



**Colégio Valsassina**

Um projecto pedagógico com tradição de integrar valores culturais e sociais.

Introdução às Tecnologias da Informação e da Comunicação – 9º Ano

# **A Internet**

## **Funcionamento e**

## **Serviços Disponíveis**

José Rainho

Alunos do 9º Ano do Colégio Valsassina

Janeiro de 2009

## Índice

1. Apresentação .....	3
2. História da Internet .....	3
3. Funcionamento da Internet .....	5
4. Serviços disponíveis.....	9
4.1. World Wide Web .....	9
4.2. Motores de busca .....	9
4.3. Correio electrónico .....	10
4.4. Listas de correio .....	10
4.5. Transferência de ficheiros.....	10
4.6. Grupos de discussão (Newsgroups).....	11
4.7. Comunicação em tempo real.....	11
4.8. Videoconferência .....	11
5. Segurança Informática .....	13
5.1. Malware .....	13
5.2. Hackers e crackers .....	14
5.3. Ataques de Phishing.....	14
5.4. Engenharia Social .....	15
5.5. Gestão de Passwords .....	15
6. Notas Finais .....	16

## 1. Apresentação

A Unidade 3 do programa da disciplina de Introdução às Tecnologias da Informação e da Comunicação do 9º ano de escolaridade abrange a Internet e os seus serviços. Este documento resume alguns aspectos essenciais desta temática, acrescentando ainda algumas noções básicas de Segurança Informática.

## 2. História da Internet

Uma rede de computadores é um conjunto de dois ou mais computadores ligados entre si.

A Internet é a maior rede de computadores do mundo. Está disponível por todo o globo e, por isso mesmo, é apelidada de “a rede das redes”.

A Internet nasceu no final dos anos 60, nos Estados Unidos, como uma rede de computadores chamada ARPAnet que estava ao serviço do Departamento de Defesa norte-americano. Em plena Guerra Fria, a Informação era o bem mais importante, e os Estados Unidos começaram então a utilizar este novo canal de comunicação, ainda desconhecido dos soviéticos, para troca de mensagens entre as bases militares.

A ARPAnet era uma rede sem hierarquias, ou seja, não tinha um servidor central que, em caso de falha, inutilizasse toda a rede:

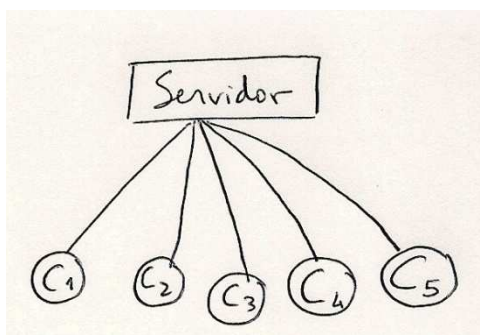


Figura 1 - Rede com hierarquia

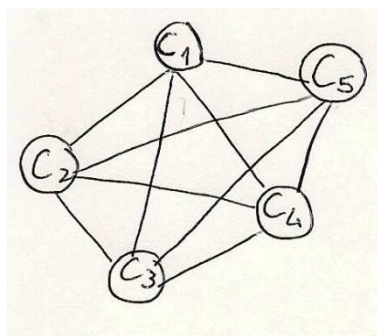


Figura 2 - Rede sem hierarquias

As universidades acabaram por ser as entidades que se seguiram na interligação dos seus *campus* através de uma rede de computadores. Nesta altura, toda a comunicação era baseada na troca de mensagens textuais.

Nos anos 80, a Internet foi aberta às redes internas das empresas e a outras sub-redes, sendo que em 1987 passou a ser permitido a utilizadores domésticos terem também acesso. Até ao final dos anos 80, a Internet espalhou-se um pouco por todo o mundo.

Em 1992, Tim Berners-Lee criou a World Wide Web, um serviço da Internet que possibilitava a partilha de documentos multimédia baseados em hipertexto, ou seja, dotados de uma estrutura de navegação que permitia, através de hiperligações, a passagem de umas secções a outras com um simples clique do rato.

Com o advento da World Wide Web, a Internet ganhou uma enorme popularidade mundial nos anos 90, e hoje em dia é o suporte informático do “mundo global”, sendo utilizada por mais de 1000 milhões de pessoas diariamente.



