

<b>Política de uso aceitável dos ativos</b>		 <b>Laboratório Nacional de Computação Científica</b>	MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INovações	
<b>CÓDIGO</b>	<b>VERSSÃO</b>	<b>TIPO DE ACESSO</b>	<b>NÍVEL DE ACESSO</b>	
27-PUAA	7.0	Externo	Público	
<b>CONTROLES DA ABNT NBR ISO/IEC 27001:2022</b>		<b>PUBLICADO EM</b>	<b>PAGINAÇÃO</b>	
A.5.10 - Uso aceitável de informações e outros ativos associados		15/08/2025	1/4	

## SUMÁRIO

<b>1</b>	<b>Objetivo</b>	<b>1</b>
<b>2</b>	<b>Campo de aplicação</b>	<b>1</b>
<b>3</b>	<b>Responsabilidade</b>	<b>1</b>
<b>4</b>	<b>Documentos de referência</b>	<b>1</b>
<b>5</b>	<b>Documentos complementares</b>	<b>2</b>
<b>6</b>	<b>Siglas</b>	<b>2</b>
<b>7</b>	<b>Termos e definições</b>	<b>2</b>
<b>8</b>	<b>Diretrizes gerais</b>	<b>2</b>
<b>9</b>	<b>Diretrizes para elaboração das políticas específicas</b>	<b>2</b>
<b>10</b>	<b>Diretrizes gerais dos ativos do Supercomputador Santos Dumont (SSD)</b>	<b>3</b>
<b>11</b>	<b>Diretrizes gerais dos ativos da infraestrutura do CPD do LNCC</b>	<b>3</b>
<b>12</b>	<b>Uso de Ativos de Terceiros e Ambientes Colaborativos</b>	<b>3</b>
<b>13</b>	<b>Histórico da revisão e quadro de aprovação</b>	<b>4</b>

### 1 Objetivo

Assegurar que as informações e outros ativos associados sejam devidamente protegidos, usados e manuseados, assim como definir as diretrizes gerais de uso aceitável dos ativos de informação do Laboratório Nacional de Computação Científica (LNCC).

### 2 Campo de aplicação

Convém que os controles e diretrizes apontados na política sejam aplicados em todas as unidades organizacionais do LNCC. Para os ativos que fazem parte do escopo certificado em conformidade à ABNT NBR ISO/IEC 27001:2022 o conteúdo da política é de execução obrigatória.

### 3 Responsabilidade

O Coordenador de TIC e o Gestor de Segurança da Informação do LNCC são os responsáveis pela elaboração e análise crítica desta política. A aprovação é de responsabilidade do Coordenador de TIC, enquanto o Gestor de Segurança da Informação é o responsável pela publicidade do procedimento.

Os proprietários dos ativos devem definir e divulgar as regras de uso aceitável para cada um deles. Recomenda-se que formalizem essas regras para os ativos de informação.

A COTIC deve prover os recursos necessários para a implementação e o monitoramento do uso aceitável dos ativos. O Gestor de Segurança da Informação deve acompanhar esse monitoramento.

A equipe da COTIC e os proprietários dos ativos devem implementar e monitorar as regras de uso aceitável.

Os usuários e demais colaboradores devem se comprometer a respeitar as regras de uso aceitável de cada ativo. Os usuários são responsáveis por qualquer recurso de tratamento das informações.

### 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 27001:2022	Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos
ABNT NBR ISO/IEC 27002:2022	Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação
Glossário de Segurança da Informação	Portaria GSI/PR nº 93, de 18 de outubro de 2021 ( <a href="https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370">https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370</a> )
Regimento Interno do Laboratório Nacional de Computação Científica	PORTRARIA MCTI Nº 7.061, DE 24 DE MAIO DE 2023 ( <a href="https://www.in.gov.br/en/web/dou/-/portaria-mcti-n-7.061-de-24-de-maio-de-2023-485541159">https://www.in.gov.br/en/web/dou/-/portaria-mcti-n-7.061-de-24-de-maio-de-2023-485541159</a> )

 <p><b>Laboratório Nacional de Computação Científica</b></p>	<p>MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INovações</p> 	<b>CÓDIGO</b>	<b>VERSÃO</b>	<b>PAGINAÇÃO</b>
		27-PUAA	7.0	2/4
Sistema de Gestão de Segurança da Informação (08-ISMS)	Visão geral do Sistema de Gestão de Segurança da Informação (SGSI) do LNCC (Laboratório Nacional de Computação Científica).			
Política de Segurança da Informação do LNCC (02-PSI)	Institui a Política de Segurança da Informação (PSI), no âmbito do Laboratório Nacional de Computação Científica (LNCC), com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação ( <a href="https://www.gov.br/lncc/pt-br/acesso-a-informacao/institucional/politica-de-seguranca-1/politicas-de-seguranca-da-informacao/politicas-de-seguranca-da-informacao-psi">https://www.gov.br/lncc/pt-br/acesso-a-informacao/institucional/politica-de-seguranca-1/politicas-de-seguranca-da-informacao/politicas-de-seguranca-da-informacao-psi</a> )			

