Sistema de Gestão de Segurança da Informação (SGSI-SSD/LNCC)

Controle Interno	08-ISMS
Classificação	Público
Grupo Responsável	Gestão de Segurança da Informação
Autor(es)	Luís Rodrigo de Oliveira Gonçalves
Versão	4.0
Data do Documento	04 de abril de2022
Número de Páginas	34
Controles da ISO	Seções 4 a 10 da 27001
Tipo do Documento	Política

Diretor
Fábio Borges de Oliveira

Setor de Governança de Tecnologia da Informação - SESTI
Rogério Albuquerque de Almeida

Gestão de Segurança da Informação - GSI
Luís Rodrigo de O. Goncalves

Histórico das Versões

Versão	Data	Descrição	Revisor(es)
1.0	11/10/2019	Documento Inicial.	Rogério Albuquerque de Almeida
2.0	27/02/2020	Atualização da estrutura organizacional do LNCC; das informações sobre o Modelo de gestão de segurança da informação.	Luís Rodrigo de O. Gonçalves
3.0	01/03/2020	Atualização das seções Público alvo; Estrutura organizacional do LNCC; Modelo de gestão de segurança da informação; Gerenciamento de Ativos; Partes Interessadas e LNC ISMS.	Luís Rodrigo de O. Gonçalves
3.1	25/05/2020	Aplicação dos Rótulos de Classificação	Luís Rodrigo de O. Gonçalves
3.2	08/03/2021	Atualizado com as informações do novo regimento interno da instituição.	Luís Rodrigo de O. Gonçalves
3.3	22/04/2021	Adequação do documento ao novo formato	Rogério Albuquerque de Almeida
4.0	04/05/2022	Revisão anual, atualização com as informações da PSI, consolidação das informações do MSO dentro do ISMS	Luís Rodrigo de O. Gonçalves

Sumário

1) Introdução

O Laboratório Nacional de Computação Científica (LNCC) é unidade de pesquisa integrante da estrutura do Ministério da Ciência, Tecnologia e Inovações. O LNCC é uma "Instituição Científica, Tecnológica e de Inovação (ICT)"

Este documento apresenta uma visão geral do Sistema de Gestão de Segurança da Informação (SGSI) do LNCC (Laboratório Nacional de Computação Cientifica), em um melhor nível de detalhamento.

1.1) Propósito

O Laboratório Nacional de Computação Científica (LNCC) aplica a norma ISO 27001:2013 para a implementação do seu Sistema de Gestão de Segurança da Informação (SGSI).

Na subseção 4.4 - Sistemas de Segurança da Informação, a Norma ABNT NBR ISO/IEC 27001:2013 determina que:

> *"A organização deve estabelecer, implementar, manter e continuamente melhorar um sistema de gestão da segurança da informação, de acordo com os requisitos desta Norma."*

1.2) Abrangência

O Sistema de Gestão de Segurança da Informação (SGSI), implementado para ISO 27001:2013, abrange somente o ambiente do Supercomputador Santos Dumont (SSD)

A definição do SGSI deve ser aprovada e assinada pela Direção do LNCC e pelo gestor de segurança da informação, que serão os responsáveis por aprovar o escopo de certificação e sua aplicabilidade dentro do ambiente supracitado.

1.3) Público alvo

Este documento deve ser de conhecimento da direção da instituição, do presidente do Comitê de Segurança da Informação e Comunicações e de Segurança Física (CSIC), do gestor de segurança da informação, dos auditores, dos servidores e dos colaboradores do LNCC diretamente envolvidos na segurança da informação e no processo de certificação da ISO/IEC 27001.

1.4) Distribuição deste documento.

A documentação relevante ao SGSI é assinada, armazenada e gerenciada em um sistema eletrônico (SEI-MCTIC - Sistema Eletrônico de Informações). O acesso pode ser controlado conforme necessário.

Os documentos serão revisados e atualizados periodicamente, de acordo com desenvolvimentos regulatórios, necessidades do mercado e melhores práticas. Os

documentos também são publicados e estão disponíveis para todos os servidores e colaboradores, autorizados, no site https://sec.lncc.br. Todos os manuais de processo são publicados no mesmo repositório. Todos os documentos classificados como públicos, poderão ser obtidos a partir do site da instituição (https://www.lncc.br)

1.5) Documentação Relacionada.

Esta seção lista os documentos relacionados ao SGSI:

- **02-PSIC:** política de segurança da informação geral da instituição
- **03-PSISD:** política de segurança da informação do Supercomputador Santos Dumont (SSD)
- **37-MAR:** descreve a Metodologia de Avaliação de Risco utilizada no SGSI

2) O Sistema de Gestão da Segurança

Esta seção descreve o Sistema de Gestão de Segurança (SGSI) do Laboratório Nacional de Computação Científica (LNCC).

2.1) Escopo

Este Sistema de Gestão da Segurança da Informação (SGSI) abrange somente o ambiente do Supercomputador Santos Dumont (SSD) e toda a infraestrutura do LNCC vinculada a ele.

A definição do perímetro, inclusão e exclusões é descrita no Anexo A – Inclusão e Exclusão deste documento.

Partes internas e externas, incluindo organismos de certificação, podem usar este documento para avaliar a capacidade da organização em atender aos requisitos de clientes, regulamentares, legais e da própria organização.

2.2) Contexto da organização

Desde sua criação em 1980 o LNCC tem como atividades precípuas a pesquisa, o desenvolvimento e a formação de recursos humanos em Computação Científica, assim como implantar, manter e disponibilizar à comunidade científica de todo o país uma plataforma computacional de alto desempenho.

Sua origem se identifica com a atuação de grupos de pesquisadores com interesse em pesquisar, desenvolver e aplicar metodologias matemáticas e computacionais na solução de problemas multidisciplinares originados de mais diversas áreas, notadamente, das Engenharias, Física, Biologia, Ciências Sociais e na percepção da importância que a Computação Científica então assumia tanto no suporte à pesquisa científica e tecnológica em diversas áreas, como representando uma nova metodologia de se fazer ciência.

Em 2000 começaram a ser desenvolvidas no LNCC aplicações da Computação Científica na Bioinformática e em Medicina, com a criação dos laboratórios LABINFO – Laboratório Nacional de Bioinformática, com uma unidade de Genômica Computacional, e o HeMoLab – Laboratório de Modelagem em Hemodinâmica.

Atualmente, as atividades de pesquisa e desenvolvimento do LNCC estão centradas em duas coordenações, a de Métodos Matemáticos e Computacionais e a de Modelagem Computacional, agregando pesquisadores nas linhas de pesquisa em: métodos numéricos e algoritmos; modelagem computacional de sistemas complexos; sistemas, controles e sinais; computação de alto desempenho; ciência de dados; biologia computacional.

Projetos de aplicações são desenvolvidos em diversas áreas, notadamente, em bioinformática; na medicina assistida por computação científica; fenômenos de transporte; reservatórios de petróleo, água e gás; sísmica; processamento de grande massa de dados; ambientes colaborativos e multimídia; redes e computação distribuídas.

Ao longo de sua história, o LNCC tem disponibilizado, como Laboratório Nacional, o uso compartilhado de sua plataforma computacional de alto desempenho para toda a comunidade científica e tecnológica do país. A aquisição do Supercomputador Santos Dumont (SSD) em 2015 representou um marco fundamental para a desenvolvimento da computação de alto desempenho no Brasil. No início de 2016, o Santos Dumont iniciou sua operação, sendo disponibilizado à toda comunidade científica do país, que passou a contar com uma alta capacidade de processamento para a solução de problemas complexos que envolvem grande número de cálculos e de manipulação de dados. Com uma capacidade petaflópica (com velocidade de processamento de até 1,1 quatrilhão de operações matemáticas por segundo), o Supercomputador Santos Dumont é a plataforma computacional acadêmica de mais alto desempenho da América Latina.

O LNCC é o nó principal do Sistema Nacional de Processamento de Alto Desempenho (SINAPAD) exercendo também a função de coordenador desse Sistema.

Com a criação do programa de pós-graduação em Modelagem Computacional no ano 2000, o Laboratório passou a contribuir diretamente na formação de pesquisadores com elevado grau de qualificação e perfil interdisciplinar oriundos de diferentes áreas de conhecimento.

Periodicamente são realizados diversos eventos científicos, tais como: Escolas, Seminários e Workshops, além de eventos de divulgação da Ciência à sociedade através da organização de palestras e atividades, entre as quais, “O LNCC de portas abertas”, a Semana Nacional de Ciência e Tecnologia em Petrópolis e várias Visitas Técnicas de estudantes de todos os níveis.

O LNCC atua na promoção da inovação e empreendedorismos através da Incubadora LNCC. Implantou a Fundação de Apoio à Computação Científica (FACC) que hoje apoia projetos de pesquisa em todas as Unidades de Pesquisa do MCTI no Rio de Janeiro, e está vinculado ao Núcleo de Inovação Tecnológica (NIT-Rio) assim como outras Unidades de Pesquisa do MCTIC.

O LNCC coordena o INCT “Ciência dos Dados” e co-coordena o INCT “Medicina Assistida por Computação Científica”.