### *Para estudar...*

- Manual da disciplina: páginas 132-135
- <http://pt.wikipedia.org/wiki/ARPANET>
- <http://www.manuelamelo.net/moodle/file.php/1/INTERNET.pdf>

### 3. Funcionamento da Internet

Para aceder à Internet é necessário:

- Um modem – aparelho que liga o computador à rede;
- Contrato com um ISP (*Internet Service Provider*) – uma empresa que contratamos para termos acesso à Internet;
- Software apropriado – programas para utilizar os vários serviços. Exemplos: um *browser* (navegador) para consultar páginas Web; um programa de conversação para aceder à comunicação em tempo real; etc...

Podemos classificar uma ligação à Internet quanto à sua velocidade:

- Ligação de banda estreita (menos de 256 kbps de largura de banda): modems analógicos e linhas RDIS;
- Ligação de banda larga (256 kbps ou mais): ADSL, cabo, linhas dedicadas, redes 3G.

Eis como podemos proceder à previsão do tempo de download de um ficheiro:

- $velocidade = \frac{\text{dados transferidos}}{\text{tempo}}$
- Basta ter cuidado com as unidades!
- Exemplo: tenho, em minha casa, uma ligação à Internet com largura de banda de 16 Mbps, ou seja, 16384 kbps. A que velocidade real, expressa em kbps, decorreu a transferência de um ficheiro de 3 MB que demorou 55 segundos?

$$3 \text{ MB} = 3 \times 8 \text{ Mb} = 24 \text{ Mb}$$

$$\frac{1 \text{ Mb}}{1024 \text{ kb}} = \frac{24 \text{ Mb}}{x} \Leftrightarrow x = \frac{24 \times 1024}{1} = 24576 \text{ kb}$$

$$velocidade = \frac{24576 \text{ kb}}{55 \text{ s}} = 446,84 \text{ kbps}$$

Como podemos ver pelo exemplo, as velocidades que os ISPs anunciam são sempre máximos teóricos. Devido ao congestionamento das redes e dos servidores, à distância a que os nossos computadores estão da central telefónica e por vezes à fraca qualidade das linhas, essas velocidades nunca são atingidas.

Por onde passam os dados quando dois computadores comunicam entre si através da Internet?

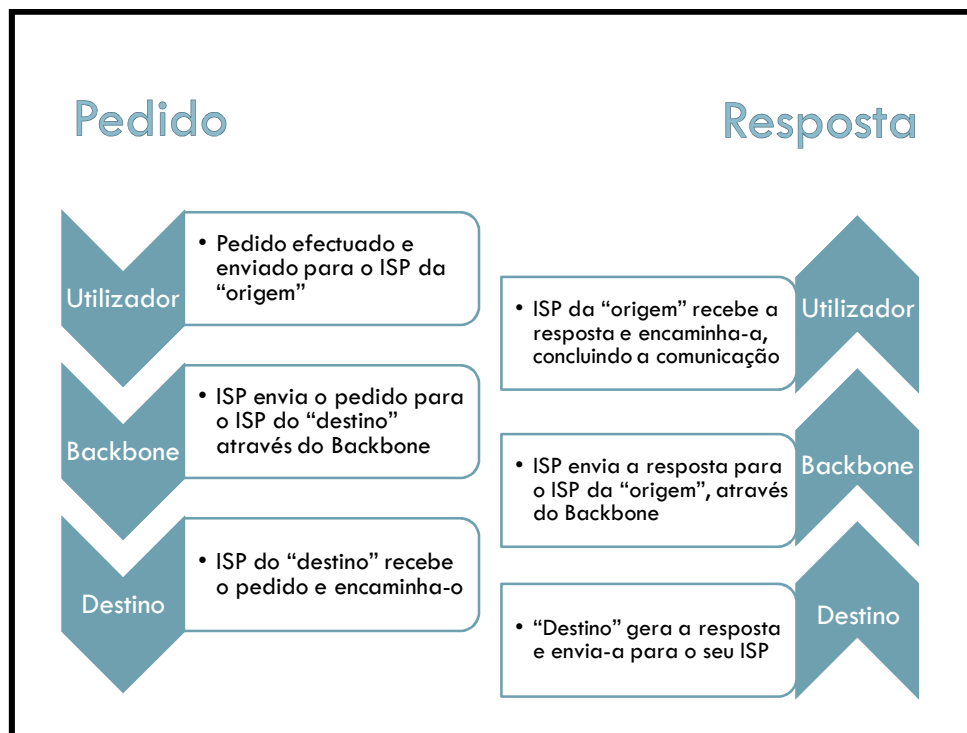


Figura 3 - Representação esquemática do encaminhamento de pedidos na Internet

Imaginemos então que estamos em Lisboa e que o nosso ISP é, por exemplo, a Netcabo. Estamos a comunicar através do Messenger com alguém em Los Angeles, cujo ISP é a AOL (America OnLine).

