



# **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO**

DA PROCURADORIA-GERAL DO ESTADO DO CEARÁ

## **NR02 - Uso de Senhas**

Setembro/2022



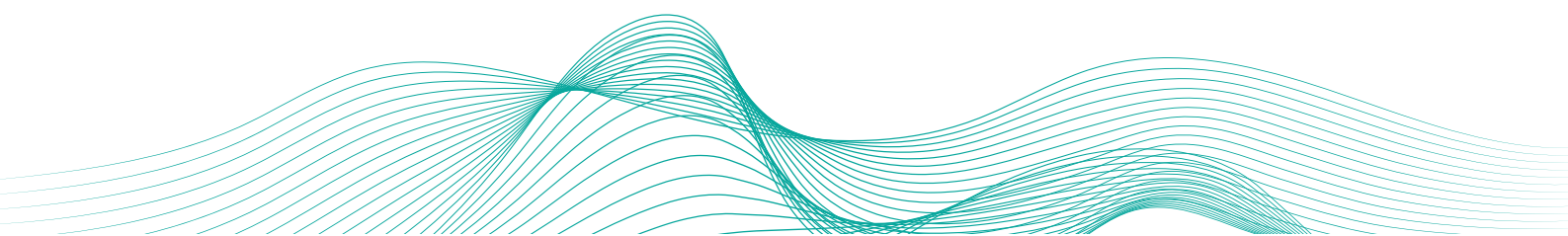
**CEARÁ**  
GOVERNO DO ESTADO  
PROCURADORIA-GERAL DO ESTADO

## CONTROLE DE VERSÕES

Versão	Data	Responsável	Alteração principal
00	07/11/2022	Coordenadoria de TI	Elaboração inicial

## SUMÁRIO

1. INTRODUÇÃO	3
2. OBJETIVO	3
3. ABRANGÊNCIA	3
4. USO DE SENHAS	3



## 1. INTRODUÇÃO

As credenciais de acesso (login e senha) são fundamentais no controle de acesso aos recursos tecnológicos da PGE-CE, e é através dessas credenciais que os usuários são identificados no ambiente de rede. Dada a importância, se faz necessário que as senhas tenham controles que garantam padrões mínimos de segurança.

## 2. OBJETIVO

Definir padrões mínimos de segurança na formação das senhas de acesso aos recursos tecnológicos da PGE-CE, garantindo que as senhas sejam fortes, inibindo e/ou dificultando que pessoas mal intencionadas consigam acesso indevido ao ambiente de rede da PGE-CE.

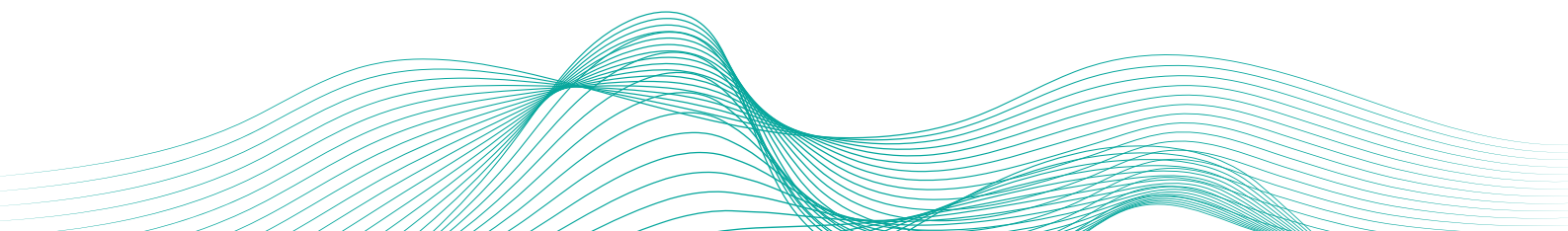
## 3. ABRANGÊNCIA

Estes controles se aplicam a todos os usuários, internos ou externos, que utilizam os recursos tecnológicos da PGE-CE.

