



Telegram

SEGURANÇA

NAS REDES SOCIAIS



CEARÁ
GOVERNO DO ESTADO
SECRETARIA DA SEGURANÇA
PÚBLICA E DEFESA SOCIAL

EXPEDIENTE CARTILHA SEGURANÇA NAS REDES SOCIAIS

GOVERNADOR DO ESTADO DO CEARÁ

Camilo Sobreira de Santana

SECRETÁRIO DA SEGURANÇA PÚBLICA E DEFESA SOCIAL (SSPDS/CE)

Sandro Luciano Caron de Moraes

SUPERINTENDENTE DE PESQUISA E ESTRATÉGIA DE SEGURANÇA PÚBLICA (Supesp/CE)

José Helano Matos Nogueira

DIRETOR DE ESTRATÉGIA EM SEGURANÇA PÚBLICA (Diesp/Supesp)

Anderson Duarte Barboza

DIRETORA DE PESQUISA E AVALIAÇÃO DE POLÍTICAS DE SEGURANÇA PÚBLICA (Dipas/Supesp)

Manuela Chaves Loureiro Cândido

GERENTE DE ESTATÍSTICA E GEOPROCESSAMENTO (Geesp/Supesp)

Franklin de Sousa Torres

AUTOR

José Helano Matos Nogueira

DESIGNER

Juliana Mendes Teixeira de Lima

REVISÃO

Ascom/Supesp



TELEGRAM (fonte: <https://core.telegram.org/techfaq>)

○ **Telegram** é um aplicativo de mensagens criptografadas e que podem se autodestruir. O aplicativo salva os dados das conversas na nuvem. Assim é possível acessar as conversas em praticamente qualquer dispositivo com *login* ativo, seja um computador, um tablet, um ou mais celulares. Você pode usar o **Telegram** em todos os seus dispositivos ao mesmo tempo – suas mensagens serão sincronizadas em todos os dispositivos sem precisar ter o celular por perto. O aplicativo possui compatibilidade com chamadas de voz com criptografia de ponta a ponta.

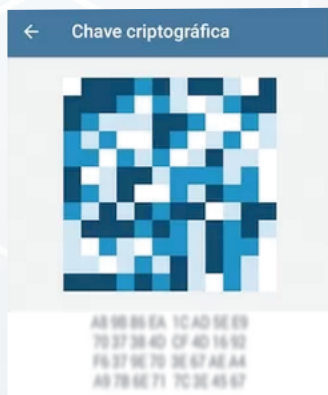
DICAS GERAIS

■ ○ **Telegram** oferece suporte a duas camadas de criptografia segura. A criptografia cliente-servidor, que é usada em chats na nuvem (chats privados e em grupo). Os chats secretos usam uma camada adicional de criptografia cliente-cliente. Todos os dados, independentemente do tipo, são criptografados da mesma maneira seja texto, mídia ou arquivos.

■ Se você tiver motivos para se preocupar com sua segurança pessoal é recomendado usar somente “**Chats Secretos**” em aplicativos oficiais.

■ ○ **Telegram** utiliza criptografia de ponta a ponta apenas nos “**Chats Secretos**”. Ao armazenar os dados das conversas dos chats normais na nuvem, bem como oferecê-los em tempo real em múltiplos dispositivos, se os usuários não utilizarem os chats secretos (**encriptados de ponta a ponta**) e/ou a verificação em duas etapas, estão sujeitos a ter suas conversas vazadas com maior facilidade.

CRIPTOGRAFIA



1 Todas as mensagens do **Telegram** são sempre criptografadas com segurança.

2 Mensagens em “**Chats Secretos**” usam criptografia cliente-cliente (ponta a ponta), enquanto os chats na nuvem usam criptografia cliente-servidor/servidor-cliente e são armazenadas criptografadas na “**Nuvem do Telegram.**”

Isso permite que as mensagens na nuvem sejam tanto seguras quanto imediatamente acessíveis a partir de qualquer um de seus dispositivos — mesmo se você perder completamente o dispositivo.

3 A criptografia de ponta a ponta é usada em bate-papos secretos por telegrama.

■ Quando um chat secreto é criado, a comunicação entre as duas pessoas é feita pela troca de chaves.

■ Ao comparar essa imagem com o chat do outro contato, elas devem ser iguais. Com isso, pode-se ter certeza que a troca de informações é segura e o chat encriptado.

