

COMO PROTEGER SEU CELULAR CONTRA ROUBOS/FURTOS

LGPD NA PRÁTICA





**Experiência, agilidade e inovação:
três competências que marcam o nosso DNA**

A expertise nas mais variadas áreas do Direito nos permite oferecer soluções criativas às demandas de nossos clientes nacionais e internacionais e garante segurança a suas atividades.

**NOSSA ÁREA DE PROTEÇÃO DE DADOS
E CYBERSECURITY**

**Dedicação integral na solução dos desafios
mais complexos da era digital.**

Nossa área de Proteção de Dados e *Cybersecurity* é focada na solução de problemas e na resposta a situações desafiadoras que envolvem o ativo mais valioso das organizações nos tempos atuais: dados. Sabendo da importância desse tema para nossos clientes, o BMA possui uma equipe altamente especializada, com conhecimentos em tecnologia e segurança da informação, e dedicada integralmente a auxiliar nossos clientes a enfrentar os complexos desafios do mercado atual e da digitalização forçada ocorrida ao longo dos últimos anos.

Nosso time conta com experiência prática na resposta aos cenários mais adversos, na gestão de crises ocasionadas por incidentes de segurança e por ataques cibernéticos, como casos de ransomware, sendo capaz de prontamente auxiliar nossos clientes nos momentos críticos, acompanhando investigações forense, elaborando estratégias de respostas e comunicações, interagindo com órgãos reguladores e com titulares de dados, e defendendo seus interesses em processos administrativos, judiciais ou arbitrais.

FOTO CAPA

Unsplash

FECHAMENTO: JUNHO, 2026

Este material foi redigido para fins de informação e debate, não devendo ser considerado como opinião legal para operações ou transações específicas.

Os textos desta publicação foram produzidos por profissionais do BMA Advogados.

A reprodução de qualquer artigo depende de prévia autorização.

bma@bmalaw.com.br

NOSSAS PRINCIPAIS ÁREAS DE ATUAÇÃO:

ADVOCACY CONCORRENCIAL
AGRONEGÓCIO
AMBIENTE, CLIMA E MINERAÇÃO
ARBITRAGEM
BANCOS E SERVIÇOS FINANCEIROS
BLOCKCHAIN E INOVAÇÃO
CHINA DESK
COMPLIANCE, INVESTIGAÇÕES E DIREITO SANCIONADOR
CONCORRENCIAL
CONTRATOS COMERCIAIS E FRANQUIAS
DUE DILIGENCE
ENERGIA
ESG
ESPORTES E ENTRETENIMENTO
FRENCH DESK
GERENCIAMENTO DE CRISE
IBERIAN DESK
INDÚSTRIA
INDÚSTRIA MINERAL E METALÚRGICA
INFRAESTRUTURA, REGULAÇÃO E ASSUNTOS GOVERNAMENTAIS
MERCADOS FINANCEIRO E DE CAPITAIS
NEGÓCIOS IMOBILIÁRIOS
ÓLEO E GÁS
PENAL EMPRESARIAL
PLANEJAMENTO PATRIMONIAL E SUCESSÓRIO
PRIVATE EQUITY
PRIVATIZAÇÕES E CONCESSÕES
PROJETOS DE CONSTRUÇÃO
PROPRIEDADE INTELECTUAL
PROTEÇÃO DE DADOS E CYBERSECURITY
REESTRUTURAÇÃO E INSOLVÊNCIA
RELAÇÕES GOVERNAMENTAIS
SEGUROS
SERVIÇOS DE PAGAMENTO E FINTECH
SOCIETÁRIO E M&A
SOLUÇÃO DE CONFLITOS
TECNOLOGIA E NEGÓCIOS DIGITAIS
TELECOMUNICAÇÕES
TRABALHISTA
TRIBUNAIS SUPERIORES
TRIBUTÁRIO

NOSSOS ESCRITÓRIOS:

SÃO PAULO

Av. Presidente Juscelino Kubitschek, 1.455
10º andar - Itaim Bibi - São Paulo - SP
CEP 04543-011
T +55 11 2179.4600

RIO DE JANEIRO

BMA Corporate - Largo do Ibam, 1
4º andar - Humaitá - Rio de Janeiro - RJ
CEP 22271-070
T +55 21 3824.5800

BRASÍLIA

SHS Quadra 6 - Conjunto A - Bloco E
19º andar - Complexo Brasil 21 - Asa Sul -
Brasília - DF
CEP 70316-902
T +55 61 3218.0300

BELO HORIZONTE

Avenida do Contorno, 6594 - 7º andar
Savassi - Belo Horizonte - MG
CEP 30110-044
T +55 31 2391.7399



Sumário

04 INTRODUÇÃO

05 PROTEÇÕES UNIVERSAIS

- 05 1. Multifator de Autenticação (“MFA”)
 - 09 2. Senhas
-

11 PROTEÇÕES PARA IPHONE

- 11 1. Proteção de Dispositivo Roubado
 - 12 2. Buscar (Find My)
 - 14 3. Código de Desbloqueio
 - 15 4. Atualizações Automáticas
 - 17 5. Bloqueio da Central de Controle
 - 18 6. Bloquear alteração de Face ID, Código e Buscar
 - 21 7. Bloqueio de Apps por Tempo
 - 22 8. Ocultar Notificações
 - 23 9. Bloqueio Automático de Tela
 - 24 10. Limitação do AirDrop
 - 25 11. Restringir Acesso a Apps
 - 26 12. Bloqueio de Notas
-

27 PROTEÇÕES PARA ANDROID

- 27 1. Proteção Contra Roubo
- 28 2. Find My Device
- 29 3. Bloqueio Seguro e Smart Lock
- 30 4. Bloqueio Automático de Tela
- 31 5. Ocultar Notificações

INTRODUÇÃO

A Lei nº 13.709/2018 (“Lei Geral de Proteção de Dados Pessoais” ou “LGPD”), que entrou em vigor em 18 de setembro de 2020, inaugurou um sistema protetivo especial em relação ao tratamento de dados pessoais realizado por empresas, órgãos públicos e até pessoas físicas.

Dentre as obrigações trazidas pela legislação, uma das mais relevantes está relacionada à segurança da informação, aspecto fundamental para garantir conformidade com a norma.

De acordo com o art. 46 da LGPD, agentes de tratamento devem implementar medidas técnicas e administrativas para proteger os dados pessoais que tratam contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Embora a Agência Nacional de Proteção de Dados (“ANPD”) ainda não tenha editado norma que estipule padrões técnicos mínimos de segurança da informação que devem ser adotados, há diversas medidas reconhecidas no mercado e pela ANPD como boas práticas para esses fins.

O intuito dessas medidas é garantir maior proteção aos pilares da segurança da informação: confidencialidade, integridade e disponibilidade. O primeiro desses pilares é potencialmente o mais problemático em muitos casos, já que sua violação resulta nos conhecidos “vazamentos de dados”.

No cenário atual, é comum que colaboradores de uma empresa acessem dados tratados por sua organização através de seus celulares, sejam eles aparelhos corporativos ou pessoais.

Se você possui acesso ao seu e-mail corporativo ou ao comunicador instantâneo oficial da sua empresa (como Microsoft Teams, Slack, entre outros) no seu celular, ou se usa o WhatsApp ou outros serviços de mensageria para fins profissionais, quando o seu aparelho é roubado/furtado isso pode resultar num vazamento de dados.

Nessas circunstâncias, um terceiro (que pegou seu aparelho de forma indevida) poderá ter acesso não autorizado às informações contidas no seu celular.

Situações como essa acontecem diariamente, especialmente em grandes centros urbanos no Brasil, e, além dos prejuízos materiais que acarretam, trazem outra consequência indesejável: uma potencial violação à LGPD.

Este e-book apresenta dicas práticas de como proteger os dados que estão no seu celular em caso de roubo/furto. São medidas que podem ser implementadas de forma fácil e rápida, seja pelo seu empregador ou por você mesmo.

Ainda que a sua implementação possa não impedir por completo o acesso indevido de terceiros aos dados contidos no seu celular, elas inevitavelmente são práticas recomendadas para garantir maior aderência ao dever de segurança da informação previsto na LGPD.

PROTEÇÕES UNIVERSAIS

1

Multifator de Autenticação (“MFA”)

A autenticação em multifator é uma camada adicional de segurança que exige duas ou mais formas de autenticação (como o envio de código por SMS). Ela é especialmente relevante quando alguém descobre a sua senha, já que somente com a senha não será possível acessar suas contas.

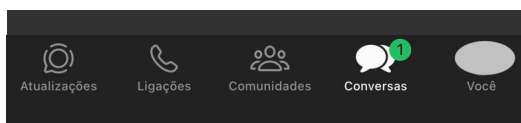
A maior parte das aplicações que você usa diariamente permite a habilitação do MFA, sendo necessário realizar a sua habilitação individualmente, em cada aplicação específica.

Abaixo são apresentados exemplos de como habilitar o MFA em duas aplicações frequentemente utilizadas: WhatsApp e Gmail.

