Colecção
INOVAÇÃO E GOVERNAÇÃO NAS AUTARQUIAS

TECNOLOGIAS E SISTEMAS DE INFORMAÇÃO, REDES E SEGURANÇA

Sociedade Portuguesa de Inovação

F I C H A T É C N I C A

Título
TECNOLOGIAS E SISTEMAS DE INFORMAÇÃO, REDES E SEGURANÇA

Autor
Pedro Veiga

Editor

Consultadoria Empresarial e Fomento da Inovação, S.A.
Edifício "Les Palaces", Rua Júlio Dinis, 242,
Piso 2 – 208, 4050-318 PORTO
Tel.: 226 076 400; Fax: 226 099 164
spiporto@spi.pt; www.spi.pt
Porto • 2004

Produção Editorial
Principia, Publicações Universitárias e Científicas
Av. Marques Leal, 21, 2.º
2775-495 S. JOÃO DO ESTORIL
Tel.: 214 678 710; Fax: 214 678 719
principia@principia.pt
www.principia.pt

Revisão
Marília Correia de Barros

Projecto Gráfico e *Design*
Mónica Dias

Paginação
Xis e Érre, Estúdio Gráfico, Lda.

Impressão
MAP – Manuel A. Pacheco

ISBN 972-8589-39-5

Depósito Legal 220231/04

Produção apoiada pelo Programa Operacional Emprego, Formação e Desenvolvimento Social (POEFDS), co-financiado pelo Estado Português, e pela União Europeia, através do Fundo Social Europeu.

Ministério da Segurança Social e do Trabalho.

TECNOLOGIAS E SISTEMAS DE INFORMAÇÃO, REDES E SEGURANÇA

Pedro Veiga

Sociedade Portuguesa de Inovação

INTRODUÇÃO

As evoluções nas redes de comunicação, nos computadores, nos sistemas operativos e nas aplicações vieram trazer alterações ao modo como estes sistemas são concebidos e estruturados.

Por outro lado, tem crescido de maneira significativa o modo como as organizações usam os sistemas de informação e das redes. A rede mais representativa, a Internet, foi criada para permitir a interligação de computadores de um modo simples e com tolerância a falhas, inicialmente para aplicações militares. Estas características vieram a ser os aspectos decisivos numa tecnologia que se tornou a solução central para a ligação dos principais sistemas de informação e, também, a tecnologia de comunicação, base da sociedade de informação neste início do século XXI.

Contudo, são as aplicações que são relevantes para os utilizadores finais. A simplicidade e flexibilidade destas aplicações têm tornado possível a sua implementação em sistemas muito diferentes, desde computadores de grande porte, aos computadores pessoais e até em computadores de bolso e telemóveis. Nesta obra são apresentadas as principais famílias de aplicações e, nalguns casos, como estas são integradas nos sistemas de informação e nas redes das organizações.

A complexidade dos sistemas de informação e das redes actuais tem levado à necessidade de criar modos expeditos e eficientes para os desenvolver. Neste manual faz-se uma breve análise das técnicas usadas, graças ao tipo de tecnologias informáticas actualmente disponíveis, abordando-se estas técnicas em termos de linguagens, ferramentas computacionais e arquitecturas de concepção de sistemas informáticos.

Nesta obra, na sua parte final, analisam-se os aspectos de segurança. Com efeito, a crescente importância que os sistemas de informação e as redes têm para a nossa sociedade e para o nosso bem-estar obriga, naturalmente, a que tenhamos de ter confiança no seu uso. Existem actualmente muitas tecnologias que, se forem bem aplicadas, ajudam a garantir a segurança e a confiança de que podemos usar quer os sistemas de informação, quer as redes. Porém, na área da segurança informática, como aliás em todas as áreas onde a segurança é um factor relevante, a tecnologia só resolve os nossos problemas se estiver integrada numa política de segurança bem definida, concebida de modo rigoroso, bem implementada e cuja aplicação deve ser auditada de modo independente.

CAPÍTULO

1

ARQUITECTURA DOS SISTEMAS DE INFORMAÇÃO E DAS REDES

OBJECTIVOS

- São apresentadas as arquitecturas dos sistemas de informação actuais, os sistemas informáticos que os suportam e inicia-se uma introdução às redes que os interligam.
- É feita uma breve introdução à arquitectura dos actuais computadores e dos sistemas operativos sob os quais operam.

P O N T O D A S I T U A Ç Ã O

A informatização dos serviços autárquicos é hoje uma realidade na maioria das situações, se bem que o nível de penetração do uso dos computadores varie muito de caso para caso.

Da simples informatização para funções de escritório electrónico à automatização da maioria dos serviços autárquicos, passando pelo uso de Sistemas de Informação Geográfica (SIG) há uma enorme diversidade de situações, como apontam diversos estudos.

A necessária modernização da prestação dos serviços pelas autarquias passa pela informatização da maioria, ou mesmo da totalidade dos processos autárquicos. Para isso ser feito há que instalar redes locais e, nos casos em que as autarquias estão distribuídas por vários edifícios, interligar as redes locais entre si.

Além disso há que instalar as aplicações em servidores bem dimensionados onde estarão alojadas todas as bases de dados e ficheiros necessários.

A disponibilização de informação aos utentes dos serviços autárquicos deve ser hoje em dia uma prioridade e deve ser complementada, sempre que possível, pela prestação de serviços em linha. Apesar da primeira fase referida, a disponibilização de informação em linha aos utentes dos serviços autárquicos pode ser feita com relativa facilidade e com custos muito moderados. Estudos recentes, dos quais se salienta um elaborado pela Universidade do Minho, mostra que ainda há muitas Câmaras Municipais que não dispõem de um sítio na Internet. Noutros casos o sítio foi criado, mas, após este passo inicial, não se cuidou da sua actualização nem, muito menos, da sua evolução para uma plataforma de prestação de serviços em linha.

1.1. ARQUITECTURA DOS SISTEMAS COMPUTACIONAIS

Desde que foram comercializados os primeiros computadores, no início da década de 50, a sua arquitectura básica pouco mudou. Os actuais computadores ainda seguem a chamada *arquitectura de von Neuman* em homenagem ao cientista que definiu que um computador era composto por três componentes fundamentais (ver figura 1.1):

- O CPU (*Central Processing Unit*), o componente responsável pela execução das instruções;
- A Memória Central, ou simplesmente memória, onde estão armazenados os dados e as instruções dos programas que o computador irá executar;
- Os periféricos, os componentes através dos quais a informação é trocada com o exterior.

Estes três componentes são interligados entre si através de um dispositivo a que é dado o nome de BUS ou barramento do computador. É através deste que os três componentes trocam informação. Do ponto de vista técnico o BUS tem três subcomponentes: o BUS de dados, o BUS de endereços e o BUS de controlo. Além da velocidade do CPU a velocidade a que a informação é transferida através do BUS controla a eficiência global do computador.

Todavia, ao longo dos 50 anos que se seguiram, verificou-se uma notável evolução da velocidade, capacidade e diversidade destes componentes, o que conduziu a que os actuais computadores, na realidade, tenham pouco a ver com os computadores da década de 50 do século XX, excepto por manterem a mesma arquitectura básica.

