



**INTERNET SEGURA**  
**PARA SEUS FILHOS**  
**2ª EDIÇÃO**

SUA PARTICIPAÇÃO É MUITO IMPORTANTE!

Realização: **cert.br nic.br cgi.br**

Apoio de Divulgação: **gov.br**

## PRODUÇÃO:

### CERT.BR

(Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil)

### NIC.BR

(Núcleo de Informação e Coordenação do Ponto BR)

### CGI.BR

(Comitê Gestor da Internet no Brasil)

## COORDENAÇÃO GERAL:

Cristine Hoepers

## REDAÇÃO:

Miriam von Zuben

## ILUSTRAÇÕES:

Hector Gomez e Shutterstock

## PROJETO GRÁFICO E EDITORAÇÃO:

Maricy Rabelo, Klezer Uehara, Giuliano Galvez

## REVISÃO E CONTRIBUIÇÃO:

André Lucas Fernandes, Caroline D'Avo, Evelyn Eisenstein (Rede ESSE Mundo Digital), Everton Teles Rodrigues, Helena Martins, Jorge Luiz Pinto de Souza (EMPREL), Leandro Morales B. Stefano, Marcelo H. P. C. Chaves, Maria Sílvia Lordello Marques, Raquel Lima Saraiva, Rodrigo Nejm (Equipe SaferNet Brasil)



Esse guia está disponível em <https://internetsegura.br/>  
Caso queira receber uma cópia impressa, tenha sugestões ou encontre erros, envie e-mail para [doc@cert.br](mailto:doc@cert.br)



ATRIBUIÇÃO-NÃO COMERCIAL-SEM DERIVAÇÕES 4.0 INTERNACIONAL (CC BY-NC-ND 4.0)

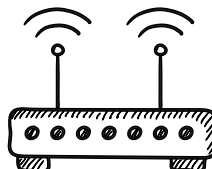
### VOCÊ TEM O DIREITO DE:

- Compartilhar — copiar e redistribuir o material em qualquer suporte ou formato

### DE ACORDO COM OS TERMOS SEGUINTE:

- ATRIBUIÇÃO**  
Você deve dar o crédito apropriado, prover um link para a licença e indicar se mudanças foram feitas. Você deve fazê-lo em qualquer circunstância razoável, mas de maneira alguma que sugira ao licenciante a apoiar você ou o seu uso.
- USO NÃO COMERCIAL**  
Você não pode usar o material para fins comerciais.
- SEM DERIVAÇÕES**  
Se você remixar, transformar ou criar a partir do material, você não pode distribuir o material modificado.

[https://creativecommons.org/licenses/by-nc-nd/4.0/deed.pt\\_BR](https://creativecommons.org/licenses/by-nc-nd/4.0/deed.pt_BR)



