



POLÍTICA DE SENHAS

segurança da informação

1 VISÃO GERAL

1.1 Propósito da política

Senhas são uma parte importante dos esforços feitos pelo **MPSC** para proteger os sistemas de TI e os ativos de informação, garantindo que apenas indivíduos autorizados possam acessar estes sistemas e ativos. Se um terceiro tiver posse dela pode agir em seu nome e em nome do Ministério Público Catarinense e a sociedade é prejudicada.

No entanto, o **MPSC** reconhece que a senha tem sérias fraquezas como um controle de acesso. Para sistemas de maior risco, serão considerados outros métodos de autenticação ou controles compensatórios que fornecem níveis maiores de confiança e responsabilização.

Ainda assim, virtualmente todos os sistemas do **MPSC** ainda dependem apenas de senhas. Esta política tem o propósito de abordar as suas fraquezas estabelecendo melhores práticas para a composição, o tempo de vida e o uso geral de senhas.

1.2 Pessoas afetadas

Todos os colaboradores da força de trabalho do **MPSC** (incluindo contratados, estagiários e terceirizados) que têm direito de acesso a sistemas e informações da instituição são afetados por esta política. Entendemos como desafios a resistência que alguns usuários podem ter a adotar senhas muito complexas e o compartilhamento de senhas para resolver necessidades que a instituição e a TI não conseguem atender de forma flexível ou ágil o bastante. Estas questões devem ser tratadas pelas áreas envolvidas com consistência e reconhecida relevância.

1.3 Estrutura da política

Esta política possui as seguintes seções:

1. Visão Geral

2. A Política

3. Responsabilidades dos usuários finais

4. Responsabilidades dos operadores de suporte

5. Responsabilidades dos desenvolvedores e administradores de sistemas

1.4 Garantia de cumprimento

Esta política será garantida por controles técnicos sempre que for viável, como indicado no texto.

Em outros casos, a chefia imediata deverá zelar pelo cumprimento da política quando viável, sem esbarrar no sigilo da própria senha, especialmente no tocante a casos em que tome conhecimento do mau uso da senha.

Todos os colaboradores têm a responsabilidade de imediatamente reportar para a chefia qualquer caso conhecido de não conformidade com a política.

1.5 Consequências do não cumprimento

Infrações à esta política podem resultar em procedimento disciplinar, conforme previsões nas leis (Lei n. 12.527/2011, Lei n. 8.429/1992 e Lei Estadual n. 6.745/1985), sem prejuízo de outras legislações aplicáveis e sob o rito da Lei Complementar n. 491/2010.

Em alguns casos, a infração pode constituir crime, sendo tratado de acordo com a norma penal.

1.6 Linguagem

Nas seções de Responsabilidades desta política (3, 4 e 5), as expressões “**precisa**”, “**não pode**”, “**deve**”, “**não deve**” e “**pode**” devem ser interpretadas como segue:

- “**Precisa**” e “**não pode**” significam que a conformidade com a regra da política é obrigatória.
- “**Deve**” e “**não deve**” significam que a conformidade com a regra da política é fortemente recomendada. Embora essas recomendações

não são requeridas se questões técnicas, operacionais ou de negócio as tornem inviáveis, em caso de auditoria ou levantamento de conformidade os responsáveis pela desconformidade podem ser citados para esclarecer as razões.

- “**Pode**” significa que a conformidade com a regra da política é recomendada, mas opcional.

2 A POLÍTICA

As subseções a seguir apresentam as disposições, os princípios e as diretrizes da política de senhas de uso pessoal.

2.1 Confidencialidade

Uma senha pessoal pode efetivamente autenticar apenas se é conhecida única e exclusivamente pelo usuário titular. Usuários finais deverão garantir a confidencialidade de suas senhas em qualquer momento. Administradores de sistemas e desenvolvedores garantirão que os sistemas não armazenem senhas em texto claro.

