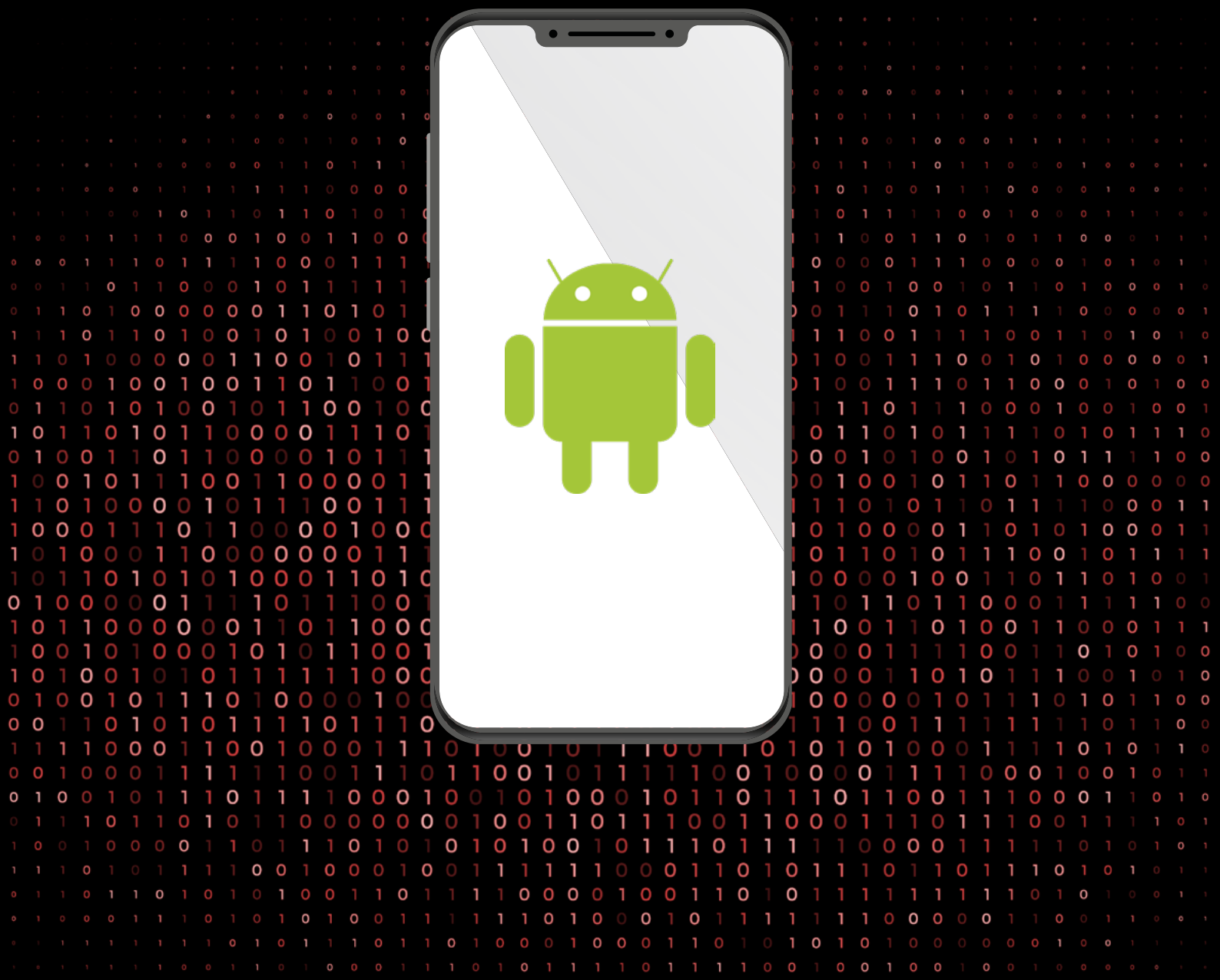
APCS/DGPAd

Departamento Estadual
de Investigações Criminais
DEIC

DIVISÃO DE CRIMES
CIBERNÉTICOS

Smartphone protegido
(“Android”)



Modelo “Android”

A escolha de senhas é um passo importante para segurança do seu smartphone.

1. Escolha senhas difíceis. **Evite:**

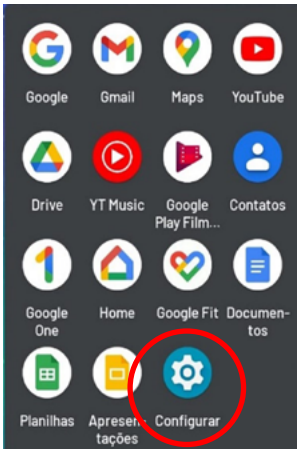
- Sequências numéricas, por exemplo: 1,2,3,4.
- Datas de nascimento ou casamento.
- CPF ou RG.
- Número do próprio telefone.

Para mais informações acesse:
https://www.avg.com/pt/signal/how-to-create-a-strong-password-that-you-wont-forget

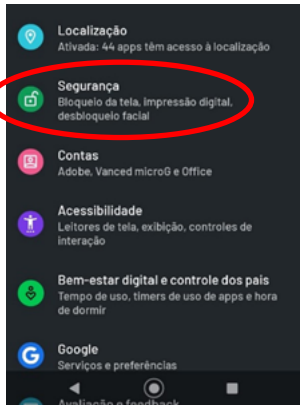
2. Utilize um aplicativo de cofre de senhas pago, pois esta é uma forma segura de armazenar senhas no seu celular.

