

Projecto Internet Segura

Segurança no Computador

## Índice

<b>1 - Projecto Internet Segura</b>	<b>3</b>
1.1 Visão	3
1.2 Missão	4
1.3 Estratégia	5
<b>Ligações Úteis</b>	<b>8</b>
<b>2 - Segurança no Computador</b>	<b>9</b>
2.1. Actualização do Sistema Operativo	9
2.2. Vírus	9
2.3. Antivírus, anti-spyware e firewall	11
2.4. Palavras-chave	11
2.5. Sair em segurança	12
2.6. Cópias de segurança	13
<b>Ligações Úteis</b>	<b>14</b>

# 1 - Projecto Internet Segura

---

## 1.1 Visão

A utilização das Tecnologias de Informação e Comunicação (TIC) tem transformado profundamente a maneira como as pessoas vivem, como aprendem, trabalham, ocupam os tempos livres e interagem, tanto nas relações pessoais como com as organizações.

A par de todas as possibilidades e benefícios da utilização das TIC, nomeadamente no acesso ao conhecimento, na colaboração entre pessoas e organizações, na inclusão social e na criação de riqueza, é necessário assegurar, como para qualquer outro meio de interacção, mecanismos e estratégias apropriados para minimização de eventuais abusos ou ilegalidades que ocorram com a utilização destas tecnologias.

A Comissão Europeia lançou em 1999 o programa *Safer Internet*, a que se seguiu em 2005 o programa *Safer Internet Plus*, com o objectivo de dinamizar projectos dos Estados Membros de promoção da utilização segura da Internet.

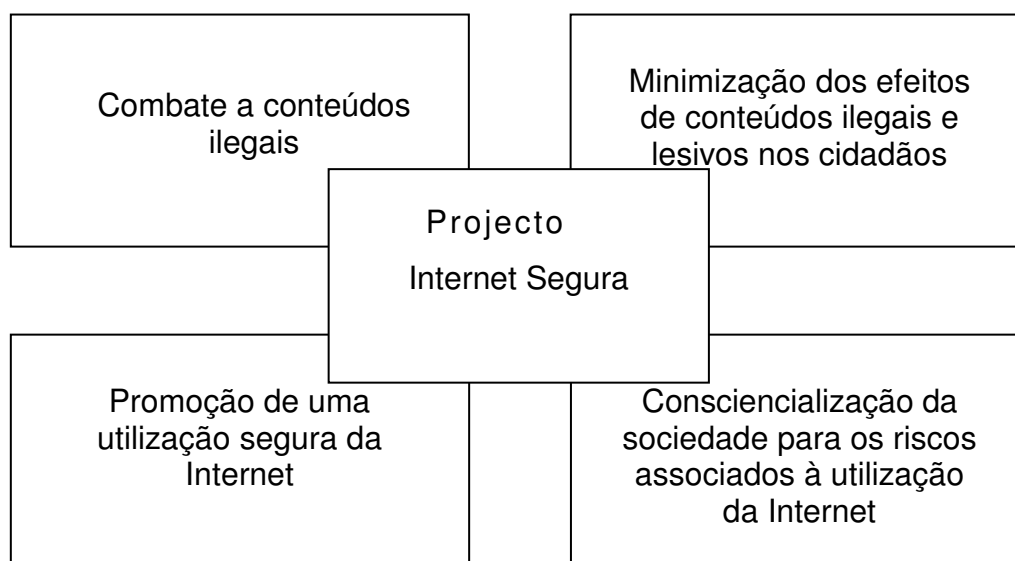
No âmbito do programa *Safer Internet*, a Direcção Geral de Inovação e Desenvolvimento Curricular, através da Equipa de Missão Computadores, Redes e Internet (DGIDC-CRIE) do Ministério da Educação, desenvolveu, em 2004, o projecto Seguranet, para a promoção de uma utilização esclarecida, crítica e segura da Internet junto dos estudantes do ensino básico e secundário.

Uma das orientações estratégicas do programa de acção LigarPortugal, adoptado pelo Governo em Julho de 2005, é "Assegurar a Segurança e a Privacidade no Uso da Internet", mais especificamente "garantir que todos, e em particular as famílias, dispõem de instrumentos para protecção de riscos que possam ocorrer no uso da Internet e têm informação sobre como os utilizar".