2.3) Bens e serviços fornecidos a sociedade

O LNCC orienta-se pelas perspectivas da relevância global e do alto valor estratégico da Computação Científica, bem como pelo seu mandato de atuar como um Laboratório Nacional disponibilizando a infraestrutura de computação de alto desempenho para o uso compartilhado com toda a comunidade de pesquisa científica e tecnológica do país. Nessa qualidade, contribui ativamente para o desenvolvimento autônomo do País na área estratégica em que atua.

O LNCC contribui significativamente para o avanço da ciência e da tecnologia, em benefício da sociedade brasileira e do desenvolvimento do país, por meio da realização de pesquisas científicas e desenvolvimentos tecnológicos em Computação Científica e suas aplicações, da formação de novos pesquisadores, da disponibilização e facilitação do uso da sua infraestrutura computacional de alto desempenho para o meio acadêmico e setor empresarial, do incentivo à inovação e da promoção e disseminação da ciência.

A equipe de pesquisadores do LNCC atua na construção de modelos e métodos matemáticos e computacionais para compreender, analisar e resolver problemas científicos e tecnológicos de diversas áreas do conhecimento. Estas pesquisas buscam simular condições, testar hipóteses e prever a evolução de processos e fenômenos.

As pesquisas desenvolvidas no LNCC são relevantes para a validação e o aumento da confiabilidade na análise dos fenômenos. A abrangência das áreas científicas e tecnológicas em que o LNCC atua permite desenvolver aplicações na modelagem computacional de problemas complexos em setores da indústria, comércio, serviços e governos.

Como exemplos da relevância das modelagens matemática e computacional no tratamento de problemas importantes para a sociedade mencionam-se algumas das pesquisas que o LNCC desenvolve atualmente:

i. Sequenciamento genético e análises de bioinformática e biologia computacional de organismos importantes na área da saúde humana, por exemplo: os vírus Zika e Chikungunya; agropecuária e ambiental;

ii. Modelagem do crescimento tumoral;

iii. Modelagem de reservatórios de petróleo na região do pré-sal;

iv. Modelagem do sistema cardiovascular humano para apoio ao diagnóstico, treinamento e planejamento de cirurgias e tratamento médico;

v. Aplicação da ciência de redes na análise de dados massivos em setores como saúde, transporte aéreo, telefonia, entre outras;

vi. Modelagem de sistemas moleculares, entre os quais processos de acoplamento (docking) de ligantes em estruturas de proteínas que permitem a síntese de fármacos;

vii. Desenvolvimento de inovadores algoritmos numéricos e computacionais para as novas gerações de arquiteturas massivamente paralelas com aplicações na área de energia.

viii. Como nó principal e coordenador do Sistema Nacional de Alto Desempenho – SINAPAD – disponibiliza à comunidade científica de todo o país a capacidade petaflópica do Supercomputador Santos Dumont (SSD) e suporta os portais científicos do SINAPAD, dentre os quais o BioInfo e o DockThor desenvolvidos no LNCC.

Em **2019** foram publicados 86 artigos científicos, 6 livros e 16 capítulos de livros, desenvolvidos 112 projetos de pesquisa, incluindo cooperação com 199 entidades parceiras; foram desenvolvidos 199 projetos no supercomputador Santos Dumont. Os 16 portais disponíveis à comunidade científica atenderam a mais de 5.000 usuários em todo o Brasil, em diversas áreas do conhecimento.

Ainda em **2019**, o Programa de Pós-Graduação em Modelagem Computacional do LNCC formou 11 Doutores e 14 Mestres. Das pesquisas realizadas na Pós-Graduação resultaram 73 publicações. Foram desenvolvidos 3 cursos de extensão e aperfeiçoamento, resultando na emissão de 1.342 certificados. Foram promovidos 4 eventos científicos, com a participação de 418 pesquisadores. Ocorreram 16 eventos de popularização da ciência com público de 3.276 pessoas.

Os indicadores do LNCC, referentes ao ano de 2019, estão disponíveis no "**Relatório Anual do Exercício 2019 do Termo de Compromisso de Gestão (TCG-2019)** ". Este relatório pode ser acessado a partir do site da instituição (https://arquivosadm.lncc.br/documentos/transparencia_9508.pdf)

No ano de **2020**, a Plataforma Lattes registrou um total de 239 publicações referentes ao LNCC, distribuídas da seguinte forma: Apresentações de trabalho (19), Artigos aceitos (18), Artigos publicados (91), Capítulos de livro (12), Cursos ministrados (9), Livros publicados (4), Organizações de evento (18), Relatórios de pesquisa (1), Software (2), Textos em jornal/revista (1), Trabalhos em evento (48), e Trabalhos técnicos (16).

Em **2020**, foram desenvolvidos 103 projetos de pesquisa, sendo que 32 deles realizados em parceria formal com instituições estrangeiras. O reconhecimento internacional do LNCC pode ser resumido pela assinatura da cooperação com o INRIA (França) para que o LNCC participe de pesquisas conjuntas, visando ser o representante daquele instituto no Brasil.

Ainda em **2020**, a Infraestrutura de Alto Desempenho (HPC) do LNCC atendeu a 1579 usuários. Estiveram ativos 236 projetos de P&D, destes 86 foram iniciados naquele ano e 17 foram concluídos

Em **2020**, a plataforma computacional teve 13.046 mil horas de CPU utilizadas pelos processos (Jobs) dos usuários, 8% acima da meta de 12.000 mil horas. A Disponibilidade da Plataforma Computacional foi de 0,927, 0,8 % acima da meta de 0,920.

Os indicadores do LNCC referentes ao ano de 2020 estão disponíveis no "Relatório Anual do Exercício 2020 do Termo de Compromisso de Gestão" que pode ser acessado a partir do site da instituição (https://arquivosadm.lncc.br/documentos/transparencia_9732.pdf)

Os **Termos de Compromisso de Gestão (TCG)** do LNCC podem ser obtidos a partir da URL abaixo:

- https://www.gov.br/lncc/pt-br/acesso-a-informacao/institucional/termo-de-compromisso-de-gestao-1

2.4) Estrutura organizacional do LNCC

O Laboratório Nacional de Computação Científica (LNCC) tem sua estrutura organizacional definida pelo seu Regimento Interno publicado na portaria Nº 3.454, de 10 de setembro de 2020, assinada pelo Ministro de Estado da Ciência, Tecnologia e Inovação Substituto (https://www.gov.br/mcti/pt-br/rede-mcti/lncc/acesso-a-informacao/institucional/reg_interno-_lncc2020.pdf/view).

O LNCC é dirigido por um Diretor, cujo cargo é provido pelo Ministro Chefe da Casa Civil da Presidência da República por indicação do Ministro de Estado da Ciência, Tecnologia, Inovações.

O objetivo do corpo diretivo do LNCC é atender aos requisitos de seus clientes, fornecendo os serviços definidos de acordo com os compromissos acordados.

Para atingir estes objetivos foi adotado e implementado o Comitê de Segurança da Informação e Comunicações de acordo com a norma ISO 27001:2013.

O diretor no uso da competência que lhe foi delegada, constituiu vários Comitês e Grupo que lhe fornecem apoio. A seguir temos uma lista dos principais comitê e grupos relacionados a Tecnologia da Informação, Governança e Segurança da Informação:

i. Comitê de Segurança da Informação e Comunicações e de Segurança Física - **CSIC** (Portaria Nº 94/2020/SEI-LNCC de 07 de dezembro de 2020)

ii. Gestão de Segurança da Informação – **IN03**/GSI/PR (Portaria Nº 18/2021/SEI-LNCC de 20 de setembro de 2021)

iii. Gestores de Segurança da informação - **GSI** (Portaria Nº. 122/2019/SEI-LNCC de 05 de dezembro de 2019)

iv. Equipe de Tratamento e Resposta a Incidentes Cibernéticos – **ETIR** (PORTARIA Nº 116/2021/SEI-LNCC de 23 de fevereiro de 2021)

v. Comitê de Gestão de Risco do LNCC – **CGR** (PORTARIA Nº 52/2021/SEI-LNCC de 17 de dezembro de 2021)

vi. Comitê de Governança Digital – **CGD** (PORTARIA Nº 172/2022/SEI-LNCC de 26 de janeiro de 2022)

vii. Comitê Estratégico de Tecnologia da Informação e Comunicação - **CETIC** (Portaria Nº 012/2021/SEI-LNCC de 09 de setembro de 2021)

viii. Conselho de Pesquisa e de Formação de Recursos Humanos - **CPFRH** (PORTARIA Nº 24/2021/SEI-LNCC de 15 de outubro de 2021)

ix. Autoridade designada para realizar o monitoramento Lei de Acesso à Informação **(LAI),** conforme determina o Artigo nº 40 da Lei de Acesso a Informação (Portaria Nº 76/2020/SEI-LNCC de 16 de outubro de 2020)

x. Ponto focal de interlocução do Laboratório Nacional de Computação Científica - LNCC, na implantação da Lei Geral de Proteção de Dados **(LGPD)** do MCTI, conforme determinado no OFÍCIO Nº 141/2021/LNCC - 07 de abril de 2021

xi. Comitê Gestor de Uso dos Recursos da Expansão do Supercomputador Santos Dumont - CGSD-LIBRA (PORTARIA SEI Nº 25, DE 24 DE ABRIL DE 2020)

xii. Comitê Gestor do SDumont - CG-SD (PORTARIA N.º. 010 DE 23 DE FEVEREIRO DE 2016)

A Figura 1: Organograma do LNCC descreve o organograma do Laboratório Nacional de Computação Científica. Este organograma baseia-se no regimento interno que foi aprovado pelo Ministro de Estado da Ciência, Tecnologia e Inovações, via **portaria MCTI Nº 3.454, de 10 de setembro DE 2020** e publicado no Diário Oficial da União em 11 de setembro de 2020.