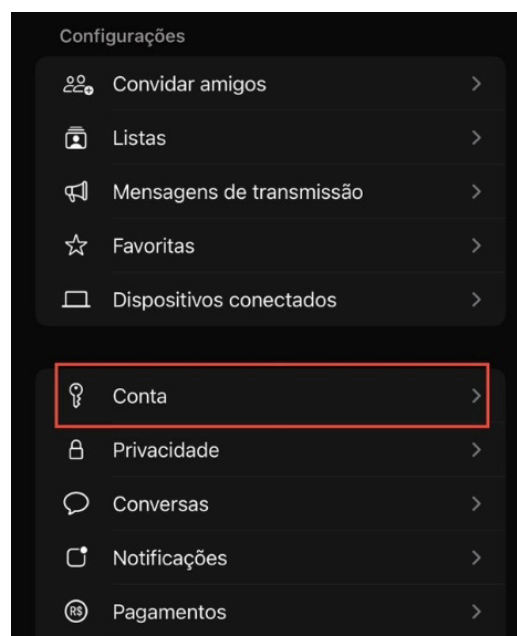
WhatsApp



Na barra inferior (em iPhones)¹, toque no botão no canto direito, que pode ser a sua imagem (na versão pessoal do WhatsApp) ou o botão configurações (na versão WhatsApp Business):

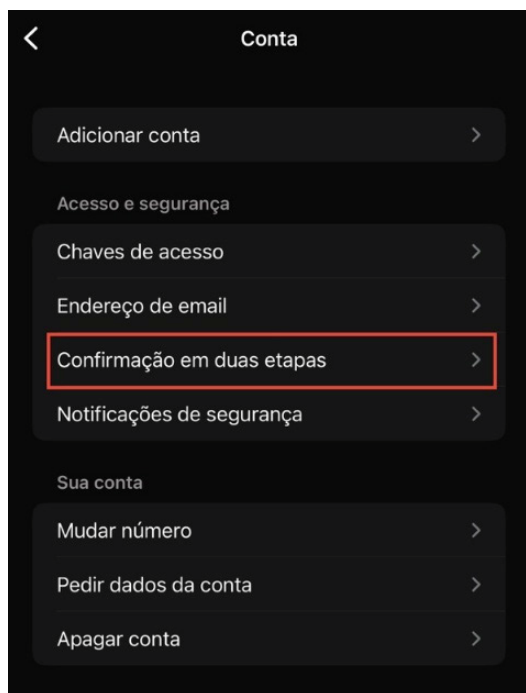


Toque em *Conta*:

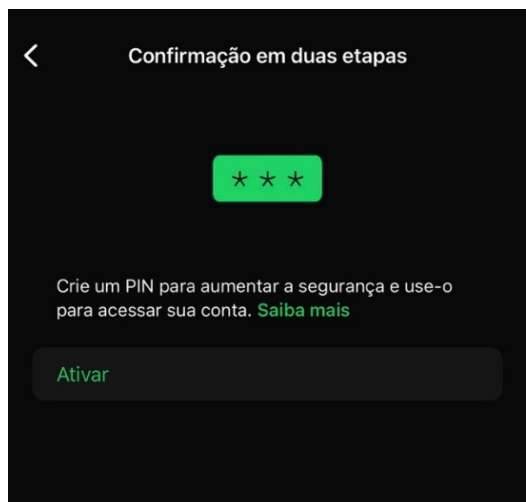


1. Em celulares Android, a opção de configurações pode aparecer clicando nos três pontos no topo direito da tela.

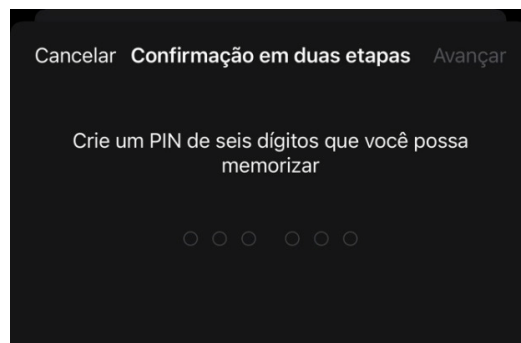
Toque em *Confirmação em duas etapas*:



Toque em *Ativar*:

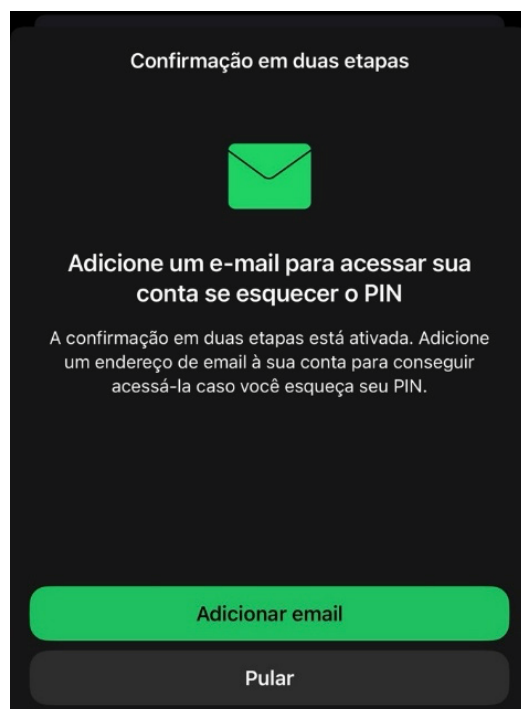


Crie um PIN de 6 dígitos
(é fundamental que você lembre
desse código, já que para acessar o
WhatsApp em outro telefone será
necessário digitar esse código):



Confirme o PIN.

Caso queira, insira e confirme seu
endereço de e-mail:

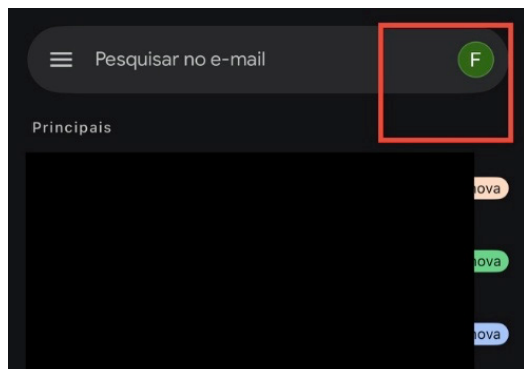


**Nunca compartilhe
seu PIN com terceiros.**

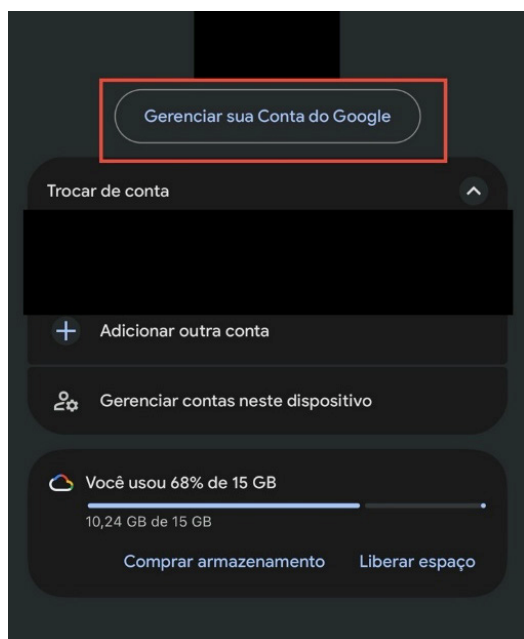
Gmail



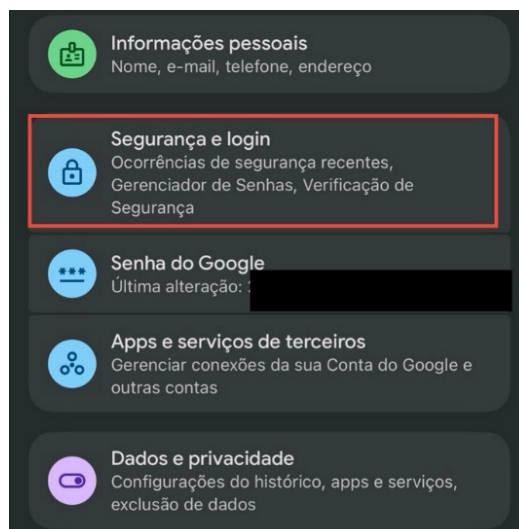
Toque na *inicial do seu nome*, no topo direito da tela:



Toque em *Gerenciar sua Conta do Google*:



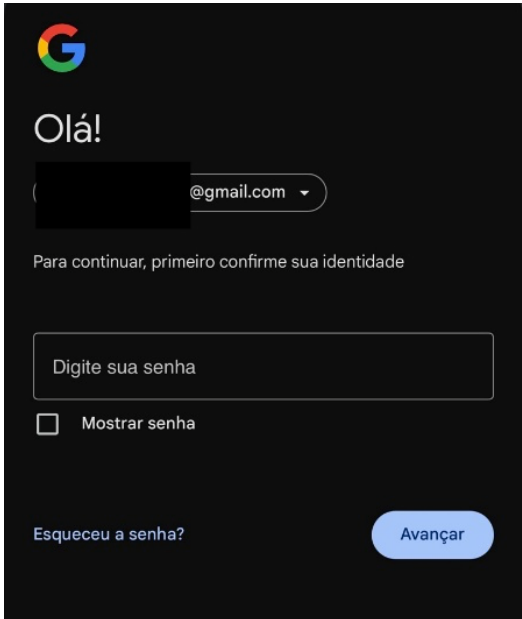
Toque em *Segurança e login*:



Toque em *Verificação em Duas Etapas*:



Insira sua Senha:



The image shows the Google login interface. At the top is the Google logo. Below it, the text "Olá!" is displayed. A text input field contains an email address ending in "@gmail.com". Below the input field, the text "Para continuar, primeiro confirme sua identidade" is shown. A password input field with the placeholder "Digite sua senha" is present, along with a checkbox labeled "Mostrar senha". At the bottom left is a link "Esqueceu a senha?" and at the bottom right is a blue button labeled "Avançar".