## 4. CONTROLE DE ACESSO

### **Senhas de Uso Normal (usuários comuns):**

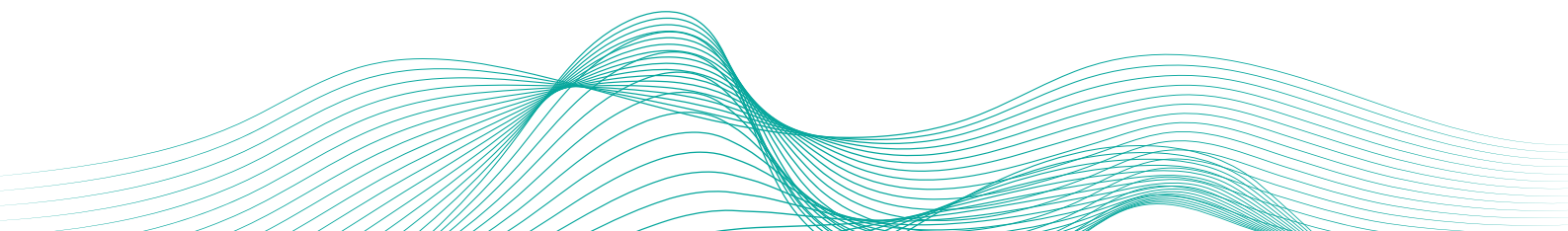
- 4.1. O usuário é responsável exclusivo pelo uso de suas credenciais de acesso. Considerando que a senha é a principal ferramenta de autenticação, ela deve ser individual, intransferível e mantida em segredo, sendo o usuário responsabilizado por qualquer transação efetuada durante o seu uso;
- 4.2. O gestor imediato será responsável pelas contas de acesso pertencentes à sua área e/ou setor, sendo sua a responsabilidade de solicitar a criação, com os acessos necessários, e informar sobre o desligamento dos usuários;
- 4.3. Para a criação, o gestor imediato deverá solicitar à Coordenação de TI, por meio de chamado, informando: Nome completo do usuário, Setor, Permissões de acesso à rede e quais sistemas internos serão utilizados;



- 4.4. As solicitações de recuperação de senhas, por esquecimento ou outro motivo, devem ser realizadas através da Central de Serviços ou através da geração de senha automatizada, quando disponível (ex: esqueci minha senha) e seguirão um procedimento de validação de informações do usuário, para serem fornecidas senhas iniciais temporárias com a obrigatoriedade da troca no primeiro acesso;
- 4.5. As senhas iniciais devem ser fornecidas diretamente aos usuários e configuradas de forma que, no primeiro acesso, a solicitação de troca ocorra automaticamente;
- 4.6. A senha não deverá ser revelada por telefone, e-mail, formulários, questionários, ou até mesmo para colegas de trabalho;
- 4.7. A senha não deverá ser armazenada em local visível, no computador ou em navegadores de internet;
- 4.8. A senha deverá conter, no mínimo, 8 (oito) caracteres, sendo estes definidos por letras, números e caracteres especiais;
- 4.9. As senhas devem ser individuais, secretas, intransferíveis e ser protegidas com grau de segurança compatível com a informação associada.
- 4.10. Todas as senhas de acesso à rede, sistemas e serviços deverão ser trocadas a cada 6 meses;
- 4.11. As contas de usuário que ficarem inativas por mais que 90 (noventa) dias corridos deverão ser bloqueadas;
- 4.12. Os sistemas, serviços e dispositivos do ambiente tecnológico da PGE-CE devem ser configurados para que os padrões mínimos de senha forte sejam exigidos na criação e autenticação;

#### Senhas de Uso Privilegiado (usuários administradores):

- 4.13. Os acessos privilegiados, por questões de segurança, devem ser realizados por uma quantidade mínima de usuários, que terão perfis de administradores e autorização de acesso para essas funcionalidades;
- 4.14. As senhas não devem ser introduzidas em linhas de comando abertas (códigos fontes), mas, caso seja necessário, devem ser criptografadas e consideradas “contas de serviço”;
- 4.15. As senhas de acesso privilegiado, aquelas que possuem acesso irrestrito aos serviços e servidores da rede, deverão conter no



- mínimo 10 (dez) caracteres, compostos por caracteres, números e símbolos;
- 4.16. As contas administrativas não poderão conter em sua formação, algo que as identifique (Ex.: Admin, Adm, Administrador, Administratoꝝ etc);
  - 4.17. Deverá ser guardado um histórico das últimas 9 (nove) senhas, a fim de que as senhas anteriores não possam ser reutilizadas;
  - 4.18. As senhas de administradores de servidores e de domínios devem ter validade de 90 (noventa) dias;
  - 4.19. As senhas de administrador local terão validade indeterminada;

#### Boas práticas para a Criação de Senhas:

- 4.20. Deve-se utilizar:
  - a. Números aleatórios;
  - b. Diferentes tipos de caracteres;
  - c. Caracteres especiais;
  - d. Frase longa contendo letras e números;
  
- 4.21. Deve-se evitar a utilização de:
  - a. Nomes, sobrenomes, nomes de contas de usuários e dados de membros da família (ex.: Rodrigo, Marques, etc.);
  - b. Números de documentos ou de telefone;
  - c. Placa de carros;
  - d. Datas de aniversário;
  - e. Sequência de teclado (ex.: qwertpoiuy);
  - f. Palavras do dicionário;
  - g. Times de futebol, música, personagens de filmes, etc.