## HISTÓRICO DE VERSÕES:

Fevereiro/2017 - Primeira Edição  
Outubro/2022 - Segunda Edição

# PROTEJA SEUS FILHOS,

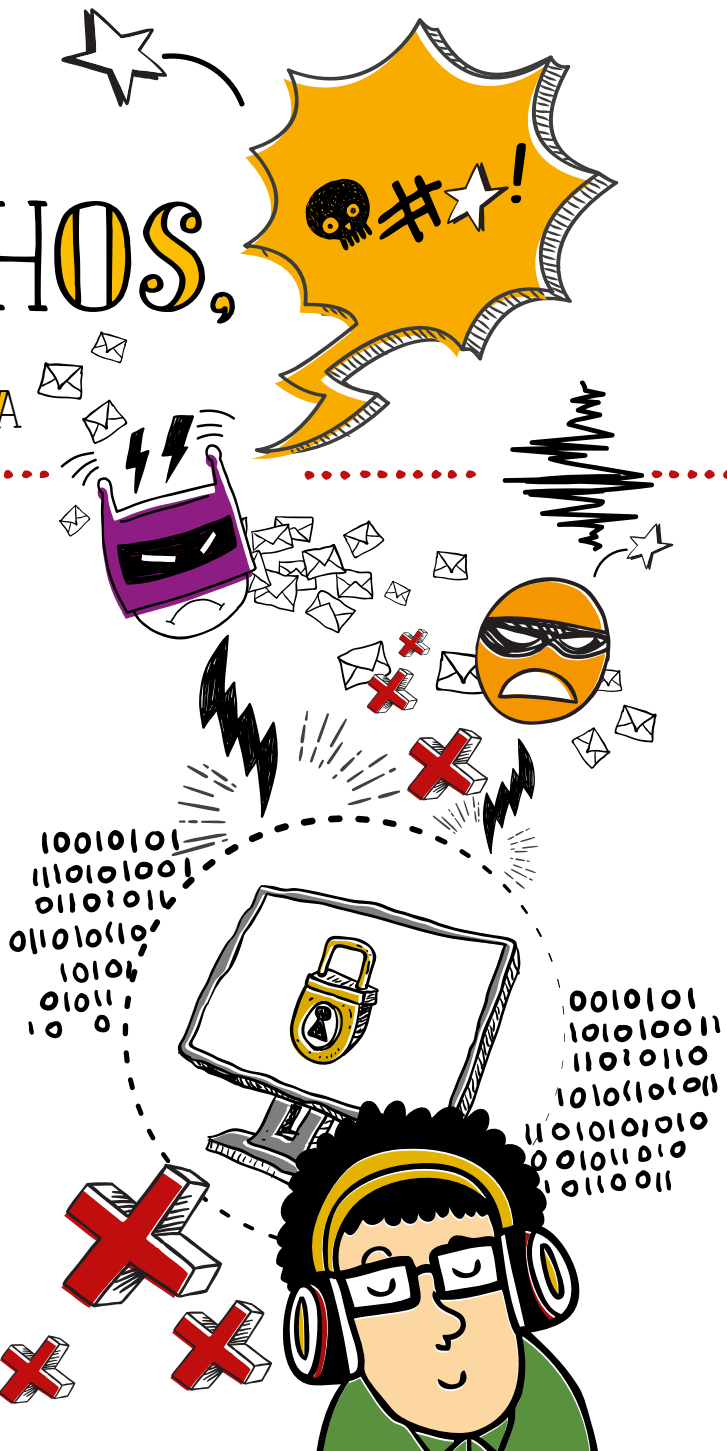
## ENSINE-OS A USAR A INTERNET COM SEGURANÇA

Da mesma forma como você orienta seus filhos para não conversar com estranhos e olhar para os dois lados ao atravessar a rua, também precisa alertá-los sobre os perigos na Internet.

Como fazer isso? **A MELHOR PREVENÇÃO É A INFORMAÇÃO**, conhecendo os riscos mais facilmente seus filhos conseguirão se prevenir.

Pensando nisso, criamos o **GUIA INTERNET SEGURA**, com dicas para que as crianças possam aprender de forma divertida a se proteger. Você pode acessá-lo em [HTTPS://INTERNETSEGURA.BR/](https://internetsegura.br/).

Nesse processo de aprendizagem acreditamos que a participação da família é essencial. Assim, criamos também esse guia complementar com dicas e sugestões para que vocês – pais e responsáveis – possam orientar seus filhos a usar a Internet com mais segurança.



# CONHEÇA OS RISCOS



A Internet tem qualidades inegáveis e bastante conhecidas. A cada dia novas possibilidades surgem e muito ainda está por vir.

Sem deixar de reconhecer todas as coisas boas que a Internet oferece aos seus filhos, é importante lembrar que ela não tem nada de virtual e apresenta situações de riscos que você precisa conhecer.



O uso excessivo da

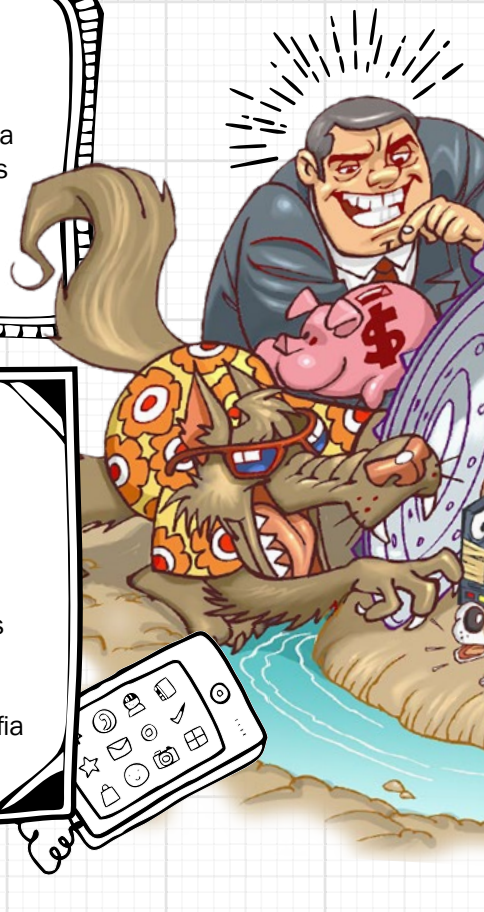
Internet pode colocar em risco a saúde física e psicológica dos seus filhos, atrapalhar o rendimento escolar e afetar a vida social.