Crie uma senha ou outra medida para acesso ao celular. Veja a seguir como definir o bloqueio de tela em um dispositivo “Android” usando um “PIN” (“Personal Identification Number”), um padrão, impressão digital ou uma senha:

1. Abra o app “Configurar” do smartphone.

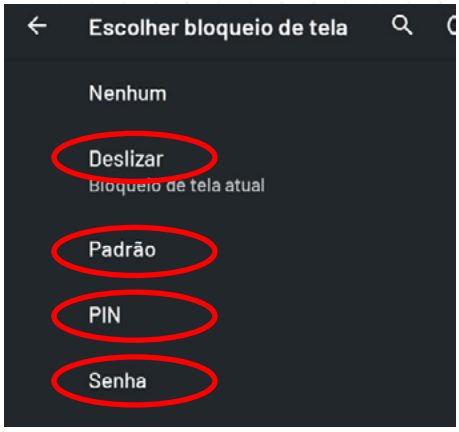


2. Toque em “Segurança”.



3. Para escolher um tipo de bloqueio de tela, toque em “Bloqueio de tela” (**se você já havia configurado algum bloqueio, será necessário inserir o “PIN”, o padrão ou a senha antes de escolher um outro bloqueio diferente**).

4. Escolha e toque na opção de bloqueio de tela que você deseja usar. Depois siga as instruções da tela.

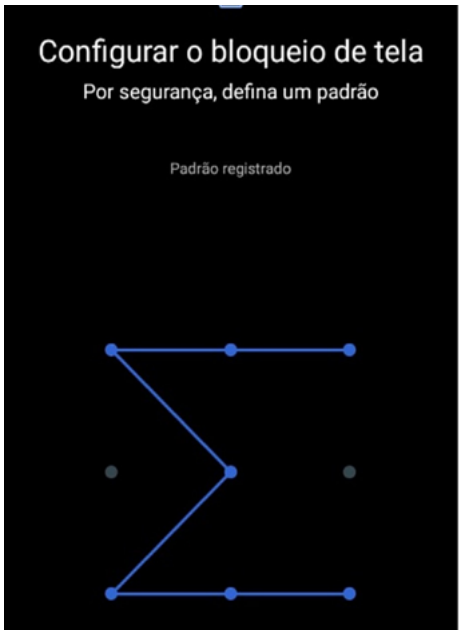


Conheça as opções de bloqueio de tela:

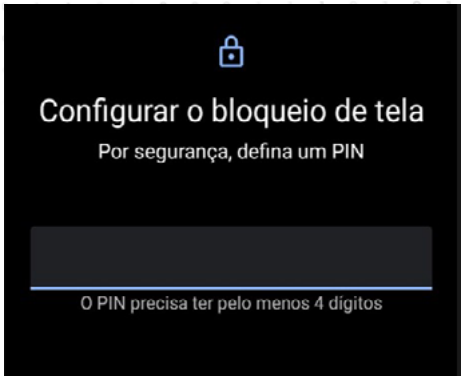
Nenhum: nesta opção, seu smartphone permanece desbloqueado em tempo integral, o que não oferece nenhuma proteção, mas permite o acesso rápido à tela inicial e seus aplicativos.

Deslizar: Basta deslizar o dedo na tela para desbloquear o telefone, o que não oferece nenhuma proteção, mas permite o acesso rápido à tela inicial.

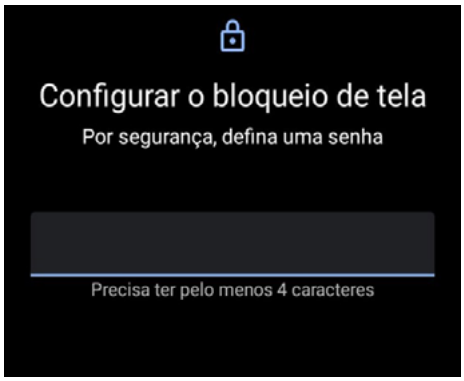
Padrão: Crie um desenho (padrão) que será solicitado sempre que desejar desbloquear a tela do smartphone.



“PIN”: Crie uma senha **numérica** (PIN) de quatro ou mais dígitos. “PINs” mais longos tendem a ser mais seguros.



Senha: Crie uma senha com quatro ou mais **letras e números**. Uma senha forte é a opção de bloqueio de tela mais segura.



Desbloqueio por Impressão digital:

Após definir um dos tipos de bloqueio de tela acima, você também pode adicionar um desbloqueio por impressão digital, caso seu smartphone tenha leitor de impressão digital.

Acesse novamente as “Configurações”, depois toque em “Segurança” e “Impressão Digital”. Será solicitado seu padrão, “PIN” ou senha para prosseguir. Por fim, toque em “Adicionar impressão digital” e siga as instruções da tela.

Você pode cadastrar mais de uma impressão digital.

O desbloqueio da tela por impressão digital é instantâneo, mas você ainda poderá usar o outro tipo de bloqueio escolhido, se preferir (padrão, “PIN” ou senha).

Caso haja algum erro de leitura de sua impressão digital, será solicitado seu padrão, “PIN” ou senha.

Desbloqueio facial:

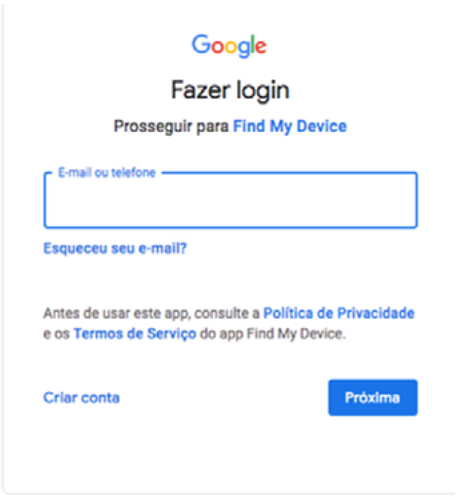
Alguns aparelhos possuem o recurso de leitura facial. Para adicionar um desbloqueio facial acesse as “Configurações”, depois toque em “Segurança” e “Desbloqueio facial”. Será solicitado seu padrão, “PIN” ou senha para prosseguir. Por fim, toque em “Adicionar Desbloqueio facial” e siga as instruções da tela.

