SENHA SEGURA NO RHE

MANUAL DE BOAS PRÁTICAS

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

RHE Recursos Humanos do Estado RS

TESOURO do Estado do RS

GOV RS NOVAS FAÇANHAS NA FAZENDA

SENHA SEGURA NO RHE

MANUAL DE BOAS PRÁTICAS

Este manual foi desenvolvido pelo Tesouro do Estado

Subsecretário do Tesouro do Estado
Bruno Queiroz Jatene

Subsecretários Adjuntos do Tesouro do Estado
Eduardo Rosemberg Lacher | Elói Astir Stertz | Guilherme Correa Petry

CONCEPÇÃO, ARGUMENTO E ELABORAÇÃO
Tatiane de Sousa | tatianeps@sefaz.rs.gov.br

TEXTOS E REVISÃO
Nelson Roncarati | nelsons@sefaz.rs.gov.br
Nelson Korman | nelsonak@sefaz.rs.gov.br
Juliana Debaquer | julianad@sefaz.rs.gov.br
Carmen Karina Garcia Paiva | carmengp@sefaz.rs.gov.br
Heloísa Helena Tomaske Claas | heloisac@sefaz.rs.gov.br
Igor Ramos de Oliveira | igoro@sefaz.rs.gov.br

DESIGN GRÁFICO
Kelin Alida Räsch Ströher | kelins@sefaz.rs.gov.br

RHE Recursos Humanos do Estado RS

TESOURO do Estado do RS

GOV RS NOVAS FAÇANHAS NA FAZENDA

APRESENTAÇÃO

Trabalho em rede, aplicativos, páginas na internet são facilidades que se evidenciaram cada vez mais nos últimos anos, sobretudo, a partir da necessidade criada com a Covid-19, que aumentou a demanda por serviços digitais e fomentou o desenvolvimento de novas tecnologias. Por outro lado, empresas, órgãos públicos e cidadãos também ficaram mais expostos a ataques cibernéticos.

No início de 2021, o vazamento de cem milhões de contas telefônicas e a **exposição de dados de 223 milhões de pessoas** acendeu um alerta para os brasileiros. Já no Rio Grande do Sul, um **ataque cibernético** no Sistema Eletrônico de Informação (SEI) do Tribunal de Justiça do Estado do Rio Grande do Sul (TJ/RS) **deixou 75% dos processos sem acesso e tanto o trabalho remoto quanto o uso de estações no TJ de dentro da rede tiveram que ser interrompidos.** Esse não foi o primeiro ataque hacker ao sistema judiciário brasileiro: no ano passado, o Superior Tribunal suspendeu suas atividades após um hacker exigir pagamento para liberação dos dados criptografados.

A Tecnologia da Informação tem papel cada vez mais relevante no trabalho de instituições públicas. No entanto, evidencia-se a necessidade de criar mecanismos para proteção de dados, sob pena de prejuízos para cidadãos, andamento de serviços e, sobretudo, para proteção financeira dos recursos do Estado. Pesquisa da Gartner Group aponta que **70% das ocorrências** de segurança que provocam prejuízos financeiros nos negócios **têm alguma relação com pessoas internas da empresa**.

Em agosto de 2018, foi aprovada a lei nº 13.709, a Lei Geral de Proteção de Dados Pessoais (LGPD), com vigência a partir de agosto de 2020 e que afetou diferentes setores e serviços, e todos os brasileiros, seja no papel de indivíduo, empresa ou governo. Para entender a importância do assunto, é necessário saber que a nova lei pretende um cenário de segurança jurídica, com a padronização de normas e práticas, para promover a proteção, de forma igualitária e dentro do país e no mundo, dos dados pessoais de todo cidadão que esteja no Brasil. E, para que não haja confusão, a lei trouxe de primeira o que são dados pessoais, definiu que há alguns desses dados sujeitos a cuidados ainda mais específicos, como os sensíveis e os sobre crianças e adolescentes, e que dados tratados tanto nos meios físicos como nos digitais estão sujeitos à regulação (https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd). Importante salientar que no seu artigo 52, a Lei trouxe uma série de sanções às infrações cometidas.