O projecto Internet Segura contribui para a concretização desta orientação estratégica. Este projecto é da responsabilidade de um consórcio coordenado pela UMIC – Agência para a Sociedade do Conhecimento e que também envolve a DGCI-CRIE, a Fundação para a Computação Científica Nacional – FCCN e a Microsoft Portugal. Após avaliação e aprovação da candidatura do projecto apresentada ao programa europeu *Safer Internet Plus*, o respectivo contrato entre o consórcio e a Comissão Europeia foi assinado em Junho de 2007.

O Projecto Internet Segura tem os seguintes objectivos estratégicos:

1. Combate a conteúdos ilegais;
2. Minimização dos efeitos de conteúdos ilegais e lesivos nos cidadãos;
3. Promoção de uma utilização segura da Internet;
4. Consciencialização da sociedade para os riscos associados à utilização da Internet.



## 1.2 Missão

Para cumprir os objectivos estratégicos do projecto Internet Segura foram identificados os seguintes objectivos operacionais:

1. Criação de um Conselho Consultivo, constituído por personalidades e entidades relevantes;
2. Criação de um serviço on-line para denúncia de conteúdos ilegais;
3. Disponibilização de informação sobre os perigos associados à utilização da Internet, tendo em conta diferentes públicos-alvo e suportes comunicacionais;
4. Disponibilização de conteúdos informativos, formativos e interactivos relevantes para a utilização segura da Internet;
5. Promoção do envolvimento do sector privado em acções que promovam a utilização da Internet em Segurança.

O projecto Internet Segura tem também uma missão internacional ao cooperar com duas entidades internacionais: *o Insafe e o Inhope*.

O Insafe é uma rede de cooperação dos projectos dos Estados Membros que promovem a sensibilização e consciencialização para uma utilização mais segura da Internet pelos cidadãos. Desde 2004 que Portugal integra o *Insafe* colaborando em eventos internacionais e na participação de Portugal nas actividades associadas ao Dia Europeu da Internet Segura.

O Inhope é uma Associação Internacional de linhas de atendimento de denúncias de conteúdos susceptíveis de serem considerados ilegais. A cooperação de todas as linhas de denúncia permite uma troca de informação mais eficaz no combate a conteúdos ilegais e ilícitos que se encontrem alojados em países fora da jurisdição do país onde os mesmos são comunicados. O *Inhope* presta ainda auxílio à instalação e desenvolvimento de novas linhas de denúncia como acontece com o caso português.

### 1.3 Estratégia

Em 2006, 36% da população portuguesa entre os 16 e 74 anos utilizou a Internet, com uma taxa de utilização de cerca de 80% entre as pessoas com o nível educacional secundário, 87% com o nível educacional superior e uma taxa de 96% de utilizadores entre os estudantes. De 17% de lares com ligações em banda larga em Dezembro de 2004, passou-se para 34% em Dezembro de 2006, o dobro em apenas dois anos.

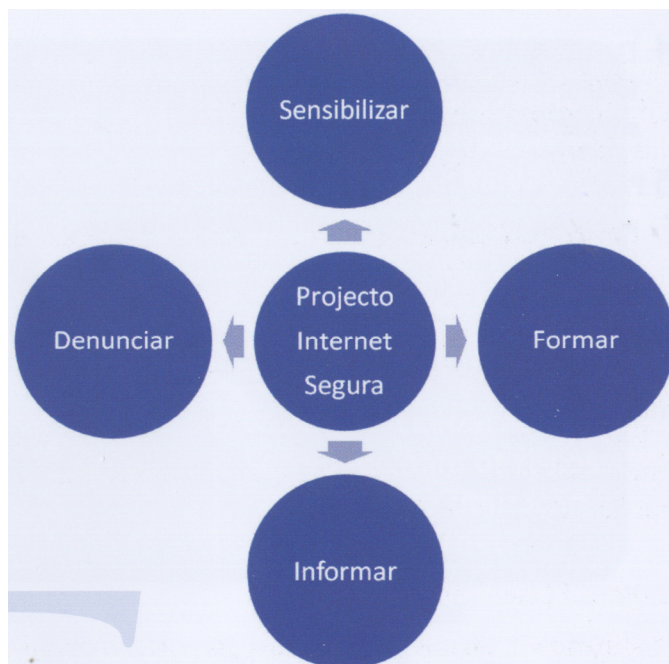
As actividades desenvolvidas com o recurso à Internet pelos cidadãos são diversificadas, nomeadamente actividades de comunicação, de pesquisa de informação e utilização de serviços on-line, comércio electrónico e acções de educação e formação. Dado que a utilização da Internet também pode envolver alguns riscos, a prevenção e a sensibilização da população para uma navegação mais segura e consciente da Internet é a melhor forma de evitar e mitigar potenciais problemas.

