A segurança da informação está diretamente relacionada com a proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança da informação: confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

E para oferecer uma camada extra de segurança nos acessos aos sistemas disponibilizados pela Dataprev será implementado o "Duplo Fator de Autenticação", que é um recurso já consagrado como eficiente e de fácil utilização.

Existem várias soluções disponíveis no mercado para viabilizar a autenticação em dois fatores e uma das mais utilizadas é o "Google Authenticator", um aplicativo de segurança gratuito que viabiliza a autenticação em dois fatores ao gerar "chaves de acesso" para serem usadas neste processo.

A primeira etapa da autenticação no sistema parceiro é formada pelo Identificador e Senha da conta do usuário no GERID.

A segunda etapa consiste em consultar o aplicativo 'Google Authenticator" para que se verifique o código numérico de 6 dígitos, que deverá então ser preenchido no campo correspondente.

Este código numérico se renova aleatoriamente a cada 30 segundos e **pode ser consultado sem Internet**, o que viabiliza a utilização mesmo em situações de falta de conexão.

Recomendações importantes:

Assim como sua senha, o código numérico é sigiloso e deve ser mantido em segredo. Não deve ser exibido para outras pessoas e, principalmente, nunca deve ser fornecido para quem quer que seja, em ligações telefônicas.

Não empreste seu celular e caso necessite entregá-lo para manutenção, antes remova o aplicativo 'Google Authenticator".

Use apenas seu aparelho celular com o "Google Authenticator" não instale em telefones de terceiros.

As etapas a seguir contém os procedimentos que terá de realizar para:

5. O que fazer para reiniciar o código do Duplo Fator de Autenticação

Em caso de impossibilidade definitiva na consulta ao aplicativo "Google Authenticator", por exemplo devido a roubo ou extravio permanente do seu aparelho móvel ou até mesmo a utilização de todos os seus 5 códigos de backup, será necessário reiniciar seu vínculo de autenticação de dois fatores para viabilizar o acesso novamente. Siga o roteiro:

5.1 Faça o login com seu identificador e senha

5.2 Escolha a opção "Reiniciar Dispositivo MFA" na tela seguinte Obs: MFA do inglês Multi Factor Authentication – Autenticação Multifator

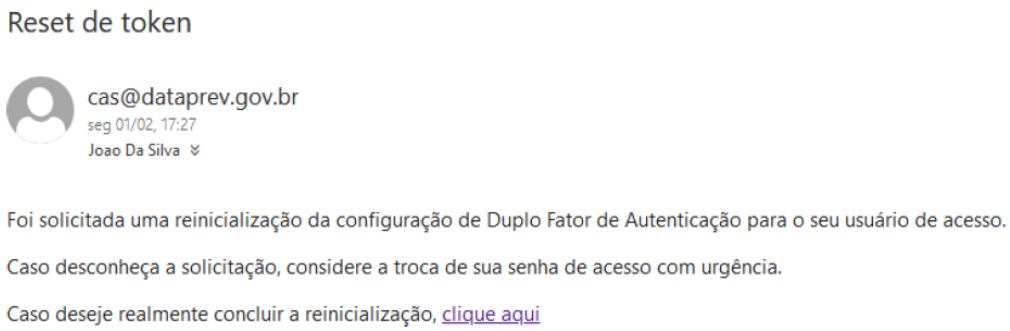
5.3 Digite algum e-mail cadastrado no LDAP (corporativo ou particular) no caso de acordos digite o e-mail informado durante o cadastro no GID.

Importante: O e-mail precisa estar previamente cadastrado no perfil de usuário do LDAP. Sem este cadastramento o usuário não receberá a mensagem para reiniciar a chave de acesso. Se o e-mail informado for igual ao existente no cadastro de usuários, você receberá um link para efetuar a reinicialização.

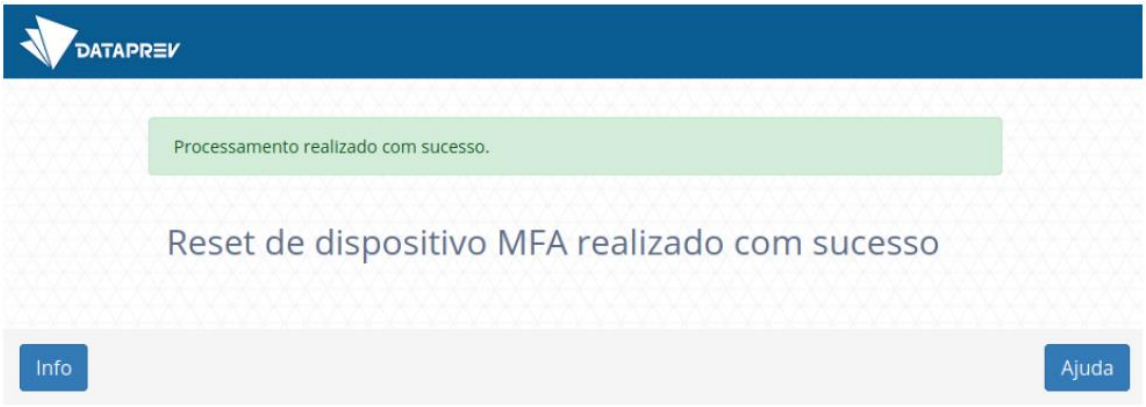
Caso a mensagem não apareça em sua caixa de entrada, verifique sua caixa de SPAM.