Encontrar, bloquear ou limpar um dispositivo “Android” perdido:

Se você perder seu dispositivo com o sistema “Android”, poderá encontrá-lo, bloqueá-lo ou limpá-lo. Veja como encontrar, bloquear ou limpar remotamente seu smartphone:

1. Acesse www.android.com/find e faça login na sua Conta do Google.

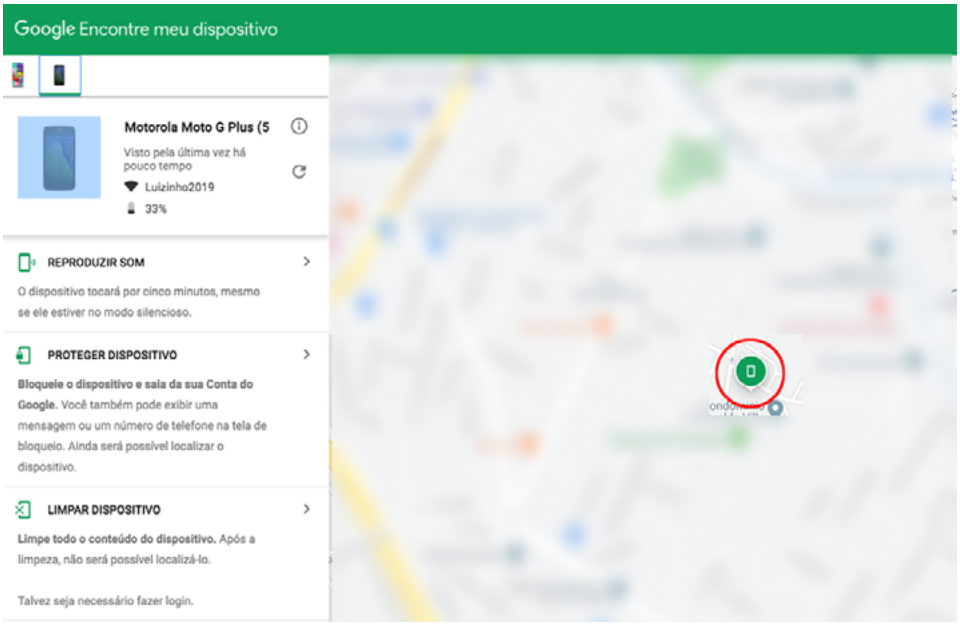
    • Se você tem mais de um dispositivo, clique naquele que foi perdido na parte superior da tela.
    • Se o smartphone perdido tiver mais de um perfil de usuário, faça login com uma conta do Google que esteja no perfil principal.



2. O smartphone perdido recebe uma notificação.

3. No mapa, você pode ver informações sobre onde ele está.

- A localização é aproximada.
- Se não for possível encontrar o smartphone, você verá o último local conhecido dele, caso esteja disponível.



4. Escolha o que deseja fazer. Se necessário, primeiro clique em “**Ativar bloqueio e limpeza**”.

Reproduzir som: faz o smartphone tocar no volume máximo por cinco minutos, mesmo que ele esteja no modo silencioso ou de vibração.

Proteger dispositivo: bloqueia o smartphone com seu “PIN”, padrão ou senha. Caso você não tenha um bloqueio, é possível configurar um. Para ajudar uma pessoa a devolver o smartphone para você, **adicione uma mensagem ou um número de telefone à tela de bloqueio**.

Limpar dispositivo: exclui permanentemente todos os dados do seu smartphone, mas não exclui os dados dos cartões SD. Depois que você limpar o smartphone, o “Encontre Meu Dispositivo” deixará de funcionar nele. **Importante: se você encontrar seu smartphone após a limpeza, provavelmente precisará da senha da sua Conta do Google para usá-lo novamente.**

Dica: se você vinculou seu smartphone ao Google, é possível encontrá-lo ou fazê-lo tocar pesquisando por “encontrar meu smartphone” em google.com.br

Para mais informações acesse: https://support.google.com/accounts/answer/6160491?hl=pt

Altere a senha (“PIN”) do “SIM CARD”

O “SIM CARD” (também chamado de “chip”) possui uma opção de segurança muito útil. É possível trocar a senha padrão do “SIM CARD”. Assim, toda vez que o aparelho for desligado e religado, ou o chip for retirado e recolocado,a senha será solicitada, aumentando a segurança contra criminosos.

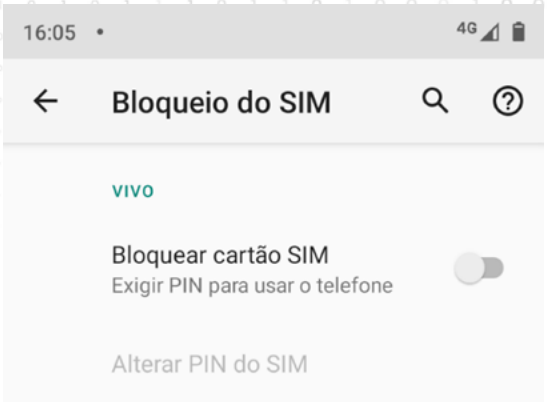
Por padrão, o desbloqueio do chip por meio do “PIN” vem desativado pelas operadoras quando adquirimos um novo “sim card”. Para ativar o código “PIN” no seu celular, basta seguir as instruções abaixo.

Para celulares com sistema “Android”:

1. Acesse o aplicativo “Config”, também encontrado com o nome “Configurações” ou “Configurar”.

2. Acesse o item “Segurança”.

3. Ative a opção “Bloquear cartão SIM”.



4. Se for a primeira vez que você realiza esse procedimento, será necessário inserir o “PIN” padrão do “chip”, da sua operadora. O “PIN” padrão pode ser acessado no verso do cartão plástico em que veio o seu “chip” no momento da compra. Caso prefira, confira abaixo a lista de “PINs” padrão das principais operadoras:

Claro: 3636
Vivo: 8486
TIM: 1010
Oi: 8888
Nextel: 0000
Algar Telecom/CTBC: 1212

5. Se você tentou o “PIN” padrão da sua operadora mas não obteve sucesso, será necesssário entrar em contato com a central de atendimento para solicitar o “PIN” padrão.