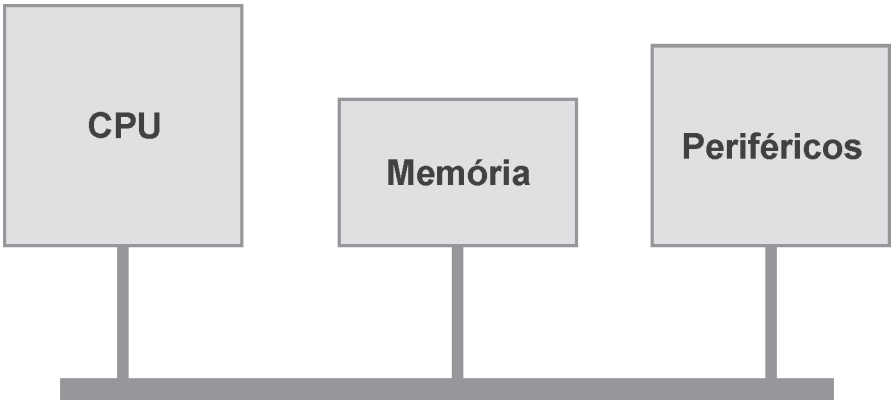

Figura 1.1 • Arquitectura básica de um computador

Portanto, os computadores não têm tido grandes alterações nesta arquitectura básica, todavia, tem havido mudanças tecnológicas que têm marcado de modo significativo as facilidades obtidas dos computadores, hoje em dia. Foram os avanços tecnológicos na área da microelectrónica, na mecânica de precisão, nas tecnologias das telecomunicações e nas tecnologias de visualização que tiveram maior impacto a nível do *hardware*. Em paralelo, o progresso nas tecnologias do *software* permitiu fazer aplicações cada vez mais complexas, mais modulares e fáceis de alterar e de integrar, e usadas em cada vez mais áreas aplicacionais.

1.1.1. O *HARDWARE*

Os computadores actuais, apesar de manterem a arquitectura dos primeiros computadores comercializados na década de 50 do século XX, be-

neficiam de uma série de evoluções tecnológicas que marcam de modo decisivo a sua utilização.

Em primeiro lugar, as evoluções na microelectrónica têm vindo a permitir fazer CPU cada vez mais poderosos e rápidos. Isto tem sido possível devido à miniaturização dos transístores num circuito integrado. Assim é possível colocar cada vez mais transístores num circuito integrado, fazendo-se sistemas com muito maior capacidade e complexidade. Por outro lado, os outros componentes do computador também têm dimensões cada vez mais reduzidas e complexidade acrescida.

Em relação à memória do computador também se conseguiram melhorias extraordinárias desde os primeiros computadores. Hoje em dia a memória dos computadores é de grande dimensão e tem um custo muito reduzido. Como a memória do computador é uma componente crítica para o funcionamento eficiente podem ter-se computadores com memórias de grande dimensão a custos reduzidos, o que também permite aos sistemas operativos e às aplicações um bom funcionamento. Com excepção de algumas tarefas computacionalmente muito exigentes, a velocidade do CPU não é, normalmente, um factor crítico para o funcionamento de um computador, mas sim a dimensão da memória central é a que mais limita o funcionamento global do computador, sendo, por vezes, apenas necessário aumentar a memória do computador, através da instalação de mais uns circuitos integrados, para se obter um melhor desempenho.

Outros resultados da miniaturização dos componentes são a redução do consumo de energia para colocar em funcionamento os componentes do computador, e a acrescida fiabilidade destes resultante do mesmo facto. Sistemas que consomem menos energia têm maior autonomia, quando usados em equipamentos portáteis, e como dissipam menos energia também se tornam menos susceptíveis a avarias resultantes dos choques térmicos associados ao seu funcionamento.

A nível do *hardware* do computador as alterações mais marcantes e que vieram a definir as características e o uso dos computadores actuais foi a grande evolução nos periféricos, que são os dispositivos que fazem a interacção do computador com o exterior e que analisamos de seguida.

1.1.1.1. Os periféricos

Os primeiros computadores tinham um número limitadíssimo de dispositivos para comunicarem com o exterior. Resumiam-se, na maioria dos casos, a um leitor de cartões, que era o principal dispositivo para a entrada de dados, e a uma impressora, onde eram escritos os resultados. Havia ainda um

dispositivo do tipo de uma máquina de escrever que possibilitava a entrada e a saída de dados em pequenos volumes.

Ao longo dos anos foi sendo desenvolvida uma diversidade de periféricos, sendo esta uma das áreas em que os actuais computadores quase nada têm a ver com os seus «antepassados».

Os periféricos actuais podem ser classificados em dois grandes grupos:

- Os periféricos para armazenamento de dados, que funcionam como uma extensão à memória do computador e com a capacidade de armazenar informação, mesmo com o computador desligado (são chamadas memórias não voláteis), onde se incluem, entre outros, os discos, as disquetes, os CD-ROM e os vários tipos de fitas magnéticas;
- Os periféricos de comunicação com o exterior que permitem ou a comunicação entre o exterior e o computador, ou entre este e o exterior.

Pela sua diversidade analisamos os periféricos de seguida. Antes desta análise, porém, devemos chamar a atenção para outro aspecto crucial na evolução dos computadores: o modo como estes periféricos estão integrados no computador. Representamos na figura 1.2 um esquema simplificado da arquitectura de um computador, onde se analisa a parte dos periféricos. Aqui podemos chamar a atenção do leitor para o seguinte:

- Os periféricos estão interligados entre si e ligados a um controlador de periféricos;
- O controlador de periféricos está ligado ao BUS geral do computador, onde agora e em relação à figura 1.1 se analisou a composição do BUS geral nos seus três subcomponentes.

Os controladores de periféricos têm um papel muito importante nos computadores actuais. Esta importância advém, entre outros, de dois factores fundamentais: i) os periféricos têm a capacidade de processamento autónomo e, assim, podem estar a efectuar operações de entrada ou de saída sem ocupar o CPU, o qual se limita a dar instruções ao controlador do periférico, actuando posteriormente de modo autónomo; e ii) havendo um controlador de periféricos para cada um há uma grande especialização do controlador, conseguindo assim ter uma boa eficiência na realização das suas tarefas.

Um computador dispõe de vários controladores de periféricos, um para cada classe (discos, vídeo, impressora, etc.).

Para um mesmo tipo de periférico podem haver vários tipos de controladores, que se distinguem pela sua capacidade em suportar vários periféricos, velocidade de transferência, capacidade de expansão, etc. Por exemplo, para ligar vários discos a um computador há um tipo de controlador específico, o

controlador SCSI (*Small Computer System Interface*) que é muito popular pela sua elevada eficiência associada ao seu custo moderado.

Também para o sistema de vídeo há vários tipos de controladores que se diferenciam pela resolução de visualização, velocidade de representação no ecrã, número de cores representadas em simultâneo, capacidade de efectuar algumas operações gráficas a nível do controlador, etc. Para algumas aplicações, por exemplo, para operações de CAD (*Computer Aided Design*) pode ser muito importante ter um controlador de vídeo de elevado desempenho para as aplicações funcionarem de modo mais avançado.

