+ Cross Security +


+ Cross Security +
+ Cross Security +

# Manual de Melhores Práticas de Segurança para Proteção de Dispositivos Móveis (Smartphones/Tablets/Notebooks)

**Grupo TecBan** | Superintendência de Segurança | Vanderlei Reis

Documento elaborado pelas **equipes de CyberSecurity** (**Blue** Team e **Red** Team)

**Classificação deste documento: PÚBLICO** **TLP: WHITE**

**Versão05_MB20211201**

# Prefácio

TecBan
cross-security@tecban.com.br

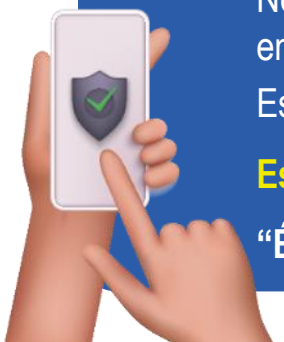
**Este é um trabalho colaborativo** e as informações disponibilizadas neste documento tem o objetivo de **mitigar riscos, prejuízos financeiros, danos de imagem e de segurança** (pessoal, profissional e corporativo), para você, seus familiares, amigos, contatos, empresas etc, **em caso de perda, furto ou roubo de dispositivos móveis** (smartphones, tablets, notebooks etc).

As dicas de segurança descritas neste documento te ajudará a **maximizar o nível de segurança** dos seus dispositivos móveis e também possibilitará **"ganhar tempo"** para executar o mais rápido possível (caso ocorra o sinistro) diversas **ações mitigatórias,** reduzindo/eliminando potenciais riscos, prejuízos e danos diversos.

A realidade Brasileira: **Ladrão tem mão leve e também pesada**, ora consegue furtar o dispositivo que está no seu bolso, na mochila ou na sua bolsa, surrupiam com a **"mão leve"**, ou através da força bruta, no famoso jargão **"tomar de assalto"**, vulgo **"mão pesada",** praticam o roubo na cara dura, na luz do dia, e da noite/madrugada também, na "correria" e distração no seu dia-a-dia enquanto você utiliza o dispositivo (celular, tablet etc...).

**A violência urbana é real e surreal no nosso país,** as estatísticas evidenciam esse grave problema, como por exemplo: são furtados e roubados milhares de celulares por mês no Brasil, números alarmantes e terríveis.


**Sensibilizados com o expressivo aumento desses casos**, especialmente quando tomamos conhecimento que familiares, amigos, colegas de trabalho e "conhecidos de alguns conhecidos" passaram por essas agressões/traumas, por vezes de ordem física, psicológica, com prejuízos financeiros e de imagem, **investimos algumas horas de trabalho e reunimos neste documento diversos conceitos, conhecimentos de segurança** e também discorremos sobre a importância de manter sistemas/aplicativos/ferramentas atualizados (***"up to date"***), ações consideradas **Fatores Críticos de Sucesso** (FCS).



Neste Manual de Melhores Práticas de Segurança para Proteção de Dispositivos Móveis, listamos uma série de **conceitos** que podem ser aplicados em qualquer aparelho (smartphones/tablets), desde que possuam os recursos embarcados nos dispositivos (slides a seguir).

Esse documento é **público** (TLP: WHITE) **e não tem restrição de compartilhamento**, então você pode dividir com seus familiares, amigos e colegas!

**Este manual será atualizado periodicamente e a sua publicação será feita através do perfil da TecBan no LinkedIn**

**"É melhor saber e não precisar, do que precisar e não saber..."** | Boa leitura e aquisição de conhecimento! **Vanderlei Reis**

# Índice

TecBan
cross-security@tecban.com.br

# Antes de tudo, você sabe o que fazer caso ocorra um sinistro? [1/2]

TecBan
cross-security@tecban.com.br

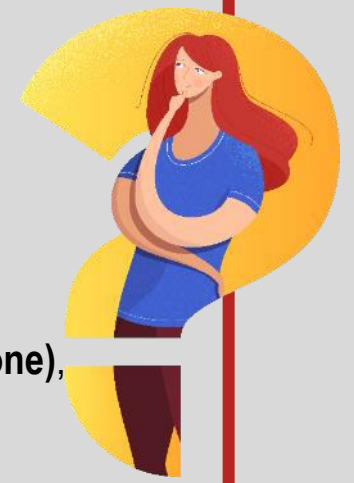
Preventivamente, é fundamental que você **tenha anotado e guardado** (local de fácil acesso) **na sua residência alguns dados/informações importantes**, como por exemplo: número do IMEI ("Identificação Internacional de Equipamento Móvel") dos dispositivos, telefones de contatos da sua empresa, dos seus bancos (incluindo dados da sua agência/conta/cartões/códigos de segurança), das operadoras de telefonia celular etc, pois facilitará a execução dos **principais procedimentos** (caso ocorra o sinistro)**, a seguir:**

**LEMBRE-SE:** Após eventual furto ou roubo do seu telefone, você terá no máximo de 20 a 30 minutos para executar os procedimentos abaixo e mitigar diversos riscos e prejuízos financeiros nas suas contas bancárias, e-mails e aplicativos. **Isso mesmo, de 20 a 30 minutos no MÁXIMO!**

1. **Imediatamente** (em até 5 ou 10 minutos, pós sinistro), **entre em contato** com os seus bancos/instituições financeiras, **informe o sinistro** e solicite os bloqueios temporários das contas bancárias, cartões de crédito/débito, revogação dos dispositivos/aplicativos que acessam suas contas bancárias e também solicite as revogações/substituições de todas as senhas e códigos/tokens. É muito importante que seja solicitado aos atendentes (do seu Banco) os **números dos protocolos** dos atendimentos, pois serão extremamente importantes **para o registro do** Boletim/Registro de Ocorrência **(BO/RO)**. Não espere chegar em casa para ligar para os seus bancos, **ligue da rua mesmo.**

2. Acesse suas contas (iCloud, Samsung Account, Google Account etc) e **execute o comando remoto de formatação do dispositivo** (wipe/apagar). Esta ação somente será possível se o dispositivo estiver com conectividade (online).
**Lembre-se:** ative/habilite preventivamente este recurso (localização/Buscar/Encontrar meu telefone) nas suas contas de e-mails e nos dispositivos móveis;

3. Entre em contato com a operadora da sua linha telefônica, **solicite o bloqueio temporário do chip/linha** e também o **bloqueio definitivo do IMEI** do dispositivo móvel (celular ou tablet). **O bloqueio do IMEI é importante para inutilização do dispositivo (telefone)**, evitando que seja reutilizado ou vendido pelos criminosos. **Não financie involuntariamente a criminalidade!**
O número do IMEI deve ser anotado e guardado em local de fácil acesso na sua residência. Este número pode ser **encontrado na etiqueta da caixa** do dispositivo **ou digitando *#06#** no celular/tablet (simulando uma ligação telefônica);



# Antes de tudo, você sabe o que fazer caso ocorra um sinistro? [2/2]

cross-security@tecban.com.br

4 Caso tenha ocorrido sinistro de algum dispositivo móvel corporativo, **entre em contato imediatamente com a equipe de Segurança do Grupo TecBan** (ou da sua empresa) comunique o sinistro, solicite o **bloqueio/revogação** (temporário) das credenciais sistêmicas (Usuário, Senhas, VPN, E-mail, Tokens/duplo fator de autenticação etc) **e também** do chip/linha telefônica corporativa. Ato contínuo, siga todos os passos do item de 1 ao 6. Mitigue riscos e ameaças contra a sua empresa;

5 **Substitua imediatamente as senhas das suas contas de e-mails, aplicativos/sistemas** (e-mails, Facebook, Instagram, iCloud, Google Account, Samsung Account, OneDrive, DropBox, WhatsApp, Telegram, Twitter etc);

6 Após realizar todas as ações supracitadas (itens de 1 a 5), é imprescindível que você **registre um Boletim/Registro de Ocorrência** (BO/RO) **junto a Delegacia de Polícia Civil do bairro** onde ocorreu o sinistro. Declare os fatos ocorridos para a autoridade policial, solicite que seja registrado no **BO/RO** o IMEI do dispositivo **e também os números de protocolos** de atendimentos dos bancos, instituições financeiras e operadoras de telefonia celular.

**ATENÇÃO: NUNCA ANOTE SENHAS NO TELEFONE** (e demais dispositivos), **por exemplo, em:**
BLOCO DE NOTAS, E-MAILs, SMS, WHATSAPP, TELEGRAM **etc**, já que normalmente os criminosos vasculham todas as informações que estão armazenadas no dispositivo, em busca de senhas e códigos para invadir suas contas bancárias e e-mails.

Reflita sobre essas importantes orientações, e perceba **o ENORME risco** caso esteja anotando (guardando), senhas e códigos de segurança nos seus telefones (e demais dispositivos móveis).

Em caso de dúvidas e/ou sugestões, envie e-mail para cross-security@tecban.com.br

# Principais benefícios dos dispositivos móveis

**Múltiplas possibilidades/facilidades** (transações bancárias, trabalho, entretenimento, estudos, conectividade etc)

TecBan
cross-security@tecban.com.br

## Realizar transações financeiras (aplicativos de bancos e fintechs)

(abertura e movimentação de contas, investimentos, consultas, empréstimos etc)

## Entretenimento, pesquisas, redes sociais, produtividade, conectividade etc

(Google, Facebook, Instagram, YouTube, Twitter, WhatsApp, Telegram, Skype, Webex, TikTok, Club House, LinkedIn, Waze, Google Maps, Banco24Horas, Uber, Netflix, Spotify, Google Authenticator, Teams, Twitch, calculadora, despertador, áudio e videoconferências, automatizações etc)

## Acesso corporativo (trabalho remoto, reuniões)

Acesso as diversas ferramentas corporativas (VPN, e-mail, áudio e videoconferência, documentos etc)

## Realizar compras online

(iFood, Uber Eats, Mercado Livre, Americanas, Magazine Luiza, OLX, Amazon, Steam etc)

## Acessar e-mails, sites de notícias etc

(Outlook, Gmail, Hotmail, Yahoo, UOL, G1, R7 etc)

## Armazenar, Compartilhar fotos, vídeos e documentos

(No próprio dispositivo móvel, Google Drive, iCloud, OneDrive, Dropbox, Evernote, CNH, e-CRLV etc)

Apesar de todas essas facilidades, infelizmente os riscos estão estabelecidos e estamos enfrentamos momentos difíceis no que tange a criminalidade que assola diversos estados da federação (UFs).
**Você sabia que são furtados/roubados milhares de celulares por dia no Brasil?**
As estatísticas são alarmantes e denunciam a **grave violência urbana** que vivemos no nosso país.

# Roubo de dispositivos desbloqueados

## Quadrilhas especializadas

TecBan
cross-security@tecban.com.br

# O principal problema é o furto ou **roubo de dispositivos móveis desbloqueados**

Normalmente os criminosos aproveitam a distração do usuário para subtrair o dispositivo **enquanto você utiliza** o Waze, ou falando ao celular, enviando mensagem, usando redes sociais, Spotify, Uber, fazendo compras etc).

Nestas situações o aparelho estando **desbloqueado**, e **ocorrendo o sinistro** os bandidos conseguem em poucos minutos (em média entre 20 e 30min após o sinistro) acessar **todas as funções do aparelho e também dos aplicativos, e podem realizar diversas transações bancárias.** Caso os dispositivos/aplicativos não possuam as configurações de segurança (descritas neste documento), **infelizmente seus problemas serão potencializados e o sucesso dos criminosos estará garantido...**

De posse do aparelho desbloqueado, o primeiro passo dos fraudadores é tentar **trocar todas as suas senhas de: e-mails, apps de bancos, redes sociais, iCloud, Google Drive, OneDrive e demais aplicativos...**

Nos slides a seguir, aprenda sobre o que você **NÃO DEVE FAZER** e também quais são as **Melhores Práticas de Segurança** para mitigar potenciais riscos.

# O Brasil está na posição “top 5” dos países mais atacados por hackers...

De modo geral, o sucesso dos criminosos está relacionado a falta de conhecimentos básicos de segurança da população/empresas

TecBan
cross-security@tecban.com.br

De posse do celular desbloqueado, os fraudadores forçam o envio de códigos de segurança (através da função *“esqueci minha senha”*) para resetar todas as suas senhas: e-mails, contas de bancos, redes sociais, iCloud e demais aplicativos... **Normalmente esses códigos de recuperação de senhas são entregues no próprio aparelho furtado/roubado, podendo ser por SMS, por e-mail ou através de aplicativos de geração de tokens (Microsoft Authenticator, Google Authenticator, Authy etc).**

A partir deste momento/estágio, os malfeitores possuem a disposição (literalmente “nas mãos”) **um potencial lucrativo “portfólio” de golpes para aplicar, sendo**:

- **Subtrair valores, “limpar” as contas bancárias** (saldo e limite), realizar empréstimos, **principalmente transferências via Pix**, DOCs, TEDs etc;
- **Enviar solicitações de transferências de dinheiro para contatos gravados na sua agenda** através de aplicativos de mensagem (WhatsApp, Telegram, Messenger etc);
- **Abrir contas bancárias, fazer** empréstimos utilizando os seus dados pessoais existentes no seu aparelho e/ou nos aplicativos e repositórios (OneDrive, Google Drive etc);
- **Extrair dados e informações pessoais/confidenciais** (fotos de cartões, contratos, documentos etc) para posterior extorsão, reset de senhas e outros **crimes de maior potencial ofensivo/gravidade...**

# “Quick wins”: procedimentos e vitórias rápidas

Top 10 ações com alto potencial de benefícios e controle de danos (financeiros e de imagem: pessoal, profissional e corporativo)

TecBan
cross-security@tecban.com.br

**Crie SENHAS FORTES (complexas)** para inicializar e/ou desbloquear os seus dispositivos (celular/tablet), senhas individuais para cada aparelho. **Esta senha é extremamente importante, pois é utilizada para configurar, incluir, excluir ou alterar diversos recursos de segurança dentro dos seus dispositivos**, por exemplo: adicionar ou excluir novas digitais biométricas, alterar as senhas das suas contas (iCloud, ID Apple) etc.

**Configure/habilite o reconhecimento biométrico** (TouchID ou FaceID) **apenas** para desbloquear os seus dispositivos e apps, mas **jamais de bancos! NUNCA habilite este recurso para acessar seus aplicativos bancários.** Acesse seus aplicativos bancários somente digitando os dados da conta/agência e senha pessoal. Crie senhas fortes (complexas) e DIFERENTES para acessar/desbloquear cada aplicativo/conta.

**Crie senhas fortes, diferentes e individuais** para desbloqueio de tela dos seus dispositivos e também para acessar contas, aplicativos etc. Configure a Autenticação em Duas Etapas **(2FA)** em todas as suas contas bancárias, e-mails, aplicativos etc. **NUNCA REUTILIZE e/ou guarde SENHAS** nos seus dispositivos (**Blocos de Notas...**), também não anote em papel/caderno! Utilize um gerenciador de senhas (Cofre de Senhas) criptografado com senha forte.

**Configure uma senha (PIN) no chip da sua linha telefônica (celular).** Guarde o PUK1/PUK2 para recuperação do chip em caso de bloqueio do PIN. Os códigos PIN, PUK1 e PUK2 estão localizados no cartão/embalagem do chip quando foi comprado. Nos próximos slides, ensinaremos “como configurar”.

**Não permita acesso local ou remoto aos seus dispositivos,** pois pessoas mal intencionadas e/ou fraudadores, podem instalar programas maliciosos sem que você perceba, e sem a sua permissão. **Se estiver desatento**, e permitir acesso ao seu dispositivo, **a sua segurança estará fragilizada**.

**Mantenha seus dispositivos atualizados (*“up to date”*)**
**Force manualmente as atualizações**, ao menos uma vez por semana, e verifique se existem novas versões disponíveis para seus dispositivos (iOS, AndroidOS e Windows), **aplicativos etc**.

**Não utilize e/ou exponha seus dispositivos em locais públicos, Táxi, Uber, Ônibus, Trem, Metrô, Eventos, Shows etc**
**Não vacile,** saiba que nesses locais você sempre será um alvo fácil e preferido dos criminosos**!**

**Ative o recurso “Buscar/encontrar meu telefone”** para localizar seu dispositivo **e/ou apagá-lo remotamente**. Aprenda nos próximos slides como realizar essa configuração.

**Crie um e-mail exclusivo para recuperação de senhas**. Utilize/Acesse esse e-mail (ex: Outlook) **somente através de outro dispositivo confiável/próprio. Não mantenha este e-mail configurado nos seus dispositivos**, já que os fraudadores utilizarão o recurso **“esqueci minha senha”** para receber um código de recuperação, e se esse e-mail estiver configurado no dispositivo sinistrado, o sucesso do criminoso estará garantido! **Percebe o enorme risco?**

**Se ligarem no telefone da sua casa ou no seu celular se passando por algum funcionário dos seus bancos/instituições**, **desconfie**, anote o número de origem, solicite o nome da pessoa e desligue em seguida. **Ato contínuo**, ligue para a central de atendimento do seu banco, relate o caso e questione se foram eles que fizeram a ligação. Nunca informe seus dados pessoais, cartões, senhas ou códigos para ninguém, incluindo seus familiares.

# Aprenda sobre o que você NÃO DEVE FAZER

TecBan

**“Uma ‘única’ vulnerabilidade**, descuido ou falta de conhecimento, **é tudo o que os criminosos precisam”**

Window Snyder

# 20 ações que você NÃO deve fazer! 1/2

TecBan
cross-security@tecban.com.br

## 1 Não anote ou guarde senhas nos TELEFONES (e dispositivos móveis) ou envie/armazene senhas por SMS, e-mail ou aplicativos mensagens.

**Jamais, em hipótese alguma ANOTE (atrás do celular) ou GUARDE senhas nos seus dispositivos móveis** (ex.: bloco de notas) **ou envie por mensagens** (SMS, WhatsApp, e-mail etc). Essa prática garantirá o sucesso dos criminosos, já que estando de posse do seu aparelho conseguirão acessar essas senhas e invadir as suas contas, inclusive bancárias. **Percebe a enorme fragilidade?**

## 2 Não utilize seus dispositivos em vias ou locais públicos, em Eventos/Shows ou em ambientes com aglomerações. Celulares em bolsas e mochilas serão furtados!

Evite andar na rua falando ao celular, respondendo mensagem ou ouvindo música. Evite também utilizar o celular desbloqueado no painel do carro (Waze), no Uber, taxi, ônibus, metrô, trem **em eventos**. Normalmente os criminosos aproveitam a distração do usuário para subtrair os dispositivos.

## 3 Não configure/mantenha seu e-mail de recuperação de senhas (reset) no mesmo aparelho que você utiliza no seu dia-a-dia

Em caso de perda, furto ou roubo do celular/tablet, os criminosos estarão com o seu dispositivo em mãos e terão acesso aos códigos para realizar as substituições das senhas das suas contas, credenciais, bancos, aplicativos etc. **Não configure este tipo e-mail no seu dispositivo móvel!**

## 4 Não compartilhe com ninguém seus códigos de segurança ou de recuperação de senhas, contas bancárias, aplicativos, e-mails etc

Os códigos de segurança enviados por SMS, e-mail ou tokens são utilizados para confirmação de identidade ou recuperação de senhas. Nunca compartilhe ou informe esses códigos para outras pessoas. Sempre desconfie se alguém solicitar qualquer tipo de código. **Fique atento e seja resiliente!**

## 5 Não armazene senhas, fotos e vídeos de cartões bancários, documentos pessoais e/ou sigilosos nos dispositivos/E-mails/Aplicativos...

Os criminosos procuram informações sensíveis armazenadas nos dispositivos para trocar as senhas junto aos bancos, **abrir contas**, solicitar empréstimos etc. **"O céu é o limite para os fraudadores"...**



## 6 Não habilite ou utilize o recurso de salvamento automático de senhas ("lembrar/salvar/preencher senha")

**DESATIVE o recurso "lembrar/salvar/preencher" senhas nos seus dispositivos**, aplicativos ou navegadores. As senhas ficam salvas no histórico e podem ser acessadas facilmente pelos criminosos (localmente ou remotamente). Não aceite esse risco, assim não fará parte das estatísticas (vítimas)!

## 7 Não registre os nomes completos e não descreva o grau de parentesco ou cargos dos seus contatos na agenda telefônica

Na sua agenda de contatos, não registre os nomes completos e não utilize descrições como pai, mãe, filho, esposa/esposo, cargos, nome de empresa etc. pois em caso de acesso indevido aos seus dispositivos, **estes contatos serão alvos fáceis, preferidos e próximas vítimas dos criminosos.**

## 8 Não aceite pedidos/mensagens solicitando transferências de dinheiro

Faça uma via videochamada com o seu contato (através do telefone oficial) e confirme o pedido indesejado. Na dúvida, evite transferir qualquer valor (R$) para contas bancárias de desconhecidos. Caso identifique que é um golpe, avise os seus contatos e denuncie para o aplicativo (Whatsapp, Telegram etc)

## 9 Não conecte ou recarregue seus dispositivos em tomadas ou portas USBs públicas (aeroportos, rodoviárias, shoppings etc) ou de desconhecidos...