6. Caso você tenha bloqueado seu “chip” por excesso de tentativas do procedimento acima, será necessário utilizar um código de desbloqueio chamado “PUK” (Personal Unblocking Key). Este código possui oito dígitos e também pode ser acessado na parte trazeira do cartão em que seu “chip” veio no momento da compra. Se você não tiver mais o cartão ou por outro motivo não souber o código “PUK”, será necessário entrar em contato com a central de atendimento da operadora.

Cuidado: se você digitar o código “PUK” errado mais de dez vezes, seu chip é bloqueado definitivamente e você deverá comprar outro.

7. Somente após a inserção bem sucedida do “PIN” padrão será possível alterá-lo para outro número de sua preferência, na opção “Alterar PIN do SIM”. Memorize o novo número, pois ele será solicitado sempre que desligar e religar o celular, recolocar o chip ou quando você quiser mudar novamente o “PIN” do “chip”.

Confira abaixo os telefones das centrais de atendimento das principais operadoras:

Vivo: *8486 de um número Vivo e 1058 de qualquer telefone.
Claro: 1052 de qualquer telefone.
TIM: *144 do seu número Tim ou 1056 de qualquer telefone.
Oi: *144 do seu número Oi ou 1057 de qualquer telefone.
Nextel: 1050 de qualquer telefone.
Algar Telecom/CTBC: 1055 de qualquer telefone.

Desative a caixa postal do seu dispositivo “Android”

Os criminosos podem recuperar senhas de aplicativos como o whatsapp pela caixa postal do seu smartphone.

TIM: O serviço de correio de voz da TIM é o **TIM Recado Backup** e o ele pode ser acessado com uma ligação para o número *100.
O processo de cancelamento deste serviço não é possível por aplicativo ou pelo site da TIM, sendo necessário ligar para *144 ou 1056 e solicitar o cancelamento do Tim Recado Backup a um atendente.

Vivo: O serviço de correio de voz da Vivo é o **Vivo Recado** e pode ser acessado ligando para *555. O cancelamento desta caixa postal é feito com o envio de uma mensagem SMS para os seguintes números:
Vivo Recado: escreva SAIR para 5550;
Vivo Recado Premium: escreva SAIR para 5557.
Caso haja dúvidas ou o processo de cancelamento não ocorra, entre em contato com a Vivo pelos números *8486 ou 1058 e solicite ao atendente.

Claro: O correio de voz da Claro é o **Claro Recado** e pode ser acessado ligando para o número *555. O cancelamento pode ser feito por SMS ou por ligação. Tente enviar um SMS com os dizeres SAIR para 555 — você deve receber um SMS de confirmação da Claro.
Caso não dê certo, entre em contato com a Claro pelo número 1052 e solicite o cancelamento do Claro Recado para um atendente.

Oi: O correio de voz da Oi é chamado de **Caixa Postal** e pode ser acessado ligando para *100. Por padrão, o correio de voz da operadora vem desativado, mas é possível cancelar ou ativar esse serviço através da página Minha Oi (https://www.oi.com.br/minha-oi/). Entre nesta página, clique em Detalhes e Serviços, Ativação e Desativação de Serviços e desative o Pacote Caixa Posal Básico. Caso não dê certo, ligue para a operadora pelo número *144. e solicite ao atendente.

Nextel: O correio de voz da Nextel se chama **Caixa Postal** e pode ser acessado ligando para *100 — a senha padrão é 9999. A única forma de desativar o serviço é ligando para a operadora pelo número 1050.

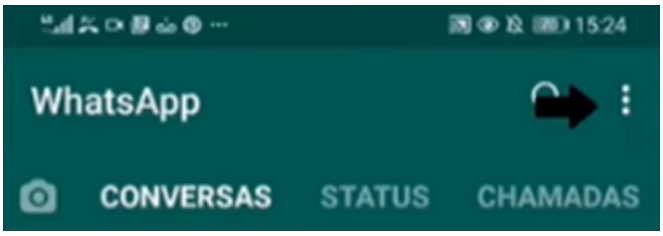
Confira abaixo os telefones das centrais de atendimento das principais operadoras:

Vivo: *8486 de um número Vivo e 1058 de qualquer telefone.
Claro: 1052 de qualquer telefone.
TIM: *144 do seu número Tim ou 1056 de qualquer telefone.
Oi: *144 do seu número Oi ou 1057 de qualquer telefone.
Nextel: 1050 de qualquer telefone.
Algar Telecom/CTBC: 1055 de qualquer telefone.

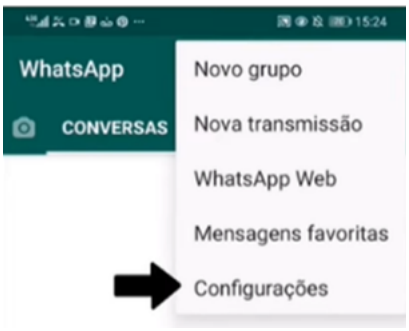
Ative a verificação em duas etapas no Whatsapp

Uma forma de proteger dados do whatsapp e evitar a clonagem é definir a autenticação em duas etapas do referido aplicativo de mensagens.

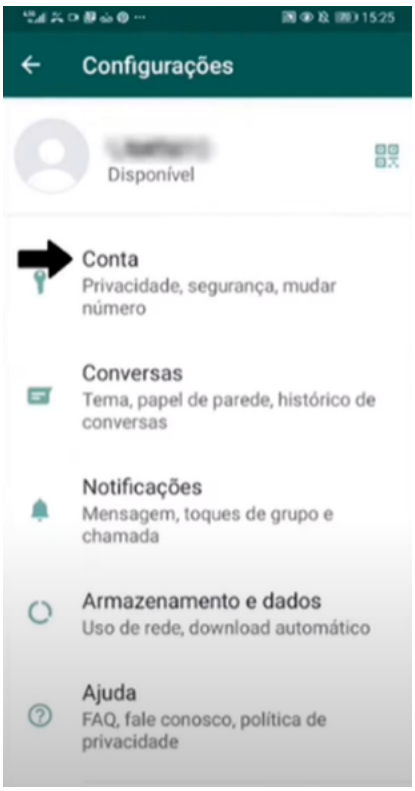
1. Abra o whatsapp e toque nos “três pontinhos” do canto superior direito.