É, assim, fundamental adoptar uma estratégia positiva que contribua para a formação de uma sociedade mais esclarecida e consciente, capaz de se proteger de eventuais problemas na utilização da Internet.

O projecto Internet Segura tem quatro linhas de actuação principais:

1. Sensibilização para a importância da navegação na Internet em segurança;
2. Informação sobre mecanismos e soluções para a navegação segura na Internet;
3. Formação de cidadãos e profissionais na utilização segura da Internet;
4. Operacionalização de uma linha de atendimento de denúncias de conteúdos ilegais e/ou ilícitos por qualquer pessoa, que, em estreita colaboração com as forças judiciais e os fornecedores de serviços de Internet, dê maior celeridade à avaliação dos conteúdos assinalados e à concretização de medidas adequadas.

As acções a desenvolver estão organizadas em projectos estruturantes, projectos de intervenção transversal e projectos de intervenção focalizada.



### **Projectos estruturantes**

Os projectos estruturantes têm como principal objectivo a promoção concertada de acções da responsabilidade das diferentes entidades que compõem o consórcio.

#### **1. Conselho Consultivo do projecto Internet Segura**

O Conselho Consultivo será composto por responsáveis de entidades governamentais e não governamentais e terá como principal responsabilidade acompanhar e emitir pareceres sobre as actividades desenvolvidas no âmbito do projecto Internet Segura. Caberá também a este Conselho Consultivo promover a visibilidade pública do projecto.

#### **2. Portal InternetSegura.pt**

Destinado a todos os públicos-alvo, o portal disponibilizará conteúdos informativos, formativos e interactivos sobre a utilização segura da Internet. Pretende-se um portal dinâmico e interligado com outros sítios da Internet para actualização automática de informação.

#### **3. Protocolo com ISPs e forças de segurança**

Pretende-se com estes protocolos a colaboração de prestadores de serviços de Internet (ISPs) e das forças de segurança para acções que venham a ser desenvolvidas pelo projecto Internet Segura, nomeadamente para facilitar o trabalho de cooperação necessário ao funcionamento eficaz da linha de atendimento de denúncias de conteúdos potencialmente ilegais.

#### **4. Rede Internet Segura**

A rede Internet Segura resultará de parcerias formais e/ou informais com entidades do poder central, local, sociedade civil e sector privado com vista à promoção e disseminação de acções integradas e articuladas de sensibilização para uma utilização segura e consciente da Internet.

##### **Projectos de intervenção transversal**

###### **1. Linha de denúncia de conteúdos**

No âmbito do projecto Internet Segura foi já criada uma infra-estrutura que receberá denúncias de qualquer pessoa relativas a conteúdos na Internet potencialmente ilegais. Uma equipa técnica analisa as denúncias efectuadas, encaminhando para as forças de investigação criminal e segurança os conteúdos comunicados, articulando com as entidades prestadoras de serviços de Internet o bloqueio dos mesmos.

Sempre que os conteúdos comunicados estejam alojados em servidores localizados fora de Portugal a linha de denúncia nacional encaminhará a caso reportado para as entidades relevantes no país em causa, em articulação com o *Inhope*.

###### **2. Guias de boas práticas**

É objectivo do projecto Internet Segura disponibilizar guias de boas práticas de utilização da Internet orientados para a administração pública, pequenas e médias empresas, escolas, estudantes e para os cidadãos em geral. Estes guias estarão acessíveis no portal InternetSegura.pt e serão de igual forma disponibilizados em papel aos vários públicos-alvo em locais apropriados à sua divulgação.

###### **3. Acções de formação**

Serão desenvolvidas acções de formação, presenciais e não presenciais, destinadas a segmentos diversificados da população. Estas acções de formação serão da responsabilidade do projecto Internet Segura, mas procurar-se-á o envolvimento de entidades da sociedade civil cujo âmbito de intervenção é a actividade de formação em TIC.