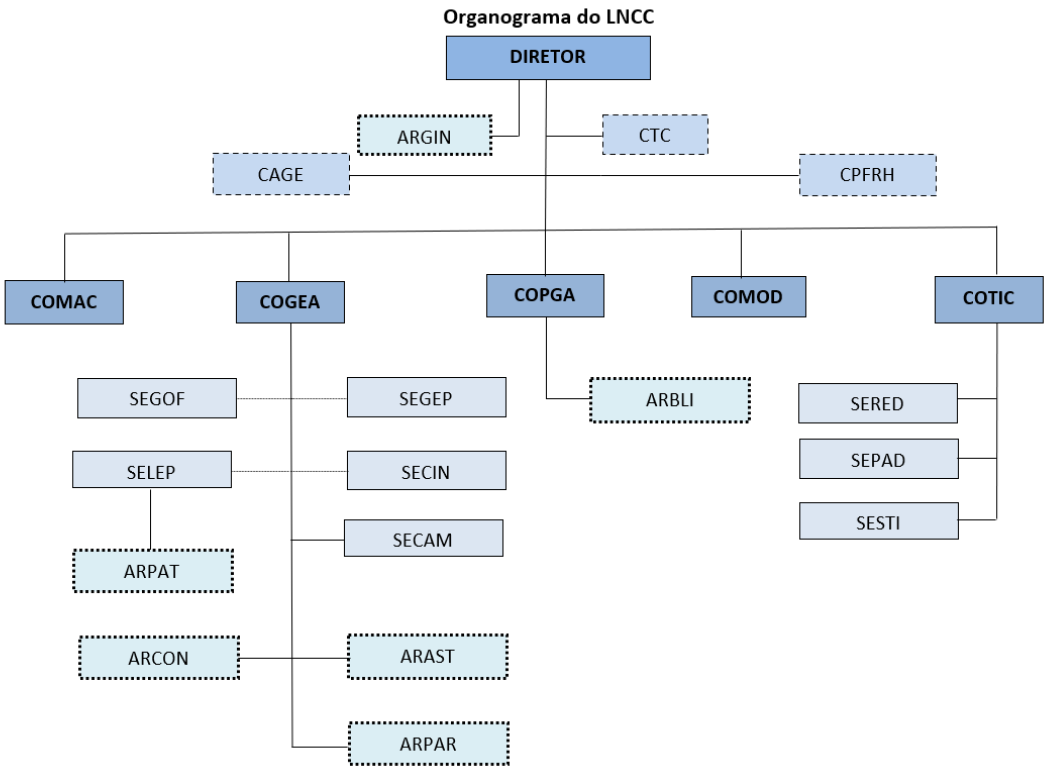


Figura 1: Organograma do LNCC

Das equipes apresentadas na Figura 1: Organograma do LNCC, estão diretamente envolvidos com os processos gerenciais e técnicos do Supercomputador Santos Dumont: (i) o Diretor do LNCC, (ii) os membros do CTC, (iii) os membros do CPFRH, os (iv) membros do CAGE, o Coordenador da COTIC, o Coordenador da COGEA. Além destes estão envolvidos os colabores vinculados aos seguintes serviços/núcleos/áreas: SERED, SEPAD, SESTI, SEGOF, SEGEP, SELEP, SECIN, SECAM.

Conselhos	
CTC	Conselho Técnico Científico
CAGE	Conselho de Atividades de Gestão
CPFRH	Conselho de Pesquisa e de Formação de Recursos Humanos
Coordenações	
COGEA	Coordenação de Gestão e Administração
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
Serviços, Seções e Setores	
SECAM	Seção de Administração do Campus
SECIN	Serviço de Comunicação Institucional
SEGEP	Serviço de Gestão e Desenvolvimento de Pessoas
SEGOF	Serviço de Gestão Orçamentária e Financeira
SELEP	Serviço de Logística e Patrimônio
SEPAD	Serviço de Processamento de Alto Desempenho
SERED	Serviço de Suporte de Sistemas e Redes
SESTI	Setor de Governança de Tecnologia da Informação
Áreas	
ARGIN	Área de Gestão da Inovação (PO LNCC nº 87/2020)
ARPAR	Área de Protocolo e Arquivo (PO LNCC nº 088/2020)
ARCON	Área de Contratos e Convênios (PO LNCC nº 89/2020)
ARAST	Área de Assessoria Técnica (PO LNCC nº 82/2020)
ARPAT	Área de Patrimônio (PO LNCC nº 90/2020)
ARBLI	Área de Biblioteca (PO LNCC nº 86/2020)

3) Segurança do LNCC

O objetivo do SGSI é proteger os ativos do LNCC e de seus parceiros, contra as ameaças: internas ou externas, deliberadas ou acidentais.

O escopo da certificação ISO 27001 é o Supercomputador Santos Dumont e apenas a infraestrutura do LNCC a ele vinculada.

3.1) Alocação de Recursos

A adequação dos recursos necessários é revisada através da reunião anual com a alta gestão, baseado nos recursos da União disponibilizado para o LNCC. Cabe a alta gestão definir como estes recursos serão destinados.

3.2) Competências

As competências necessárias para trabalhar no Laboratório Nacional de Computação Científica (LNCC), Unidade de Pesquisa do Ministério da Ciência, Tecnologia e Inovação (MCTI),

são publicadas nos editais de Concursos Públicos de Provas e Títulos. As informações de pré-requisitos e competências são publicadas no Diário Oficial da União (DOU), são demonstrados conhecimentos teóricos e metodológicos sólidos nas áreas requisitadas através do edital.

No caso de recursos terceirizados, os pré-requisitos e competências são especificados no termo de referência dos editais de licitação pública, os quais são demonstrados por meio de provas de títulos e comprovação de experiência. O gestor do contrato, que é um servidor com atribuições gerenciais, é designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual.

3.3) Modelo de gestão de segurança da informação

O modelo de Gestão da Segurança da Informação do LNCC baseia-se na norma ISO/IEC 27001 e distribui-se na atuação dos seguintes grupos:

i. **Comitê de Segurança da Informação e Comunicações e de Segurança Física – CSIC:** compete ao comitê em âmbito de atuação: (i) assessorar a direção do LNCC na implementação das ações de segurança da informação; (ii) garantir que a governança corporativa seja tratada de forma adequada, com a finalidade de estabelecer políticas e diretrizes estratégicas de segurança em tecnologia da informação e comunicações; (iii) realizar a comunicação das ações de segurança da informação ao campus do LNCC. As atribuições deste comitê são indicadas na política de segurança e complementadas na portaria de nomeação.

ii. **Gestor de segurança da informação:** de atribuições que são indicadas na política de segurança e complementadas na portaria de nomeação, destacam-se: (i) promover cultura de segurança da informação e comunicações; (ii) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança; (iii) propor recursos necessários às ações de segurança da informação e comunicações; (iv) realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações; (v) manter contato com o Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSI) para o trato de assuntos relativos à segurança da informação e comunicações; propor diretrizes relativas à segurança da informação e comunicações.

iii. **Comitê de Governança Digital - CGD:** órgão colegiado de natureza deliberativa e de caráter permanente, de cunho estratégico e executivo, para deliberar sobre assuntos relativos à Governança Digital e às ações, aos programas, às políticas e aos projetos de Tecnologia da Informação e Comunicação – TIC. Das atribuições indicadas em sua na portaria, compete ao CGD deliberar sobre princípios, políticas, diretrizes, normas de governança e objetivos e estratégias relacionados a transformação digital, governança de TIC, segurança da informação, proteção e privacidade de dados pessoais e governança de dados, no âmbito do LNCC.

iv. **Comitê de Gestão de Risco – CGR:** conforme seu regimento interno, compete ao comitê: (i) promover práticas e princípios de conduta e padrões de comportamentos; (ii) institucionalizar estruturas adequadas de governança, gestão de riscos e controles internos; (iii) promover o desenvolvimento contínuo dos agentes públicos e incentivar

a adoção de boas práticas de governança, de gestão de riscos e de controles internos; (iv) garantir a aderência às regulamentações, leis, códigos, normas e padrões, com vistas à condução das políticas e à prestação de serviços de interesse público; (v) aprovar política, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos e dos controles internos;

v. **Comitê Estratégico de Tecnologia da Informação e Comunicação - CETIC**: dentre as competências definidas em sua portaria destacam-se: (i) elaborar o Plano Diretor de Tecnologia da Informação e Comunicações PDTIC na definição da estratégia das Políticas e Diretrizes de TIC no âmbito do LNCC; (ii) elaborar e propor o Plano de Ações e Investimentos em TIC para o LNCC e acompanhar os valores definidos no orçamento; (iii) definir prioridades de execução de projetos de TIC, segundo estratégias previamente formuladas, considerando-se as demandas apresentadas pelas coordenações e pelas assessorias que compõem a estrutura do LNCC; (iv) propor programa orçamentário específico para as ações de segurança da informação e comunicações

vi. **Conselho de Pesquisa e de Formação de Recursos Humanos - CPFRH**: é o órgão colegiado com função de assessoramento ao Diretor do Laboratório Nacional de Computação Científica no planejamento e avaliação das atividades pesquisa, desenvolvimento, inovação e formação de recursos humanos em nível de pós-graduação e aperfeiçoamento técnico-científico. Dentre as competências deste comitê destacam-se: (i) propor políticas e diretrizes, acompanhar e avaliar a implementação, para todas as atividades de formação de recursos humanos no âmbito do Laboratório; (ii) assessorar o Diretor na definição de perfis profissionais a serem recrutados no programa de formação de recursos humanos do Laboratório;

vii. **Conselho Técnico-Científico – CTC:** órgão colegiado com função de orientação e assessoramento ao diretor no planejamento das atividades científicas e tecnológicas do Laboratório Nacional de Computação Científica, cuja competência é definida no regimento do interno da instituição

viii. **Conselho de Atividades de Gestão – CAGE:** órgão colegiado com função de assessoramento ao Diretor do Laboratório Nacional de Computação Científica no planejamento e avaliação das atividades administrativas e de infraestrutura, cuja competência é definida no regimento do interno da instituição.

