MANUAL DO USUÁRIO

Guia completo do *ARMOR*

Todas as telas, todos os recursos e um passo a passo de configuração do zero: do cadastro até o aparelho do seu filho protegido e funcionando. Este manual cobre o app ARMOR em teste, que reúne as duas linhas, ARMOR Família e ARMOR Guard. Para guias curtos, veja a **ajuda do ARMOR Família** e a **ajuda do ARMOR Guard**.

ÍNDICE

01 Começando
02 Configuração passo a passo
03 Início e níveis de proteção
04 Identidade digital
05 Família e convites
06 Proteção infantil: o que é analisado
07 Preparar o aparelho do menor
08 Permissões do aparelho do menor
09 Controle do Dispositivo
10 Proteção de Rede e filtros
11 Modo criança (o que ela vê)
12 Acessar o aparelho do filho
13 Guardião anti-desinstalação
14 Alertas
15 AURA, a assistente
16 Planos e assinatura
17 Perfil e conta
18 Privacidade e LGPD
19 Segurança infantil e denúncias
20 Solução de problemas
21 Perguntas frequentes
22 Suporte

01 Começando

O que é o ARMOR

ARMOR (*Automated Recognition of Malicious Online Requests*) é a plataforma de proteção digital da sua família e sua. Ele faz quatro coisas:

- **Protege o aparelho do menor** (ARMOR Família): filtra sites, controla horários e tempo de tela, e analisa mensagens e imagens em busca de aliciamento, golpes e conteúdo sexual, com a análise começando *dentro do próprio aparelho*.
- **Protege você contra golpes** (ARMOR Guard): Verificar mensagem, Guarda de Pix e as proteções que você liga no seu próprio aparelho.
- **Vigia seus dados**: avisa quando seu e-mail ou telefone aparece em vazamentos conhecidos. Para CPF não existe base pública de consulta automática; o app orienta a consulta nos birôs de crédito.
- **Coloca você no controle**: todo alerta traz o que aconteceu e o que fazer. A decisão é sempre do adulto responsável.

Instalar no Android

1. Durante o teste, o app é distribuído por convite: abra o **link de download** do convite que você recebeu ou, se você é testador, a página **Beta** (com senha).
2. Toque no arquivo baixado. Se o Android pedir, autorize a instalação de "fontes desconhecidas" para o navegador.
3. Abra o app e crie sua conta.

📱 O app instala a partir do **Android 7**. No aparelho do menor, é no Android que a proteção é mais ampla: controles de tempo, bloqueio de tela e análise de mensagens e imagens dependem de recursos que o iPhone não oferece a apps de terceiros.

Instalar no iPhone (iOS)

No iPhone (iOS 15.1 ou mais recente), instale pelo **TestFlight** (convite) durante o teste; a versão definitiva chegará pela App Store.

⚠️ **No iPhone a supervisão do menor é diferente.** O filtro de sites é feito por um *perfil de configuração* instalado no aparelho. No app de teste, um iPhone com iOS 16 também pode parear pelo código e usar o Tempo de Uso da Apple para horários, limite diário, pausa dos apps e trava de instalação; esse modo ainda está em validação, e a tela não trava (os apps ficam pausados). Nenhum app lê as mensagens ou as fotos de outro app no iPhone: lá, quem protege esse conteúdo é a própria Apple, na Conta de Criança.

Criar conta

- **E-mail e senha**: cadastro direto no app; ou
- **Conta Google**: um toque, e sua foto de perfil já aparece no app.

Confirmar o e-mail

Ao se cadastrar com e-mail e senha, você recebe uma mensagem com um link de confirmação. **Enquanto não confirmar, o login é recusado**. O app mostra o motivo e um botão para reenviar.

- Não chegou? Confira a caixa de spam e toque em **Reenviar confirmação**.
- O link vale uma vez só. Se aparecer "link já utilizado", provavelmente seu app de e-mail o pré-carregou. Sua conta já está confirmada, basta entrar.

Confirmar o telefone

No cadastro e no **Perfil**, o telefone é digitado duas vezes numa caixa de confirmação. Não é burocracia: o telefone é para onde vão os **alertas de segurança sobre a sua criança** por WhatsApp. Um dígito errado faz um estranho receber esses avisos.

> 💡 O app formata e valida enquanto você digita: DDD válido, nove dígitos para celular, e recusa números repetidos. O nome exibido, o e-mail e o CPF podem ser ajustados depois em **Perfil → Dados pessoais → Editar**. O CPF é opcional: serve para você acompanhar o próprio CPF na aba Identidade, onde o app orienta a consulta nos birôs de crédito.

02 Configuração passo a passo

Este é o caminho completo, do zero até o aparelho do menor protegido. Reserve cerca de **15 minutos** e tenha os **dois aparelhos em mãos**: o seu e o dele.

Parte 0: as primeiras telas, passo a passo

Estas são as primeiras telas do aplicativo, na ordem em que aparecem, e o que cada elemento faz.

ABERTURA: 4 TELAS DE APRESENTAÇÃO

1. **Contador (1/4).** São quatro telas explicando o que o app faz. Você pode ler ou saltar.
2. **Pular.** Vai direto para a entrada, sem ler a apresentação.
3. **Pontos de navegação.** Mostram em qual das quatro telas você está.
4. **Continuar.** Avança para a próxima tela de apresentação.

5. **Já tenho conta.** Atalho para quem só está instalando em mais um aparelho.

💡 **Os três caminhos levam ao mesmo lugar:** "Pular", o "Continuar" da última tela e "Já tenho conta" terminam todos na tela de **entrada**. É por isso que o acesso do menor fica lá: assim ele é alcançável em qualquer instalação nova, não importa por onde a pessoa saia da apresentação.

ENTRADA E O ACESSO DO MENOR

1. **A marca.** Confira que é o aplicativo certo antes de digitar qualquer senha.
2. **"Este aparelho é de uma criança". Este é o botão que você usa no celular do seu filho.** Não crie conta nele. Toque aqui.
3. **"Tenho um código de pareamento".** Explica para que serve o botão acima: é onde se digita o código de 6 dígitos que aparece no *seu* celular.
4. **Entrar.** O formulário do **responsável**, com e-mail e senha. Use só no seu aparelho.

⚠️ **O erro mais comum da instalação.** Muita gente cria uma segunda conta no celular da criança. Não faça isso: o aparelho dela não tem conta própria. Ele é **pareado** ao seu, pelo botão **"Este aparelho é de uma criança"**. Criar conta ali deixa o aparelho como "responsável" e nada é supervisionado.