Procedimentos administrativos que precisem de uma exceção temporária a este princípio serão mantidos em um mínimo absoluto.

2.1.1 EXCEÇÃO À CONFIDENCIALIDADE

Quando um operador manualmente reseta uma senha de usuário ou cria uma nova conta, ele **precisa** informar o usuário. Neste ponto a senha é necessariamente do conhecimento de duas pessoas. O sistema precisa sempre forçar o usuário a trocar a senha quando receber uma gerada pela TI.

2.2 Construção da senha

Requisitos de comprimento e complexidade da senha oferecem resistência a tipos comuns de ataques. Por motivos de restrições tecnológicas, as regras de construção de senha podem variar de um sistema para outro, mas elas irão atender (ou exceder) estes requisitos sempre que possível.

O **MPSC** reconhece que senhas longas e complexas podem ser difíceis para os usuários se lembrarem, e, portanto, esta política oferecerá orientações para criação de senhas memorizáveis que atendam a estes requisitos.

2.2.1 REGRAS DE CONSTRUÇÃO DE SENHA

Uma senha **deve** consistir de:

- Dez (10) ou mais caracteres
- Utilizar pelo menos três, das quatro opções a seguir:
 - letras maiúsculas
 - letras minúsculas
 - numerais (de 0 a 9)
 - caracteres especiais ([!{}#%*+=_-/\ | ?&.,;:@&\$, etc)

Uma senha **não deve** ser apenas uma palavra de dicionário.

O usuário **não pode** utilizar seu nome ou *login* como parte da senha.

Uma senha **não deve** incluir nada que seja significativo para o usuário, como um nome (real ou fictício), uma data (como aniversários), números de telefone, placas de carro, etc.

Uma senha **não deve** constar na lista das senhas conhecidas mais usadas, disponibilizada pela COTEC.

Uma senha **não deve** ser a simples repetição de caracteres (ex: ABC1abc1A-BC1), assim considerada quando a senha contiver um arranjo de mais de 3 caracteres que ocorra mais de uma vez.

2.3 Alteração e reuso de senha

Os usuários **precisarão** trocar suas senhas periodicamente, para minimizar a janela de oportunidade para um invasor que tenha descoberto a senha de um usuário.

A nova senha **precisa** ser completamente diferente de qualquer senha usada recentemente.

2.3.1 REGRAS DE ALTERAÇÃO E REUSO DE SENHA

A senha expira em 2 anos e **precisa** ser trocada.

A nova senha **precisa** ser diferente das 6 últimas senhas usadas.

A nova senha **não deve** ter mais do que 4 caracteres contíguos existentes na senha atual.

Por exemplo, se a sua senha é “antiLope1000”, uma nova senha “antiLope2000” é inaceitável, mas “antiApex8080” não.

2.4 Limite de tentativas

O sistema permitirá 10 tentativas de login antes de suspender o usuário. Caso seja suspenso ele deverá entrar em contato com o Serviço de Suporte ao Usuário para reativar o acesso.

Esta medida é uma proteção contra programas que tentam descobrir a senha testando várias possibilidades.

2.5 Armazenamento de senhas

Os sistemas **não poderão** armazenar senhas em texto claro (não criptografado).

Os sistemas **devem** utilizar uma transformação criptográfica irreversível aprovada para proteger as senhas dos usuários.

Os sistemas que armazenam as senhas de usuários para intermediar e entregar essas senhas para outros sistemas em nome do usuário, **precisarão** usar um algoritmo criptográfico reversível aprovado.

3 RESPONSABILIDADES DOS USUÁRIOS FINAIS

Se você é um usuário final dos sistemas do **MPSC**, você tem as seguintes responsabilidades no que concerne a senha utilizada.

Estas responsabilidades se aplicam mesmo que o sistema não force a aplicação das regras.

a) Você **precisa** manter sua senha confidencial a todo tempo.

O uso da senha é pessoal e por isso não pode ser compartilhada.