Diante do exposto, **este manual pretende estimular boas práticas a fim de aumentar a segurança no sistema RHE - Recursos Humanos do Estado e demais sistemas relacionados**, reduzir as possiblidades de fraudes e aperfeiçoar a escolha e o uso de senhas, além de promover o hábito de vigilância sobre elas, incentivando a utilização de caracteres alfa-numéricos e atualizações periódicas.

O material **destina-se tanto aos usuários da gestão, que realizam consultas e acompanhamento de dados, quanto aos que operam os sistemas, efetuando diversos lançamentos**. Atualmente, nas Secretarias, Fundações e Autarquias que compõem o Executivo Estadual, existem aproximadamente mais de 10.500 usuários ativos. Desde a implantação do RHE, já são mais de 20.000 servidores e estagiários que, em algum momento, utilizaram o sistema.

1. 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.

1.1 O QUE É A INTEGRIDADE DE INFORMAÇÕES?

Consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital.

1.2 O QUE É A CONFIDENCIALIDADE DE INFORMAÇÕES?

Significa a garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, ou façam uso delas, de forma acidental ou proposital, sem que possuam autorização para tal procedimento.

1.3 O QUE É A AUTENTICIDADE DE INFORMAÇÕES?

É a garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações.

1.4 O QUE É A DISPONIBILIDADE DE INFORMAÇÕES?

Consiste na garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, no prazo requerido, durante o período necessário e para a finalidade prevista.

Um elemento essencial da LGPD é o consentir. Ou seja, o consentimento do cidadão é a base para que dados pessoais possam ser tratados. Mas há algumas exceções a isso. É possível tratar dados sem consentimento se isso for indispensável para: cumprir uma obrigação legal; executar política pública prevista em lei; realizar estudos via órgão de pesquisa; executar contratos; defender direitos em processo; preservar a vida e a integridade física de uma pessoa; tutelar ações feitas por profissionais das áreas da saúde ou sanitária; prevenir fraudes contra o titular; proteger o crédito; ou atender a um interesse legítimo, que não fira direitos fundamentais do cidadão, sendo que devem ser utilizados dados anonimizados sempre que for possível.

2. POR QUE É IMPORTANTE ZELAR PELA SEGURANÇA DE INFORMAÇÕES NO RHE?

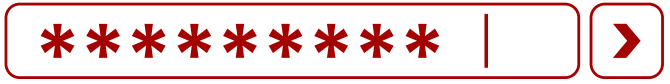
Porque a informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais crítico.

Informações adulteradas, não disponíveis ou sob conhecimento de pessoas de má-fé podem comprometer, significativamente, a credibilidade do serviço prestado e dos servidores envolvidos nos processos.

A LGPD traz em seu art. 2º "A disciplina da proteção de dados pessoais tem como fundamentos:

I. o respeito à privacidade;
II. a autodeterminação informativa;
III. a liberdade de expressão, de informação, de comunicação e de opinião;
IV. a inviolabilidade da intimidade, da honra e da imagem;
V. o desenvolvimento econômico e tecnológico e a inovação;
VI. a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII. os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

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.

3. COMO ACESSAR O SISTEMA RHE?

Siga o passo a passo para acessar o Sistema RHE a partir da Rede RS.

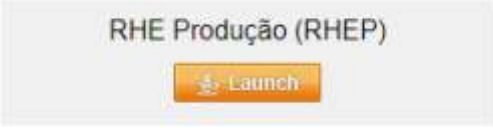
PASSO A PASSO

Para acessar o Sistema RHE a partir da Rede RS, digite o seguinte endereço no navegador para acesso à tela de instruções de instalação do aplicativo:

https://secweb.intra.rs.gov.br/forms/frmservlet?config=rhe-p

1.

