PRÁTICAS DE SEGURANÇA E PROTEÇÃO DE DADOS PESSOAIS PARA SERVIDORES

PROGEP
Pró-Reitoria de Desenvolvimento
e Gestão de Pessoal | UFPA

Reitor
Emmanuel Zagury Tourinho

Vice-reitor
Gilmar Pereira da Silva

Pró-Reitor de Desenvolvimento e Gestão de Pessoal (PROGEP)
Ícaro Duarte Pastana

Diretor de Gestão de Pessoal (DGP)
Liovanny Alves de Miranda

Coordenadora de Atendimento ao Usuário (CAU)
Nerivane da Silva Mendes

Elaboração:
Nerivane da Silva Mendes
Benjamim da Costa Araújo
Erika Gomes da Costa
Manoel Luiz de Carvalho Melo

Projeto Gráfico e Diagramação
Arnaldo da Silva Mota

SUMÁRIO

Apresentação

A fim de prevenir possíveis fraudes e golpes no uso dos sistemas institucionais, assim como diminuir os números de casos de violação de direitos com a obtenção e uso indevido de dados pessoais, a Pró Reitoria de Desenvolvimento e Gestão de Pessoal (Progep), em consonância com a Lei Geral de Proteção de Dados (LGPD) e as práticas de segurança da informação, preparou esta cartilha com informações úteis aos usuários.

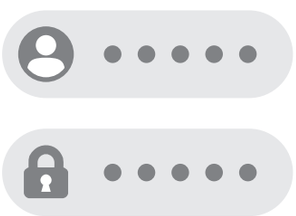
LGPD, SAIBA PARA QUE ELA SERVE!

A **Lei Geral de Proteção de Dados Pessoais** (LGPD) nº 13.709/2018 prevê a proteção dos direitos fundamentais de liberdade e de privacidade e a livre formação de personalidade de cada indivíduo. Por isso, institui que os dados obtidos, em regra, devem ser utilizados ou compartilhados com a **expressa autorização do titular** e para **finalidade específica** acordada.

FORMAS SIMPLES PARA PROTEGER DADOS PESSOAIS

Apenas forneça informações e dados pessoais quando realmente necessário e, nestes casos, exija sempre um documento em que esteja explícito que os dados serão **utilizados unicamente para o fim especificado** previamente.

Não utilize blocos ou papéis avulsos para anotar dados pessoais, afinal, caso caiam em mãos erradas, podem representar um risco.



Ao utilizar meios digitais, **evite acionar o preenchimento automático** de dados. Apesar de mais prático, não é seguro deixar seus dados e senhas armazenadas no dispositivo.

Não envie cópias/fotos de documentos pessoais, assim como financeiros, por redes sociais, pois estas podem ser utilizadas indevidamente por quem as recebeu, além do risco de vazamento de dados caso a rede social seja invadida por terceiros.

DICAS GERAIS DE SEGURANÇA NO USO DE SENHAS, DOMÍNIOS E ATAQUES

- Ao criar suas senhas não use dados pessoais, sequências de teclado, palavras de listas publicamente conhecidas, nem dados relativos ao serviço ou equipamento em que elas serão usadas.
- Use senhas longas, compostas de números aleatórios e diferentes tipos de caracteres.
- Não forneça sua senha para outra pessoa.
- Ao usar padrões de desbloqueio, configure para que o rastro fique invisível e mantenha seus dedos e a superfície da tela limpos.
- Ao usar equipamentos compartilhados, feche sua sessão (logout) ao acessar sites que requeiram o uso de senhas.
- Ao usar perguntas de segurança, evite escolher questões cujas respostas sejam facilmente deduzidas.
- Use conexões seguras (https) quando o acesso a um site envolver o fornecimento de senha.
- Altere imediatamente suas senhas sempre que desconfiar que elas tenham sido descobertas, vazadas ou usadas em um equipamento invadido ou infectado.
- Mantenha seus equipamentos seguros, evite instalar programas de fontes duvidosas e instale antivírus e o mantenha sempre atualizado.
- Ao usar interface web para acessar as mensagens de seu aplicativo, fique atento(a) à página em que o código QR está sendo mostrada. Apenas escaneie um código QR após se certificar de realmente estar na interface web do aplicativo de mensagens.
- Evite escanear códigos QR de sites que você não conheça.
- Realize varredura em seu computador ou celular para verificar a eventual existência de programas que realizem captura de senhas e/ou credenciais de acesso, bem como atualizar o aplicativo de antivírus.