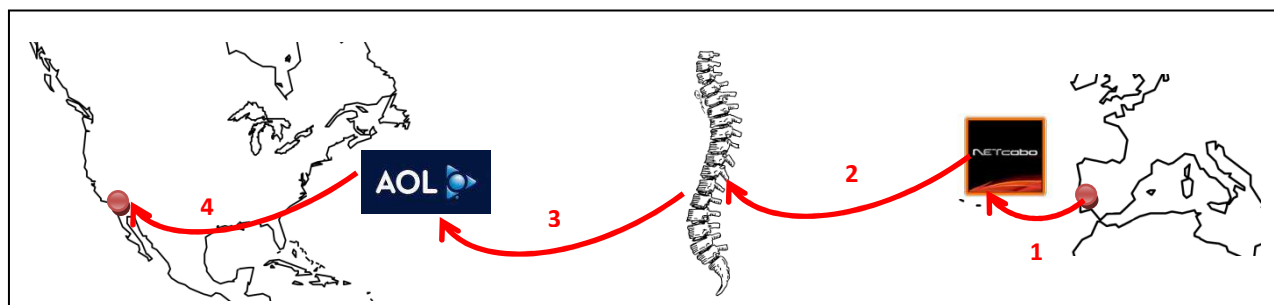


Figura 4 - Encaminhamento de um pedido na Internet

Não existe nenhum cabo que nos ligue directamente ao destino. O que se passa é que a mensagem começa por ser enviada do nosso computador para o nosso ISP (1).

Em seguida, o nosso ISP encaminha a mensagem (2) até ao ISP do destino (3) utilizando o backbone, que é o conjunto de ligações de elevado débito que funciona como a “espinha dorsal” da Internet. Finalmente, o ISP do nosso destinatário entrega-lhe a mensagem.

Quando o nosso interlocutor responde, a comunicação segue o caminho inverso:

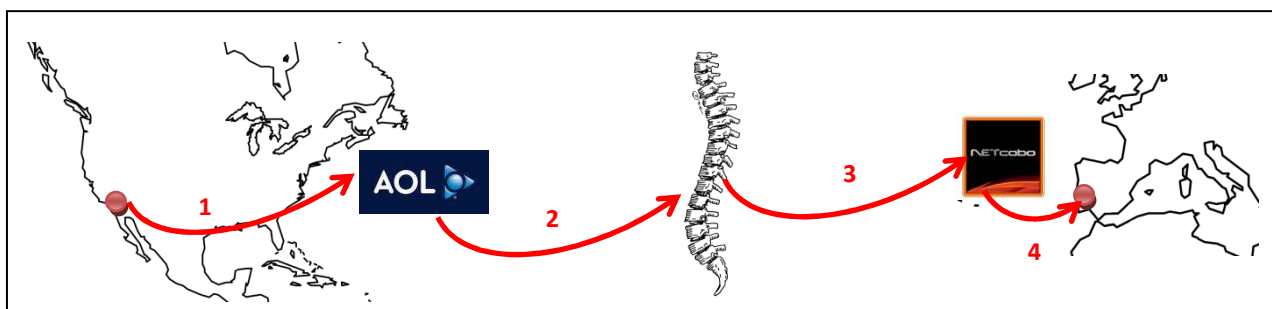


Figura 5 - Encaminhamento de uma resposta na Internet

Cada computador é identificado na Internet através de um endereço composto por quatro números entre 0 e 255 separados por pontos, como por exemplo, 213.24.144.78. Este endereço denomina-se por **endereço IP**.

Com o advento da World Wide Web, tornava-se pouco prático referirmo-nos aos *sites Web* pelo seu endereço IP. Para facilitar a memorização, criou-se um endereço legível chamado URL (*uniform resource locator*), como por exemplo,

<http://www.cvalsassina.pt/noticias/desporto.htm>

Um endereço URL pode decompor-se em 3 partes:

- Protocolo (neste exemplo, **http://**) – indica o tipo de comunicação que está a ser efectuado. Neste caso, trata-se de um pedido de página Web.
- Servidor (neste exemplo, **www.cvalsassina.pt**) – indica qual o servidor em que o recurso pretendido se encontra alojado. A extensão desta parte do endereço fornece uma indicação acerca do conteúdo ou da localização do servidor. Neste exemplo, .pt indica que o servidor é português.