## 5 Documentos complementares

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

17-PGA	Define o procedimento geral para gestão de acesso lógico ao ambiente computacional do CPD e do Supercomputador Santos Dumont.
--------	---

## 6 Siglas

SGSI	Sistema de Gestão de Segurança da Informação
SSD	Supercomputador Santos Dumont

**Nota:** As siglas das UO do LNCC podem ser acessadas no Regimento Interno do Laboratório Nacional de Computação Científica (<https://www.in.gov.br/en/web/dou/-/portaria-mcti-n-7.061-de-24-de-maio-de-2023-485541159>).

## 7 Termos e definições

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

Escalonador	Software para gerenciamento e alocação dos recursos computacionais
SSH	Secure Shell (SSH) é um protocolo de rede criptográfico para operação de serviços de rede de forma segura sobre uma rede insegura
VPN	Rede privada virtual, mais conhecida por VPN, refere-se à construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública

## 8 Diretrizes gerais

**8.1** Convém que regras para o uso aceitável e procedimentos para o manuseio de informações e outros ativos associados sejam identificados, documentados formalmente e implementados.

**8.2** Para todos os ativos, ou grupo de ativos, identificados no inventário dos ativos contidos no escopo certificado em conformidade à ABNT NBR ISO/IEC 27001:2022, deve-se definir as regras de uso aceitável.

**8.3** Convém que usuários internos e externos que usem ou tenham acesso às informações e outros ativos associados estejam conscientes dos requisitos de segurança da informação para proteger e lidar com as informações e outros ativos associados.

**8.4** Deve-se realizar a publicitação das regras para o uso aceitável e procedimentos para o manuseio de informações e outros ativos associados as partes interessadas.

**8.5** A partir do primeiro acesso, os usuários, a contar da data de publicação das regras, realizam o aceite automático das regras de uso aceitável do respectivo ativo.

**8.6** Caso o usuário não esteja de acordo com as regras de utilização, ele tem o direito de não mais utilizar o ativo e deve solicitar a remoção do seu respectivo direito de acesso ao mesmo.

## 9 Diretrizes para elaboração das políticas específicas

**9.1** As diretrizes de uso aceitável dos ativos devem levar em consideração as regras a serem observadas durante todo o ciclo de vida das informações, sua classificação e os riscos identificados.

**9.2** As diretrizes específicas de uso aceitável devem declarar minimamente:

- i. comportamentos esperados e inaceitáveis dos indivíduos do ponto de vista de segurança da informação;
- ii. uso permitido e proibido de informações e outros ativos associados;
- iii. atividades de monitoramento que estão sendo realizadas pela organização.

 <b>Laboratório Nacional de Computação Científica</b>	 <b>MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INovações</b>	<b>CÓDIGO</b>	<b>VERSÃO</b>	<b>PAGINAÇÃO</b>
		27-PUAA	7.0	3/4

**9.3** As diretrizes específicas de uso aceitável devem considerar os seguintes itens:

- i. restrições de acesso que apoiam os requisitos de proteção para cada nível de classificação;
- ii. manutenção de registro dos usuários autorizados de informações e outros ativos associados;
- iii. proteção de cópias temporárias ou permanentes de informações a um nível consistente com a proteção das informações originais;
- iv. armazenamento de ativos associados a informações de acordo com as especificações dos fabricantes;
- v. marcação clara de todas as cópias de mídia de armazenamento (eletrônico ou físico) para a atenção do destinatário autorizado;
- vi. autorização de descarte de informações e outros ativos associados e métodos de descarte de apoio.

## **10 Diretrizes gerais dos ativos do Supercomputador Santos Dumont (SSD)**

**10.1** A infraestrutura de armazenamento, de rede e todos os hosts devem ser administrados pela equipe da COTIC e pela equipe da empresa responsável pela manutenção do SSD.

**10.2** Apenas a equipe da COTIC e a equipe da empresa responsável pela manutenção do SSD devem ter privilégios administrativos aos ativos do supercomputador.

**10.3** O acesso administrativo aos equipamentos e a infraestrutura deve ser controlada conforme descrito no documento 17-PGA - Procedimentos para Gestão de Acesso.

**10.4** Os usuários não devem executar seus jobs diretamente no ambiente de login.

**10.5** Os nós de processamento devem ser utilizados conforme disponibilidade de recursos alocados pelo escalonador (software para gerenciamento e alocação dos recursos computacionais).

**10.6** Os usuários não devem executar seus “Jobs” diretamente no ambiente de processamento.

**10.7** Os nós de serviço somente devem ser acessados pela equipe da COTIC e pela equipe da empresa responsável pela manutenção do SSD.