##### **Projectos de intervenção focalizada**

###### **1. Seguranet.pt**

Com enfoque no ensino básico e secundário, está já disponível o sítio da Seguranet.pt, com informações e guias de utilização para uma navegação segura da Internet. Para além da informação orientada para alunos e professores, o sítio disponibiliza também informação adequada a encarregados de educação.

###### **2. Articulação com as entidades europeias**

Em estreita articulação com o *Insafe* e com o *Inhope*, o consórcio assegurará a presença do projecto Internet Segura nas reuniões internacionais destas duas entidades, de forma a articular as iniciativas portuguesas com as de âmbito europeu. Um exemplo dessa articulação ocorre no Dia Europeu da Internet Segura com o envolvimento de Portugal desde 2005.

## Ligações Úteis

SeguraNet

<http://www.seguranet.pt/>

UMIC – Agência para a Sociedade do Conhecimento

<http://www.unic.pt/>

FCCN – Fundação para a Computação Científica Nacional

<http://www.fccn.pt/>

DGIDC

<http://www.dgicd.min-edu.pt/>

Internet Segura

[www.internetsegura.pt](http://www.internetsegura.pt)

Internet Segura – Conteúdos ilegais

<http://linhaalerta.internetsegura.pt/>

Microsoft – Segurança e Privacidade

[www.microsoft.com/portugal/seguranca](http://www.microsoft.com/portugal/seguranca)

InHope

[www.inhope.org](http://www.inhope.org)

InSafe

[www.saferinternet.org](http://www.saferinternet.org)

Safer Internet Plus

[http://ec.europa.eu/information\\_society/activities/sip/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/index_en.htm)

## 2 - Segurança no Computador

---

### 2.1. Actualização do Sistema Operativo

Para aumentar a segurança no computador pessoal, basta seguir alguns conselhos simples e básicos, que protegem o computador de muitos dos problemas identificados.

**Actualize o computador:** garantir que o sistema operativo e programas instalados apresentam as últimas actualizações é um importante reforço de segurança do computador. Tal como um carro, o computador também necessita de manutenção. Por isso, actualize com frequência o sistema operativo.

#### **Diversificação de software**

O sistema operativo Windows está presente na grande maioria dos computadores e, conseqüentemente, o Internet Explorer também. O problema é que existe uma infinidade de pragas digitais (spywares, vírus, etc) que exploram falhas desse navegador. Por isso, use outros navegadores como o Opera ou o Firefox, pois embora estes também possam ser explorados por pragas, isso ocorre com uma frequência muito menor.

Se preferir usar o Internet Explorer, use um navegador alternativo nos sítios que considere suspeitos (sites que abrem muitas janelas, por exemplo). Diversifique os programas do computador, usando produtos alternativos e menos populares e, logo, menos atractivos para os piratas informáticos. Por exemplo, Opera ou Netscape (*browser*), MacOS ou Linux (sistema operativo) e Thunderbird, Pegasus Mail ou Foxmail (programa de *e-mail*), etc.

### 2.2. Vírus

#### **O que é um vírus informático?**

Um vírus de computador é um programa informático que tem como propósito infectar o computador, fazendo com que o seu sistema operativo fique corrompido.

O vírus ataca agregando-se a um determinado programa já instalado no computador, de forma a que, quando este arranca, o vírus arranca com ele, propagando uma infecção. Este fenómeno ocorre, normalmente, sem o conhecimento do utilizador. Ao infectar o sistema operativo, um vírus poderá replicar-se a si mesmo e tentar infectar outros computadores, através de diversos meios.

Um vírus tanto pode ser um inofensivo programa que pouco mais faz que incomodar ligeiramente, como pode ir ao extremo de destruir ficheiros e tornar um computador inoperável. Contudo, uma característica comum a todos

os vírus é a velocidade com que se propagam, contaminando outros ficheiros e computadores ligados à Internet que se revelem mais vulneráveis.

### **Como funcionam os vírus?**

Uma das formas mais comuns de transmissão de vírus é através do e-mail. Há programas virais que se propagam de máquina em máquina através do uso das moradas de correio electrónico que figuram na lista do utilizador infectado. Outro método usado é pelo envio de uma mensagem de correio electrónico que, por exemplo, prometa prémios caso o cibernauta descarregue o ficheiro que se encontra nessa mensagem.