Não conecte ou recarregue seus dispositivos em tomadas e portas USBs públicas (aeroportos, rodoviárias, cybercafé, shoppings etc) ou de desconhecidos. Não há como saber quem está no controle dessas conexões. Essas entradas/portas podem estar comprometidas. **Você poderá ser hackeado!.**

## 10 Não instale aplicativos fora das lojas oficiais (Apple Store, Play Store etc)

Aplicativos baixados (downloads) fora das lojas oficiais podem possuir códigos maliciosos com o objetivo de copiar/vazar dados e informações dos seus dispositivos. A decisão sempre será sua, arriscar e o seu dispositivo ser infectado... **E aí, vai correr o risco? Melhor não, né?**

# 20 ações que você NÃO deve fazer! 2/2

TecBan
cross-security@tecban.com.br

## 11 Phishing: Não clique em links (URLs), enviados por e-mails, SMS ou baixe/abra arquivos de desconhecidos e/ou suspeitos. Não clique em links "encurtados"...

Saiba que mensagens de fontes desconhecidas (via e-mail, SMS, WhatsApp, Telegram etc) que contenham links (URLs) ou arquivos devem ser considerados maliciosos e consequentemente devem ser deletados sem abrir/extrair. Faça o bloqueio imediato dos números de telefones e e-mails suspeitos.

## 12 Não utilize dispositivos de locais públicos/compartilhados (aeroportos, rodoviárias, shoppings, lojas etc) ou de pessoas desconhecidas

Não utilize dispositivos públicos (celulares, tablets e computadores) ou de pessoas desconhecidas. Seu histórico de navegação e credenciais de acessos podem ficar salvos nestes dispositivos e serão utilizadas pelos fraudadores. **Já ouviu falar de "Key Logger"? Dá um Google e conheça os riscos...**

## 13 Não publique seus dados e/ou informações pessoais em fóruns ou redes sociais

**Não publique nenhuma foto de:** documentos, dados e informações pessoais como endereços, número do celular, data de nascimento, CPF, cartões de créditos, bilhetes de viagem, passaporte, localização (check-in) etc. **Caso faça, saiba que você e seus familiares são potenciais alvos dos criminosos!**

## 14 Não mantenha os recursos de Wi-fi, Bluetooth, NFC ativos enquanto não os utiliza

Evite deixar estes recursos ativos/habilitados enquanto não utiliza, pois os criminosos podem aproveitar o sinal de propagação do seu dispositivo para realizar ataques, explorar vulnerabilidades ou realizar transações por aproximação (NFC). **Se ignorar, você poderá ser a próxima vítima!**

## 15 Não compre celulares, tablets e computadores de desconhecidos (esses dispositivos podem ser de origem de perda, furto ou roubo)

Existem vários relatos no mercado que equipamentos de origens duvidosas podem possuir programas/códigos maliciosos para monitorar, copiar e vazar seus dados/informações pessoais.

## 16 NUNCA, JAMAIS utilize sinal de Wi-fi ou rede de dados de locais públicos ou de desconhecidos. Já ouviu falar em redes Wi-Fi falsas? Pois é...

Redes públicas/desconhecidas podem ser utilizadas pelos hackers para enviar códigos maliciosos e invadir dispositivos (celular, tablet ou notebook). Redes gratuitas são passíveis de interceptações de dados e escutas telefônicas sem o seu conhecimento/autorização. **"Não existe almoço de graça!"**

## 17 Não cadastre seu e-mail corporativo em sites de propaganda ou para qualquer finalidade de uso particular. Seja responsável, proteja a sua empresa!

Criminosos podem utilizar o seu e-mail corporativo para enviar mensagens de phishing, malwares, ramsonware e/ou enganar pessoas da sua empresa para obter acesso não autorizado aos sistemas e redes da empresa que você trabalha. Proteja suas credenciais corporativas (usuário, senha, token etc).

## 18 Não permita acesso local ou remoto aos seus dispositivos

Não permita acesso local ou remoto aos seus dispositivos, seja de uso particular ou corporativo, se permitir será possível instalar programas maliciosos sem você perceber, além de fragilizar a sua segurança pessoal, os negócios da sua empresa também estarão em total risco! **Faça a sua parte, proteja-nos!**

## 19 Não utilize porta cartões/documentos ou escreva senhas/códigos nas capas dos dispositivos (celular, tablets e notebooks). Proteja as suas senhas!

Se cometer essa falha, **saiba que você ajudará os criminosos a terem acessos privilegiados** ao seu dispositivo, as suas contas bancárias, aplicativos, e-mails etc? **Lembre-se:** Anotar dados, senhas, códigos etc nos próprios dispositivos **É UM ERRO FATAL para a sua segurança! NÃO FAÇA ISSO!**

## 20 Não aceite e não utilize pendrive/cartão de memória (ou dispositivos removíveis) de outras pessoas e desconhecidos.

Dispositivos removíveis podem possuir vírus ou programas maliciosos para invadir seus aparelhos (celular, tablets, notebook etc) e interceptar/copiar/vazar dados/informações (senhas, documentos e informações sigilosas). Lembra da técnica "Key Logger"? Dá um Google aí...

# Melhores práticas de segurança

TecBan

"Muitas vezes, as áreas de Segurança são vistas como excessivas, até o dia que não são suficientes" (materialização de ataques/prejuízos...) William H. Webster

# Melhores práticas de segurança 1/3

TecBan
cross-security@tecban.com.br

## 1 Crie SENHAS FORTES (complexas) para inicializar e/ou desbloquear os seus dispositivos (celular/tablet).

**Esta senha é extremamente importante, pois é utilizada para configurar (incluir/alterar) diversos recursos de segurança dentro dos seus dispositivos**, Senhas fracas facilitam a vida dos fraudadores, pois conseguirão adicionar novas digitais, alterar as senhas das suas contas (iCloud, IDApple) etc.

## 2 Configure/habilite o reconhecimento biométrico (TouchID ou FaceID) apenas para desbloquear seus dispositivos e alguns aplicativos (jamais apps bancários!)

**NUNCA habilite este recurso para acessar seus aplicativos bancários.** Acesse seus aplicativos bancários somente digitando os dados da conta/agência e senha pessoal. Crie senhas fortes (complexas) e DIFERENTES para acessar/desbloquear os aplicativos etc...

## 3 Crie senhas fortes e diferentes para desbloqueio de tela dos seus dispositivos e também para acessar contas, aplicativos etc. Nunca reutilize senhas antigas!

**Defina senhas diferentes e fortes para cada acesso/sistema**, caso alguma senha tenha sido comprometida (vazada/descoberta) o risco ficará isolado apenas a conta relacionada a senha exposta. **NUNCA REUTILIZE** e/ou guarde SENHAS (em texto claro) nos seus dispositivos, também não anote em papel/caderno! **Utilize aplicativo gerenciamento de credenciais e senhas (Cofre de Senhas).**

## 4 Mantenha seus dispositivos e aplicativos sempre atualizados (*"up to date"*). Reinicie seus dispositivos frequentemente para aplicar/finalizar as atualizações

Os fabricantes de dispositivos e aplicativos, recorrentemente disponibilizam novas funcionalidades e corrigem vulnerabilidades de segurança. Verifique e force manualmente a atualização dos seus dispositivos e aplicativos. Atualizações críticas de segurança somente são aplicadas (instaladas) após a reinicialização do sistema/dispositivos. Execute este procedimento pelo menos uma vez por semana.

## 5 Configure uma senha (PIN) no chip da sua linha telefônica (celular)

Essa ação impedirá que o chip seja instalado em outro celular e receba SMS ou ligações. Guarde em um local seguro os códigos PUK1 e PUK2 para recuperação do chip em caso de bloqueio definitivo do PIN.

## 6 Configure no seu smartphone (ou tablet) o recurso "Tempo de Uso" para abrir/bloquear os aplicativos. Essa é mais uma importante camada de proteção!

Configure no seu smartphone o recurso "Tempo de Uso" e crie uma senha (diferente das demais) para acessar os aplicativos instalados no seu celular. Caso o criminoso esteja com o seu dispositivo desbloqueado, ele não conseguirá abrir os aplicativos bloqueados, pois estarão protegidos com senha!

## 7 Crie um e-mail alternativo para recuperação de senhas e NUNCA mantenha configurado nos seus dispositivos (smartphone, tablets, notebook)

Utilize um e-mail diferente do que está configurado no seu aparelho para recuperação de senhas. **Quando necessário acesse esse e-mail somente através de outro computador seguro/confiável, após coletar as informações encerre a sessão (sair/desconectar).**

## 8 Clique apenas em links de origem confiável. Ao receber, desconfie e principalmente não clique em links encurtados (Goo.gl/xxx. Bit.ly/xxx, Ow.ly/xxx etc)

Clique apenas em links de origem confiável. **Esteja atento aos remetentes de e-mails e SMS. Faça leitura minuciosa da mensagem.** Desconfie quando a mensagem indicar urgência de alguma ação ou medida de sua parte. **Não clique em links encurtados** (Goo.gl/xxx, Bit.ly/xxx, Ow.ly/xxx etc). Sempre desconfie de facilidades e assim não cairá em golpes digitais/eletrônicos.

## 9 Acesse as suas contas bancárias e REDUZA os limites (R$) de cartões de crédito/débito, pagamentos, transferências (TED/DOC), empréstimos e PIX

Normalmente os limites (R$) de suas transações estão definidos com valores altos, reduza esses limites de acordo com os valores que você realmente utiliza no seu "dia-a-dia".

## 10 Diminua o tempo de bloqueio automático da tela do seu dispositivo

Configure a tela de bloqueio automático para o menor tempo disponível (máximo 15 ou 30 **segundos**) quando estiver ocioso. Se existir a opção de "bloqueio imediato", **configure imediatamente.**

# Melhores práticas de segurança 2/3

TecBan
cross-security@tecban.com.br

## 11 Fique atento ao digitar suas credenciais e senhas, proteja a sua digitação (no teclado) e evite que alguém tente visualizar os códigos. Golpe clássico!

Fique atento com pessoas olhando a digitação da sua senha nos dispositivos, celular, tablet, notebook, ATMs (caixas eletrônicos). **Dica imbatível para evitar visualização indevida da sua senha: Ao digitar a sua senha UTILIZE uma das suas mãos para cobrir (parcial) o teclado durante a digitação.**

## 12 Revise as permissões de acesso dos aplicativos. Aqui mora um grande perigo!

Muitos aplicativos solicitam permissões para acessar seus contatos, e-mails, fotos e outras informações pessoais os quais não são imprescindíveis para o funcionamento do serviço. Cuidado com essas permissões... Revise e não permita a fuga/perda de seus dados e informações.

## 13 Desative nos seus dispositivos todas as funcionalidades/notificações que são apresentadas com a tela bloqueada

Por padrão, os smartphones permitem pré-visualizar notificações, utilizar a assistente de comando (Ex.: Siri) para acessar a galeria de fotos e configurações do aparelho **mesmo com a tela bloqueada**. Desative essa funcionalidade, já que facilitará muito a vida dos bandidos. **Aqui não!!!**

## 14 Desconfie de ligações e/ou solicitações de seus dados pessoais, códigos, senhas etc. Não caia em golpes amplamente conhecidos como "Engenharia Social"

Desconfie de ligações e/ou solicitações dos seus dados pessoais, códigos de acessos/senhas e/ou qualquer outra informação pessoal. **Lembre-se: na maioria dos casos, os criminosos atingem o sucesso, pois você colaborou ao passar voluntariamente os seus dados/informações. Reflita!**

## 15 Utilize um aplicativo gerenciador de senhas (Cofres de Senhas) para organizar e proteger suas credencias e senhas (ex: Dashlane, LastPass, 1Password, Keeper etc)

Utilize algum aplicativo com a função de Cofres de Senhas para gerenciar suas credenciais de acesso (usuários e senhas). Mantenha esse aplicativo criptografado com senha forte e restrita a você!.

## 16 Ative o recurso duplo fator de autenticação para acessar suas contas bancárias, e-mails, aplicativos etc

Configure/habilite a autenticação em duas etapas (2FA - duplo fator de autenticação) em todas as suas contas bancárias, e-mails, aplicativos, iCloud, ID Apple, Google Account etc.

## 17 Ative as notificações de acesso ao seu e-mail através de outros computadores. Habilite esse recurso nas suas contas bancárias/transações realizadas.

Ative as notificações para saber se acessaram seu e-mail através de outro dispositivo. Ative também as notificações nos aplicativos bancários para avisar quando alguma transação for realizada. Facilitará a identificação de possíveis transações indevidas. **Em caso de suspeitas, TROQUE SUAS SENHAS!**

## 18 Ative o recurso "Buscar/encontrar meu telefone"

**Ative o recurso "Buscar/encontrar meu telefone"** para localizar seu dispositivo e/ou apagá-lo remotamente. Em 99,99% dos casos de sinistros, os usuários não recuperam os seus dispositivos, após serem furtados/roubados, **então formate-o (apague) remotamente.** Ficará bloqueado para sempre!

## 19 Caso tenha algum dispositivo móvel sinistrado, altere as senhas de todas as suas contas bancárias, e-mails, rede sociais e de aplicativos/sites diversos

Substitua imediatamente todas as suas senhas e revogue (desconectar/sair) todas as sessões abertas nos diversos dispositivos que você utiliza. **"Não pague para ver e perder"..**

## 20 Efetue o "log out" ("sair ou encerrar sessão") de sites/apps após a realização de pagamentos, compras e transações bancárias

Efetue o "log out" (encerre a sessão) após realizar pagamentos, compras ou utilizar aplicativos bancários, pois em alguns casos a sessão fica aberta no navegador/aplicativo e poderá ser reutilizada indevidamente. **Os malfeitores adoram quando o usuário esquece de fazer isso....**

# Melhores práticas de segurança 3/3

TecBan
cross-security@tecban.com.br

## 21 Faça backup (local e na nuvem) semanalmente dos seus dispositivos/aplicativos

Faça backup semanal dos seus dispositivos, pois em caso de perda, furto ou roubo do aparelho você não perderá suas informações na totalidade. Existem serviços “em nuvem” que possibilitam realizar backups automaticamente. Recomendamos que mantenha um backup “offline” criptografado no seu computador.

## 22 Desabilite o cartão físico (crédito e débito) para compras online e habilite somente os virtuais

A grande vantagem dos cartões virtuais é que você tem uma janela de tempo para utilizá-lo, o que aumenta sua segurança contra golpes em ambientes online, e também não é possível reutilizar o cartão após o seu uso. **A maioria dos bancos disponibilizam esse recurso de segurança.**

## 23 Instale um bom antivírus para proteger seus dispositivos móveis (celular, tablet ou notebook)

Instale um antivírus de qualidade em seu aparelho (somente baixe aplicativos através das lojas oficiais da Apple e Google). O antivírus evitará que vírus, malwares e outras ameaças cibernéticas danifiquem seu dispositivo ou roubem informações confidenciais. Além disso, ele fornecerá proteção durante a navegação na internet.

## 24 CAIXA POSTAL ou Caixa de Mensagens de voz: Crie uma senha (diferente das demais que você utiliza) de 4 dígitos para acesso a sua caixa postal da sua linha...

**A maioria dos aplicativos/ferramentas oferecem a opção de envio de códigos de segurança** (cadastro ou recuperação de senhas) **através de ligação telefônica (mensagem de voz).** Aqui mora o perigo! **Existem técnicas criminosas para forçar o envio de códigos através de ligações e podem ser direcionadas para a caixa postal da sua linha telefônica** (celular, por exemplo). A maioria das caixas postais não possuem senha ou permitem acessá-las pelo código padrão “1234 ou 0000”. **Nessas condições os criminosos estão com enormes vantagens e a sua caixa postal será invadida**, acessada indevidamente! **Vamos lá, crie uma senha e não compartilhe com ninguém, ninguém mesmo!** Lembre-se, todo e qualquer código secreto, senhas, são de uso pessoal e intransferível.

## 25 Proteja (cubra) fisicamente a sua câmera/webcam. Segurança física é imbatível!

Cibercriminosos podem acessar uma webcam através de conexões remotas e não autorizadas. Muitos malwares permitem que bandidos ativem a câmera remotamente, comprometendo sua segurança e privacidade. **Reflita agora:** se alguém acessar a sua câmera neste momento? ☹

## 26 Anote e guarde alguns dados/informações importantes para facilitar as principais ações mitigatórias (pós sinistro) para bloqueio do dispositivo/celular

Guarde em local de fácil acesso (residência) alguns dados/informações como: IMEIs, dados de cartões, telefones de contatos (empresa, bancos, operadoras de telefonia etc) para conseguir realizar os devidos bloqueios em caso de sinistro.

## 27 Golpe de boletos bancários falsos. Fique atento ao receber boletos através de e-mails não oficiais, sempre confira o endereço eletrônico de origem

Positive se você adquiriu algum produto ou serviço daquele remetente. Em caso de dúvidas entre em contato com o remetente/prestador de serviços, através de um telefone oficial, e confirme os dados do boleto/QRCode. Sempre confira o valor, conta de destino, nome do beneficiário, CPF/CNPJ etc.

## 28 Desative das suas contas (e-mails, aplicativos etc) o envio de códigos de segurança e recuperação de senhas por SMS

Evite utilizar o recurso de envio de SMS para receber códigos de segurança e recuperação de senhas, pois este **método é considerado um dos mais vulneráveis** do mercado. É importante optar por autenticações através de aplicativos com função de token (Microsoft Authenticator, Authy etc), ou ao menos por e-mail...

## 29 Cadastre o telefone de alguma pessoa de confiança ou de um celular backup (próprio) para verificar sua identidade ao iniciar a sessão da conta do iCloud

Este procedimento é importante para evitar que os criminosos, de posse do seu dispositivo, acessem a sua conta do iCloud e explorem seus dados/informações disponíveis tanto no seu telefone quanto na nuvem. Aprenda como configurar (próximos slides).


TecBan
cross-security@tecban.com.br

Dispositivos Apple

Antes de qualquer ação, ATUALIZE a versão do seu iOS para **15.1** ou superior

"Uma 'única' vulnerabilidade ou descuido, é tudo o que os criminosos precisam"
Window Snyder

# Configurações de **Segurança**

## Mitigação de riscos em caso de **perda, furto ou roubo** do dispositivo

# Crie uma senha forte para inicializar/desbloquear seus dispositivos

Lembre-se: “Uma corrente é tão forte quanto o seu elo mais fraco”. Não seja o elo mais fraco!...

William James

TecBan
cross-security@tecban.com.br


**Crie uma SENHA FORTE (complexa)** para inicializar e/ou desbloquear os seus dispositivos (celular/tablet). **Esta senha é extremamente importante, já que é utilizada para configurar (incluir/alterar) diversos recursos de segurança dentro dos seus dispositivos**, por exemplo: adicionar novas digitais (biometria), alterar as senhas das suas contas (iCloud/ID Apple) etc.

Por padrão, o código para desbloquear dispositivos Apple é constituído por 6 números, o que torna a senha vulnerável a ponto de ser “facilmente” observada/copiada durante a sua digitação. **Crie uma senha forte (alfanumérica), composta por letras, números e caracteres especiais!**

## Veja o passo a passo para configurar a senha alfanumérica


**Dica para evitar visualização de senha durante a digitação:** Seja no caixa eletrônico (ATM) **ou** no seu celular, **UTILIZE uma das suas mãos (parcial ou total) para encobrir o teclado enquanto você digita a sua senha.** Conceito proteção escudo!