**10.8** A infraestrutura física e lógica dos sistemas de armazenamento deverá ser mantida e gerenciada pela COTIC.

**10.9** Os usuários devem ter acesso exclusivamente à sua área de dados.

**10.10** Os usuários devem zelar pela privacidade de seus dados e devem promover a privacidade dos dados dos demais usuários.

**10.11** Os usuários não devem acessar, nem forçar o acesso a área de dados de outros usuários.

**10.12** Os usuários devem utilizar o concentrador de VPN (Virtual Private Network) do SSD ou os servidores de acesso para se conectar ao ambiente.

**10.13** Os usuários que estiverem conectados ao segmento da rede interna do LNCC poderão ter acesso ao SSD por conexões via SSH.

**10.14** Os usuários deverão receber o termo de uso do supercomputador antes do primeiro acesso.

**10.15** Ao realizar o primeiro acesso os usuários aceitam automaticamente o termo de uso do supercomputador.

**10.16** O termo de uso do supercomputador deverá estar disponível no website com as informações do supercomputador (<https://sdumont.lncc.br/>)

## **11 Diretrizes gerais dos ativos da infraestrutura do CPD do LNCC**

**11.1** Todos os equipamentos hospedados no ambiente do CPD do LNCC e conectados ao SSD devem ser gerenciados e administrados somente pela equipe de suporte da COTIC.

**11.2** Equipamentos não gerenciados pela equipe da COTIC (colocation ou equipamentos de projetos de pesquisa) devem ser hospedados em segmentos de rede específicos.

**11.3** Equipamentos de administração compartilhada (equipe da COTIC e equipe do proprietário do ativo) devem ser formalmente registrados e auditados regularmente.

**11.4** O acesso privilegiado aos equipamentos de administração compartilhada, quando originado fora da rede do LNCC, deverá passar por ativos de segurança definidos pela COTIC.

## **12 Uso de Ativos de Terceiros e Ambientes Colaborativos**

**12.1** Quando os ativos em questão não pertencerem diretamente ao LNCC, tais como serviços públicos em nuvem ou outros ativos gerenciados por terceiros, o uso desses ativos e quaisquer ativos do LNCC a eles associados (por exemplo,

 <p><b>Laboratório Nacional de Computação Científica</b></p>	<p>MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INovações</p> 	<b>CÓDIGO</b>	<b>VERSÃO</b>	<b>PAGINAÇÃO</b>
		27-PUAA	7.0	4/4

informações, software) devem ser identificados e controlados de forma apropriada.

**12.2** Convém que o controle do uso desses ativos de terceiros seja formalizado por meio de acordos contratuais ou outros instrumentos formais com os provedores de serviços (como provedores de serviços em nuvem), que devem especificar claramente os requisitos e responsabilidades de segurança da informação.

**12.3** Cuidados adicionais devem ser observados e diretrizes específicas podem ser necessárias para garantir a proteção adequada das informações e ativos do LNCC ao utilizar ambientes colaborativos de trabalho que envolvam o compartilhamento de dados ou acesso a recursos externos.

### 13 Histórico da revisão e quadro de aprovação

<b>Revisão</b>	<b>Data</b>	<b>Itens Revisados</b>
1.0	17/03/2020	Documento Inicial.
1.1	19/05/2020	Classificação e rotulação do documento
1.2	06/05/2021	Adequação do documento ao novo formato.
2.0	11/05/2021	Revisão do conteúdo e estrutura do documento
3.0	29/05/2022	Análise crítica do conteúdo, ajuste da numeração dos itens e revisão do texto
4.0	24/05/2023	Aplicação do novo template utilizado no SGSI.
5.0	14/06/2024	Revisão e atualização da referência aos documentos e normativas do governo. Remoção da seção “POLÍTICA DE TRANSIÇÃO PARA ADEQUAÇÃO DA NORMA”.
6.0	16/12/2024	Atualização da estrutura da política; Atualização das diretrizes conforme versão 2022 das normas ISO 27001 e 27002; Atualização das URLs; Revisão Ortográfica; Alteração do nome do artefato para política.
7.0	15/08/2024	Foram incluídas orientações sobre Comportamentos Inaceitáveis e Uso Proibido, assim como diretrizes específicas para Ativos de Terceiros e Ambientes Colaborativos.

**Quadro de Aprovação**

	<b>Nome</b>	<b>Atribuição</b>
<b>Elaborado por:</b>	Luís Rodrigo de Oliveira Gonçalves	Gestor de segurança da informação
<b>Verificado por:</b>	Bruno Alves Fagundes Rhamine Carin Vieira	Chefe do SERED Colaboradora da COTIC
<b>Aprovado por:</b>	Wagner Vieira Leo	Coordenador da COTIC

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