Ela atribui a sua identidade às ações realizadas pelo seu login.

b) Você **não pode** revelar sua senha a ninguém, incluindo a chefia e o pessoal de suporte técnico, mesmo que estes exijam.

Se você for exigido a entregar a senha, **deverá** acionar a **Coordenação de Inteligência e Segurança Institucional** imediatamente.

c) Você **não pode** usar em qualquer sistema ou site externo (incluindo e-mail, internet banking e redes sociais) uma senha que você utilize em qualquer sistema do **MPSC**.

Uma senha única evita que vazamentos na internet exponham o seu acesso na instituição.

d) Você **não deve** fazer anotação de sua senha, seja em papel, em arquivos ou em aplicativos.

Caso seja **inevitável** manter uma anotação sobre a senha, faça-a com a devida diligência e cuidado:

- 1 Mantenha a anotação segura fisicamente, em uma carteira por exemplo, e trate-a como algo de alto valor.
- 2 Evite identificar a anotação como sendo de uma senha e/ou onde ela é usada.
- 3 Ao invés de escrever a senha em si, anote dicas que ajudem a lembrá-la.
- 4 Em qualquer caso, você **não pode** ter a anotação em qualquer lugar perto do computador ou mesa de trabalho, mesmo que "escondido", por exemplo, sob o mouse pad ou dentro de uma gaveta.

5 Criando uma senha segura e fácil de lembrar, você pode evitar a necessidade de anotá-la em papel. A COTEC disponibilizará orientações para tal.

e) Você **pode** utilizar um aplicativo gerenciador de senhas, desde que reconhecido por sua confiabilidade e desenvolvido especificamente para esse propósito, o qual deverá utilizar criptografia forte para proteger as senhas.

f) Você **não pode** usar a opção de “lembrar senha” em qualquer computador que não seja de seu uso exclusivo e em perfil protegido pela própria senha de rede.

g) Você **precisa** escolher uma senha que atenda ou exceda os requisitos elencados na seção 2.2.1 - Regras de construção de senha.

Esta responsabilidade é sua, mesmo se um sistema específico não exigir a aplicação das regras.

Um operador de suporte técnico, administrador de sistema ou outro usuário nunca devem pedir que você escolha uma senha que não atenda aos requisitos. Se isto acontecer, você **precisa** acionar a **Coordenadoria de Inteligência e Segurança Institucional** imediatamente.

h) Você **precisa** fazer trocas de senhas de acordo com a seção 2.3.1 - Regras de alteração e reuso de senha.

i) Você **deve** utilizar sua senha apenas em dispositivos que você confia, como o seu próprio computador, com antivírus atualizado.

j) Caso você suspeite que sua senha tenha sido violada você **deve** trocá-la imediatamente.

4 RESPONSABILIDADES DOS OPERADORES DE SUPORTE

Se você é um operador de suporte do **MPSC**, ou um administrador de sistemas realizando suporte, você tem as seguintes responsabilidades no que concerne às senhas de qualquer sistema do **MPSC** que você suporte.

a) Quando um usuário pede que você resete a senha, você **precisa** comprovar a identidade alegada pelo usuário de acordo com os procedimentos documentados no **Guia de operador de suporte para redefinição de senhas de usuário**.

b) Você **não pode** pedir ao usuário que revele sua senha.

c) Se o usuário oferecer a senha para qualquer fim, inclusive resolver um problema, você **deve** negar e instruí-lo de que deve manter a confidencialidade e observar esta política.

d) Se mesmo assim a senha deixar de se tornar apenas do conhecimento de seu titular, você deve imediatamente redefinir a senha do usuário de acordo com o **Guia de operador de suporte para redefinição de senhas de usuário** e entrar em contato com usuário informando-o do vazamento.

e) Caso haja suspeita de violação de senha, o gestor da área deverá solicitar ao Serviço de Atendimento ao Usuário que redefina imediatamente a senha, caso em que o usuário deverá ser notificado.