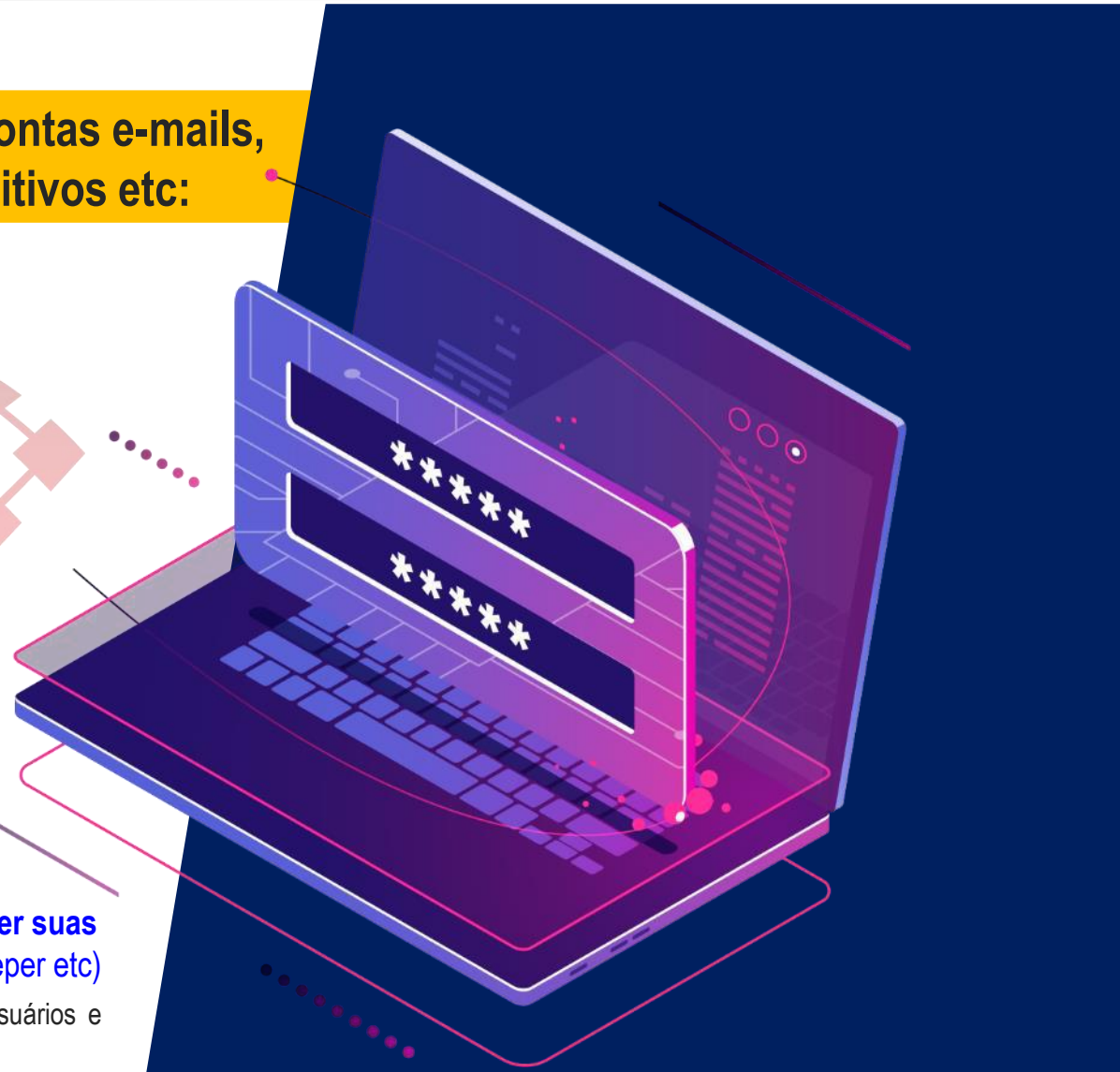
1. Vá em *“Ajustes”*
2. Vá em *“Touch ID e Código”* ou *“Face ID e Código”*
3. Digite seu código atual
4. Vá em *“Alterar Código”*
5. Digite seu código atual (anterior)
6. Selecione *“Opções de Código”*
7. Selecione *“Código Alfanumérico Personalizado”*
8. Digite seu novo código composto por letras, números e caracteres especiais

# Regras de como criar senhas fortes

## Proteja seus dispositivos, aplicativos e sistemas

TecBan
cross-security@tecban.com.br

**Dicas de como elaborar senhas fortes para as suas contas e-mails, serviços bancários, de redes sociais e demais dispositivos etc:**



1. Não insira partes do seu nome, sobrenome, data de nascimento, e-mail etc
2. Não repita às senhas utilizadas anteriormente ou em outros aplicativos/dispositivos.
3. Crie senhas com no mínimo 12 caracteres (o ideal são 15)
4. Utilize todas as seguintes características nas suas senhas
   - Letras maiúsculas
   - Letras minúsculas
   - Números
   - Caracteres especiais ( exemplos: ! Ç @ # $ % & *| )
5. Substitua com frequência suas senhas (no máximo a cada 90 dias)

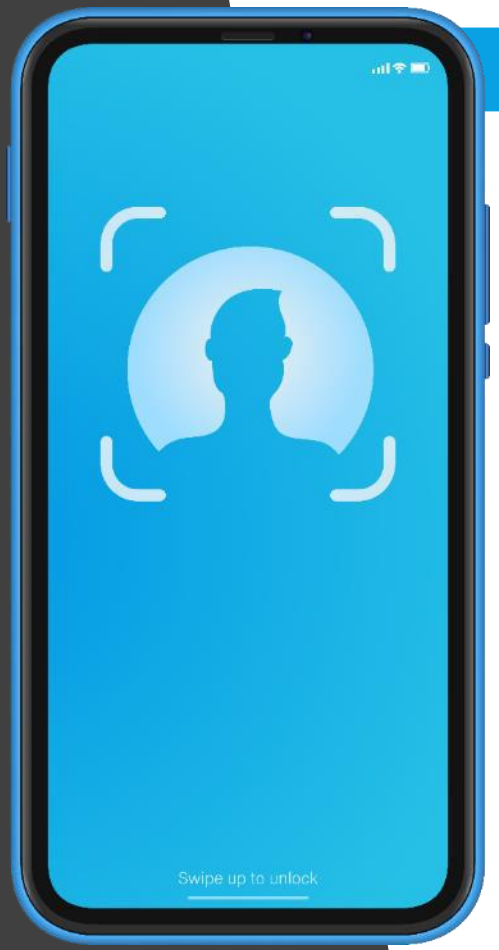
**Utilize algum aplicativo gerenciador de senhas** (Cofres de Senhas) **para organizar e proteger suas credenciais e senhas** (exemplos de “Cofres de Senhas”.: Dashlane, LastPass, 1Password, Keeper etc)

Utilize algum aplicativo com a função de Cofres de Senhas para gerenciar suas credenciais de acesso (usuários e senhas). Mantenha esse aplicativo criptografado com senha forte e restrita a você! **NÃO COMPARTILHE!**

# Configure o Touch ID / Face ID para desbloquear seus dispositivos

## Tela de bloqueio do iPhone ou iPad

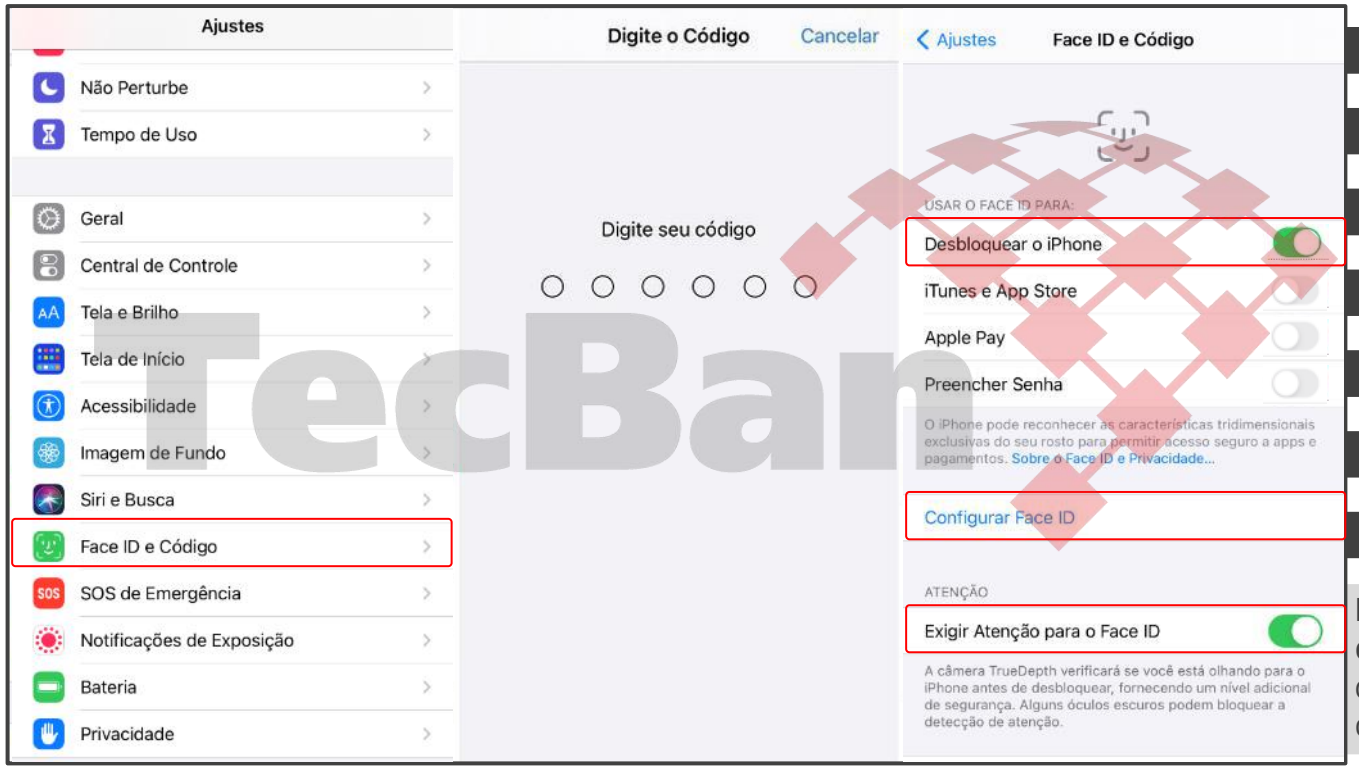
TecBan
cross-security@tecban.com.br




Ative o reconhecimento biométrico (Touch ID / Face ID) para desbloquear seus dispositivos (caso tenha a tecnologia disponível).

**Lembre-se:** Sempre crie senhas fortes (complexas) e DIFERENTES para acessar/desbloquear cada dispositivo, aplicativo, conta e e-mail.

## Veja o passo a passo para configurar o Touch ID / Face ID




1. Vá em *"Ajustes"*
2. Vá em *"Touch ID ou Face ID e Código"*
3. Digite seu código atual
4. Vá em *"Configurar Touch ID / Face ID"*
5. Siga o procedimento para configurar o reconhecimento por biometria
6. Ative a opção *"Desbloquear o iPhone"*
7. *No caso do FaceID, ative a opção "Exigir Atenção para o Face ID"*

**Evite utilizar a função de desbloqueio automático do celular com uso do Apple Watch**, pois se os dois forem roubados/furtados os criminosos conseguirão desbloquear o seu celular.

**NUNCA habilite este recurso para acessar seus aplicativos bancários. Reflita:** Se os criminosos tiverem acesso a sua senha para desbloqueio do dispositivo, eles conseguirão inserir novos dados biométricos, e com isso terão acesso irrestrito no seu aparelho. **Crie senhas fortes (complexas) e DIFERENTES para acessar/desbloquear cada aplicativo, contas bancárias e e-mails.**

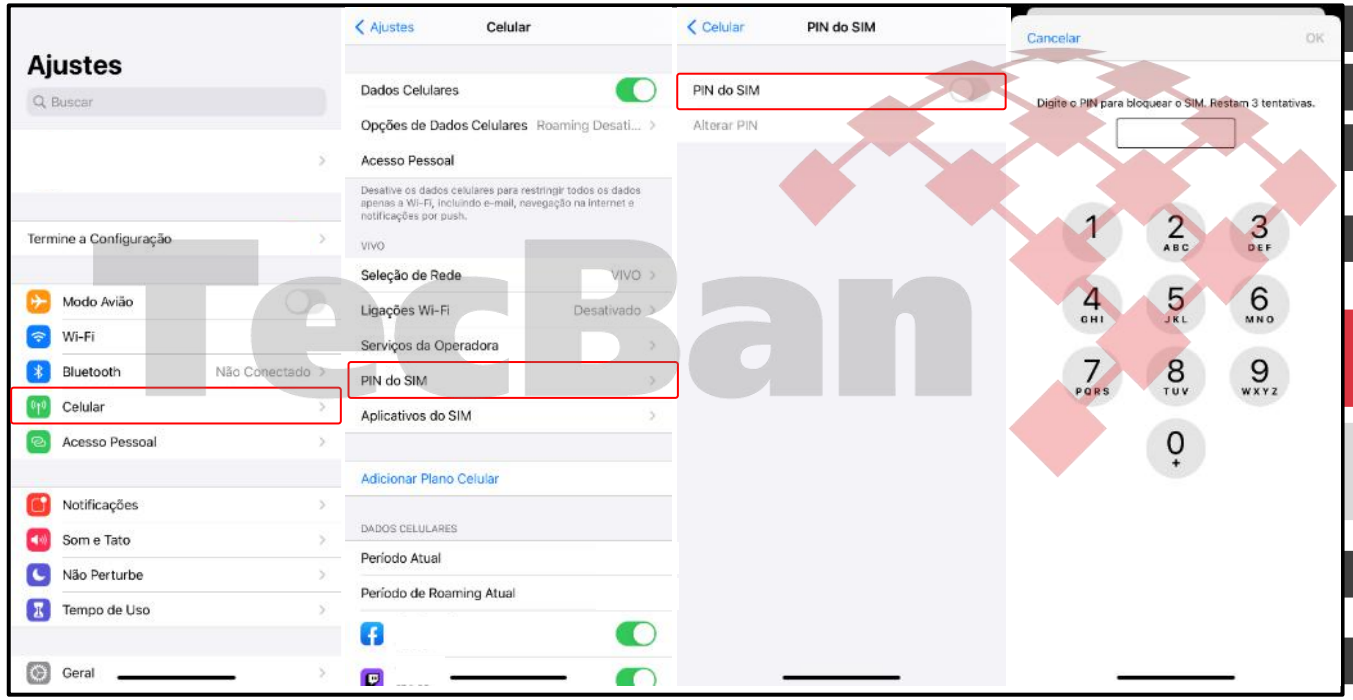
# Configure uma senha (PIN) no chip da sua linha telefônica (celular)

## PIN do chip

cross-security@tecban.com.br

Essa camada de segurança é muito importante! Defina uma senha no chip da sua linha telefônica (celular). Desta forma, os criminosos não conseguirão utilizar o seu chip em outro celular, e principalmente, não terão acesso as mensagens de áudios (via CAIXA POSTAL) para recuperar os códigos de recuperação de senhas. **Simples Assim!**

## Veja o passo a passo para configurar uma senha (PIN) no chip da sua linha celular




1. Vá em *"Ajustes"*
2. Vá em *"Celular"*
3. Selecione "*PIN do SIM*"
4. Digite o PIN atual. O código PIN está localizado no cartão/embalagem que você comprou o chip, juntamente com o PUK1 e PUK2.

**Atenção!** Não tente adivinhar o PIN. Caso erre 3 vezes a senha, seu chip será **bloqueado.**

Caso não tenha os códigos do PIN original, entre em contato com a operadora da sua linha telefônica

5. Após a inserção do PIN correto, será habilitado a opção *"Alterar PIN"*
6. Digite o novo PIN e **memorize bem ele!**

Após a configuração, toda vez que o dispositivo for iniciado será solicitado a senha do chip para ativar os recursos de rede da linha telefônica. Lembre-se de guardar em um local seguro (na sua casa) os **códigos PUK1 e PUK2 para recuperação do chip em caso de bloqueio do PIN.**

# Anote e guarde o IMEI do seu celular

## Faça o bloqueio do celular junto a operadora em caso de perda, furto ou roubo

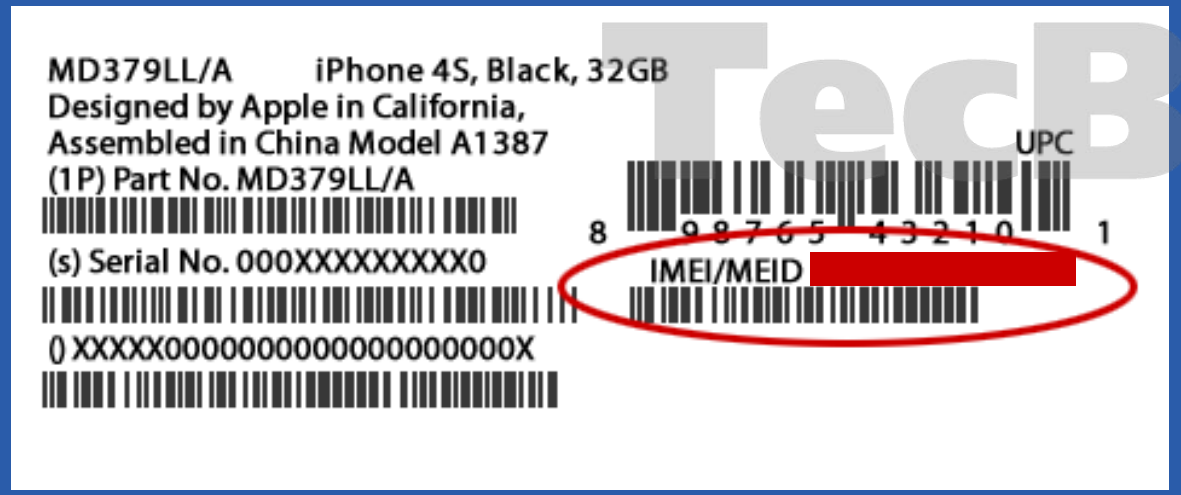
TecBan
cross-security@tecban.com.br

O código IMEI (Identificação Internacional de Equipamento Móvel, em português) é um número de identificação único e global, presente em aparelhos telefônicos como celulares e tablets. **Ele é composto de 15 números e pode ser utilizado para bloquear (inutilizar) o aparelho junto a operadora em caso de perda, furto ou roubo.**

## Veja como localizar o IMEI do seu dispositivo

### Embalagem original do produto

O IMEI pode ser encontrado na embalagem (caixa) original do produto ou na nota fiscal



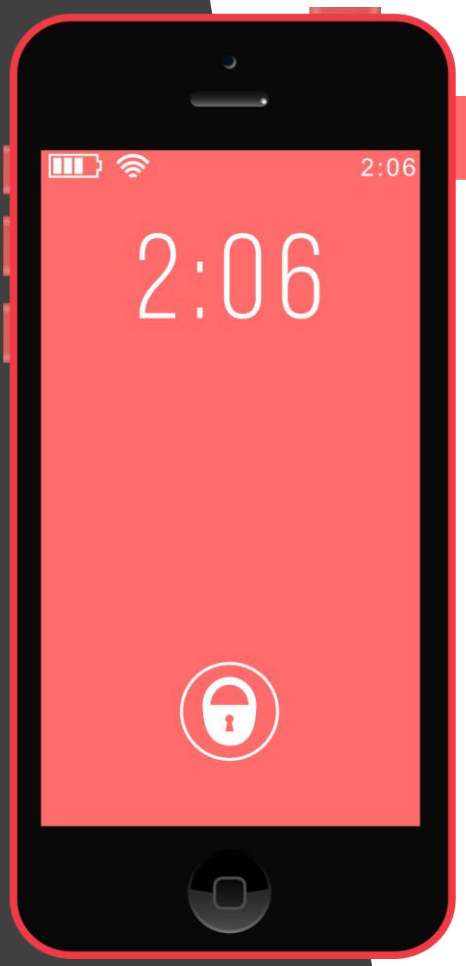

### Direto no aparelho

Para descobrir o IMEI do seu aparelho, digite ***#06#** no telefone, como se você fosse efetuar uma ligação. **O código, com 15 dígitos, será imediatamente exibido na tela.**

# Reduza o tempo de bloqueio automático da tela

## Tela de bloqueio (celulares/tablets/notebooks)

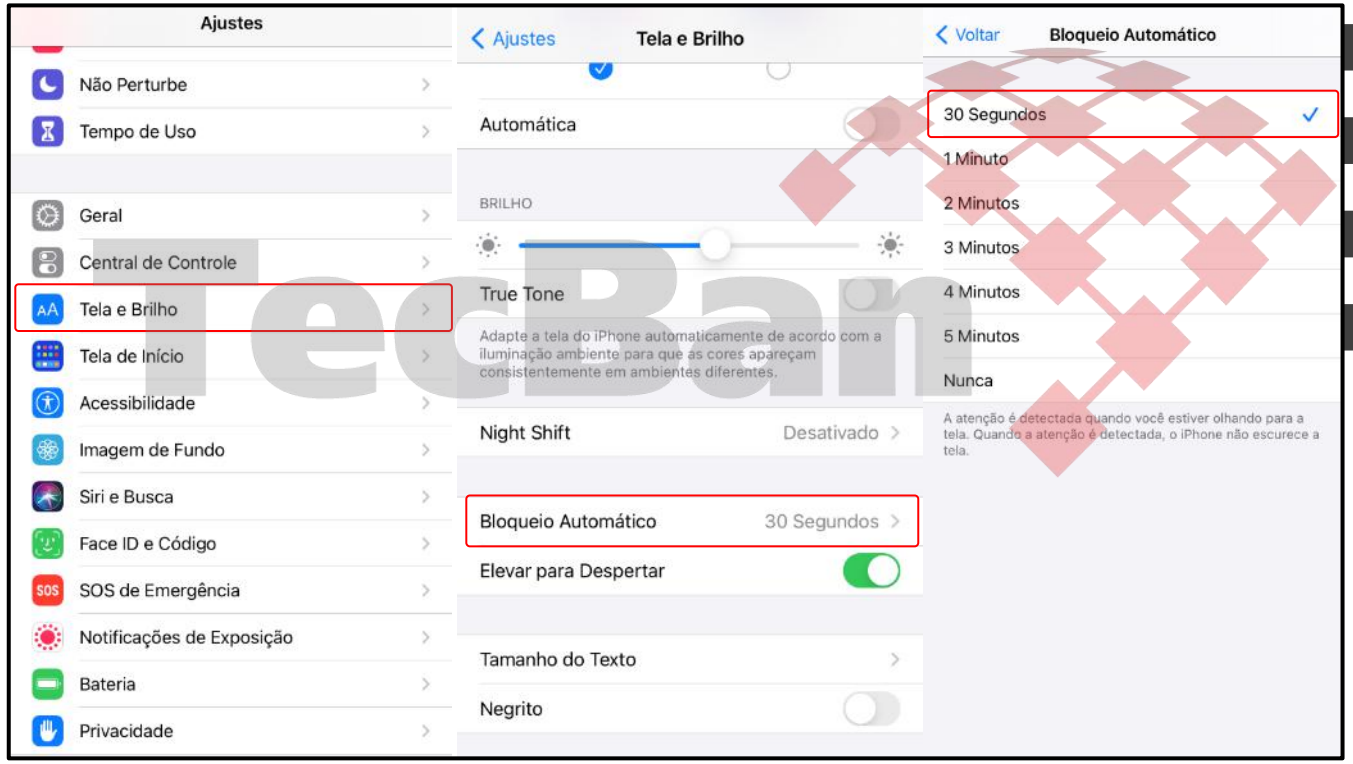
TecBan
cross-security@tecban.com.br




SEMPRE mantenha o seu dispositivo configurado para bloquear automaticamente a tela do aparelho quando estiver ocioso (sem utilização).