Ao navegar na Internet seus filhos podem ter acesso a conteúdos impróprios, falsos, incompletos ou ofensivos, como boatos, correntes, pornografia e violência. Filtrar essas informações exige senso crítico e, dependendo da idade e da maturidade dos seus filhos, eles podem não estar preparados para isso.



Algumas pessoas se aproveitam da falsa sensação de anonimato da Internet para se aproximar de crianças e cometer crimes, como aliciamento, chantagem, pornografia infantil e sequestro.





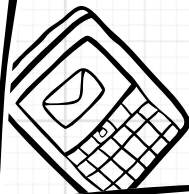
A divulgação de informações pessoais sobre seus filhos pode comprometer a privacidade deles, assim como eles podem postar informações que comprometam a privacidade da família e dos amigos.



Fotos e vídeos dos seus filhos podem “viralizar” e, rapidamente, eles podem se tornar “webcelebridades”, terem as vidas superexpostas ou, ainda, serem ridicularizados em função disso.



Aquilo que é divulgado na Internet pode se espalhar rapidamente e dificilmente ser excluído. Fotos e vídeos dos seus filhos poderão estar disponíveis mesmo quando eles já forem adultos.



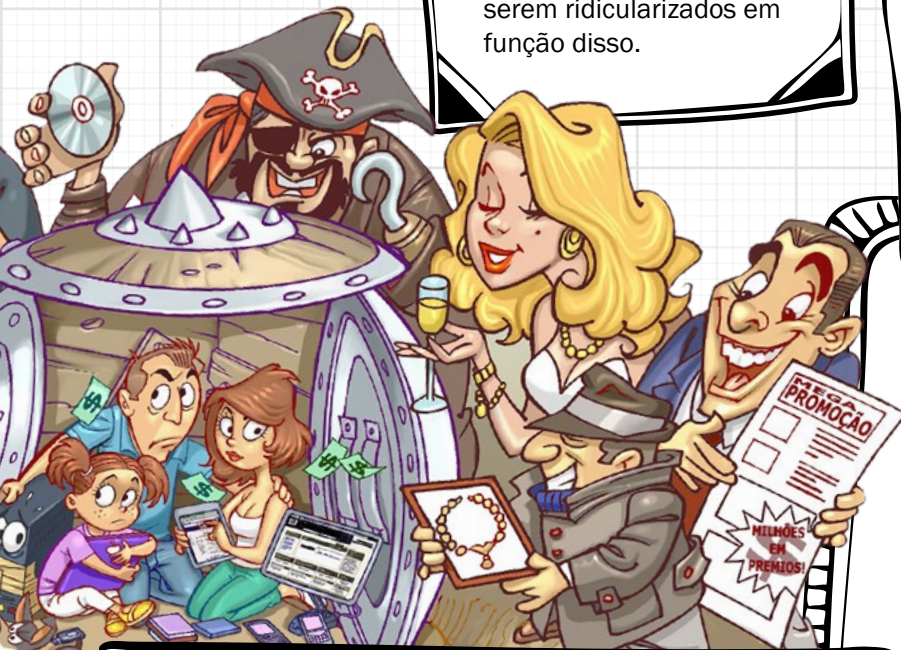
Seus filhos podem ser vítimas de *cyberbullying* ou acusados de tal prática, caso postem, curtam ou compartilhem fotos, vídeos e mensagens difamando e humilhando os colegas.



Crianças ainda estão em período de formação de personalidade, não possuem maturidade emocional e não sabem lidar com a opinião ou o desprezo dos demais. Imagens dos seus filhos postadas podem gerar neles a expectativa de como serão recebidas e poderá ser frustrante caso elas não sejam “curtidas” ou, ainda, caso recebam comentários negativos.



Os equipamentos usados por seus filhos podem ser infectados por códigos maliciosos (*malware*), o que pode levar à perda de dados e ao acesso não autorizado às informações pessoais.



# NÃO SEJA VOCÊ O VILÃO

ALGUNS DOS RISCOS QUE AS CRIANÇAS ENCONTRAM NA INTERNET SÃO CRIADOS PELA PRÓPRIA FAMÍLIA QUE, GERALMENTE POR INGENUIDADE E DESCONHECIMENTO DOS PERIGOS, AS EXPÕE EXCESSIVAMENTE.

