

CEDIP

**Centro de Digitalização
do Estado do Paraná**



IMPLEMENTANDO A COMPLEXIDADE DE SENHA NO DOCUWARE

Docuware



Complexidade de Senhas

IMPORTÂNCIA DE SENHAS SEGURAS PARA ACESSO A SISTEMAS

As senhas seguras desempenham um papel fundamental na proteção de informações pessoais e organizacionais em ambientes digitais. A seguir, destacamos a importância de utilizar senhas robustas ao acessar sistemas:

- 1. Proteção de Dados Sensíveis:** Senhas fortes ajudam a proteger dados confidenciais, como informações financeiras, registros pessoais e dados empresariais críticos, contra acessos não autorizados.
- 2. Prevenção de Acesso Não Autorizado:** Um sistema de segurança baseado em senhas eficaz reduz significativamente o risco de invasões, garantindo que apenas usuários autorizados possam acessar determinadas áreas do sistema.
- 3. Mitigação de Riscos de Fraude:** Senhas fracas são um dos principais alvos de hackers. Usar senhas complexas e únicas dificulta tentativas de fraudes e roubo de identidade.
- 4. Conformidade com Regulamentações:** Muitos setores têm regulamentações rigorosas sobre segurança de dados. O uso de senhas seguras é muitas vezes um requisito para atender a normas de compliance e proteger a integridade das informações.
- 5. Aumento da Confiança do Usuário:** Quando os usuários percebem que um sistema adota práticas de segurança rigorosas, como a exigência de senhas fortes, isso aumenta a confiança na plataforma e na proteção de seus dados.
- 6. Facilidade na Recuperação de Contas:** Senhas seguras frequentemente são associadas a métodos de autenticação adicionais (como a autenticação em duas etapas), facilitando a recuperação de contas em caso de esquecimento.
- 7. Educação em Segurança Cibernética:** Promover o uso de senhas seguras também incentiva uma cultura de conscientização sobre segurança cibernética, educando usuários sobre práticas que ajudam a proteger não apenas suas contas, mas também a rede como um todo.
- 8. Prevenção de Ataques Automatizados:** Senhas complexas são mais resistentes a ataques automatizados, como tentativas de força bruta, onde hackers tentam várias combinações até encontrar a correta.

Em resumo, a adoção de senhas seguras é uma das primeiras linhas de defesa na segurança cibernética, essencial para proteger informações sensíveis e garantir a integridade dos sistemas. Investir tempo na criação e manutenção de senhas robustas é um passo fundamental para todos os usuários em um mundo cada vez mais digital.



Complexidade de Senhas

IMPLEMENTANDO A COMPLEXIDADE DE SENHAS NO DOCUWARE

Após a ativação da complexidade de senhas no Docuware, o sistema passará a verificar se a senha inserida pelos usuários durante o login atende às regras de segurança configuradas. Caso a senha esteja em conformidade com as políticas definidas, o login será efetuado normalmente. No entanto, se a senha não atender aos critérios exigidos, o sistema exibirá uma mensagem solicitando que o usuário realize a troca da senha, conforme será detalhado nas páginas seguintes.

REGRAS PARA AS SENHAS NO DOCUWARE

- Complexidade – a senha deverá conter:
 - Letra maiúscula;
 - Letra minúscula;
 - Um número;
 - Caractere especial;
 - Tamanho mínimo de 10 caracteres;
 - Número máximo de tentativas antes de bloquear (5) – refere-se à quantidade de vezes que um usuário pode tentar acessar sua conta antes que seu acesso seja temporariamente bloqueado;
 - Bloqueado por 3 minutos – tempo em que a conta será bloqueada para login após 5 tentativas sem sucesso;
 - Expira em 90 dias – tempo em que a senha terá validade, após esse período a senha terá que ser trocada pelo usuário;
 - Notificação em 7 dias antes de expirar – o sistema irá emitir uma mensagem de expiração de senha, solicitando a troca da mesma.

Complexidade de Senhas

TELA DE LOGIN



A tela de login é a porta de entrada para o sistema DocuWare, permitindo que os usuários acessem suas contas de forma segura e eficiente. A interface é projetada para ser intuitiva, com os seguintes elementos:

Logo do Sistema: Exibido na parte superior da tela, o logo reforça a identidade visual da plataforma.