ix. **Coordenação de Tecnologia da Informação e Comunicação – COTIC**: dentre as competências desta coordenação destacam-se: (i) coordenar as atividades de gestão das plataformas computacionais, de rede de dados interna e externa, de segurança; (ii) coordenar as atividades que englobam a computação de alto desempenho e a governança de tecnologia da informação; (iii) orientar ou colaborar na elaboração da documentação dos processos; e (iv) gerenciar o sistema de segurança da informação para a proteção de dados.

x. **Equipe de Tratamento e Resposta a Incidentes Cibernéticos – ETIR**: tem por objetivo agir proativamente, receber, analisar, monitorar, coordenar e propor respostas a notificações. e atividades relacionadas a incidentes de segurança da informação no âmbito da Política de Segurança da Informação do LNCC, garantindo o direito à

privacidade.

xi. **Serviço de Suporte de Sistemas e Rede – SERED:** serviço vinculado à Coordenação de Tecnologia da Informação e Comunicação; dentre as competências deste serviço destacam-se: (i) elaborar e executar projetos relacionadas com o estudo, levantamento, implantação, modernização, avaliação de produtos e serviços, aquisição, expansão, remanejamento, segurança e utilização dos recursos computacionais e de alto desempenho e redes de dados interna e externa; (ii) propor a adoção de normas, padrões e procedimentos para o uso eficiente e seguro dos recursos computacionais disponíveis, incluindo as interconexões de rede; (iii) planejar, implementar e supervisionar os meios de comunicação de dados e sistemas computacionais, avaliando o desempenho e a correta utilização desses recursos; (iv) executar o monitoramento proativo, a detecção, a correção das vulnerabilidades e o tratamento dos incidentes de segurança nos sistemas computacionais do Laboratório.

xii. **Setor de Governança de Tecnologia da Informação – SESTI:** vinculado à Coordenação de Tecnologia da Informação e Comunicação; dentre as competências deste setor destacam-se: (i) estimular a aplicação das melhores práticas da governança de tecnologia da informação; (ii) executar as atividades de gerenciamento e monitoramento de contratações de soluções de tecnologia da informação; (iii) propor a padronização de normas, processos e políticas de tecnologia da informação;

xiii. **Serviço de Processamento de Alto Desempenho – SEPAD:** vinculado à Coordenação de Tecnologia da Informação e Comunicação, dentre as competências deste serviço destacam-se: (i) prover apoio computacional aos usuários da plataforma computacional de Processamento de Alto Desempenho – PAD; (ii) monitorar o uso dos recursos computacionais de PAD; (iii) gerenciar o Centro de Processamento de Alto Desempenho do Rio de Janeiro – CENAPAD.

xiv. **Coordenação de Gestão e Administração – COGEA:** dentre as competências desta coordenação destacam-se: (i) planejar e coordenar a execução das atividades relativas aos Sistemas de Serviços Gerais, de Administração Financeira, de Contabilidade Federal e de Pessoal Civil, no âmbito de sua competência; (ii) coordenar a execução das atividades e serviços relativos às áreas de gestão de pessoas, contabilidade, orçamento, finanças, patrimônio, almoxarifado, aquisição de bens e contratação de serviços, gestão de contratos e convênios, importação, documentação, protocolo, arquivo e comunicação institucional; (iii) coordenar o planejamento estratégico e a elaboração de planos de implementação; (iv) coordenar as atividades de comunicação institucional, informação e divulgação científica alinhadas às Políticas Institucionais, Ouvidoria e Serviço de Informação ao Cidadão - e-SIC

xv. **Serviço de Gestão Orçamentária e Financeira – SEGOF:** vinculado à Coordenação de Gestão e Administração, dentre as competências deste serviço destacam-se: (i) elaborar proposta orçamentária anual e reformulá-la, quando necessário; (ii) executar os trâmites relativos às operações orçamentária e financeira; (iii) manter atualizados os procedimentos referentes à administração orçamentária, financeira e contábil, observando o cumprimento da legislação;

xvi. **Serviço de Gestão e Desenvolvimento de Pessoas – SEGEP**: vinculado à Coordenação

de Gestão e Administração, dentre as competências deste serviço destacam-se: (i) participar da definição de políticas, diretrizes e metas, no âmbito de sua competência; (ii) preparar atos relacionados a ingresso, provimento, exercício e afastamentos, temporário ou definitivo, vacância de cargos e funções, aposentadorias e pensões; (iii) realizar os atos de lotação e movimentação interna dos servidores; (iv) identificar necessidades de treinamento, planejar e viabilizar a realização e ou participação em cursos, encontros, palestras, seminários e similares para a capacitação e ao desenvolvimento de recursos humanos; (v)

xvii. **Serviço de Logística e Patrimônio – SELEP:** vinculado à Coordenação de Gestão e Administração, dentre as competências deste serviço destacam-se: (i) definir diretrizes e planejar o processo de aquisição de bens e serviços; (ii) orientar e apoiar as unidades requisitantes na elaboração dos documentos editalícios, tais como Termos de Referência, mapa de riscos e minutas de editais de licitação; (iii) providenciar a publicidade dos atos relativos à licitação; (iv) prestar apoio às comissões de licitação subsidiando, quando necessário, na elaboração dos Editais de licitação; (v) gerenciar informações sobre as aquisições de bens e contratações de serviços realizados pelo Laboratório; (vi) efetuar o tombamento, classificação, registro de bens móveis e a movimentação e saída de material permanente mediante atualização dos relatórios de carga e termos de responsabilidade; (vi) gerenciar os processos de alienação, desfazimento e baixa de materiais de consumo e bens móveis; (vii) supervisionar os trabalhos relativos ao levantamento e atualização do inventário patrimonial dos bens móveis e imóveis.

xviii. **Serviço de Comunicação Institucional – SECIN**: vinculado à Coordenação de Gestão e Administração, dentre as competências deste serviço destacam-se: (i) desenvolver atividades de assessoria de imprensa; (ii) elaborar matérias de comunicação institucional, (iii) planejar e gerenciar os perfis institucionais nas mídias sociais; (iv) coordenar e implementar estratégias de comunicação institucional, para o público externo e interno; (v) coordenar a edição de conteúdo do sítio do Laboratório; (vi) organizar e desenvolver ações de comunicação interna; (vii) elaborar, orientar e acompanhar a produção de material promocional institucional; (viii) propor campanhas institucionais, programas de integração, de responsabilidade social, ambiental, cultural; (ix) planejar e gerenciar a utilização dos recursos institucionais destinados à comunicação.

xix. **Seção de Administração do Campus – SECAM**: vinculado à Coordenação de Gestão e Administração, dentre as competências desta seção destacam-se: (i) supervisionar a execução de obras civis, vigilância, transportes, manutenção de veículos e recepção atuando, quando necessário, junto aos prepostos dos contratos, seus fiscais e gestores; (ii) planejar e acompanhar o almoxarifado quanto ao suprimento, registro, armazenamento, distribuição e controle dos materiais de uso comum destinados ao atendimento das necessidades de consumo dos usuários internos; (iii) controlar a demanda de energia elétrica, de água e de outros insumos.

xx. Autoridade de monitoramento da Lei de Acesso a Informação - LAI: conforme o Artigo nº 40 da Lei de Acesso à Informação, cabe a autoridade de monitoramento exercer as seguintes funções: (i) assegurar o cumprimento das normas relativas ao acesso à

informação; (ii) monitorar a implementação do disposto nesta Lei; (iii) recomendar as medidas indispensáveis à implementação e ao aperfeiçoamento das normas e procedimentos necessários ao correto cumprimento do disposto nesta Lei e (iv) orientar as respectivas unidades no que se refere ao cumprimento do disposto nesta Lei e seus regulamentos

xxi. **Ponto focal de interlocução do Laboratório Nacional de Computação Científica (LNCC), na implantação da Lei Geral de Proteção de Dados (LGPD) do MCTI**: conforme § 2º do Art. 1º da Instrução Normativa SGD/ME Nº 117, DE 19 DE NOVEMBRO DE 2020, caberá aos órgãos que compõem o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, no âmbito de suas competências: (i) adequar políticas e diretrizes de Tecnologia da Informação; (ii) adaptar os sistemas, serviços e a infraestrutura de Tecnologia da Informação; e (iii) prestar informações e suporte técnico ao Encarregado pelo Tratamento dos Dados Pessoais.