## VOCÊ JÁ CRIOU PERFIS EM NOME DOS SEUS FILHOS?

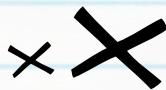
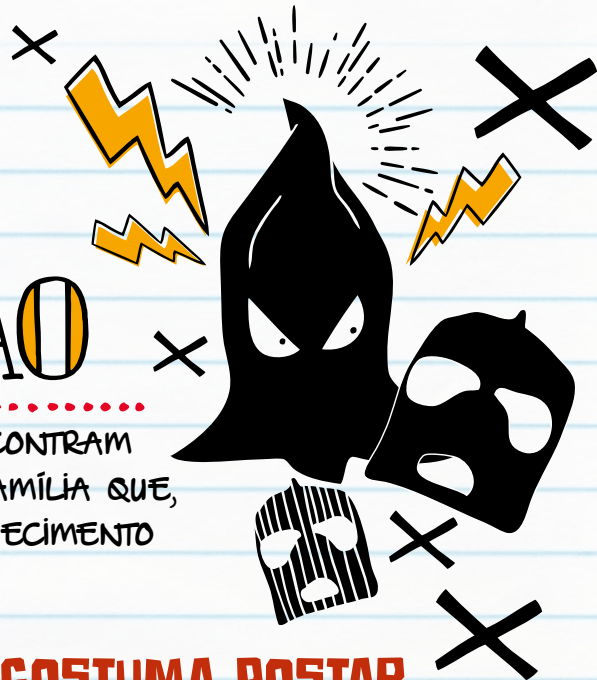
Alguns pais criam perfis em nome dos filhos, postam sobre eles e até interagem como se as próprias crianças estivessem fazendo aquilo. Tem criança que ainda nem nasceu mas já possui perfil nas redes sociais. Você já imaginou como essas crianças se sentirão lendo opiniões que não foram emitidas por elas? Como será possível diferenciar no futuro o que elas postaram daquilo que alguém postou em nome delas?

**LEMBRE-SE QUE ALGUMAS REDES SOCIAIS TÊM IDADE MÍNIMA PARA CRIAÇÃO DE CONTAS.** Se os próprios pais, que costumam ser o exemplo para os filhos, não obedecem às regras, como poderão cobrar dos filhos mais tarde?

## VOCÊ COSTUMA POSTAR MENSAGENS NAS REDES SOCIAIS DOS SEUS FILHOS?

Aquilo que é privado, típico da relação familiar, não precisa ser postado nos perfis dos seus filhos. Respeite a privacidade, a individualidade e a intimidade deles. A criança deve ter o direito de não querer ser exposta e de construir ela própria o seu espaço na Internet, de acordo com o amadurecimento da sua personalidade e da educação sobre o uso das tecnologias.

Evite postar mensagens chamando-os por apelidos usados somente entre vocês ou tratando-os de forma infantil. Não dê broncas e nem os repreenda por meio das redes sociais. Converse antes sobre a publicação de alguma foto ou conteúdo familiar. **LEMBRE-SE QUE A INTERNET É UM LUGAR PÚBLICO E, COMO DIZ O DITADO, "ROUPA SUJA SE LAVA EM CASA".**





## VOGÊ COSTUMA POSTAR FOTOS E VÍDEOS DOS SEUS FILHOS?

Você já parou para pensar até onde vai o seu direito em expor a privacidade dos seus filhos? Onde começa o direito deles de não querer ser expostos pelos pais? A partir de qual idade eles passam a ter direito à própria privacidade?

Aquilo que você considera “bonitinho”, eles podem considerar constrangedor, e ainda ser usado para a prática de *bullying* contra eles. Lembre-se que o contexto familiar é privado.