5.4 Uma segunda mensagem irá solicitar que você confirme novamente a operação

5.5 Clique no Link que foi enviado a seu e-mail particular. Ao clicar, sua vinculação anterior será reiniciada.



5.6 Após a reinicialização do vínculo será apresentada esta mensagem na tela do GERID



5.7 Refaça os procedimentos de Vinculação e backup dos códigos de segurança, descritos na Etapa 2 – Vincular o Aplicativo “Google Authenticator” ao GERID

1. Instalar o Aplicativo do “Google Authenticator” em seu celular

1.1 Utilize o seu celular para acessar a loja de aplicativos do seu sistema operacional (Play Store para o Android ou App Store para o iOS) e pesquisar por “Google Authenticator”. Em seguida realize o processo de instalação.

1.2 Ao abrir o “Google Authenticator”, leia as instruções sobre os primeiros passos.

1.3 O aplicativo “Google Authenticator” irá informar que para configurar uma conta você terá de usar o código QR (para isso você terá de autorizar o aplicativo a utilizar sua câmera) ou a chave secreta de configuração (chave secreta de registro do GERID).

2. Vincular o Aplicativo ao Google Authenticator" ao GERID

Leia antes estas observações importantes e depois siga o roteiro logo a seguir:

a) A impressão dos códigos backup (detalhes na pág 8) deverá ser feita antes de clicar na opção "Registrar".

É de sua responsabilidade a correta preservação destas informações de maneira segura. Porém é importante observar que se o processo **não for concluído no mesmo momento**, ao retornar à esta tela posteriormente o código QR, a chave secreta de registro e os códigos de backup (8 dígitos) aqui apresentados serão alterados.

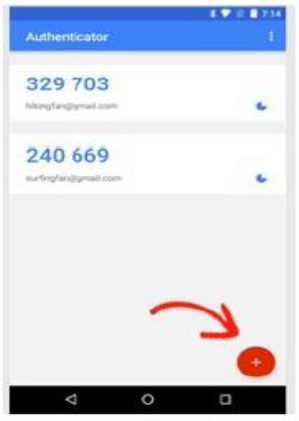
b) Nunca compartilhe os códigos de backup e guarde-os em lugar seguro e confiável.

c) Não clique na opção "Registrar" sem antes ter realizado o vínculo com o "Google Authenticator" porque senão terá de reiniciar a chave de segurança e não conseguirá concluir o processo.

2.1 Ao acessar o endereço do sistema desejado, o GERID será chamado, e na primeira vez será apresentada a tela de uso habitual. Faça o login normalmente com seu identificador e senha ou certificado.

2.2 Ao clicar na opção “Entrar” será apresentada a próxima tela. Você fará esta operação apenas uma vez para vincular o acesso ao GERID/INSS para acesso ao sistema desejado, utilizando o “Google Authenticator”.