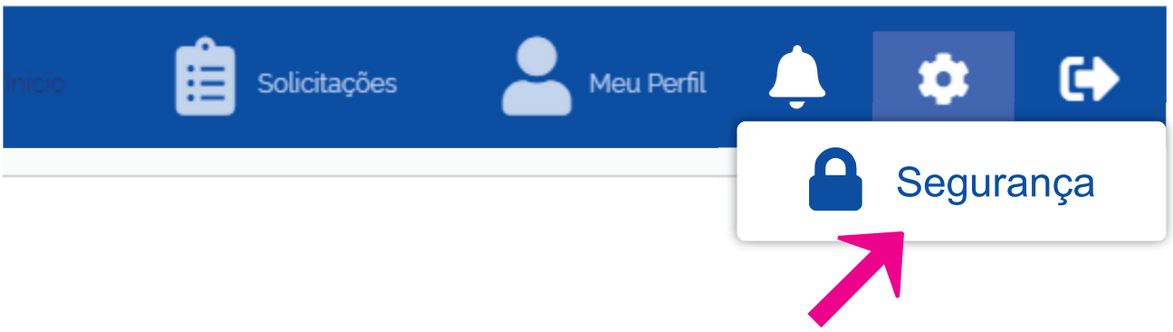
RECURSOS PARA SEGURANÇA DURANTE O USO DO SOUGOV

O SouGov é um aplicativo com serviços de gestão de pessoas exclusivos para servidores públicos federais ativos, aposentados, pensionistas e anistiados políticos do poder Executivo Federal Civil.
Para resguardar o usuário, o sistema apresenta algumas medidas e políticas de segurança da informação e proteção de dados pessoais, como:

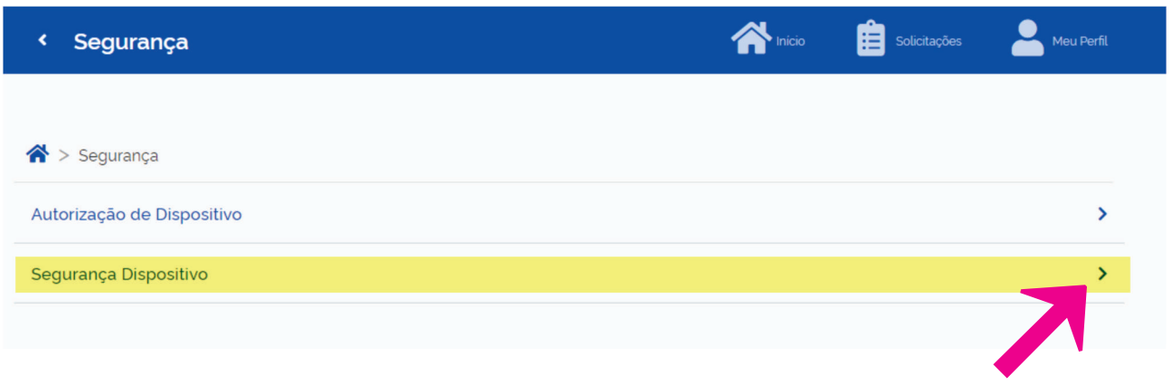
1 Gerência de sessões ativas, dispositivos autorizados e biometrias habilitadas.
Com esse recurso, você pode desautorizar dispositivos, desabilitar o uso de biometria e deslogar logins ativos nos dispositivos móveis e web, com a possibilidade de realizar todas essas ações em um único clique no botão **"Encerrar Todas"**.