xxii. **Comitê Gestor de Uso dos Recursos da Expansão do Supercomputador Santos Dumont - CGSD-LIBRA** - dentre as atribuições deste comitê destacam-se: (i) avaliar as demandas de uso da parcela preferencial assim como pedidos de alteração nos quantitativos já aprovados de projetos em curso, estabelecendo o volume de recursos a serem alocados e, se necessário, as prioridades relativas ao atendimento dos projetos submetidos; (ii) emitir recomendações ao LNCC quanto à admissão, alteração ou extinção de projetos; (iii) fazer recomendações ao LNCC em aspectos relativos à política de uso; (iv) 7. avaliar as atividades de manutenção não emergencial no ambiente do Santos Dumont quanto ao risco de indisponibilidade do ambiente e impacto nos trabalhos em execução ou em planejamento.

xxiii. **Comitê Gestor do SDumont - CG-SD** - dentre as atribuições deste comitê destacam-se: (i) avaliar as demandas de uso dos recursos computacionais do supercomputador Santos Dumont (SDumont); (ii) submeter ao CATC-SD projetos de P&D&I que demandam o uso do SDumont para análise de mérito e recomendações; (iii) emitir recomendações ao LNCC quanto à admissão, alteração ou extinção de projetos; (iv) avaliar as políticas de uso do SDumont e propor ao LNCC mudanças que julgue apropriadas.

xxiv. **Comitê Assessor Técnico-Científico do Supercomputador Santos Dumont (CATC-SD) - SD** - dentre as atribuições deste comitê destacam-se: (i) analisar projetos de pesquisa e desenvolvimento submetidos ao CGSD; (ii) fazer recomendações ao LNCC e ao CGSD em aspectos relativos à política de uso e à otimização do desempenho do sistema e atendimento de demandas;

Tendo como base os **documentos governamentais, a legislação vigente, a norma ISO/IEC 27001 e na estrutura interna da instituição**, o **Comitê de Segurança da Informação** e o **Gestor de Segurança da Informação** devem propor as normas relativas à segurança da informação e comunicações do LNCC.

3.4) Gerenciamento de Ativos.

O LNCC protegerá seus ativos, físicos e intelectuais (pessoas, informações, incluindo dados pessoais, sites, materiais, propriedade intelectual) de acordo com leis, contratos,

regulamentos internos, regulamentos externos e sua avaliação de riscos.

Dentro do escopo da certificação da ISO 27001, estão todos os ativos do Supercomputador Santos Dumont classificados de acordo com as seguintes categorias de ativos:

- Hardware (equipamentos e servidores, estações de trabalho ou redes);
- Software (software de servidores, estações de trabalho ou redes);
- Informações.

3.5) Política da segurança da informação

A Política de Segurança da Informação é uma declaração formal do 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/LNCC. Ela está definida no documento 03-PSISD (Política de Segurança da Informação LNCC – SANTOS DUMONT). No âmbito interno, esta política pode ser facilmente ser acessada no site https://sec.lncc.br/site.

Esta Política de Segurança da Informação foi elaborada pelo LNCC, com base na norma técnica ABNT NBR ISO/IEC 27001:2013, de acordo com a legislação vigente, realidade e requisitos de negócio das entidades.

> "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."

3.6) ABNT NBR ISO/IEC 27002:2013

Este sistema de gestão e seus processos, para assegurar os aspectos de segurança da informação, é baseado na Norma ISO/IEC 27001:2013 ("Information Technology - Security Techniques - Information Security Management Systems - Requirements"),

Este sistema de gestão prevê 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.

3.7) Conscientização em Segurança da Informação

Todos os colaboradores devem participar dos treinamentos de conscientização da segurança da informação e procedimentos organizacionais relacionados à Segurança da Informação. Os treinamentos serão realizados de uma das seguintes formas: (i) presencial ou (ii) à distância utilizando o ambiente virtual de aprendizagem do LNCC ou no formato de webinar.

Os colaboradores que não puderem estar presentes no dia dos treinamentos presenciais deverão realizá-los utilizando uma das plataformas disponibilizada.

É necessário conscientizar todos os colaboradores para conhecer e entender o que são:

1. Sistema de Gestão Segurança;
2. Comitê de Segurança da Informação e Comunicação;
3. Política de Segurança da Informação e Comunicação;
4. Como todos os colaboradores podem contribuir.

Em caso de não execução do treinamento da segurança da informação o "Agente Público" estará sujeito as sanções descritas na LEI Nº 8.027, DE 12 DE ABRIL DE 1990, código de ética do servidor público.

3.8) Informação documentada

Toda a documentação relevante ao SGSI está armazenada e disponibilizada no repositório **https://sec.lncc.br/cotic/**, exclusivamente para uso interno dos usuários da rede do LNCC. Nele podem ser consultados modelos, procedimentos e todo o material utilizado nas auditorias interna e externa. Todos os documentos controlados podem ser encontrados na pasta denominada "**Lista de Documentos**".

Os documentos do sistema de gestão são controlados através da planilha denominada "**01-LDC - Lista de Documentos Controlados**" e serão referenciados como "documentos controlados". A lista de documentos é controlada através de uma planilha do Excel, criada com a finalidade de controlar exclusivamente os relatórios, políticas e outros documentos gerados no escopo do SGSI.

O documento que descreve em detalhes a documentação do SGSI é denominado "**Procedimento para Gestão Documental e Classificação da Informação**", cujo Controle Interno é "**39-PGDCI**".

Todos os documentos classificados como públicos são também disponibilizados no site https://sec.lncc.br e no site da instituição (http://www.lncc.br).

O SGSI também utiliza o SEI-MCTI (Sistema Eletrônico de Informações), que é o sistema oficial para os documentos governamentais. O acesso a este sistema pode ser controlado conforme necessário. O uso do SEI é justificado principalmente por permitir a assinatura eletrônica dos documentos. Desta forma, além de facilitar o acesso aos documentos controlados não há a necessidade do servidor se deslocar até o LNCC para assinar os documentos toda vez que houver uma alteração e exigência de assinatura.

Os procedimentos técnicos relacionados a TI serão armazenados em sistema de documentação próprio e devem estar disponíveis no site: https://csrdoc2.sre.lncc.br/

Os documentos do SGSI devem ser revisados e atualizados periodicamente, de acordo com desenvolvimentos regulatórios, necessidades do mercado e melhores práticas. Todos os documentos controlados devem estar disponíveis no SEI-MCTI.

3.9) Auditoria interna

A auditoria interna poderá ser executada através de recursos internos do LNCC ou através de empresas terceirizada, a contratada deve garantir a aderência à estrutura de controle da ISO/IEC 27001:2013. As regras aplicáveis aos padrões ISO são descritas no documento que será elaborado pela empresa de auditoria contratada.

A auditoria interna deve ser realizada ao menos uma vez por ano, conforme descrito no documento **19-PA - Procedimento de Auditoria**.

4) Partes Interessadas

O LNCC está comprometido em estabelecer, manter e melhorar um sistema de gerenciamento alinhado com a norma ISO/IEC 27001:2013, estabelecendo uma governança forte com capacitação, definição, atribuições claras de papéis das pessoas envolvidas no processo.

O LNCC analisa as necessidades e expectativas de suas partes interessadas e o ambiente em que opera. Os resultados dessa análise e os desafios associados ajudam a moldar sua estratégia e a implementação específica do Sistema de Gestão da Segurança da Informação, determinando assim a maneira como o LNCC/Supercomputador Santos Dumont gerencia o seu sistema de gestão.

4.1) Partes Interessadas Internas

Partes Interessadas	Principais Interesses
Diretoria	LNCC executando a estratégia acordada.
Colaboradores do LNCC	Local de trabalho seguro, recompensa proporcional, emprego interessante, carreira e oportunidades.

4.2) Partes Interessadas Externas

Partes Interessadas	Principais Interesses
Comunidade Cientifica	Suporte a projetos de pesquisa científica e de inovação tecnológica para o avanço do conhecimento e o atendimento às demandas da sociedade.
Escolas e Universidades	Oportunidades de treinamento; estagiários e proposta de emprego; atratividade.
Autoridades Locais e Governamentais	Conformidade com a legislação local e internacional ou requisitos regulamentares. Contribuir com a comunidade cientifica, pesquisas e parcerias.
Auditores Externos	Transparência e qualidade da informação para permitir uma boa opinião.
Mídia, Mercado Financeiro	Mensagens claras, disponibilidade e informações confiáveis.
Fomentador	Fornece recursos para desenvolvimento de projetos em parceria com o LNCC.
Parceiros	Relações confiáveis e mutuamente benéficas.
Auditoria Externa	Transparência e qualidade das informações.

4.3) Requerimentos de negócios de acordo com as políticas e leis

O Sistema de Gestão de Segurança da Informação do LNCC/Supercomputador Santos Dumont visa atender aos seguintes requisitos de negócios:

- **Diretoria:** Gerenciar e executar a estratégia;

- **Colaboradores LNCC:** Local de trabalho seguro, recompensa proporcional, trabalho interessante, carreira e oportunidades;
- **Comunidade Cientifica:** Suporte a projetos de pesquisa científica e de inovação tecnológica;
- **Escolas e Universidades:** Oportunidades de treinamentos; estagiários e proposta de trabalho; atratividade;
- **Autoridades Legais:** Conformidade com a legislação ou com os requisitos regulamentares;
- **Autoridades Locais e Governamentais:** Conformidade com a legislação local e internacional ou com os requisitos regulamentares; Conformidade com programas públicos de P&D; Contribuição para o crescimento econômico nacional;
- **Auditoria Externa:** Transparência e qualidade das informações para permitir uma opinião sólida;
- **Mídia, Mercado Financeiro:** Mensagens claras, informações disponíveis e confiáveis. Comunicação sustentável canais;
- **Fomentador:** Fornecer recurso para desenvolvimento de projetos;
- **Parceiros:** Relações confiáveis e mutuamente benéficas.