QUEM ESTÁ CONFIGURANDO ESTE APARELHO

1. **Sou a criança/adolescente.** Segue para digitar o código de 6 dígitos e, depois, para a tela de consentimento, que a criança precisa aceitar.
2. **Sou o responsável.** Volta atrás, para o caso de você ter tocado no botão errado. Nada é gravado até o pareamento dar certo, então desistir aqui não deixa o aparelho preso em modo criança.

Parte 1: no seu celular (5 min)

1. **Instale e crie a conta.** Instale pelo link do convite ou pela página Beta, cadastre-se e **confirme o e-mail** pelo link que chegar.
2. **Confirme seu telefone** no cadastro. É o canal dos alertas urgentes.
3. **Crie a família.** Aba **Família → Convidar familiar**. Preencha nome, parentesco e **idade**. Menor de 18 é classificado como criança automaticamente.
4. **Escolha o avatar** (menino, menina ou neutro), que aparece na tela inicial do aparelho dele.

5. **Envie o convite** ou anote o **código de 6 dígitos** que aparece na tela. Você vai digitá-lo no aparelho do menor.

> 🔑 Perdeu o código ou ele expirou? Não precisa refazer nada: na aba **Proteção → Dispositivos e Proteção de Rede**, cada aparelho tem a ação 🔑 **Código**, que gera um novo na hora.

Parte 2: no aparelho do menor (7 min)

1. **Instale o app** pelo mesmo caminho: o link de download do convite ou a página Beta.
2. **Abra e vá até a tela de entrada.** Toque em **"Este aparelho é de uma criança / Tenho um código de pareamento"**.
3. **Digite o código de 6 dígitos.**
4. **Leia o consentimento com ela.** A tela explica, em linguagem adequada à idade, o que será supervisionado. **A criança precisa aceitar**: sem isso a supervisão não ativa.
5. **Libere as permissões pelo checklist.** A tela inicial do aparelho mostra um checklist com cada permissão. Toque em cada item pendente: ele abre a tela certa das Configurações e diz o que fica desligado sem ele. A seção Permissões explica cada uma.

> ⚠️ **O passo que trava quase todo mundo:** no Android 13 ou superior, com o app instalado fora da loja, o botão da **Acessibilidade** aparece *cinza e não clicável*. Não é defeito. Vá em **Configurações → Apps → ARMOR → menu ⋮ (canto superior) → Permitir configurações restritas**. Só depois disso o botão liga.

Parte 3: confirmar que está funcionando (2 min)

Ainda no aparelho do menor, a tela inicial mostra o **checklist de permissões**. Confira que todos os itens estão marcados. Se algum estiver pendente, toque nele: o app abre a tela certa das Configurações e mostra o que fica desligado sem ele.

No **seu** celular, abra **Proteção → Dispositivos e Proteção de Rede**. O aparelho deve aparecer como **ativo**, com contato recente. Se disser que está offline, o app do menor não está rodando.

Parte 4: ajustar as regras (o resto do tempo)

Toque no aparelho para abrir o **Controle do Dispositivo** e configure na ordem que fizer sentido para a sua família:

- **Filtro de Conteúdo**: marque as categorias a bloquear. Cada toque salva na hora.
- **Agenda de Uso**: a janela em que o aparelho pode ser usado.
- **Horário Escolar**: bloqueia nos horários de aula.

- **Limite Diário de Uso**: teto de minutos por dia.
- **Contatos Confiáveis**: na agenda sincronizada do aparelho, marque as pessoas de confiança. A marcação aparece no alerta quando a mensagem vem de uma delas; ela não muda a análise de risco.

⚠️ **Marcar "Streaming" não é o mesmo que bloquear YouTube por tempo.** O filtro de conteúdo bloqueia o *acesso*; o limite por categoria conta *minutos*. Se você quer que o YouTube pare depois de X minutos, use o limite da categoria **Vídeo/Streaming** na aba Tempo. Marcar a categoria no filtro apenas bloqueia o site por completo.

Parte 5: alguns aparelhos exigem um passo extra

Xiaomi/POCO (MIUI), Oppo, realme, vivo e alguns Samsung desligam apps em segundo plano de forma agressiva. Nesses aparelhos, ative o **"Início automático"** (ou "Autostart") para o ARMOR nas configurações do fabricante. Sem isso a proteção pode não voltar depois de reiniciar o aparelho, e **não existe forma de o app fazer isso sozinho**.

03 Início e níveis de proteção

A tela **Início** tem um cartão com duas abas, **Nível de Proteção** e **Proteção da Família**, e a diferença entre elas importa:

Nível de Proteção (0% a 100%)

Mede a **sua exposição pessoal**: quantos vazamentos dos seus dados estão em aberto e quão graves são. Quanto maior o número, melhor. O botão **Escanear agora** faz a verificação na hora: o anel vai de 0% a 100% enquanto verifica e, no fim, mostra o seu nível.

`100% sem nada em aberto: Seguro` `80% ou mais, sem ameaça aberta: Protegido`
`50% ou mais: Atenção` `abaixo de 50%: Em risco`

A curva é logarítmica de propósito: quem tem centenas de vazamentos antigos vê o nível **subir de verdade** conforme resolve, em vez de ficar travado no fundo da escala.

Proteção da Família

Mede a **postura de proteção** da família, também de 0% a 100% (100% é família segura), a partir de seis fatores, cada um com um texto explicando o que fazer:

FATOR	O QUE MEDE
Exposição do responsável	Seus vazamentos em aberto
Menor sem aparelho	Criança na família sem nenhum aparelho supervisionado
Ameaças ao menor	Alertas de risco nos últimos 30 dias
Aparelho sem contato	Aparelho supervisionado que sumiu há mais de 8h
Aparelho sem regra	Aparelho ativo sem filtro nem horário configurado
Filtro de sites desligado	Android com a proteção de rede desligada, ou iPhone com o app sem o perfil de filtro

💡 **Ler um alerta não muda o nível.** O peso de uma ameaça cai sozinho depois de 30 dias, ou na hora se você marcar o alerta como **Não é um alerta**. Isso é deliberado: o nível mede a proteção da criança, não a atenção do adulto.

Outros elementos

- **Escanear agora**: varredura imediata dos seus dados monitorados.
- **Relatório semanal**: resumo dos últimos 7 dias.
- Atalhos para supervisionar um aparelho e outras ações frequentes.

04 Identidade digital

A aba **Identidade** monitora se seus dados apareceram em vazamentos conhecidos. No topo, o mesmo cartão da tela inicial mostra o **nível de proteção**, de 0% a 100%, os riscos por gravidade e a última verificação; abaixo dele, o que forma esse nível.