Confira o passo a passo:
1º) Ao acessar a página do SOUGOV.BR, **versão Web**, clique no ícone de Configuração (engrenagem na parte superior à direita):

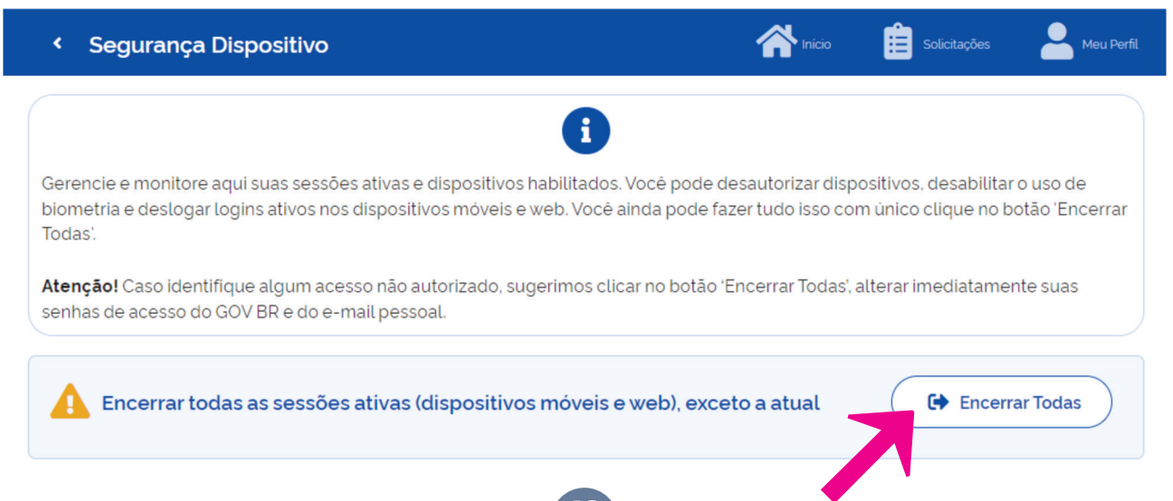
2º) Em seguida, clique na opção "**Segurança**":



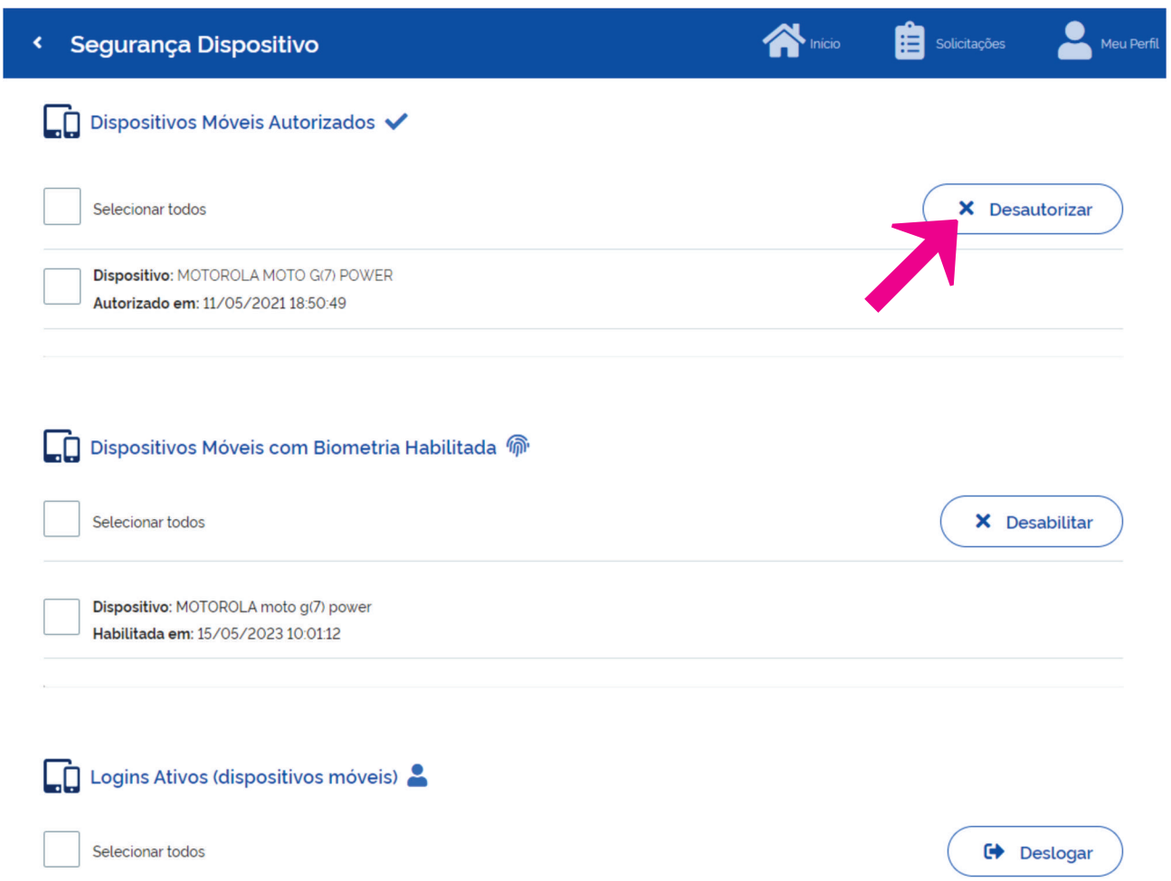
3º) No ícone de Segurança, clique na seta de "**Segurança Dispositivo**":