Campos de Login:

- **Empresa:** Campo para inserção de qual empresa será feito o acesso;
- **Nome do Usuário:** Um campo para inserção do login;
- **Senha:** Um campo protegido que oculta a senha digitada;
- **Esqueceu sua senha?** Um link que envia um e-mail de redefinição de senha – é necessário ter um e-mail cadastrado.
- **Botão de Login:** Um botão destacado que, ao ser clicado, processa as informações fornecidas e direciona o usuário ao painel principal, caso as credenciais estejam corretas.
- **Mensagens de Erro:** Notificações que aparecem de forma clara e visível quando as credenciais estão incorretas ou se há problemas com a conexão, garantindo que o usuário saiba como proceder.

A tela de login é fundamental para garantir uma experiência de usuário fluida e segura, promovendo a confiança no sistema desde o primeiro acesso.



Complexidade de Senhas

TELA DE ATUALIZAÇÃO DE SENHA



A tela de atualização de senha é projetada para permitir que os usuários mudem sua senha de forma fácil e segura. A interface é intuitiva e contém os seguintes elementos:

Logo do Sistema: Exibido na parte superior, reforçando a identidade da plataforma.

Campos de Senha:

- **Organização:** Nome da empresa a qual está fazendo a troca de senha;
- **Nome do usuário:** Login do usuário que fará a troca de senha;
- **Senha Antiga:** Um campo para inserção da senha atual;
- **Nova Senha:** Um campo para criação da nova senha – dentro da política de complexidade de senha;
- **Confirmar a Senha:** Um campo adicional para que o usuário repita a nova senha, assegurando que não haja erros de digitação.
- **Alterar a Senha:** Um botão destacado que, ao ser clicado, valida as informações e atualiza a senha no sistema. Mensagens de sucesso ou erro devem ser exibidas após a ação.

Mensagens de Validação: Feedback em tempo real que indica se a nova senha atende aos critérios de segurança, e se a confirmação está correta.

A tela de atualização de senha é uma parte crucial da experiência do usuário, garantindo que as mudanças sejam feitas de maneira simples e segura, promovendo uma boa prática de gerenciamento de senhas.



Complexidade de Senhas

LINK ESQUECEU SUA SENHA?

Conta do DocuWare

Empresa:

Nome do usuário:

Senha:

[> Esqueceu sua senha?](#)

☐ Manter-me conectado

☐ Abrir o Client em uma nova janela

Login



ESQUECEU SUA SENHA?
O e-mail foi enviado com êxito.

Este aviso informa que um e-mail foi enviado para o endereço cadastrado na sua conta, contendo instruções para redefinir sua senha. Conforme abaixo:

Redefinir sua senha do DocuWare

SD Serviços Gerais Docuware

Para: Seg, 07/10/2024 15:19

[Não sei do que se trata.](#) [Não funcionou.](#) [Não consigo entrar.](#)

Para iniciar o processo de redefinição da senha para sua Conta do DocuWare, clique no link abaixo:
http://localhost/DocuWare/Platform/WebClient/ClientAccount/Login#rp_token=f51a660c-59c2-45b2-81c8-90eaac251ba0
Caso não funcione ao clicar no link acima, copie e cole o URL em uma nova janela do navegador.

Caso você tenha recebido este e-mail por erro, provavelmente outro usuário inseriu seu endereço de e-mail por engano ao tentar redefinir uma senha. Caso você não tenha iniciado a solicitação, não será necessário tomar nenhuma medida e poderá desconsiderar com segurança este e-mail.

[Responder](#) [Encaminhar](#)



Complexidade de Senhas

Siga as orientações abaixo para completar o processo de redefinição:

1. **Verifique sua Caixa de Entrada:** Acesse o e-mail que você usou para registrar sua conta. O e-mail pode ter chegado à sua caixa de entrada, mas também verifique a pasta de spam ou lixo eletrônico caso não o encontre.

2. **Clique no Link de Redefinição:** Dentro do e-mail, você encontrará um link para redefinir sua senha. Clique neste link para ser redirecionado para a tela de criação de uma nova senha.

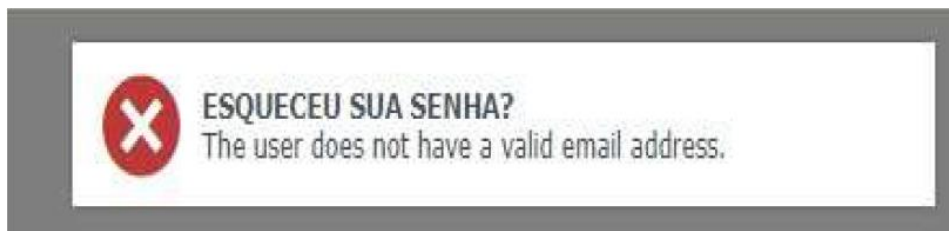
3. **Crie Uma Senha:** Na tela de redefinição, siga os requisitos de segurança para criar uma senha forte e segura. Lembre-se de que sua nova senha deve ser diferente da antiga.