Adicionar um dado ao monitoramento

1. Toque em **+ Adicionar** e escolha o tipo: **e-mail**, **CPF** ou **telefone**.
2. Digite o valor: o app valida na hora (e-mail com formato real, CPF com dígitos verificadores, telefone com DDD).
3. Pronto: o dado entra na verificação diária e aparece **mascarado** na lista (ex.: j•••@gmail.com). E-mails e telefones são consultados em bases públicas de vazamentos (como Have I Been Pwned, BreachDirectory e LeakCheck); o CPF não é enviado a nenhuma base, porque não existe consulta pública automática para ele.

Vazamentos encontrados

Se um dado aparecer em vazamento, você verá a fonte, a gravidade e o que foi exposto, com o que fazer na ordem (trocar senha, ativar a verificação em duas etapas etc.). Quando terminar, toque em **Marcar como resolvido**; se o vazamento não tiver relação com você, use **Não é um alerta**.

> 📋 **A primeira varredura de um e-mail antigo pode achar centenas de vazamentos de uma vez.** Nesse caso o app agrupa tudo em **um único alerta-resumo**, em vez de encher a lista e disparar centenas de notificações. Nas varreduras seguintes, quando o normal é achar poucos, cada um vira um alerta próprio com o nome do serviço.

Remover um dado

Toque no item e em **Remover**. O histórico de vazamentos associado a ele também é removido.

> 🔒 Os limites de monitoramento variam por plano (número de e-mails, CPFs e telefones). Veja a seção Planos.

05 Família e convites

Convidar um membro

1. Aba **Família → Convidar familiar**.
2. Preencha nome, e-mail, parentesco e **idade**. Menor de 18 é classificado automaticamente como criança. A etiqueta mostra **Menor**, **Adulto** ou **Idoso** (60+).
3. Para menores, aparecem os chips de **avatar**: menino, menina ou neutro.
4. Se quiser, informe o telefone (WhatsApp) da pessoa: o convite chega também por lá. Toque em **Escolher da agenda de contatos** para preencher nome, e-mail e telefone a partir da agenda do seu celular.
5. Envie. Você também pode copiar o link, compartilhar por outro app, ou usar o **código de 6 dígitos** que aparece na tela.

O que acontece quando o convite é aceito

- **Menor:** ao abrir o link no celular dele, o app entra direto no **modo criança**, já pareado com você, sem senha e sem acesso ao painel dos pais.
- **Adulto com conta:** a conta existente é vinculada à família; basta entrar com o próprio e-mail.

- **Adulto sem conta:** o app orienta o cadastro; ao criar a conta com o mesmo e-mail do convite, o vínculo é feito sozinho.

🔁 O link do convite pode ser reaberto sem erro. Expirou? Reenvie pela aba Família, ou use o código de 6 dígitos. Os dois caminhos levam ao mesmo lugar.

Remover um membro

Toque no membro → **Remover**. Os aparelhos supervisionados e registros associados a ele são removidos juntos.

⚠️ Se você quer apenas tirar *um aparelho* da lista, não remova o membro. Use **Excluir** no próprio aparelho, em Proteção → Dispositivos. Remover o membro apaga tudo o que está ligado a ele.

06 Proteção infantil: o que é analisado

Esta é a parte mais sensível do produto, então vale ser exato sobre o que acontece.

A análise começa DENTRO do aparelho

O ARMOR **lê** as mensagens recebidas pelas notificações e **olha** as fotos novas da galeria do aparelho do menor. A primeira análise acontece **no próprio aparelho**, por modelos de inteligência artificial embarcados no app, e a maior parte do conteúdo nunca sai dele.

Quando uma **mensagem** tem sinal de risco, o texto e o nome de quem mandou vão ao servidor do ARMOR para uma conferência e são descartados depois da análise. O alerta guarda a categoria (ex.: "aliciamento"), a gravidade, os sinais, o remetente e um código que evita repetir o aviso, **nunca o texto**. Com uma **foto**, só o resultado viaja: a categoria, a nota e uma impressão que não reconstrói a imagem. **O arquivo da imagem nunca sai do aparelho.**

🔍 É a diferença entre um cão farejador e uma câmera. O modelo passa pelo conteúdo e aponta o que é perigoso; o servidor confere só o trecho suspeito. Você recebe o aviso, não a conversa nem a foto.

O que é examinado

FONTE	O QUE PROCURA
Mensagens recebidas (WhatsApp, Telegram, Instagram, Messenger, Discord, Snapchat, TikTok, Kik, Roblox, Minecraft e outros)	Aliciamento, sextorsão, golpes, phishing
SMS (pela notificação do app Mensagens do Google)	Golpe do Pix, falso banco, vale-presente, falsa emergência
Fotos novas da galeria	Nudez e conteúdo sexual explícito (o modelo não estima idade e pode errar)
Arquivos baixados	Aplicativos (.apk) baixados fora da loja (só o nome do arquivo sai do aparelho)
Navegação (com a Acessibilidade)	Buscas e páginas com sinal de risco; os sites de categorias bloqueadas são barrados pelo filtro de rede

⚠️ **A varredura de fotos cobre a galeria a partir da instalação.** O acervo anterior (as fotos que já estavam no aparelho antes de você instalar o app) não é varrido. É uma decisão de produto: examinar anos de álbum de família custaria dias de bateria e atrasaria justamente a foto que acabou de chegar. Vídeos não são analisados.

Funciona com o app fechado

Mensagens, fotos e downloads são capturados e classificados mesmo com o app do menor fechado e mesmo **sem internet**; os bloqueios por horário e o limite de tempo continuam valendo offline, com as regras da última conexão. O que foi detectado sem internet fica guardado no aparelho (até 7 dias) e é enviado quando a proteção volta a rodar com conexão (na próxima mensagem recebida, quando o app é aberto ou quando você manda um comando), e o alerta mostra a hora em que foi detectado.

Simular detecção

Quer ver como funciona sem esperar um caso real? Toque em **Simular detecção**, escolha um filho menor de idade cadastrado e cole uma conversa ou use um exemplo. A simulação usa regras próprias, diferentes da análise que gera os alertas: procura só sinais de aliciamento e trata toda conversa como vinda de um contato desconhecido, por isso nem uma conversa comum sai como segura. O texto é analisado no servidor do ARMOR, não vira alerta e não fica guardado.

Alertas de risco

Quando um padrão suspeito aparece, você recebe um alerta com:

- **Sinais encontrados** (ex.: pedido de segredo, pedido de foto, ameaça, cobrança urgente);
- **Quem mandou**, quando a origem é uma mensagem;
- **O que fazer agora**: recomendações práticas, na ordem.

Nos casos de aliciamento, extorsão ou imagem íntima, o alerta leva ao roteiro com os canais oficiais de denúncia (SaferNet, Disque 100 e Polícia Federal).

