PORQUE FUNCIONA?

Em Outubro de 2025, a imprensa divulgou documentos internos de uma empresa de extracção forense (Cellebrite) que listavam Pixels com GrapheneOS actualizado como inacessíveis às suas ferramentas. Em Novembro de 2025, a imprensa e a procuradoria francesas associaram o projecto ao crime; o projecto respondeu que privacidade não é crime. Ferramentas de privacidade são usadas por jornalistas, activistas, pessoas sobreviventes de violência e qualquer pessoa que valorize os seus direitos.

AJUDA

- Guia oficial: grapheneos.org
- Fórum oficial: discuss.grapheneos.org

Inspirado livremente em guias de segurança digital de outros movimentos. Texto original, escrito para um movimento não-violento pela habitação.

Série Prevenção Anti-Censura: n.º 1 O Telemóvel é um Bufo, n.º 2 Mensagens Encriptadas, n.º 4 Tails.

Informação revista a 25 de Outubro de 2026: confirma sempre em grapheneos.org. Copia, partilha, melhora.

Habitação é um direito. Privacidade também.

ACAMPADA
ASSEMBLEIA POPULAR

LISBOA · OUT. 2026

SÉRIE PREVENÇÃO ANTI-CENSURA
N.º 3 DE 4

GRAPHENE OS 101

Um telemóvel mais privado para quem organiza e para quem está em risco

LÊ · COPIA · PARTILHA

PREVENÇÃO ANTI-CENSURA

PORQUÊ ISTO?

O telemóvel sabe onde dormimos, com quem falamos, que fotos tiramos e a que reuniões vamos. Num movimento pela habitação, isso não é só sobre nós: é sobre a vizinhança ameaçada de despejo, pessoas migrantes, quem tem medo de represálias da parte proprietária.

Proteger estes dados é cuidado colectivo. Não é esconder nada: é exercer o direito à privacidade e à liberdade de associação, previstos na Constituição e na Carta dos Direitos Fundamentais da UE.

O **GrapheneOS** é um sistema operativo gratuito e de código aberto, baseado em Android, que:

- não traz serviços Google instalados de origem;
- reforça a encriptação e a protecção contra ataques e spyware;
- dá controlo fino sobre o que cada app pode ver.

Não é magia. É uma camada a mais, que funciona melhor junto com bons hábitos e com conversas em grupo sobre segurança.

HÁBITOS E LIMITES

HÁBITOS QUE FAZEM A DIFERENÇA

- Desliga o telemóvel à noite ou quando não o levas. Desligado é quando a encriptação protege mais.
- **Signal** com mensagens temporárias nos grupos de organização (ver zine n.º 2).
- Fotos de acções: tapa caras e remove metadados antes de publicar.
- Em Wi-Fi público, usa uma **VPN de confiança** e activa "bloquear ligações sem VPN".

O QUE O GRAPHENEOS NÃO FAZ

- Não esconde a tua localização da operadora: se tens SIM, as antenas sabem onde estás.
- Não protege o que tu ou outras pessoas mostram ou escrevem.
- Não te torna invisível na rua nem nas redes sociais.

SE NÃO PUDERES MUDAR DE TELEMÓVEL

- **iPhone:** activa o **Modo de Isolamento** (Lockdown Mode), que bloqueia anexos e ligações arriscadas.
- **Android 16 ou mais:** liga a **Protecção Avançada**: protege a porta USB, reinicia após 72 h e bloqueia redes 2G.

PIN DE COACÇÃO: LER COM ATENÇÃO

O GrapheneOS permite definir um **PIN e uma palavra-passe de coacção**. Se forem escritos em vez do código verdadeiro, o telemóvel **apaga-se por completo, de forma imediata e irreversível**, incluindo eSIMs.

Para que serve: roubo, ou uma pessoa abusiva que te obriga a desbloquear o telemóvel.

