Sistema de Gestão de Segurança da Informação		Laboratório Nacional de Computação Científica / MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES	
CÓDIGO	**VERSÃO**	**TIPO DE ACESSO**	**NÍVEL DE ACESSO**
08-ISMS	6.0	Externo	Público
CONTROLES DA ABNT NBR ISO/IEC 27001:2013		**PUBLICADO EM**	**PAGINAÇÃO**
Seções 4 a 10 da 27001		18/06/2024	1/15

SUMÁRIO

1 OBJETIVO

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).

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."

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

2 CAMPO DE APLICAÇÃO DO SGSI

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

A definição do perímetro, inclusão e exclusões, deste documento é a seguinte:

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

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.

3 RESPONSABILIDADE

A definição do SGSI deve ser elaborada pela direção do LNCC, com o apoio do gestor de segurança da informação.

Esta norma deve ser aprovada e assinada pela direção do LNCC.

A direção e o gestor de segurança da informação serão os responsáveis por aprovar o escopo de certificação e sua aplicabilidade dentro do ambiente do LNCC.

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
Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020	Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal (https://www.in.gov.br/en/web/dou/-/instrucao-normativa-n-1-de-27-de-maio-de-2020-258915215)
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 (https://www.in.gov.br/en/web/dou/-/instrucao-normativa-gsi/pr-n-3-de-28-de-maio-de-2021-322963172)
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)
Portaria MCTI Nº 7.061, DE 24 DE MAIO DE 2023	Regimento Interno do Laboratório Nacional de Computação Científica (https://www.gov.br/lncc/pt-br/acesso-a-informacao/institucional/regimento-interno)

5 DOCUMENTOS COMPLEMENTARES

03-PSISD	Política de Segurança da Informação LNCC– SANTOS DUMONT
04-RA	Análise de Risco - Risk Assessment
07-BIA	Relatório da Reunião – BIA
19-PA	Procedimento de Auditoria
24-PAIO	Planilha de Avaliação da Importância dos Objetivos do LNCC - Santos Dumont
25-PPAR	Planilha dos Planos de Ação e Riscos
26-ACAD	Análise Crítica da Alta Direção
37-MAR	Metodologia da Avaliação de Risco.
42-PANCOM	Planilha de avaliação e acompanhamento de NCs e OMs
58-NEPI	Necessidades e Expectativas das Partes Interessadas

6 SIGLAS

SGSI	Sistema de Gestão de Segurança da Informação
CENAPAD	Centro Nacional de Processamento de Alto Desempenho
PAD	Processamento de Alto Desempenho
SDumont	Supercomputador Santos Dumont
SINAPAD	Sistema Nacional de Processamento de Alto Desempenho
SSD	Supercomputador Santos Dumont
TIC	Tecnologia da Informação e Comunicação

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

7 TERMOS E DEFINIÇÕES

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;
Colaborador	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, Glossário de Segurança da Informação do GSI/PR e 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 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 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 das 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 o 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 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

[1] Glossário de Segurança da Informação - Portaria GSI/PR nº 93, de 18 de outubro de 2021 do Gabinete de Segurança Institucional da Presidência da República

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".

8.1 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.

Os dados históricos sobre as ações realizadas pelo LNCC podem ser acompanhados pelos Termos de Compromisso de Gestão (TCG), disponibilizados no site oficial da instituição[2]

8.2 ESTRUTURA ORGANIZACIONAL DO LNCC

O Laboratório Nacional de Computação Científica (LNCC) tem sua estrutura organizacional definida pelo seu Regimento Interno

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

publicado como Portaria[3], assinada pelo Ministro de Estado da Ciência, Tecnologia e Inovação.

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 Privacidade e Segurança da Informação de acordo com a norma ISO 27001:2013.

