo LNCC devem conter cláusulas que determinem a observância desta Política e seus documentos complementares.

11 DIRETRIZES ESPECÍFICAS

11.1 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.

11.2 Gestão da Segurança da Informação

11.2.1 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.

11.2.2 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.

11.2.3 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.

11.2.4 Os processos relacionados à gestão de segurança da informação devem estar alinhados com os controles internos do LNCC.

11.2.5 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.

11.2.6 Conforme definido na IN GSI/PR Nº 3, a gestão de segurança da informação será constituída pelos seguintes processos de realização obrigatória:

a) mapeamento de ativos de informação;
b) gestão de riscos de segurança da informação;
c) gestão de continuidade de negócios em segurança da informação;
d) gestão de mudanças nos aspectos de segurança da informação; e
e) avaliação de conformidade de segurança da informação.

11.2.7 Os processos referentes a gestão da segurança da informação, indicados no item anterior, serão regulamentados por normas específicas.

11.3 Tratamento da Informação

11.3.1 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.

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

11.3.3 Quando documentos relacionados a segurança da informação, como as políticas, as normas e os procedimentos, forem disponibilizados para acesso externo, deve-se assegurar a proteção de informações confidenciais ou restritas.

11.4 Segurança em Recursos Humanos

11.4.1 Os colaboradores devem ter ciência:

a) das ameaças e preocupações relativas à segurança da informação e comunicações;
b) de suas responsabilidades e obrigações conforme estabelecidos nesta Política.

11.4.2 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.

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

11.4.4 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.

11.5 Gestão de Ativos da Informação

11.5.1 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.".

11.5.2 Os ativos de informação devem:

a) ser inventariados e protegidos;
b) ter identificados, formalmente, seu proprietário e, quando aplicável, os custodiantes.
c) ter mapeadas as suas ameaças, vulnerabilidades e interdependências;
d) ter sua entrada, sua movimentação, e saída nas dependências do LNCC comunicadas, autorizadas e registadas ao setor de patrimônio do LNCC, quando o ativo for um bem patrimoniado;
e) 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;
f) 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.

11.5.3 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.

11.5.4 O custodiante do ativo de informação deve ser formalmente designado pelo proprietário do ativo de informação.

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

Nota - Os proprietários dos ativos podem delegar tarefas de segurança da informação para outros. Todavia, eles permanecem responsáveis pela segurança do ativo.

11.5.5 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.

11.5.6 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.

11.6 Gestão de Riscos

11.6.1 As áreas responsáveis pelos 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.

11.6.2 O processo de gestão de risco deve estar alinhado com a IN GSI/PR Nº 3/2021.

11.6.3 A gestão de riscos de segurança da informação deve ser regulamentada por norma específica.

11.7 Gestão do Uso dos Recursos Operacionais e de Comunicações

11.7.1 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.

11.7.2 Cabe à 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 infraestruturas mantidas pela instituição,

atendendo às necessidades operacionais e de segurança desta política.

11.8 Relação com Terceiros

11.8.1 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.

11.8.2 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.

11.9 Controle de Acesso

11.9.1 Deve-se implementar um procedimento formal de registo e cancelamento de usuário.

11.9.2 A concessão e uso de privilégios deve ser restrita e controlada.

11.9.3 A concessão de senhas deve ser controlada por meio de um processo de gerenciamento formal.

11.9.4 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.

11.9.5 As diretrizes de controle de acesso, complementares, serão regulamentadas por norma específica.

11.10 Gestão de Continuidade

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

11.10.2 O processo de gestão de continuidade de negócios deve estar alinhado com a IN GSI/PR Nº 3/2021.

11.10.3 A Gestão de continuidade será regulamentada por norma específica.

11.11 Auditoria e Conformidade

11.11.1 O processo de auditoria deve ser definido segundo os objetivos estratégicos do LNCC.

11.11.2 O processo de avaliação de conformidade deve estar alinhado com a IN GSI/PR Nº 3/2021.

11.11.3 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.

11.11.4 As diretrizes relacionadas a Auditoria e Conformidade serão regulamentadas por norma específica.

11.12 Segurança Física e do Ambiente

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

11.12.2 As diretrizes relacionadas a Segurança Física e do Ambiente serão regulamentadas por norma específica.

11.13 Gestão de Incidentes em Segurança da Informação

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

12.12.2 O processo de gestão de incidentes de segurança de informação deve estar alinhado com a IN GSI/PR Nº 3/2021.

12.12.3 A Gestão de incidentes em segurança da informação será regulamentada por norma específica.

12 DESVIOS E EXCEÇÕES

13.1 A não observância desta Política e dos documentos do SGSI, 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.

13.2 Casos omissos e exceções a esta política devem ser tratadas pelo GSI, pelos membros do CPSI e posteriormente encaminhadas para a direção.

13 MANUTENÇÃO, DISTRIBUIÇÃO E VIDÊNCIA

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

13.2 Este documento é de distribuição pública e destina-se a todos os colaboradores do LNCC e as partes interessadas.

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

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

13.5 Os documentos relacionados à segurança da informação serão publicados e disponibilizados segundo os critérios de classificação e rotulação definidos pela instituição.

a) Os documentos públicos devem ser disponibilizados em site próprio (https://sec.lncc.br), assim como no site oficial da instituição (https://www.lncc.br);
b) Os manuais de processo e de operação devem ser publicados em um repositório definido pela equipe responsável.

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

14 HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Versão	Data	Descrição
--	30/07/2019	Portaria nº 81/2019/SEI-LNCC de 30 de julho de 2019
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.
2.0	16/04/2024	Análise crítica do documento; adequação a estrutura do CPSI; adequação a legislação.

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborado por	Luís Rodrigo de O. Gonçalves	Gestor de Segurança da Informação
Verificado por	Comitê de Privacidade e Segurança do LNCC - Portaria LNCC/MCTI nº 420/2024	Membros do Comitê de Privacidade e Segurança do LNCC
Aprovado por	Fábio Borges de Oliveira	Diretor do Laboratório Nacional de Computação Científica

Documento assinado eletronicamente no Processo SEI nº 01209.000061/2020-55.