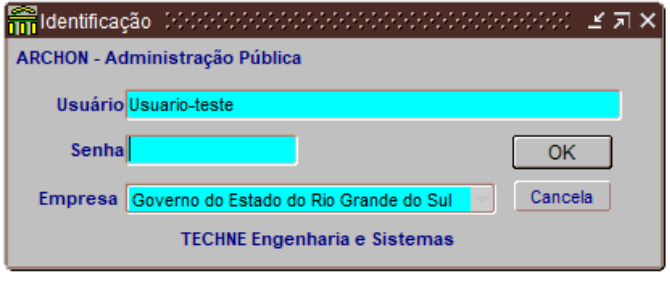
Localize e clique no botão abaixo. Siga o passo a passo sugerido conforme o navegador que estiver utilizando:



2.

Após concluída a instalação, clique no aplicativo salvo na sua área de trabalho. Você receberá a janela de identificação do usuário:

3.



Informe a sua identificação de usuário, selecione a empresa à qual está vinculado, informe a senha de acesso temporária fornecida pelo administrador de segurança do RHE do seu Órgão/Empresa e clique no botão “OK”:

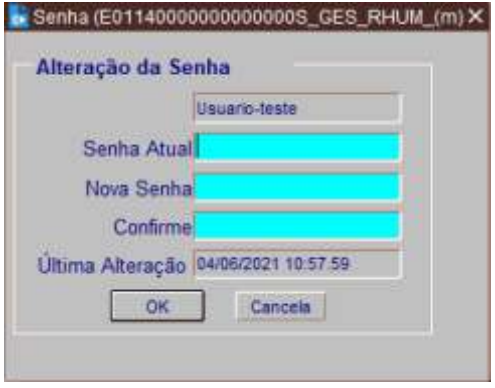
PASSO A PASSO

4.

Ao acessar o sistema pela primeira vez ou após o login ter sido reativado pelo administrador de segurança, o pedido de alteração da senha será solicitado automaticamente.

5.

Informe a senha temporária no campo **"Senha Atual"**, e nos demais cadastre e confirme sua nova senha pessoal conforme orientado pelo administrador de segurança.



6.

Clique no botão OK para confirmar. Você receberá a mensagem de confirmação da atualização.

7.

Clique no botão "OK" para concluir o procedimento e iniciar a sessão no RHE.

ALTERAÇÃO DA SENHA

Para alterar a senha de acesso ao sistema a qualquer momento, utilize o menu: **Archon >Segurança >Usuários>Senha**.
Após clicar no menu, você recebe a janela Senha.

Para alterar a sua senha, siga os passos 5, 6 e 7 do tópico anterior.

4. 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.

5. 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.

Para que os controles de senha funcionem:

Não compartilhe senha.

Mantenha a confidencialidade da sua senha.

Não utilize no sistema senhas usadas em outros acessos de rede, aplicativos, redes sociais ou compras on-line.

Altere a senha em intervalos regulares.

Escolha uma senha de boa qualidade, evitando o uso de senhas muito curtas ou muito longas.

Nunca registre a senha em papel.

Não inclua a senha em processos automáticos de acesso ao sistema (por exemplo, nos favoritos e macros).

Altere a senha sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha.

6. QUAL SENHA É CONSIDERADA FORTE?

Uma boa senha é aquela que diminui as chances de ser descoberta e de fácil lembrança para o usuário. Siga as dicas para construir uma senha forte.

Dicas:

- O ideal é que a senha tenha pelo menos seis caracteres misturando números, letras e caracteres especiais.
- Não convém que você crie uma senha forte se, quando for usá-la, não conseguir recordá-la. Também evite criar uma senha fácil de ser lembrada se ela puder ser facilmente descoberta.