**É importante definir o menor tempo de bloqueio de tela (30 segundos ou menos),** pois caso seu celular seja perdido, furtado ou roubado, o bloqueio automático poderá evitar acessos indevidos aos seus dados/informações.

## Veja o passo a passo para reduzir o tempo de bloqueio automático da tela

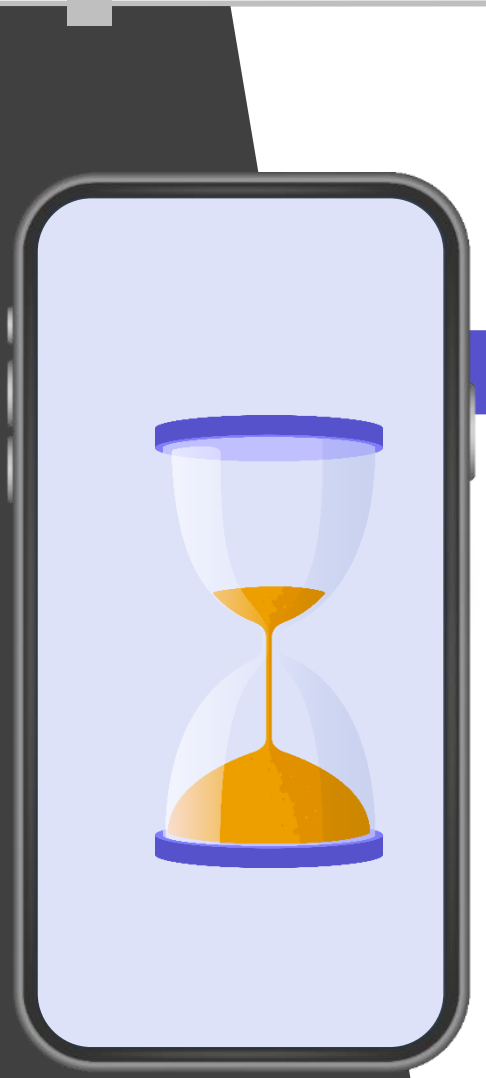



1. Vá em *"Ajustes"*
2. Vá em *"Tela e Brilho"*
3. Selecione *"Bloqueio Automático"*
4. Selecione a opção *"30 Segundos"*

# Configure o recurso “Tempo de Uso” & “Limites de Apps”

## Esse recurso possibilita manter bloqueado (com senha) os acessos aos aplicativos

TecBan
cross-security@tecban.com.br



O recurso “Tempo de Uso” permite limitar o tempo que os aplicativos podem ser utilizados. Quando o usuário atinge o limite de tempo estipulado, é solicitado uma senha para liberar o acesso ao aplicativo por mais 1 min, 15 min, 1 hora ou “aprovar o dia inteiro”. Recomendamos manter bloqueada todas as funções (“Tudo (Apps e Categorias”). Defina o tempo: “1min, Todos os Dias”

**Não mantenha a configuração no formato “aprovar o dia inteiro”, pois caso precise sair da sua residência e tenha a infelicidade de sofrer um sinistro, os aplicativos estarão desbloqueados. Sempre avalie qual o nível de risco você está disposto correr ou aceitar... Quanto maior o risco, significa aceitar, potencialmente, maior prejuízo...**

## Veja o passo a passo para habilitar o recurso “Tempo de Uso”


1. Vá em *“Ajustes”*
2. Depois em *“Tempo de Uso”*
3. Selecione a opção *“Usar Código do Tempo de Uso”*
4. Crie uma senha de 4 dígitos, diferente das senhas que você possui em outras ferramentas/aplicativos
5. Informe seus dados do ID Apple caso seja necessário recuperar a senha
6. Voltando ao menu do *“Tempo de Uso”*, clique em *“Limites de Apps”*
7. Recomendamos manter a opção *“Tudo (Apps e Categorias)”* habilitado/ativado, e definir para bloquear após 1 minuto de utilização dos apps

Este recurso passa a funcionar automaticamente de 5 a 10 minutos após da habilitação/configuração deste recurso

# Desative todos os recursos para visualização com a tela bloqueada

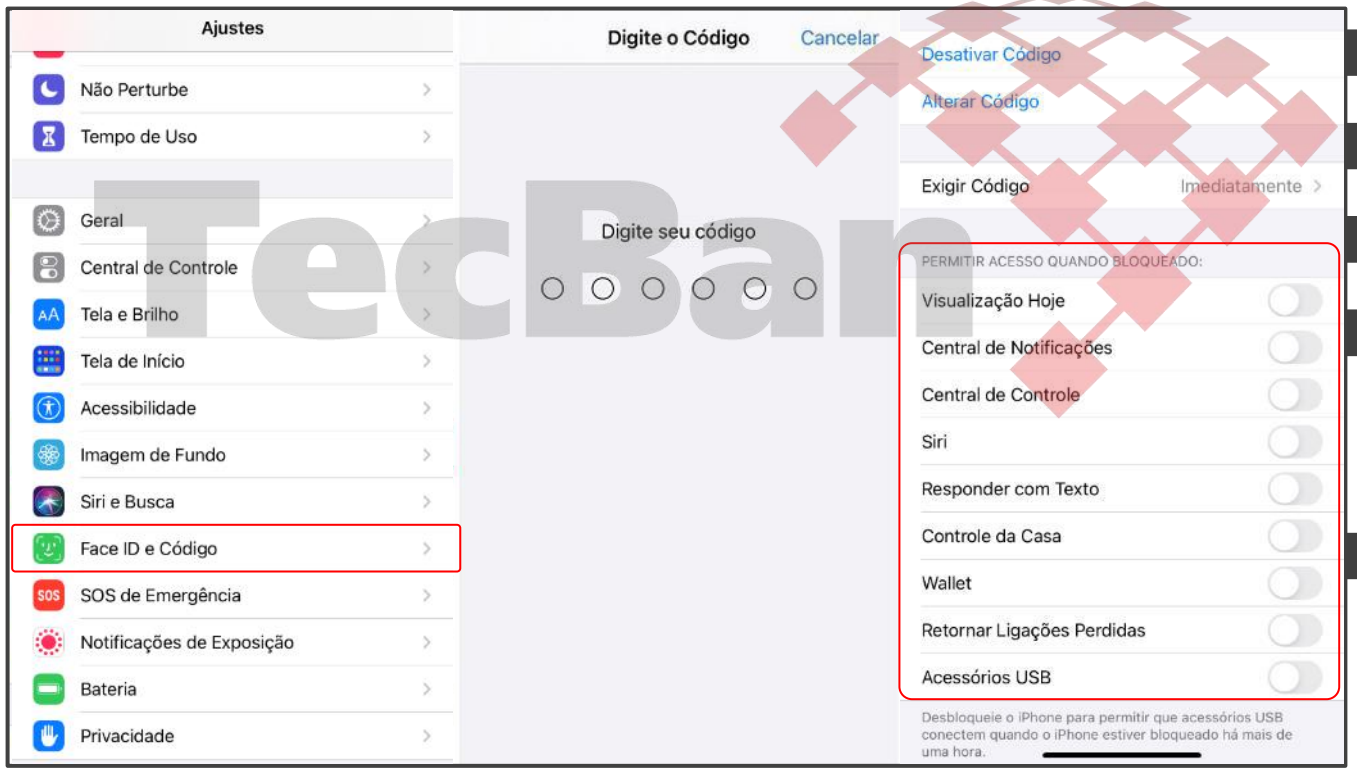
## Desative todas as opções “Permitir Acesso Quando Bloqueado”

TecBan
cross-security@tecban.com.br


Os dispositivos móveis possibilitam acessar/visualizar diversos recursos mesmo com a tela bloqueada. É possível, por exemplo, checar os widgets, notificações, responder mensagens e ligações, utilizar a câmera, visualizar fotos, utilizar a SIRI, abrir a central de controle etc

Desative todos estes recursos e evite que os criminosos consigam acessar dados/informações para realizar fraudes/golpes. Também é importante desativar estes recursos, pois os criminosos não conseguirão colocar seu dispositivo no modo avião (evitando que o aparelho seja rastreado e impedido de ser formatado (wipe) remotamente.

## Veja o passo a passo para desativar todos os recursos disponíveis com a tela bloqueada




1. Vá em *“Ajustes”*
2. Vá em *“Touch ID e Código”* ou *“Face ID e Código”*
3. Digite seu código atual
4. **Desative todos os recursos** na guia *“Permitir acesso quando bloqueado”*

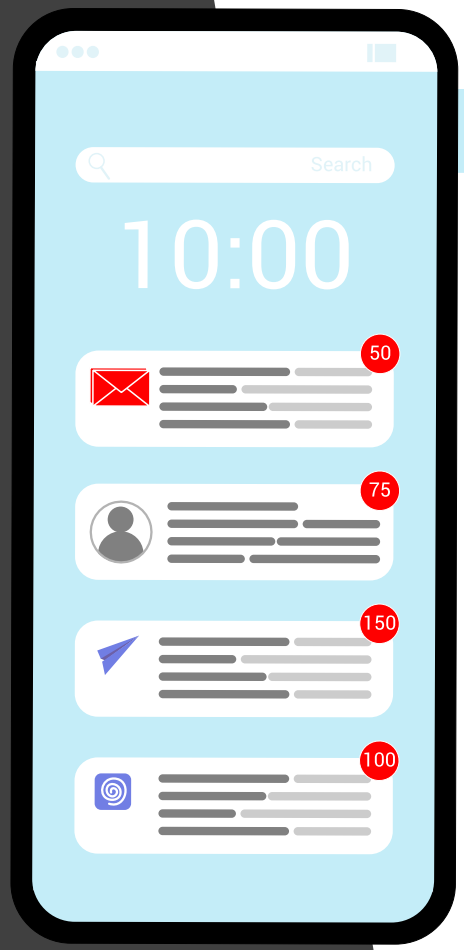
**Mantenha todas as opções do quadro ao lado (esquerdo) desativadas.**

5. **Revise periodicamente essas configurações, pois em alguns casos quando ocorre a atualização do sistema operacional, algumas opções podem ser habilitadas automaticamente.**

# Desative a pré-visualização de notificações com a tela bloqueada

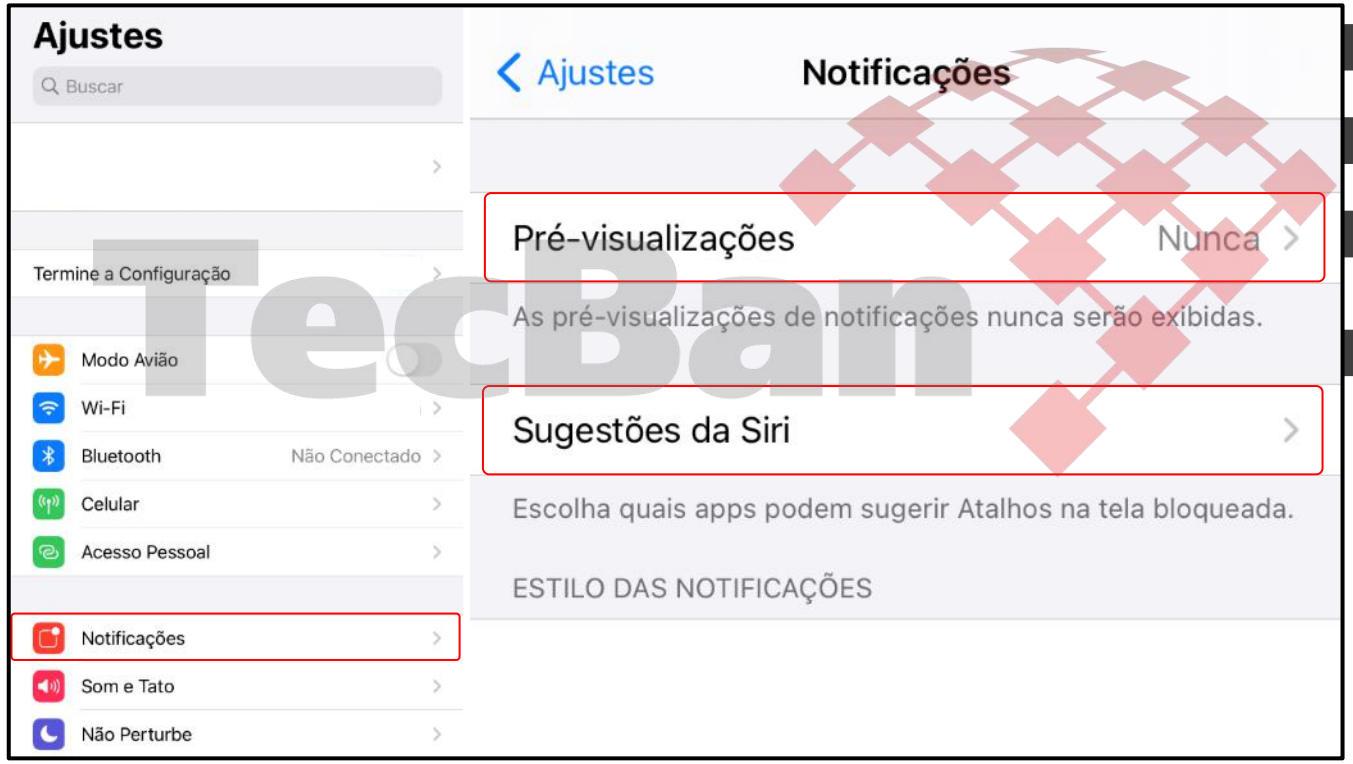
## Desative todas as Notificações de mensagens com a tela bloqueada

TecBan
cross-security@tecban.com.br




Mesmo com a tela bloqueada é possível ler o conteúdo de mensagens (WhatsApp, Telegram, Facebook), e-mails, SMS etc, através da pré-visualização de notificações. Desative esses recursos abaixo.

## Veja o passo a passo para desativar a pré-visualização de notificações na tela bloqueada




1. Vá em *"Ajustes"*
2. Vá em *"Notificações"*
3. Em *"Pré-visualizações"* selecione "**NUNCA**"
4. Em "Sugestões da Siri" + "Sugestões na Tela Bloqueada", MANTENHA ESSA OPÇÃO **DESATIVADA**

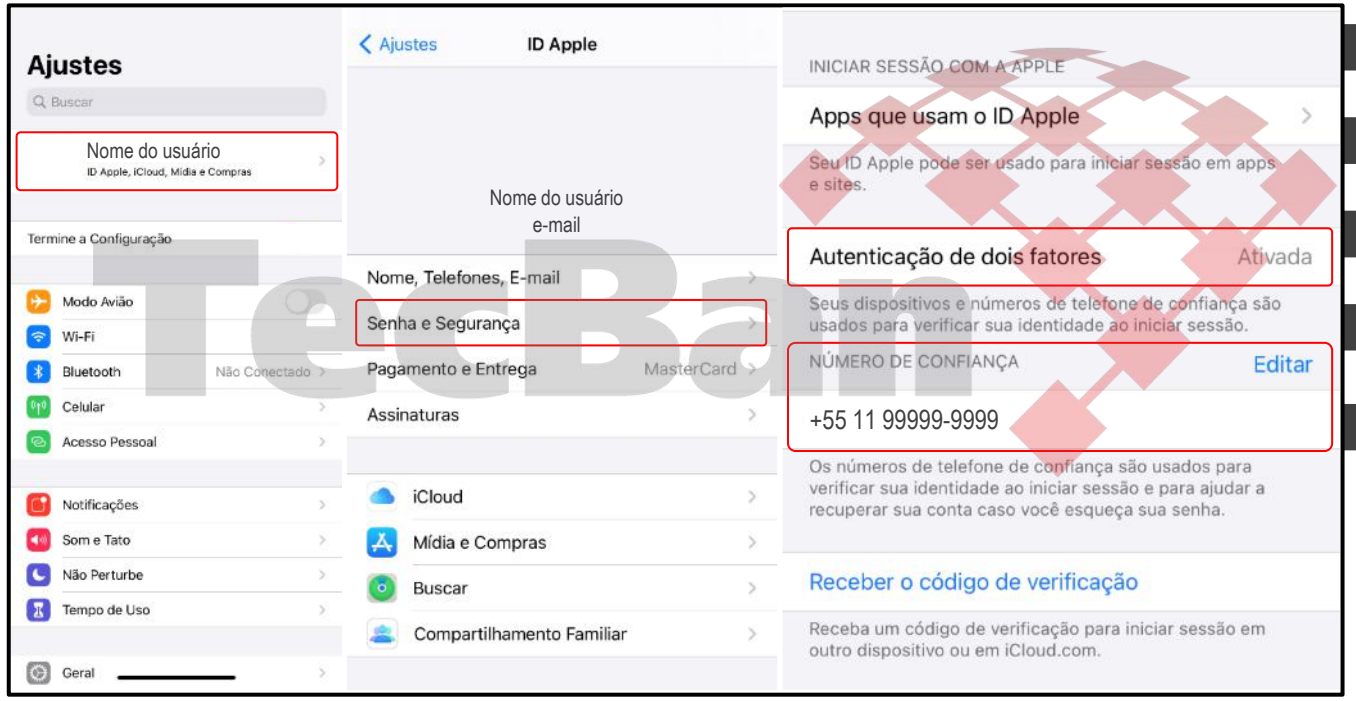
# Ative o duplo fator de autenticação e informe um número de confiança

## Dupla camada de segurança para acesso ao iCloud/ID Apple de forma segura

TecBan
cross-security@tecban.com.br

Ative o duplo fator de autenticação e defina um telefone de confiança para iniciar sessão/login no iCloud/ID Apple. **Com este recurso, além da digitação da senha pessoal, será necessário informar um código de verificação de segurança que será enviado por SMS ou Token através de um dispositivo confiável** (autorizado/cadastrado previamente por você).

## Veja o passo a passo para ativar o duplo fator de autenticação para iniciar sessão no iCloud



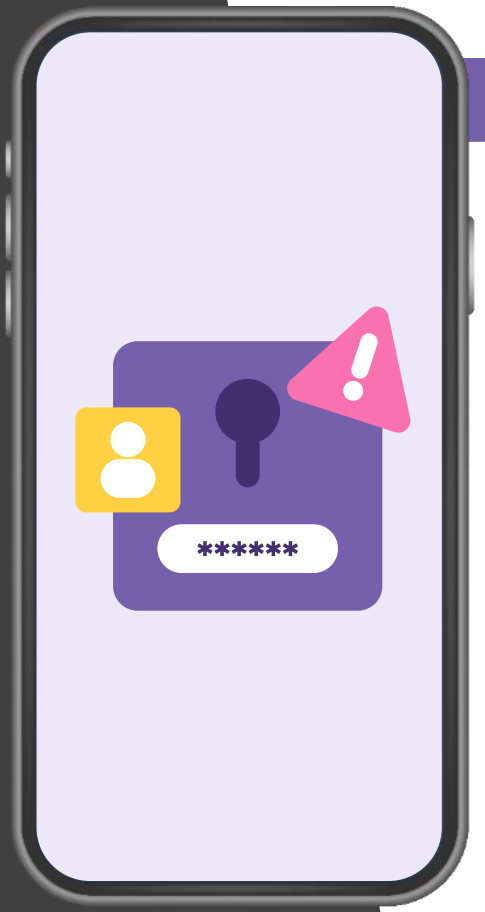

1. Vá em *"Ajustes"*
2. Clique no seu nome de usuário
3. Vá em *"Senha e Segurança"*
4. Ative a opção *"Autenticação de dois fatores"*
5. Informe um *"Número de Confiança"*

Atenção! **Não configure o mesmo número telefônico do seu aparelho**, na função "número de confiança" pois os malfeitores utilizarão o recurso "esqueci minha senha" para receber o código de recuperação no dispositivo sinistrado. Informe um número de confiança (telefone celular) de um contato de confiança, ou de outra linha que você possui. OK?