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

i. Comitê de Privacidade e Segurança da Informação - CPSI
ii. Gestores de Segurança da informação - GSI
iii. Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR
iv. Comitê de Gestão de Risco do LNCC - CGR
v. Comitê de Governança Digital - CGD
vi. Comitê Gestor de Uso dos Recursos da Expansão do Supercomputador Santos Dumont - CGSD-LIBRA
vii. Comitê Gestor do SDumont – CG – SD
viii. Conselho Técnico-Científico – CTC
ix. Conselho de Pesquisa e de Formação de Recursos Humanos – CPFRH
x. Conselho de Atividades de Gestão – CAGE
xi. Coordenação de Tecnologia da Informação e Comunicação – COTIC
xii. Coordenação de Gestão e Administração – COGEA
xiii. Autoridade designada para realizar o monitoramento Lei de Acesso à Informação (LAI), conforme determina o Artigo nº 40 da Lei de Acesso à Informação
xiv. Ponto focal de interlocução do Laboratório Nacional de Computação Científica - LNCC, na implantação da Lei Geral de Proteção de Dados (LGPD) do MCTI

As seguintes equipes estão diretamente envolvidas com os processos gerenciais, técnicos e de segurança da informação do Supercomputador Santos Dumont: (i) o Diretor do LNCC, (ii) os membros do CTC, (iii) os membros do CPFRH, (iv) os membros do CAGE, (v) o Coordenador da COTIC, (vi) o Coordenador da COGEA.

Além destas estão envolvidos os colabores vinculados aos seguintes serviços/núcleos/áreas:

i. Serviço de Suporte de Sistemas e Redes - SERED
ii. Setor de Governança de Tecnologia da Informação - SESTI
iii. Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR
iv. Serviço de Gestão e Desenvolvimento de Pessoas - SEGEP
v. Serviço de Logística e Patrimônio - SELEP
vi. Serviço de Comunicação Institucional - SECIN
vii. Setor de Administração do Campus - SECAM.

[3] https://www.gov.br/lncc/pt-br/acesso-a-informacao/institucional/regimento-interno

A Figura 1: Organograma do LNCC, descreve o organograma[4] do Laboratório Nacional de Computação Científica.

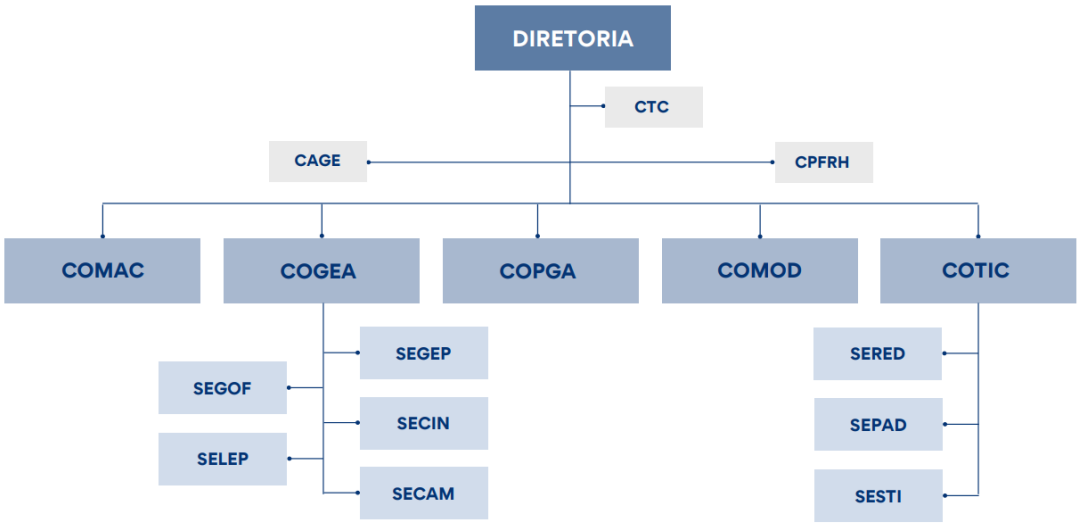


Figura 1: Organograma do LNCC
Fonte: Plano Diretor da Unidade (PDU) para o período de 2023 a 2027

8.3 ALOCAÇÃO DE RECURSOS

A adequação dos recursos necessários ao LNCC 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.