Outras formas de infecção podem incluir o download accidental de programas maliciosos que se encontrem “escondidos” dentro de outros programas, ou clicando em determinadas áreas de certos sítios de Internet menos bem intencionados.

A segunda maior causa de infecção deve-se ao facto de o utilizador não manter o seu sistema operativo actualizado, com a instalação dos “patches” (“remendos”) que o fabricante vai disponibilizando à medida que vai detectando falhas.

Apresentamos de seguida algumas técnicas de “auto-preservação” dos vírus:

#### **Ocultação nas pastas do sistema**

Dado que uma grande parte dos utilizadores de computadores não possui conhecimentos especializados em informática, os vírus implantam-se no sistema operativo, a fim de evitar que o utilizador comum tente removê-los. Esta técnica acaba por ser dissuasora, porque o utilizador médio terá receio de remover ficheiros do sistema, corrompendo o normal funcionamento do seu sistema.

#### **Encriptação**

Os vírus “escondem-se” encriptando os seus próprios dados: assim, o seu código será mais dificilmente detectado pelos antivírus e será mais difícil a sua remoção, embora cada vez mais os antivírus estejam melhor preparados para esta técnica. O propósito desta técnica é manter a infecção o maior tempo possível no computador.

#### **Tentativas de desactivar o antivírus**

Esta é a melhor forma de evitar a detecção e remoção de vírus.

#### **Que perigos podem apresentar os vírus?**

Um vírus de computador está programado para se esconder da melhor forma possível, para evitar a sua detecção e remoção.

Uma infecção por vírus pode trazer sérias consequências para o proprietário do material infectado, pois corrompe ficheiros, podendo até inutilizá-los, torna o sistema operativo muito mais lento e, em ocasiões, pode até usurpar os dados pessoais do utilizador.

## 2.3. Antivírus, anti-spyware e firewall

Se tomamos alguns cuidados para garantir a nossa protecção quando saímos de casa é porque sabemos do risco de assaltos e outros crimes. A Internet também se mostra por vezes como um lugar perigoso e é necessário ter alguns cuidados para evitar golpes, roubo de arquivos e senhas, ou mesmo espionagem das nossas actividades no nosso PC.

### Actualização do antivírus e do anti-spyware

**Instale um Antivírus e um AntiSpyware:** é importante que o computador tenha estes programas instalados, já que permitem detectar, anular e eliminar os vírus e *spywares* informáticos. Podemos destacar que o computador com um vírus instalado tem um funcionamento mais lento do que é habitual.

Não basta instalar um antivírus no computador para ficar protegido. É necessário actualizá-lo regularmente, caso contrário, o antivírus não saberá da existência de novos vírus. Praticamente todos os antivírus disponíveis permitem configurar uma actualização automática. Além disso, use um anti-spyware com frequência para tirar arquivos e programas maliciosos de seu computador. Em ambos os casos, verifique no manual do software ou no site do fabricante, como realizar as actualizações.

**Utilize uma firewall:** desta forma estará a impedir o acesso ao seu computador por parte de estranhos, através da Internet. Podemos fazer a seguinte comparação: ligar-se à Internet sem uma *firewall* é como deixar a porta de sua casa aberta. Uma firewall é uma protecção adicional contra a entrada de programas indesejados no seu computador, pelo que a deverá ter sempre activa e actualizada.

Assim, utilize sempre um antivírus, um *anti-spyware* e uma *firewall*, mesmo que gratuitos, e mantenha as definições actualizadas. Em caso de dúvidas, recorra à ajuda do manual.

## 2.4. Palavras-chave

### Memorização da palavra-chave

Quem navega na Internet encontra muitas vezes sítios que pedem o registo com palavra-chave. Para evitar a multiplicação de senhas e facilitar a sua memorização, há utilizadores que introduzem sempre a mesma. Mas tal não é recomendável: se alguém mal-intencionado descobrir a senha num dos sítios, ficará indefeso nos restantes.

Outros utilizadores colocam um visto na secção "Memorizar senha". Quando acedem àquele sítio, ao escreverem o nome de utilizador, a senha aparece automaticamente sob a forma de •••••. Não é seguro confiar a memorização da palavra-chave ao programa de navegação (ou *browser*).

Para desactivar a opção de memorização da palavra-chave, siga os passos.

No *Firefox*: Ferramentas > Opções > Segurança > em Memorizar as senhas para sítios, retire o visto. Se clicar sobre o botão Mostrar senhas, poderá visualizar as que estão guardadas e removê-las. No final, clique Ok.