4. **Confirmação de Alteração:** Após inserir e confirmar sua nova senha, você receberá uma mensagem confirmando que a alteração foi bem-sucedida.

Importante:

Segurança da Conta: Se você não solicitou a redefinição de senha, é recomendável alterar sua senha imediatamente e contatar o suporte técnico para relatar a situação.

LINK ESQUECEU SUA SENHA? MAS SEM E-MAIL CADASTRADO



Esta mensagem é apresentada quando um usuário clica em "Esqueceu sua senha?" e tenta solicitar uma redefinição, mas não possui um e-mail cadastrado no sistema. A interface é projetada para ser clara e informativa, com os seguintes elementos:

- **Mensagem de Aviso:** Um texto claro que informa ao usuário de que o e-mail inserido não está cadastrado no sistema. Por exemplo: "O usuário não possui um endereço de e-mail válido."

Sugestões de Ação:

1. **Abrir um Registro de Atendimento ao Cliente** na plataforma XMANAGER: Um chamado para equipe de sistemas solicitando o reset de senha (redefinição) e/ou cadastro de e-mail válido.

Complexidade de Senhas

PLATAFORMA XMANGER: <https://unimedparana.wtisoftware.com.br/login.x>

Autenticação

Usuário

Senha

Fazer login com **Usuário Local** ▼

☐ Login Automático

[Esqueceu sua Senha?](#)

A Unimed Paraná está lhe oferecendo a solução mais conceituada no mercado.
Para qualquer dúvida, sugestão ou suporte envie um email para centralservicos@unimedpr.coop.br

Para informações técnicas, envie um e-mail para centralservicos@unimedpr.coop.br

Service Desk ▼

Service Desk > Chamado > Novo Chamado

Assistente Chamado

O usuário seleciona uma classificação para iniciar a abertura do chamado.

Classificação	Descrição do Chamado	Classificações Associadas
Selecione uma classificação Pesquisar por Classificação Informação não disponível - Classificação do Chamado - COMITÊS CHAMADOS INTERNOS - Assessoria Jurídica - Gestão de Suprimentos - Assessoria de Imprensa - Auditoria Prospectiva - Auditoria Retrospectiva e de Oncologia - Compliance - Contabilidade/ DP - Assessoria Regulamentar - Contas Médicas - Gestão de Operações Administrativa - Programas de Gestão em Saúde - Gestão Financeira - Gestão da Comunicação e Marketing - Gestão da Estratégia e Projetos - Gestão de Serviços Personalizados em Saúde - Gestão de Clientes - Gestão de Intercâmbio e Rede prestadora - Gestão de Negociação e Valor em Saúde - Gestão de Pessoas e NDH Gestão de Processos Cadastrais - CADASTRO - CEDIP - Solicitação		



Complexidade de Senhas

Esta tela tem como objetivo fornecer um feedback claro ao usuário e orientá-lo sobre os próximos passos, garantindo uma experiência mais fluida e evitando frustrações.

SUA SENHA PRECISA SER ALTERADA



SUA SENHA PRECISA SER ALTERADA

A senha não cumpre a política de segurança: Deve ter no mínimo 10 caracteres. É necessário incluir uma letra maiúscula. É necessário incluir uma letra minúscula. É necessário incluir um caractere especial.

Este aviso indica que a sua senha atual não atende aos requisitos de complexidade estabelecidos pelo sistema. A alteração é necessária para garantir a segurança da sua conta e a proteção das suas informações. A seguir, estão os requisitos que sua nova senha deve atender – conforme definido nas REGRAS PARA AS SENHAS NO DOCUWARE:

1. Mínimo de Caracteres: A nova senha deve ter pelo menos 10 caracteres. Isso ajuda a garantir que a senha seja difícil de adivinhar.
2. Uso de Letras: A senha deve incluir letras maiúsculas e minúsculas. Isso aumenta a diversidade dos caracteres e dificulta tentativas de quebra.
3. Inclusão de Números: A nova senha deve conter pelo menos um número. Isso torna a senha mais robusta.
4. Caracteres Especiais: É necessário incluir pelo menos um caractere especial (como @, #, \$, %, etc.). Esses caracteres adicionais ajudam a fortalecer a segurança.