- Localização (neste exemplo, **/noticias/desporto.htm**) – indica, dentro do servidor, o caminho para chegar ao recurso pretendido. Neste caso, pediu-se a página **desporto.html** que está dentro da pasta **noticias**.

O encaminhamento dos pedidos para um servidor ou qualquer outro computador na Internet é sempre feito utilizando o seu endereço IP. Quando pedimos acesso a um servidor utilizando o seu URL, o nosso computador tem de consultar um servidor DNS para ficar a saber qual é o endereço IP que corresponde ao URL que queremos consultar.



### *Para estudar...*

- Manual da disciplina: páginas 138-139
- [http://en.wikipedia.org/wiki/Internet\\_backbone](http://en.wikipedia.org/wiki/Internet_backbone)
- <http://www.velocimetro.com.pt>
- [http://www.ipv6-tf.com.pt/documentos/noticias/not\\_03012004\\_3.pdf](http://www.ipv6-tf.com.pt/documentos/noticias/not_03012004_3.pdf)
- [http://www.nwe.ufl.edu/writing/help/web/intro/url\\_explanation.shtml](http://www.nwe.ufl.edu/writing/help/web/intro/url_explanation.shtml)

## 4. Serviços disponíveis

Na Internet podemos utilizar vários serviços, entre eles:

### 4.1. World Wide Web

A WWW é o conjunto de todas as páginas Web. Uma página Web é normalmente produzida em hipertexto utilizando a linguagem HTML. Todas as páginas Web e as imagens e documentos nelas contidos estão alojados em servidores Web.

Para navegar na Web precisamos de um *browser*. Os mais conhecidos são o Internet Explorer, com uma quota de mercado de cerca de 45%, o Mozilla Firefox, que detém 35% do mercado, o Google Chrome com 10% dos utilizadores e o Safari, utilizado maioritariamente em computadores da Apple, que reúne a preferência de cerca de 8% dos utilizadores.

### 4.2. Motores de busca

Um motor de busca é um site Web que nos permite localizar informação e encontrar outros sites Web.

Há dois tipos de motores de busca:

- Os *spiders*, dos quais o exemplo mais famoso é o Google, percorrem a WWW de forma automática indexando todas as páginas.
- Os directórios, como por exemplo o Yahoo, que dependem das sugestões dos utilizadores para adicionarem websites à sua base de dados.

Na maioria dos motores de busca, para encontrar páginas Web devemos pesquisar utilizando palavras-chave relevantes ao assunto que nos interessa. No entanto, se procuramos páginas que incluam uma frase ou expressão concreta, devemos colocá-la entre aspas.

### 4.3. Correio electrónico

O correio electrónico consiste no envio de mensagens assíncrono entre dois utilizadores. A mensagem enviada só será entregue ao destinatário quando ele consultar a sua conta de *email*.

A maioria dos servidores de correio electrónico permite a consulta do mesmo através de uma página Web (*webmail*). Alguns fornecem dados que nos permitem configurar programas específicos (como o Outlook, o Windows Mail ou o Eudora) para enviar e receber as mensagens.

Ao criarmos uma mensagem, temos de preencher alguns campos:

- Destinatário: o endereço de *email* da pessoa a quem queremos enviar a mensagem (na forma [username@servidor.de.mail](#));
- Cópia (cc): Endereços de email de pessoas a quem queremos enviar uma cópia da mensagem;
- Cópia Oculta (bcc): Endereços de *email* de pessoas a quem queremos enviar uma cópia da mensagem, mas sem que os restantes destinatários se apercebam;
- Assunto da mensagem;
- Texto da mensagem;
- Documentos anexos à mensagem.

### 4.4. Listas de correio

Trata-se de listas de endereços de *email* em que as pessoas se inscrevem para poderem comunicar entre si sobre um determinado tema. A lista possui um endereço próprio e todas as mensagens para lá enviadas são reencaminhadas automaticamente para todos os membros da lista.