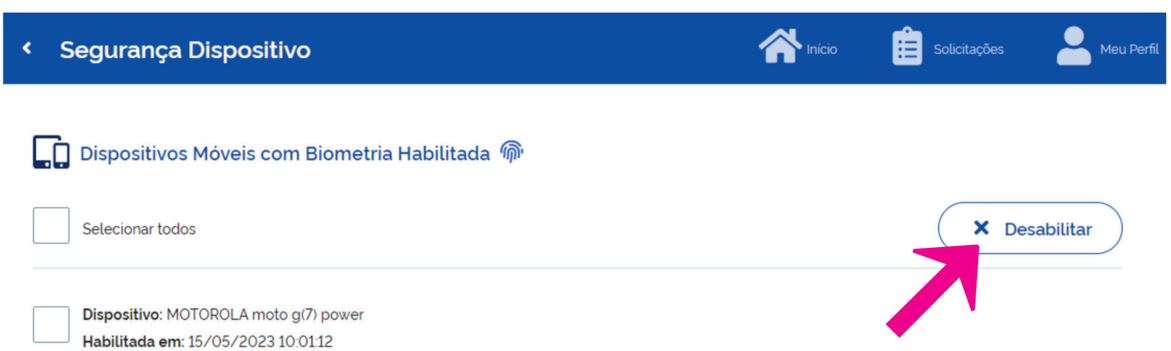
4º) Caso identifique algum acesso não autorizado, sugerimos clicar no botão '**Encerrar Todas**', alterar imediatamente suas senhas de acesso do GOV BR e do e-mail pessoal:



5º) Você também pode desautorizar os dispositivos móveis autorizados, para isso, selecione o dispositivo que deseja **desautorizar**, clique no botão "**Desautorizar**" e confirme a operação:



6º) Você também pode desabilitar os dispositivos móveis com biometria habilitada, para isso, selecione o dispositivo que deseja desabilitar, clique no botão "**Desabilitar**" e confirme a operação:



Importante: atente-se às mensagens enviadas para seu e-mail quando é realizado o login em um dispositivo móvel ou navegador web diferente daquele utilizado anteriormente. Nesse caso, você receberá a seguinte mensagem de alerta por e-mail:

"Foi detectado um novo login em sua conta SouGov

Data/Hora: 10/02/2022 11:04:46

dekstop Windows 10

Navegador Chrome

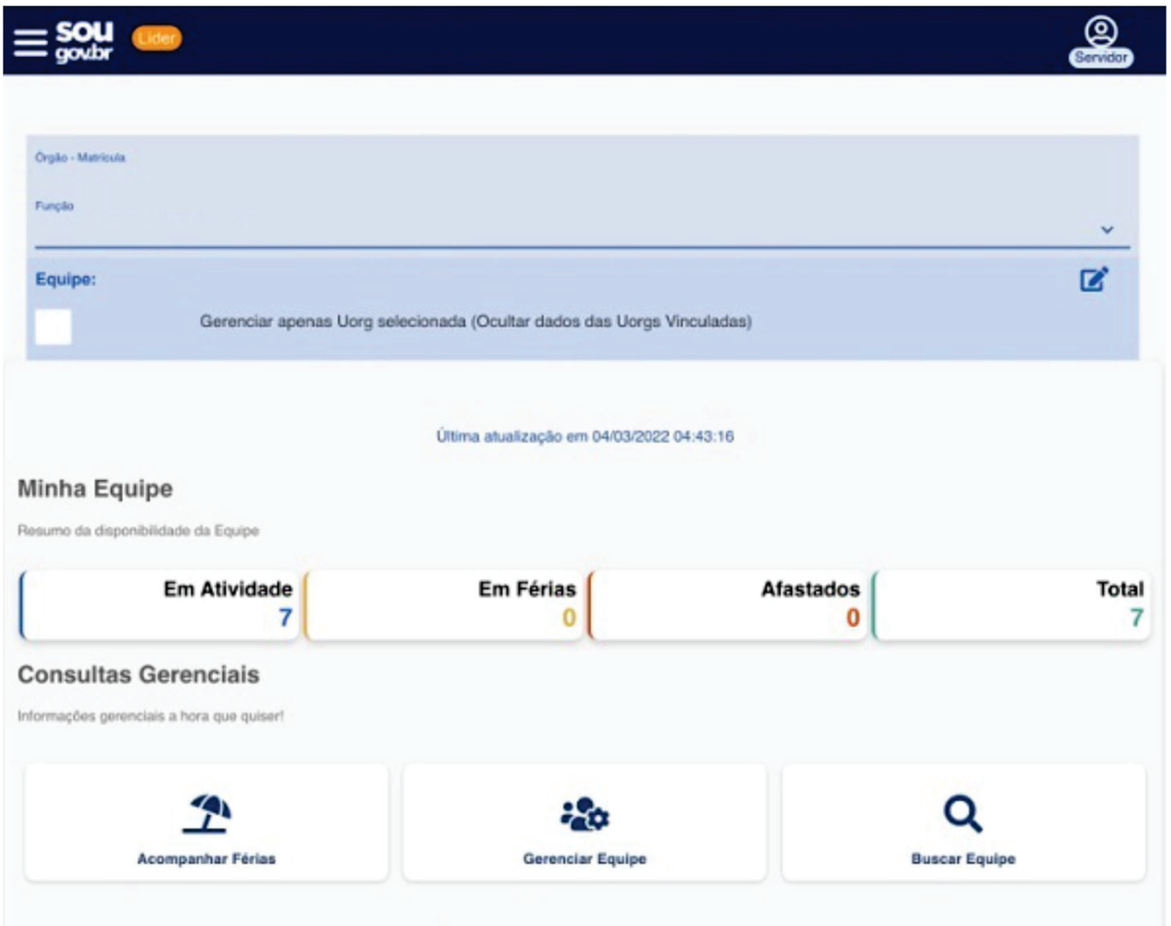
IP:

Se o login for efetuado por você, nenhuma ação será necessária.