# Desative o recurso “Preencher Senhas”

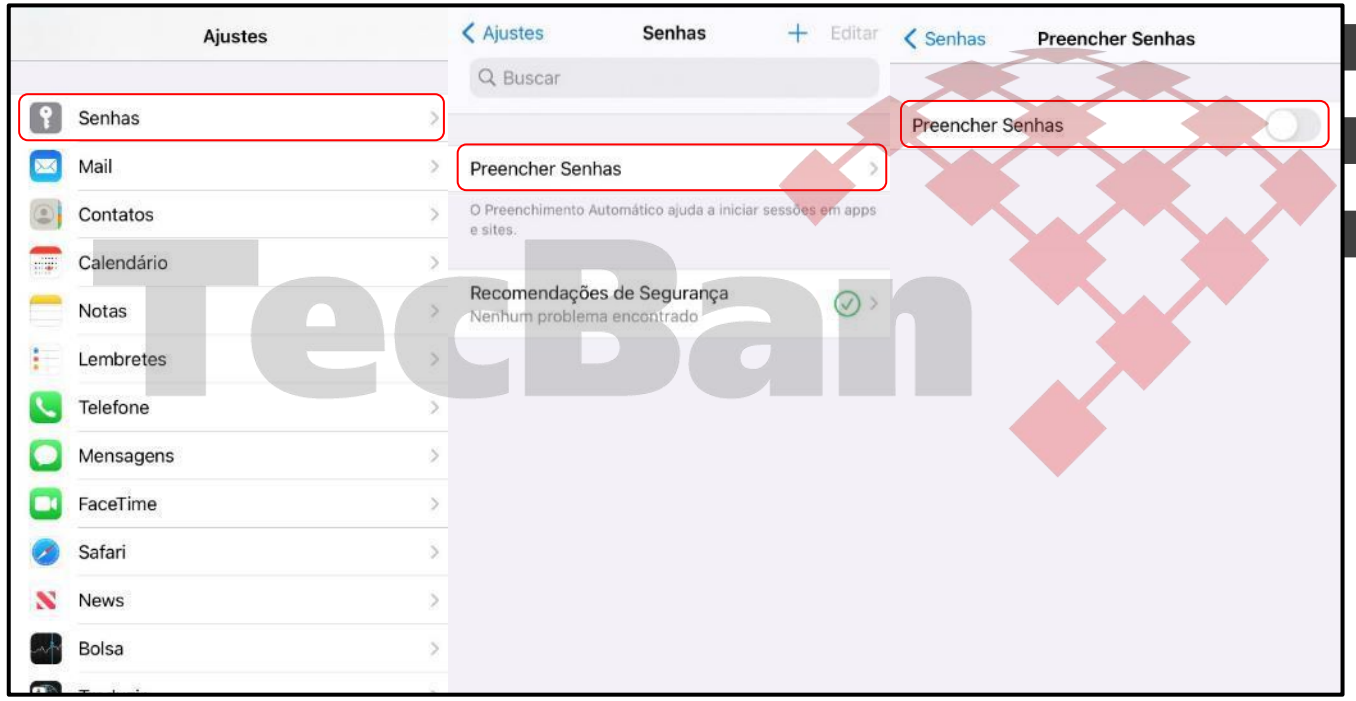
## Não utilize o recurso de salvamento automático de senhas (“lembrar/salvar/preencher senha”)

TecBan
cross-security@tecban.com.br




DESATIVE o recurso “lembrar/salvar/preencher” senhas nos seus dispositivos, aplicativos ou navegadores (browsers). **As senhas ficam salvas no histórico e podem ser acessadas facilmente pelos criminosos (localmente ou remotamente). Não aceite esse risco, assim não fará parte das estatísticas (vítimas)!**

## Veja o passo a passo para desativar o recurso “Preencher Senhas” do iOS




1. Vá em *“Ajustes”*
2. Vá em *“Senhas”*
3. Clique em *“Preencher Senhas”* e **desative o recurso**

Aqui é possível visualizar as senhas caso este recurso seja habilitado por padrão. **Caso tenha senhas salvas aqui, apague-as imediatamente**. Utilize algum aplicativo com a função de Cofres de Senhas (ex: Dashlane, LastPass, 1Password, Keeper etc) para gerenciar suas credenciais de acesso (usuários e senhas). Mantenha esse aplicativo criptografado com senha forte e restrita a você!

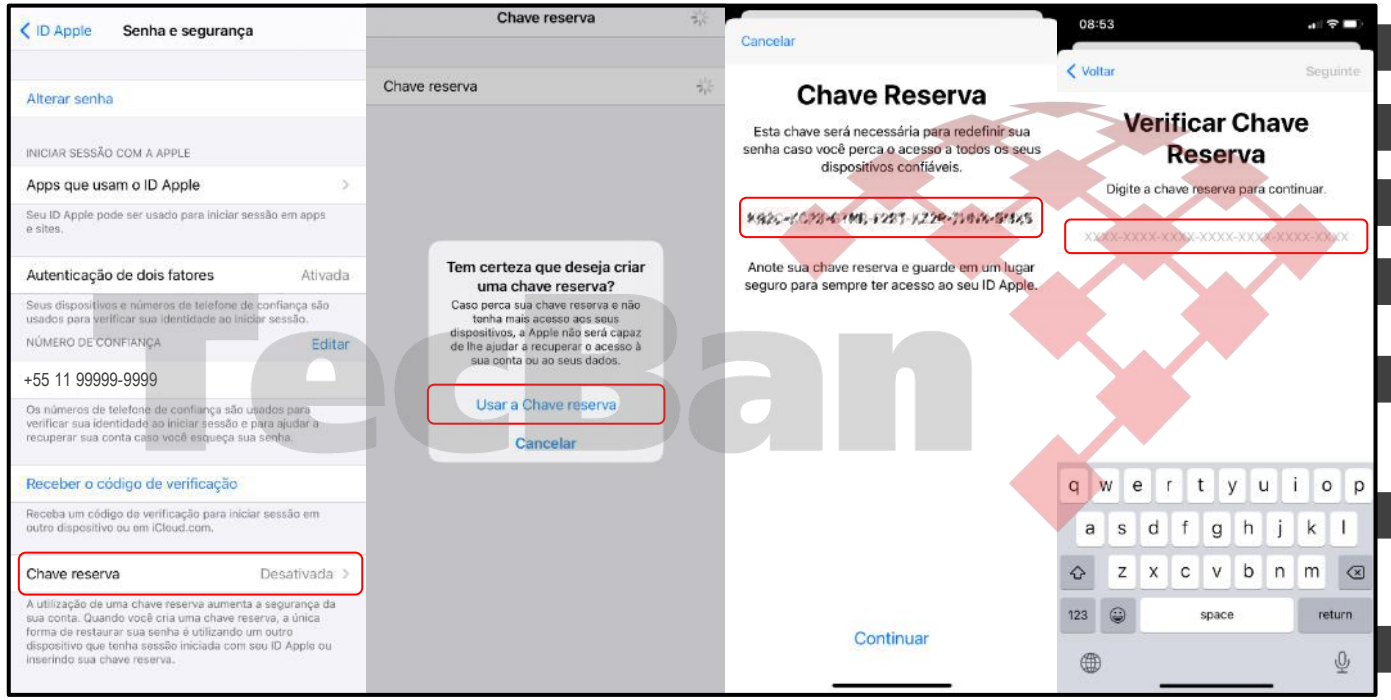
# Configure a Chave Reserva na sua conta iCloud/ID Apple

## Essa Chave Reserva aumenta expressivamente a segurança da sua conta iCloud/ID Apple

TecBan
cross-security@tecban.com.br

Após ativar o duplo fator de autenticação (número de confiança), é possível gerar um Chave Reserva (código de 28 caracteres aleatórios) **que pode ser usada para redefinir a senha e/ou recuperar o acesso ao ID Apple.** Esse recurso aumenta expressivamente a segurança da sua conta e te ajuda a recupera-la imediatamente. **Mas, lembre de guardar em local seguro essa Chave Reserva.**

## Veja o passo a passo para gerar a Chave Reserva da sua conta iCloud/ID Apple




1. Vá em *"Ajustes"*
2. Clique no seu nome de usuário
3. Vá em *"Senha e Segurança"*
4. Selecione a opção *"Chave Reserva"*
5. Leia com atenção a mensagem e clique em *"Usar chave reserva"*
6. **A chave com 28 caracteres será apresentada na tela.** Anote e guarde em um local seguro
7. Digite a chave gerada para finalizar a configuração

**Atenção!** Se você esquecer a senha do ID Apple, poderá recuperá-la utilizando um outro dispositivo que tenha uma sessão iniciada com o seu ID Apple, como por exemplo: iPad, MacBook ou iPhone. Outra opção é usar a Chave Reserva, o número de confiança (número informado na autenticação de dois fatores) e um dispositivo Apple para redefinir a senha.
**Lembre-se: A Apple não tem acesso a sua Chave Reserva, caso não tenha a chave ou outro dispositivo com uma sessão iniciada com o seu ID Apple, não será possível recuperar sua conta e/ou trocar a senha.**

# Recuperando sua conta iCloud/ID Apple com a Chave Reserva

## Passo a passo de como recuperar sua conta/trocar senha utilizando a Chave Reserva

TecBan
cross-security@tecban.com.br

Em outro dispositivo Apple (iPad, MacBook ou iPhone), instale o aplicativo *"Suporte da Apple"* via loja de aplicativo (Apple Store).
Dentro do app, vá em "Senha e segurança", clique em "Redefinir senha do ID Apple", depois clique em "Introdução" e siga os passos abaixo:

**1**

**Informe seu ID Apple**


**2**

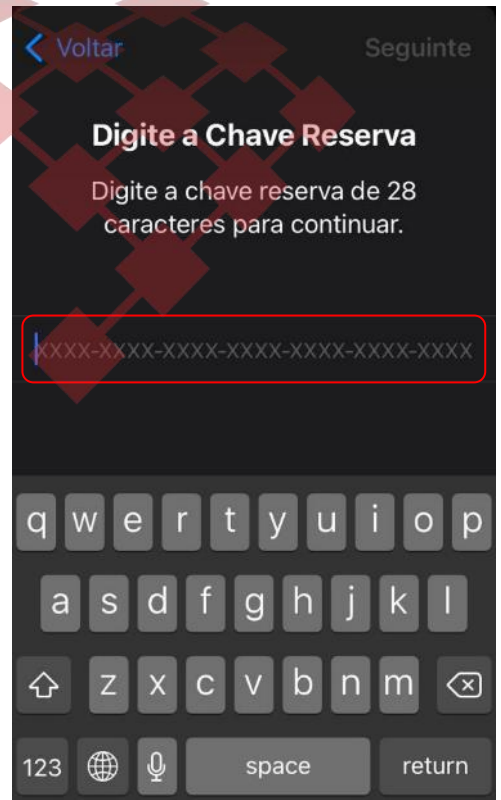
**Informe o número do telefone de confiança** (número configurado na autenticação de dois fatores para recebimento dos códigos de segurança)


**3**

**Um notificação para troca de senha será enviado para seu dispositivo.**
Caso não tenha mais acesso a ele (perda, furto ou roubo), clique em *"Não consegue acessar seu dispositivo?"*


**4**

**Informe a Chave Reserva da sua conta iCloud/ID Apple** (código de 28 caracteres)



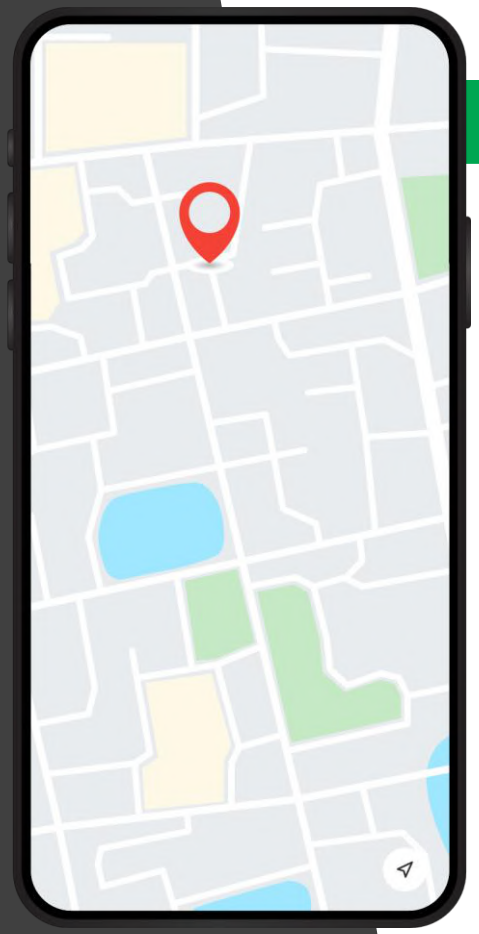

**5**

Caso os dados estejam corretos, **será apresentado uma tela para a definição de uma nova senha**

# Ative o recurso “Buscar meu iPhone”

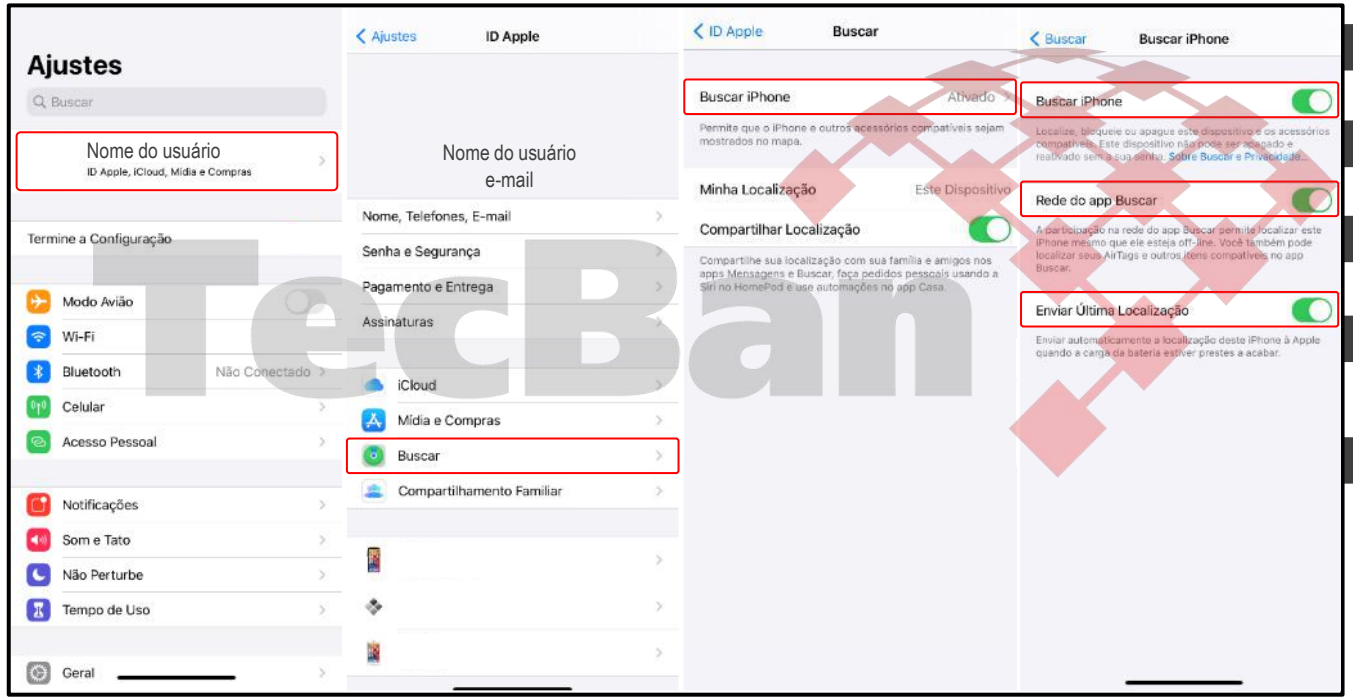
## Localizar dispositivo

TecBan
cross-security@tecban.com.br



A Apple oferece o recurso Buscar iPhone (Find My iPhone), que poderá te ajudar a encontrar seu dispositivo em caso de perda, furto ou roubo. Basta iniciar uma sessão no iCloud para **ver no mapa o dispositivo perdido, bloquear ou apagar seus dados remotamente.**

## Veja o passo a passo para ativar o recurso “Buscar meu iPhone”

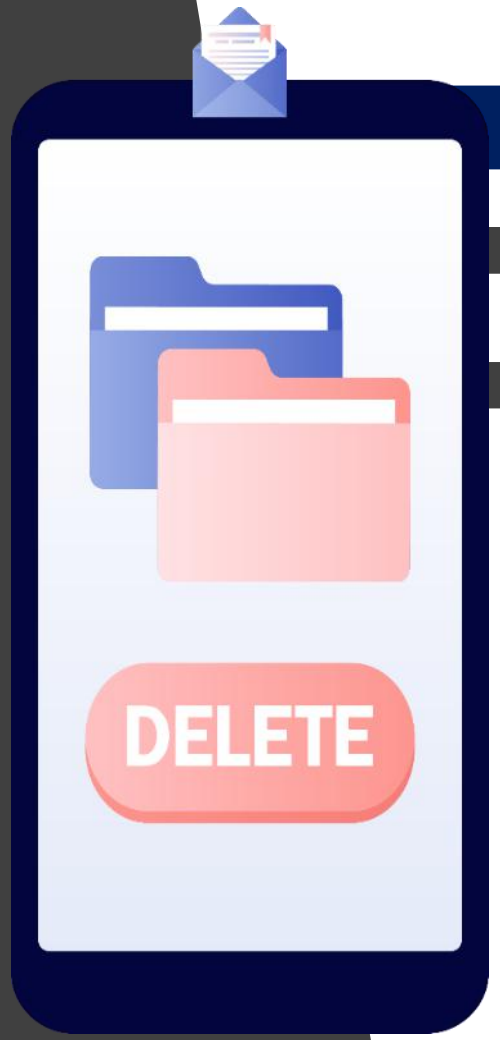



1. Vá em *“Ajustes”*
2. Clique no seu nome de usuário
3. Vá em *“Buscar”*
4. Ative a opção *“Buscar iPhone”*
5. Dentro de *“Buscar iPhone”*, ative as demais opções *“Rede de app Buscar”* e *“Enviar Última Localização”*

# Em caso de sinistro, apague remotamente os dados do seu dispositivo

Apague (função conhecida como wipe) os dados em caso de perda, furto ou roubo do dispositivo

TecBan
cross-security@tecban.com.br



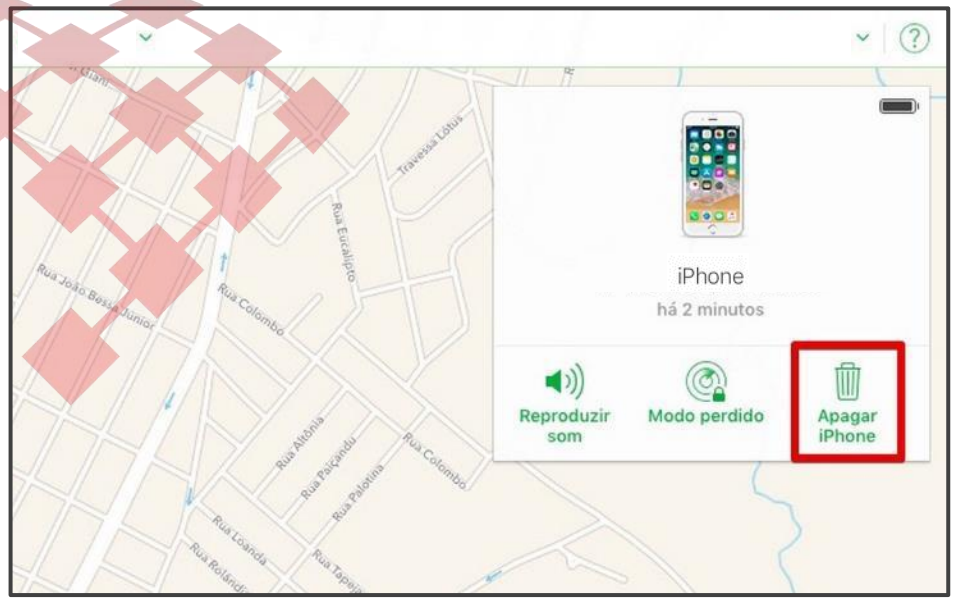

Se seu dispositivo Apple for perdido ou roubado, você poderá apagá-lo através do recurso Buscar meu iPhone no https://www.icloud.com/find

## Veja o passo a passo para apagar remotamente os dados do seu dispositivo

1 Acesse o site do iCloud e faça login na sua conta Apple (também chamada de ID Apple). É importante usar a mesma conta que está logada no dispositivo. Em seguida, clique em *"Buscar iPhone"*. **NUNCA clique em links solicitando atualização de cadastros do ID Apple ou dos seus e-mails. SEMPRE digite você mesmo a URL/Site, pois existem vários golpes no mercado para induzir os usuários a clicar em URLs/Sites parecidos com o oficial.**

2 No topo da página, vá em *"Todos os dispositivos"* e, na lista que aparece, clique sobre o nome do aparelho que você quer apagar.


3 A última localização conhecida do seu celular será exibida no mapa. No menu à direita, clique em *"Apagar iPhone"*.




Se seu dispositivo estiver **on-line**, o apagamento remoto começará depois que você seguir as instruções na tela. Se estiver **off-line**, ele será apagado remotamente na próxima vez que estiver on-line.

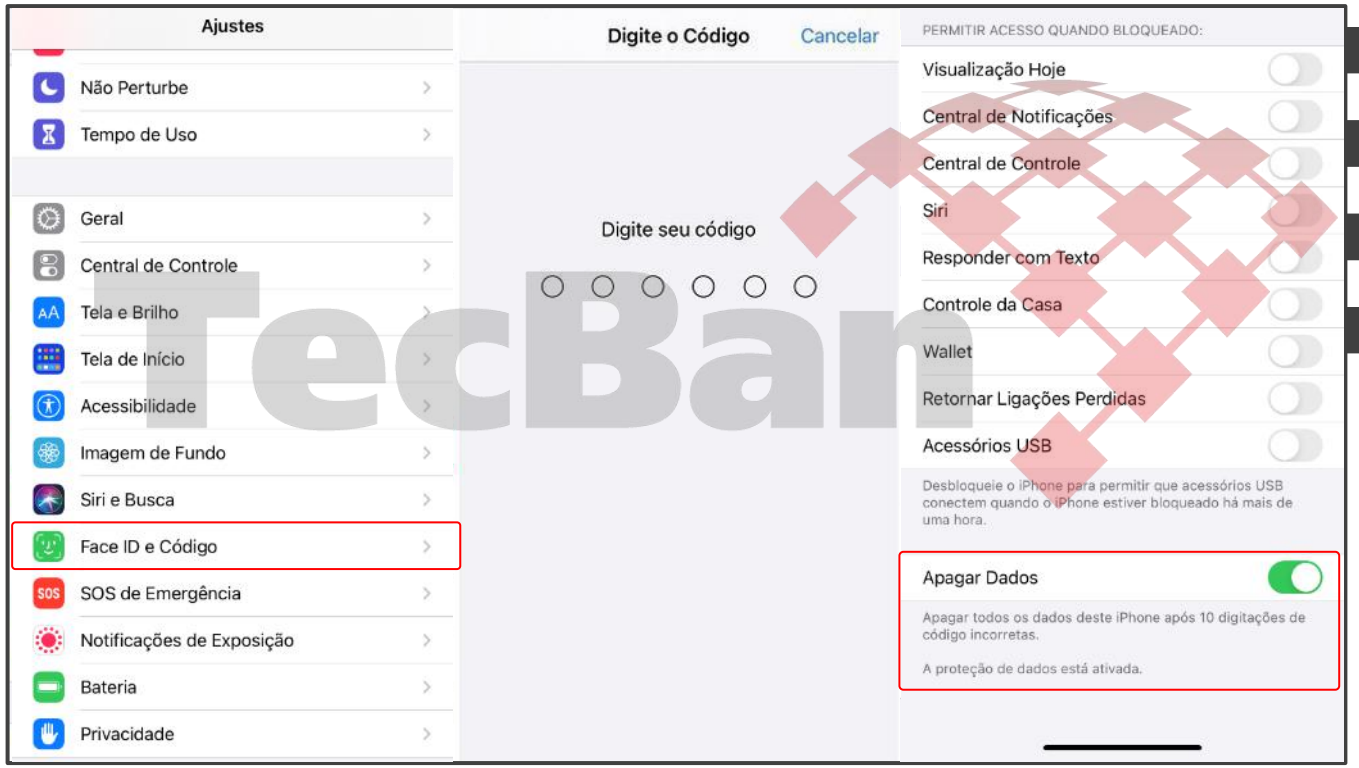
# Habilite preventivamente a função “Apagar Dados”

Todos os dados do seu dispositivo serão apagados após 10 digitações de código incorretas (tentativas de desbloqueios de tela)

TecBan
cross-security@tecban.com.br

Os dispositivos Apple permitem configura-los para apagar todos os dados do aparelho após 10 tentativas de desbloqueio sem sucesso.