5) Projetos

No escopo sistema de gestão de segurança do LNCC/SSD, são mantidos projetos com os seguintes parceiros:

- **Grupo Atos**: A Atos é líder global em transformação digital, com 120.000 funcionários em 73 países e receita anual de € 13 bilhões. Número um na Europa em nuvem, segurança cibernética e computação de alto desempenho, o Grupo fornece soluções híbridas de nuvem híbrida orquestrada, *big data*, aplicativos de negócios e ambiente de trabalho digital de ponta a ponta através de sua *Digital Transformation Factory*, além de serviços transacionais através da *Worldline*, *European* líder no setor de pagamentos.
- **Petrobrás**: Presente em 19 países dos continentes, administrando a exploração de óleo e gás destas áreas. Através de *joint ventures* e demais parcerias, nossas unidades incorporam o mais avançado em tecnologia, mantendo-se referência mundial no setor energético. Empresa integrada de energia, com foco em óleo e gás, que evolui com a sociedade, gera alto valor e tem capacidade técnica única.
- **Comunidade Cientifica**: Os parceiros da comunidade científica são apresentados conforme demanda dos projetos em andamento e estão declarados na página "Projetos em andamento": (https://sdumont.lncc.br/projects_view.php?pg=projects&status=ongoing),

6) Planejamento de ações para endereçar riscos e oportunidades

O objetivo de gestão de riscos da Segurança de Informação do LNCC é identificar os

principais riscos aos macroprocessos do LNCC. A análise de riscos é controlada e executada com o apoio do pelo Gestor da Segurança da Informação e está documentada através da planilha Matriz de riscos, apresentada no documento **37-MAR - Metodologia da Avaliação de Risco**.

Os riscos e oportunidades são avaliados regularmente. No processo de análise de riscos, o LNCC realiza a avaliação baseada em metodologia própria. Os impactos potenciais, são mapeados, definidos, endereçados e planejados para tratar e minimizar os riscos.

As auditorias são conduzidas anualmente para avaliar o status dos controles internos, conforme descrito no documento **19-PA - Procedimento de Auditoria.**

O Gerenciamento de Riscos é garantido pela Matriz de Riscos, descrevendo os riscos por categoria, frequência, vulnerabilidade etc. Disponível no documento **04-RA - Análise de Risco - Risk Assessment.**

A Análise de Impacto do Negócio (BIA) é realizada para avaliar os riscos e os impacto no negócio. E o resultado da última reunião do BIA está disponível no documento **07-BIA - Relatório da Reunião – BIA.**

O planejamento de controles operacionais e o tratamento dos riscos está descrito no documento **25-PPAR - Planilha dos Planos de Ação e Riscos**. As ações e as tratativas dos riscos são descritas na aba “ações”. Neste documento são gerenciados todos os planejamentos operacionais referentes ao sistema de gestão da segurança e objetivos.

7) Objetivos da segurança da informação

A gestão de segurança da informação e comunicações baseia-se no processo de melhoria contínua, denominado ciclo **PDCA** (Plan-Do-Check-Act), referenciado pela norma ABNT NBR ISO/IEC 27001:2013. Estes processos estão diretamente ligados à política de segurança da informação do LNCC-Supercomputador Santos Dumont (SSD).

No escopo deste sistema de gestão, os objetivos a serem alcançados, são definidos no documento **24-PAIO - Planilha de Avaliação da Importância dos Objetivos do LNCC - Santos Dumont**.

O nível de importância dos objetivos é definido baseado nos valores obtidos a partir da análise de risco.

7.1) Planejamento para o alcance dos objetivos

Todos os anos são definidos planos de ação para garantir uma melhoria contínua na gestão de segurança da informação.

No ano de **2019** foram realizadas as seguintes ações:

- Constituir o Comitê da segurança da Informação e Comunicações e de Segurança Física;
- Adequação física do perímetro de segurança do Santos Dumont;
- Revisão da política de segurança do LNCC;
- Definição de papéis e responsabilidades para o sistema de gestão da segurança da

informação através da portaria 122/2019/SEI-LNCC de dezembro de 2019;

- Campanha de divulgação e conscientização da segurança da informação;
- Implementação de controles de segurança nos Racks que possuem os ativos de segurança do Santos Dumont no CPD.

No ano de **2020** foram realizadas as seguintes ações:

- Foi planejada e contratada uma consultoria externa para atender todos os requisitos e certificação da ISO/IEC 27001:2013
- Executada uma auditoria externa de certificação da ISSO/IEC 27001:2013;
- Adequação do Comitê de Segurança a Instrução Normativa GSI Nº 1 de 27 de maio de 2020 e a Instrução Normativa GSI Nº 2 - 24 de julho de 2020.
- Finalizou-se o processo de elaboração do edital de contratação da obra de adequação do LNCC.

No ano de **2021**, foram realizadas as seguintes ações

- Foi emitida uma portaria atualizando e reestruturando a equipe de tratamento de incidentes de acordo com as normativas do Departamento de Segurança da Informação;
- Disponibilização do Treinamento de Conscientização em Segurança da Informação no ambiente virtual de aprendizagem (AVA) do LNCC, este treinamento passou a contar com um Quizz ao final de cada seção;
- Disponibilização de um novo treinamento de Fundamentos em Segurança da Informação que será oferecido aos Colaboradores que não possuem nenhum conhecimento em segurança da informação;
- Em março de 2021 ocorreu a auditoria interna da ISO/IEC 27001;

Para o ano de 2021, foi planejada e contratada uma consultoria externa para atender todos os requisitos e certificação da ISO/IEC 27001:2013.

8) Indicadores – monitoramento, desempenho e avaliação

Esta seção descreve os indicadores utilizados no monitoramento deste sistema de gestão.

8.1) Indicadores do Termo de Compromisso de Gestão (TCG)

O Termo de Compromisso de Gestão (TCG) e o seu relatório anual, descrevem e reportam os valores apurados dos Indicadores de Gestão do Laboratório Nacional de Computação Científica para o cumprimento das metas anuais e destina-se à avaliação pela sociedade e pelo MCTI.

As metas do TCG são recomendadas pelo Conselho de Pesquisa e de Formação de Recursos Humanos (CPFRH) do LNCC, posteriormente são submetidas ao MCTI, podendo haver reorientação pela Subsecretaria de Unidades Vinculadas (SUV/MCTI), neste caso elas são revisadas, as revisões são aprovadas pelo CPFRH, finalmente o TCG segue para aprovação

pelo Ministro do MCTI e ocorre a sua publicação.

O Plano Diretor da Unidade (PDU), que orienta o TCG, foi desenvolvido sob orientação do MCTI para o período de 2018-2022, apresentando descrição de missão, visão, valores e princípios da instituição.

Neste sistema de gestão, adotamos os indicadores da Infraestrutura de Alto Desempenho (HPC) indicados abaixo:

- **Indicador 6: UPC** - Utilização da Plataforma Computacional
- **Indicador 7: DiPC** - Disponibilidade da Plataforma Computacional
- **Indicador 8: IO** - Índice de Ocupação
- **Indicador 9: NPAe** -Número de projetos de PAD (HPC)
- **Indicador 10: SADC** – Software Aplicações Disponibilizadas a Comunidade

8.1.1) Indicador 6: UPC - Utilização da Plataforma Computacional

A fórmula de cálculo do indicador foi modificada para 2019, considerando o tempo de uso das CPUs, de forma a adequar o indicador ao novo indicador IO. Neste caso, o tempo de CPU leva em conta o número de processadores de cada equipamento.

Este indicador é influenciado diretamente pelo número de projetos, cada um deles com demandas diferentes sobre a capacidade da plataforma de computação de alto desempenho.

Objetivo: medir a ocupação da capacidade física da plataforma computacional de alto desempenho do LNCC por projetos de pesquisa, desenvolvimento e inovação por todos os usuários do Supercomputador Santos Dumont e da infraestrutura de computação de alto desempenho, externos e internos.

Fórmula: UPC = número de horas de CPU utilizadas pelos processos (Jobs) dos usuários.

Unidade: milhares de horas.

8.1.2) Indicador 7 - DiPC - Disponibilidade da Plataforma Computacional

Este indicador avalia o impacto das atividades de manutenção e desenvolvimento do sistema de processamento de dados em termos de hardware – incluindo facilities – e software.

Objetivo: medir a eficiência dos serviços de apoio computação e de manutenção aplicados na plataforma computacional de alto desempenho.

Fórmula: DiPC = NHD / NHP

Unidade: número decimal com três casas.

Sendo:

NHD = Número de horas realmente disponíveis da plataforma computacional.

Unidade: milhares de horas.

NHP = Número de horas de disponibilidade prevista da plataforma computacional.

Fórmula: Número de processadores dos equipamentos X 8640 horas anuais.