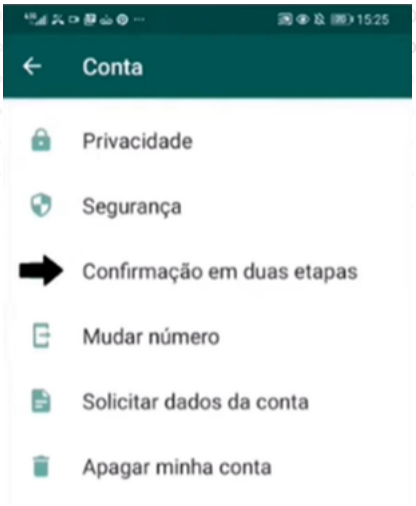
2. Toque em “Configurações”.



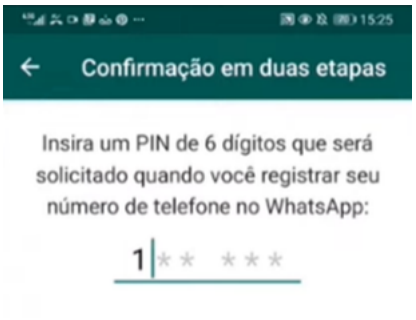
3. Toque em “Conta”.



4. Toque em “Confirmação em duas etapas.

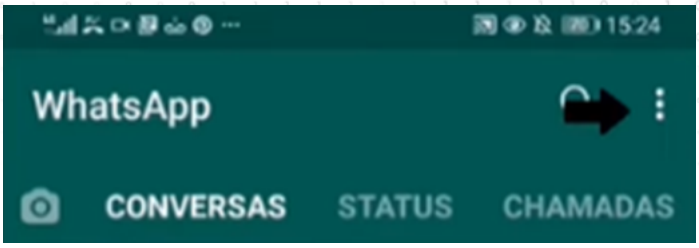


5. Ative a opção e crie uma senha de seis dígitos para a autenticação em duas etapas. Essa senha será solicitada sempre que você desinstalar e reinstalar o whatsapp em seu smartphone ou se você trocar de aparelho e desejar usar seu whatsapp nele.

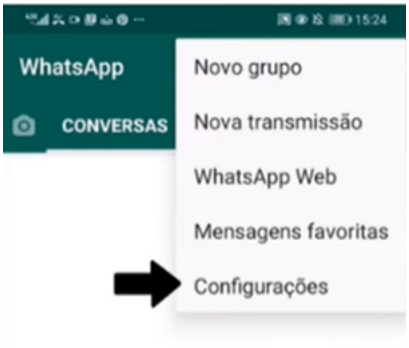


Aumente a privacidade no whatsapp

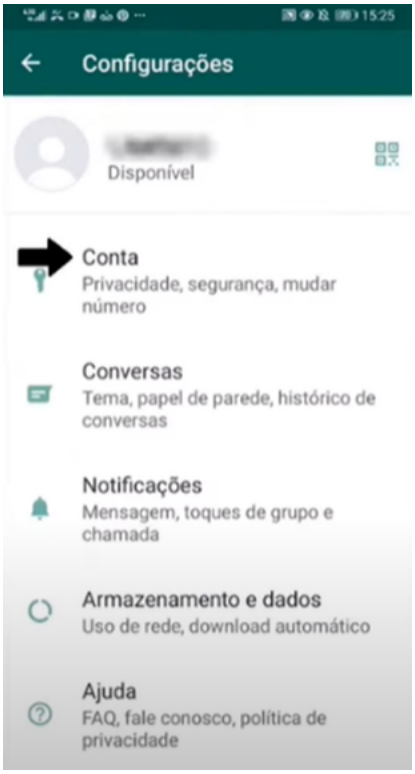
1. Abra o whatsapp e toque nos “três pontinhos” do canto superior direito.



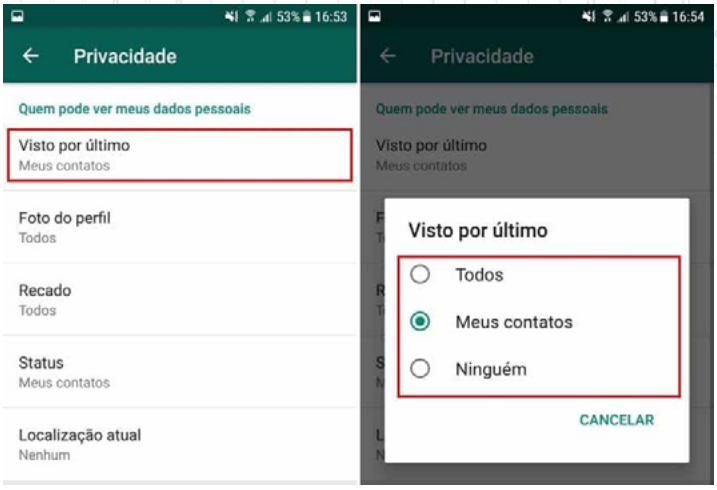
2. Depois toque em “Configurações”.



3. Selecione “Conta”.



4. Em “Privacidade” ajuste todas as opções para “Meus contatos”. Fazendo isso, somente as pessoas que realmente estiverem dentre os seus contatos poderão ver quando você foi visto por último, sua foto de perfil, seus recados, seu status e sua localização.



Para mais informações acesse: https://www.whatsapp.com/privacy/?lang=pt_br

Proteja sua conta do Gmail com a verificação em duas etapas

Com a verificação em duas etapas, também conhecida como autenticação de dois fatores, você adiciona uma camada a mais de segurança à sua conta para o caso de sua senha chegar ao conhecimento de golpistas ou pessoas não autorizadas.