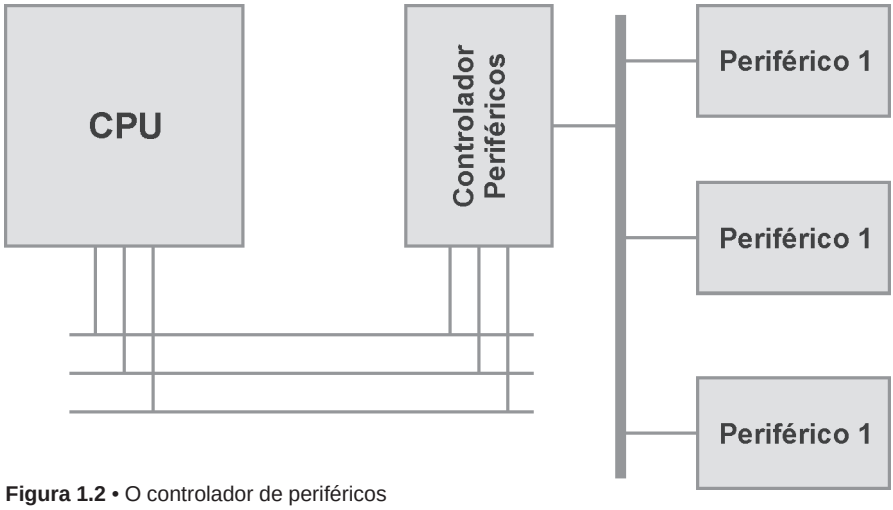

Figura 1.2 • O controlador de periféricos

Ainda em relação à representação da figura 1.2 chamamos a atenção para o BUS que liga o controlador aos periféricos.

1.1.1.2. Periféricos de armazenamento

Nesta classe de periféricos verificaram-se enormes evoluções ao longo dos anos. Incluem-se neste grupo os discos magnéticos (*vulgo*, os discos), as disquetes, vários tipos de bandas magnéticas (cartucho, cinta, DAT, etc.), os CD (*Compact Disk*), os DVD (*Digital Versatile Disk)* e outros menos vulgares.

Os discos estão permanentemente inseridos no computador e têm como principal finalidade servirem para armazenar dados de modo permanente, mesmo quando o computador está desligado. Funcionam como uma memória não volátil, já que não perdem a informação quando o computador está desligado. Nos actuais computadores são usados para várias funções, sendo as mais relevantes: i) a função de extensão da memória central do

computador, realizando parte das funções de gestão de memória do sistema operativo; trata-se de uma função pouco visível ao utilizador comum; e ii) guardando informação entre sessões de trabalho sob a forma de entidades lógicas designadas por **ficheiros**. Estes são as entidades onde os utilizadores guardam a sua informação que podem recuperar em futuras sessões de trabalho.

Nos últimos anos, devido a avanços da electrónica e da mecânica de precisão, têm-se verificado substanciais evoluções na capacidade dos discos, na sua velocidade de transferência e na sua fiabilidade. Em simultâneo, o custo unitário de armazenamento tem diminuído pelo que, no computador, é cada vezes menos relevante o custo do espaço em disco.

As disquetes têm um funcionamento semelhante aos discos, isto é, servem para armazenamento permanente de informação e, pelo facto de serem amovíveis, servem para transportar informação entre sistemas. O seu uso está a diminuir, devido à sua baixa capacidade e baixa fiabilidade.

As bandas ou cintas magnéticas são sistemas que armazenam a informação, sob a forma magnética, numa fita que se enrola em dois rolos. A sua forma varia de caso para caso, desde as bandas antigas de grande dimensão até aos diferentes tipos de cartuchos mais recentes.

As bandas e cintas guardam informação de modo permanente a um custo unitário muito reduzido. Além disso, num pequeno volume, conseguimos guardar grandes quantidades de informação. Podemos dizer que a sua única desvantagem tem a ver com o modo como são escritas e lidas: a escrita e leitura são feitas de modo sequencial, pelo que, quando queremos ler algo que está «no fim» da fita, é necessário percorrer toda a informação anterior. Esta característica leva a que as bandas e cintas magnéticas sejam usadas para fazer cópias de segurança do que está nos discos ou para transporte entre computadores com grandes volumes de dados.

O CD e o DVD são dispositivos também muito importantes. Estes guardam informação em dígitos sob a forma de orifícios feitos por laser numa superfície metálica do disco. Nos discos mais comuns o que é escrito não pode ser apagado.

A vantagem destes dispositivos é de que num volume muito reduzido se consegue guardar um grande volume de dados: em condições normais cerca de 640 Mbytes (MB) para os CD e cerca de 4,7 Gbytes (GB) para os DVD mais vulgares.

Outra grande vantagem dos CD e DVD é que não necessitam de ser acedidos sequencialmente, como acontece nas bandas, e assim o acesso à informação é muito eficiente. Estes dispositivos são hoje largamente usados para distribuição de *software*, para fazer cópias de segurança de informação e para troca de dados entre computadores.

1.1.1.3. Periféricos de entrada/saída

Os periféricos de entrada e de saída, que analisamos nesta secção, são, para o utilizador comum, aqueles com os quais há um maior contacto directo e, também, aqueles onde se têm verificado maiores evoluções. Estas evoluções verificam-se em duas vertentes: i) periféricos convencionais que vão sendo melhorados e com características cada vez mais avançadas; e ii) novos periféricos para preencherem lacunas de interacção entre os utilizadores e o computador.

Os periféricos podem ser só de entrada, só de saída ou serem em simultâneo de entrada e de saída. Este último caso pode ser na realidade assemelhado a dois periféricos separados, um de entrada e outro de saída, que partilham a mesma caixa física.

Nos periféricos convencionais incluem-se, entre muitos outros, aqueles a que todos estamos habituados: teclado, rato, impressoras, *scanners*, saída de som, microfone, etc.

Não iremos naturalmente analisar todos os tipos de periféricos de entrada e de saída, mas iremos focar aqueles que são mais relevantes ou aqueles para os quais se perspectiva uma maior evolução nos próximos anos.

1.1.1.4. Periféricos de visualização

Trata-se de uma classe de periféricos onde a evolução tem sido muito rápida e com um impacto muito significativo na percepção que os utilizadores têm do uso dos computadores.

De um modo simplificado podemos classificar e caracterizar as principais evoluções nos seguintes termos:

- ecrãs mais avançados e diversificados, com dimensões que variam entre alguns centímetros até grandes dimensões; abandono progressivo da tecnologia dos CRT para a tecnologia dos TFT com enormes vantagens na redução de peso, fiabilidade e de transporte; capacidade de representação de muitas cores, com níveis de contraste elevados mesmo na presença de luz do dia;
- sistemas de visualização com características físicas de grande robustez, muito finos e com dimensões físicas muito diversas, o que permitirá que sejam integrados em sistemas de uso comum (automóveis, óculos, etc.)
- ecrãs tácteis, possibilitando a entrada de dados, o que permite uma nova geração de sistemas em que o teclado pode ser removido, sendo a interacção com o utilizador baseada no paradigma de apontar ou escrever

directamente sobre os dados apresentados; estes tipos de ecrãs já são relativamente vulgares nalgumas áreas aplicacionais, como em terminais POS, nos *tablet*-PC e em quiosques;

- controladores de ecrã com acrescidas capacidades a nível de resolução; rapidez de apresentação de grandes volumes de informação gráfica sem sobrecarregar o CPU; miniaturização dos componentes, permitindo a integração em sistemas portáteis de sistemas de visualização de elevada complexidade.

Resumindo, trata-se de um tipo de periféricos que poderá ter uma significativa importância na penetração e na crescente utilização dos computadores em muitas áreas aplicacionais, na medida em que a interface visual é uma das que mais contribui para a maioria dos utilizadores.

