Norma para Utilização de Credenciais e Senhas

PREFEITURA

Mais **cidade**. Mais **vida**.

Normativa para Utilização de Credenciais e Senhas da Prefeitura Municipal de Porto Alegre

Secretaria Municipal de Planejamento e Assuntos Estratégicos

Coordenação de Planejamento e Gestão de Tecnologia da Informação e Comunicação

(SMPAE – CGTI)

Versão 1.0

Última atualização 14 de Setembro de 2022

PREMISSAS

Todos os servidores públicos, secretarias, órgãos, fornecedores, prestadores de serviço e demais parceiros vinculados devem ter conhecimento de seu importante papel no contexto de **Segurança da Informação (SI)** sendo um dever seguirem as diretrizes e orientações contidas na **Política de Segurança da Informação (PSI)** em sua íntegra, assim evitando expor a informação e os recursos de processamento a situações adversas como comprometimento, alteração, furto e desvio.

.

CONCEITOS

Com base nas orientações da ISO 27002 esta política objetiva informar aos usuários sobre o correto uso de suas credenciais e senhas e as implicações deste uso, estabelecendo desde já que **TUDO É PROIBIDO, ATÉ QUE EXPRESSAMENTE PERMITIDO**. O contrário pode trazer consequências diversas a **SI**.

Atualmente uma grande parte dos crimes cibernéticos, vem de ataques por engenharia social, ou quebra de senhas fracas. Logo cabe ao usuário manter uma senha de qualidade, em sigilo, protegida, jamais anotada em papel ou registrada em arquivos. Nenhuma instituição séria, correta, vai solicitar que o usuário informe seu ID e senha. Logo, nunca forneça esta informação ou a compartilhe.

Evite o uso de uma senha única para todos os seus acessos eletrônicos. Senhas de redes sociais não devem ser as mesmas da rede de trabalho. A senha da sua conta bancaria não deve ser a mesma do e-mail e assim outros exemplos de cuidados simples, mas que impactam diretamente na eficiência da **SI** como um todo. De nada adiantará a rede **PMPA** e a de seu banco serem altamente protegidas com criptografia e protocolos de segurança, se os demais recursos acessados com a mesma senha não forem. Se a sua senha for capturada, a porta de entrada para todos os demais estará aberta.

DIRETRIZES

- Senhas são de uso pessoal devendo ser preservada a sua confidencialidade;
- Não compartilhar senhas em nenhuma hipótese;
- Não anotar senhas, seja em papel, post-its, arquivos ou dispositivos móveis, salvo se armazenadas de forma segura por métodos aprovados na **PMPA**.
- Selecionar senhas de boa qualidade que:
  - Sejam de fácil lembrança;
  - Não sejam triviais e previsíveis como informações pessoais, datas, nomes e telefones;
  - Não usem palavras comuns ao dicionário para evitar ataques desta natureza (ex: casa123);
  - Não usem caracteres idênticos consecutivos (ex: 8855ab);
  - Utilizem números e caracteres alternados, preferencialmente com letras maiúsculas e minúsculas (ex: Rmt54vd).
- Alterar a senha sempre que existir suspeita de possível comprometimento do sistema ou da própria senha;
- Alterar a senha em intervalos regulares, sendo o tempo máximo recomendado a cada 180 dias;
- As senhas deverão ter um tamanho mínimo de oito caracteres;
- Alterar senhas temporárias no primeiro acesso ao sistema;
- Não reutilizar senhas alteradas anteriormente;
- Não incluir senhas em processos automáticos de acesso ao sistema (ex: armazenadas em macros ou cache de navegador).
- Não deixar cartões de acesso e tokens desacompanhados. Quando for se ausentar leve com você ou guarde em local seguro.

SENHAS QUE NÃO DEVEM SER UTILIZADAS:

- Nome do usuário;
- Identificador do usuário (ID), mesmo que os caracteres estejam embaralhados;
- Nome de membros de sua família ou de amigos íntimos;
- Nomes de pessoas ou lugares em geral;
- Nome do sistema operacional ou da máquina que está sendo utilizada;
- Nomes próprios;
- Datas;
- Números de telefone, de cartão de crédito, de carteira de identidade ou de outros documentos pessoais;
- Placas ou marcas de carro.

TAXONOMIA PARA CRIAÇÃO DE SENHAS:

- Os tipos de caracteres utilizados para a formação da senha devem ser letras maiúsculas e minúsculas, números e pelo menos um caractere especial (!@#$%&*+-);
  - Não são permitidos caracteres acentuados ou “Ç”.

Histórico de Revisões

Versão	Data	Alterações	Autor	Revisor
1.0	14/09/2022	Versão inicial	(CGTI-SMPAE) Eduardo Hoppe Fernando Delazeri	(CGTI-SMPAE) Eduardo Hoppe