### 4.5. Transferência de ficheiros

Os servidores FTP (*file transfer protocol*) disponibilizam para transferência ficheiros dos mais variados tipos. Os servidores FTP mais comuns pertencem a empresas que os usam para distribuir *software* pelos seus clientes. Por exemplo, a Microsoft tem um servidor de FTP onde podem ser encontradas actualizações para os seus programas.

A maioria dos *browsers* consegue descarregar ficheiros alojados em servidores de FTP, mas para navegar num destes servidores é mais prático utilizar um programa concebido especificamente para o efeito, como o FileZilla.

#### 4.6. Grupos de discussão (Newsgroups)

Os grupos de discussão são servidores ou páginas Web onde os utilizadores podem deixar mensagens que podem ser lidas e, eventualmente, respondidas pelos restantes utilizadores.

Para utilizar os *newsgroups* é necessário software apropriado, sendo que o mais conhecido é o Outlook. De há uns anos a esta parte, os *newsgroups* têm caído em desuso em detrimento dos fóruns, que funcionam em normais sites *Web* mediante o registo dos participantes.

#### 4.7. Comunicação em tempo real

A comunicação em tempo real consiste no envio de mensagens de texto a outros utilizadores. A diferença entre este tipo de comunicação e o *email* prende-se com a entrega da mensagem: enquanto no *email* o destinatário apenas vê a mensagem quando consultar a sua caixa de correio, na comunicação em tempo real a mensagem é entregue imediatamente no ecrã do computador do nosso interlocutor.

Para utilizar este serviço é necessário software específico. O mais usado na actualidade é o Windows Live! Messenger.

#### 4.8. Videoconferência

Trata-se de uma variante da comunicação em tempo real em que a comunicação se estabelece por vídeo. Ambos os participantes dispõem de uma câmara Web (*webcam*) que filma e transmite a imagem do utilizador ao seu interlocutor.

O Windows Live! Messenger permite este tipo de comunicação, mas existem programas específicos para o efeito, como o Microsoft NetMeeting.



## *Para estudar...*

- Manual da disciplina: páginas 140-145, 168, 170-173
- <http://www.webconfs.com/search-engine-spider-simulator.php>
- <http://www.cultura.ufpa.br/dicas/net1/mailcam.htm>
- [http://pt.wikipedia.org/wiki/Instant\\_Messaging](http://pt.wikipedia.org/wiki/Instant_Messaging)

## 5. Segurança Informática

A informação guardada nos nossos computadores é preciosa e pessoal. Os ataques a essa informação podem causar perda de dados ou fazer com que ela caia em mãos alheias. Desta forma, é necessário conhecer os riscos que corremos e as medidas que devemos tomar para nos precavermos.

### 5.1. Malware

Chamamos *malware* a todo e qualquer software que tenha sido criado com intuítos maliciosos. A maioria destes programas difunde-se por *email*. O *malware* divide-se em:

- Vírus – são programas que se propagam automaticamente, infectando outros programas no nosso computador. Podem causar perda de dados, apagando ou alterando ficheiros importantes.
- Worms – são programas que se propagam automaticamente numa rede de computadores. Este tipo de *malware* explora vulnerabilidades dos computadores para se instalar neles.
- Trojans – são programas que fingem ter uma determinada função e que levam os utilizadores a executá-los voluntariamente. Por exemplo, um programa que diz ser um visualizador de fotografias mas que, na verdade, ao ser executado infecta o nosso computador.
- Spyware – são programas que se instalam no nosso computador, muitas vezes agregados a outros programas que recolhemos na Internet, e que têm como intuito reunir informação pessoal sobre nós e sobre a nossa utilização do computador e enviá-la para o seu criador.

Para nos mantermos protegidos de *malware*, devemos:

- Instalar um anti-vírus e mantê-lo actualizado. O AVG, disponível em <http://free.avg.com>, é gratuito e bastante eficaz.
- Manter o nosso sistema operativo devidamente actualizado para minimizar a existência de vulnerabilidades que possam ser exploradas por worms.
- Instalar um programa anti-spyware e mantê-lo devidamente actualizado, executando regularmente limpezas ao nosso computador. O Ad-Aware, disponível em <http://www.lavasoft.pt/>, possui uma versão gratuita e bastante fiável. O Windows Vista já inclui um programa anti-spyware, chamado Windows Defender.

- Não executar ficheiros que sejam enviados por *email* ou que estejam em páginas Web suspeitas.
- Não instalar todo e qualquer software que encontramos na Web. Instalar apenas programas bem conhecidos, dos quais encontremos boas referências, e sempre recolhidos dos sites oficiais dos respectivos fabricantes.