O que NÃO fazer: nunca o uses perante a polícia ou outras autoridades, nem num telemóvel apreendido ou que vá ser apreendido. Pode ser visto como destruição de prova ou desobediência, com consequências legais sérias para ti.

Em contacto com a polícia: mantém a calma, não resistas e pede apoio jurídico. Sobre o que tens ou não de dizer, e sobre códigos de desbloqueio, fala **antes** com advogade.

OUTRAS REGRAS

- Tens de ter cópias de segurança, senão perdes tudo.
- Escolhe um código que não escrevas por engano.
- Explica a quem vive contigo que o telemóvel tem esta função.

PARA QUEM É?

Faz sentido sobretudo para:

- **pessoas que organizam**: coordenam GTs, têm listas de contactos, falam com a imprensa;
- **pessoas em situação vulnerável**: em processo de despejo, sem documentos regularizados, com histórico de assédio;
- **quem guarda dados de outras pessoas**: fotos de acções, actas, listas de inscrição.

Pode não ser prioridade se o teu telemóvel só serve para ver o horário do metro. A segurança é colectiva: um telemóvel muito protegido num grupo onde todo o resto está desprotegido ajuda pouco.

ANTES DE AVANÇAR, PERGUNTA-TE

1. Que informação tenho que, se exposta, prejudica outras pessoas?
2. Quem pode querer essa informação (empresas, partes proprietárias, pessoas abusivas, quem rouba telemóveis)?
3. O que acontece se perder o telemóvel amanhã?

Se as respostas te deixam desconfortável, continua a ler.

DE QUE PRECISAS

Um Google Pixel (sim, da Google: é o hardware com os chips de segurança que o projecto exige). Compra **livre de operadora**.

Recomendados (Out. 2026): **Pixel 8, 8a, 9, 9a, 10, 10a** e versões Pro/Fold. Têm actualizações garantidas durante pelo menos 7 anos desde o lançamento.

Evita: Pixel 6 (fim do suporte em Outubro 2026) e Pixel 7 (fim em Outubro 2027). O Pixel 11 ainda **não** era suportado em Outubro 2026: confirma em grapheneos.org/faq.

PREÇOS APROXIMADOS EM PORTUGAL

- Pixel 10a novo: cerca de 560 €
- Pixel 9a novo em promoção: cerca de 450 €
- Pixel 8a recondicionado: cerca de 250 a 300 €

Um usado serve, desde que não esteja bloqueado.

Também precisas: computador com Chrome, Edge ou Brave; cabo USB-C bom; 1 hora sem pressa; cópia de segurança do que tens no telemóvel actual (a instalação apaga tudo).

A Motorola anunciou em 2026 uma parceria com o GrapheneOS. Ainda não há modelos à venda.

LISTA DE DEFINIÇÕES

Faz isto no perfil Principal, com a ajuda de alguém se precisares.

☐ **Reinício automático:** 18 horas (o padrão) ou menos. Se o telemóvel ficar bloqueado esse tempo, reinicia e volta ao estado mais protegido.

☐ **Porta USB-C:** "só carregar" ou "só carregar quando bloqueado" (o padrão). Impede que ligações por cabo leiam dados.

☐ **Baralhar o PIN:** os números mudam de lugar, para ninguém decorar o teu código por cima do ombro.

☐ **Modo só LTE** (se tiveres SIM): desliga 2G, 3G e 5G e reduz ataques pela rede móvel.

☐ **Bloqueio de ecrã:** 1 minuto ou menos.

☐ **Bluetooth, localização, câmara, microfone:** desliga quando não usas.

☐ **Instalação de apps nos perfis secundários:** desactivada depois de configurados.

☐ **Actualizações:** automáticas. Reinicia quando o telemóvel pedir.

☐ **Sem cópias na nuvem:** guarda ficheiros importantes num disco encriptado em casa.

Os nomes dos menus podem variar com as versões.