9 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. 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.

9.1 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 Privacidade e Segurança da Informação - CPSI**: 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 - GSI**: das 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 a área do Gabinete de Segurança Institucional da Presidência da República (GSI) responsável pelas ações relacionadas à segurança da informação e cibernética[5] 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

[4] https://www.gov.br/lncc/pt-br/acesso-a-informacao/institucional/organograma
[5] https://www.gov.br/gsi/pt-br/ssic

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. **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.

vi. **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.

vii. **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.

viii. **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.

ix. **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.

x. **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 relacionados 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.

xi. **Setor de Governança em 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.

xii. **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.

xiii. **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

xiv. **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)

xv. **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.

xvi. **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.

xvii. **Setor 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.

xviii. **Autoridade de monitoramento da Lei de Acesso à 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.

xix. **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.

xx. **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.

xxi. **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.

xxii. **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 Privacidade e Segurança da Informação e o Gestor de Segurança da Informação devem propor as normas e políticas relativas à segurança da informação e comunicações do LNCC.

10 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 norma ISO/IEC 27001, estão todos os ativos do Supercomputador Santos Dumont (SSD) classificados de acordo com as seguintes categorias de ativos:

i. Sites ou instalações (locais físicos que hospedam outros ativos);
ii. Hardware (equipamentos e servidores, estações de trabalho ou redes);
iii. Software (software de servidores, estações de trabalho ou redes);
iv. Pessoas;
v. Informações.

11 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. No âmbito interno, esta política pode ser facilmente 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."

11.1 ABNT NBR ISO/IEC 27002:2013

Este sistema de gestão e seus processos, para assegurar os aspectos de segurança da informação, são baseados 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 aos ativos críticos de uma organização.

11.2 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 um ambiente virtual de aprendizagem ou no formato de webinar.

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

É necessário conscientizar todos os colaboradores para que conheçam e entendam o que são:

i. Sistema de Gestão de Segurança;
ii. Comitê de Segurança da Informação e Comunicação;
iii. Política de Segurança da Informação e Comunicação;
iv. 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[6], que dispõem sobre normas de conduta dos servidores públicos. Para maiores informações também pode-se consultar o "Manual de Conduta do Agente Público Civil do Poder Executivo Federal"[7]

12 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. Os documentos restritos serão disponibilizados na pasta "Restritos"

Os documentos do sistema de gestão são controlados através da planilha denominada "01-LDC - Lista de Documentos

[6] https://www.planalto.gov.br/ccivil_03/leis/l8027.htm
[7] https://www.gov.br/mcom/pt-br/acesso-a-informacao/manualdecondutadoagentepublicocivil.pdf

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 devem ser disponibilizados no site https://sec.lncc.br. Os documentos classificados como públicos (externos) podem ser disponibilizados na área do site da institucional destinada à Segurança da Informação[8].

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 TIC serão armazenados em sistema de documentação próprio e devem estar disponíveis no site: https://csrdoc2.sre.lncc.br/

Os documentos do SGSI devem ser analisados criticamente de forma periódica, de acordo com desenvolvimentos regulatórios, necessidades do mercado e melhores práticas. Todos os documentos controlados devem estar disponíveis no SEI-MCTI.

13 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.

14 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.

As informações sobre as necessidades e expectativas das partes interessadas estão disponíveis no documento 58-NEPI.

15 PROJETOS

No escopo do 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"[9] do site do Supercomputador Santos Dumount.

16 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 seus macroprocessos. A análise de riscos é controlada e executada com o apoio do Gestor de Risco da Segurança da Informação e está documentada

[8] https://www.gov.br/lncc/pt-br/acesso-a-informacao/institucional/politica-de-seguranca-1
[9] https://sdumont.lncc.br/projects_view.php?pg=projects&status=ongoing

através da planilha matriz de riscos, apresentada no documento 37-MAR.