Unidade: milhares de horas.

8.1.3) Indicador 8 - IO - Índice de Ocupação

Indicador novo, substituindo o indicador anterior denominado NUA, para alcançar maior precisão na avaliação do uso da capacidade de processamento de alto desempenho.

O supercomputador possui 1.528 CPU e, portanto, o número total de horas de CPU provisionais é de 1.528 cpu x 8.760 h/ano = 13.385.280 cpu x h/ano e uma CPU é utilizada em determinado momento se estiver efetivamente sendo utilizada ou em estado “idle” dentro do processo de job alocado a um usuário.

Objetivo: medir a efetiva utilização da plataforma de computação de alto desempenho.

Fórmula: UPC/número total de horas de CPU provisionadas pelo supercomputador, descontadas as horas de manutenção programada.

Unidade: percentual com uma casa decimal.

8.1.4) Indicador 9 - NPAe - Número de projetos utilizando processamento de alto desempenho (HPC)

O indicador contabiliza os projetos selecionados para uso do supercomputador Santos Dumont. Ele inclui projetos que foram executados e aqueles que foram aprovados e foram considerados no planejamento de uso da plataforma, mas podem não ter sido ativados pelos usuários.

Objetivo: medir o alcance do uso da plataforma de processamento de alto desempenho do LNCC.

Fórmula:

NPAe = Número de projetos desenvolvidos na infraestrutura de processamento de alto desempenho do LNCC.

Unidade: número inteiro.

8.1.5) Indicador 10 - SADC - Softwares Aplicativos disponíveis à Comunidade

Objetivo: medir o provimento de serviços computacionais especializados à comunidade científica.

Fórmula:

SADC = Número de sistemas de softwares e portais desenvolvidos e mantidos no LNCC, com um propósito determinado e distinto, e cuja utilização esteja franqueada a comunidade científica e de pesquisa. Engloba tanto softwares novos disponibilizados no ano de avaliação quanto softwares que tenham sido desenvolvidos em anos anteriores e que estejam sendo mantidos em perfeitas condições de funcionamento.

Unidade: número inteiro.

8.2) Indicadores HPC Santos Dumont

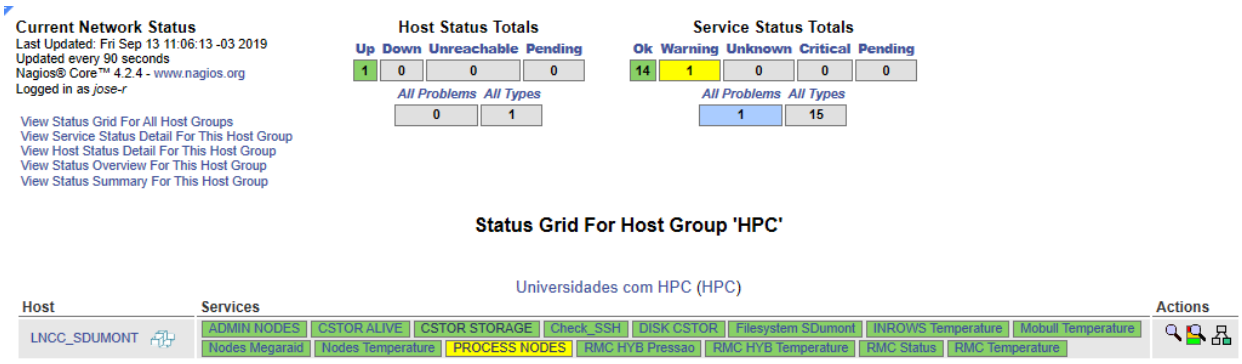
O monitoramento dos indicadores de funcionamento do Supercomputador Santos Dumont é executado pela operação técnica da empresa Atos, com SLA de atendimento 24x7, estes são responsáveis por monitorar o ambiente diariamente, estando ciente de qualquer problema técnico no desempenho dos supercomputadores.

Mensalmente a Atos entrega para o gestor do contrato do LNCC um relatório da gestão dos serviços, com os resultados requeridos contratualmente, onde é feita a análise dos indicadores pelo gestor responsável pelo contrato. Baseado nesta análise são executados os ajustes operacionais no processo de monitoração e os ajustes contratual para a entrega do serviço.

O desempenho da gestão de segurança da informação é medido e monitorado conforme segue:

Eventos de falha de hardware ou software: monitoração 24x7 dos equipamentos via Nagios.

Segue abaixo os itens de hardware e infra que são monitorados pela aplicação Nagios:



Descrição dos Grupos de Serviço:

- **ADMIN NODES**: Monitoração dos nós de administração, up ou down.
- **CSTOR ALIVE**: Monitoração dos appliances de storage, up ou down.
- **CSTOR STORAGE**: Monitoração dos discos dos appliances de storage.

- **Check_SSH**: Monitoração de acesso ao Santos Dumont (sdumont0).
- **DISK CSTOR**: Monitoração dos discos do clustersotor.
- **Filesystem Sdumont**: Monitoração de uso dos filesystems dos nós de administração.
- **Inrow temperature**: Monitoração da temperatura do inrows.
- **Mobull temperarure**: Monitoração da temperatura no interior do Santos Dumont.
- **Nodes megaraid**: Monitoração dos discos internos dos nós de monitoração.
- **Process nodes**: Monitoração da quantidade de nós de processamento disponíveis no cluster.
- **RMC HYB Pressão:** Monitoração da pressão do glicol na HYC.

A imagem abaixo representa um exemplo de histórico de monitoração do serviço PROCESS NODES, sendo considerado *warning* com 95% dos nós de processamento disponível, abaixo de 95% *critical* e acima como OK.

Service State History

PROCESS NODES

LNCC_SDUMONT

Report covers from: **2019-09-01 00:00:00** to **2019-09-13 11:07:29**

Showing 1-18 of 18 total records

Page 1 of 1 | 100 Per Page

Date / Time	Host	Service	State	State Type	Attempt	Information
2019-09-13 10:41:46	LNCC_SDUMONT	PROCESS NODES	WARNING	HARD	5 of 5	WARNING - Porcentagem de servidores disponiveis 95 % (722 up, 36 down)
2019-09-13 04:41:56	LNCC_SDUMONT	PROCESS NODES	CRITICAL	HARD	5 of 5	CRITICAL -Porcentagem de servidores disponiveis 94 % (717 up, 41 down)
2019-09-12 19:51:34	LNCC_SDUMONT	PROCESS NODES	WARNING	HARD	5 of 5	WARNING - Porcentagem de servidores disponiveis 95 % (724 up, 34 down)
2019-09-10 20:36:56	LNCC_SDUMONT	PROCESS NODES	OK	HARD	5 of 5	OK - Porcentagem de servidores disponiveis 96 % (733 up, 25 down)
2019-09-10 19:19:31	LNCC_SDUMONT	PROCESS NODES	WARNING	HARD	5 of 5	WARNING - Porcentagem de servidores disponiveis 95 % (721 up, 37 down)
2019-09-09 03:09:12	LNCC_SDUMONT	PROCESS NODES	OK	HARD	5 of 5	OK - Porcentagem de servidores disponiveis 97 % (737 up, 21 down)
2019-09-09 02:36:09	LNCC_SDUMONT	PROCESS NODES	WARNING	HARD	5 of 5	WARNING - Porcentagem de servidores disponiveis 95 % (726 up, 32 down)
2019-09-06 11:28:50	LNCC_SDUMONT	PROCESS NODES	OK	HARD	5 of 5	OK - Porcentagem de servidores disponiveis 97 % (737 up, 21 down)
2019-09-05 04:23:41	LNCC_SDUMONT	PROCESS NODES	CRITICAL	HARD	5 of 5	CRITICAL -Porcentagem de servidores disponiveis 93 % (705 up, 53 down)
2019-09-05 02:42:23	LNCC_SDUMONT	PROCESS NODES	WARNING	HARD	5 of 5	WARNING - Porcentagem de servidores disponiveis 95 % (726 up, 32 down)
2019-09-04 17:31:17	LNCC_SDUMONT	PROCESS NODES	OK	HARD	5 of 5	OK - Porcentagem de servidores disponiveis 96 % (731 up, 27 down)
2019-09-04 17:12:52	LNCC_SDUMONT	PROCESS NODES	WARNING	HARD	5 of 5	WARNING - Porcentagem de servidores disponiveis 95 % (721 up, 37 down)
2019-09-02 08:45:07	LNCC_SDUMONT	PROCESS NODES	OK	HARD	5 of 5	OK - Porcentagem de servidores disponiveis 97 % (738 up, 20 down)
2019-09-02 08:06:07	LNCC_SDUMONT	PROCESS NODES	WARNING	HARD	5 of 5	WARNING - Porcentagem de servidores disponiveis 95 % (727 up, 31 down)
2019-09-01 22:52:27	LNCC_SDUMONT	PROCESS NODES	OK	HARD	5 of 5	OK - Porcentagem de servidores disponiveis 97 % (736 up, 22 down)
2019-09-01 22:33:53	LNCC_SDUMONT	PROCESS NODES	WARNING	HARD	5 of 5	WARNING - Porcentagem de servidores disponiveis 95 % (723 up, 35 down)
2019-09-01 07:16:36	LNCC_SDUMONT	PROCESS NODES	OK	HARD	5 of 5	OK - Porcentagem de servidores disponiveis 97 % (739 up, 19 down)
2019-09-01 06:21:30	LNCC_SDUMONT	PROCESS NODES	WARNING	HARD	5 of 5	WARNING - Porcentagem de servidores disponiveis 95 % (727 up, 31 down)

8.3) Indicadores expecíficos

Esta seção apresenta os indicadores específicos deste sistema de gestão e que estão diretamente alinhados aos objetivos de segurança da informação.