Depois de configurar a verificação em duas etapas, você fará login na conta usando:

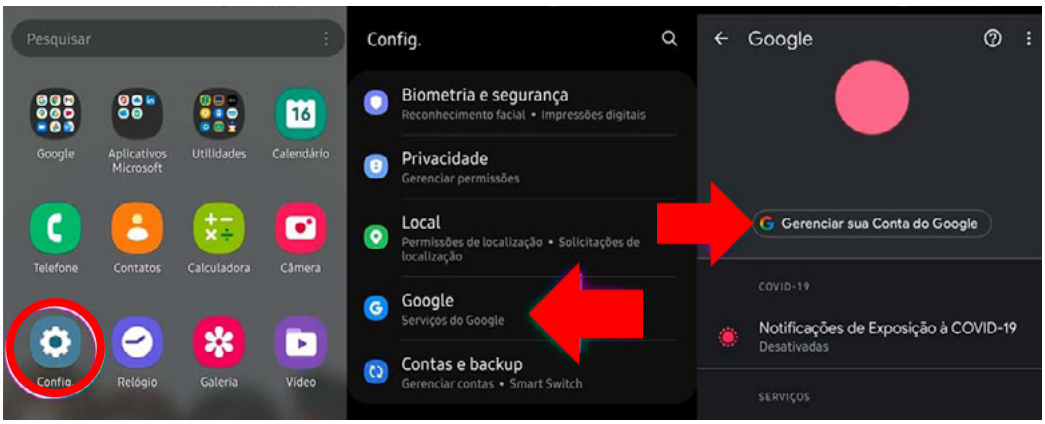
- Algo que você sabe, como sua senha;
- Algo que você possui, como seu smartphone.

Veja como ativar a verificação em duas etapas no Gmail

1. Abra o app “Config” do smartphone.

2. Selecione “Google”.

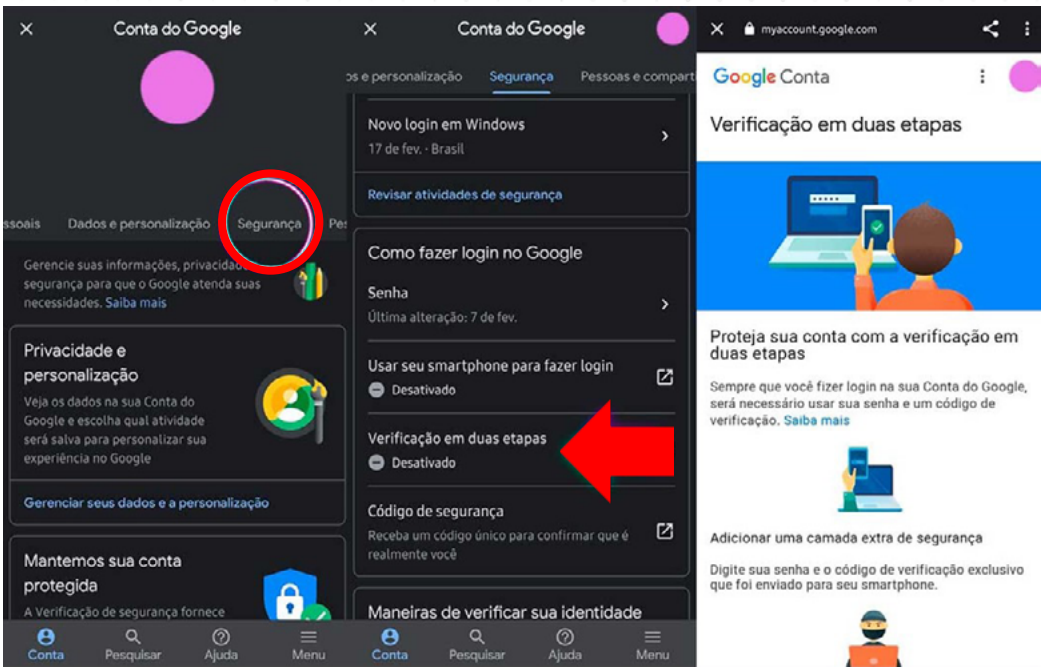
3. toque em “Gerenciar sua conta do Google”.



4. No painel de navegação, selecione “Segurança”.

5. No quadro escrito “Como fazer login no Google”, selecione “Verificação em duas etapas” e “Primeiros passos”.

6.Siga as etapas exibidas na tela.



Caso sua conta “usuario@gmail.com” esteja associada ao seu trabalho ou à sua escola e não seja possível configurar a verificação em duas etapas, entre em contato com seu administrador.

Verificar sua identidade com uma segunda etapa

Depois de ativar a verificação em duas etapas, você precisará concluir uma segunda etapa para verificar sua identidade durante o login. Para ajudar a proteger sua conta, o Google pedirá que você conclua uma segunda etapa específica.

Para mais informações acesse:
https://support.google.com/accounts/answer/185839?hl=pt-BR&co=GENIE.Platform%3DAndroid&oco=1

Verificação de segurança no facebook

A Verificação de segurança ajudará você a:

- Receber alertas quando alguém tentar entrar em sua conta em um computador ou dispositivo móvel não reconhecido.
- Saber como proteger sua senha.