1.1.1.5. Periféricos de rede

A evolução da informática tem sido orientada, desde há vários anos, numa direcção em que não faz sentido um computador estar isolado mas sim deve estar integrado numa rede.

Desde uma empresa em que os computadores usados pelos funcionários estão integrados na rede local ou alargada da empresa, à Universidade, onde todos os computadores estão integrados numa rede de grande abrangência geográfica, ao teletrabalhador ou ao trabalhador móvel que precisa de estar em contacto frequente com os computadores da sua empresa para receber e enviar dados relativos ao progresso do seu trabalho, há uma diversidade de situações que obrigam a que se torne cada vez mais importante que cada computador tenha vários modos de se ligar às redes.

Há ainda equipamentos que o utilizador comum não está habituado a ver como um computador, como é o caso do telemóvel. Mas mesmo um telemóvel integra, na realidade, um computador que realiza uma parte significativa das operações de interacção com o utilizador e terá cada vez mais importância a sua ligação à Internet para fornecer serviços de dados aos seus utilizadores. É de esperar que, em breve, surjam no mercado telemóveis com capacidade de se ligarem a redes informáticas, tendo de origem controladores adequados (por exemplo, WIFI [*Wireless Fidelity*]).

A multiplicidade de redes existentes, como veremos nos capítulos seguintes, obriga a que cada computador deva ter **controladores de rede** para os vários tipos de rede que pretenda vir a ligar-se. Infelizmente as características técnicas das diferentes redes não possibilitam que um único controlador permita a ligação de um computador a todos os tipos de redes.

Normalmente os computadores vêm equipados de origem com controladores para as redes mais vulgares. As situações mais correntes são:

- Rede Ethernet, a tecnologia de rede local (LAN) mais vulgar e normalizada pelo IEEE;
- *Modem*, para permitir a ligação através de uma rede telefónica analógica;
- WIFI, a tecnologia de ligação a redes sem fios usando as normas do IEEE, e cujos controladores já começam a ser vulgares nos computadores portáteis.

Para os tipos de rede que são menos vulgares, mas quando o utilizador de computador precisa de as utilizar, há sempre a alternativa de adicionar ao computador um controlador para esse tipo de rede específico. Por exemplo, se um utilizador de um computador se quiser ligar à rede RDIS tem de instalar no seu computador um controlador para RDIS.

Resumindo, a diversidade de tecnologias de rede que existem e que serão criadas nos próximos anos obriga a que para cada tipo de rede seja incorporado no computador um controlador específico para essa mesma tecnologia.

1.1.1.6. Periféricos de reconhecimento de fala

Uma das tecnologias que tem demorado a despontar e a penetrar no mercado é a do reconhecimento de fala. Trata-se de uma tecnologia muito complexa e que necessita de muitos recursos computacionais. Todavia, é uma tecnologia muito importante para diversas aplicações dos computadores e será de esperar que este tipo de periféricos se vá tornando mais vulgar nos próximos anos, dando origem a famílias de sistemas sem teclado reagindo apenas a comandos de voz.

1.1.1.7. Leitores biométricos

Já estão a surgir no mercado alguns computadores equipados de origem com leitores de impressão digital. Do mesmo modo, começam a surgir alguns ratos que incluem um leitor de impressão digital.

Com os crescentes problemas de segurança colocados pela utilização cada vez maior dos computadores são necessários novos mecanismos para garantir o controlo de acesso e outros modos de identificação dos utilizadores. O sistema comum de Código de Utilizador combinado com Código de Acesso (Username/Password) tem as suas limitações.

Sem dúvida que a autenticação dos utilizadores mediante tecnologias biométricas irá crescer e, assim, os leitores de dados biométricos (impressão digital, leitura de íris, reconhecimento de características da fala, etc.) irão tornar-se periféricos comuns dentro de alguns anos.

1.1.2. OS SISTEMAS OPERATIVOS

Talvez mais impressionante que a evolução em termos de *hardware* dos computadores será a evolução dos sistemas operativos. Grande parte das potencialidades e da flexibilidade dos actuais computadores é da responsabilidade do sistema operativo e das aplicações que integra.

O sistema operativo é um componente fundamental dos actuais sistemas de informação. Sem este o computador é praticamente inútil.

O sistema operativo pode ser definido como um vasto conjunto de programas que precisam de estar no computador, desde que este começa a funcionar, e fazem a gestão de todos os recursos de *hardware*, desde o CPU, à memória e a todos os periféricos. Na figura 1.3 podemos ver como é que, do ponto de vista lógico, o sistema operativo está localizado.

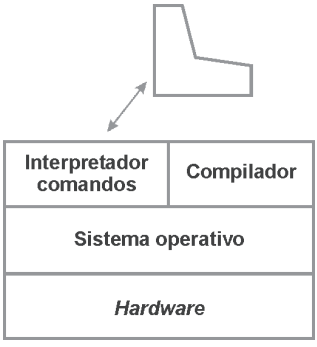

Figura 1.3 • Localização funcional do sistema operativo

Toda a interacção entre os utilizadores e o *hardware* é feita com intermediação do sistema operativo.

O sistema operativo é um extenso conjunto de programas que têm várias funções das quais salientamos as mais importantes e que estão logicamente representadas na figura 1.4:

- Gerir todos os componentes do *hardware* do computador;
- Gerir todos os programas que o computador está a executar (normalmente designa-se por ***processo*** um programa em execução);

- Gerir a memória do computador, promovendo a sua ocupação óptima e libertando espaço de memória se tal fizer falta, levando para o disco os programas que não estão a ser executados num certo momento;
- Executar as operações de Entrada/Saída (E/S), dando aos utilizadores os chamados **periféricos virtuais,** que mascaram a complexidade de cada periférico e dão a cada utilizador a ideia de que os periféricos são todos iguais;
- Criar sobre os periféricos de armazenamento um nível de abstracção que oculte as particularidades de cada disco e dê a visão ao utilizador que dispõe de um conjunto de entidades, chamadas **ficheiros,** que estão organizados logicamente de acordo com paradigmas largamente aceites, as **pastas;**
- Como muitos computadores são usados em simultâneo por vários utilizadores, num ambiente em que estes estão a executar tarefas diferentes, o sistema operativo cria para cada utilizador um ambiente virtual que o isola dos outros utilizadores do computador;
- Implementar mecanismos de segurança que protejam cada utilizador dos outros, impedindo acessos não autorizados à informação que cada um guarda no computador;
- Concretizar mecanismos de salvaguarda que permitam recuperar informação que seja perdida por falha do *hardware* ou por erros dos utilizadores.

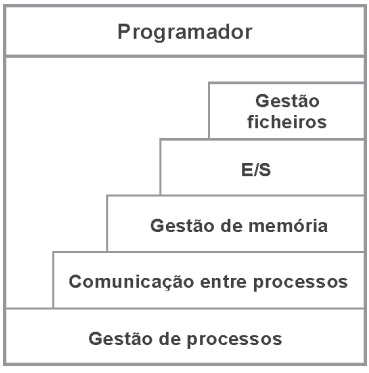

Figura 1.4 • Camadas funcionais de um sistema operativo

Os sistemas operativos mais comuns, como o LINUX™ e as várias versões do UNIX™, o Windows™ ou o MacOS™ todos partilham estas funções concretizando-as de maneiras tecnicamente diferentes, apesar de poderem parecer distintas ao utilizador comum e com uma interface para o utilizador diferente.