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 ações são planejadas para tratar e minimizar os riscos.

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

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

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

O planejamento de controles operacionais e o tratamento dos riscos está descrito no documento 25-PPAR.

17 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.

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

17.1 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: (i) constituição do Comitê da segurança da Informação e Comunicações e de Segurança Física; (ii) adequação física do perímetro de segurança do Santos Dumont; (iii) revisão da política de segurança do LNCC; (iv) 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; (v) campanha de divulgação e conscientização da segurança da informação; (vi) 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: (i) planejada e contratada uma consultoria externa para atender todos os requisitos e certificação da ISO/IEC 27001:2013; (ii) executada uma auditoria externa de certificação da ISSO/IEC 27001:2013; (iii) 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 e (iv) 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: (i) emitida uma portaria atualizando e reestruturando a equipe de tratamento de incidentes de acordo com as normativas do Departamento de Segurança da Informação; (ii) disponibilização do Treinamento de Conscientização em Segurança da Informação no ambiente virtual de aprendizagem (AVA) do LNCC, este treinamento passou a contar com um Quiz ao final de cada seção; (iii) 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; (iv) em março de 2021 ocorreu a auditoria interna da ISO/IEC 27001 e (v) em maio de 2021 ocorreu a auditoria externa da ISO/IEC 27001.

No ano de **2022**, além da auditoria interna e da auditoria externa da ISO/IEC 27001, foram iniciados vários processos de contratação, dentre eles destacam-se: a aquisição de uma nova solução de firewall do tipo NGFW, a atualização a infraestrutura de rede do CPD que além de outras funcionalidades proverá a redundância de ativos e de canais de comunicação, a atualização da infraestrutura da rede sem fio, a atualização da infraestrutura do segmento da rede interna e a contratação de uma nova solução combate a malware.

No ano de **2023**, ocorreu a entrega e o início da implantação da nova solução de firewall da instituição, a realização de um Gap Analysis do SGSI, a realização da contratação de uma solução de SOC para o escopo certificado e finalizamos os processos de contratação relacionados a redes e segurança da informação para o CPD do LNCC. Ainda realizamos as auditorias internas e externas da ISO/IEC 27001.

No ano de **2024**, já foi realizado o Gap Analysis do SGSI, estão ocorrendo as auditorias da ISO/IEC 27001, está ocorrendo a implantação da solução redes e segurança da informação no CPD do LNCC e ainda está sendo planejada a contratação da solução de Endpoint de segurança.

18 INDICADORES – MONITORAMENTO, DESEMPENHO E AVALIAÇÃO

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

18.1 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 2023-2027, apresentando descrição de missão, visão, valores e princípios da instituição.

Neste sistema de gestão, adotamos os indicadores de Computação De Alto Desempenho.

As informações sobre o Termo de Compromisso de Gestão – TCG e seus indicadores estão disponíveis no site do LNCC[10].

