

# Quais aplicativos devo usar para documentar?

Última revisão: 31 de janeiro de 2020

Existem muitos aplicativos que os documentadores podem usar para capturar imagens em vídeo, desde o [aplicativo de câmera original](#) do seu telefone até aplicativos de documentação mais especializados, como o [ProofMode](#), o [Tella](#), e o [Eyewitness to Atrocities](#). Alguns aplicativos têm recursos que dependem de conexões online, portanto, lembre-se de que esses recursos podem não estar disponíveis caso haja um bloqueio à internet.

Não podemos dizer qual aplicativo específico é o mais adequado para você, pois isso depende da sua situação, das suas necessidades e dos riscos que enfrenta (confira esta publicação do blog para mais informações sobre [como avaliar quais são os seus riscos e ameaças](#)). Com sua avaliação de risco em mãos, as perguntas de orientação abaixo podem ajudar você a avaliar qual aplicativo de documentação de vídeo pode funcionar melhor para a sua situação.

## Quem fez o aplicativo, e eu confio nessas pessoas?

Você deve sempre levar em consideração quem são os criadores de qualquer aplicativo que você baixa e instala em seu dispositivo, e se você pode ou não confiar neles para não o colocarem em uma situação de risco, intencional ou não.

Algumas questões a serem levadas em consideração:

- O desenvolvedor do aplicativo é confiável? O que as pessoas de sua comunidade e de sua rede mais ampla estão dizendo sobre esses desenvolvedores e suas ferramentas?
- O desenvolvedor do aplicativo está vulnerável? Considere o contexto do desenvolvedor, e a probabilidade de eles serem obrigados a entregar seus dados ou a criar uma backdoor (porta dos fundos) no aplicativo para fornecer acesso às autoridades; saiba também se já fizeram isso no passado. Em que país os dados são armazenados, e quais são as leis relativas às ordens judiciais nessa jurisdição?
- O desenvolvedor do aplicativo mantém o aplicativo atualizado? Ferramentas sem manutenção são suscetíveis a hackers, que exploram vulnerabilidades descobertas. Verifique o site do desenvolvedor ou a página do aplicativo no Google Play para saber a data da “última atualização”.
- O desenvolvedor do aplicativo está estabelecido e parece que ele será capaz de cuidar e fazer a manutenção do aplicativo ao longo do tempo?
- O aplicativo é de código aberto? Os aplicativos que estão abertos para análise são mais propensos a terem seus problemas de segurança resolvidos ou pelo menos identificados. O desenvolvedor está sendo transparente sobre a eficácia e a segurança do aplicativo?

- Que motivações ou incentivos impulsionam o trabalho do desenvolvedor de aplicativos e como isso pode influenciar o seu nível de confiança? Por exemplo, eles são motivados por uma missão? Tem fins lucrativos? São patrocinados por um determinado financiador?
- Embora não seja um indicador direto de confiabilidade, o preço do aplicativo pode ser um fator importante a se considerar. Alguns aplicativos têm um alto custo de assinatura mensal ou têm uma taxa por vídeo.

Confira o guia de autodefesa contra a vigilância da [EFF](#) para obter mais informações sobre como [escolher aplicativos](#).

## De onde o aplicativo pode ser baixado?

Você deve sempre baixar e instalar aplicativos apenas de lojas de aplicativos ou de sites confiáveis. Mesmo que você tenha feito uma pesquisa completa para determinar a confiabilidade de um aplicativo, lojas de aplicativos inseguras podem adulterar seus produtos e fazer com que você baixe um aplicativo impostor e ilegítimo, criado com objetivos nefastos. Por exemplo, no ano passado, a organização de direitos digitais [SMEX](#) emitiu [um alerta](#) sobre vários sites que faziam propaganda de um aplicativo chamado "WhatsApp Plus" (para ser claro, esse não é um produto do WhatsApp!), que poderia salvar e vender dados de usuários, ou possibilitar que telefones que o instalavam fossem hackeados.

Alguns desenvolvedores preocupados com a segurança até fornecem chaves criptográficas que permitem verificar a sua autenticidade. Eles geralmente fornecem uma explicação sobre como verificar essas identificações.

## Onde os dados serão armazenados?

Alguns aplicativos de documentação apenas armazenam os seus dados e a sua documentação localmente em seu dispositivo, enquanto outros enviam e armazenam seus dados em outro lugar. Em muitos casos, essa função é inerente ao design e à finalidade do aplicativo, como no caso do app Eyewitness to Atrocities, que envia uma cópia inalterada de sua documentação para uma instalação de armazenamento Lexis Nexis, de modo que a Eyewitness possa se assegurar da proteção e da integridade do material. Você só pode exportar os seus registros para fora da galeria criptografada do aplicativo Eyewitness *depois que* eles tiverem sido enviados para proteção.

Cabe a você determinar se é necessário que a sua documentação permaneça em seu dispositivo apenas, se é preciso que ela seja enviada e armazenada em um local remoto que você controla (como é uma opção com o [Tella](#)), ou se você precisa enviá-la para uma organização ou plataforma externa à qual você concede acesso e direito de uso de sua documentação. Tenha em mente que, durante um bloqueio da internet, você não poderá transmitir a sua documentação pela internet de modo imediato, então precisará de um aplicativo que permita armazenar (e, idealmente, fazer backup) a sua documentação localmente pelo menos de modo provisório (Confira [Como fazer backup da mídia do telefone sem internet ou computador](#)).

Se seus dados forem enviados para um local remoto, saiba em quais países os dados ficarão armazenados. Quão vulneráveis estão os dados nesses países, quais são as chances de serem expostos, seja por ordens judiciais ou outros meios? Quais riscos você corre ao ter seus dados lá guardados expostos?