1.1.2.1. O modelo cliente/servidor

O modo como os computadores são utilizados foi progredindo ao longo dos anos, dependendo das evoluções tecnológicas.

Inicialmente, cada computador era usado por um conjunto de pessoas no sítio onde estava localizado. Eram os tempos do processamento centralizado.

Com o desenvolvimento das telecomunicações, alguns utilizadores puderam estar localizados a distância. Passou-se para a era dos primeiros sistemas de teleprocessamento. Cada utilizador, quer local quer a distância, tinha à sua frente um terminal com capacidades muito básicas mas que lhe dava acesso ao computador central.

Com o aparecimento dos primeiros computadores pessoais (PC) introduziu-se um modelo em que cada utilizador tinha um computador dedicado, que usava em regime de exclusividade no local onde aquele estava sedeado. Estes computadores tinham uma potência significativa e muitas vezes só uma pequena parte dessa potência era utilizada pelo seu utente.

Com a vulgarização das redes, os computadores centrais passaram a estar ligados a essas redes, o mesmo acontecendo aos computadores pessoais. Esta situação trouxe uma alteração fundamental ao modo como os computadores são usados. Muitas aplicações informáticas foram redesenhadas para poderem aproveitar a grande capacidade dos computadores centrais e, também, a capacidade dos computadores pessoais que lhes estavam ligados. Este é um paradigma muito vulgar na informática actual, chamado modelo cliente-servidor (representado na figura 1.5), e muitas das aplicações actuais funcionam deste modo.

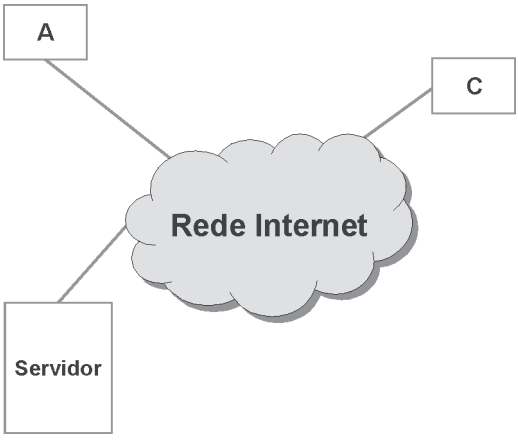

Figura 1.5 • Representação esquemática do modelo cliente-servidor

Segundo o paradigma cliente-servidor há computadores especializados na realização de certas funções, os servidores, que podem ser acedidos e usados por computadores que a eles estejam ligados através de uma rede, os clientes.

O exemplo mais vulgar desta situação é quando acedemos à Internet. Há computadores espalhados pela Internet que disponibilizam conteúdos muito diversos (por exemplo, um jornal, um banco, uma universidade) em formatos normalizados. Quando um de nós quer aceder a esses conteúdos dá comandos ao seu computador cliente para ir buscar os conteúdos ao servidor em questão. Estes conteúdos são transferidos do servidor para o cliente, que depois os mostra ao seu utilizador. Manipulações feitas no computador do cliente que não envolvam mais trocas de informação com o servidor, como, por exemplo, alterações ao tamanho e formato da janela de visualização ou impressão da página que fomos buscar, são feitas exclusivamente no cliente sem envolver o computador servidor. Esta solução tem a vantagem de não sobrecarregar o servidor com tarefas que o cliente pode fazer e também contribui para reduzir o tráfego total que atravessa a rede.

O modelo cliente-servidor é a base da concepção de muitas aplicações modernas. Apoia-se no facto de os computadores clientes terem uma capacidade significativa de computação autónoma, libertando os servidores para o desempenho mais especializado das suas funções (servidor de base de dados, servidor de disco, servidor de impressão, servidor de correio electrónico, etc.).

Para pequenas organizações o modelo cliente-servidor é adequado à sua estrutura, ficando o servidor alojado nas instalações de uma empresa especializada através de um pagamento desse serviço, libertando a empresa das tarefas de gestão do servidor, do seu alojamento e da sua segurança. Além disso como a empresa que faz o alojamento do servidor tem, regra geral, uma ligação de alta capacidade para a Internet, o servidor da empresa está acessível a toda a Internet sem sobrecarregar o acesso da empresa à mesma.

1.1.2.2. Normalização

A evolução da informática tem sido fortemente marcada por desenvolvimentos feitos por empresas que procuram impor as suas soluções para poderem moldar as evoluções do mercado.

Este posicionamento, que se entende por parte destas empresas, tem levado, por outro lado, os utilizadores e os governos a preocuparem-se na criação de normas que os tornem menos dependentes de soluções proprietárias de uma empresa e que contribuam para criar mercados mais alargados pela massificação que as normas potenciam. Esta massificação conduz, regra ge-

ral, a produtos mais baratos, devido ao aumento da base de clientes, e também mais robustos por serem testados por mais utilizadores.

Por outro lado, a normalização origina forçosamente consensos para criação das normas e pode, portanto, tornar mais lenta a introdução de novas soluções tecnológicas no mercado.

Na área dos sistemas de informação e das redes há diversos organismos que são relevantes para a normalização, apresentando-se de seguida uma breve descrição das áreas em que estes intervêm.

1.1.2.3. IEEE

O IEEE, *Institute of Electrical and Electronics Engineers*, é uma associação profissional e científica de engenheiros, com sede nos Estados Unidos mas com delegações em muitos países do mundo, incluindo Portugal. O IEEE tem um papel muito importante na normalização ligada a alguns protocolos das redes de dados em especial no que se refere à tecnologia Ethernet nas suas várias vertentes, o que inclui as tecnologias sem fios vulgarmente designadas por WIFI.

O IEEE também tem estado envolvido em aspectos de normalização ligados aos sistemas operativos, em especial o POSIX, *Portable Operating System Interface*.

A informação sobre o IEEE está disponível em www.ieee.org.

1.1.2.4. IETF

O IETF, *Internet Engineering Task Force*, é o organismo responsável pela produção de normas relativas aos protocolos da Internet. É uma organização aberta que envolve engenheiros de redes, operadores, fabricantes de *hardware* e *software*, investigadores e todos os que estão interessados com a evolução e a operação estável da Internet.

A informação sobre o IETF está disponível em www.ietf.org.

1.1.2.5. W3C

O W3C, *World Wide Web Consortium*, é uma organização privada sem fins lucrativos que desenvolve tecnologias interoperáveis (especificações,

linhas de orientação, *software* e ferramentas informáticas) relacionadas com a World Wide Web e funciona como um fórum de troca de informação, comércio e comunicação à volta da WWW.

A informação sobre o W3C está disponível em www.w3c.org.

1.1.2.6. ISO

O ISO, *International Standards Organization*, é uma organização internacional que produz normas numa série de áreas, muitas delas relevantes para a informática e para as redes (por exemplo, as normas das séries ISO 9000 e ISO 14000 entre muitas outras).

O ISO é uma rede de institutos de normalização de 148 países que trabalham colaborativamente e que envolvem governos, indústria, empresas e consumidores.

A informação sobre o ISO está disponível em www.iso.org.

CAPÍTULO

2

CONCEITOS BÁSICOS SOBRE A ARQUITECTURA DA INTERNET

OBJECTIVOS

- É feita uma breve referência aos princípios subjacentes à concepção da Internet e que conduziram ao seu sucesso.
- São apresentados os princípios da arquitectura e dos protocolos da Internet.