Escolha a forma de verificação, que pode ser, por exemplo, o envio de um código por SMS ou a utilização de um aplicativo específico de MFA (como o *Google Authenticator*).



The image shows the "Verificação em duas etapas" (Two-step verification) screen. At the top, the title "Verificação em duas etapas" is displayed. Below the title is an illustration showing a smartphone, a key icon, and a checkmark. The text "Sua conta está protegida com a verificação em duas etapas" is followed by instructions: "Use uma camada extra de segurança para evitar que hackers acessem sua conta." and "A menos que você faça login usando uma chave de acesso, será necessário concluir a segunda etapa mais segura disponível na sua conta. Você pode atualizar suas segundas etapas e opções de login nas configurações quando quiser. Acesse as Configurações de segurança". Below this is a section titled "Segundas etapas" with the instruction "Mantenha essas informações atualizadas e adicione mais opções de login para que você possa sempre acessar sua Conta do Google". Two options are listed: "Chaves de acesso e de segurança" with a yellow warning icon and the text "Adicione uma chave de acesso", and "Solicitação do Google" with a green checkmark icon and the text "2 dispositivos". Both options have a right-pointing arrow.

É preferível sempre utilizar um aplicativo de MFA como forma de autenticação, em vez do envio de códigos por SMS. Isso evita ataques sofisticados conhecidos como *SIM Swapping*, quando o atacante consegue transferir o seu número para um cartão SIM controlado por ele, de forma que ele receberia o código enviado por SMS.

Algumas opções de aplicativos de MFA, que podem ser baixados na loja de aplicativos do seu celular:



**Google
Authenticator**



**Microsoft
Authenticator**



**Twilio
Authy**

A habilitação do MFA é recomendada pela ANPD no Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte (“Guia Orientativo da ANPD”)².

2. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_seguranca_da_informacao_para_atpps_defeso_eleitoral.pdf/@@display-file/file. Acesso em: 8 jun. 2026. Parágrafo 41.



2

Senhas

A primeira porta de entrada para as suas contas é a sua senha. A utilização de MFA fortalece a fechadura da sua porta, mas a sua senha continua sendo relevante.

Criar uma senha forte em 2026 depende de dois fatores principais: o tamanho da sua senha (quantidade de caracteres) e a complexidade da senha (utilização de números, letras maiúsculas, letras minúsculas e caracteres especiais).

O problema de uma senha curta e pouco complexa é que ela pode ser facilmente quebrada por métodos de tentativa e erro (chamados de ataques de força bruta), que podem ser implementados de forma automatizada, com milhares de tentativas por segundo.

O gráfico abaixo indica o tempo necessário para quebrar uma senha de acordo com seu tamanho e complexidade e com base no poder computacional disponível em 2025:

Time it takes a hacker to brute force your password in 2025³

Hardware: 12 x RTX 5090 | Password hash: bcrypt (10)

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years



Senhas maiores são tão relevantes quanto senhas complexas.

3. Elaborado por Hive Systems. Disponível em: <https://www.hivesystems.com/blog/are-your-passwords-in-the-green>

Se for necessário escolher entre uma senha com 12 caracteres formadas só por números, ou uma senha de 4 caracteres formadas por números, letras maiúsculas, letras minúsculas e símbolos, a primeira opção é melhor.

Mas escolher uma única senha forte não é suficiente. É importante ter uma senha para cada aplicação diferente. Uma senha para o banco, uma para o e-mail, uma para o Instagram, uma para o LinkedIn, etc.

Como lembrar de tantas senhas é quase impossível, o ideal é utilizar um gerenciador (ou cofre) de senhas. iPhones e celulares Android possuem gerenciadores nativos de senhas (*Chaveiro iCloud* e *Gerenciador Google*, respectivamente), mas há também opções como *Bitwarden* e *NordPass*.

A função desses aplicativos é criar senhas específicas para cada aplicação, para que você não precise recordar de todas as senhas, somente copiar e colar as senhas que estão no gerenciador.

Uma dica essencial:

a senha do gerenciador de senhas precisa ser efetivamente forte, preferencialmente com mais de 20 caracteres.



PROTEÇÕES PARA IPHONE



1

Proteção de Dispositivo Roubado

Ativar a *Proteção de Dispositivo Roubado* faz com que algumas ações, como acessar senhas no Chaveiro iCloud, exijam autenticação biométrica por Face ID ou Touch ID e o decurso de ao menos 1 hora para que determinadas configurações possam ser alteradas.

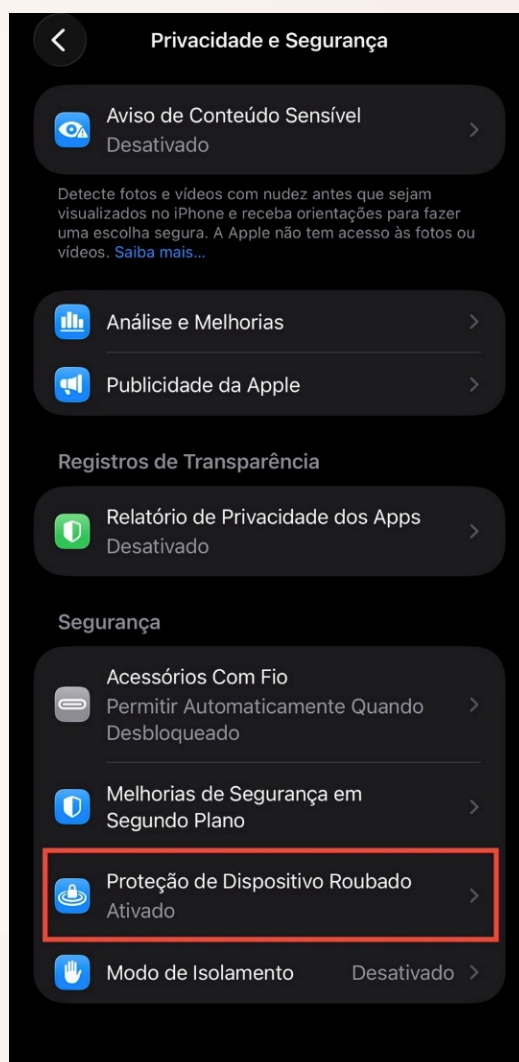
Para ativar, toque no ícone de *Ajustes*:



Depois toque em *Privacidade e Segurança*:



Depois toque em *Proteção de Dispositivo Roubado*:



Ative a proteção (caso esteja desativada) e escolha entre exigir adiamento de segurança *longe de locais familiares* (locais que você frequenta constantemente, como sua casa ou seu trabalho) ou *sempre* (opção mais segura).



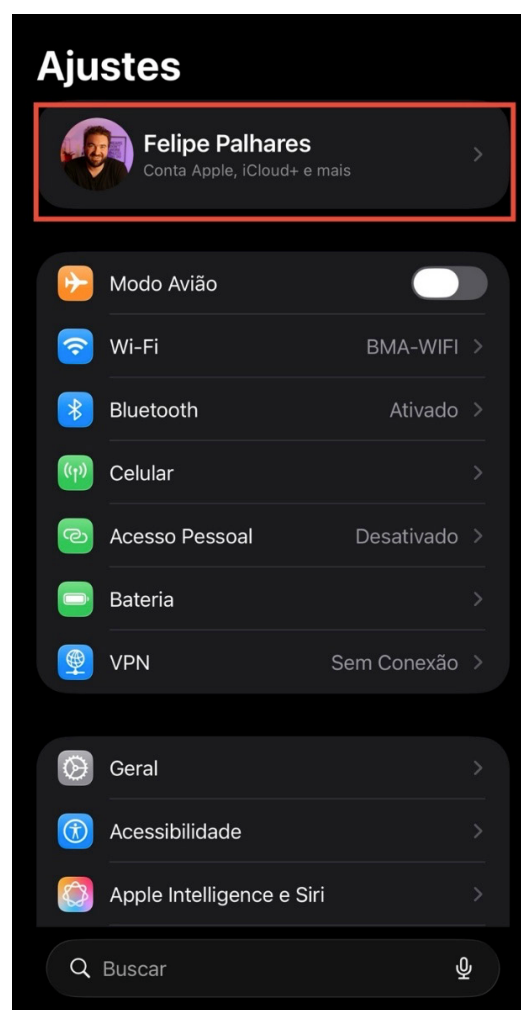
2 Buscar (Find My)

O recurso Buscar (Find My) permite localizar o seu celular por meio de outro dispositivo conectado à sua conta do iCloud ou através do site <https://www.icloud.com/find>.