## O aplicativo criptografa a documentação que produz?

Alguns aplicativos, como o Tella e o Eyewitness to Atrocities, oferecem criptografia de arquivos e / ou armazenamento criptografado para a sua documentação, de modo separado da galeria principal de seu telefone e da criptografia de seu telefone para que sua mídia e metadados nunca sejam descriptografados em seu dispositivo, exceto se acessados por meio do aplicativo com uma senha. Isso significa que, mesmo se o telefone estiver desbloqueado, a documentação permanecerá criptografada. Isso pode fornecer um nível extra de proteção para a sua documentação.

Se o aplicativo enviar e armazenar a sua mídia em um local remoto após a restauração da internet, verifique também se você precisa que os seus arquivos estejam criptografados enquanto estiverem sendo enviados e guardados no local remoto, algo que o aplicativo EyeWitness, por exemplo, faz.

Lembre-se de que, embora a criptografia seja legal na maioria dos lugares, alguns países podem ter leis que restringem ou criminalizam o seu uso. Este [mapa](#) (abrangente, mas de 2017) fornece um bom ponto de partida se você tiver dúvidas sobre as leis em seu país.

## O aplicativo captura metadados importantes (sem internet)?

[Metadados](#) são dados que descrevem seu vídeo ou foto, como a hora e a data ou o local do registro. Essas informações são valiosas para se identificar, entender, autenticar e verificar o seu vídeo ou foto como sendo a documentação de um evento específico. No contexto de um bloqueio da internet, a capacidade de um aplicativo de coletar automaticamente determinados metadados e / ou permitir que você insira facilmente informações descritivas úteis é especialmente valiosa, pois pode demorar um longo período antes que você possa compartilhar a documentação com outra pessoa (e, durante esse período, os detalhes podem ser esquecidos, as circunstâncias podem mudar, etc, etc).

A maioria dos aplicativos de documentação especializados, como o ProofMode, têm recursos de metadados aprimorados e reúnem mais metadados do que os aplicativos de câmera integrados convencionais. Os metadados aprimorados podem incluir vários dados do sensor, sinais de wi-fi ou bluetooth próximos, dados do dispositivo, função hash criptográfica e informações fornecidas pelo usuário. Todos esses itens podem facilitar a autenticação e verificação da mídia posteriormente.

Lembre-se de que, durante o bloqueio da internet, você precisará de um aplicativo que não dependa da transmissão de dados para gerar ou registrar os metadados. Alguns aplicativos

podem depender da internet, em vez dos sensores de hardware, para coletar certos metadados. Por exemplo, se os dados de localização forem capturados a partir de pesquisas no dispositivo, os metadados podem refletir a última localização quando o dispositivo teve conexão de dados, em vez da posição real do aparelho. Idealmente, o aplicativo também deve permitir que você armazene os metadados localmente, sem internet, incluindo o salvamento de todos os formulários que estiver preenchendo (como, por exemplo, o “modo offline” do aplicativo Tella).

## Posso exportar dados do aplicativo?

Dependendo das suas intenções para a documentação, pode ser crucial ser capaz de exportar a documentação em vídeo e os seus metadados do aplicativo, em um formato que não seja de propriedade daquele aplicativo. Ou seja, pode ser importante para você ser capaz de abrir, visualizar e usar a mídia e os metadados fora do aplicativo. A capacidade de exportar significa que você e outras pessoas não vão depender de um único aplicativo ou de um provedor de serviços para acessar a sua documentação. Isso dá a você mais margem de manobra para trabalhar com o conteúdo no futuro. Lembre-se de que alguns metadados podem não ser compreensíveis se você não tiver acesso a determinados bancos de dados ou gráficos de conversão para interpretar os números (por exemplo, no caso de IDs de torre de celular ou de redes Wi-Fi).

Observe que alguns aplicativos podem ter uma cadeia de custódia deliberadamente fechada e não permitir que os usuários exportem seus dados, enquanto alguns aplicativos podem simplesmente não ser projetados tendo a exportação em mente. Esteja ciente também de que alguns aplicativos, como o Eyewitness to Atrocities, podem não permitir que você exporte os dados até ter carregado a mídia para um servidor remoto (algo que exige conexão à internet). Alguns aplicativos podem permitir que você exporte a mídia, mas não os metadados (exceto quaisquer metadados que estejam no próprio arquivo).

Se você precisar exportar, idealmente seu aplicativo deve permitir que você exporte uma cópia da mídia sem quaisquer alterações ou transformações, e uma cópia dos metadados em um formato de texto legível padronizado. Os metadados do Tella, por exemplo, são armazenados criptografados na galeria do aplicativo, mas podem ser exportados como CSV. Além disso, durante um bloqueio da internet é necessário ter opções para exportar os dados para aplicativos offline ou serviços não dependentes da rede. A maioria dos aplicativos que permitem a exportação tem algum tipo de botão “Compartilhar”, que aciona um menu de compartilhamento, e então o Android oferece uma lista de aplicativos em seu telefone que são capazes de lidar com esse tipo de conteúdo. Infelizmente, os desenvolvedores de aplicativos podem personalizar seus menus de compartilhamento e não há padrões consistentes entre os aplicativos.

Para uma quantidade maior de arquivos, pode ser mais eficiente acessar os arquivos armazenados por meio de um aplicativo gerenciador de arquivos e copiar os arquivos de lá, embora você não consiga acessar os metadados armazenados no banco de dados de um

aplicativo dessa forma. Essa opção também não está disponível para aplicativos que fornecem suas próprias galerias seguras, pois os arquivos estarão criptografados ao serem armazenados. Para esses aplicativos, é necessário ter uma função de compartilhamento dentro do aplicativo.