Para ver essa imagem criptográfica, acesse:

1 Entre no “**Chat Seguro**”.

2 Toque no “**Nome do Contato**” para ver as informações.

3 Selecione “**Chave Criptográfica**”.

VERIFICAÇÃO EM DUAS ETAPAS

1 É fortemente recomendado que você ative a verificação em duas etapas e configure uma **senha forte** para bloquear seu aplicativo. Fazer **login** com um **código SMS é um padrão**, mas se você estiver procurando mais segurança ou tiver motivos para duvidar recomenda-se proteger seus chats na **nuvem com uma senha adicional**.

2 Você pode fazer isso em “**Configurações > Privacidade e Segurança > Verificação em Duas Etapas.**” Uma vez habilitada, você precisará do código SMS e também da sua senha para entrar. Você também pode definir um e-mail para recuperação, que ajudará obter acesso novamente caso esqueça sua senha. Se fizer isso, lembre-se de que é importante que o e-mail de recuperação também seja protegido com uma senha forte e “Verificação em Duas Etapas”, quando possível.

BATE-PAPO NA NUVEM

■ **Telegram** é um serviço de nuvem. Mensagens, fotos, vídeos e documentos de seus bate-papos são armazenados na nuvem em servidores para que você possa acessar seus dados a partir de qualquer dispositivo a qualquer momento, sem precisar depender de *backups* de terceiros.

■ Não criptografar todos os chats permite que eles sejam salvos na nuvem e armazenados nos servidores para serem acessados em qualquer outro dispositivo, configurado com a conta do usuário, restaurando todo o conteúdo.

■ Todos os dados são armazenados criptografados e as chaves de criptografia em cada caso são armazenadas em vários outros “**datacenters**” em jurisdições diferentes. Dessa maneira, engenheiros locais ou intrusos físicos não podem obter acesso aos dados do usuário.

BATE-PAPO PÚBLICO

- O **Telegram** também suporta canais públicos e grupos públicos. Todos os chats públicos são chats na nuvem.
- Como tudo, os dados que você publica nas comunidades públicas são criptografados, tanto no armazenamento quanto no transporte - mas tudo o que você publica em público estará acessível a todos.

CHATS SECRETOS

- Os chats secretos são destinados a pessoas que querem mais sigilo do que a pessoa comum.
- Todas as mensagens em chats secretos usam criptografia de ponta a ponta. Isso significa que apenas você e o destinatário podem ler essas mensagens — ninguém mais pode decifrá-las, incluindo o **Telegram**. Quando um chat secreto é criado, os dispositivos participantes trocam chaves de criptografia. Depois que a conexão segura de ponta a ponta for estabelecida é gerada uma imagem que visualiza a chave de criptografia do seu chat. Você pode então comparar esta imagem com a que seu amigo tem — se as duas imagens forem iguais, o chat secreto é seguro.
- Quando você apagar as mensagens do seu lado da conversa, o aplicativo do outro lado do chat secreto será solicitado a apagá-las também.
- Todos os chats secretos são específicos do dispositivo e não fazem parte da nuvem do **Telegram**. Isso significa que você só pode acessar mensagens em um chat secreto a partir do dispositivo de origem.

ATIVACÃO DO CHAT SECRETO

■ **No iOS:** inicie uma nova mensagem (toque no ícone no canto superior direito em “Chats”) e então em “Novo Chat Secreto”.

■ **No Android:** deslize para a direita para abrir o menu e então em “Novo chat secreto”.

Lembre-se de que os chats secretos são específicos do dispositivo. Se você iniciar um chat secreto com um amigo em um de seus dispositivos, este chat estará disponível somente no dispositivo em que foi iniciado. Você pode criar vários chats secretos com o mesmo contato se desejar.

MENSAGENS AUTODESTRUTIVAS

■ Você pode configurar suas mensagens, fotos, vídeos e arquivos para autodestruição, em um determinado período depois, que eles foram lidos ou abertos pelo destinatário. Depois de definir o tempo e enviar a mensagem, o texto ou mídia desaparecerá para ambas as pessoas dentro da conversa.

■ O “**Timer de Autodestruição**” está disponível para todas as mensagens em “Chats Secretos” e para mídias em chats privados. As opções do **timer** variam de alguns segundos até uma semana.

■ Para definir o **timer**, basta tocar no “**Ícone de Relógio**” (na caixa de texto no iOS ou na **barra superior no Android**) e configurar o limite de tempo desejado. O relógio começa a contar no momento em que a mensagem é exibida na tela do destinatário (**recebe dois ticks verdes**).