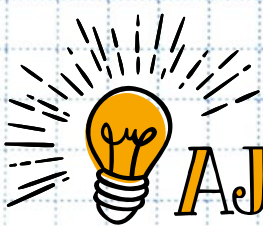
Além disso, a foto dos seus filhos nus ou seminus, tomando banho ou brincando na praia, pode ser algo inocente para você, mas essa mesma foto pode ser usada por redes de pedofilia para exploração sexual comercial. Dessa forma, **EVITE COMPARTILHAR FOTOS ONDE SEUS FILHOS APAREÇAM COM POUCA ROUPA.**

Expor os hábitos dos filhos (onde estudam, quais cursos participam, locais que frequentam) pode colocá-los em risco de serem sequestrados. Há diversos casos noticiados de sequestros de crianças que foram planejados com informações obtidas por redes sociais. Assim, **EVITE POSTAR FOTOS QUE EXPONHAM A ROTINA DOS SEUS FILHOS.**

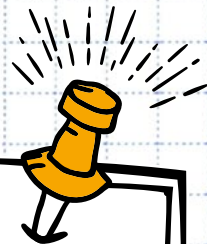
Existem também os “sequestradores digitais” que usam informações reais de crianças para criar perfis falsos e interagir com outras pessoas. Em alguns casos eles até comentam e compartilham as fotos como se fossem eles os verdadeiros pais da criança.

Para evitar isso, **TENHA CUIDADO AO ACEITAR ESTRANHOS NAS SUAS REDES SOCIAIS E UTILIZE AS CONFIGURAÇÕES DE PRIVACIDADE PARA RESTRINGIR QUEM PODE ACESSAR AS SUAS POSTAGENS.**





# AJUDE SEUS FILHOS A SE PROTEGEREM



SUA AJUDA É MUITO IMPORTANTE. CONFIRA ALGUMAS DICAS PARA QUE VOCÊ ORIENTE SEUS FILHOS A USAR A INTERNET COM MAIS SEGURANÇA.



## DÊ O EXEMPLO

Os pais costumam ser a primeira referência comportamental das crianças e é natural que elas copiem deles os hábitos e as atitudes. **MAS DE NADA ADIANTA DAR CONSELHOS SE AS ATITUDES NÃO CORRESPONDEREM AO QUE ESTÁ SENDO DITO.**

Como cobrar dos seus filhos um comportamento que você não tem? Se você faz as refeições navegando na Internet, se está sempre olhando as redes sociais enquanto conversa, se nunca tem tempo para brincar mas encontra tempo para mandar mensagens que não são urgentes, seus filhos provavelmente farão o mesmo.

## ESTIMULE O DIÁLOGO

Não adianta impedir que seus filhos acessem à Internet, pois eles poderão fazer isso escondidos. Proibições geralmente geram conflitos e atrapalham o diálogo. Por isso, esteja presente no dia a dia, tente conversar sobre as diversas possibilidades que a Internet oferece e deixe que eles falem sobre as experiências deles.

Aproveite também para tirar dúvidas, pois assim você pode indicar que há um canal de diálogo aberto entre vocês.

Ao mostrar-se interessado, será mais fácil descobrir se eles precisam de ajuda, se estão tendo algum problema ou se algo os está incomodando. **NAVEGAR JUNTO COM SEUS FILHOS PODE SER MUITO DIVERTIDO E EDUCATIVO.**

Procure estimulá-los a compartilhar com você as experiências desagradáveis que tiverem. Para isso, tente montar cenários, citar problemas já ocorridos ou aproveitar oportunidades, como casos que estão sendo noticiados e comentados. Isso os ajudará a entender os problemas, observar as consequências e servirá como alerta para que não passem pelas mesmas situações ou para que saibam como reagir.

**LEMBRE-SE QUE O DIÁLOGO EDUCATIVO, ABERTO E FRANCO É SEMPRE A MELHOR PROTEÇÃO QUE SEUS FILHOS PODEM TER DIANTE DOS DESAFIOS DA CONVIVÊNCIA EM SOCIEDADE.**





## REFORCE OS CUIDADOS QUE SEUS FILHOS DEVEM TER COM ESTRANHOS

Não há dúvidas que a Internet ajuda a aproximar as pessoas distantes e reforçar os vínculos de amizade, mas ela também facilita o contato com pessoas desconhecidas de todo tipo. Algumas até podem ser bem intencionadas mas outras se aproveitam da falsa sensação de anonimato da Internet para tentar se aproximar de crianças e cometer crimes.