P O N T O D A S I T U A Ç Ã O

A Internet foi criada para permitir a interligação de computadores de um modo simples e com tolerância a falhas, inicialmente para aplicações militares.

Estas características foram decisivas a uma tecnologia que se tornou a solução central para a ligação dos principais sistemas de informação e, também, a tecnologia de comunicação, base da sociedade da informação neste início do século XXI.

A década de 90 foi marcada pela massificação do uso da Internet pelos cidadãos, pelas organizações e pelas empresas. Esta massificação contribuiu para uma globalização do acesso à informação que obrigou à mudança de como as pessoas e os agentes económicos interagem entre si e com a Administração Pública.

2.1. CONCEITOS BÁSICOS SOBRE A ARQUITECTURA DA INTERNET

As ideias que conduziram à concepção da Internet, de como esta rede existe hoje em dia, resultaram de um projecto de investigação aplicada, iniciado na década de 60, e cujo objectivo era ligar vários computadores nos Estados Unidos de modo a que a rede criada tivesse elevada tolerância a falhas. Este requisito foi motivado pelo ambiente político da Guerra Fria e tinha como finalidade garantir que mesmo depois de uma potencial guerra em que muitos meios de comunicação e computadores desta rede fossem destruídos, os restantes sistemas podiam continuar a comunicar e a desempenhar as suas funções de apoio às operações logísticas militares.

Atendendo à fraca capacidade de comunicação das redes de telecomunicações que na altura existiam, a tecnologia que veio a ser desenvolvida também devia funcionar bem em ligações de baixa velocidade (à escala actual) e com uma multiplicidade de meios de comunicação, como circuitos terrestres de vários tipos e ligações satélite.

2.1.1. A COMUTAÇÃO DE PACOTES

Uma das ideias fundamentais de qualquer rede de comunicação de dados, como a Internet, é de que a informação a trocar entre os computadores é dividida em pequenas quantidades de informação a que se atribui a designação de **pacote.**

Quando um computador pretende, por exemplo, enviar um ficheiro para outro computador, parte-o em pacotes e submete-os à rede para serem transmitidos para o computador de destino. No esquema da figura 2.1 podemos ver quatro computadores ligados à Internet. Se o computador A pretende enviar informação para o computador D, divide essa informação em três pacotes e submete-os, separadamente, à Internet que trata de os enviar para o computador de destino, o D. O trajecto que cada pacote segue para chegar ao destino pode ser diferente, podendo chegar ao computador D por uma ordem diferente daquela em que foi enviado. Pode também acontecer que alguns pacotes não cheguem ao destino por falha momentânea da rede. Esta situação pode parecer estranha mas como veremos existem mecanismos para corrigir estas situações e foram, inclusive, estas características da Internet, tornando-a uma rede tecnologicamente mais robusta que outras tecnologias que foram desenvolvidas mas que acabaram por ser abandonadas.

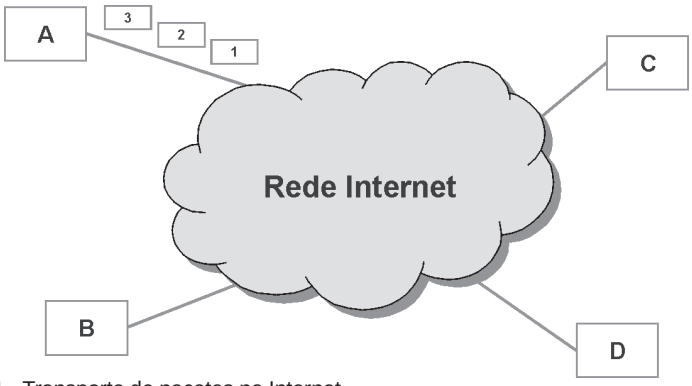

Figura 2.1 • Transporte de pacotes na Internet

Para ultrapassar estas particularidades da Internet, onde não se garante uma entrega ordenada e fiável dos pacotes (diz-se que a Internet funciona segundo o paradigma do «melhor esforço», ou seja a rede *tenta o melhor possível* fazer chegar os pacotes ao destino), há mecanismos que permitem ordenar os pacotes que chegam fora de ordem e pedir o reenvio daqueles que não chegam ao destino.

2.1.2. OS PROTOCOLOS DA INTERNET

Para ultrapassar as situações referidas na secção anterior há um conjunto de regras que são usadas para conseguir que o fluxo de informação através da Internet seja ordenado e tenha sucesso.

Designa-se por **protocolo** um conjunto de regras que definem o modo como a informação é formatada – os pacotes – e como os sistemas que constituem a Internet interagem de modo a garantir o fluxo coerente e eficiente de informação na Internet.

Os protocolos estruturais da Internet são dois, o IP (*Internet Protocol*) e o TCP (*Transmission Control Protocol*), e costumam ter a designação de TCP/ /IP. Estes protocolos funcionam nos sistemas internos da Internet, como os que constituem a Rede Internet esquematizada na figura 2.1, e também nos computadores e outros sistemas que pretendemos ligar à Internet (por exemplo, um computador, um telemóvel).

2.1.2.1. Os protocolos organizados em camadas

Os protocolos de qualquer rede de comunicação e os da Internet, em particular, estão organizados em camadas, isto é, um protocolo relaciona-se com protocolos adjacentes, como se representa na figura 2.2.

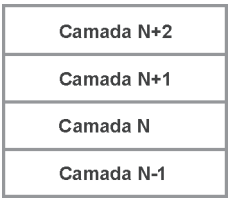

Figura 2.2 • Arquitectura de uma rede em camadas

Há muitas vantagens nesta organização mas a principal é a modularidade e independência de concepção que cada protocolo tem dos outros. Assim é possível alterar o protocolo N à vontade, desde que se mantenham as suas interfaces com os seus níveis adjacentes acima e abaixo (N+1 e N-1). Para os outros protocolos, por exemplo N+2, as alterações ao protocolo N são irrelevantes. Consegue-se, com esta arquitectura de camadas, um nível de modularidade que tem sido um dos sucessos da Internet, ao permitir alterações incrementais a uma camada sem que isso seja visível ou cause qualquer tipo de perturbação na rede. Só assim tem sido possível à Internet crescer e ser adaptada às suas necessidades de evolução de um modo transparente para os seus utilizadores.

No caso da Internet os protocolos TCP e IP relacionam-se como se representa na figura 2.3. Aqui podemos ver que o protocolo TCP está acima do protocolo IP.

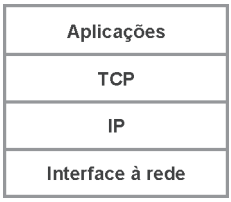

Figura 2.3 • Arquitectura de camadas da Internet

O estrato do protocolo IP costuma designar-se camada (ou nível) de rede e a camada do TCP designa-se transporte, pelas funções que desempenha na condução fiável de informação através da Internet.

2.1.2.2. O protocolo IP

O protocolo IP destina-se a definir como os pacotes são enviados de um computador origem a um computador destino e são compostos, de modo simplificado, por três partes fundamentais:

- Endereço do computador de destino;
- Endereço do computador de origem;
- Dados a transmitir.