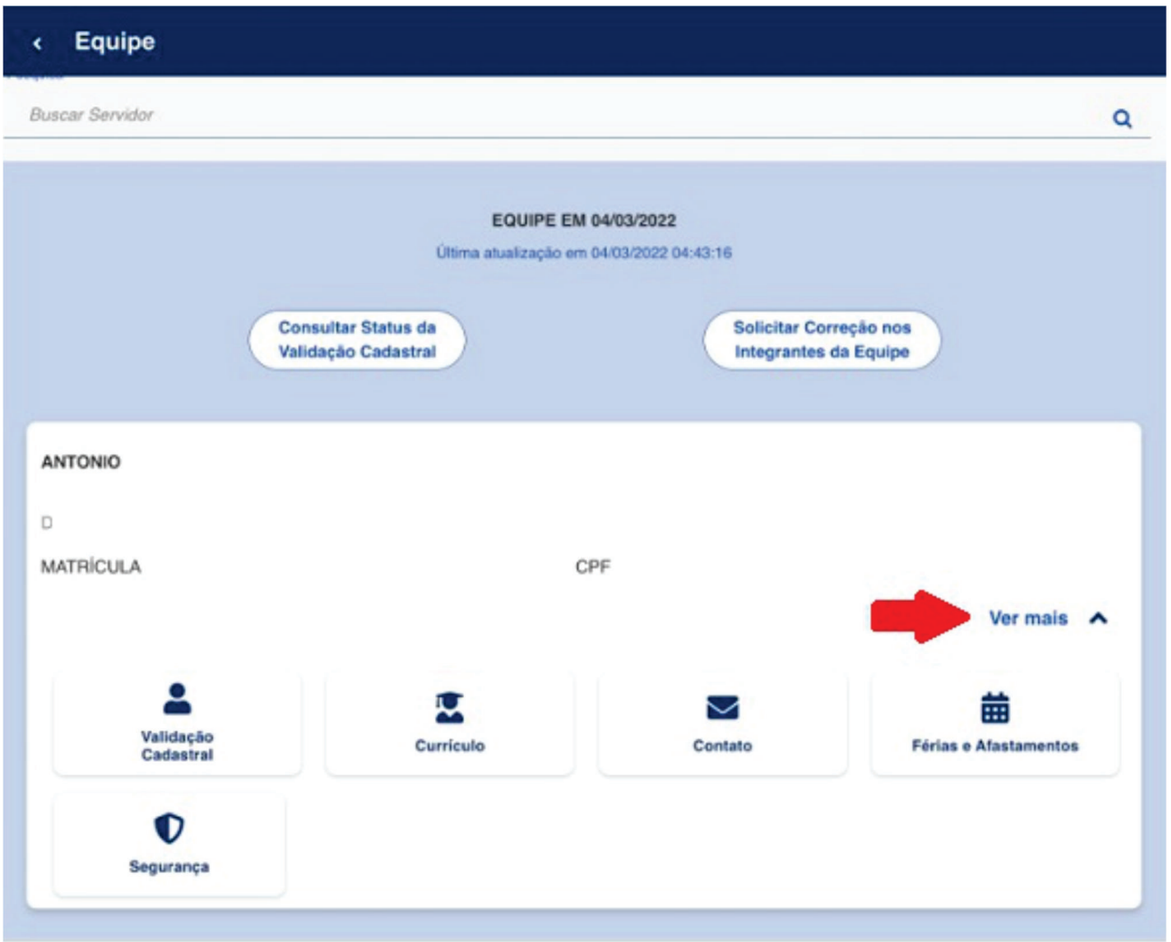
Caso não reconheça este acesso, favor acessar o Sou Gov.br versão WEB, no endereço: https://sougov.economia.gov.br"

2 Desautorização de login via Gerência da Chefia Imediata

1º) Caso seja identificado alguma fraude na conta do SOUGOV.BR de um membro da equipe, a chefia imediata pode acessar o **"Gerenciamento Equipe"** para visualizar a sua equipe:



2º) Em seguida, clique no nome da pessoa que solicitou a desautorização do dispositivo não reconhecido e em buscar no ícone "**Ver mais**" para visualizar os dados dos dispositivos logados:



3º) Após verificar os logins ativos dos dispositivos móveis e os dispositivos autorizados, a chefia deve clicar em "**Deslogar**" e "**Desautorizar**" os dispositivos não reconhecidos:

3 Autenticação de dois fatores

A instalação do aplicativo **MEU GOV.BR** no celular é necessária para ativar a autenticação de dois fatores, Que fornece uma camada extra de proteção que dificulta o acesso de terceiros aos seus dispositivos e contas online.