Instruções para Alteração

- Campo para Nova Senha: Insira a nova senha no campo indicado.
- Confirmação da Nova Senha: Repita a nova senha para garantir que não houve erros de digitação.
- Botão de Atualizar: Após preencher os campos corretamente, clique no botão para confirmar a alteração.

Importância da Complexidade da Senha

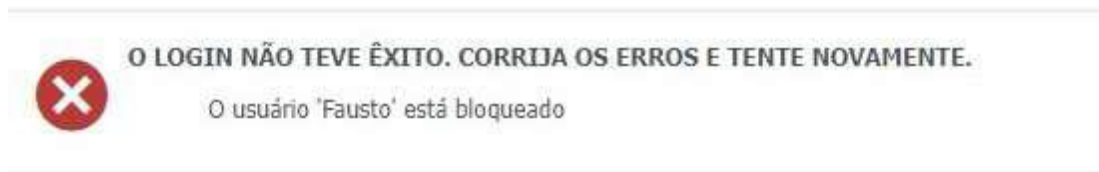
A exigência de senhas complexas é uma medida crucial de segurança. Senhas fortes ajudam a proteger sua conta contra acessos não autorizados e ataques cibernéticos, garantindo a integridade dos seus dados.

Caso tenha dúvidas ou precise de ajuda, entre em contato com o suporte técnico no e-mail: gedfederacao@unimedpr.coop.br



Complexidade de Senhas

O LOGIN NÃO TEVE ÊXITO



Este aviso informa que a tentativa de login não foi bem-sucedida. Essa situação pode ocorrer por diversos motivos, e é importante verificar as informações inseridas. Abaixo estão algumas causas comuns e orientações para resolver o problema:

1. Credenciais Incorretas:

Usuário ou E-mail: Certifique-se de que o nome de usuário ou o e-mail foi digitado corretamente, sem erros de digitação.

Senha: Verifique se a senha está correta, lembrando que as senhas são sensíveis a maiúsculas e minúsculas.

2. Conta Inativa ou Bloqueada:

Se a sua conta estiver inativa ou temporariamente bloqueada por razões de segurança, você não conseguirá acessar. Entre em contato com o suporte técnico para mais informações.

3. Problemas de Conexão:

Verifique sua conexão com a internet. Problemas de conectividade podem afetar a comunicação com o servidor.

4. Limite de Tentativas:

Caso tenha excedido o número máximo de tentativas de login, sua conta pode ter sido temporariamente bloqueada. Siga as instruções fornecidas para desbloqueá-la ou aguarde o período de espera.

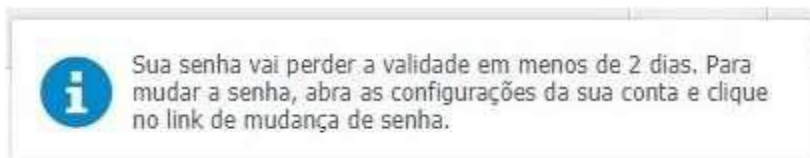
Próximos Passos

- **Reinsérer Credenciais:** Volte à tela de login e insira novamente seu usuário/e-mail e senha, conferindo cada detalhe.
- **Recuperação de Senha:** Se você não conseguir lembrar sua senha, utilize a opção “Esqueci minha senha” para redefini-la.
- **Contato com Suporte:** Se após várias tentativas você ainda não conseguir acessar sua conta, entre em contato com o suporte técnico para assistência.



Complexidade de Senhas

AVISO DE VALIDADE DA SENHA



Este aviso tem o objetivo de informar o usuário sobre a validade da sua senha e orientá-lo a realizar a alteração dentro do prazo. Após o prazo de validade o acesso será bloqueado e a tela de atualização de senha será apresentada.

SENHA EXPIRADA



Esta mensagem é exibida ao usuário quando sua senha atingiu o prazo máximo de validade definido pelo sistema. A senha expirada impede o acesso às funcionalidades até que seja atualizada, garantindo a segurança das contas de usuário.

Usuários de serviço utilizado em integrações podem ser configurados para não expirar a senha, mas não estão isentos das regras de complexidade.

Se você tiver alguma dúvida ou precisar de mais informações, fique à vontade para entrar em contato conosco.

Contato:

CEDIP: CENTRO DE DIGITALIZAÇÃO DO ESTADO DO PARANÁ
E-mail: gedfederacao@unimedpr.coop.br