Para ativar, toque no ícone de *Ajustes*:



Toque no *seu nome*, no topo da tela:



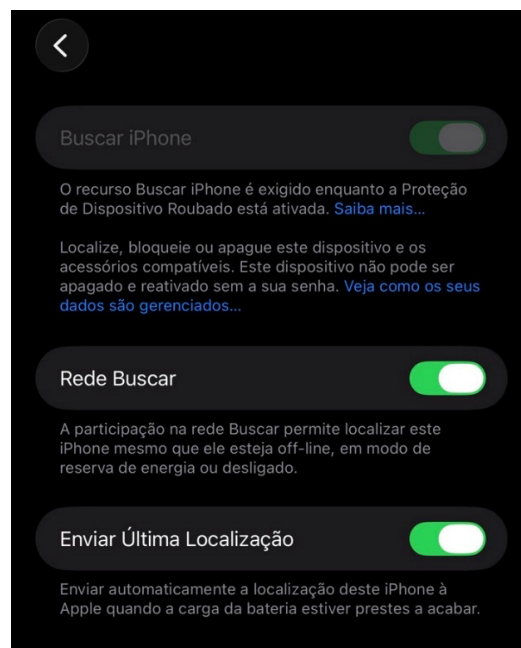
Toque em *Buscar*:



Toque em *Buscar iPhone*:



Ative a opção de *Buscar iPhone*, bem como as opções da *Rede Buscar* (que permite a localização mesmo offline) e de *Enviar Última Localização* (que envia automaticamente a posição quando a bateria está acabando).



3

Código de Desbloqueio

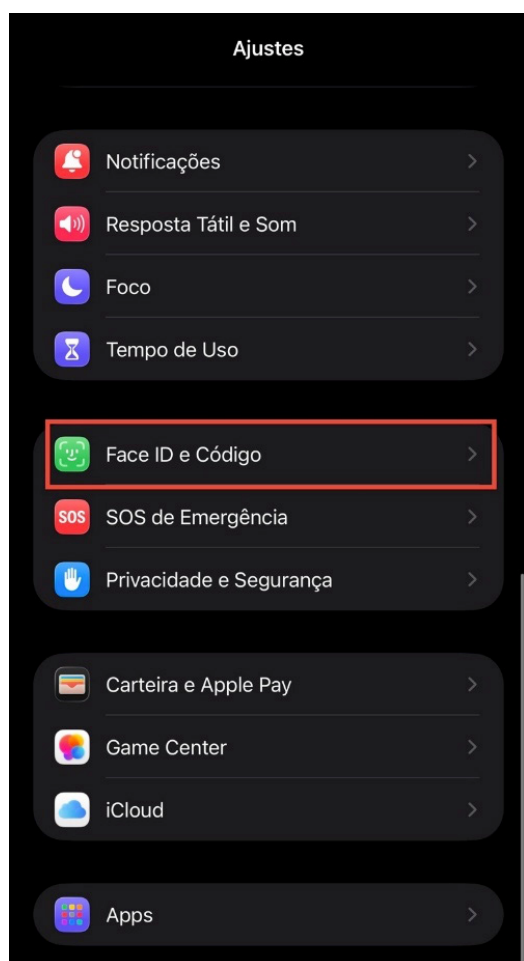
O iPhone permite a configuração de códigos de desbloqueio em quatro formatos: de 4 números, de 6 números, só números sem limite e alfanuméricos.

Embora as duas primeiras sejam as mais comuns, a opção alfanumérica é a mais segura, pelas razões já indicadas no item *Senhas* da seção de *Proteções Gerais*.

Para configurar uma senha alfanumérica no iPhone, toque em *Ajustes*:



Depois toque em *Face ID e Código*:



Depois toque em *Alterar Código*:



Depois toque em *Opção de Código* e escolha a opção *Código Alfanumérico Personalizado*:



Uma dica para criar uma senha forte: pense num trecho de uma música que você gosta e inclua alguns números e caracteres especiais.

Algo como:

UmavezFlamengosempreFlamengo!1081

4

Atualizações Automáticas

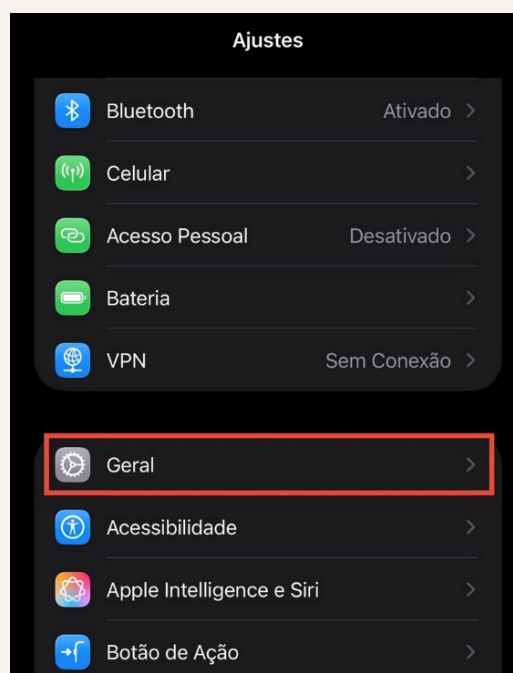
Manter o sistema operacional do seu celular e os aplicativos que você usa atualizados é fundamental. Atualizações são comumente liberadas pelos desenvolvedores para corrigir falhas identificadas, que podem incluir fragilidades de segurança. Nesse sentido, continuar utilizando um sistema operacional ou aplicativos desatualizados abre uma brecha de segurança relevante.

No Guia Orientativo da ANPD, é mencionada a relevância de manter aplicativos atualizados e instalar todas as correções de segurança disponíveis⁴.

Para que seu celular faça atualizações do sistema operacional de forma automática, toque em *Ajustes*:



Depois toque em *Geral*:

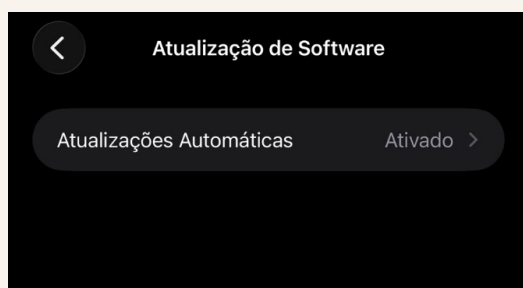


4. Parágrafo 56.

Depois toque em *Atualização de Software*:



E ative a opção *Atualizações Automáticas*:



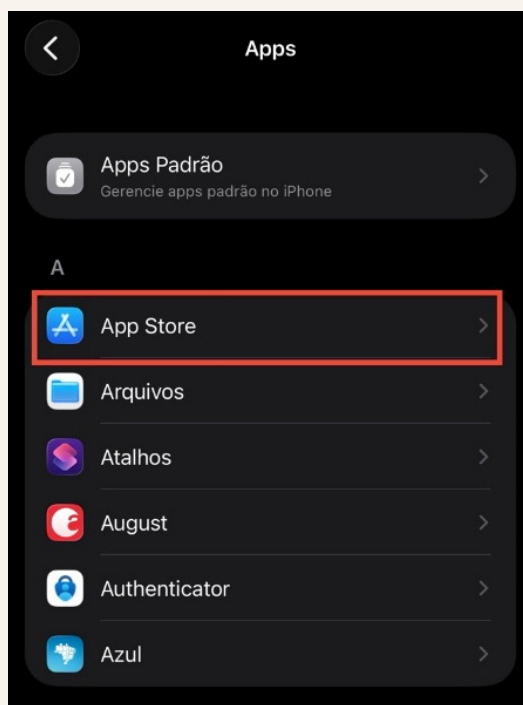
Para garantir que seus aplicativos também sejam atualizados de forma automática, toque em *Ajustes*:



Depois toque em *Apps*:



Depois toque em *App Store*:



E ative a opção *Atualizações de Apps*:



5

Bloqueio da Central de Controle

A Central de Controle, que aparece quando você arrasta o seu dedo do topo direito da tela para baixo, permite realizar diversas ações em poucos toques, como habilitar o Modo Avião ou desabilitar a conexão de dados do seu celular.

Mesmo com o celular bloqueado, pode ser possível acessar a Central de Controle e realizar tais ações, dificultando que o seu celular seja localizado após ser furtado/roubado.

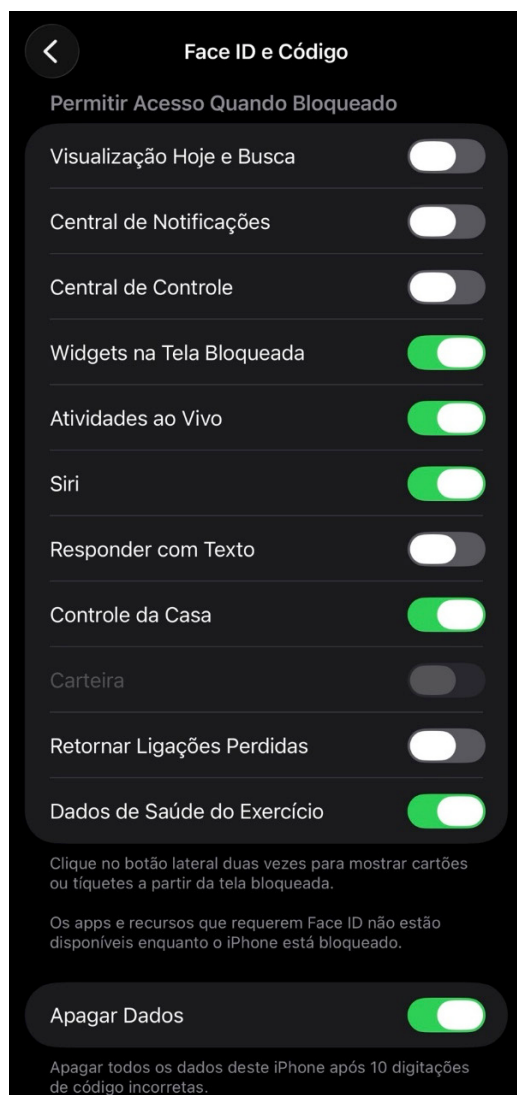
Para evitar que isso aconteça, toque em *Ajustes*:



Depois toque em *Face ID e Código*:



Na seção *Permitir Acesso Quando Bloqueado*, desative a opção *Central de Controle*:



6 Bloquear alteração de Face ID, Código e Buscar

Uma das primeiras ações realizadas por criminosos após o furto/roubo do seu celular é tentar alterar o Face ID e o código de desbloqueio, e desabilitar a opção *Buscar*.

