Política de Segurança da Informação do LNCC-SANTOS DUMONT			
CÓDIGO	**VERSÃO**	**TIPO DE ACESSO**	**NÍVEL DE ACESSO**
03-PSISD	03	Externo	Público
CONTROLES DA ABNT NBR ISO/IEC 27001:2013		**PUBLICADO EM**	**PAGINAÇÃO**
A.5.1 - Orientação da Direção para segurança da informação		23 de maio de 2023	1/3

Sumário

1 OBJETIVO 1
2 CAMPO DE APLICAÇÃO 1
3 RESPONSABILIDADE 1
4 DOCUMENTOS DE REFERÊNCIA 1
5 DOCUMENTOS COMPLEMENTARES 2
6 SIGLAS 2
7 TERMOS E DEFINIÇÕES 2
8 POLÍTICA DE TRANSIÇÃO 2
9 PAPEIS E RESPONSABILIDADES 2
10 ABNT NBR ISO/IEC 27001:2013 2
11 CONTROLES E DIRETRIZES 3
12 TREINAMENTO 3
13 ANÁLISE CRÍTICA 3
14 HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO 3

1 OBJETIVO

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 no que tange ao Supercomputador Santos Dumont.

Esta Política de Segurança da Informação foi elaborada pelo LNCC, com base: (i) nas normas técnicas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013, (ii) na legislação vigente, (iii) na realidade e (iv) nos 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.".

2 CAMPO DE APLICAÇÃO

Esta política se aplica a todas as unidades organizacionais do LNCC que atuam nos processos que fazem parte do escopo certificado em conformidade à ABNT NBR ISO/IEC 27001. Este documento é de distribuição pública e destina-se a todos os colaboradores do LNCC e as partes interessadas

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

Esta política considera a abrangência da segurança da informação nos aspectos físico, lógico, comportamental, de pessoas, processos e tecnologias, preservando a confidencialidade, a integridade e a disponibilidade das informações do LNCC relacionados ao Supercomputador Santos Dumont ou sob sua salvaguarda.

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, 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.

3 RESPONSABILIDADE

A responsabilidade pela elaboração, revisão e publicação desta norma é do Comitê de Segurança da Informação e Comunicação do LNCC. A responsabilidade pela aprovação e cancelamento desta norma é do diretor do LNCC. 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)
Política de Segurança da Informação do LNCC	Institui 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 (https://www.gov.br/lncc/pt-br/acesso-a-informacao/institucional/politica-de-seguranca-1/02-PSI%20LNCC)

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

SGSI Sistema de Gestão de Segurança da Informação

ISMS Information Security Management System.

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 (https://www.in.gov.br/web/dou/-/portaria-n-3.454-de-10-de-setembro-de-2020-276999290).

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 e ABNT NBR ISO 9000:2015, 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 POLÍTICA DE TRANSIÇÃO

8.1 O prazo para adequação dos processos e procedimentos aos novos requisitos desta norma será até dezembro/2023.

8.2 Após essa data, os documentos que não tenham sido adequados à presente versão serão considerados não conformes com relação aos novos requisitos.

9 PAPEIS E RESPONSABILIDADES

9.1 O Diretor do LNCC é o responsável pela aprovação e pelo cancelamento desta norma.

9.2 O comitê de segurança da informação é o responsável pela análise crítica desta política.

9.3 Esta política se aplica a todos os colaboradores do LNCC, quais sejam: funcionários servidores efetivos ou comissionados, estagiários, menores aprendizes, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações deste órgão no que tange ao Supercomputador Santos Dumont.

9.4 Os colaboradores do LNCC envolvidos no espoco definido anteriormente devem ser informados acerca certa desta política de segurança.

9.5 O SECIN é o responsável por realizar a divulgação desta política para os colaboradores e demais partes interessadas.

9.6 Quando da identificação, os colaboradores e demais partes interessadas devem realizar a notificação de não conformidade, riscos e oportunidades de melhorias ao Gestor de Segurança da Informação (gsi@lncc.br)

10 ABNT NBR ISO/IEC 27001:2013

10.1 Para assegurar os aspectos apresentados na seção 1 OBJETIVO, deve-se colocar em prática um processo de gestão de

segurança da informação. Este processo, baseado na Norma ISO/IEC 27001:2013 (“Information Technology - Security Techniques - Information Security Management Systems - Requirements”), é o chamado SGSI - Sistema de Gestão de Segurança da Informação (em inglês, ISMS - Information Security Management System).

10.2 O Sistema de Gestão de Segurança da Informação (SGSI) deve prever diversas ações, subprocessos, políticas e procedimentos de segurança, praticando a missão de reduzir continuamente os riscos à segurança das informações e aos ativos críticos de uma organização

11 CONTROLES E DIRETRIZES

11.1 Esta política define e padroniza o uso, o tratamento, o controle e a proteção das informações que possam causar impactos no desempenho financeiro, na participação no mercado e na imagem do LNCC, agregando valor à operação e eficiência na prestação de serviços ou no relacionamento com as partes interessadas, definidas no documento "Sistema de Gestão de Segurança da Informação (SGSI-SSD/LNCC) ".

11.2 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 27001:2013 e a Política de Segurança da Informação do LNCC, bem como informações contratuais estatutárias e do processo.

11.3 A política inclui o compromisso com o processo da melhoria contínua do Sistema de Gestão da Segurança da Informação.

11.4 Os requisitos estatutários da “Política de Segurança da Informação do LNCC” são também parte obrigatória dessa política, de acordo com os requisitos do negócio do Supercomputador Santos Dumont e com as leis e regulamentações aplicáveis.

12 TREINAMENTO

12.1 Os colaboradores do LNCC devem receber orientações de Segurança da Informação. Para tanto, podem ser aplicadas ações de capacitação e desenvolvimento, campanhas de comunicação via e-mail institucional ou via publicações nos murais de comunicação disponíveis nas dependências do LNCC.

13 ANÁLISE CRÍTICA

13.1 Este documento deve ser analisado criticamente, quanto à sua eficácia e adequação ao SGSI do LNCC, sempre que necessário, ao menos, uma vez ao ano.

14 HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens Revisados
1.0	02/03/2020	Documento Inicial.
1.1	20/05/2020	Inclusão da classificação e tipo de acesso.
1.2	28/04/2021	Revisão da estrutura do documento e atualização do *template*.
1.3	18/05/2021	Revisão das seções 3.5 e 4.
2.0	01/06/2022	Análise crítica do documento; revisão do texto; ajuste nas nomenclaturas.
3.0	23/05/2022	Análise crítica do documento; atualização do template;

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborado por	Luís Rodrigo de O. Gonçalves	Gestor de Segurança da Informação
Verificado por	Bruno Alves Fagundes	Gestor Substituto de Segurança da Informação
Aprovado por	Fábio Borges de Oliveira	Diretor do Laboratório Nacional de Computação Científica