O endereço é um componente fundamental da Internet e é o meio usado para identificar de modo unívoco cada computador, que num certo momento está ligado à Internet. Do mesmo modo que, por exemplo, cada telemóvel tem um número que o identifica, da mesma maneira cada computador ligado à Internet dispõe de um endereço específico. Os endereços dos computadores ligados à Internet, designados endereços IP, são conjuntos de 32 bits e costumam ser representados por questões de legibilidade sob a forma de quatro números decimais separados por um ponto, por exemplo 215.168.0.12 é um endereço IP de um computador ligado à Internet.

Os endereços IP são a identificação básica de qualquer computador ligado à Internet e são usados para, entre outros aspectos, a rede conseguir levar um pacote desde a origem até ao destino.

Com os 32 bits de endereços podem haver cerca de 4000 milhões de computadores distintos ligados à Internet, o que é considerado hoje uma séria limitação e que, como veremos, levou ao desenvolvimento de uma nova versão do protocolo IP, que se designa IPv6, o qual não tem estas limitações.

2.1.2.3. O protocolo TCP

Este outro protocolo é responsável por detectar perdas de pacotes IP ou pela chegada ao destino de pacotes IP fora de ordem. Este protocolo é executado nos computadores que pretendem comunicar e numera, sequencialmente, cada pacote enviado para a rede. No destino detecta pacotes em falta e pede a sua retransmissão ao computador de origem. O TCP também é responsável pela reordenação dos pacotes que chegam fora de ordem, usando para isso a numeração que introduziu.

A finalidade do TCP pode ser descrita como aquela que fornece um fluxo de bits entre os dois computadores que comunicam, independentemente das limitações ou falhas da rede Internet durante a comunicação.

O protocolo TCP tem ainda outras funções, cuja análise ultrapassa o âmbito deste manual mas que, de modo sintético, tem a ver com a adaptação da velocidade de transmissão às condições da rede em cada momento e aos meios de transmissão atravessados no percurso entre os dois computadores comunicantes.

2.1.2.4. A interface à rede

Para um utilizador comum são os protocolos aplicacionais que concretizam as aplicações que lhe interessam. Para um utilizador comum o que lhe interessa é enviar uma mensagem de correio electrónico ou ter acesso a um sítio na Internet. Estes protocolos estão conceptualmente localizados sobre o nível TCP e serão por nós analisados em maior detalhe no próximo capítulo.

Vamos agora analisar a camada da interface à rede, a qual fornece os meios físicos que permitem transportar os pacotes IP entre quaisquer dois computadores localizados em qualquer sítio podendo, por exemplo, estes dois computadores estarem em pontos opostos do planeta.

Contrariamente a outros protocolos que foram usados durante vários anos mas vieram a ser substituídos, o IP tem a particularidade de poder funcionar sobre um número muito diverso de meios de telecomunicações. Esta flexibilidade foi uma outra das razões do sucesso do protocolo IP. Nos seus primórdios as primeiras experiências com o protocolo IP foram feitas em circuitos de telecomunicações de baixa velocidade e de elevada taxa de erros, em linhas telefónicas e em circuitos por satélite.

Com a enorme evolução tecnológica das telecomunicações o protocolo IP foi sendo adaptado, e hoje em dia funciona sobre uma grande diversidade

de meios de telecomunicações e tem tido capacidade de se adaptar às novas tecnologias que vão surgindo.

Os meios de telecomunicações mais utilizados para concretizar a interface à rede do protocolo IP são:

- Linhas telefónicas analógicas, que foram durante vários anos os meios mais usados por utilizadores que precisam de baixa velocidade e que ainda hoje são muito utilizados; servem para ligar um único computador, o qual necessita de um *modem,* que é o dispositivo que adapta o mundo digital do computador ao mundo analógico da linha telefónica;
- Acessos através da televisão por cabo, em que os operadores de telecomunicações instalaram uma capacidade de transmissão bidireccional na sua infra-estrutura de distribuição por cabo, colocando um *cable-modem* em casa do cliente que se liga ao computador;
- Acesso por ADSL (*Asymmetrical Digital Subscriber Loop*) que permite, mediante a linha telefónica convencional, ter, além de uma conversa telefónica normal, uma comunicação de dados que é usada para suportar o protocolo IP; esta tecnologia tem a vantagem de usar a infra-estrutura da rede telefónica que chega a quase todos os locais, necessitando apenas dos investimentos para instalar capacidade ADSL nas centrais; a ligação está sempre disponível e tem a particularidade de ter uma velocidade de recepção superior à da transmissão, o que torna esta tecnologia adequada para instituições consumidoras de tráfego; todavia é pouco adequada caso se pretenda fornecer informação, por exemplo, para uma empresa que aloja nas suas instalações um servidor Internet.
- Circuitos dedicados são normalmente usados para ligar empresas ou outras organizações que precisem de débitos de recepção e do envio de dados mais elevados; a velocidade nos dois sentidos é igual, sendo uma solução melhor que o ADSL quando se tem um servidor dentro da organização;
- Fibra óptica é uma tecnologia muito avançada, porque permite velocidades de transmissão muito elevadas e tem taxas de erro muito baixas; a sua instalação é mais cara que os outros tipos de tecnologias, especialmente por causa da maior dificuldade em efectuar as ligações, se bem que nos últimos anos este custo se tenha reduzido de modo significativo; além disso há muito pouca fibra instalada pelo que a sua escassez também determina o seu elevado custo;
- Rede WIFI é uma tecnologia de ligação sem fios que utiliza bandas de frequência que estão livres (Banda ISM) em torno dos 2,4 GHz e dos 5 GHz; o computador precisa de ter um controlador de WIFI e de

estar próximo de uma antena com autorização de acesso (distâncias até 50 metros dependendo das condições da instalação em uso); a velocidade de comunicação entre o computador e a antena é de 11 Mbps ou de 54 Mbps, dependendo do tipo de equipamento utilizado; trata-se de uma tecnologia muito promissora face aos custos muito moderados dos equipamentos necessários para construir as redes WIFI;

- Rede móvel de 2.ª ou 3.ª gerações, dos telemóveis, consiste em usar a capacidade de comunicação em pacotes das redes dos telemóveis, usando-as para transmitir pacotes IP; a 2.ª geração de telemóveis tem uma capacidade de comunicação bastante limitada, enquanto que a 3.ª geração, que foi concebida de raiz para se adequar à transmissão de dados de alta velocidade, permite antecipar a boa adequação como tecnologia de ligação à Internet, também sem fios; tem maior capacidade de alcance prevendo-se que, após a sua instalação, esteja disponível em qualquer ponto do país;
- As ligações por satélite permitem ligar um computador à Internet, também sem fios, mas recorrendo à transmissão através de um satélite; este tipo de ligação permite uma velocidade de comunicação elevada e tem a vantagem de permitir a ligação rápida em qualquer local, mesmo que não existam outras infra-estruturas de comunicações.

2.1.2.5. O *router*

A ligação à rede Internet é então feita usando uma das tecnologias que acabámos de descrever de modo sucinto. Quando se quer ligar um só computador à Internet, basta ter um equipamento que faça a adaptação entre o computador e o tipo de interface de rede em uso (*modem*, *cable-modem*, *modem* ADSL, etc.). Todavia, há muitas situações em que se pretende ligar vários computadores à Internet. Aliás, esta é a situação mais frequente numa organização onde há vários computadores interligados entre si através de uma rede local e se pretende que todos tenham acesso à Internet. Para esta situação entre a rede local e o acesso à Internet é preciso um equipamento chamado *router* (encaminhador, em português).