É possível bloquear alterações a essas funções por meio do *Tempo de Uso*.

Essa ferramenta foi primordialmente concebida para permitir controle parental do aparelho, mas serve também para fortalecer a sua proteção. Primeiro é necessário configurar uma senha para o *Tempo de Uso*. Essa senha é diferente do código de desbloqueio do aparelho, e sem ela não será possível alterar o Face ID, o código ou desabilitar a função *Buscar*.

Para isso, toque em *Ajustes*:



Depois toque em *Tempo de Uso*:



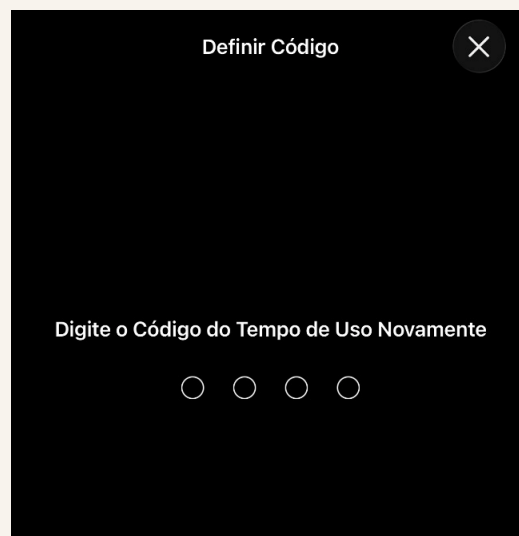
Depois toque em *Bloquear Ajustes do Tempo de Uso*:



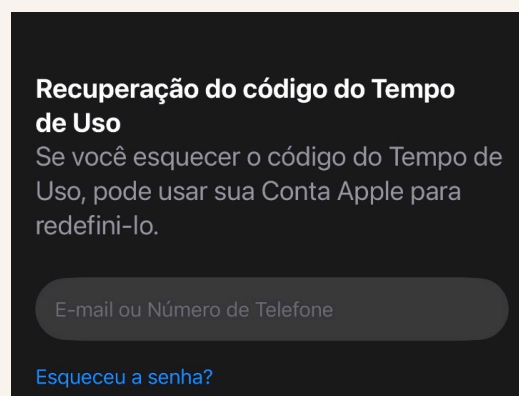
Crie uma senha de 4 dígitos (que é a única opção permitida para essa função):



Confirme a senha de 4 dígitos:



Faça login com a sua conta Apple:

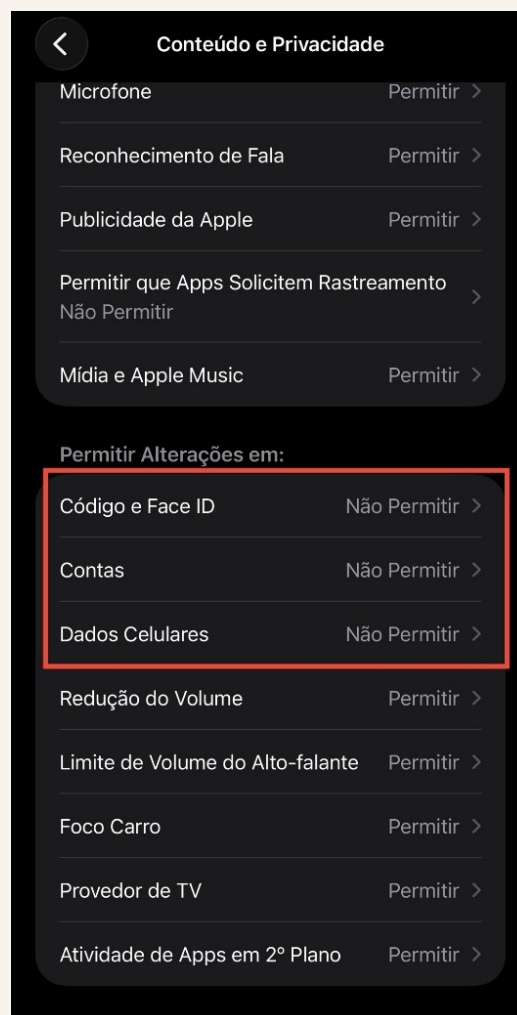


Agora que o código do *Tempo de Uso* foi ativado, é hora de criar as restrições.

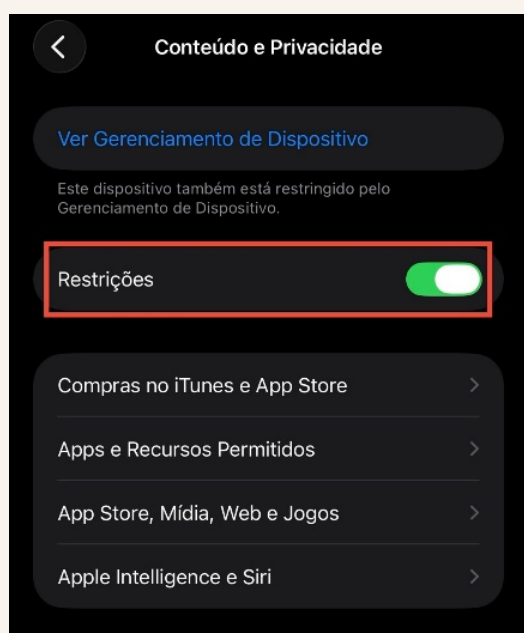
Para isso, dentro de *Tempo de Uso*, toque em *Conteúdo e Privacidade*:



Na seção *Permitir Alterações*, troque *Código e Face ID*, *Contas* e *Dados Celulares* para *Não Permitir*:



Ative o item *Restrições*:



7 Bloqueio de Apps por Tempo

A função Tempo de Uso também permite configurar limites diários de uso de aplicativos específicos.

Esse bloqueio pode ser especialmente relevante para aplicativos de bancos. Com ele ativado, após o decurso do período definido, será necessário digitar o código do Tempo de Uso para continuar a sua utilização.

Para isso, dentro do menu do *Tempo de Uso*, toque em *Limites de Apps*:



Selecione os apps que você deseja limitar o uso (como apps de bancos) e escolha o período de utilização. Uma boa prática é deixar o limite em 0 horas e 0 minutos, de modo que o aplicativo imediatamente exigirá o código do Tempo de Uso.

Só há uma exceção importante: é possível solicitar 1 minuto adicional de uso sem digitar o código do Tempo de Uso. Mas, depois disso, o uso do aplicativo num mesmo dia só será possível após ser digitado o código do Tempo de Uso.

8

Ocultar Notificações

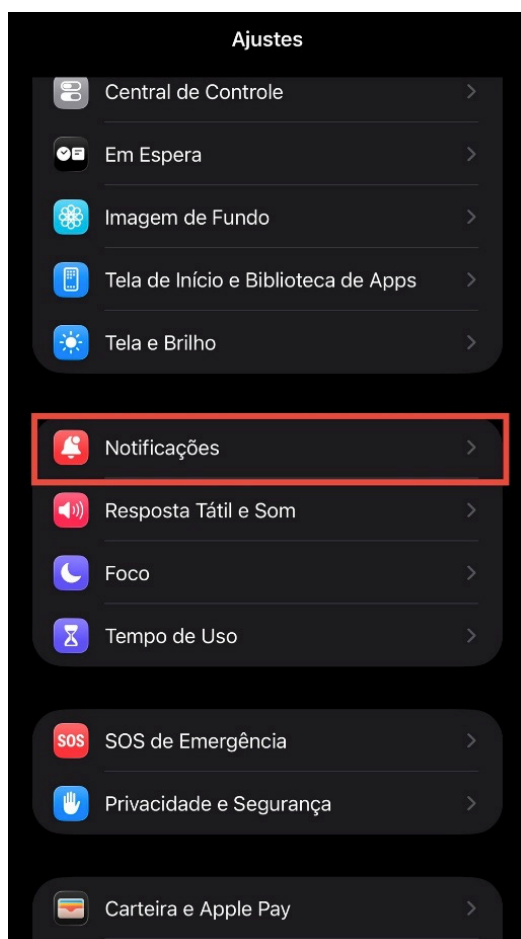
Por padrão, as notificações enviadas por aplicativos (como WhatsApp, Outlook, etc.) ficam visíveis mesmo quando o celular está bloqueado.

Com isso, caso seu celular seja furtado/roubado, quem tiver acesso ao seu aparelho conseguirá ler as mensagens contidas nas notificações.