O que evitar na criação da senha:

Não utilize senhas com caracteres seguidos no teclado do computador. Ex.: qwer, zxcv.

Não elabore senhas baseadas em informações pessoais, como nomes, sobrenomes, número de documentos, placas de carros, telefones e datas.

Evite uso de objetos ou locais que podem ser vistos a partir da mesa do usuário (nome de um livro na estante, nome de uma loja vista pela janela).

Não crie senhas com caracteres repetidos ou sequenciais. Ex.: aa22, abcde, ab123.

Não utilize senha com menos de 6 caracteres.

7. 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.

8. 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.

• No primeiro acesso e a cada reinicialização de senha realizada por administrador de usuários, o sistema exigirá a troca da senha provisória.

• Ao trocar de setor, o servidor terá seus acessos removidos e deverá solicitar novo papel* ao seu RH.

• Há usuários que, por atuarem de forma concomitante em áreas e/ou níveis diferentes, podem ter acesso a mais de um "papel", bastando selecionar a opção desejada no botão "cartola".

• No Sistema RHE, é representado pelo símbolo "cartola", localizado na barra de botões do RHE, sendo atribuído ao usuário pelo administrador de segurança da sua Secretaria de Estado ou Fundação/Autarquia observando o nível de responsabilidade e área de atuação ou atividade por ele a ser exercida.

**"Papel" é um conjunto de permissões de acesso ao Sistema RHE que habilita transações para consultas, manutenções, execuções de rotinas e demais funcionalidades necessárias ao exercício de atividades sobre determinado universo de servidores.*

9. 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.

O GOVERNADOR DO ESTADO DO RIO GRANDE DO SUL, no uso de suas atribuições constitucionais;

considerando que os sistemas informatizados, ferramentas e programas de computador foram implantados para agilizar e automatizar as tarefas de suporte técnico e administrativo,

considerando que o processo de informatização é fator determinante para que este Poder Executivo exerça na plenitude suas atribuições legais,

considerando que correio eletrônico (e-mail) e acesso à rede mundial de computadores INTERNET foram exclusivamente disponibilizados para a consecução das atribuições funcionais dos servidores, bem como para agilizar a comunicação entre os diversos órgãos das Administrações Direta e Indireta e possibilitar rápido acesso às informações necessárias para o bom andamento dos trabalhos,

considerando que a administração pública deve obedecer sempre os princípios constitucionais de legalidade, economicidade e eficiência, não fazendo mau uso dos recursos públicos,

considerando que o Tribunal de Contas publicou a Resolução nº 540/2000 no Diário Oficial de 04 de maio de 2000, dispondo sobre a matéria;

DETERMINA:

Art. 1º - Fica autorizada a utilização dos recursos e sistemas informatizados, acesso à rede mundial de computadores - INTERNET e correio eletrônico (e-mail) aos servidores estaduais da Administração Direta e Indireta, somente quando em conformidade com a finalidade e interesse da administração pública.

Parágrafo único - Entenda-se como interesse da administração pública, toda e qualquer informação que possa contribuir para o bom desempenho das funções do servidor, nos estritos termos constitucionais e legais.

Art. 2º - Deverá ser fornecida senha unipessoal e intransferível, com nível estritamente necessário ao trabalho sob responsabilidade do servidor, para acesso aos sistemas informatizados, à rede mundial de computadores - INTERNET e ao correio eletrônico (e-mail), disponibilizados pela administração pública.

§ 1º - Haverá preservação de sigilo no uso dos recursos de informática, incluindo o de senha, que observará os termos da Lei 10.098/94, art. 191, XIV;
§ 2º - Os acessos de que trata o caput deste artigo que permanecerem por período igual ou superior a 45 dias sem utilização deverão ser bloqueados pela Assessoria de Informática do respectivo Órgão da Administração Direta ou Indireta, e somente serão liberados mediante solicitação por escrito do interessado, autorizada e justificada pela chefia imediata.