Se usar o Internet Explorer: Ferramentas > Opções da Internet > Conteúdo > no campo Conclusão Automática, clique em Definições > em Nomes de utilizador e palavras-chave em formulários, retire o visto. No final, clique Ok.

### **Alguns truques para criar palavras-chave**

- Em sítios de bancos e lojas, etc., use uma senha para cada.
- Use um mínimo de 8 caracteres, alternando letras em maiúsculas e minúsculas com números e outros ( \_ - ou . )
- Não divulgue as suas palavras-chave.
- Não guarde suas senhas ficheiro ou de qualquer outro programa. Se necessitar guardar uma senha em papel (em casos extremos), destrua-o assim que decorar a sequência.
- Não utilize senhas fáceis de serem descobertas, como nome de parentes, data de aniversário, placa do carro, etc. Dê preferência a sequências que misturam letras e números.
- Não aceda à Internet como administrador do computador. Crie e use antes uma conta limitada de utilizador.

## **2.5. Sair em segurança**

Ao aceder à conta de e-mail ou outra conta (site de comércio electrónico, *home banking* ou plataforma) em que se exige o nome do utilizador e uma senha, clique sempre no botão/link de nome Logout, Logoff, Sair, Desconectar ou equivalente para sair do site. Pode parecer óbvio, mas simplesmente sair do site e fechar a janela do navegador de Internet ou entrar em outro endereço. Isso é arriscado porque o site não recebeu a instrução de encerrar o acesso naquele momento e alguém mal-intencionado pode abrir o navegador de Internet e aceder às informações da conta, caso esta realmente não tenha sido fechada devidamente.

## 2.6. Cópias de segurança

Faça cópias de segurança regulares de ficheiros importantes para um CD, DVD ou disco externo.

A protecção no "mundo virtual" pode ser um pouco trabalhosa, mas é importante para evitar transtornos maiores. A maioria dos golpes e das armadilhas pode ser evitada se o utilizador estiver atento, por isso é essencial seguir algumas regras:

- Tenha o seu sistema operativo actualizado
- Tenha o antivírus e o spyware actualizados
- Tenha a firewall sempre activa
- Bloqueie as linguagens Java, JavaScript e ActiveX no seu browser.
- Convém encriptar (codificar) documentos importantes e dados pessoais.
- Faça cópias de segurança regulares de ficheiros importantes para um CD, DVD ou disco externo.
- Se o browser sugerir a memorização da palavra-chave, não aceite.
- Não divulgue as suas palavras-chave.
- Faça o *log-out* antes de sair de um sítio onde esteja registado.

## Ligações Úteis

SeguraNet

<http://www.seguranet.pt/>

Internet Segura

<http://www.internetsegura.pt/>

Linha Alerta

<http://linhaalerta.internetsegura.pt/>

Microsoft – Segurança e Privacidade

<http://www.microsoft.com/portugal/seguranca/default.msp>

UMIC – Agência para a Sociedade do Conhecimento

<http://www.umic.pt/>

FCCN – Fundação para a Computação Científica Nacional

<http://www.fccn.pt/>

Europa – Sociedade da Informação

[http://europa.eu/pol/infos/index\\_pt.htm](http://europa.eu/pol/infos/index_pt.htm)

InSafe

<http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

### **Nós Europeus InSafe**

Áustria <http://www.saferinternet.at/>

Espanha <http://www.protegeles.com/>

UK <http://www.uclan.ac.uk/host/cru/>

Bélgica <http://www.saferinternet.be/>

Holanda <http://www.digibewust.nl/>

Alemanha <http://www.klicksafe.de/>

Itália <http://www.saferinternetday.it/>

Polónia <http://www.saferinternetday.pl/>

Hungria <http://www.baratsagosinternet.hu/mss/alpha>

Dinamarca <http://andk.medieraadet.dk/>

Finlândia <http://www.tiukula.fi/index.php>

Grécia <http://www.saferinternet.gr/>

Islândia <http://www.heimiliogskoli.is/>

Irlanda <http://www.ncte.ie/InternetSafety/>

Lituânia <http://www.bite.lt/en/>

Noruega <http://www.saftonline.no/>

Eslovénia <http://www.safe.si/>

Suécia <http://www.medieradet.se/>