## Veja o passo a passo para apagar os dados do dispositivo após 10 tentativas de desbloqueio




1. Vá em *“Ajustes”*
2. Vá em *“Touch ID e Código”* ou *“Face ID e Código”*
3. Digite seu código atual
4. Ative a opção *“Apagar Dados”*

Atenção! Se você ativar este recurso (“Apagar Dados”), **todos os dados do seu dispositivo serão apagados após 10 digitações de código incorretas.**

# Faça backup semanalmente dos seus dispositivos

## Faça backup manual via iTunes no seu PC/Windows ou MacOS dos seus dispositivos = iPhone e iPad

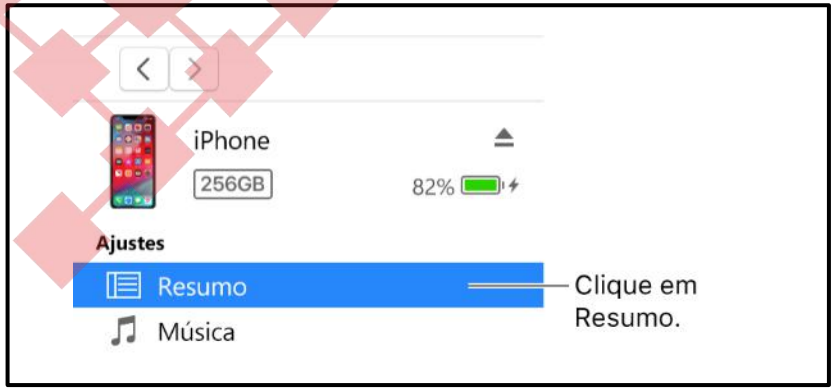
TecBan
cross-security@tecban.com.br

**Pense rápido! E se o seu dispositivo for sinistrado agora?** Certamente, passou um filme na sua cabeça neste exato momento...
**Você aceitaria perder todas as fotos e vídeos de viagens** (momentos eternizados)**, de amigos, da família, documentos?**
Creio que a resposta será NÃO!!!! ENTÃO, FAÇA BACKUP, NO MÍNIMO SEMANAL, DOS SEUS DISPOSITIVOS. Não arrisque e "pague" para ver.
Somente instale o aplicativo iTunes via loja de aplicativo (Apple Store ou Microsoft Store). **É muito importante que você faça um backup offline (local) dos seus celulares/tablets em algum computador (PC/Windows ou MacOS) de sua confiança,** pois caso os seus dispositivos (telefone ou tablet) **sejam sinistrados** (perdido, furtado ou roubado)**, você conseguirá recuperar seus documentos, fotos, vídeos, mensagens etc.**

## Veja o passo a passo para realizar o backup do seu dispositivo via iTunes

**1** Conecte o dispositivo ao computador para sincronizar. No app iTunes do PC, clique no botão *"Dispositivo"* próximo à parte superior da janela do iTunes


**2** Clique em *"Resumo"*




**3** Clique em *"Fazer Backup Agora"*. Para criptografar os backups, selecione *"Criptografar backup do [dispositivo]"*, digite uma senha e clique em Definir Senha.

**SEGURANÇA EM CAMADAS: Caso decida fazer backup na nuvem** (iCloud, Google Drive, One Drive, etc), lembre-se de criar uma senha forte para acesso e também ative o duplo fator de autenticação

# Riscos de Segurança

## Golpe do sequestro/clonagem de contas (WhatsApp e Telegram)

# Golpe do sequestro/clonagem de contas (WhatsApp e Telegram)

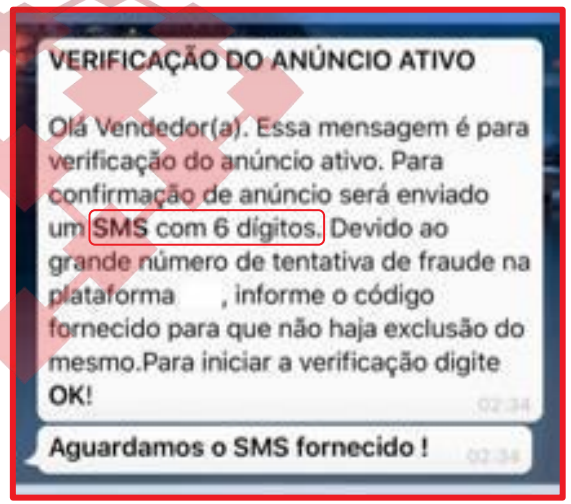
## Riscos de segurança

TecBan
cross-security@tecban.com.br

## Um golpe muito utilizado pelos criminosos é o sequestro/clonagem de contas (WhatsApp e Telegram)

Os criminosos descobrem seu número e fazem o cadastro no WhatsApp/Telegram. Agora eles precisam do **código de confirmação de 6 dígitos** que é enviado via SMS. Para conseguir este código, os fraudadores utilizam diversas **técnicas de engenharia social.**

Uma forma muito comum é enviar uma mensagem **simulando ser representante ou atendente de uma empresa famosa**. Normalmente de alguma empresa onde você realizou um cadastro (iFood, Rappi, WebMotors, Mercado Livre etc)




Se o código for repassado, **o criminoso terá acesso a sua conta e todas as mensagens armazenadas**

**Caso sua conta do WhatsApp tenha sido sequestrada/clonada, envie um e-mail para support@whatsapp.com, relate o caso e informe o número da sua linha. Será realizado o bloqueio temporário da sua conta até você conseguir recuperá-la.**

# Ative a confirmação/verificação em duas etapas

## Passo a passo nos aplicativos: WhatsApp e Telegram

TecBan
cross-security@tecban.com.br

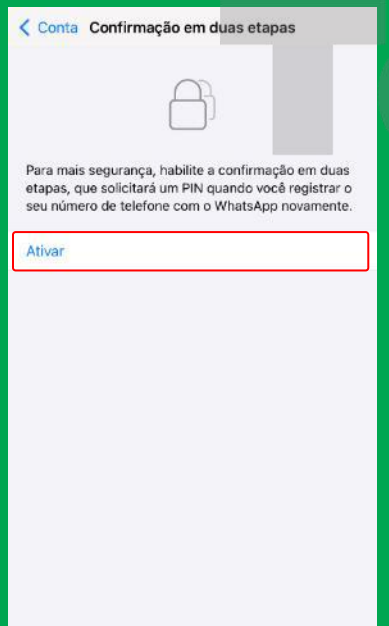
Para evitar o golpe do sequestro/clonagem de contas, é possível adicionar uma confirmação/verificação em duas etapas (senha) para registrar seu número no WhatsApp ou Telegram, ou seja, além do código enviado por SMS, **também será solicitado uma senha para concluir o registro.**

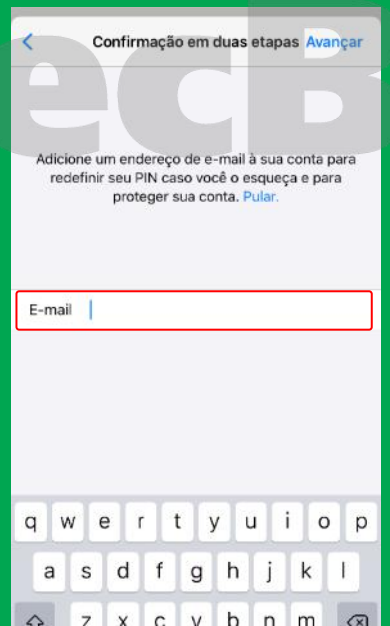
## Veja como ativar a confirmação/verificação em duas etapas

**NUNCA** repasse/compartilhe para outras pessoas o código de confirmação de **6 dígitos e/ou a sua senha**

### WhatsApp

1. Dentro do app, vá em ***"Configurações"***, depois vá em ***"Conta"*** e por último clique em ***"Confirmação em Duas Etapas"***
2. Clique em ***"Ativar"*** e insira uma senha de 6 dígitos
3. Informe um **e-mail** caso seja necessário recuperar a senha

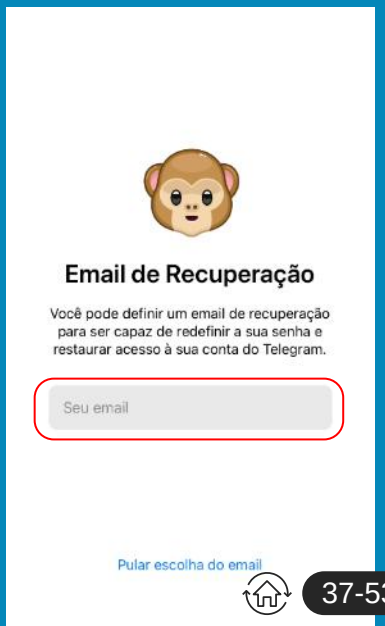




### Telegram

1. Dentro do app, vá em ***"Configurações"***, depois vá em ***"Privacidade e Segurança"*** e por último clique em ***"Verificação em Duas Etapas"***
2. Clique em ***"Definir Senha Adicional"*** e insira uma senha forte composta por letras, números e caracteres especiais
3. Informe um **e-mail** caso seja necessário recuperar a senha





# Verifique e encerre as sessões ativas em outros dispositivos

## Passo a passo nos aplicativos: WhatsApp e Telegram

TecBan
cross-security@tecban.com.br

O WhatsApp e Telegram permitem acessar suas conversas através do computador (versão web) ou de outros dispositivos.

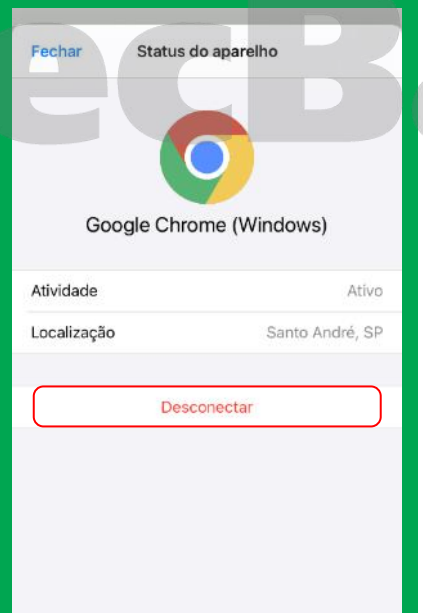
**Atenção! Se você não encerrar as sessões (logout), outro usuário do computador/dispositivo poderá acessar suas conversas e/ou trocar suas senhas.**

## Veja como encerrar as sessões ativas em outros dispositivos

### WhatsApp

1. Dentro do app, vá em ***"Configurações"***, depois vá em ***"Aparelhos conectados"***
2. Será mostrado os dispositivos onde você tem uma sessão ativa
3. Clique no dispositivo que você deseja encerrar a sessão e clique em ***"Desconectar"***






### Telegram

1. Dentro do app, vá em ***"Configurações"***, depois vá em ***"Dispositivos"***
2. Será mostrado os dispositivos onde você tem uma sessão ativa
3. Deslize para o lado esquerdo no dispositivo que você deseja encerrar a sessão e clique em ***"Terminar"***



# Riscos de Segurança

TecBan

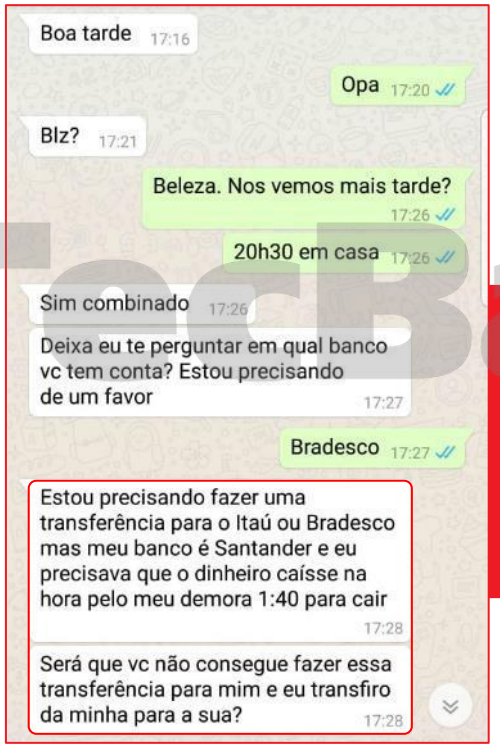
## Golpe de solicitação de empréstimo de dinheiro (WhatsApp e Telegram)

# Golpe solicitação de empréstimo de dinheiro (WhatsApp e Telegram)

## Riscos de segurança

TecBan
cross-security@tecban.com.br

A partir do sequestro/clonagem de contas do WhatsApp e Telegram, um golpe muito aplicado é o de **solicitação de empréstimo de dinheiro**




Após conseguir sequestrar/clonar uma conta do WhatsApp e Telegram, os criminosos fingem ser essa pessoa, criam uma narrativa e **passam a enviar solicitações de empréstimo de dinheiro para familiares, amigos e contatos.**

**Não aceite pedidos/mensagens solicitando transferências de dinheiro**

Faça uma via videochamada com o seu contato (através do telefone original) e confirme o pedido indesejado. Na dúvida, nunca transfira qualquer valor (R$) para contas bancárias de desconhecidos. Caso identifique que é um golpe, avise seus contatos e denuncie para o aplicativo (Whatsapp, Telegram).

# Privacidade: Restrinja o acesso aos seus dados

## Veja abaixo o “passo a passo” para configurar essas proteções nos aplicativos: WhatsApp e Telegram

TecBan
cross-security@tecban.com.br

**Normalmente, alguns dados como número de telefone e foto de perfil ficam disponíveis para serem visualizados por qualquer pessoa.** Criminosos podem usar essas informações para criar perfis “fakes” para enganar seus amigos, familiares e demais contatos. Configure para somente os seus contatos da agenda terem acesso a foto do seu perfil.

## Veja como restringir o acesso as suas informações no WhatsApp e Telegram

### WhatsApp

1 Dentro do app, vá em ***“Configurações”***, depois vá em ***“Conta”*** e por último clique em ***“Privacidade”***

2 Restrinja o acesso aos dados apenas para seus contatos



### Telegram

1 Dentro do app, vá em ***“Configurações”***, depois vá em ***“Privacidade e Segurança”***

2 *Dentro da guia* ***“Privacidade”,*** restrinja o acesso aos dados apenas para seus contatos


# Configurações de Segurança/Privacidade

TecBan

## Aplicativos

# Ative o Touch ID ou Face ID para acessar seus aplicativos

## Passo a passo nos aplicativos: Outlook, WhatsApp, Telegram e LinkedIn

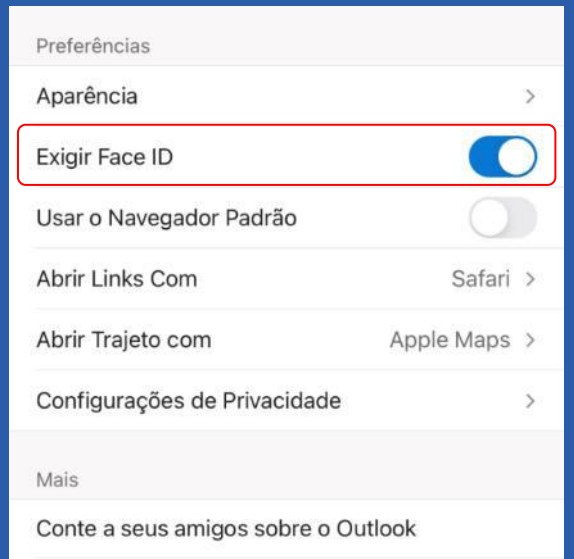
TecBan
cross-security@tecban.com.br

É importante configurar este recurso, pois em caso de perda, furto ou roubo do seu dispositivo (com tela bloqueada), não será possível abrir os aplicativos e acessar suas informações.

**Atenção: Caso os criminosos tenham acesso a sua senha de desbloqueio do dispositivo, este recurso poderá ser desativado. Proteja sua senha!**

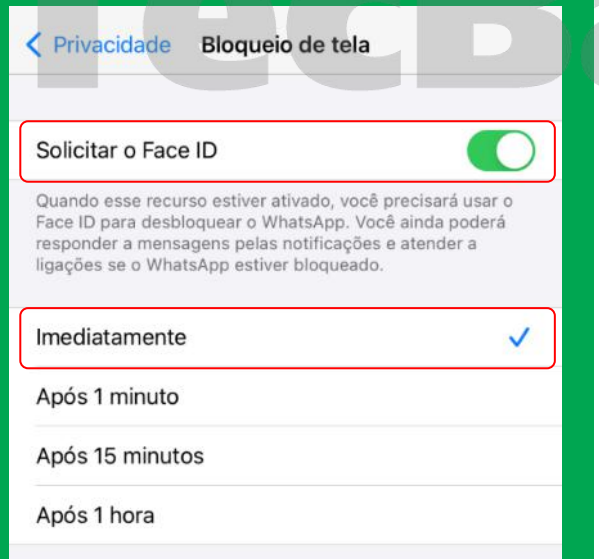
### Outlook

1. Dentro do app, vá em ***"Configurações"***
2. Ative a opção ***"Exigir Face/Touch ID"***



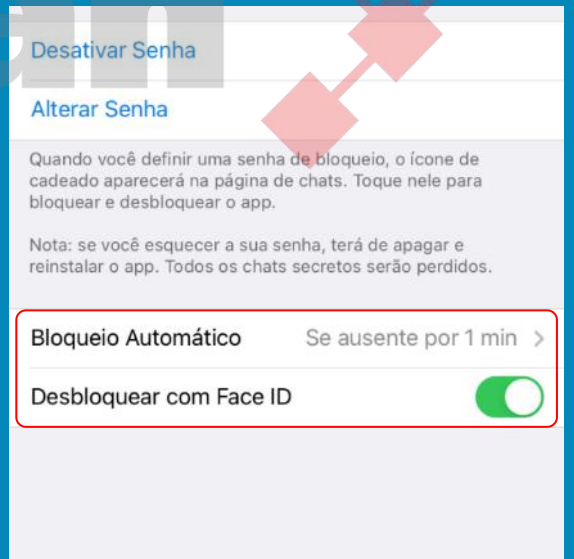

### WhatsApp

1. Dentro do app, vá em ***"Configurações"***
2. Vá em ***"Conta"***, depois em ***"Privacidade"*** e por último em ***"Bloqueio de tela"***
3. Ative a opção ***"Solicitar o Face/Touch ID"*** Configure para solicitar ***"imediatamente"***



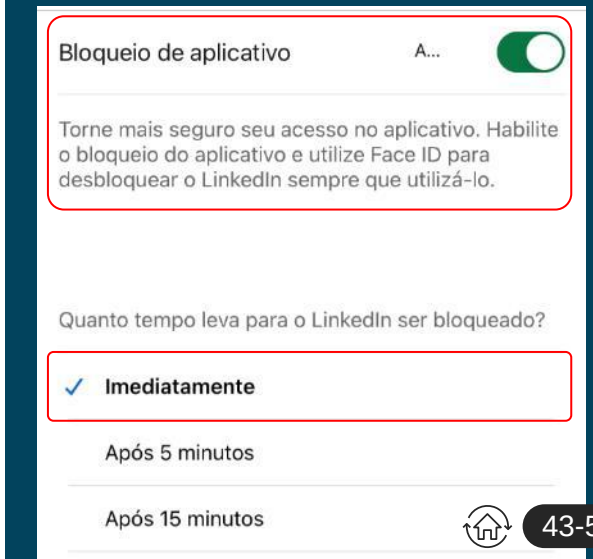

### Telegram

1. Dentro do app, vá em ***"Configurações"***
2. Vá em ***"Privacidade e Segurança"*** e depois em ***"Senha & Face/Touch ID"***
3. Ative a opção ***"Desbloquear com Face/Touch ID"*** Configure o bloqueio automático ***"Se ausente por 1 min"***




### LinkedIn

1. Dentro do app, vá em ***"Configurações"***
2. Vá em ***"Acesso e Segurança"*** e depois em ***"Bloqueio do Aplicativo"***
3. Ative a opção ***"Bloqueio de aplicativo"*** Configure o bloqueio automático para ***"Imediatamente"***



# Outlook/Hotmail: Ative o duplo fator de autenticação para iniciar sua sessão/login

TecBan
cross-security@tecban.com.br

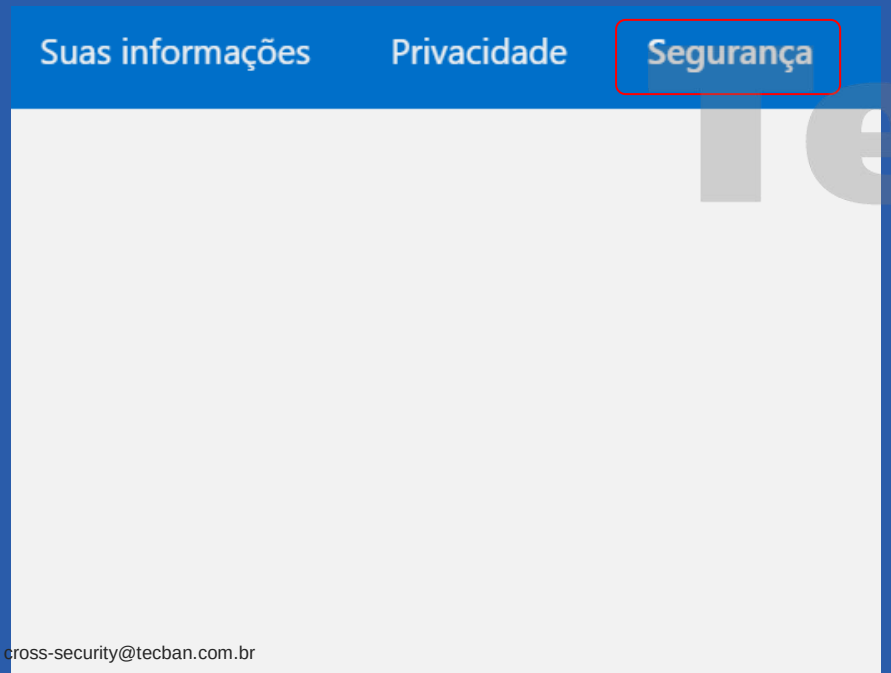
Ative o duplo fator de autenticação para iniciar sessão/login nos seus aplicativos/sistemas. Este recurso é muito importante para evitar acesos indevidos nas suas contas.