1º) Digite o CPF na tela inicial do https://acesso.gov.br e clique no botão continuar para que possa inserir a sua senha.

2º) Após logar, deve-se clicar no menu **"Segurança"**, dentro do campo **"Minha área"**, e clicar no link **"Habilitar verificação em duas etapas"**.

3º) Digite o código enviado no aplicativo Meu Gov.br e clique no botão **"Habilitar"**.

4º) A verificação em duas etapas estará habilitada. Agora todas as vezes que você digitar sua senha Gov.br será necessário digitar o código de segurança mostrado no seu aplicativo Meu Gov.Br

PROVIDÊNCIAS PARA CASOS DE SUSPEITA DE ACESSO INDEVIDO À CONTA SOUGOV

1. Efetue a troca de sua senha GOV.BR e a troca do seu e-mail pessoal cadastrado nas plataformas do Governo.

2. Encerre as sessões ativas do aplicativo SouGov, bem como desabilite as biometrias cadastradas.

3. Verifique regularmente se existem autorizações de empréstimos consignados no aplicativo SouGov. Caso sim, cancele. Contudo, se a autorização já houver sido utilizada e um consignado for realizado na sua conta, redija um termo de reclamação de consignação via Sigepe, e combinado a isso registre um boletim de ocorrência junto à autoridade policial.

Para saber como redigir o termo de reclamação de consignação acesse aqui ou escaneie o qrcode ao lado.

4. Efetue a troca da sua senha do SIGAC, pois a mesma pode ser utilizada para obter o selo prata na conta GOV. BR.

5. Consulte o sistema **Registrato** do Banco Central, verificando se ocorreu a abertura de conta corrente em outras instituições financeiras com seu nome.

Acesse aqui o sistema Registrato ou escaneie o qrcode ao lado.

PASSATEMPO

Caça-palavras

As palavras deste caça-palavras estão escondidas na horizontal, vertical e diagonal.

~~SISTEMA~~
AUTENTICAÇÃO
DISPOSITIVO
SENHA
SOUGOV
PRIVACIDADE
SEGURANÇA

F	S	O	N	W	A	T	O	U	L	P	M	T	Ç	A	T	D	U
R	I	L	Y	O	E	U	E	N	R	N	T	H	E	R	S	F	N
E	S	T	I	T	E	A	T	I	E	T	O	T	N	N	O	L	O
A	T	G	L	A	D	E	V	E	H	N	N	O	T	U	O	W	S
S	E	D	M	A	O	A	A	P	N	I	N	P	R	W	R	E	U
A	M	H	L	Y	C	A	T	N	R	T	T	T	O	E	G	E	E
L	A	G	D	I	S	P	O	S	I	T	I	V	O	U	E	C	W
E	Ç	Y	D	D	O	S	S	W	S	E	L	C	R	R	S	L	R
L	H	A	S	O	U	G	O	V	H	E	L	A	A	F	E	N	K
H	D	L	U	T	H	R	D	C	I	S	N	W	N	Ç	N	E	S
E	E	C	Q	E	I	E	I	T	F	Ç	H	H	O	U	Ã	E	R
U	O	R	R	W	K	T	N	U	A	D	X	C	A	P	E	O	L

Referências

https://faq-login-unico.servicos.gov.br/en/latest/_perguntasdafaq/comoativarautenticacao2fatores.html

https://new.safernet.org.br/content/privacidade-online-e-linguagem-oculta-da-internet

https://pt.theastrologypage.com/password

https://puzzel.org/pt/crossword/

https://www.geniol.com.br/palavras/caca-palavras/

https://www.gov.br/servidor/pt-br/acesso-a-informacao/faq/sou-gov.br/seguranca-sougov

https://www.gov.br/servidor/pt-br/assuntos/sou-gov

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

PROGEP

Pró-Reitoria de Desenvolvimento
e Gestão de Pessoal | UFPA