⚠️ A AURA **sinaliza**; a decisão é sempre sua. Em risco imediato à vida, ligue **190** (Polícia) ou **192** (SAMU).

07 Preparar o aparelho do menor

Os dois caminhos

CAMINHO	COMO É
Link do convite	A criança recebe por WhatsApp e toca. O app entra no modo criança já pareado.
Código de 6 dígitos	Você lê o código em voz alta ou anota. No aparelho dela, na tela de entrada, toque em **"Este aparelho é de uma criança"** e digite.

🔑 O código vale 30 minutos. Se expirar, gere outro em **Proteção → Dispositivos →** 🔑 **Código**, quantas vezes quiser.

O consentimento do menor

Depois de parear, a criança vê uma tela explicando o que será supervisionado, em linguagem adequada à idade. **Ela precisa aceitar.** Sem esse aceite a supervisão fica pendente e nada é aplicado.

A LGPD exige o consentimento do responsável e que o tratamento atenda ao melhor interesse da criança (art. 14). O ARMOR vai além: no Android, a supervisão só começa depois que a criança lê o que é acompanhado e aceita, e no iPhone com o app ela também lê e aceita no aparelho. É o que separa proteção de espionagem. Converse com ela antes de instalar.

✅ São **dois consentimentos**: o seu, como responsável, dado quando você cria o aparelho no painel; e o dela, no aparelho. A supervisão só ativa com os dois.

Se ela não concordar

O aparelho fica pendente e nada é supervisionado. A recusa é registrada e **não é desfeita sozinha**. Você é avisado e pode conversar e tentar de novo.

Aparelho dedicado (opcional, proteção máxima)

Num aparelho **novo ou restaurado de fábrica**, é possível provisionar o ARMOR como "dono do dispositivo". Hoje isso é feito por cabo, com apoio técnico (o QR Code está em preparação). Nesse modo a instalação de apps é travada de verdade e a desinstalação exige o responsável; o filtro de rede segue sujeito aos limites descritos em "O que não é coberto". Em aparelho já em uso esse modo não está disponível: o Android só permite no primeiro boot.

08 Permissões do aparelho do menor

A tela inicial do app do menor traz um **checklist ao vivo** com nove itens no Android. Cada um abre a tela certa das Configurações quando tocado, e o checklist se reavalia sozinho quando você volta ao app.

PERMISSÃO	PARA QUE SERVE	SEM ELA
Proteção de rede (VPN)	Filtro de sites por categoria	Nenhum site é bloqueado
Acesso a notificações	Ler mensagens de WhatsApp, Telegram e afins	Aliciamento e golpes não são detectados
Acessibilidade	Guardião anti-desinstalação e captura de navegação	A criança consegue desinstalar o app
Bloqueio de tela (admin)	Travar a tela nos horários e limites	Horários e limite diário não travam nada
Acesso ao uso	Contar minutos por app e por categoria	Limite diário e por app não valem
Acesso às fotos	Varredura de imagens da galeria	Nudez e conteúdo sexual não são detectados
Certificado de segurança	Mostrar o aviso do ARMOR quando um site é bloqueado	O site bloqueado aparece como erro do navegador
Notificações do ARMOR	Lembretes e recados dos responsáveis	Os lembretes e os recados não aparecem
Agenda de contatos	Mostrar no alerta se quem mandou está na agenda e deixar o responsável marcar os de confiança	O responsável não vê a agenda

O botão da Acessibilidade está cinza

⚠️ No **Android 13 ou superior**, com o app instalado fora da Play Store, o Android bloqueia o botão da Acessibilidade por padrão. Ele aparece cinza e não responde ao toque.

A saída: Configurações → Apps → ARMOR → toque no **menu** ⋮ no canto superior direito → **Permitir configurações restritas**. Volte à tela de acessibilidade e o botão estará liberado.

Esse passo não é adivinhável e é o que mais trava instalações. Faça-o antes de tentar ligar a Acessibilidade.

O que depende de quê

Se você não conseguir conceder a Acessibilidade agora, boa parte da proteção continua valendo:

DEPENDE DA ACESSIBILIDADE	NÃO DEPENDE
Guardião anti-desinstalação	Captura de WhatsApp/Telegram e SMS
Captura de páginas visitadas	Filtro de sites (VPN)
Interceptar a tela do instalador de apps	Bloqueio de tela, limite diário, horários
	Varredura de galeria

09 Controle do Dispositivo

Em **Proteção → Dispositivos e Proteção de Rede**, toque num aparelho ativo. A tela abre em seis abas.

📊 Atividade

O que aconteceu no aparelho: sites visitados por categoria, bloqueios aplicados e eventos recentes. É onde você confere se o filtro está de fato pegando o que deveria.

🕐 Tempo

Tudo o que envolve relógio e minutos:

- **Pedidos de mais tempo**: quando a criança pede minutos extras, o pedido chega aqui para você aprovar ou recusar. Aprovar suspende o limite pelo tempo concedido.
- **Agenda de Uso**: a janela em que o aparelho pode ser usado (ex.: 07:00 às 21:00). Fora dela, a tela trava.
- **Horário Escolar**: blocos que bloqueiam nos horários de aula, com as categorias que continuam liberadas (pesquisa, educação).
- **Limite Diário de Uso**: teto de minutos por dia no aparelho inteiro. Zero = sem limite.
- **Limite por aplicativo**: minutos por dia para apps específicos, ou bloqueio total de um app.
- **Quadro de Horários**: lembretes e bloqueios em horários fixos (ex.: "hora do dever de casa", 30 min).

💡 **Quando o limite diário estoura, nem tudo trava.** A tela inicial do aparelho, o próprio ARMOR e a tela ociosa continuam acessíveis, de propósito. Se travasse tudo, a criança nunca conseguiria alcançar o botão de *pedir mais tempo*.

⚠️ **Mudar a data no aparelho não burla os horários.** O app mantém um relógio próprio, ancorado no servidor e contado a partir do tempo de funcionamento do aparelho. Adiantar ou atrasar a data em Configurações não afeta os bloqueios por horário nem o limite diário. Duas exceções: depois de reiniciado sem internet, o aparelho só impede voltar a data até a próxima conexão; e o limite por tipo de app ainda conta o dia pela data do aparelho.

📱 Apps

Lista dos aplicativos instalados no aparelho do menor. Daqui você define limites e bloqueios por app. O tempo de uso de cada app ainda não aparece no painel.

Instalação Remota: em aparelho dedicado (dono do dispositivo), você pode instalar um app à distância.

👥 Contatos

Contatos Confiáveis: cadastre família e amigos conhecidos, e marque, na agenda sincronizada do aparelho, as pessoas de confiança. A marcação da agenda aparece no alerta quando a mensagem vem de uma delas, e as duas listas aparecem na tela de transparência do filho. Nenhuma delas muda a análise de risco.

