Prefeitura Municipal de Maricá

Instituto de Ciência, Tecnologia e Inovação de Maricá

Anexo III - Norma para Credenciais e Senhas

Maricá, abril de 2025

Presidente

Cláudio de Souza Gimenez

Diretor de Infraestrutura

Laercio Aguiar da Rocha

Equipe Técnica

Emerson Lacerda Alencar

Giovanni Di Carlo

Márcio Santarém Nogueira

Histórico de Revisões

Versão	Data	Histórico	Autor	Revisor
1.0	abril de 2025	Versão inicial	Emerson L. Alencar Márcio S. Nogueira	Laércio A. Rocha

Sumário

1. PREMISSAS

1.1. É fundamental que todos os servidores públicos, diretorias, fornecedores, prestadores de serviços e demais parceiros vinculados compreendam o seu papel crucial no contexto da Segurança da Informação (SI). É um dever seguir rigorosamente as diretrizes e orientações estabelecidas na Política de Segurança da Informação (PSI) do ICTIM, a fim de evitar exposição indevida das informações e dos recursos de processamento a situações adversas, tais como comprometimento, alteração, furto e desvio.

2. CONCEITOS

2.1. Com base nas diretrizes da ISO 27002, esta política tem por objetivo informar aos usuários sobre o uso adequado de suas credenciais e senhas, destacando as implicações desse uso. Estabelecemos, desde já, que **tudo é proibido, até que expressamente permitido**. Qualquer violação pode resultar em diversas consequências para a segurança da informação.

2.2. Atualmente, uma parcela significativa dos crimes cibernéticos resulta de ataques por engenharia social ou exploração de senhas fracas. Portanto, é responsabilidade do usuário manter uma senha robusta, mantendo-a em sigilo e protegida, evitando anotá-la em papel ou armazená-la em arquivos. É importante ressaltar que nenhuma instituição séria ou legítima solicitará que o usuário divulgue seu ID e senha. Assim, é fundamental nunca fornecer nem compartilhar essas informações.

2.3. Evite utilizar a mesma senha para todos os seus acessos eletrônicos. É importante manter senhas distintas para diferentes tipos de contas, como redes sociais, ambiente de trabalho e contas bancárias. Este cuidado básico é fundamental para fortalecer a Segurança da Informação como um todo. Mesmo que a rede do seu local de trabalho e a do seu banco sejam altamente protegidas, se utilizar a mesma senha em outros recursos, estará aumentando o risco de acesso não autorizado caso essa senha seja comprometida. Em caso de captura da senha, isso poderá resultar na abertura de portas para acessos não autorizados em diversos outros serviços.

3. DIRETRIZES

3.1. As senhas são de uso pessoal e intransferível. É crucial preservar sua confidencialidade;

3.2. Não compartilhar senhas em nenhuma hipótese;

3.3. Evite anotar senhas em papel, post-its, arquivos ou dispositivos móveis, a menos que sejam armazenadas de forma segura por métodos aprovados pelo ICTIM.

3.4. Selecionar senhas de boa qualidade que:

a. Sejam de fácil lembrança;

b. Não sejam triviais e previsíveis como informações pessoais, datas, nomes e telefones;

c. Não usem palavras comuns ao dicionário para evitar ataques desta natureza (ex: casa123);

d. Não usem caracteres idênticos consecutivos (ex: 8855ab);

3.5. Utilizem números e caracteres alternados, preferencialmente com letras maiúsculas e minúsculas (ex: Rmt54vd).

3.6. Alterar a senha sempre que existir suspeita de possível comprometimento do sistema ou da própria senha;

3.7. Alterar a senha em intervalos regulares, sendo o tempo máximo recomendado a cada 180 dias;

3.8. Alterar senhas temporárias no primeiro acesso ao sistema;

3.9. Não reutilizar senhas alteradas anteriormente;

3.10. As senhas deverão ter um tamanho mínimo de oito caracteres;

3.11. Não incluir senhas em processos automáticos de acesso ao sistema (ex: armazenadas em macros ou cache de navegador);

3.12. 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:

3.13. Nome do usuário;

3.14. Identificador do usuário (ID), mesmo que os caracteres estejam embaralhados;

3.15. Nome de membros de sua família ou de amigos íntimos;

3.16. Nomes de pessoas ou lugares em geral;

3.17. Nome do sistema operacional ou da máquina que está sendo utilizada;

3.18. Nomes próprios;

3.19. Datas;

3.20. Números de telefone, de cartão de crédito, de carteira de identidade ou de outros documentos pessoais;

3.21. Placas ou marcas de carro.

Taxonomia para criação de senhas:

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

3.23. Não são permitidos caracteres acentuados ou “Ç”.