Uso aceitável dos ativos		Laboratório Nacional de Computação Científica / MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES	
CÓDIGO	**VERSÃO**	**TIPO DE ACESSO**	**NÍVEL DE ACESSO**
27-PUAA	5.0	Externo	Público
CONTROLES DA ABNT NBR ISO/IEC 27001:2013		**PUBLICADO EM**	**PAGINAÇÃO**
8.1.3 Uso aceitável dos ativos		14/06/2024	1/3

SUMÁRIO

1 OBJETIVO

O ambiente computacional do Supercomputador Santos Dumont (SSD) é composto por três grupos de hots: (i) os nós de processamento, os (ii) nós de login e os (iii) nós de serviços. Além destes hosts há (i) a infraestrutura de armazenamento de dados, (ii) a infraestrutura de rede, (iii) sistema de climatização, (iv) sistema de fornecimento de energia, (v) sistema de vigilância e (vi) controle de acesso físico.

A infraestrutura hospedada no CPD do LNCC, conectada ao Supercomputador Santos Dumont (SSD), é formada por: (i) ativos de segurança (Firewall, IPS, Concentrador de VPN), (ii) ativos de rede (Switchs, Roteadores), (iii) storage e (iv) servidores.

Este documento define as diretrizes gerais de uso aceitável dos ativos de informação do Supercomputador Santos Dumont (SSD) e da infraestrutura localizada no CPD do Laboratório Nacional de Computação Científica (LNCC) a ele conectado.

2 CAMPO DE APLICAÇÃO

Este procedimento se aplica a todas as unidades organizacionais do LNCC que atuam nos processos que fazem parte do escopo certificado em conformidade à ABNT NBR ISO/IEC 27001.

3 RESPONSABILIDADE

O Coordenador de TIC e o Gestor de Segurança da Informação são os responsáveis pela elaboração e análise crítica deste procedimento. A responsabilidade pela aprovação deste procedimento é do Coordenador de TIC. O Gestor de Segurança da Informação é o responsável pela publicação deste procedimento.

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
Glossário de Segurança da Informação	Portaria GSI/PR nº 93, de 18 de outubro de 2021 (https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370)
Regimento Interno do Laboratório Nacional de Computação Científica	PORTARIA MCTI Nº 7.061, DE 24 DE MAIO DE 2023 (https://www.in.gov.br/en/web/dou/-/portaria-mcti-n-7.061-de-24-de-maio-de-2023-485541159)
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 Cientifica).
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 (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)

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

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 na 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 PAPEIS E RESPONSABILIDADES PELO PROCESSO

8.1 A COTIC deve prover os recursos para a implementação e monitoramento do uso aceitável dos ativos.

8.2 O Gestor de Segurança da Informação deve acompanhar o monitoramento do uso aceitável dos ativos.

8.3 A equipe da COTIC e da empresa contratada responsável pela manutenção do SSD devem implementar e realizar o monitoramento das regras de uso aceitável dos ativos.

8.4 A equipe do SECIN deve realizar a divulgação das regras de uso aceitável para as partes interessadas.

8.5 Os usuários e demais colaboradores devem se comprometer e respeitar as regras de uso aceitável.

9 ATIVOS DO SUPERCOMPUTADOR SANTOS DUMONT (SSD)

9.1 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.

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

9.3 O acesso administrativo aos equipamentos e a infraestrutura deve ser controlada conforme descrito no documento 17-PGA.

9.4 Os usuários devem utilizar os nós de login para conectar-se ao SSD, preparar e submeter os seus “Jobs”.

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

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

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

9.8 Os nós de serviço não devem ser acessados diretamente pelos usuários finais.

9.9 A infraestrutura física de armazenamento deve ser gerenciada e configurada pela equipe da empresa responsável pela manutenção do SSD.

9.10 A infraestrutura lógica de armazenamento deve ser gerenciada e configurada pela equipe da COTIC e pela equipe da empresa responsável pela manutenção do SSD.

9.11 Os usuários devem ter acesso restrito à sua área de dados. Os usuários não devem ter acesso a outras áreas de dados.

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

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

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

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

10 ATIVOS DA INFRAESTRUTURA DO CPD DO LNCC

10.1 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.

10.2 Os usuários do supercomputador devem ter acesso restrito à sua área de armazenamento de dados no storage, conectado ao SSD.

11 ANÁLISE CRÍTICA

11.1 Este documento deve ser analisado criticamente, quanto à sua eficácia e adequação ao SGSI do LNCC, ao menos, uma vez ao ano, ou quando ocorrem mudanças.

12 HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens Revisados
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”

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborado por:	Luis Rodrigo de Oliveira Gonçalves	Gestor de segurança da informação
Verificado por:	Bruno Alves Fagundes	Serviço de Suporte de Sistemas e Redes
Aprovado por:	Wagner Vieira Leo	Coordenação de Tecnologia da Informação e Comunicação

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