🔒 A lista manual de Contatos Confiáveis é guardada como **hash** (sem o número em texto claro). Já a agenda sincronizada do Android do filho fica no servidor com nome e número, visível só para você, para mostrar quem mandou uma mensagem com risco.

💬 Recados

Mande um recado que aparece na tela do aparelho do menor. Serve para avisos rápidos ("hora do jantar") sem precisar de outro app. Você vê quando foi lido e pode apagar os já lidos.

🛡️ Controle

As ações imediatas:

CONTROLE	O QUE FAZ
🧭 **Filtro de Conteúdo**	Marque categorias (adulto, apostas, redes sociais, jogos, streaming, violência, drogas, malware...). Os sites caem numa página "bloqueado pelo responsável", com opção de a criança **solicitar acesso**.
⛔ **Bloqueio de Emergência**	Corta toda a internet do aparelho na hora, não só alguns apps. Um toque liga e desliga. Pode ter prazo ("30 min") e expira sozinho.
📵 **Bloqueio de Tela**	Trava a tela. Aplica automaticamente em emergência, horário escolar, bloqueio do quadro e fora do horário permitido.
🛑 **Bloqueio de Instalação**	Impede instalar apps novos sem você liberar. Em aparelho dedicado (dono do dispositivo), a trava é do próprio Android; nos demais, depende da proteção de rede e da Acessibilidade.
🔐 **PIN de acesso**	Gera um código de 6 dígitos, de uso único, para você destravar o guardião ou abrir o painel no aparelho dela. Veja **Acessar o aparelho do filho**.
🔍 **Revarredura de fotos**	Manda o aparelho reexaminar as fotos desde a instalação com o classificador atual. Útil depois de uma atualização do app.

⚠️ **O filtro de conteúdo salva a cada toque; as abas de horário não.** No Filtro de Conteúdo, cada categoria é gravada no servidor assim que você toca. Se o servidor recusar, o marcador volta atrás sozinho, para nunca mostrar um estado que não existe. Já as abas de **agenda**, **horário escolar** e **limite diário** são formulários de vários campos e mantêm o botão **Salvar** de propósito: salvar a cada tecla mandaria estado pela metade. Se você sair sem salvar, o app avisa.

10 Proteção de Rede e filtros

Como o bloqueio funciona

Como um *Websense/Fortinet doméstico*, o ARMOR aplica os bloqueios no próprio aparelho da criança, sem depender do roteador. Toda consulta de nome de site passa pelo nosso filtro, que decide pela categoria.

Gerenciar aparelhos

AÇÃO	O QUE FAZ
⏸ **Pausar**	Suspende a supervisão temporariamente.
▶ **Retomar**	Volta a supervisionar.
✔ **Consentimento**	Registra a sua autorização para o iPhone protegido só pelo perfil de rede, em que o filho não usa o app.
🔑 **Código**	Gera novo código de pareamento de 6 dígitos.
🔐 **PIN de acesso**	Gera o PIN temporário de responsável.
📥 **Perfil**	Baixa o perfil de supervisão do iPhone.
🗑 **Excluir**	Remove o aparelho e seu histórico, de vez.

Bloqueios contra tentativas de burlar

- **"DNS seguro" do navegador**: navegadores modernos podem resolver nomes por conta própria, furando o filtro. O ARMOR reconhece os provedores usados nessa manobra e os bloqueia quando há qualquer filtro ligado, forçando o navegador de volta ao nosso filtro.
- **Instalar outra VPN**: se outra VPN derrubar a nossa, os bloqueios de horário, tempo e tela continuam valendo. Só o filtro de sites depende do túnel.
- **Mudar a data**: sem efeito, como explicado na aba Tempo.
- **Reiniciar o aparelho**: a proteção volta sozinha no boot.

🔐 **Certificado de segurança:** no checklist do aparelho do menor, toque em **Certificado de segurança** e siga os passos da tela do sistema. Sem ele, o site bloqueado aparece como erro do navegador em vez do aviso do ARMOR.

⚠️ **Nenhum controle parental é à prova de tudo.** Quem apagar os dados do app pelas Configurações do Android zera a proteção, mas isso exige as mesmas permissões que desinstalar, e você é avisado quando o aparelho some do painel.

Aparelho sumido

Se um aparelho supervisionado ficar **mais de 8 horas sem contato**, você recebe um aviso, fora do horário das 21h às 7h. No primeiro aviso, o app pergunta se você quer continuar recebendo; se você não responder, ele não avisa de novo. O limite é de 8

horas, e não de 30 minutos, de propósito: um celular desligado à noite não pode virar alarme de madrugada. No iPhone protegido só pelo perfil, o sinal de vida é a navegação.

11 Modo criança (o que ela vê)

No aparelho do menor o app roda em modo criança: sem painel de pais, com informações claras do que está ativo. A transparência é parte do desenho: ela sabe o que é supervisionado.

Tela inicial

- Avatar escolhido por você (menino, menina ou neutro) e o nome dela.
- **Checklist de permissões** com o que ainda falta autorizar.
- **Pedir mais tempo**: envia o pedido para você aprovar.
- **Pedir acesso a um site**: quando algo é bloqueado, ela pode solicitar liberação.
- Recados que você mandou.

Configurações da criança

Uma tela de transparência mostra a ela, em linguagem simples:

- ⏰ **Horário de uso**: a janela permitida e o limite diário;
- 🔒 **Sites bloqueados**: quais categorias estão ativas;
- 📞 **Contatos de confiança**: nome, relação e canal (o número em si não é mostrado, porque nem nós o guardamos em texto claro).

Sair do modo criança

Existe uma saída definitiva, que desliga a supervisão de vez, e ela **sempre exige a senha do responsável, validada no servidor**. Não basta ter o aparelho na mão. Quando usada, o aparelho é marcado como não supervisionado e você recebe um alerta.

12 Acessar o aparelho do filho

Você vai precisar mexer no celular dela em algum momento: conferir uma configuração, aprovar algo. Antes isso exigia desligar a proteção. Não mais.

Sessão temporária de responsável

Digite a sua senha no aparelho dela e você abre uma sessão de **30 minutos** com o painel completo. Durante ela:

- O aparelho **continua supervisionado**: filtro de rede, papel de criança e proteção intactos;
- Uma faixa fixa avisa "proteção ativa · toque para voltar";
- O **bloqueio de tela é pausado**, para a tela não travar na sua cara enquanto você usa;
- A sessão expira sozinha e **não sobrevive a um reinício**.

> 🔐 O bloqueio de emergência e o filtro de conteúdo **continuam valendo** durante a sessão. Ela pausa apenas a trava de tela: a criança não ganha acesso a nada bloqueado.

