POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE EDUCAÇÃO DE PERNAMBUCO

PC01 – POLÍTICA DE USO DE SENHAS

Faça disso um hábito!

HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
15/02/17	1.0	Versão elaborada e publicada	Equipe de Elaboração
31/07/18	2.0	Versão revisada	Equipe de Elaboração

SUMÁRIO

INTRODUÇÃO

As credenciais de acesso (conta de usuário e senha) são mecanismos fundamentais de autenticação. A senha certifica que o usuário é quem diz ser e que tem o direito de acesso ao recurso disponibilizado. Uma senha forte minimiza os riscos e inibe uma ação mal-intencionada; uma senha fraca, por sua vez, pode comprometer todo o ambiente tecnológico da SEE-PE. Por conta disto, todos os usuários que necessitam de acesso restrito devem seguir os padrões estabelecidos nesta política.

Uma senha forte é aquela que é difícil ser descoberta e fácil de ser lembrada. Desta maneira, uma senha deve ser formada por vários mecanismos que a tornem complexa suficiente para um atacante e, por estratégias ou artifícios, que seja fácil de ser lembrada pelo usuário, sem que seja necessário escrevê-la.

OBJETIVO

Estabelecer um padrão de criação e utilização de senhas fortes, no intuito de evitar que pessoas mal-intencionadas descubram-nas e se passem por outras pessoas, acessando, por exemplo, contas de correio eletrônico, de rede, de computador e de sistemas; sites indevidos ou informações privilegiadas da SEE-PE, como se proprietário fosse.

ABRANGÊNCIA

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

DIRETRIZES DO USO DE SENHAS

1. Senhas de Uso Normal

a) 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;

b) As senhas não devem ser trafegadas em mensagens de e-mail ou em outros formulários de uso de comunicação eletrônica;

c) Os sistemas, serviços e dispositivos do ambiente tecnológico da SEE-PE devem ser configurados para que os padrões mínimos de senha forte sejam exigidos na criação e autenticação. A descrição das regras de senha forte deve constar em **documento interno da SEE-PE;**

d) As solicitações de acesso devem ser realizadas através da Central de Serviços e autorizadas pelo gestor da área ou superior, através de formulário específico a ser arquivado para fins de auditoria;

e) 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 (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;

f) As senhas iniciais devem ser fornecidas diretamente aos usuários e configuradas de forma que, no primeiro acesso, a solicitação de troca ocorra automaticamente.

2. Senhas de Uso Privilegiado

a) Todas as contas e senhas padrões privilegiadas (ex: administrator, sa, root, etc.) devem ser trocadas, renomeadas e desabilitadas;

b) As contas privilegiadas dos administradores dos ambientes, sistemas, aplicativos e dispositivos devem utilizar senha forte, conforme descrição nos procedimentos de uso de senhas.

c) 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;

d) Caso as contas privilegiadas não possam ter as senhas trocadas ou renomeadas, serão desabilitadas e consideradas “contas de serviço” não sendo utilizadas para qualquer tipo de acesso;

e) As senhas não devem ser introduzidas em linhas de comando (códigos fontes) abertas, mas, caso seja necessário, devem ser criptografadas e consideradas “contas de serviço”.

3. Boas práticas para Criação de Senhas

a) Evitar a utilização de:

- Nomes, sobrenomes, nomes de contas de usuários e dados de membros da família (ex.: Maria, Souza, msilva);
- Números de documentos ou de telefone (ex.: 121521487-63, 988356215);
- Placa de carros (ex.: REC1805);
- Datas de aniversários, festivas, etc. ex.: 16/05/2016, 25/12/2016);
- Sequência do teclado (ex.: asdfg123);
- Palavras do dicionário (ex.: Paralelepípedo);
- Nomes de times de futebol, de música, de produtos, de personagens de filmes (ex.: Garota de Ipanema, GGTISee, Mickey, Mcdonalds).

b) Utilizar:

- Números aleatórios;
- Vários e diferentes tipos de caracteres;
- Caracteres especiais;
- Substituir uma letra por número com semelhança visual;
- Frase longa com letras e números;
- A primeira, segunda ou última letra de uma frase incluindo números (ex.: “Água mole em pedra dura, tanto bate até que fura” pode gerar a senha “Am3Pd,Tba9F”).