## 5.2. Hackers e crackers

Um hacker é um indivíduo com grandes conhecimentos de informática e de redes que tenta obter acesso a servidores sem que lhe seja fornecida autorização. O termo hacker costuma referir-se a pessoas que efectuam este crime mas sem intuídos maliciosos, apenas pretendendo testar os seus conhecimentos e aptidões.

Já um cracker é alguém que entra em servidores sem autorização mas com objectivos destrutivos. O termo cracker costuma também designar pessoas que efectuam modificações a programas comerciais (*cracks*) de forma a contornar as suas protecções anti-cópia e proporcionar a sua utilização gratuita.

Para evitar a invasão dos nossos computadores por crackers ou hackers mal intencionados, podemos instalar uma *firewall*, que monitoriza o nosso tráfego na rede e impede o acesso de fontes exteriores ao nosso computador. Desde a versão SP2 do Windows XP que o sistema operativo da Microsoft já inclui uma firewall bastante fiável.

## 5.3. Ataques de Phishing

Um ataque de Phishing dá-se, normalmente, quando é enviada uma mensagem de *email* (“isco”) a um utilizador, imitando o aspecto das mensagens de *email* oficiais de uma determinada entidade. O utilizador, convicto de que se trata de uma mensagem legítima, clica numa hiperligação lá incluída e abre uma página Web que é idêntica à página oficial da entidade. Coloca lá os seus dados pessoais, incluindo a sua password, e entrega-os desta forma ao criminoso autor do ataque.

Para evitarmos cair num destes ataques, tudo o que temos a fazer é nunca acreditar totalmente em mensagens de email que peçam para mudarmos uma password ou para actualizarmos os nossos dados. Nunca devemos clicar em *links* nas mensagens – devemos, isso sim, escrevermos nós próprios o endereço URL da entidade no nosso *browser* e visitarmos a sua página oficial para verificarmos se é mesmo necessária a password ou a alteração de dados pedida no *email*.

## 5.4. Engenharia Social

Um ataque de Engenharia Social é um ataque de confiança. O criminoso trava conhecimento pessoal com a vítima e ganha a sua confiança. A certa altura, a vítima está tão à-vontade com o criminoso que acaba por lhe revelar as suas passwords.

Por regra, nunca devemos revelar **a rigorosamente ninguém** as nossas passwords, nem mesmo a pessoas que se digam funcionárias da entidade a que a password diz respeito. Por exemplo, nem mesmo a alguém que diz ser funcionário do nosso ISP nós devemos fornecer a nossa password de ligação à Internet.

## 5.5. Gestão de Passwords

Falando em passwords... eis alguns conselhos para que as nossas sejam seguras:

- Uma boa password é fácil de decorar mas difícil de adivinhar. Por exemplo, podemos utilizar uma palavra de dimensão apreciável mas com algumas das suas letras substituídas por símbolos ou números: **m1crocomput@dor**
- Outra boa ideia é utilizar passphrases, ou seja, pequenas frases às quais omitimos os espaços, misturando maiúsculas com minúsculas para separar duas palavras dentro da frase: **HaCincoLindasFloresNoMeuJardim**
- Podemos ainda misturar os dois métodos, adicionando siglas e sinais de pontuação: **H@5Lind@sFNMJ!**
- Não devemos utilizar a mesma password para todos os nossos serviços;
- Recomenda-se que mudemos as nossas passwords pelo menos duas vezes por ano.



*Para estudar...*

- Manual da disciplina: páginas 122-125, 154-157
- <http://www.softinmotion.pt/artigos/200608/conselhos-seguranca-informatica.aspx>
- <http://cartilha.cert.br/>
- [http://en.wikipedia.org/wiki/Hacker\\_\(computing\)](http://en.wikipedia.org/wiki/Hacker_(computing))

## 6. Notas Finais

Este documento consiste num resumo da terceira unidade do programa de TIC do 9º Ano e foi elaborado tendo como base trabalhos efectuados pelos alunos das turmas 9ºA, 9ºB, 9ºC e 9ºD do ano lectivo 2008/09 do Colégio Valsassina.

Para quaisquer comentários, correcções ou sugestões de melhoramentos, agradecemos o envio de uma mensagem para [jose.rainho@gmail.com](mailto:jose.rainho@gmail.com).

Obrigado!