PIN de acesso (6 dígitos)

Se você não quiser digitar sua senha na frente dela, gere um **PIN de acesso** no seu celular (Proteção → Dispositivos → 🔐 PIN de acesso). Ele é de uso único, expira sozinho e tem limite de tentativas. Serve tanto para abrir a sessão quanto para destravar o guardião.

13 Guardião anti-desinstalação

Quando a criança tenta desinstalar o ARMOR, desativar o administrador do aparelho ou mexer na acessibilidade, uma tela do guardião aparece e pede o **PIN do responsável**.

O PIN é o mesmo de 6 dígitos da seção anterior: gerado no seu celular, de uso único, com prazo. Não existe PIN fixo para a criança decorar.

> ⚠️ **Sem internet, a tela não destrava.** O PIN é conferido no servidor. Isso é deliberado: um PIN validado só no aparelho seria contornável. Mas repare: o guardião é uma tela comum, o botão HOME continua saindo dela. Não destravar significa **não concluir a desinstalação**, não ficar preso no aparelho.

> ⏱️ **Janela de configuração:** nos primeiros 10 minutos após a proteção ser armada, o guardião fica desligado. Sem isso ele expulsaria da tela de acessibilidade justamente quem está terminando de configurá-lo.

O guardião depende da permissão de **Acessibilidade**. Sem ela, a criança consegue desinstalar o app, mas você é avisado quando o aparelho parar de dar sinal.

14 Alertas

A aba **Alertas** concentra tudo o que exige sua atenção, por severidade:

`Crítico: ação imediata` `Alto: risco alto` `Médio: atenção` `Baixo: risco baixo` `Informativo: sem ação necessária`

Toque num alerta para ver detalhes e ações. Alertas de risco infantil também disparam **notificação no celular** e, em casos graves, **WhatsApp** para o responsável.

Tipos de alerta

TIPO	ORIGEM
Mensagem de risco	WhatsApp, Telegram, SMS, navegação
Imagem explícita	Galeria e fotos baixadas
Arquivo suspeito	App baixado fora da loja
Vazamento de dados	Seus dados monitorados
Aparelho sem contato	Supervisão offline há mais de 8h
Ação na família	Supervisão desligada, membro removido

Resolvido ou Não é um alerta

No fim de cada alerta de detecção (mensagem, imagem, arquivo, pagamento, site de golpe, vazamento) há dois botões. **Resolvido** diz que o alerta estava certo e você já cuidou: ele continua no histórico, marcado, e um alerta sobre o seu filho segue pesando na Proteção da Família até completar 30 dias. **Não é um alerta** diz que foi um engano (uma foto de bebê classificada como nudez, por exemplo). Nesse caso:

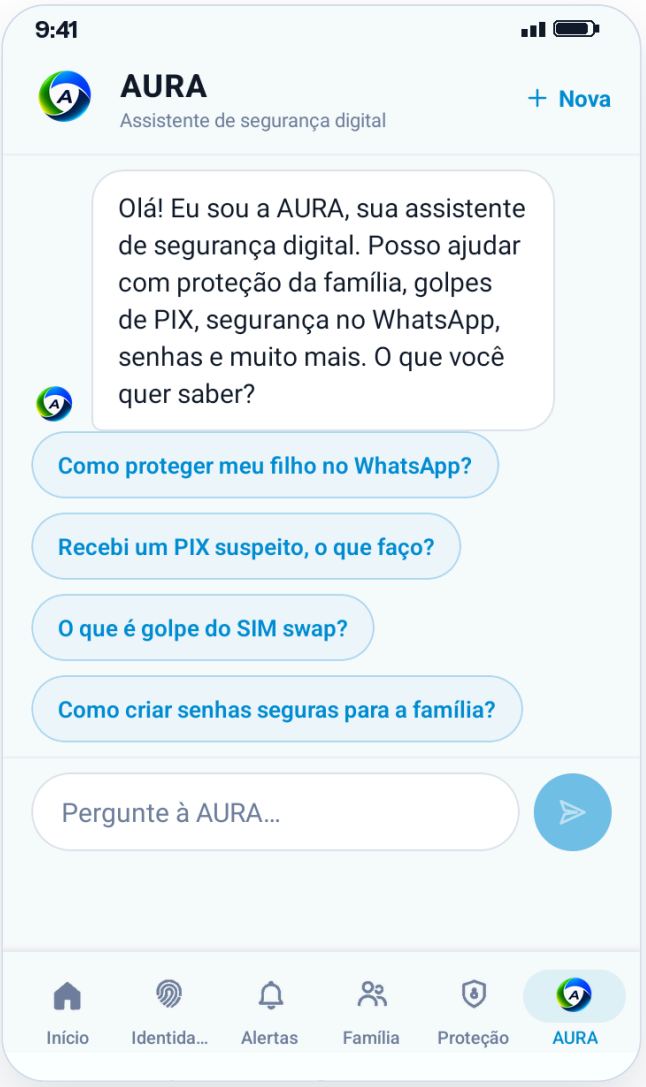
- O alerta **deixa de contar como ameaça** e sai da Proteção da Família **na hora**, sem esperar os 30 dias;
- Se era uma mensagem, uma imagem ou um arquivo, **aquele mesmo item não gera alerta de novo**. Pagamentos e sites de golpe avisam de novo numa próxima tentativa, porque ela pode ser diferente.

Os dois vereditos alimentam o treino do classificador. É a forma mais direta de o produto melhorar para a sua família. Mudou de ideia? Toque em **Desfazer** no mesmo alerta. Avisos de funcionamento (aparelho sem contato, filtro desligado, contato novo) não têm os botões: eles não são uma detecção a avaliar.

Na Identidade Digital, o detalhe de um vazamento tem o mesmo par: **Marcar como resolvido** (ele deixa de pesar no seu nível de proteção) e **Não é um alerta** (ele sai da lista e da nota, e a varredura não o traz de volta). O alerta do vazamento e a linha da Identidade são o mesmo fato: avaliar num lugar vale no outro. Os vazamentos marcados como não é um alerta ficam em **Marcados como não é um alerta**, no fim da lista, com **Desfazer** a qualquer hora. Quando a primeira varredura acha muitos vazamentos de uma vez, o alerta é um resumo: avalie cada um na Identidade Digital.

🔁 **O mesmo item não alerta duas vezes.** Mensagens, imagens e arquivos são reconhecidos por uma impressão digital técnica: reabrir o app ou reprocessar a fila não gera aviso repetido.