Art. 3º - O correio eletrônico (e-mail) disponibilizado ao servidor pela administração pública, somente poderá ser utilizado para aprimorar e contribuir com as atividades funcionais e as condizentes com as atribuições profissionais e/ou acadêmicas daquele.

Art. 4º - Cada Secretaria de Estado, Autarquia, Fundação, Empresa Pública e Sociedade de Economia Mista fica responsável por observar as diretrizes traçadas por esta Ordem de Serviço a fim de que se proceda na correta utilização dos recursos públicos.
Art. 5º - Esta Ordem de Serviço entra em vigor na data de sua publicação.

PALÁCIO PIRATINI, em Porto Alegre,
14 de junho de 2000.

10. MENSAGEM FINAL

O sistema **RHE – RECURSOS HUMANOS DO ESTADO DO RIO GRANDE DO SUL**, veio a substituir os antigos sistemas de folha de pagamento, que tinham transações duras, desconectadas e de onde o usuário não conseguia extrair informações gerenciais.

Visa dotar a administração do Estado de uma moderna, consistente e adequada ferramenta para gestão de recursos humanos, integrando dados e informações pertinentes a todas as funções gerenciais de pessoal, em termos de uma nova filosofia de controle e planejamento, ligada diretamente ao processo de folha de pagamento.

O sistema tem o objetivo de eliminar o retrabalho, excluir a redundância de informações, reduzir lançamentos manuais em folha de pagamento, revisar alocação ideal de pessoas destinadas às atividades de RH e unificar os sistemas existentes para controle de RH e folha de pagamento.

A sua implantação teve início em 2006, com a Administração Direta do Estado, entrando a Indireta em 2008 e na sequência os demais órgãos com gestão própria de sua folha de pagamento. É o sistema oficial de Recursos Humanos do Estado, portanto, todos os dados dos servidores devem constar nele e não em sistemas paralelos.

O sistema não é web, ou seja, não utiliza rede de internet, o que o torna mais seguro a ataques cibernéticos. As falhas até então encontradas foram de erros de usuários e descuido com a senha de acesso.

As manutenções lançadas estão ligadas à folha de pagamentos, sendo essa um resultado do que ocorreu na vida funcional do servidor durante o mês. Por exemplo, se faltou injustificadamente, ao efetuar o lançamento da FNJ o recolhimento se dará na folha seguinte. Da mesma forma, se foi promovido, ao haver registro da alteração de classe do servidor, o pagamento será gerado sem necessidade de lançamento de valores.

Além do RHE, há os sistemas periféricos, como o Portal de Gestão de Pessoas, em Qlik Sense, de onde se podem extrair informações gerenciais por meio de diversas combinações de dados. Ou o IF-RHE, que vem se transformando em um verdadeiro workflow, desafogando os RHs e permitindo que o próprio servidor lance seus dados, como no recadastramento e alteração de dados pessoais e na marcação de férias. Apesar de parecerem sistemas independentes, a base de dados é única e eles tanto se alimentam do RHE como devolvem os dados atualizados por meio de integrações.

Da mesma forma, o Portal e o APP do Servidor utilizam-se da base de dados do RHE. Portanto, o cuidado com as senhas ao acessar tais sistemas É O MESMO.

Por fim, estamos implementando a Lei Geral de Proteção de Dados – LGPD no Estado. Essa norma atinge a todos, serviços públicos e privados. De compras on-line a redes sociais, de hospitais, bancos, escolas a hotéis, da publicidade à tecnologia, a LGPD afeta diferentes setores e serviços, e a todos os brasileiros, seja no papel de indivíduo, empresa ou governo, o que aumenta a nossa responsabilidade no tratamento de dados pessoais.

tesouro.fazenda.rs.gov.br

RHE
Recursos Humanos do Estado RS

TESOURO
do Estado do RS

GOV RS
NOVAS FAÇANHAS
NA FAZENDA