Laboratório Nacional de Computação Científica

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES

PÁTRIA AMADA BRASIL GOVERNO FEDERAL

Política de Senhas LNCC

Controle Interno nº: NUSTI 008/2019
Classificação: Sem acesso Público
Tipo de Acesso: Interno

Petrópolis, maio de 2020

Coordenação de Tecnologia da Informação e Comunicação - COTIC
Tel.: 0xx 24 2233-6025 Fax 0xx 24 2233-6198

Diretor
Augusto César Gadelha Vieira

Coordenação de Tecnologia da Informação e Comunicação – COTIC
Wagner Vieira Léo

Núcleo de Governança de Tecnologia da Informação - NUSTI
Rogério Albuquerque de Almeida

Sumário

Termos e Abreviações

CENAPAD - Centro Nacional de Processamento de Alto Desempenho

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

ISO - International Organization for Standardization

LNCC – Laboratório Nacional de Computação Científica

NUSTI - Núcleo de Governança de Tecnologia da Informação

PAD - Processamento de Alto Desempenho

SINAPAD - Sistema Nacional de Processamento de Alto Desempenho

SSD – Supercomputador Santos Dumont

TIC – Tecnologia da Informação e Comunicações

Histórico das Versões

Versão	Data	Descrição	Autor
1.0	31/07/2019	Documento Inicial.	Rogério Albuquerque de Almeida
2.0	01/10/2019	Revisão e ajustes da política.	Bruno Alves Fagundes e Luís Rodrigo de Oliveira Gonçalves
3.0	27/11/2019	Revisão e ajustes da política.	Bruno Alves Fagundes e Luís Rodrigo de Oliveira Gonçalves
3.1	21/05/2020	Inclusão da classificação e tipo de acesso.	Rogério Albuquerque de Almeida

1. Introdução

1.1. Finalidade

A combinação de usuário e senha identifica, de forma única, todos os acessos realizados à infraestrutura computacional do LNCC. A senha certifica que o usuário é quem diz ser, sendo de seu exclusivo controle, uso e conhecimento. Ela deve ser gerada pelo próprio.

Uma senha forte minimiza os riscos e inibe uma ação mal-intencionada, enquanto uma senha fraca pode comprometer todo o ambiente tecnológico. Dessa forma, esse documento visa estabelecer um padrão de criação e utilização de senhas fortes para todos os usuários do LNCC.

Este documento está subordinado à Política de Segurança da Informação e Comunicação (POSIC) do LNCC publicada sob a portaria nº 81/2019/SEI-LNCC de 30 de julho de 2019.

2. Abrangência

Esta política se aplica a todos os colaboradores do LNCC, quais sejam: funcionários servidores ou comissionados, estagiários, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações deste órgão. Todos esses colaboradores serão tratados nesta política como usuários.

3. Diretrizes do uso de senhas

Os sistemas, serviços e dispositivos do ambiente tecnológico do LNCC devem ser configurados para que seja possível a criação de senhas fortes.

Serão considerados caracteres especiais (incluindo o espaço):

- ! #$%&*)(_+=-}{^`'~][/;?:><.,|"

Serão considerados caracteres numéricos:

- 0123456789

Serão considerados caracteres alfabéticos maiúsculos:

- ABCDEFGHIJKLMNOPQSTUVXYWZ

Serão considerados caracteres alfabéticos minúsculos:

- abcdefghijklmnopqrstuvxywz

3.1. Tamanho da senha para conta de usuário

O comprimento da senha deve ter um mínimo de 8 caracteres.

3.2. Tamanho da senha para contas administrativas no SDumont

O comprimento da senha deve ter um mínimo de 15 caracteres.

3.3. Validade da senha

As senhas devem ter um período de validade inferior a 06 meses.

3.4. Tentativas incorretas

O sistema protegido deve ter o bloqueio após 5 tentativas incorretas. As solicitações de desbloqueio deverão ser encaminhadas ao Service Desk que seguirá o procedimento de validação das informações do usuário para efetuar o desbloqueio.

3.5. Redefinição de senhas

As solicitações de redefinição de senhas devem ser realizadas pelo próprio usuário através da intranet ou, quando esta não estiver disponível, através do Service Desk que seguirá o procedimento de validação de informações do usuário para disponibilizar as senhas.

Os usuários devem alterar suas senhas imediatamente após uma redefinição de senha pela equipe do Service Desk.

3.6. Boas práticas para criação de senhas fortes

Recomenda-se utilizar:

- Quantidade mínima de caracteres numéricos: 1
- Quantidade mínima de caracteres especiais: 1
- Quantidade mínima de caracteres alfabéticos maiúsculos: 1
- Quantidade mínima de caracteres alfabéticos minúsculos: 1
- Números aleatórios;
- Substituir letras por números ou caracteres especiais;
- Criar uma frase que auxilie na memorização da senha (ex: “Utilizar uma frase para memorizar a senha é mais seguro” pode gerar a senha “u1FpMaSe+s”;
- Criar padrões para formação da senha (#ftg9@AwS, #ftg9@GmAiL e etc.).

Evitar a utilização de:

- Repetição de sequências de caracteres conhecidos ou sequências de teclas do teclado como: 123456, abcdef, asdfgh, qwerty e etc;
- Uso de nomes, sobrenomes, nomes de membros da família e demais dados pessoais;
- Uso de placas de carros;
- Uso de palavras do dicionário;
- Uso de nomes de times de futebol, filmes, músicas, personagens e etc.;
- Repetição de senhas anteriores;
- Anotar a senha em papel ou no próprio computador;
- Uso da mesma senha em mais de uma conta.

4. Adequação à política

a) Os novos projetos de desenvolvimento ou novas aquisições de sistemas devem seguir os padrões estabelecidos nesta política;

b) As implementações para o ambiente tecnológico existente deverão ser adequadas a esta política no prazo de 01 (um) ano, a partir de sua publicação;

c) Caso não seja possível a adequação das ferramentas, o responsável deverá documentar essa informação, bem como seus motivos e encaminhar ao Service Desk para fins de registro e auditoria interna.

5. Obrigações

É estritamente proibido compartilhar suas senhas. Os usuários devem alterar suas senhas imediatamente após uma redefinição de senha por um funcionário do serviço de informações ou administrador.

6. Manutenção do documento

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

Wagner Vieira Léo	Rogério A. Almeida
Coordenador da COTIC	Chefe do NUSTI