Assim que o tempo acabar, a mensagem desaparece de ambos os dispositivos. O **Telegram** pode enviar uma notificação se uma captura de tela for realizada.

■ Note que o **timer** em “Chats Secretos” só se aplica a mensagens que foram enviadas após o temporizador ser definido – ele não tem efeito nas mensagens anteriores.

VISIBILIDADE

- Você pode escolher quem vê essas informações nas configurações de **“Privacidade e Segurança do Telegram.”**
- Lembre-se de que você não verá o horário do **“Visto por Último”** de pessoas com quem você não compartilha o seu.

ALERTAS DE CAPTURA DE TELA

- Os chats secretos podem alertar quando o contato faz uma captura de tela da conversa ou da imagem que enviou, mesmo as que se autodestroem. Ou seja, você saberá sempre que alguém tirou um printscreen de algo que recebeu via chat secreto.
- O **Telegram** tenta fazer com que as notificações funcionem em todos os sistemas, mas alerta para que os usuários compartilhem informações sensíveis apenas com contatos de confiança para não ocorrer vazamentos.

NÚMERO DE TELEFONE

- Você pode enviar mensagens em chats privados e em grupos sem tornar seu número de telefone visível. Por padrão, seu número é visível apenas para as pessoas que você adicionou como contatos na sua agenda telefônica.
- Você pode modificar isso ainda mais em **“Configurações > Privacidade e Segurança > Número de Telefone.”**
- Observe que as pessoas sempre irão ver seu número se já souberem e tiverem salvo na agenda delas.

CELULAR ROUBADO

■ O número de telefone é a única maneira de identificar um usuário. O Telegram não coleta informações adicionais sobre você, portanto, quem tiver o número tem a conta.

SE TIVER ACESSO AO TELEGRAM POR OUTRO DISPOSITIVO

1 Vá para “**Configurações do Telegram > Privacidade e Segurança**” e ative a “**Verificação em Duas Etapas.**” Dessa forma, o número de telefone, por si só, não será suficiente para fazer login na sua conta.

2 Vá para “**Configurações > Privacidade e Segurança > Sessões Ativas**” e encerre sua sessão no dispositivo antigo. Quem tiver seu telefone não poderá fazer login novamente, pois não sabe sua senha.

3 Entre em contato com o seu **fornecedor de serviços telefônicos**, para que eles **bloqueiem o seu chip SIM antigo** e emitam um novo com o seu número.

4 Se você decidir mudar para um novo número de telefone, não se esqueça de ir em “**Configurações**”, tocar no “**seu número de telefone**” e alterar o número do seu Telegram para o **novo**.

REMOVENDO DADOS CONFIDENCIAIS

1 Ladrões comuns geralmente jogam fora o **chip SIM** imediatamente (**o telefone é mais difícil de localizar assim**) Mas, se você tiver motivos para se preocupar com os dados no dispositivo e não conseguir sair por outro dispositivo é melhor que você **formate o dispositivo remotamente**.

2 Você pode apagar sua conta se você estiver logado em pelo menos um dos seus outros dispositivos (**móvel ou desktop**). Observe que as contas inativas do **Telegram** se autodestroem automaticamente após um período de tempo (**seis meses sendo a configuração padrão**).

- Se você quiser apagar sua conta, faça isso na página de desativação. A exclusão da sua conta remove permanentemente todas as suas mensagens e contatos. Todos os grupos e canais que você criou ficarão órfãos, sem um criador, mas os administradores mantêm os direitos deles.

- Esta ação deve ser confirmada através da sua conta do **Telegram** e não pode ser desfeita.

- É recomendado usar um navegador *desktop* para esse processo.

- Observe que você receberá o código via **Telegram**, e não por SMS.

SUPORTE DO TELEGRAM

■ Se você tiver outras dúvidas, entre em contato com o “**Suporte do Telegram**” (no “**Telegram**, vá para **Configurações**” > **Faça uma pergunta**). Note que o suporte é feito por voluntários.

■ Há o **@TelegramBR** o canal oficial de informações em português. Lá você receberá informações sobre novas versões e também dicas.

■ Se você não conseguir fazer login na sua conta, use o formulário em <https://telegram.org/support>

REALIZAÇÃO:



CEARÁ
GOVERNO DO ESTADO
SECRETARIA DA SEGURANÇA
PÚBLICA E DEFESA SOCIAL