2.3 Acesse o aplicativo “Google Authenticator” no seu celular.

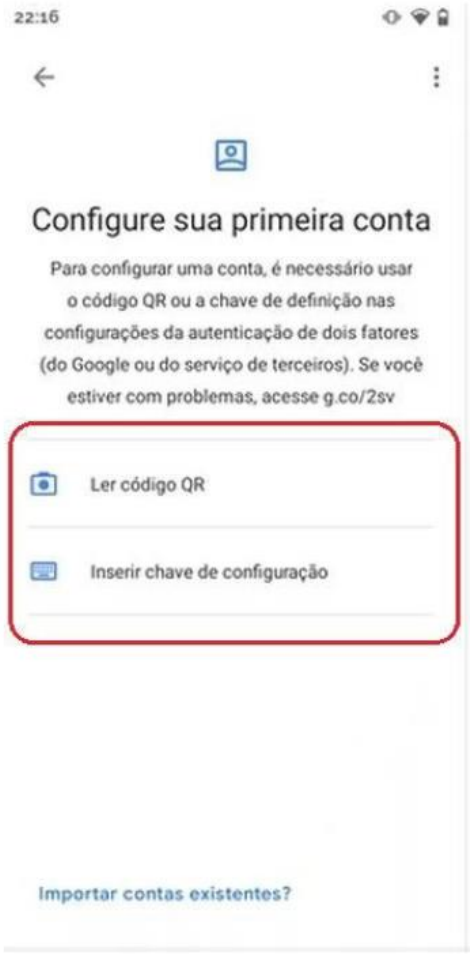


2.4 Acione o botão +

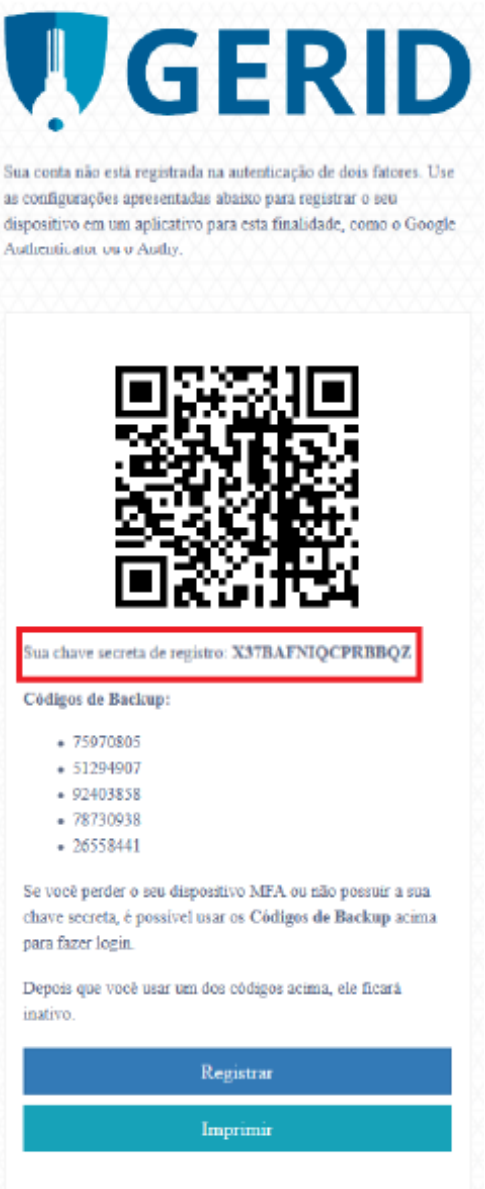
2.4 O aplicativo irá para a tela seguinte, onde você pode escolher entre “Ler código QR ou Inserir chave de configuração”.

Obs: A opção mais simples é “Ler código QR”

2.5 Aponte a câmera do celular para o código QR que está na tela do GERID



2.6 Se a câmera do celular estiver com problemas é possível escolher a opção “Inserir chave de configuração” e realizar o vínculo através da digitação no aplicativo do conjunto de letras e números “Chave Secreta de Registro” que está na tela do GERID bem abaixo da imagem do código QR no aplicativo



2.7 Depois de escanear o código QR ou digitar a Chave secreta o vínculo será realizado automaticamente e o aplicativo apresentará a opção para que você dê um nome para esta conta, como por exemplo GERID_INSS.

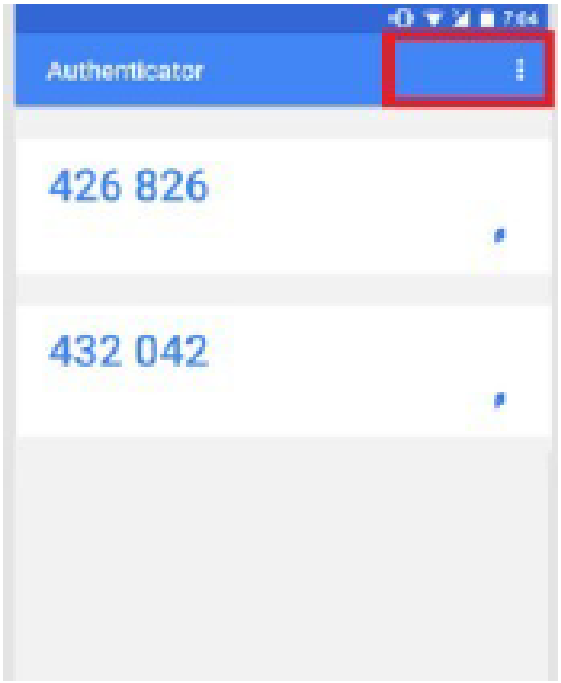
2.8 Na tela do GERID acione a opção “Imprimir” para salvar a imagem da tela em PDF ou concluir a impressão e salvar os códigos de backup.

2.9 Escolha a opção “Registrar” para concluir a operação de vínculo na autenticação de duplo Fator.

2.10 Depois desta operação será apresentada a tela com o Duplo Fator de Autenticação e a utilização do sistema poderá ser imediata através da digitação do código numérico fornecido no “Google Authenticator”. Os números são alterados automaticamente a cada 30 segundos.