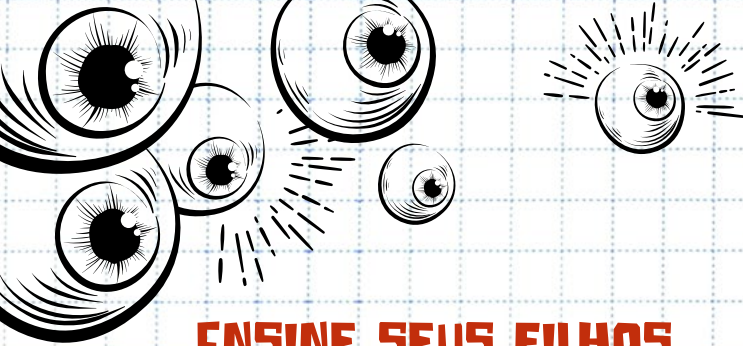
Infelizmente muitas crianças são iludidas e acabam se encontrando pessoalmente com desconhecidos e, sem que tenham noção, ficam expostas a grandes perigos. **ORIENTE SEUS FILHOS PARA JAMAIS MARCAR ENCONTROS COM PESSOAS ESTRANHAS OU QUE CONHECEM APENAS DA INTERNET.**



## OBSERVE O COMPORTAMENTO DOS SEUS FILHOS

Se você tiver um computador em sua casa, procure mantê-lo em um local onde, mesmo à distância, consiga observar o comportamento dos seus filhos. Caso eles acessem à Internet usando equipamentos individuais, esse tipo de supervisão fica mais complicada mas, mesmo assim, há alguns indícios que podem ajudar.

Atitudes como minimizar ou fechar aplicativos, trancar a porta do quarto, bloquear o celular ou *tablet* e ficar nervoso quando você está por perto podem indicar que seus filhos estão tentando esconder algo e, possivelmente, correndo riscos. Esse é o momento para tentar conversar e entender o que está ocorrendo. A relação de confiança é o mais importante. **CONVERSE E OUÇA ANTES DE JULGAR, PARA QUE ELES NÃO TENHAM MEDO DE RELATAR ALGUM INCÔMODO.**

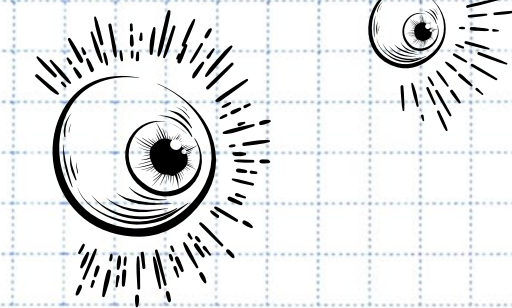
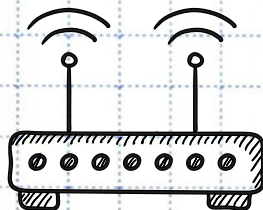


## ENSINE SEUS FILHOS SOBRE PRIVACIDADE

Converse com seus filhos sobre a importância de manter a privacidade e que informações pessoais, como endereço residencial e escola onde estudam, não devem ser compartilhadas.

**ORIENTE-OS PARA SELECIONAR O CÍRCULO DE AMIGOS NAS REDES SOCIAIS, NÃO ACEITANDO PESSOAS DESCONHECIDAS OU NÃO MUITO PRÓXIMAS.** Ajude-os a configurar o perfil para que as postagens sejam privadas, de forma que apenas os amigos consigam acessar. Ainda assim, eles precisam saber que a rede é pública e não tem como controlar quem é o amigo do amigo do conhecido... que também poderá ver, salvar o que for publicado e usar amanhã ou daqui a 5 anos.

**CONVERSE TAMBÉM SOBRE A NECESSIDADE DE PROTEGER A PRIVACIDADE DE OUTRAS PESSOAS,** não passando informações, como onde trabalham ou coisas que compraram, nem postando sem autorização fotos e vídeos em que outras pessoas aparecem.

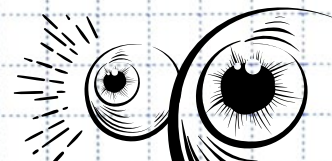


E sobre a privacidade das crianças, é adequado os pais terem as senhas e monitorarem o que elas fazem?

A resposta a essa questão é bastante polêmica e particular. Quando você era criança provavelmente não gostava que mexessem nas suas coisas ou ouvissem suas conversas mas, por outro lado, a exposição aos riscos talvez não fosse tão grande quanto é agora.

Assim como deve ter acontecido com você, a confiança dos seus pais foi conquistada aos poucos. Deixar que seus filhos naveguem sozinhos é similar a ter a chave da casa – no começo os pais se recusam a entregá-la aos filhos, depois a entregam mas com diversas recomendações, até que, por final, entregam uma cópia e já não se preocupam mais.

Enquanto que, no início, as crianças necessitam de supervisão constante para realizar as tarefas, com o tempo e com orientações, elas passam a ter autonomia e resolvem as coisas sozinhas. Quando e como ocorre essa transição depende do comportamento de cada criança e família.