Para mais informações acesse: https://pt-br.facebook.com/help/799880743466869

Autenticação em dois fatores no facebook

A autenticação em dois fatores do facebook é um recurso opcional que dá mais segurança à sua conta do facebook. Veja como ativar:

1. Acesse as “configurações”.

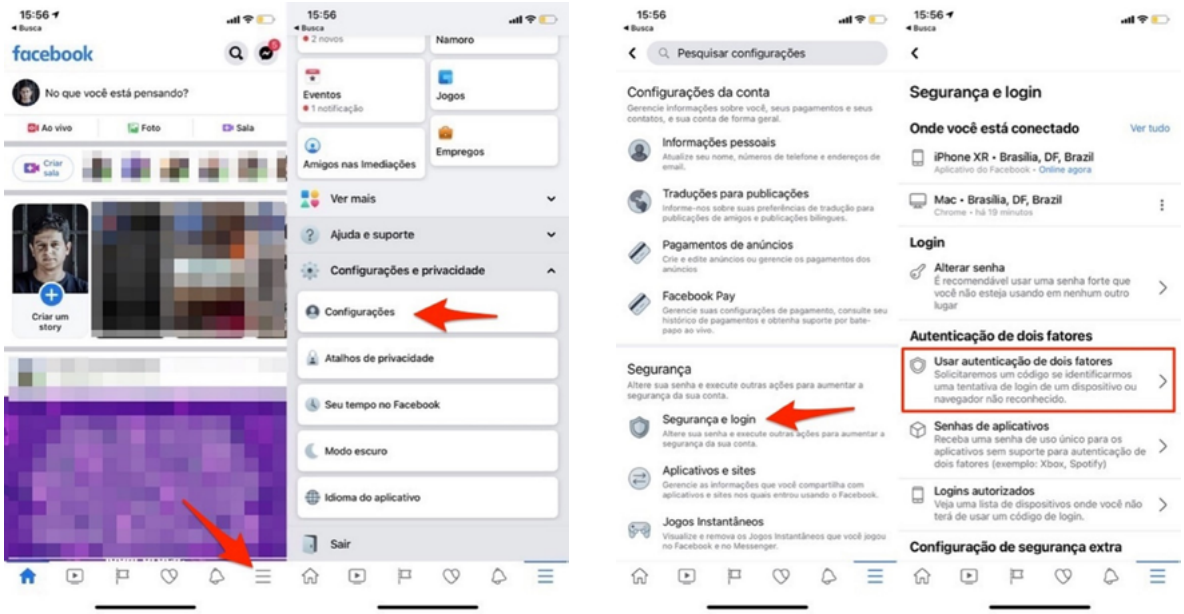
2. Clique em “senha e segurança”.

2. Role a tela para baixo até a opção “usar autenticação de dois fatores” e clique em “editar”.

3. Escolha o método de segurança que deseja adicionar e siga as instruções na tela.

4. Ao configurar a autenticação de dois fatores no Facebook, você precisará escolher um dos três métodos de segurança:

- Tocar na chave de segurança em um dispositivo compatível.
- Códigos de login de um aplicativo de autenticação de terceiros.
- Códigos de SMS no seu celular.



Para maiores informações acesse: https://pt-br.facebook.com/help/799880743466869

Autenticação de dois fatores no Instagram

Para ativar a autenticação de dois fatores no aplicativo Instagram:

1. Acesse seu perfil tocando no ícone “ ” ou na sua foto de perfil do canto inferior direito.

2. Toque no ícone “ ” no canto superior direito. Em seguida, clique em configurações “ ”

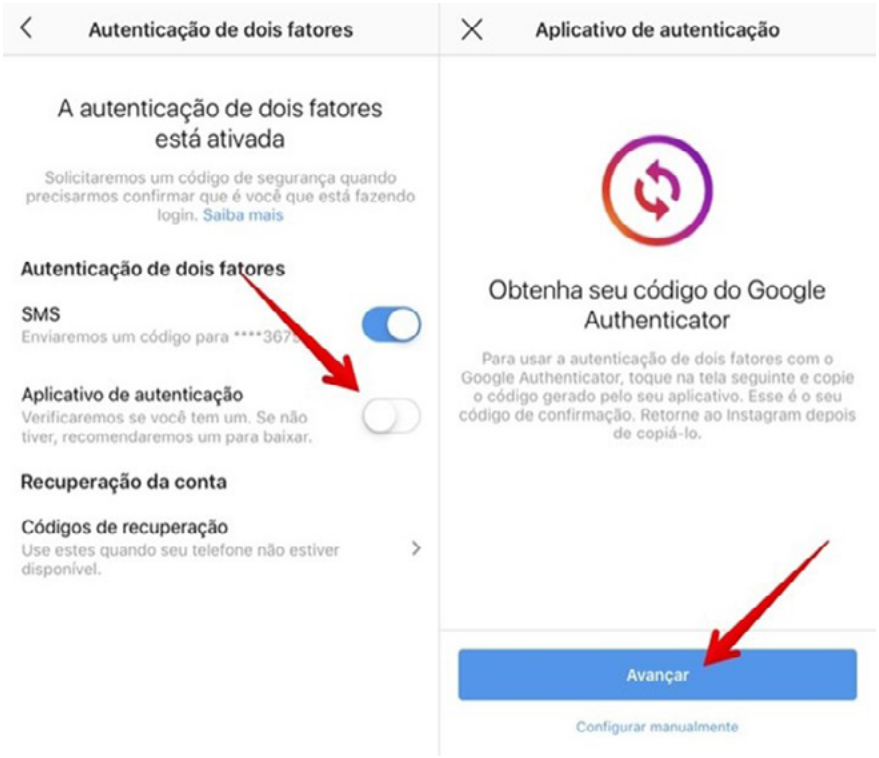
3. Toque em Segurança e em Autenticação de dois fatores.

4. Toque em Começar na parte inferior.

5. Escolha o método de segurança que deseja adicionar e siga as instruções na tela.

Ao configurar a autenticação de dois fatores no Instagram, você precisará escolher um dos dois métodos de segurança:

- Códigos de mensagem de texto (SMS) no celular.
- “Google Authenticator”.