8.3.1) Indicador de treinamento

Objetivo: Identificar o percentual de colaboradores que já realizam os treinamentos de segurança da informação.

- **Motivador**: Assessment ISO 27001 - Planilha de riscos
- **Periodicidade**: Mensal;

- **Apresentar para**: Comitê de segurança;
- **Data Inicial**: 12/2019

A partir de 2021 utilizamos o AVA (Ambiente Virtual de Aprendizagem) para obter estes indicadores.

8.3.2) Indicador do abastecimento de Diesel

Objetivo: Acompanhar o fornecimento de óleo diesel. A aquisição do combustível utilizado nos grupos geradores de energia do LNCC é realizada sob demanda. Este indicador registra a periodicidade e o volume de combustível adquirido;

- **Origem das informações**: SEI
- **Motivador**: Assessment ISO 27001 – BIA (2018)
- **Periodicidade**: Mensal;
- **Apresentar para**: Comitê de segurança;
- **Data Inicial**: 07/2019

8.3.3) Indicador dos documentos controlados

Objetivo: Acompanhar o processo de atualização dos documentos controlados do SGSI; Identificar a percentagem de documentos que foram atualizados fora do prazo;

- **Motivador**: Melhoria contínua;
- **Periodicidade**: Mensal;
- **Apresentar para**: Comitê de segurança;
- **Data Inicial**: 2019

8.3.4) Indicador da Análise de Risco

Objetivo: Acompanhar o processo de revisão e apresentação dos planos de ação para tratativa dos riscos da informação ao Comitê de Segurança e a Direção; Quantidade de Reuniões realizadas com o comitê de segurança com participação da direção; acompanhar a evolução dos riscos a serem monitorados;

- **Motivador**: Melhoria contínua
- **Periodicidade**: Mensal;
- **Apresentar para**: Comitê de segurança;
- **Data Inicial**: 12/2019

8.3.5) Indicador dos planos de ação

Objetivo: Acompanhar o processo de conclusão dos planos de ação mapeados na Planilha de Planos de Ação;

- **Motivador**: Melhoria contínua;
- **Periodicidade**: Mensal;
- **Apresentar** para: Comitê de segurança;
- **Data Inicial**: 05/2020

Indicadores subordinados:

- Planos de Ação – Status
- Planos de Ação – Grupos / Ativos
- Planos de Ação – Impacto
- Planos de Ação – P/Equipe
- Planos de Ação - % Concluído
- Planos de Ação – Ações p/ Equipe
- Planos de Ação – Ações (Finalizadas X Em Aberto)
- Planos de Ação – Ações (No prazo X Fora do Prazo)
- Planos de Ação – Ações (Pendentes X Atrasadas)
- Novos planos de ação
- Planos de ação revisados

8.3.6) Indicador de Incidentes (RATS)

Objetivo: Acompanhar os eventos de segurança que foram registrados no GLPI e tratados seguindo do procedimento do RATS.

- **Motivador**: Melhoria contínua
- **Periodicidade**: Trimestral;
- **Apresentar para**: Comitê de segurança;
- **Data Inicial**: 05/2020

8.3.7) Indicador das Utilidades (Facilities)

Objetivo: Acompanhar os eventos relacionados as Utilidades (Climatização e Elétrica).

- **Motivador**: Melhoria contínua

- **Periodicidade**: Mensal;
- **Apresentar para**: Comitê de segurança;
- **Data Inicial**: 01/2020

8.3.8) Indicado da Gestão de Capacidade

Objetivo: Facilitar a Gestão de Capacidade do SSD;

- **Motivador**: Gestão de Capacidade do SSD (Supercomputador Santos Dumont)
- **Periodicidade**: Sob demanda do Gestor do SSD;
- **Apresentar para**: do Gestor do SSD e para o Gestor de Segurança
- **Data Inicial**: 05/2021

As informações foram obtidas através de consultas à base de dados do GLPI, consultas à base de dados de accounting do gerenciador de recursos do SDumont (SLURM), consulta aos relatórios de chamados do contrato de manutenção do SDumont (disponíveis no SEI) e através de comandos executados no sistema operacional dos nós de login do SDumont.

Indicadores subordinados:

- Quantidade de Jobs Submetidos
- Relação de chamados solucionados x em aberto
- Tempo médio de solução dos chamados
- Espaço em Disco
- Relação dos chamados atendidos pelo contrato de manutenção
- Alertas das Facilities do SSD

9) Comunicação

As publicações são feitas através de diferentes canais conforme segue:

Assunto	Frequência	Meio de Comunicação	Para quem será comunicado
Comitê de Segurança da Informação	Quando necessário	Portaria interna ou no Repositório do SGSI	Depende da classificação do documento
Gestor de Segurança da Informação	Quando necessário	Portaria interna ou no Repositório do SGSI	Depende da classificação do documento
Política de Segurança da Informação e Comunicação	Quando necessário	Portaria interna	Todos os colaboradores
Portarias Internas	Mensal	Boletim de serviço	Todos os colaboradores
Comunicados em geral	Quando necessário	e-mail interno (lista de distribuição)	Todos os colaboradores

Todas as portarias e documentos controlados, relacionadas ao SGSI do LNCC, deverão ser anexados ao processo **01209.000061/2020-55** no SEI. No sistema do SEI, quando algum arquivo não puder ser assinado, deve-se associar ao mesmo um anexo para coleta de assinatura eletrônica.

Para todos os documentos controlados, que requerem encaminhamento para conhecimento e aprovação deve-se associar ao mesmo um anexo para coleta de assinatura eletrônica evidenciando o conhecimento e outro, quando necessário, para aprovação.

Os documentos referentes as reuniões do Comitê de Segurança das Informação, incluindo suas atas deverão ser anexados ao processo **01209.000086/2021-30** no SEI, cujo acesso é limitado a unidade "**LNCC_CSIC**" da qual fazem parte os membros do Comitê de Segurança de Informação do LNCC. Uma cópia das portarias emitias pelo LNCC e que estejam relacionadas ao Comitê de Segurança da Informação deverão ser disponibilizadas no processo **01209.000085/2021-95** no SEI, cujo acesso também é limitado a unidade "**LNCC_CSIC**".

10) Análise crítica da alta direção - Management review

A revisão gerencial deve ser realizada pela equipe gerencial responsável por cada resultado. Os resultados e objetivos serão analisados de acordo com as metas locais definidas pelo Diretor do LNCC. Esta atividade ocorrerá com periodicidade anual, dentro dos quais serão incluídos os requisitos solicitados pelas normas ISO 27001:2013.

O documento "**26-ACAD - Análise Crítica da Alta Direção**" contém a última análise crítica realizada pela alta direção do LNCC.

11) Melhorias

Esta seção descreve como serão tratadas as não conformidades e as oportunidades de melhoria do SGSI

11.1) Não conformidades e ações corretivas

As não conformidades apontadas na auditoria interna, são endereçadas, planejadas para ação corretiva.

Dentro de seu sistema de gestão existe o **Comitê de Segurança da Informação e Comunicação** - **CSIC**, que em seu âmbito de atuação, compete:

- gestão de riscos de forma sistemática, estruturada e oportuna, subordinada ao interesse público;
- estabelecimento de níveis de exposição a riscos adequados;
- estabelecimento de procedimentos de controle interno proporcionais ao risco, observada a relação custo-benefício, e destinados a agregar valor à organização;
- utilização do mapeamento de riscos para apoio à tomada de decisão e à elaboração do planejamento estratégico;
- utilização da gestão de riscos para apoio à melhoria contínua dos processos organizacionais

1.1. Melhoria contínua

Oportunidades de melhoria devem ser identificadas e implementadas para melhorar a eficiência do sistema de gestão. Os planos de melhoria dizem respeito a todo o sistema.

Os planos de melhoria são implementados para melhorar o sistema local, a maturidade e eficiência.

12) Manutenção do documento

Este documento deve ser revisado ao menos uma vez ao ano.

13) Glossário

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 da instituição
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*
PAD	:	Processamento de Alto Desempenho
SDumont	:	Supercomputador Santos Dumont
SESTI	:	Setor de Governança de Tecnologia da Informação
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

Fábio Borges de Oliveira
Diretor do Laboratório Nacional de Computação Científica

Luís Rodrigo de O. Gonçalves
Gestor de Segurança da Informação

[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

Anexo A – Inclusão e Exclusão

Inclusão

Localização	Endereço	
Rio de Janeiro - Petrópolis	Av. Getúlio Vargas, 333 - Quitandinha, Petrópolis - RJ, 25651-075	Supercomputador Santos Dumont em Prestação de Serviço em Tecnologia e Data Center que incluem *Hosting*, NOC e Suporte de Operação de Segurança na área de Pesquisa e Desenvolvimento.

Exclusão

Localização	Endereço	
Rio de Janeiro - Petrópolis	Av. Getúlio Vargas, 333 - Quitandinha, Petrópolis - RJ, 25651-075	LNCC - Laboratório Nacional de Computação Cientifica