APPS SEM ENTREGAR TUDO

App Store do GrapheneOS: já vem instalada. Dá as apps do próprio projecto (browser Vanadium, Câmara, Leitor de PDF, Auditor) e permite instalar:

- **Google Play em sandbox:** a loja e os serviços Google correm como qualquer outra app, sem acesso especial ao sistema. Permite usar quase todas as apps normais.
- **Accrescent:** uma loja alternativa pensada para segurança, ainda com poucas apps.

AO INSTALAR CADA APP, PENSA

- Precisa mesmo de **Rede**? Se não (calculadora, bloco de notas), desliga a permissão.
- Precisa de **Sensores** (movimento, bússola)? Normalmente não.
- Pede **acesso aos ficheiros**? Usa **Storage Scopes**: a app só vê o que escolheres.
- Pede **contactos**? Usa **Contact Scopes** e partilha só os necessários.
- **Área de transferência:** podes impedir cada app de ler o que copiaste.

Para enviar uma foto no Signal, partilha-a a partir da Galeria em vez de dar acesso a todas as fotos.

INSTALAÇÃO (VISÃO GERAL)

Faz com calma, de preferência em dupla, numa oficina do colectivo. O guia oficial está em **grapheneos.org/install/web**: segue-o passo a passo.

1. Liga o Pixel, actualiza-o e salta as contas Google.
2. Activa as **Opções de programador** (tocar 7 vezes em "Número de compilação") e liga **Desbloqueio OEM**.
3. Desliga e arranca em modo **fastboot** (botão de volume para baixo ao ligar).
4. No computador, abre o instalador web e liga o cabo directamente.
5. Carrega em **desbloquear bootloader**, depois **descarregar** e **instalar** a versão. Não mexas no telemóvel durante a instalação.
6. Carrega em **bloquear bootloader**. Este passo é essencial.
7. No primeiro arranque, mantém **desligado o Desbloqueio OEM**.
8. Faz a verificação com a app **Auditor** (página seguinte).

Atenção: só descarregues a partir de grapheneos.org. Há cópias falsas.

PRIMEIRO ARRANQUE E VERIFICAÇÃO

Palavra-passe forte. Usa uma frase com 5 ou 6 palavras aleatórias. É ela que protege a encriptação.

O GrapheneOS permite juntar impressão digital e **PIN curto como segundo factor**: o dedo sozinho não chega. Mesmo assim, em manifestações e acções, segue a regra da zine n.º 1: **sem biometria**.

Auditor. É uma app que confirma que o sistema não foi alterado.

- Precisas de outra pessoa de confiança com a app Auditor num telemóvel Android.
- Os dois telemóveis lêem códigos QR um do outro. A primeira vez cria uma ligação; nas seguintes, se tudo estiver bem, aparece um resultado verde.
- Repete de vez em quando, por exemplo nas assembleias.

Podes também activar a **verificação remota** gratuita (attestation.app), que avisa por email se o telemóvel deixar de responder ou mostrar alterações.

Se o Auditor alguma vez acusar problema: pára de usar o telemóvel para coisas sensíveis e pede ajuda (ver contracapa).

PERFIS: SEPARAR A VIDA

O GrapheneOS deixa criar **perfis de utilizador**: como ter vários telemóveis dentro de um. Cada perfil tem as suas apps, ficheiros e encriptação. Uma app num perfil não vê nada dos outros.

SUGESTÃO SIMPLES

- **Principal (Owner):** com a palavra-passe mais forte. Aqui instalas e actualizas apps. Uso mínimo.
- **Dia-a-dia:** onde usas o Signal, o browser, as fotos, as coisas do movimento.
- **Google (opcional):** só para apps que exigem serviços Google (banco, algumas apps de transportes). Usa uma conta separada com o mínimo de dados pessoais.

Para criar: **Definições > Sistema > Vários utilizadores > Adicionar utilizador**.

Quando acabares de usar um perfil, toca em **Terminar sessão**: os dados desse perfil voltam a ficar encriptados.

Liga a opção para receber notificações de outros perfis, para não perderes mensagens.