15 AURA, a assistente de segurança



ABA AURA

A AURA responde dúvidas de segurança digital, orienta em incidentes e indica o caminho no app:

- **No app:** aba AURA. Converse em linguagem natural.
- **No WhatsApp:** no número oficial do ARMOR, um menu automático responde primeiro, e a AURA responde o que ele não reconhece. Para registrar um chamado para a equipe, escreva *atendente* e informe o e-mail da conta.

📱 Convites de família e alertas importantes também chegam pelo WhatsApp oficial do ARMOR.

🔒 O chat da AURA envia o que você escreve a um provedor de inteligência artificial contratado, só depois do seu aceite no app, e a conversa fica no servidor do ARMOR por até 4 horas depois da última resposta. Uma pergunta com sinal de risco também passa pela análise do ARMOR e pode virar um alerta na sua lista, com notificação. No WhatsApp não há o aviso prévio do app: escrever para o número já inicia a conversa. Não escreva senhas, números de cartão nem dados que identifiquem seu filho. Detalhes na Política de Privacidade.

16 Planos e assinatura

PLANO	PARA QUEM	DESTAQUES
Grátis	1 responsável e 1 membro da família	1 e-mail monitorado
Essencial R$ 24,90/mês ou R$ 249/ano	até 5 membros	3 e-mails, 1 CPF e 1 celular monitorados
Plus R$ 39,90/mês ou R$ 399/ano	até 6 membros	5 e-mails, 3 CPFs e 3 celulares monitorados
Blindada R$ 99,90/mês ou R$ 999/ano	até 8 membros	E-mails, CPFs e celulares sem limite, SOS com localização acompanhado pela equipe do ARMOR e canal para furto de identidade

📋 **Em todos os planos, no app de teste:** filtro de sites e bloqueio de sites de golpe, horários, limites e bloqueios, alertas de mensagens e imagens no Android do filho, guarda de pagamentos (em validação), Verificar mensagem, Guarda de Pix e a AURA. A divisão final dos recursos entre os planos será publicada antes do lançamento.

Como funciona a assinatura

- 🛒 **Pela loja:** a assinatura será feita dentro do app, pela Google Play ou pela App Store, quando o ARMOR chegar às lojas. No app de teste os planos aparecem, mas ainda não podem ser assinados. Depois, a assinatura renova sozinha a cada período.
- 🎁 **Teste grátis:** quando a loja oferecer teste grátis no plano, a própria tela da loja mostra a data da primeira cobrança.
- 🔁 **Trocar de plano:** quando quiser; a loja mostra o valor e o crédito proporcional antes de confirmar.
- 🚫 **Cancelar:** na sua conta da loja (Play Store → Pagamentos e assinaturas, ou Ajustes do iPhone → seu nome → Assinaturas). O acesso continua até o fim do período já pago.
- 📅 **Plano anual:** equivale a ~2 meses grátis.

Cancelar

Em **Perfil → Ver planos e assinatura → Cancelar assinatura**. Você mantém os recursos até o fim do período já pago.

🆘 O **SOS** (um caso aberto para a equipe do ARMOR, com a sua localização quando você permite) é exclusivo do plano Blindada. Não é serviço de emergência nem atendimento 24 horas: em risco imediato, ligue 190 ou 192.

17 Perfil e conta

- **Dados pessoais:** nome, e-mail, telefone e CPF. Edite em **Editar**. O telefone pede confirmação em caixa dupla.
- **Foto:** quem entra com Google já vê a própria foto; senão, mostramos a inicial do nome.
- **Exportar dados (LGPD, art. 18):** o ARMOR envia um arquivo com os seus dados para o e-mail da conta.
- **Sair da conta:** encerra a sessão neste aparelho e **cancela o envio de notificações** para ele.

📲 **Você pode usar a conta em vários aparelhos** (celular e tablet, por exemplo) e **todos** recebem os alertas. Um aparelho supervisionado nunca vira destino dos seus alertas, mesmo que você tenha entrado com sua conta nele antes de pareá-lo.

18 Privacidade e LGPD

- **A análise começa no aparelho.** Mensagens e fotos passam primeiro por modelos embarcados. Só a mensagem com sinal de risco vai ao servidor do ARMOR para conferência, com o nome de quem mandou, e o texto é descartado depois da análise; o alerta guarda a categoria, a gravidade, os sinais e o remetente, nunca o texto. A imagem nunca sai do aparelho: só o resultado da análise.
- O filtro de sites registra o **nome do site**, o horário e a categoria, nunca o conteúdo das páginas. A análise do navegador, no Android acompanhado com a Acessibilidade ligada, envia o endereço e um trecho do texto só da busca ou da página com sinal de risco.
- O menor **sabe** o que está ativo: lê e aceita no aparelho dele antes de a supervisão começar (a LGPD exige o consentimento do responsável; o aceite da criança é escolha do ARMOR) e tem uma tela dedicada mostrando as regras que valem para ele.
- A agenda do Android do filho fica no servidor com nome e número, visível só para você; a lista manual de contatos confiáveis é guardada como **hash**. Dados monitorados aparecem **mascarados**.
- Você pode **exportar ou excluir** seus dados a qualquer momento.

Detalhes: Política de Privacidade · LGPD · Termos de Uso.

19 Segurança infantil e denúncias

O ARMOR tem tolerância zero com abuso e exploração sexual infantil. Nossos padrões estão publicados em armor.app.br/seguranca-infantil.

Para denunciar, use o canal no app: **Suporte → Denunciar abuso ou exploração**. Ele vai pelo WhatsApp, disponível em **todos os planos**, com atalho para o **Disque 100**.

⚠️ **Não anexe o material.** Reencaminhar imagem de abuso sexual infantil é crime (ECA, art. 241-A) mesmo com intenção de denunciar, e nós não teríamos como recebê-la, já que a classificação acontece no aparelho e a imagem nunca sai dele. Descreva a situação; o que podemos entregar a uma autoridade são registros de conta e metadados do alerta.

20 Solução de problemas

O botão da Acessibilidade está cinza

Android 13+ com app fora da loja. Configurações → Apps → ARMOR → menu ⋮ → **Permitir configurações restritas**.

A proteção não volta depois de reiniciar o aparelho

Fabricante com gestão agressiva de energia (Xiaomi/MIUI, Oppo, realme, vivo, Samsung). Ative o **"Início automático"** nas configurações do fabricante. Não há como o app fazer isso sozinho.

Marquei uma categoria e o site continua abrindo

- Confira se o item ficou marcado: o marcador só fica verde quando o servidor confirma.
- Site já aberto continua carregando por alguns segundos; feche a aba e abra de novo.
- Confirme que a **Proteção de rede** está ativa no checklist do aparelho dela.
- Categorias diferentes cobrem coisas diferentes: YouTube é **Streaming**, não "Jogos".

