Política de Senhas Aprova

Versão 02 - 06/2026

1. INTRODUÇÃO

1.1. O Aprova utiliza diversos sistemas informatizados em sua rotina operacional. Estes sistemas informatizados auxiliam na organização de notas, comunicação organizacional, gerenciamento de projetos, suporte ao cliente, organização de vendas, entre outros.

Assim sendo, dependendo da atribuição organizacional de um colaborador ou prestador, este terá credenciais de acesso em sistemas informatizados da rotina operacional.

Entre os sistemas que compõem nosso stack operacional, destacamos: Slack, Google Workspace, Notion, Salesforce, Movidesk, Omie, Jira e outros.

1.2. As credenciais de acesso (usuário e senha) individuais, são essenciais para garantir a segurança de dados do ambiente de trabalho. A senha busca certificar que o usuário é quem diz ser e que tem o direito de acesso a ferramenta.

O uso de uma senha forte minimiza os riscos e inibe uma ação mal-intencionada; uma senha fraca, por sua vez, pode comprometer todo o ambiente de trabalho.

1.3. Cada colaborador é responsável por todas as suas senhas de acesso, que são pessoais, intransferíveis e de uso exclusivo deste, que se responsabiliza pelo uso indevido destas, além de se comprometer a mantê-las em sigilo e armazená-las em segurança.

1.4. Para tanto, as senhas de acesso de plataformas e ferramentas digitais do ambiente de trabalho operacional do Aprova devem seguir os padrões de segurança aqui definidos.

2. FINALIDADE

2.1. Fixa um padrão de criação e reformulação de senhas fortes, no intuito de evitar que pessoas mal intencionadas consigam acessar, por exemplo: contas de correio eletrônico, de rede, de computador e de sistemas; sites indevidos ou informações privilegiadas do Aprova, como se este fosse o proprietário.

3. ABRANGÊNCIA

3.1. As regras e diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores do Aprova, membros do conselho, diretores, gestores, colaboradores, e prestadores de serviços do Aprova.

4. DIRETRIZES DO USO DE SENHAS

4.1. O usuário será o único responsável pelo uso e armazenamento de suas credenciais de acesso.

4.2. Considerando que a senha é a principal ferramenta de autenticação, esta deve ser individual, intransferível e mantida em sigilo, sendo o usuário responsável por transação que for efetuada durante o seu uso. Portanto, a senha não deve ser revelada, emprestada, disponibilizada nem divulgada a ninguém.

4.3. As senhas não devem ser trafegadas em mensagens de e-mail, em aplicativos de mensagens instantâneas, não devem ser anotadas e ou armazenadas em dispositivos móveis, salvo se houver algum tipo de ferramenta ou aplicativo específico para tal funcionalidade que conte com criptografia forte, para tanto, indicamos algumas ferramentas seguras que podem ser utilizadas para armazenamento e gerenciamento de credenciais e senhas, sendo estas:

4.3.1. **LastPass**; (melhor alternativa)

4.3.2. Kaspersky Password Manager;

4.3.3. Bitwarden;

4.3.4. Zoho Vault.

4.4. Em caso da necessidade de transmissão de senha para um usuário através de mensagem instantânea, a mensagem deverá ser apagada tão logo ocorra o recebimento.

4.5. Em caso de usuários de sistemas que possuem uso compartilhado, a nota que contiver a credencial de uso compartilhado deverá apenas ser compartilhada com aqueles que devem ter acesso.

4.6. Usuários do Aprova deverão cumprir as seguintes regras para a formulação de suas senhas:

4.6.1. Conter pelo menos 3 das 4 diretrizes abaixo:

4.6.1.1. Conter pelo menos uma letra maiúscula;

4.6.1.2. Conter pelo menos uma letra minúscula;

4.6.1.3. Conter números (0 a 9);

4.6.1.4. Conter símbolos, incluindo:

! @ # $ % ^ & * - _ + = { } | \ : ‘ , . ? / ` ~ “ < > ( );

4.6.1.5. Tamanho de no mínimo 8 caracteres;

4.6.1.6. Não é permitido utilizar as 5 últimas senhas cadastradas;

4.6.1.7. Responsável alterar a senha a cada 90 (noventa) dias;

4.6.2. É sabido que alguns sistemas informatizados podem conter restrições de caracteres e aceitarem apenas números, nestes casos específicos, as diretrizes acima podem ser flexibilizadas para a criação da senha.

4.7. Caso algum colaborador ou prestador tenha problema com um acesso de credencial, ou tenha sido vítima de vazamento ou violação de credencial, deverá comunicar a situação tão logo tome conhecimento através dos canais oficiais:

4.7.1. Canal “data-and-ethics” na plataforma “Slack”

4.7.2. E-mail compliance@aprova.com.br

4.8. Ao realizar o primeiro acesso aos sistemas, o usuário deverá criar sua senha inicial seguindo todos os padrões mínimos definidos no item 4.3.1, esta solicitação de troca ocorrerá automaticamente.

5. SENHAS DE USO PRIVILEGIADO

5.1. Todas as contas privilegiadas (ex: Administrador do sistema) devem apenas ser atribuídas para aqueles usuários cuja função necessite deste acesso privilegiado.

5.2. Os gestores serão responsáveis pela organização de contas de uso

privilegiados de seus times, realizando a atribuição destas para os usuários adequados.

6. BOAS PRÁTICAS PARA CRIAÇÃO DE SENHAS

6.1. Ao se criar uma senha deve-se evitar a utilização de: Nomes, sobrenomes, nomes de contas de usuários e dados de membros da família, números de documentos, números de telefone, placa de carros e datas comemorativas; Sequência de alfabeto ou do teclado (ex.: asdfg123, qwerty); Palavras do dicionário, nomes de times de futebol, de produtos, de personagens de filmes, etc.

6.2. Devemos utilizar: Números aleatórios; Vários e diferentes tipos de caracteres; Caracteres especiais; Substituição de uma letra por número com semelhança visual;

A primeira, a segunda ou a última letra de cada palavra. Exemplo: com a palavra "Dream Theater" você pode gerar a senha "$Dre4MtH34ter!", adicionando sempre símbolos em sua senha.

7. PERDA DA CREDENCIAL

7.1. No caso de perda da credencial o usuário deverá avisar imediatamente em um dos seguintes canais:

7.1.1. Canal “data-and-ethics” na plataforma “Slack”

7.1.2. E-mail compliance@aprova.com.br

7.2. Desligamento / Remoção do acesso

Em casos de interrupção de vínculo do usuário com a Aprova, deverá ser solicitado aos responsáveis pela gestão de acesso a remoção de todos os acessos com pelo menos um dia útil de antecedência;

7.3. A área de Recursos Humanos (RH) poderá solicitar, de forma proativa, a revogação de acessos;

7.4. A conta deve ser inativada de forma imediata pela equipe responsável e consequentemente bloqueados os acessos em todos os recursos tecnológicos e áreas de trabalho do Aprova.

8. DESVIO E EXCEÇÃO

8.1. Todo e qualquer desvio e/ou exceção deve ser comunicado ao Encarregado de Dados, no canal “data-and-ethics” na plataforma “Slack”, ou no E-mail compliance@aprova.com.br, que fará a devida avaliação;

8.2. Qualquer uso indevido de suas credenciais, seja intencional ou não, será escalado ao ao gestor imediato e ao Comitê de Ética, para que sejam tomadas todas as medidas administrativas e/ou legais cabíveis em cada caso.