Observação: Os códigos gerados pelo “Google Authenticator” utilizam algoritmos que se baseiam na data e hora configurados no smartphone. No entanto a data e a hora de um smartphone podem não estar exatamente sincronizados com a data e hora dos servidores do Gerid. Quando isso acontece, o código atual pode ser invalidado pelo sistema.

Caso tal situação aconteça, o Google Authenticator possui a funcionalidade de "Correção de horas para códigos". Para acessá-la, basta ir à tela inicial do app, em: Menu (três pontinhos ao lado direito do título "Google Authenticator") Configurações / Correção de horas para códigos / Sincronizar agora.



Ao término será exibida uma mensagem de confirmação da Sincronização. Clique em "OK" e retorne a tela inicial clicando na "seta para a esquerda" no canto esquerdo superior da tela

3. Realizar o acesso ao GERID/GPA com Duplo Fator de Autenticação

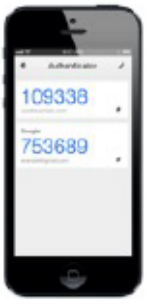
Veja a sequência de passos que terá de realizar para acessar o GERID depois da vinculação inicial:

3.1 Faça o login na primeira tela utilizando seu identificador e senha

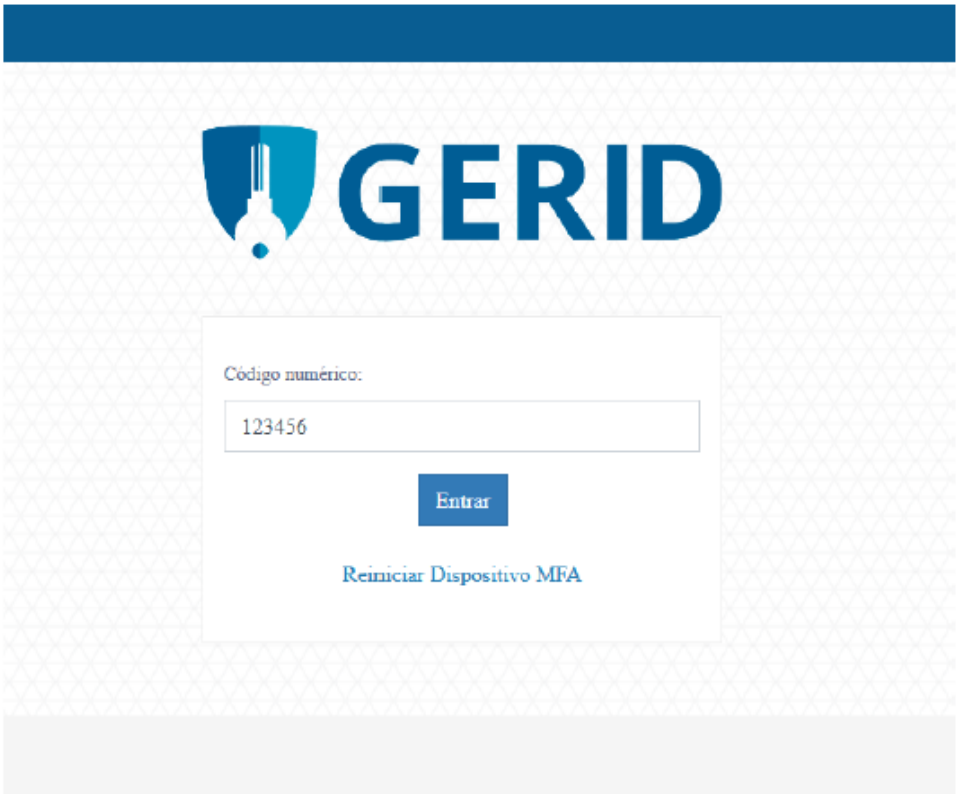
3.2 Abra o aplicativo “Google Authenticator” no seu aparelho móvel

Obs: Você não precisa estar conectado a uma rede de dados para usar o “Google Authenticator”.

3.3 Escolha a conta GERID



3.4 Digite na tela do GERID código numérico de 6 dígitos que aparecem no Aplicativo “Google Authenticator” e o seu acesso ao GERID/INSS estará liberado.



Pronto! Você obteve acesso ao sistema. Parabéns

4. Em caso de acesso emergencial usar os códigos de backup

Você pode recorrer a este recurso em caso de emergência se por algum motivo não esteja com o seu aparelho móvel e precise acessar o sistema GERID/INSS. Cada um dos 5 códigos de backup que foram salvos no momento da vinculação poderá ser usado uma única vez e devem ser digitados na tela de acesso para substituir o código aleatório gerado no "Google Authenticator".

4.1 Para fazer esta operação você precisa fazer login na primeira tela do GERID com seu identificador e senha e na segunda tela digitar um dos números de backup, que possuem 8 dígitos e poderá ser usado uma única vez.