5 RESPONSABILIDADES DOS DESENVOLVEDORES E ADMINISTRADORES DE SISTEMAS

Se você é um desenvolvedor ou administrador de sistemas, você tem as seguintes responsabilidades no que concerne às senhas de qualquer sistema do **MPSC** que você sustente, desenvolva ou mantenha.

Nota: Se a conformidade com (a), (c), (f), (g), (h), ou (i) não é tecnicamente viável por limitações do sistema, entre em contato com o Gerente de Segurança da Informação e Gestão de Riscos para acordar e documentar a exceção.

a) Você **precisa** configurar cada sistema para que exija que qualquer senha de usuário atenda aos requisitos de tamanho e complexidade elencados na seção 2.2.1 - Regras de construção de senha.

b) Você é **encorajado** a criar senhas maiores do que o tamanho mínimo exigido, desde que não tenha problemas para lembrar ou use um aplicativo gerenciador de senhas.

c) Você **deve** configurar cada sistema para que exija que qualquer

senha de usuário atenda aos demais requisitos de senha elencados na seção 2.2.1 - Regras de construção de senha.

d) Você **precisa** configurar cada sistema para expirar a senha do usuário a cada 2 anos.

e) Você **deve** configurar cada sistema para impedir o usuário de usar uma de suas últimas 6 senhas.

f) Você **deve** configurar cada sistema para que impeça o usuário de escolher uma nova senha que tenha mais do que 4 caracteres contíguos existentes na senha atual.

g) Você **precisa** configurar o campo de senha em um painel de login para mascarar a senha digitada pelo usuário para minimizar o risco de observação oportunista por outros.

h) Você **precisa** configurar cada sistema para permitir 10 tentativas sucessivas de login. Se a senha não for correta na 10ª tentativa, o sistema deve suspender a conta, de forma que o usuário terá que contatar o Serviço de Atendimento ao Usuário.

i) Você **precisa** implementar uma transformação criptográfica aprovada para proteger as senhas de usuários em cada sistema.

j) Você **precisa** implementar criptografia reversível aprovada para proteger senhas de usuários em sistemas que armazenam as senhas de usuários para intermediar e entregar essas senhas para outros sistemas em nome do usuário.

k) Todas as contas existentes **precisam** ter a sua senha obrigatoriamente redefinida, no prazo de 6 meses da entrada em vigor desta política, para garantir conformidade e mitigar risco residual de vazamento.

l) A COTEC **precisa** aplicar e manter uma política de configuração dos computadores para que o sistema bloqueie a tela após um período de inatividade de 10 minutos, exigindo a senha de rede do usuário para desbloqueio.

m) A COTEC **precisa** aplicar e manter uma política de configuração dos dispositivos móveis para que o sistema bloqueie a tela após um período de inatividade, não superior a 5 minutos, exigindo um desafio de autenticação para desbloqueio.

5.1 Requisitos para sistemas de terceiros

Todos os requisitos **obrigatórios** desta seção (isto é, aqueles qualificados com “**precisa**” e “**não pode**”) constituem parte da especificação mínima de segurança para softwares e sistemas de terceiros que o **MPSC** adquire e implementa. Isto é, é essencial que o sistema permita que administradores e desenvolvedores de sistema cumpram estas responsabilidades.

Nota: Se um sistema de terceiro não puder atender a especificação mínima de segurança, entre em contato com o Gerente de Segurança da Informação e Gestão de Riscos para acordar e documentar a exceção.

Todos os requisitos opcionais desta seção (isto é, aqueles qualificados com “**deve**” e “**não deve**”) constituem funcionalidades desejáveis dos sistemas de terceiros. Os sistemas que armazenam as senhas de usuários para intermediar e entregar essas senhas para outros sistemas em nome do usuário, precisarão usar um algoritmo criptográfico reversível aprovado.