**Além da digitação da senha pessoal, será necessário informar um código de verificação de segurança enviado por token.**

Outlook

**1**

Acesse sua conta ***outlook.com*** via browser. Quando estiver na caixa de entrada do e-mail, no canto superior direito clique na ***sua foto (perfil)*** e escolha a opção ***"Minha Conta"***. No painel superior clique em ***"Segurança"***.

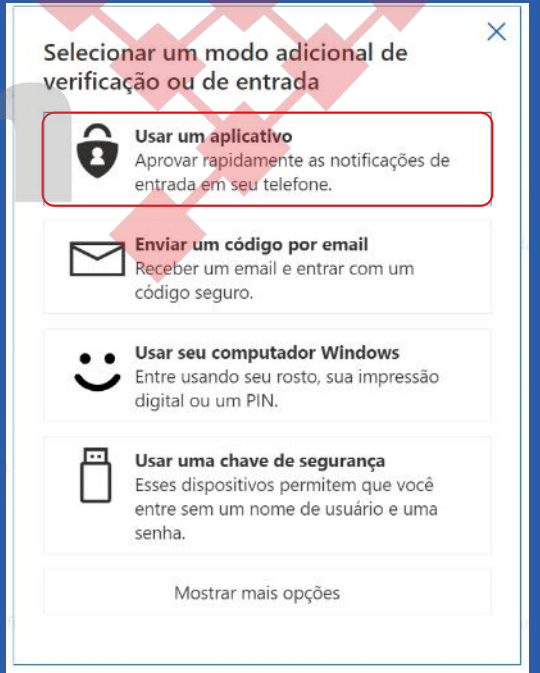



**2**

Clique em ***"Opções de segurança avançadas"***

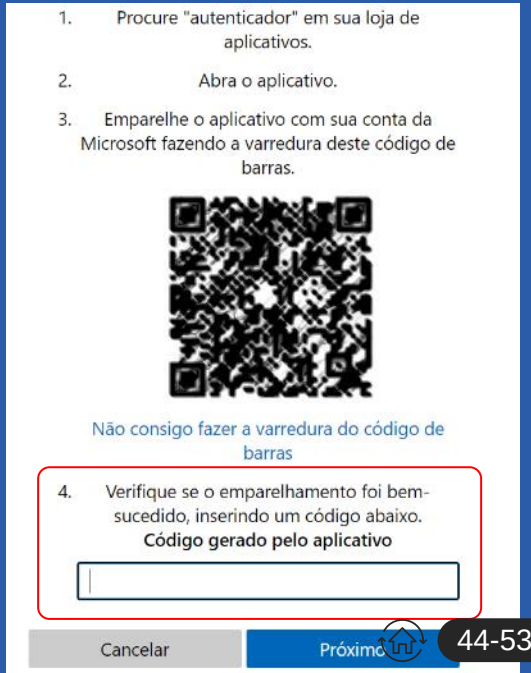

**3**

Clique em ***"adicionar um novo modo de entrada ou verificação"***. No menu aberto selecione ***"Usar um aplicativo"***




**4**

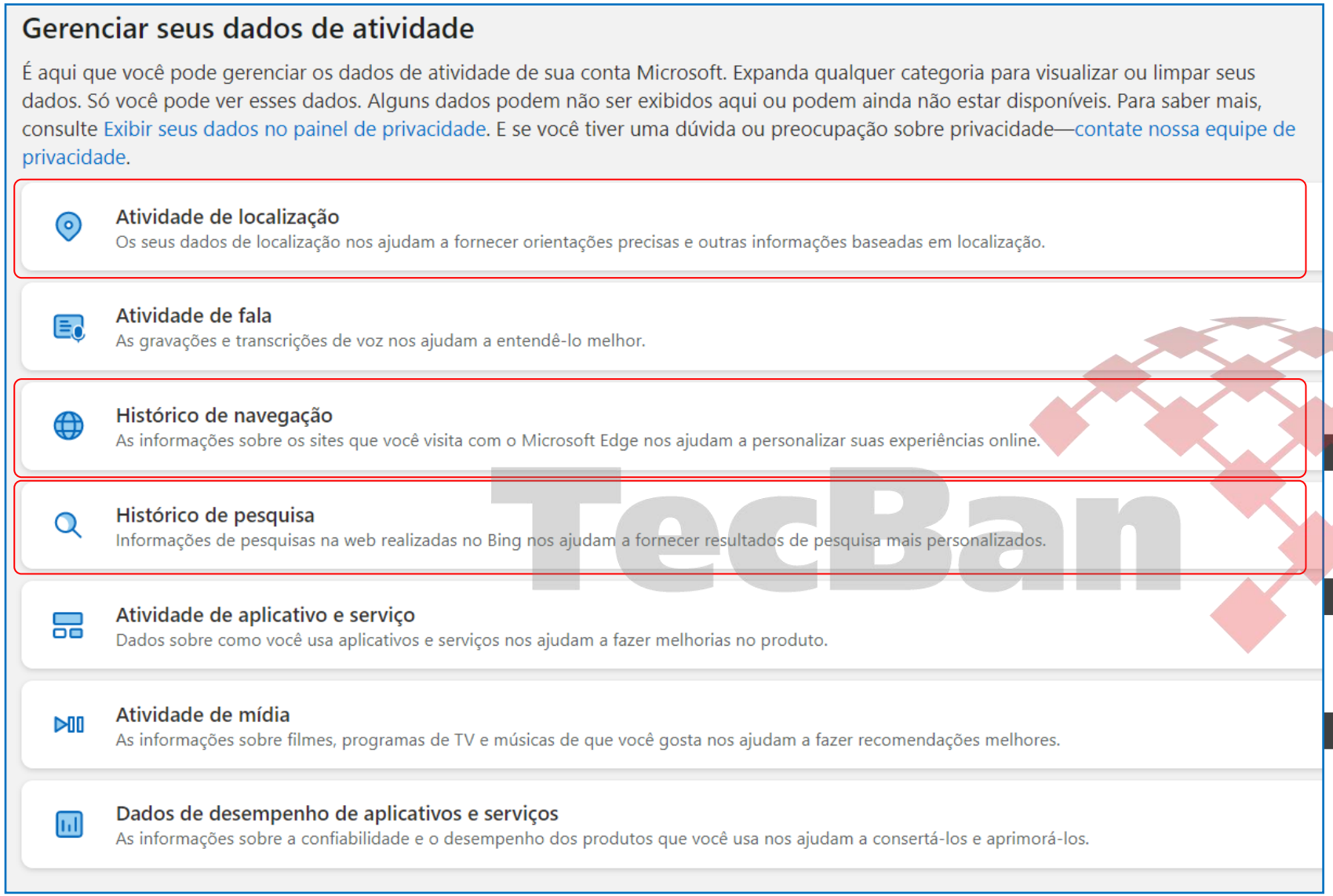
Baixe o aplicativo ***"Microsoft Authenticator"*** no seu celular, escaneie o QRCode e confirme o código gerado



# Outlook/Microsoft: Configurações de Privacidade

## Utilize a versão web para acessar todas as opções de segurança/privacidade

TecBan
cross-security@tecban.com.br




O Outlook e as contas Microsoft armazenam diversas informações referente a sua atividade realizadas nos seus dispositivos e aplicativos. **Revise periodicamente as informações armazenadas e, se necessário, limpe o histórico.**

Para acessar as informações de privacidade do Outlook/Microsoft:

1. Acesse sua conta outlook.com via browser. Quando estiver na caixa de entrada do e-mail, no canto superior direito clique na sua foto (perfil) e escolha a opção *"Minha Conta"*.
2. No menu de seleção superior, selecione *"Privacidade"*
3. Revise suas configurações de privacidade, **principalmente referente ao histórico de localização, navegação e pesquisa. Caso necessário limpe o histórico.**

# Gmail & Contas do Google: Ative o duplo fator de autenticação para iniciar sua sessão/login

TecBan
cross-security@tecban.com.br

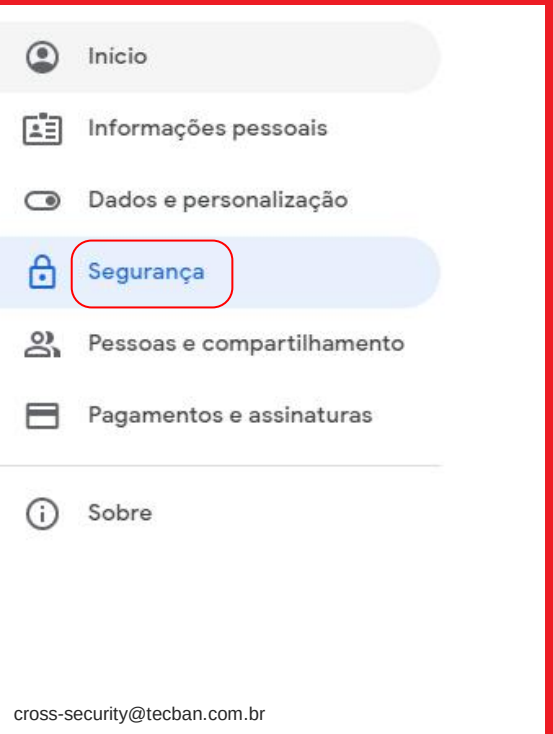
Ative o duplo fator de autenticação para iniciar sessão/login nos seus aplicativos/sistemas. Este recurso é muito importante para evitar acesos indevidos nas suas contas.

**Além da digitação da senha pessoal, será necessário informar um código de verificação de segurança, enviado por token. NUNCA cadastre seu número de telefone para acesso a conta de e-mail. Prefira criar contas de e-mails em provedores que oferecem essa opção (não obrigar cadastrar do telefone como duplo fator).**

Gmail

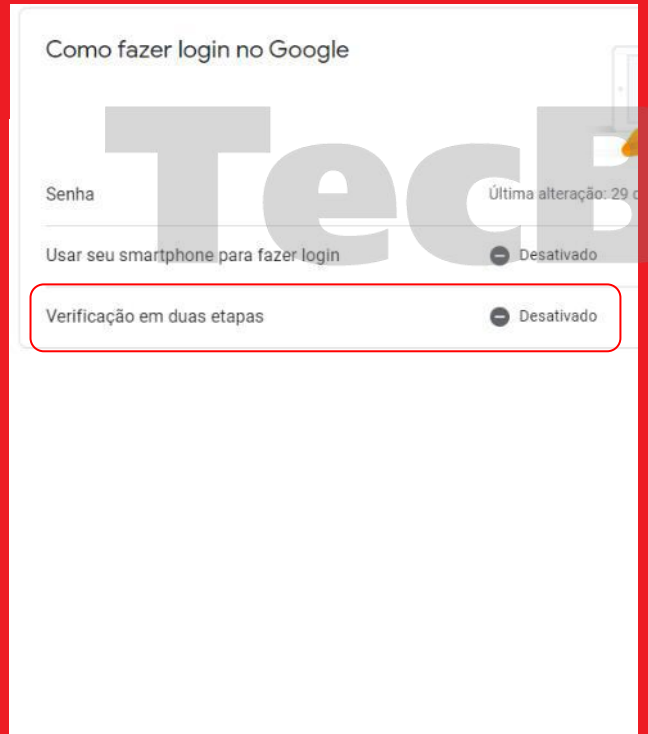
**1**

Acesse sua conta ***myaccount.google.com*** via browser. No painel lateral esquerdo, selecione ***"Segurança".***



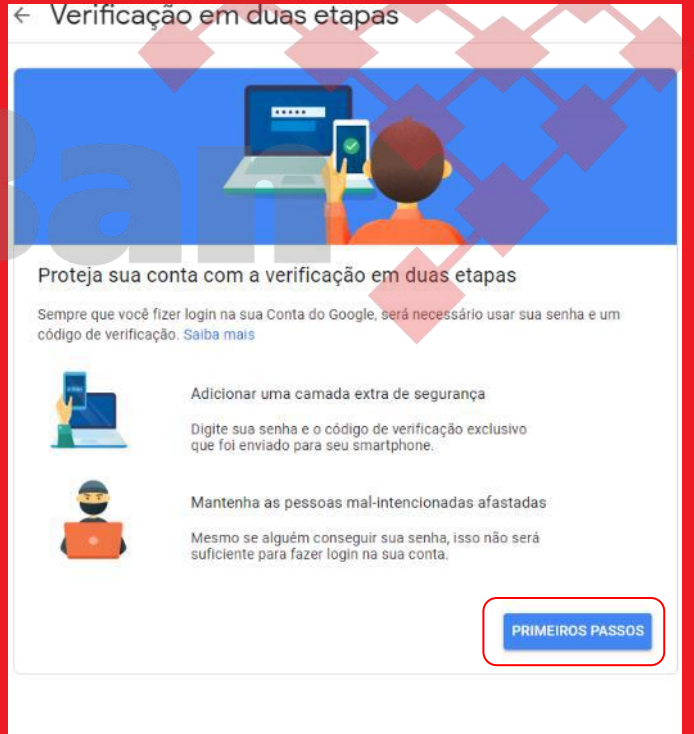

**2**

Clique em ***"Verificação em duas etapas"***



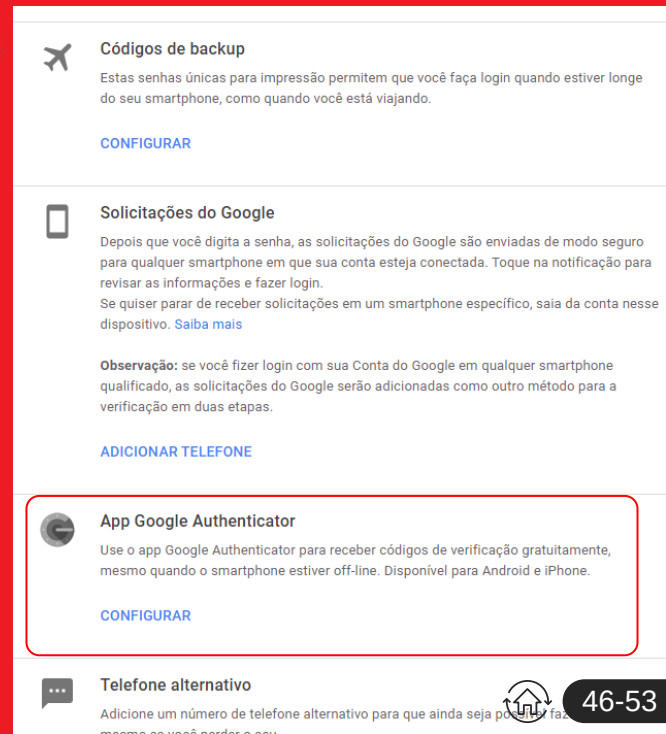

**3**

Siga as instruções. Será solicitado um número de telefone para envio dos códigos de verificação via SMS




**4**

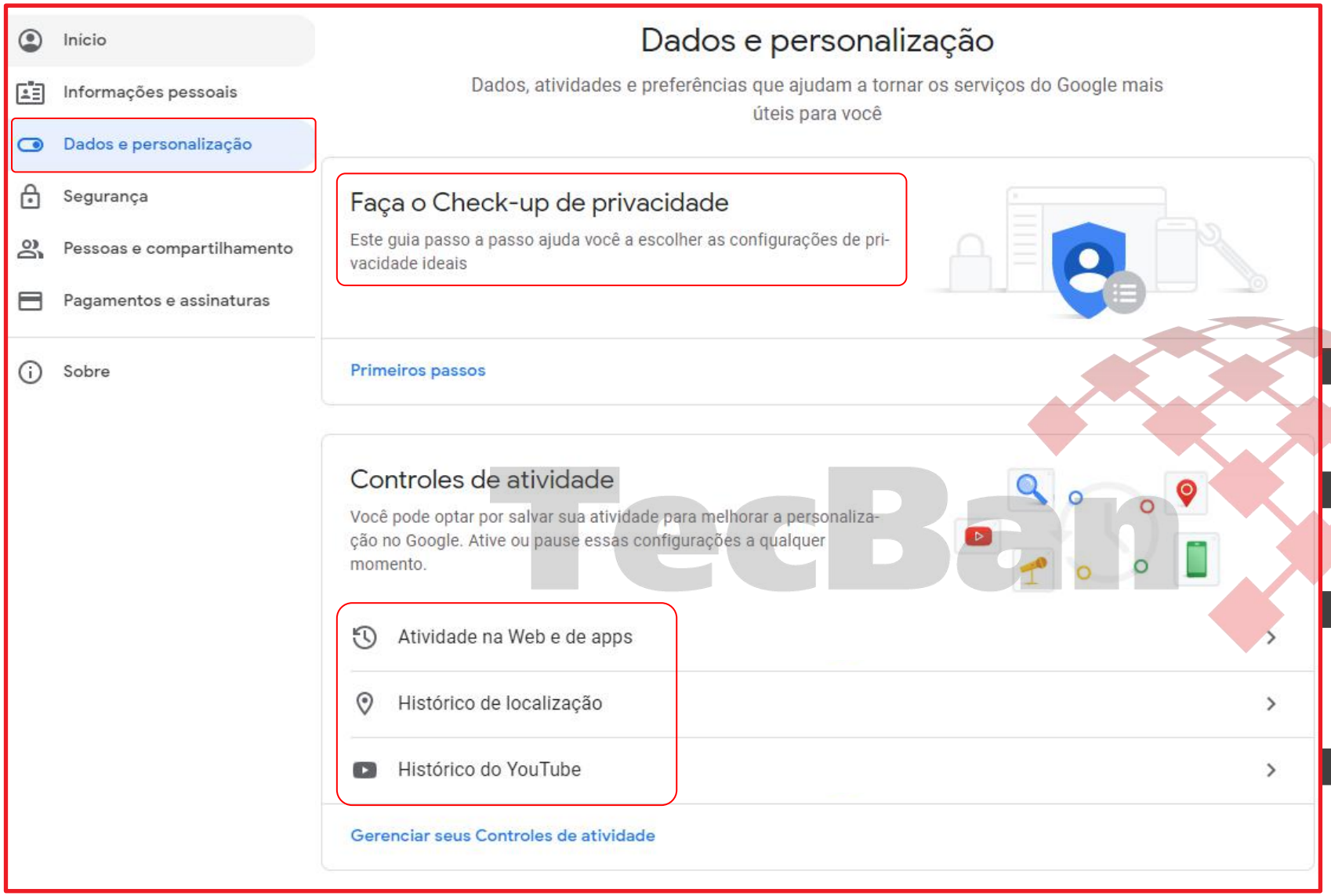
Após a configuração, é possível alterar o modo de envio do código de segurança, por exemplo utilizar o app Google Authenticator



# Gmail & Contas do Google: Configurações de Privacidade

## Utilize a versão web para configurar as opções de segurança/privacidade

TecBan
cross-security@tecban.com.br




O Gmail e as contas Google armazenam diversas informações referente a sua atividade nos dispositivos e aplicativos. **Revise periodicamente as informações armazenadas e, se necessário, limpe o histórico.**

Para acessar as informações de privacidade do Gmail/Google:

1. Acesse sua conta myaccount.google.com via browser
2. No menu de seleção lateral, selecione *"Dados e personalização"*
3. Clique em *"Faça o Check-up de privacidade"*
4. **Revise suas configurações de privacidade, principalmente referente ao histórico de localização, navegação e pesquisa. Caso necessário limpe o histórico.**

# Facebook e Instagram: Ative o duplo fator de autenticação para iniciar sua sessão/login

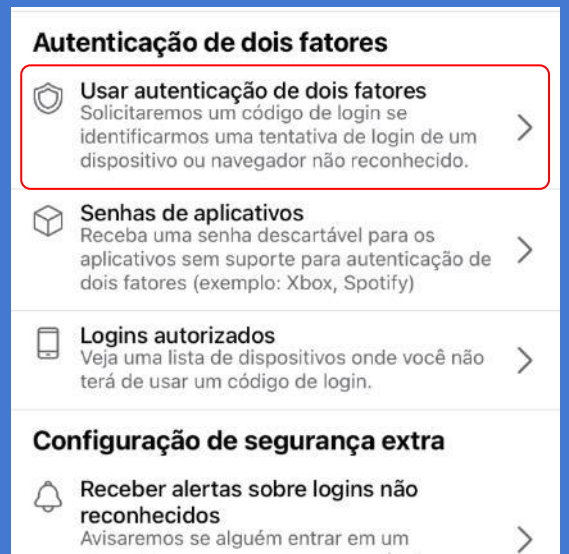
TecBan
cross-security@tecban.com.br

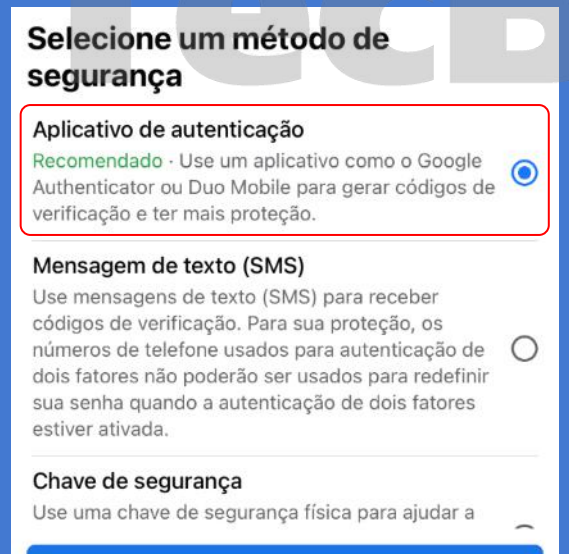
Ative o duplo fator de autenticação para iniciar sessão/login nos seus aplicativos/sistemas. Este recurso é muito importante para evitar acesos indevidos nas suas contas.