## CUIDADO COM O CYBERBULLYING

Vítimas de *cyberbullying* costumam apresentar sintomas como depressão, baixa autoestima, ansiedade, agressividade, medo e sentimentos negativos. Também costumam ter problemas de rendimento escolar e passam a evitar a escola.

**FIQUE ATENTO SE SEUS FILHOS APRESENTAREM ESSES SINAIS E TENTE SE INFORMAR NA ESCOLA SE ALGO ESTÁ OCORRENDO.** Procure conversar com eles ou estimule para que falem com outras pessoas nas quais vocês confiem, como um irmão mais velho, tio, primo ou professor.

Caso algum dos seus filhos venha a cometer *cyberbullying* você, como representante legal, poderá ser responsabilizado.


**ENSINE-OS SOBRE A IMPORTÂNCIA DE RESPEITAR AS OUTRAS PESSOAS**, para não repassarem e nem criarem conteúdos humilhantes sobre os colegas e que brincadeira tem limite e pode ofender. Faça com que eles tentem se colocar no lugar da vítima e pensem se gostariam que fizessem aquilo com eles.



## FIQUE ATENTO AOS LIMITES DE IDADE

Diversos *sites* na Internet estipulam idade mínima para os seus usuários. Algumas redes sociais, por exemplo, só podem ser usadas por quem tem mais de 13 anos.

Quando crianças com idade inferior ao estipulado pelos *sites* mentem a idade para criar contas, elas ficam expostas a riscos, como o contato precoce com pessoas mal-intencionadas e o acesso a conteúdos considerados indevidos à sua faixa etária. Além disso, os pais podem ser responsabilizados, caso algo de ruim ocorra.





## ESTABELEÇA REGRAS

Desde os primeiros acessos estabeleça limites claros de uso da Internet, como após fazer a lição de casa, só nos finais de semana, algumas horas por dia e o horário limite de uso.

**OBSERVE QUE DE NADA ADIANTA CRIAR REGRAS MUITO RÍGIDAS E IRREAIS, POIS NÃO HÁ COMO CONTROLÁ-LAS O TEMPO TODO.** Mesmo que você use o recurso de Controle Parental (que verá mais adiante) para impor as regras, as crianças podem encontrar formas de burlá-las e elas não terão as mesmas restrições em outros equipamentos, como na escola ou na casa de amigos.

Por isso, é importante que as regras sejam previamente combinadas e justificadas, respeitando as necessidades da criança e preservando a sua saúde física e mental.



# UTILIZE O CONTROLE PARENTAL

APESAR DE NADA SUBSTITUIR O DIÁLOGO E A MEDIAÇÃO DOS PAIS, A TECNOLOGIA PODE SER USADA COMO ALIADA PARA AJUDAR A PROTEGER AS CRIANÇAS DOS RISCOS DA INTERNET.

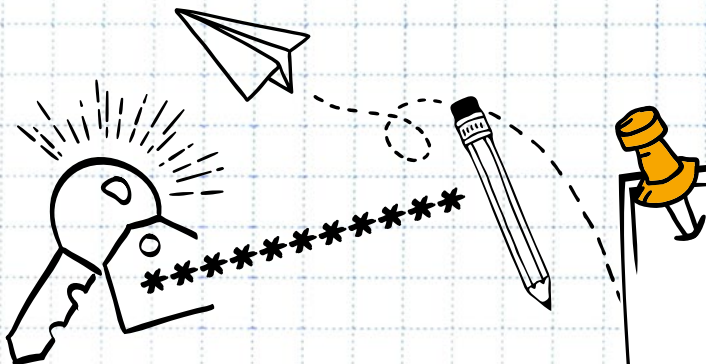
O Controle Parental (ou Controle dos Pais) é um conjunto de recursos de segurança disponível em diversos sistemas operacionais, sites e equipamentos, como roteadores e consoles de jogos. Também pode ser instalado por meio de aplicativos pagos ou gratuitos.