Para ocultar as notificações, toque em *Ajustes*:



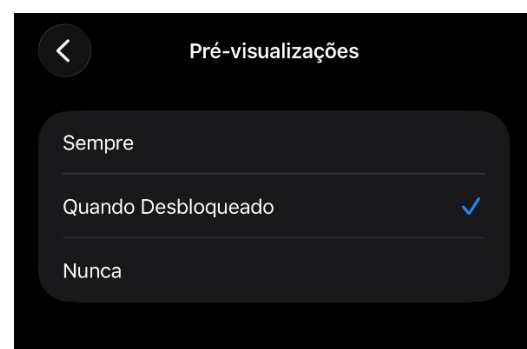
Depois toque em *Notificações*:



Depois toque em *Pré-visualizações*:



E escolha entre as opções *Nunca* ou *Quando Desbloqueado*:



9

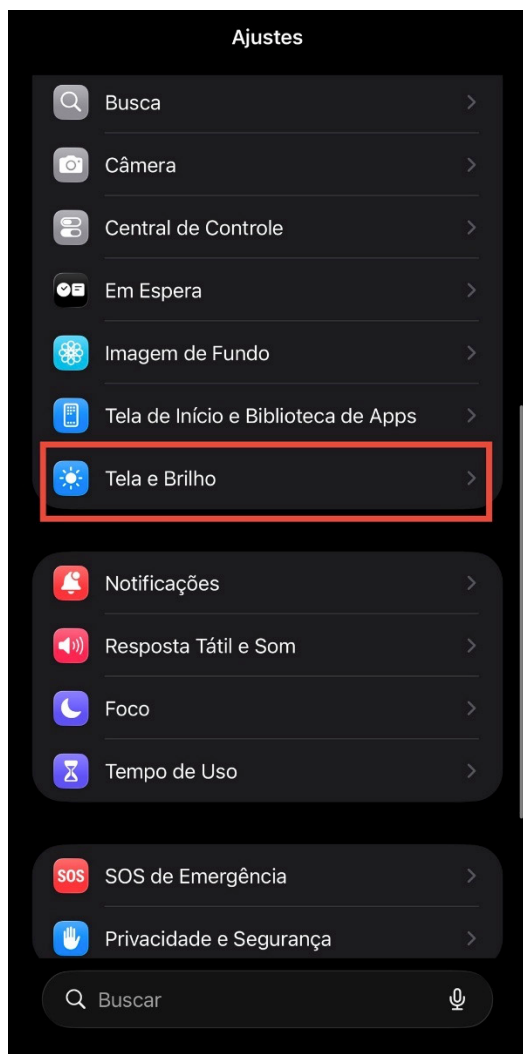
Bloqueio Automático de Tela

Depois de desbloqueado, o seu celular pode ficar acessível até ele ser propositalmente bloqueado de novo ou de forma automática, após o decurso de determinado tempo. A segunda opção é melhor.

Para ativá-la, toque em *Ajustes*:



Depois toque em *Tela e Brilho*:



Depois toque em *Bloqueio Automático*:



E selecione uma opção.

Recomendação:

30 segundos ou 1 minuto.

10 Limitação do AirDrop

A função AirDrop permite o compartilhamento de arquivos com dispositivos Apple próximos ao seu. Mas quando o recebimento de arquivos é permitido de qualquer remetente, o seu celular pode receber um arquivo indesejado e malicioso.

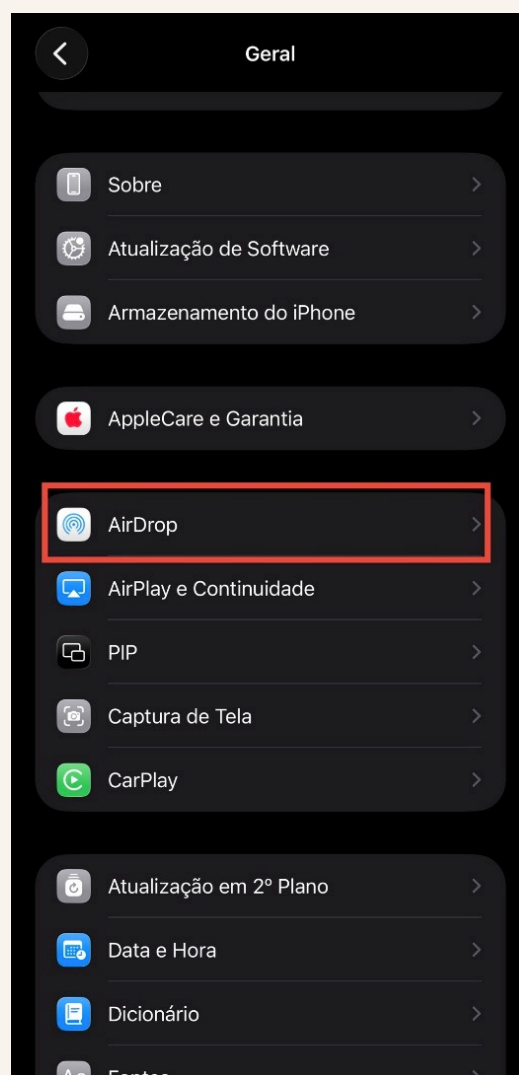
Para limitar quem pode enviar arquivos por AirDrop para você, toque em *Ajustes*:



Depois toque em *Geral*:



Depois toque em *AirDrop*:



E selecione entre as opções *Recepção Desativada* ou *Apenas Contatos*:

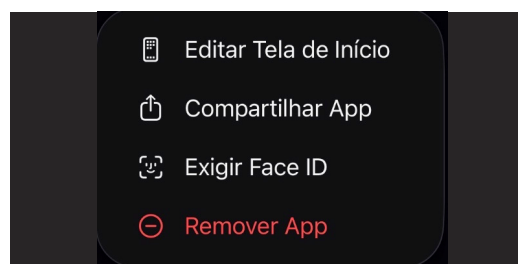


11 Restringir Acesso a Apps

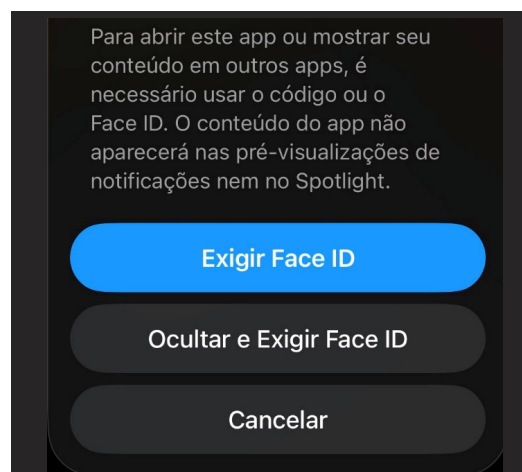
É possível configurar cada aplicativo que você usa para que ele somente possa ser aberto e utilizado depois da validação do Face ID ou digitação do código de desbloqueio.

Essa função garante maior segurança nos casos em que seu celular é furtado/roubado enquanto está desbloqueado, mas o criminoso não sabe seu código de desbloqueio.

Para ativar essa função (que precisa ser habilitada individualmente para cada aplicativo desejado), toque e segure no aplicativo por alguns segundos, até as opções abaixo surgirem:



Toque em *Exigir Face ID* e depois escolha entre *Exigir Face ID* ou *Ocultar e Exigir Face ID* (o que tira o app da sua tela inicial e coloca ele numa pasta escondida).



12

Bloqueio de Notas

O aplicativo Notas permite que notas selecionadas sejam bloqueadas com senha ou com o Face ID. O ideal é que você não inclua no aplicativo Notas informações como números de cartão de crédito ou senhas de acesso a contas bancárias ou outras aplicações. Mas caso faça isso, vale, pelo menos, bloquear essas notas.

Para ativar o bloqueio, toque em *Ajustes*:



Depois toque em *Apps*:



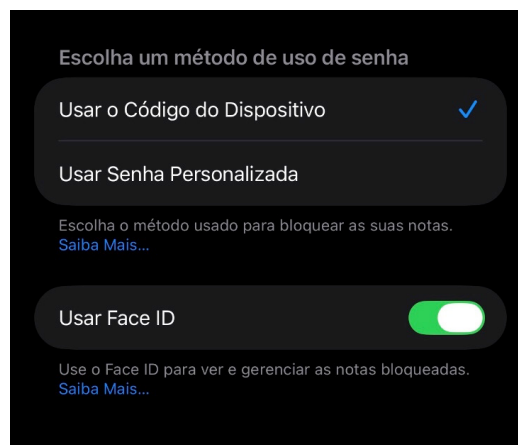
Depois toque em *Notas*:



Depois toque em *Senha*:



E escolha entre usar o código de desbloqueio do celular ou criar uma senha nova (só para o bloqueio de Notas), e permitir ou não o uso do Face ID para desbloqueio:



PROTEÇÕES PARA ANDROID



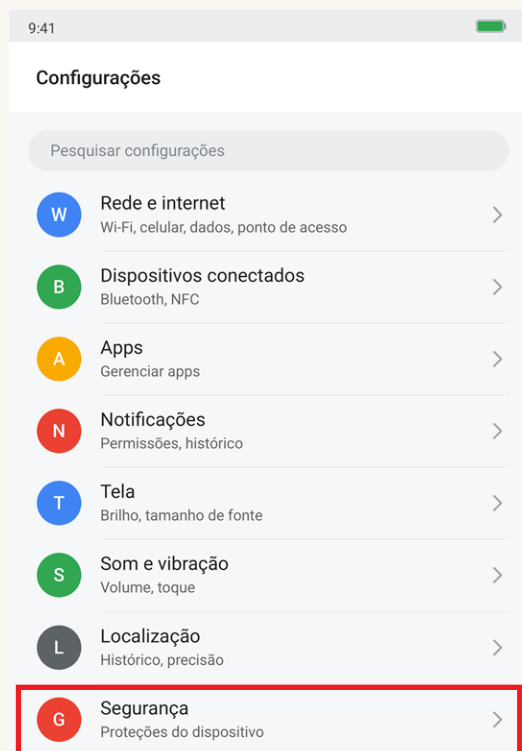
1

Proteção Contra Roubo

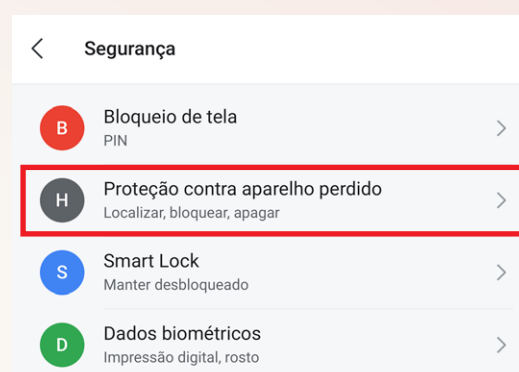
Toque em
Configurações:



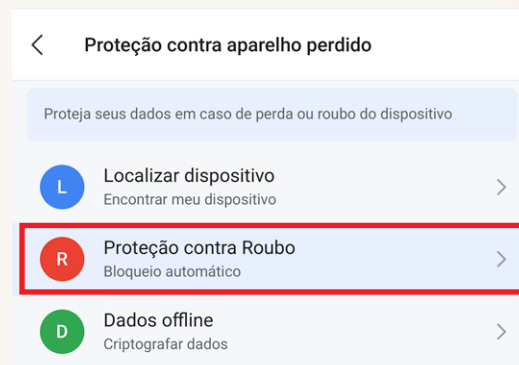
Toque em *Segurança*:



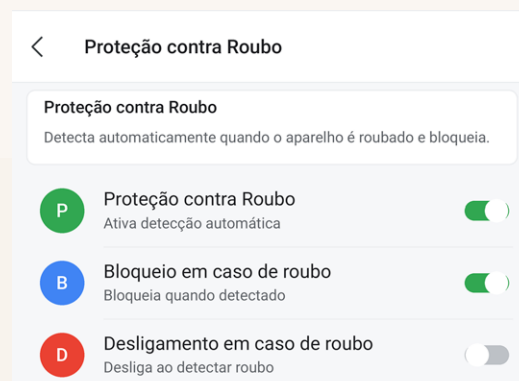
Toque em *Proteção contra Aparelho Perdido*:



Toque em *Roubo*:



Ative as proteções:



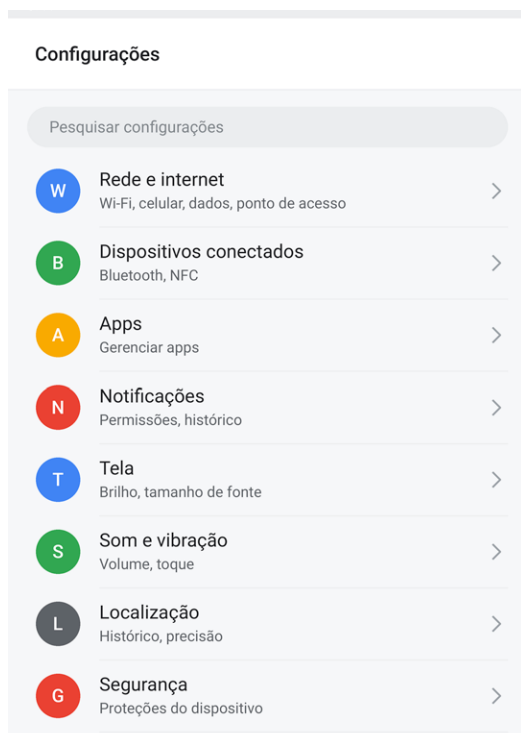
2

Find My Device

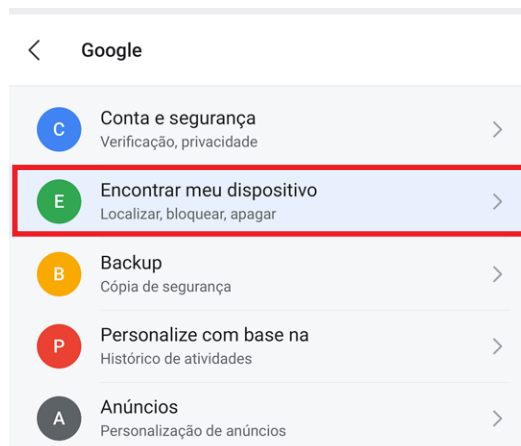
Toque em
Configurações:



Toque em *Google*:



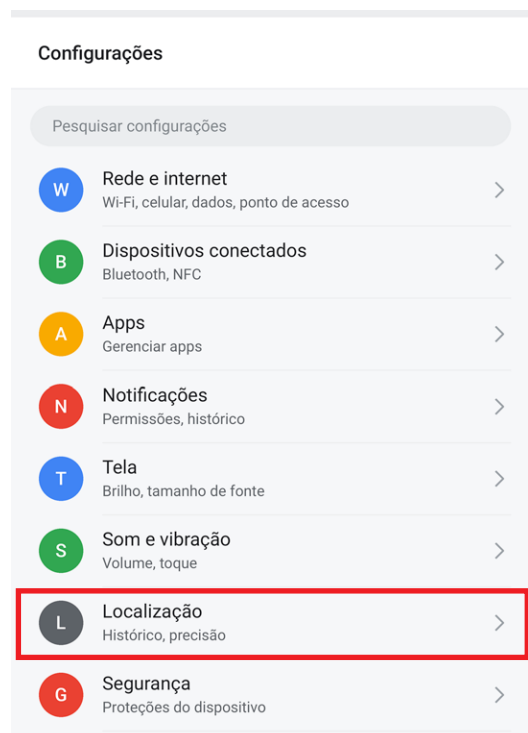
Toque em *Encontrar meu dispositivo*:



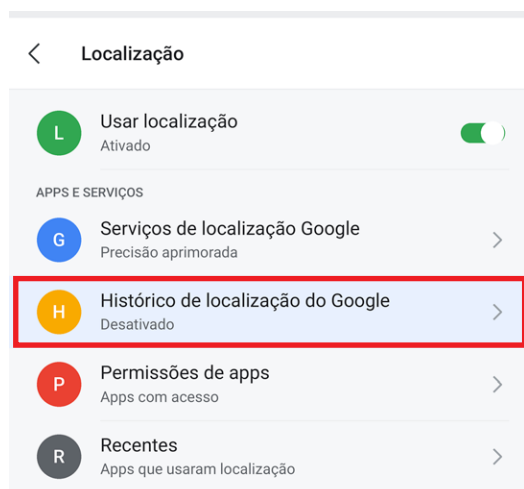
Ative *Encontrar meu dispositivo*:



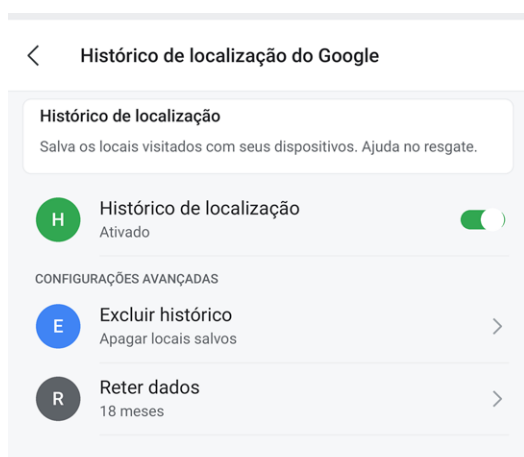
No menu *Configurações*, toque em
Localização:



Ative *Localização* e toque em *Histórico de localização do Google*.

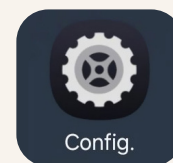


Ative *Histórico de localização*.