18.2 INDICADORES HPC SANTOS DUMONT

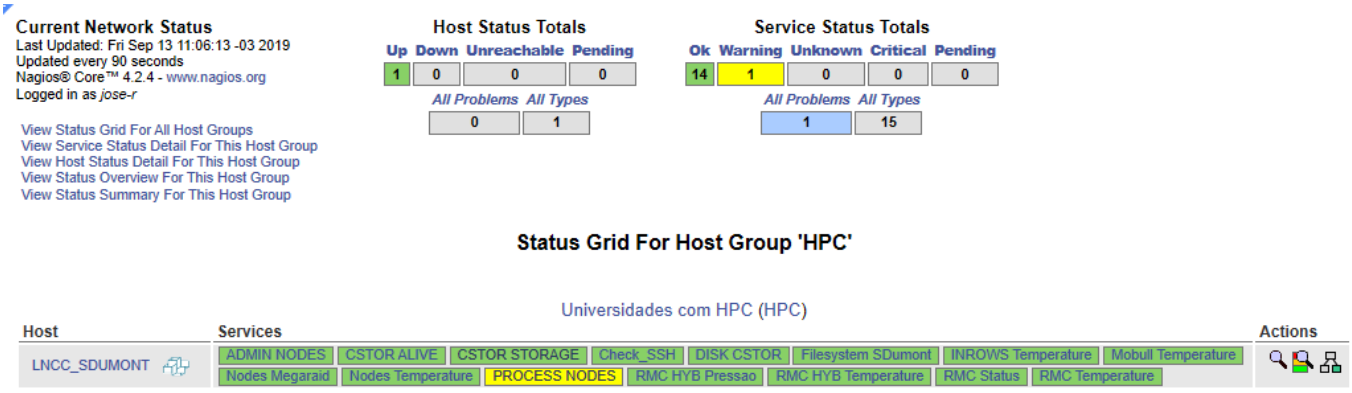
O monitoramento dos indicadores de funcionamento do Supercomputador Santos Dumont é executado pela operação técnica da empresa Atos, com SLA de atendimento 24x7, estes são responsáveis por monitorar o ambiente diariamente, estando ciente de qualquer problema técnico no desempenho dos supercomputadores.

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.

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



Descrição dos Grupos de Serviço:

- **i.** ADMIN NODES: Monitoração dos nós de administração, up ou down.
- **ii.** CSTOR ALIVE: Monitoração dos appliances de storage, up ou down.
- **iii.** CSTOR STORAGE: Monitoração dos discos dos appliances de storage.
- **iv.** Check_SSH: Monitoração de acesso ao Santos Dumont (sdumont0).
- **v.** DISK CSTOR: Monitoração dos discos do clustersotor.
- **vi.** Filesystem Sdumont: Monitoração de uso dos filesystems dos nós de administração.
- **vii.** Inrow temperature: Monitoração da temperatura do inrows.
- **viii.** Mobull temperarure: Monitoração da temperatura no interior do Santos Dumont.
- **ix.** Nodes megaraid: Monitoração dos discos internos dos nós de monitoração.
- **x.** Process nodes: Monitoração da quantidade de nós de processamento disponíveis no cluster.
- **xi.** RMC HYB Pressão: Monitoração da pressão do glicol na HYC.

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

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)

INDICADOR 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
- **Unidade organizacional:** Serviço de Suporte de Sistemas e Redes - SERED
- **Apresentar para:** do Gestor do SSD e para o Gestor de Segurança
- **Data Inicial:** 05/2021

As informações podem ser obtidas através de consultas à base de dados do sistema de gestão de incidentes utilizado pela COTIC, 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:

i. Quantidade de Jobs Submetidos
ii. Relação de chamados solucionados x em aberto
iii. Tempo médio de solução dos chamados
iv. Espaço em Disco
v. Relação dos chamados atendidos pelo contrato de manutenção
vi. Alertas das Facilities do SSD

18.3 INDICADORES ESPECÍFICOS

As informações sobre os indicadores associados aos objetivos de segurança e outros indicadores específicos do sistema de gestão de segurança da informação estão disponíveis no documento 24-PAIO.

O acompanhamento dos indicadores é realizado pela equipe responsável e são monitorados pelo gestor de segurança.

19 COMUNICAÇÃO

Os 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.

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”.

As publicações são feitas através de diferentes canais conforme segue:

Assunto	Frequência	Meio de Comunicação	Para quem será comunicado
Política de Segurança da Informação e Comunicação do LNCC – PSI	Quando necessário	Portaria interna; E-mail (lista de distribuição); Site oficial da instituição	Todos os colaboradores
Normas e Políticas complementares de segurança da informação	Quando necessário	E-mail (lista de distribuição); site oficial da instituição; repositório de documentos controlados;	Partes interessadas
Procedimento técnicos e operacionais	Quando necessário	E-mail (lista de distribuição); repositório de documentos controlados; repositório de procedimentos;	Partes interessadas
Artefatos da campanha de conscientização em segurança da informação	Mensalmente	E-mail (lista de distribuição); Site oficial da instituição; redes sociais;	Todos os colaboradores e para o público em geral
Notificação de incidentes de segurança	Quando necessário	E-mail	Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR)
Notificação de não conformidades do SGSI	Quando necessário	E-mail	Gestor de segurança da informação
Portarias Internas	Mensal	Boletim de serviço	Todos os colaboradores
Comunicados em geral	Quando necessário	E-mail interno (lista de distribuição)	Todos os colaboradores