Os recursos do Controle Parental variam de acordo com a forma como são disponibilizados. Por exemplo:



- » **SITES DE PESQUISA:** permitem definir filtros de acordo com a classificação etária do conteúdo.
- » **SISTEMAS OPERACIONAIS:** permitem restringir os sites que as crianças podem (ou não podem) acessar, os aplicativos que elas podem executar, com quem elas podem se comunicar e definir limites de tempo, como o tempo máximo de uso por dia, horário de dormir e regras específicas para dias úteis e de finais de semana. Também impedem a troca de senha e mostram o histórico de atividades, incluindo sites visitados e aplicativos usados.
- » **LOJAS DO SISTEMA OPERACIONAL:** permitem definir o nível de classificação (livre ou por idade) para os aplicativos que as crianças podem comprar, baixar e instalar ou ainda para os filmes que elas podem assistir e livros que podem ler.
- » **USUÁRIOS E PERFIS RESTRITOS:** permitem criar tipos especiais de contas nas quais as atividades são restritas e supervisionadas.
- » **SERVIÇOS VIA ALTERAÇÃO DE DNS<sup>1</sup>:** permitem filtrar os sites acessados, por meio da alteração dos servidores de DNS configurados nos equipamentos que as crianças usam ou no roteador da rede residencial. Esses servidores possuem regras específicas para impedir o acesso a sites maliciosos ou restritos a menores de 18 anos (por exemplo, com conteúdo pornográfico).

<sup>1</sup> DNS (*Domain Name System*) significa sistema de nomes de domínios e é responsável pela tradução, entre outros tipos, de nome de máquinas/domínios para o endereço IP correspondente e vice-versa.



É importante que as crianças não conheçam a senha de administração dos equipamentos ou a especificada no serviço de Controle Parental, para que não consigam desabilitar a proteção.

Apesar de ser bastante útil, **O CONTROLE PARENTAL DEVE SER USADO COMO UMA PROTEÇÃO ADICIONAL**, já que pode apresentar falhas e não estar presente em todos os dispositivos e locais onde as crianças acessam à Internet, como a escola ou a casa dos amigos. Por isso, o bom e velho diálogo constante entre pais e filhos continua sendo essencial para ajudar as crianças a reconhecerem as situações de risco e tentar evitá-las.

**A MELHOR TECNOLOGIA AINDA É A CONSCIÊNCIA E O SENSO DE RESPONSABILIDADE.** Nenhum recurso de segurança conseguirá desenvolver essa maturidade e muito menos substituir o senso de autocuidado e de autoproteção, que vale para a vida em geral, o que inclui a Internet, os jogos e os aplicativos.

## **AJUDE SEUS FILHOS A PROTEGEREM AS CONTAS DE ACESSO**

Explique aos seus filhos sobre a importância de criar boas senhas, evitando senhas fáceis de serem adivinhadas, como “123456”, “abcd”, “asdf”, nome, sobrenome, data de nascimento, nome do cachorro ou do time preferido. O recomendável é que eles escolham senhas longas e habilitem a verificação em duas etapas.

Oriente-os para sempre saírem das contas de acesso quando usarem computadores de outras pessoas ou coletivos, como na casa de amigos, em bibliotecas e escolas, para que o próximo a utilizar não consiga acessá-las.



## PROTEJA OS EQUIPAMENTOS QUE SEUS FILHOS USAM


Os equipamentos usados por seus filhos podem ser infectados por códigos maliciosos (*malware*), que podem comprometer os dados gravados, ficarem lentos e pararem de funcionar. Por isso é importante que você tome alguns cuidados:

- » MANTENHA OS EQUIPAMENTOS SEGUROS, COM TODAS AS ATUALIZAÇÕES APLICADAS E OS APLICATIVOS INSTALADOS COM AS VERSÕES MAIS RECENTES.
- » INSTALE E MANTENHA ATUALIZADOS MECANISMOS DE SEGURANÇA, COMO ANTIVÍRUS E FIREWALL PESSOAL.



Alguns sistemas possuem recursos que permitem que o equipamento seja localizado à distância e que, para funcionarem, precisam que o serviço de localização esteja ativado. Ativar esse serviço pode ser bastante útil para o caso de perda ou furto do equipamento mas é necessário ter cautela.

Quando o serviço de localização está ativado, outros aplicativos, como de redes sociais, podem ter acesso ao local onde está a criança e postar automaticamente essa informação. Alguns sistemas permitem configurações específicas por aplicativo. Se você optar por ativar esse serviço, verifique quais aplicativos terão acesso à localização dos seus filhos e desabilite os que você não deseja.



# MANTENHA-SE INFORMADO

---



**INTERNET  
SEGURA**BR

Em <https://internetsegura.br/> você encontra, além deste material, também o guia criado especialmente para seus filhos



---

Confira ainda a Cartilha de  
Segurança para Internet



<https://cartilha.cert.br/>