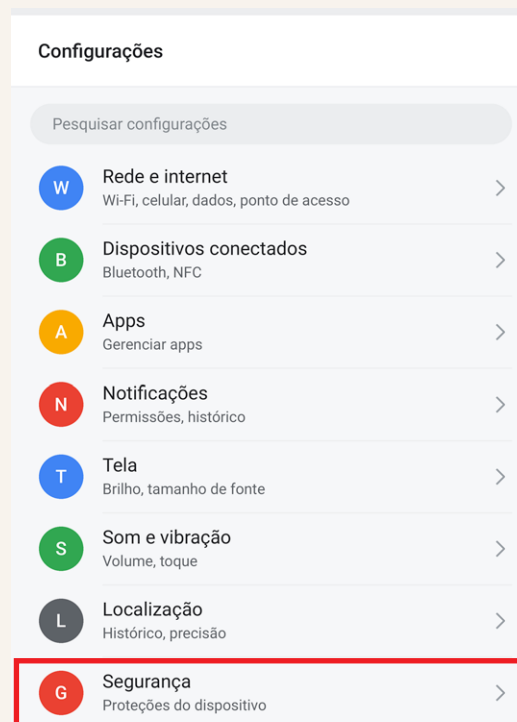


3 Bloqueio Seguro e Smart Lock

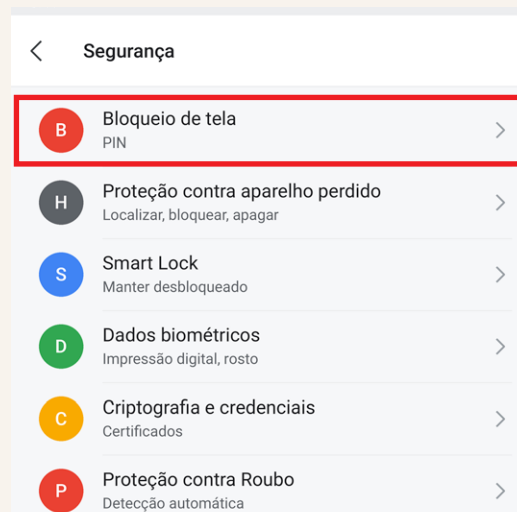
Toque em *Configurações*:



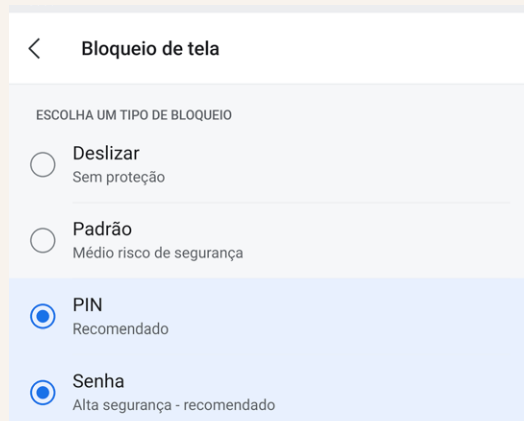
Toque em *Segurança*:



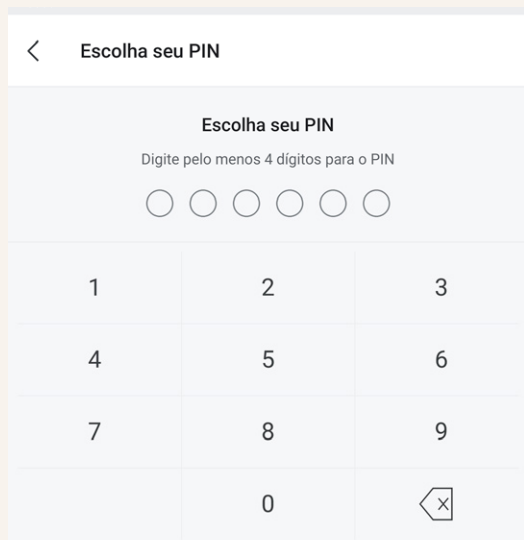
Toque em *Bloqueio de tela*:



Escolha entre *Padrão*, *PIN* ou *Senha*:



Configure sempre um *backup* (PIN ou Senha).

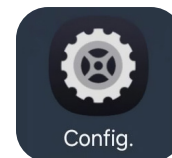


O Smart Lock pode ser uma vulnerabilidade. Desative completamente ou use apenas a opção *Deteção no corpo*. Evite as opções *Lugares confiáveis* e *Dispositivos confiáveis*.

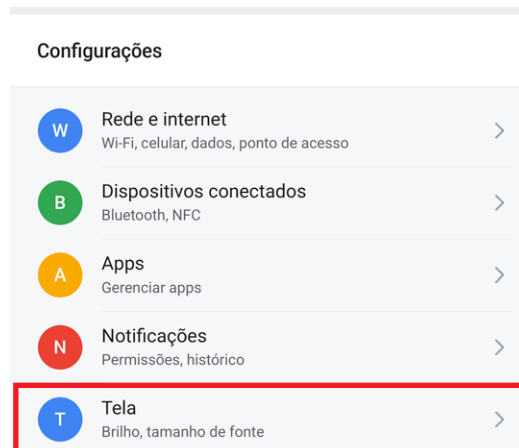


4 Bloqueio Automático de Tela

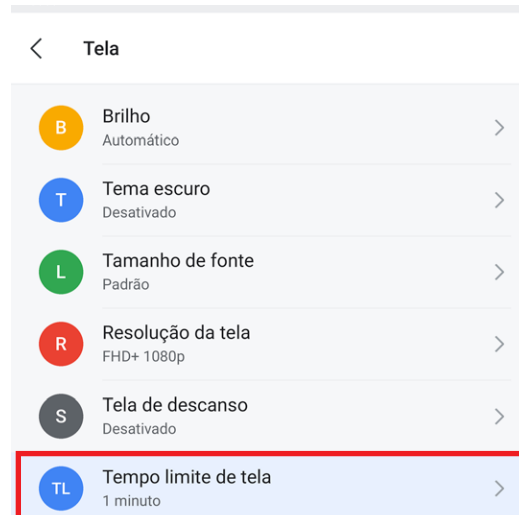
Toque em *Configurações*:



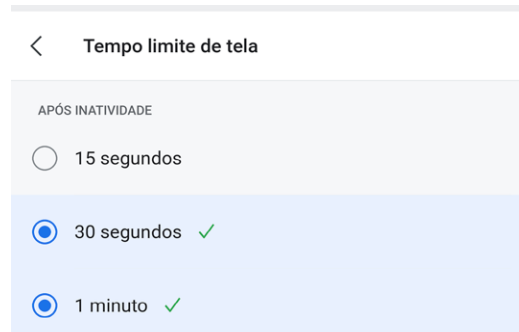
Toque em *Tela*:



Toque em *Tempo limite de tela*:



Escolha entre 30 segundos ou 1 minuto.

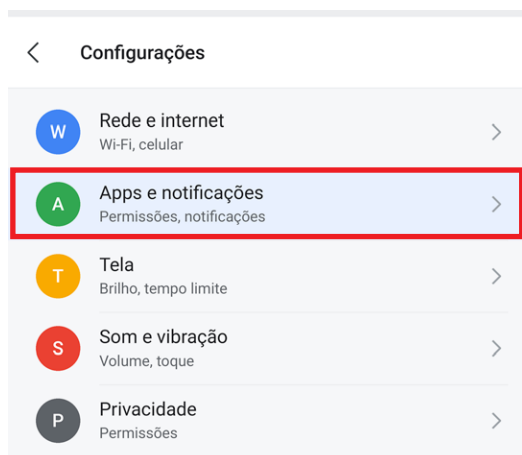


5 Ocultar Notificações

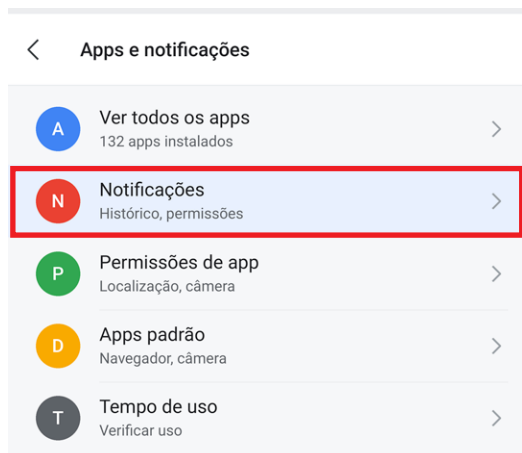
Toque em
Configurações:



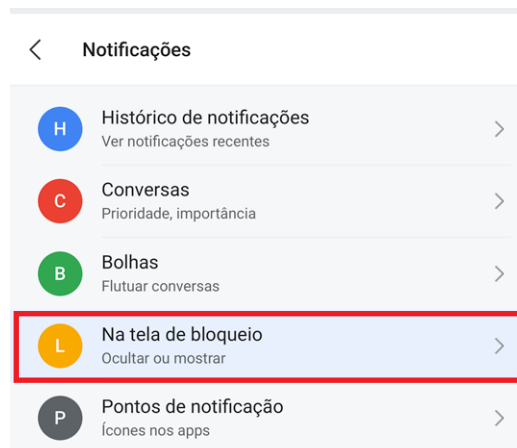
Toque em *Apps e notificações*:



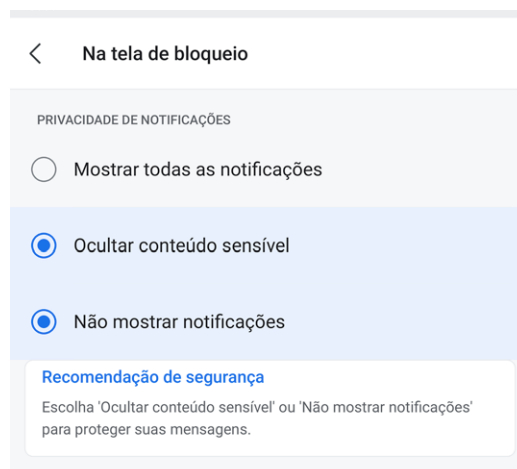
Toque em *Notificações*:



Toque em *Na tela de bloqueio*:



Escolha entre *Ocultar conteúdo sensível* ou *Não mostrar notificações*:



CONTATO



Felipe Palhares

Sócio, Proteção de Dados
e *Cybersecurity*

felipe.palhares@bmalaw.com.br



www.bmalaw.com.br