**Além da digitação da senha pessoal, será necessário informar um código de verificação de segurança, enviado por SMS ou token.**

## Facebook

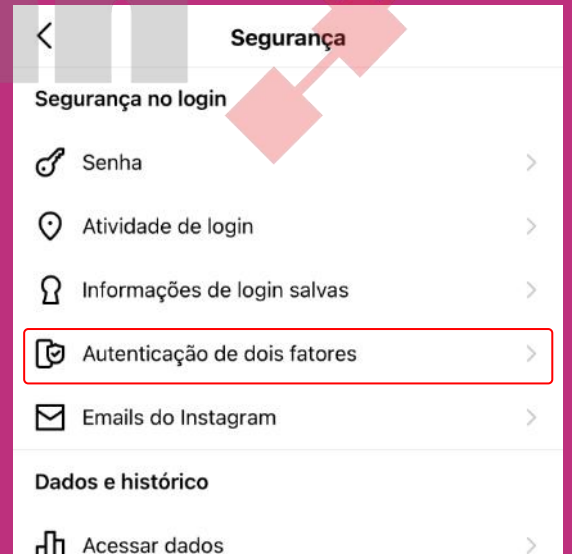
1. Dentro do app, vá em ***"Segurança e Login"*** e depois em ***"Usar autenticação de dois fatores"***
2. Caso deseje utilizar um aplicativo para gerar o token (ex: Google Authenticator), selecione a opção ***"Aplicativo de Autenticação"*** e siga as instruções
3. Caso deseje receber o código de verificação por SMS, selecione a opção ***"Mensagem de Texto (SMS)"***. Informe o número de uma pessoa de confiança.




## Instagram

1. Dentro do app, vá em ***"Configurações"***, vá em ***"Segurança"*** e depois ***"Autenticação de dois fatores"***
2. Caso deseje utilizar um aplicativo para gerar o token (ex: Google Authenticator), selecione a opção ***"Aplicativo de Autenticação"*** e siga as instruções
3. Caso deseje receber o código de verificação por SMS, selecione a opção ***"SMS"***. Informe o número de uma pessoa de confiança.

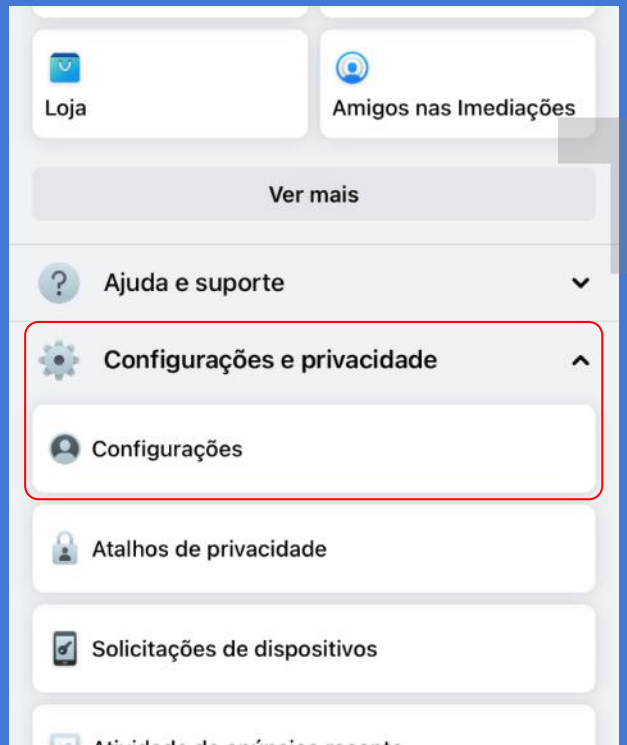



# Facebook: Revise os registros das suas “atividades fora do Facebook”

TecBan
cross-security@tecban.com.br

O Facebook recebe diversas informações de outros aplicativos que você utiliza, principalmente se você tiver vinculado sua conta do Facebook. É difícil saber quais informações/dados o Facebook armazena, mas podemos verificar no painel de "atividades fora do Facebook" quais aplicativos enviaram dados para a rede social**. Você pode desativar totalmente este recurso, ou seja, o Facebook não irá mais receber dados dos seus aplicativos, ou você pode limitar certos aplicativos. Veja o passa a passo:**

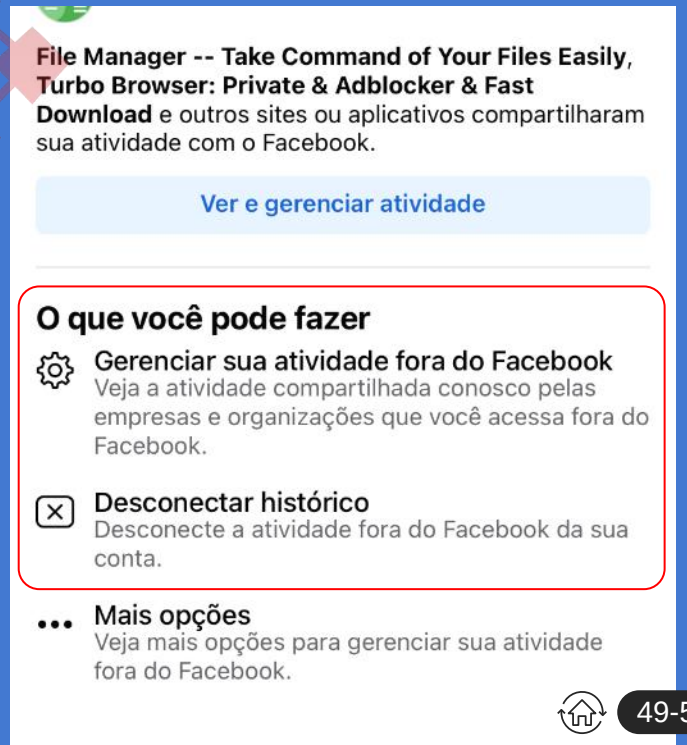
**1** Dentro do app, vá em ***“Configurações e privacidade”*** e depois em ***“Configurações”***




**2** Na parte de ***“Permissões”***, clique em ***“Atividade fora do Facebook”***


**3** Caso queira editar/limitar certos aplicativos clique em ***“Gerenciar sua atividade fora do Facebook”***

Caso queira desativar totalmente este recurso, clique em ***“Desconectar histórico”***



# Facebook: Configurações de Privacidade

## Utilize a versão web para configurar as opções de segurança/privacidade

TecBan
cross-security@tecban.com.br


O Facebook oferece diversas opções para customizar a segurança/privacidade das suas informações e perfil. **Revise as configurações e altere conforme a sua necessidade**

Para acessar as configurações de privacidade:

1. Acesse sua conta facebook.com.br via browser
2. No canto superior direito, clique em *"Configurações e privacidade"* e depois em *"Verificação de privacidade"*
3. **Revise as configurações e altere conforme a sua necessidade**

# LinkedIn e Twitter: Ative o duplo fator de autenticação para iniciar sua sessão/login

TecBan
cross-security@tecban.com.br

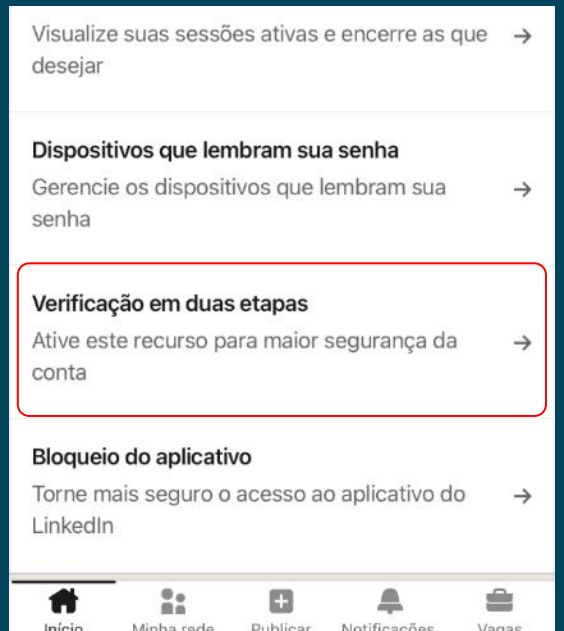
Ative o duplo fator de autenticação para iniciar sessão/login nos seus aplicativos/sistemas. Este recurso é muito importante para evitar acesos indevidos nas suas contas.

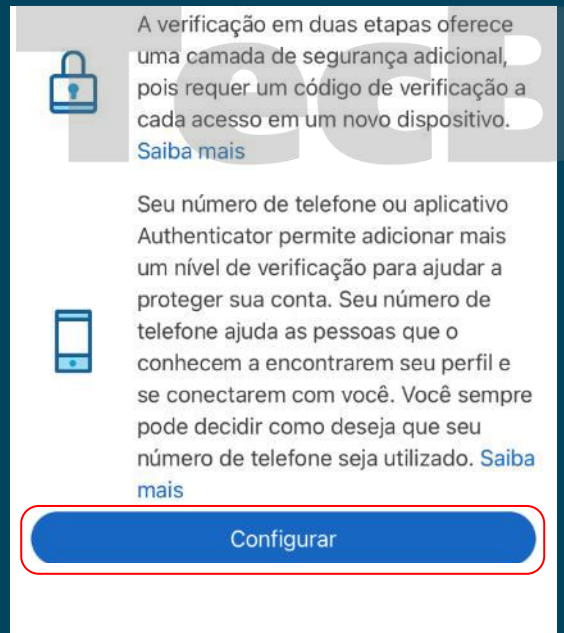
**Além da digitação da senha pessoal, será necessário informar um código de verificação de segurança, enviado por SMS ou token.**

## LinkedIn

1 Dentro do app, vá em ***"Configurações"*** *, clique em* ***"Acesso e Segurança"*** *e depois* ***"Verificação em duas etapas"***

2 Clique em ***"Configurar"***. Caso deseje receber o código de verificação por SMS, selecione a opção ***"Número de telefone (SMS)"***. Se desejar utilizar um aplicativo (ex: Google Authenticator), selecione ***"Aplicativo Authenticator"***



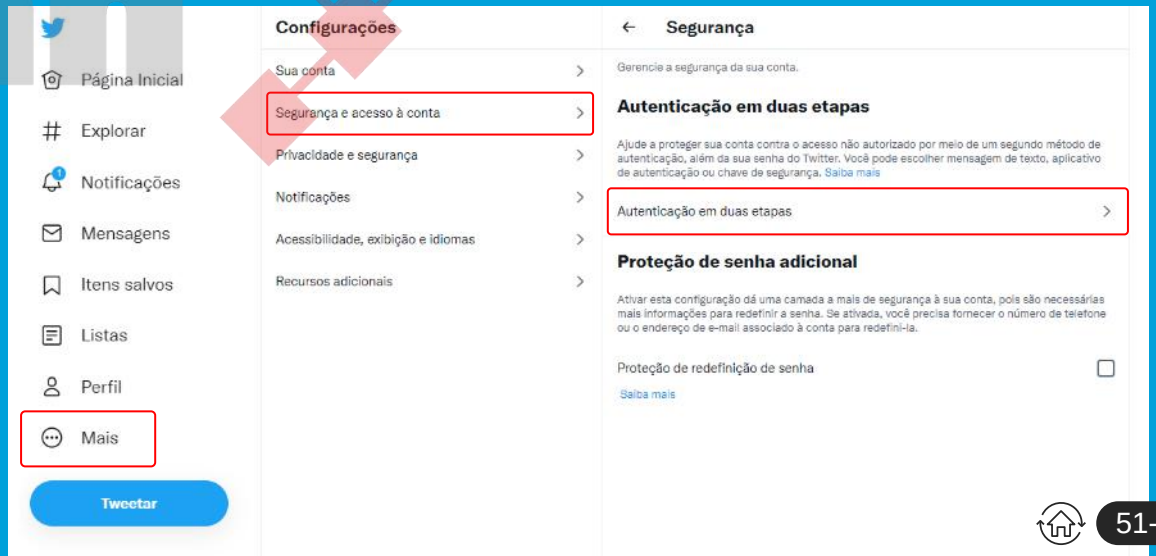




## Twitter

1 Acesse o Twitter via browser, no menu lateral clique em ***"Mais"***, clique em ***"Configurações e privacidade"***, *vá em* ***"Segurança e acesso à conta"*** e depois ***"Segurança"***

2 Selecione **"Autenticação em duas etapas"**

3 Caso deseje receber o código de verificação por SMS, selecione a opção ***"Mensagem de Texto"***. Se desejar utilizar um aplicativo (ex: Google Authenticator), selecione ***"Aplicativo de autenticação"***



# LinkedIn: Configurações de Privacidade

## Utilize a versão web para acessar todas as opções de segurança/privacidade

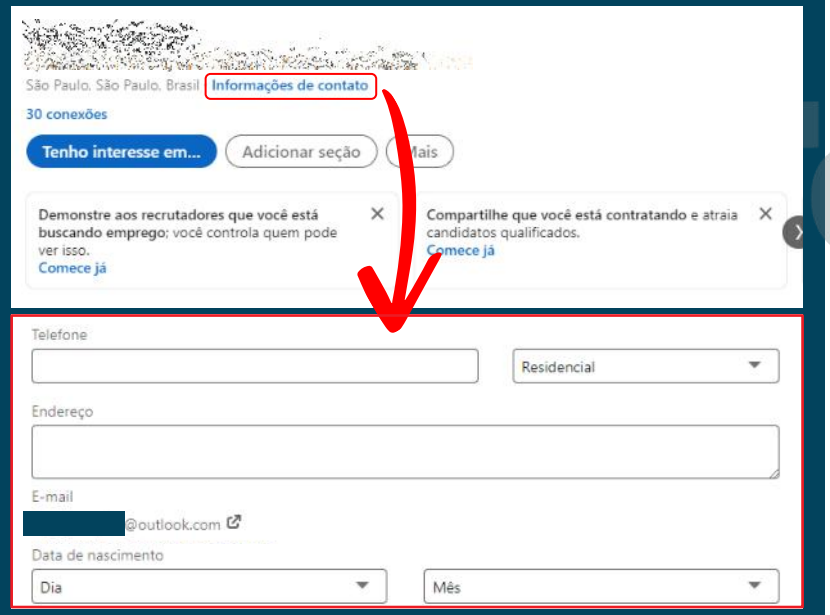
TecBan
cross-security@tecban.com.br

No LinkedIn é possível adicionar diversas informações pessoais no seu perfil, como por exemplo: telefone, endereço, e-mail e data de nascimento. **Essas informações ficam disponíveis na página principal para todos acessarem.** Nunca informe seu telefone, endereço ou data de nascimento neste formulário. Informe apenas um e-mail, se possível diferente do usado para logar, para caso precisem entrar em contato com você.

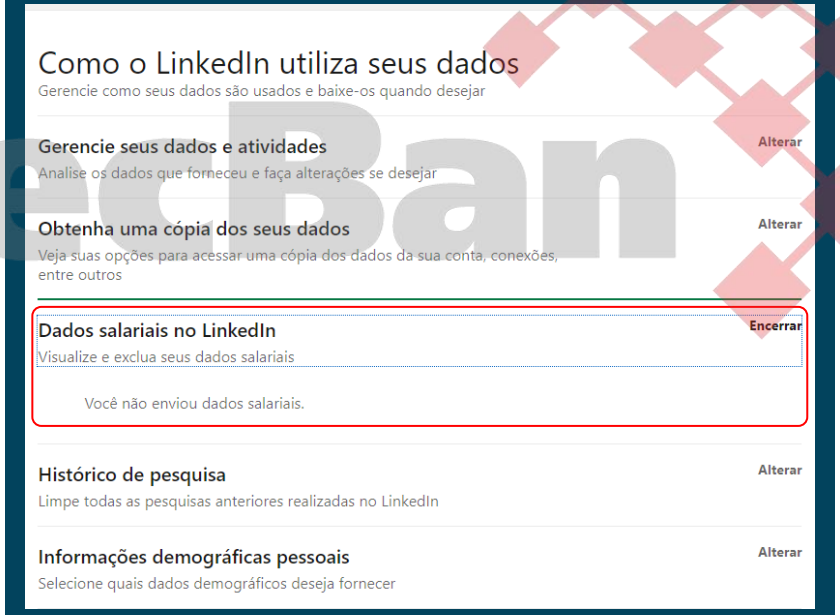
NUNCA informe deus dados salariais no LinkedIn. Confirme se possui alguma informação cadastrada indo em: ***"Configurações e Privacidade"***, no menu lateral, vá em ***"Privacidade dos dados"*** e depois ***"Dados salariais no LinkedIn"***

**O LinkedIn oferece diversas opções para customizar a visibilidade das suas informações e perfil.** Por exemplo, é possível criar um perfil público, limitar as informações que pessoas não conectadas a você pode visualizar, **limitar quem pode visualizar seu endereço de e-mail**, desabilitar marcações, etc. Para acessar vá em ***"Configurações e Privacidade"*** e no menu lateral, clique em "**Visibilidade**".

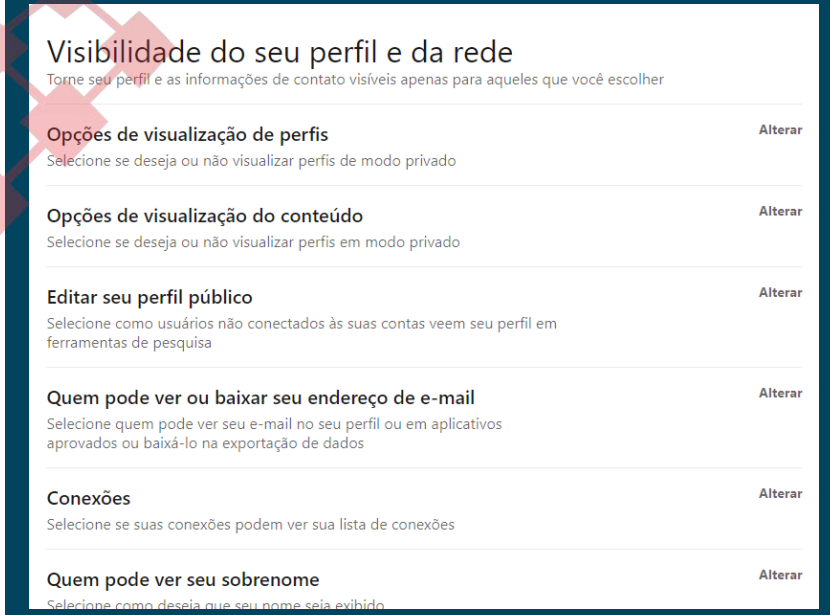
### Proteja suas **informações pessoais**




### Não informe seus **salários!**




### Revise as **configurações de visibilidade** e altere conforme a sua necessidade




# Manual de Melhores Práticas de Segurança para Proteção de Dispositivos Móveis (Smartphones/Tablets/Notebooks)

**Grupo TecBan** | Superintendência de Segurança | Vanderlei Reis

Documento elaborado pelas **equipes de CyberSecurity** (**Blue** Team e **Red** Team)

**Classificação deste documento: PÚBLICO** **TLP: WHITE** **Versão05_MB20211201**