O limite de tempo não está travando

Confira o item **Acesso ao uso** no checklist do aparelho do menor. Sem ele o app não consegue contar minutos, e os limites (diário e por app) simplesmente não valem, mesmo configurados.

Não recebo notificações no meu celular

- Confirme que o app tem permissão de notificação no **seu** aparelho.
- Se você entrou com sua conta no celular da criança, isso não rouba mais os alertas do seu, mas confirme que o seu aparelho aparece na conta abrindo o app nele uma vez.

Fotos claramente impróprias não geraram alerta

- Confira **Acesso às fotos** no checklist. No Android 14, escolher "Selecionar fotos" em vez de "Permitir tudo" faz o app não enxergar a galeria.
- Fotos anteriores à instalação **não são varridas**: só o que chega depois.
- Se o app foi atualizado recentemente, use **Revarredura de fotos** no Controle do Dispositivo.

O aparelho aparece offline no painel

O app do menor não está rodando. Abra-o no aparelho dela e confira o checklist. Se voltar a acontecer, é quase sempre o "Início automático" do fabricante.

21 Perguntas frequentes

▼ O ARMOR lê as conversas do meu filho?

Lê as mensagens recebidas pelas notificações, primeiro **dentro do aparelho dele**, por um modelo de IA embarcado no app, e apenas para classificar risco. Mensagem sem sinal de risco **não sai do aparelho**. Quando a análise local vê risco, só aquele trecho vai ao nosso servidor para conferência e é descartado em seguida: **não fica guardado**. O que chega a você é o veredito ("aliciamento", "golpe do Pix"), a gravidade, os sinais e quem mandou, nunca a conversa.

▼ Vocês guardam as fotos da galeria?

Não. A imagem é classificada no próprio aparelho e nunca é enviada. O alerta carrega a categoria, a pontuação e uma impressão digital técnica que serve só para não alertar duas vezes sobre a mesma foto.

▼ Funciona no iPhone?

Parcialmente. O filtro de sites vale pelo perfil de configuração. Com o app em validação num iPhone com iOS 16, horários, limite diário, pausa dos apps e trava de instalação valem pelo Tempo de Uso da Apple, sem travar a tela. Análise de mensagens e varredura de imagens não existem no iPhone: o iOS não abre esses recursos para apps de terceiros. Quem protege mensagens e fotos lá é a própria Apple, na Conta de Criança.

▼ A criança consegue desinstalar o app?

Com a Acessibilidade concedida, o guardião intercepta a tentativa e exige o PIN do responsável, que é gerado no seu celular, de uso único e com prazo. Sem a Acessibilidade, o guardião não roda. Em aparelho dedicado (dono do dispositivo), a remoção exige o responsável de qualquer forma. Em todos os casos, você é avisado se o aparelho parar de dar sinal.

▼ Ela pode burlar mudando a data do celular?

Em geral, não. O app mantém um relógio próprio, ancorado no nosso servidor e contado a partir do tempo de funcionamento do aparelho, que não muda quando alguém mexe na data. Vale para horários, limite diário e tempo bônus, inclusive offline. Exceções: depois de reiniciado sem internet, o aparelho só impede voltar a data até a próxima conexão; e o limite por tipo de app ainda conta o dia pela data do aparelho.

▼ E se ela ficar sem internet?

Os bloqueios por horário, o horário escolar, o quadro e os limites continuam valendo: as regras da última conexão ficam guardadas no aparelho. Comandos novos (travar a tela, liberar, aprovar mais tempo) só chegam com internet, e com o app fechado o bloqueio de tela manual não é reaplicado sem conexão. O envio dos alertas também espera a conexão: o que for detectado sem internet fica guardado no aparelho e sai quando a proteção volta a rodar, com a hora em que foi detectado.

▼ Preciso desligar a proteção para mexer no celular dela?

Não. Digite sua senha no aparelho dela e abre uma sessão de responsável de 30 minutos com o painel completo, sem derrubar a supervisão. Ou gere um PIN de 6 dígitos no seu celular, se preferir não digitar a senha na frente dela.

▼ Por que preciso confirmar meu telefone duas vezes?

Porque é o número que recebe os alertas de segurança sobre a sua criança por WhatsApp. Um dígito errado significa que um estranho passa a receber esses avisos, e você, não.

▼ Recebi um alerta que era besteira. E agora?

Abra o alerta e toque em **Não é um alerta**. Aquele item para de alertar, o peso sai da Proteção da Família na hora, e seu veredito ajuda a melhorar a detecção. Dá para desfazer.

▼ Posso trocar de plano quando quiser?

Pode, quando quiser. A troca é feita pela loja, que mostra o valor antes de confirmar. Na **Google Play** a troca vale na hora e o tempo já pago vira crédito proporcional no plano novo. Na **App Store**, subir de plano vale na hora (a Apple devolve a diferença proporcional) e descer vale na próxima renovação. Durante o teste grátis a troca é livre nos dois sentidos.

▼ O convite expirou ou deu erro. E agora?

Peça o reenvio pela aba Família, ou use o código de 6 dígitos em Proteção → Dispositivos → 🔑 Código. Os dois caminhos chegam ao mesmo lugar, e o código pode ser gerado quantas vezes quiser.

▼ O que acontece se eu remover um membro da família?

O vínculo, os aparelhos supervisionados dele e os registros associados são removidos. Os alertas históricos da sua conta são preservados. Se você só quer tirar um aparelho, use Excluir no próprio aparelho.

▼ Meu filho aceitou e depois se arrependeu. Dá para desfazer?

Sim. Pause ou exclua o aparelho a qualquer momento em Proteção → Dispositivos. A supervisão é um acordo entre vocês, não uma armadilha.

22 Suporte

- **No app:** aba **Suporte**. No plano Blindada, abra um chamado e acompanhe as respostas da equipe; nos outros planos, o botão leva ao WhatsApp do ARMOR.
- **WhatsApp do ARMOR:** um menu automático responde primeiro, e a AURA responde o que ele não reconhece. Para registrar um chamado para a equipe, escreva

atendente e informe o e-mail da conta. Para falar com a equipe por e-mail: **contato@armor.app.br**.

- **Denúncia de abuso infantil:** Suporte → **Denunciar abuso ou exploração** (todos os planos).
- **Site:** **central de ajuda** e **página de contato**.
- **Plano Blindada:** botão **SOS** na aba Suporte, que abre um caso para a equipe do ARMOR, com sua localização quando você autorizar. Não é serviço de emergência.

🆘 Em risco imediato à vida, ligue **190** (Polícia) ou **192** (SAMU). Para crimes contra crianças e adolescentes, **Disque 100**.

© 2026 ProTech-T · PROTECH/T TECNOLOGIA E SEGURANCA LTDA · CNPJ 68.149.598/0001-19