20 ANÁLISE CRÍTICA DA ALTA DIREÇÃO - MANAGEMENT REVIEW

Periodicamente, as equipes deverão encaminhar para o Gestor de segurança da informação, as informações sobre os seus indicadores. As informações sobre os indicadores e sobre os objetivos de segurança da informação serão analisadas 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/IEC 27001:2013.

O documento 26-ACAD contém as informações sobre a última análise crítica realizada pela direção do LNCC.

21 MELHORIAS

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

21.1 NÃO CONFORMIDADES E AÇÕES CORRETIVAS

As não conformidades apontadas nas auditorias interna e externa, são endereçadas, planejadas para ação corretiva.

As ações corretivas poderão ser mapeadas em planos de ação ou em ações pontuais. As informações sobre as não conformidades e oportunidades de melhoria devem estar disponíveis no documento 42-PANCOM.

O acompanhamento da execução das ações de tratativas será realizado pelos líderes das equipes e reportado ao gestor de segurança.

21.2 MELHORIA CONTÍNUA

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

Os planos de melhoria são implementados para aprimorar o sistema local, sua maturidade e sua eficiência.

As informações sobre as não conformidades e oportunidades de melhoria devem estar disponíveis no documento 42-PANCOM.

O acompanhamento da execução das ações de tratativas será realizado pelos líderes das equipes e reportado ao gestor de segurança da informação.

22 PAPEIS E RESPONSABILIDADES

Este documento deve ser de conhecimento da direção da instituição, dos membros do Comitê de Privacidade e de Segurança da (CPSI), 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.

O diretor e o gestor de segurança da informação são os responsáveis pela elaboração, pela avaliação do SGSI.

O diretor é o responsável pela aprovação desta norma.

O SECIN é o responsável por realizar a publicação desta norma no site oficial da instituição e por realizar a sua divulgação para as partes interessadas.

Periodicamente, o SECIN deve-se realizar a divulgação desta norma para a comunidade de colaboradores do LNCC.

23 ANÁLISE CRÍTICA

Este documento deverá ser analisado criticamente, quanto à sua eficácia e adequação ao SGSI do LNCC, ao menos a cada 12 meses, ou quando ocorrem mudanças.

24 HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens Revisados
1.0	11/10/2019	Documento Inicial.
2.0	27/02/2020	Atualização da estrutura organizacional do LNCC; das informações sobre o Modelo de gestão de segurança da informação.
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.
3.1	25/05/2020	Aplicação dos Rótulos de Classificação
3.2	08/03/2021	Atualizado com as informações do novo regimento interno da instituição.
3.3	22/04/2021	Adequação do documento ao novo formato
4.0	04/05/2022	Revisão anual, atualização com as informações da PSI, consolidação das informações do MSO dentro do ISMS
5.0	30/05/2023	Atualização do template utilizado no SGSI, revisão das informações sobre as equipes e seus papeis.
6.0	18/06/2024	Revisão orográfica, Remoção de seção sobre a “Política de transição”, atualização das referências as legislações e normativas; Migração das informações sobre os indicadores para o documento 24-PAIO, migração das informações sobre as partes interessadas para o documento 58-NEPI.

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborado por:	Luis Rodrigo de Oliveira Gonçalves	Gestor de segurança da informação
Verificado por:	Bruno Alves Fagundes	Gestor de segurança da informação substituto
Aprovado por:	Fábio Borges de Oliveira	Diretor do LNCC

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

_____