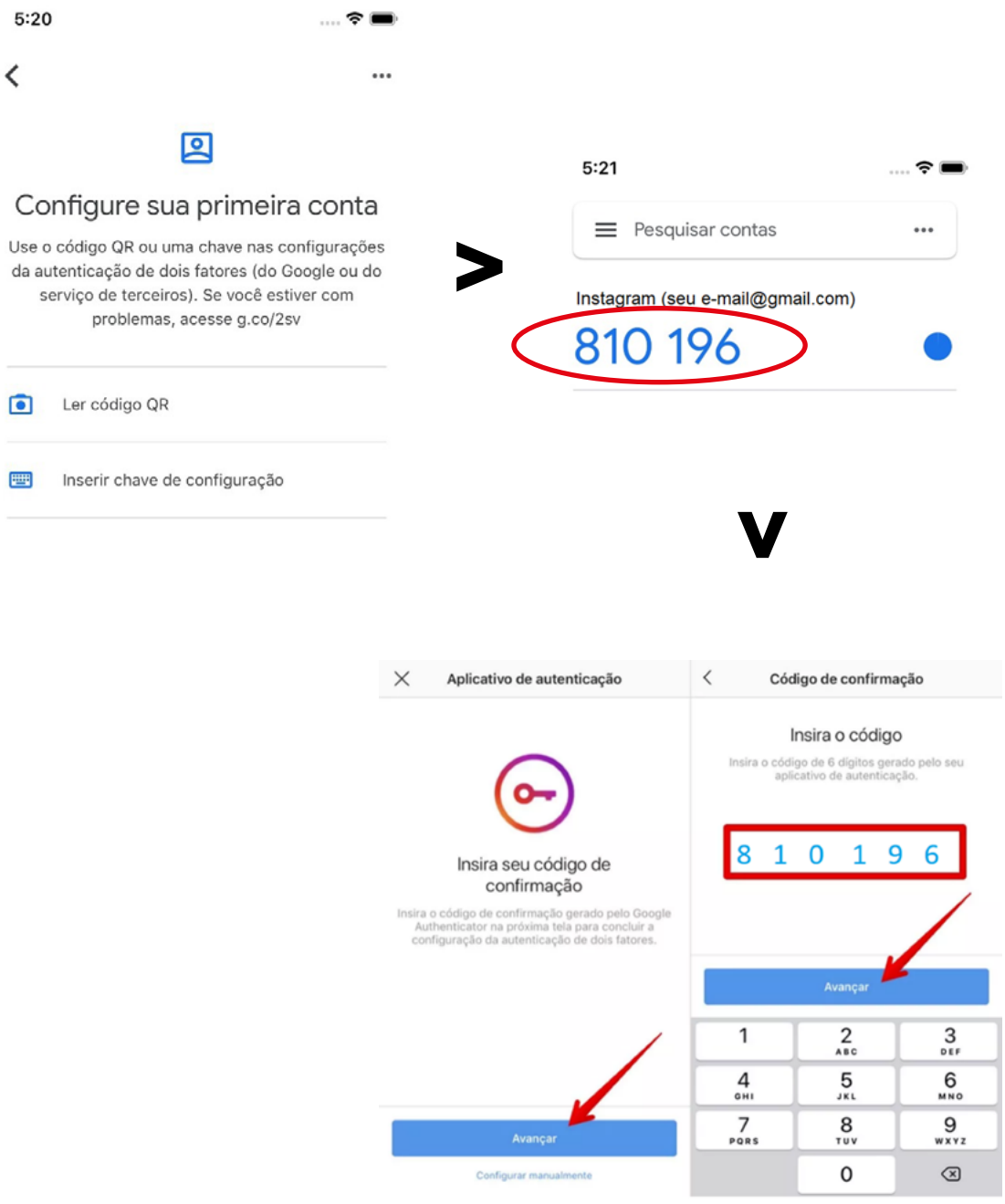


Smartphone protegido - “Android”

“Google Authenticator”

Como ativar:
1. Baixe o aplicativo na “Google Store”.
2. Instale o aplicativo.
3. Clique no botão: “ler código QR”.
4. Utilize a câmera do seu celular para efetuar a leitura do código QR.
5. Insira o código que aparece na tela para efetuar o login no Instagram.

Para maiores informações acesse: https://about.instagram.com/pt-br/community/safety



Não envie dados sensíveis por redes “wi-fi” públicas

As redes “wi-fi” abertas ou públicas não são seguras. Redes de aeroportos, hotéis e lojas podem ser monitoradas e não se sabe quem gerencia tais redes. Não é recomendável enviar ou receber materiais ou dados sensíveis ou sigilosos através dessas conexões. Se for extremamente necessário, desconecte-se da rede aberta e faça a troca pela rede de dados móveis de seu celular (rotear a internet do celular).

Cuidado com aplicativos gratuitos

O desenvolvimento de aplicativos tem um custo elevado. Assim, o dono do aplicativo visará obter lucro. Caso ele não cobre diretamente pelo aplicativo, utilizará outros meios para monetizar a operação, dente eles, vender dados dos usuários para outras empresas.

Lembre-se, se você não paga pelo produto, você é o produto.

Evite instalar aplicativos que não estejam na “Google App Store”

Instalar aplicativos de forma manual, sem utilizar a loja “Google Play”, é um procedimento de risco, uma vez que expõe o celular a programas não verificados pelo Google. Mesmo que seja um programa que você precise utilizar, na dúvida, evite instalar aplicativos que não estejam na plataforma “Google Play”.

Mantenha seu Android sempre atualizado

Procure manter o sistema “Android” do seu celular atualizado com as últimas versões do sistema operacional.

Nunca clique em “links” suspeitos

Não clique em links suspeitos enviados através de e-mails, mensagens SMS ou whatsapp, dos quais você não conhece a origem. Igualmente, evite “sites” que parecem suspeitos, como os que oferecem serviços, vantagens ou ofertas imperdíveis. Assim você elimina o risco de virar alvo de mensagens de “SPAM”, rastreadores e outros tipos de “malware” (aplicativos maliciosos).

Se você for vítima de um golpe ou tiver seu smartphone subtraído:

Procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através da Delegacia Eletrônica:
https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home

Proteja-se!

POLÍCIA CIVIL SÃO PAULO CIVIL SP