

SENHA SEGURA NO RHE



BOAS PRÁTICAS

SECRETARIA DA FAZENDA DO ESTADO DO RS
TESOURO DO ESTADO DO RS
RECURSOS HUMANOS DO ESTADO DO RS





POR QUE UMA CAMPANHA DE SEGURANÇA

- Segundo dados da Kaspersky Lab, empresa internacional de segurança virtual, **33% dos incidentes em cibersegurança ocorreram por consequência de falha humana em 2019.**
- A mudança de comportamento humano, com a adoção de dispositivos móveis, é cada vez menos segregada entre vida pessoal e profissional especialmente com o crescimento do Trabalho Remoto.
- O Brasil registrou mais de **8,4 bilhões de tentativas de ataques cibernéticos em 2020** de acordo com estudo da Fortinet Lab.



O **sistema RHE** é uma ferramenta para gestão de recursos humanos, integrando dados e informações pertinentes a todas as funções gerenciais de pessoal, em termos de uma concepção de controle e planejamento, ligada diretamente ao processo de folha de pagamento.





POR QUE SEGURANÇA DE INFORMAÇÕES NO SISTEMA RHE?

A segurança da informação nos Sistemas de Recursos Humanos do Estado visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pelo Estado, além da prestação de serviços e fornecimento de documentos para uso externo. Essas informações versam sobre dados pessoais, funcionais e dos órgãos. Há distinção de tratamento, em especial na LGPD.

Esses pilares da segurança da informação estão intimamente relacionados aos controles de acesso abordados neste manual.



BOAS PRÁTICAS AJUDAM A PROTEGER TODO O SISTEMA

A adoção de práticas rotineiras de proteção aos dados pode ser muito simples, mas gera benefícios importantes para a proteção de toda a rede envolvida no processo.



Confira algumas das principais medidas que podem ser adotadas:

Fique atento aos dados que não possam ser compartilhados com pessoas de outros setores ou externas à organização.

Não anote a senha em papel, mesmo que esse seja guardado em gaveta ou armário, embaixo do teclado ou fixado no monitor, etc. **Apenas memorize.**

Não ignore as solicitações de atualização e **mantenha sempre os softwares atualizados.**

Não disponibilize senhas e logins, mesmo que para colegas de trabalho.

Evite usar **computadores de terceiros** para acesso ao sistema.

Bloqueie o computador ao se ausentar da mesa de trabalho, ainda que rapidamente.

Não utilize redes sociais, sites de bancos ou de compras na rede de trabalho e jamais divulgue informações sigilosas ou faça contatos com desconhecidos nos computadores corporativos.



QUAL O PAPEL DE UMA SENHA NESSE PROCESSO?

A senha é a chave para ingressar no sistema e para incluir, alterar ou excluir dados. Por isso, é tão importante a escolha e proteção de uma senha que deve ser de uso pessoal, intransferível e sem compartilhamento entre colegas. Compartilhar a senha de acesso ao sistema não é uma questão de confiança entre as pessoas.



Responsabilidades do usuário no uso da senha:



É da inteira **responsabilidade do usuário** todo e **qualquer prejuízo causado pelo fornecimento de sua senha pessoal** a terceiros, independente do motivo.

Cabe exclusivamente **ao servidor**, como usuário de sistemas, **a responsabilidade pelo uso indevido de sua senha.**

Juridicamente, **o detentor da senha é responsável por todos os atos praticados por meio dela**, uma vez identificado por ela nos sistemas.

Tudo **o que for registrado com sua senha é de sua inteira responsabilidade**, podendo, até mesmo, fazer com que responda a procedimentos administrativos e jurídicos, quando do uso indevido.

O usuário acessará sua conta através de login e senha e **compromete-se a não informar a terceiros esses dados**, responsabilizando-se integralmente pelo uso que deles seja feito.





Para que os controles de senha funcionem:

Não compartilhe senha.	Altere a senha em intervalos regulares.	Não inclua a senha em processos automáticos de acesso ao sistema (por exemplo, nos favoritos e macros).
Mantenha a confidencialidade da sua senha.	Escolha uma senha de boa qualidade , evitando o uso de senhas muito curtas ou muito longas.	Altere a senha sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha.
Não utilize no sistema senhas usadas em outros acessos de rede, aplicativos, redes sociais ou compras on-line.	Nunca registre a senha em papel.	



RESPONSABILIDADES - POLÍTICA DE SEGURANÇA

ORDEM DE SERVIÇO
Nº 028/1999-2002.

Dispõe sobre o acesso e critérios de utilização dos sistemas informatizados, bem como, sobre as informações geradas, mantidas e tratadas através dos recursos de informática, no âmbito do serviço público estadual e dá outras providências.



COMO ESCOLHER UMA BOA SENHA?

São consideradas boas senhas aquelas que incluem, na composição, letras (maiúsculas e minúsculas), números e caracteres especiais embaralhados, totalizando mais de seis caracteres.

Além disso, saiba **COMO CRIAR** uma senha forte:

- Crie uma senha longa.
- Use uma combinação de palavras aleatórias, como banana, mesa, maçã e porta.
- Combine com letras maiúsculas, números e caracteres especiais para maior segurança.
- Veja se ela não é uma das senhas mais populares do mundo como 1234, abcde.
- Pense em uma frase fácil de recordar: pode ser algo simples, como “Meu filho mais novo é jogador”.
- Transforme a frase em um código usando a primeira letra de cada palavra. No caso da frase acima: Mfmnej. Evite palavras comuns como "senha" ou "minha senha", além de combinações muito usadas.
- O método de criação de senha de frase é muito interessante e pode ajudar a criar uma senha forte e fácil de memorizar. Ele consiste em usar nomes próprios, nomes de empresas, locais, figuras históricas, personalidades famosas, palavras que você conhece em outro idioma, entre outros, para criar a sua senha.





O QUE FAZER QUANDO ESQUECER OU PERDER A SENHA?

Cada Secretaria de Estado e cada empresa do tipo fundação/autarquia possui pelo menos um usuário “administrador de usuários” com permissões para:



1.

Reinicializar a senha de usuário ativo, caso haja esquecimento, desde que o último acesso tenha sido há menos de 45 dias .

2.

Reativar e reinicializar a senha de usuário bloqueado por excesso de tentativas com senha inválida ou por falta de acesso ao sistema há mais de 45 dias.

3.

Reativar totalmente usuário inativo e sem permissões, atribuindo novo pacote de acessos e reinicializando a senha.



Preparamos um manual com dicas de boas práticas ao utilizar o sistema RHE. Para acessar aponte a câmera do seu celular para o QR Code ao lado ou através do link:



https://tesouro.fazenda.rs.gov.br/upload/20210629133732manual_boas_praticas_senha_segura_no_rhe_2.pdf



tesouro.fazenda.rs.gov.br