Na figura 2.4 podemos ver esquematicamente como é que o *router* é usado para ligar a rede local de uma organização à Internet. Nesta figura representa-se a rede local (LAN – *Local Area Network*) de uma organização com quatro computadores. O papel do *router* é ligar esta rede local à Internet. O *router* analisa os pacotes que circulam na rede local e se são somente pacotes especí-

ficos à rede local nada faz. Quando se trata de um pacote destinado a um computador não pertencente à rede local, ou seja, caso se trate de um pacote destinado à Internet global, o papel do *router* é enviá-lo para esta rede. De modo análogo quando um qualquer computador quer enviar um pacote para qualquer computador desta rede local, este pacote será encaminhado pela Internet até ao *router* da organização que o entrega ao computador de destino.

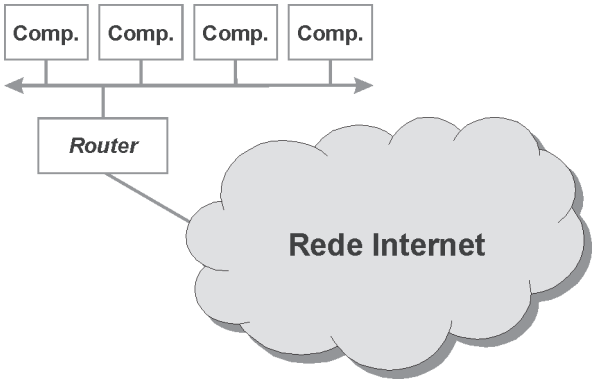

Figura 2.4 • Papel de um *router* na Internet

Desta exposição simples podemos ver que o papel do *router* é, basicamente, servir de intermediário entre um acesso à Internet e vários computadores. Mas além desta função básica os *routers* actuais têm outras funções muito mais complexas que têm a ver com a gestão da ligação à Internet, com funções de filtragem de certos tipos de tráfego, entre outras, mas cuja análise ultrapassa o âmbito deste texto. Trata-se, pois, de um elemento fundamental para a ligação de uma organização à Internet.

E S T U D O D E C A S O

É importante que exista uma rede informática a ligar todos os serviços da autarquia?

A resposta a esta pergunta é, evidentemente, afirmativa.

A necessidade de tornar mais eficientes os serviços que as autarquias prestam passa, necessariamente, pela informatização de todos os serviços. Para atingir este fim há, regra geral, que concretizar uma série de etapas de reorganização dos serviços com vista à sua informatização. Há, porém, uma infra-estrutura que tem de estar sempre presente: a rede informática da autarquia. Esta rede deverá estar disponível em todos os locais, onde a autarquia tem presença, e deverá ter diferente complexidade e abrangência consoante a dimensão e dispersão geográfica dos vários edifícios. Em cada edifício deve ser instalada uma rede local

(LAN), usando a tecnologia Ethernet, e as redes locais dos vários edifícios devem ser interligadas através de uma rede metropolitana (MAN). Para interligar os edifícios podem ser usadas várias soluções. Atendendo a que muitas autarquias já possuem condutas próprias, um cenário que deve ser equacionado é o da instalação de infra-estrutura própria de ligação aos diversos edifícios, por exemplo, através de fibra óptica própria. O custo deste investimento pode ser bastante moderado, pois o preço da fibra óptica é muito baixo e permite altas capacidades de transmissão de dados. O maior investimento já foi feito: as condutas por onde a fibra passa.

Todavia, a gestão de uma rede deste tipo é um pouco complexa, precisa de recursos humanos adequados, e a decisão de construir uma rede própria deve ser devidamente ponderada, face às disponibilidades de recursos humanos capacitados para a explorar sem problemas. Enquanto tal não acontece o mais sensato a fazer será a gestão desta infra-estrutura, através de meios externos, em regime de *outsourcing*.

2.1.2.6. O IPv6

No início dos anos 90, com o rápido crescimento da Internet, começou a prever-se que o número de endereços IP disponíveis seria escasso a curto prazo. Recorde-se que cada computador ligado à Internet precisa de ter o seu endereço IP específico, o qual tem de ser diferente do de qualquer outro computador ligado à Internet. Extrapolações feitas ao crescimento da Internet, com base em diferentes pressupostos, davam como limites de utilização do protocolo IP na sua versão actual, o IPv4 (IP *version* 4), datas entre 1997 e 2006.

Neste contexto «de crise» foi decidido desenvolver uma nova versão do protocolo IP. Este trabalho foi levado a cabo no seio do IETF e foram convidados grupos de especialistas para propor novas versões do protocolo IP que ultrapassassem as limitações já identificadas para o IPv4. As principais eram as seguintes:

- Escassez de endereços: os cerca de 4000 milhões de endereços distintos não permitiam, por exemplo, que cada habitante da Terra viesse a ter um endereço;
- Segurança: o protocolo IPv4 não tem mecanismos de segurança que permitam concretizar redes com elevados níveis de segurança;
- Autoconfiguração: o protocolo IPv4 é tão complexo que obriga a um conhecimento apreciável da sua natureza para configurar a ligação de um computador à rede;
- Mobilidade: quando se desloca um computador de uma rede para outra é necessário, em IPv4, fazer diversas alterações à configuração do computador que convém eliminar.

Do trabalho realizado no seio do IETF veio a ser escolhida uma nova versão do protocolo IP, o IPv6 (IP versão 6). Este novo protocolo supria as limitações atrás referidas e, no caso particular dos endereços, ao prever que estes passariam a ter 128 bits, aumenta significativamente a capacidade da Internet. Trata-se de um número tão grande, difícil de conceptualizar, mas podemos dizer que permite milhões de endereços para cada metro quadrado da superfície terrestre.

2.1.2.7. A introdução do IPv6

Paralelamente à criação do IPv6, outros grupos de trabalho estudaram métodos alternativos de aumentar a longevidade do IPv4, pois adivinhava-se que o trabalho de fazer transitar toda a Internet para IPv6 seria grande.

Assim foram sendo desenvolvidas iniciativas que seguiram as seguintes linhas mestras:

- Aumentar o tempo de vida do IPv4, através de uma gestão mais cuidada do espaço de endereços, disponibilizando os poucos a quem os pedia (até aí o controlo da distribuição de endereços era praticamente inexistente) e recuperando aqueles que não estavam a ser usados;
- Criar mecanismos para reaproveitamento de endereços, por exemplo, quando um computador estiver desligado, usar o seu endereço por outros utilizadores; em especial em grandes organizações ou em operadores de telecomunicações, em que nem todos os computadores estão a ser usados ao mesmo tempo, só se «gastam» endereços para os computadores que estão em uso simultâneo, fazendo-se uma reciclagem de endereços IP;
- Criar mecanismos de atribuição dinâmica de endereços no IPv4, de modo a facilitar a mobilidade dos utilizadores e simplificar a gestão de redes complexas;
- Aproveitar a arquitectura de segurança que tinha sido proposta para o IPv6 e integrar o IPv4 nessa arquitectura.

Estas medidas vieram permitir o aumento de vida do IPv4 para além do esperado, e hoje em dia já não há a certeza de qual o ano em que será necessário começar a usar como protocolo principal o IPv6.

A nível nacional e internacional já há várias redes a usar o protocolo IPv6, e a União Europeia tem desenvolvido políticas activas de promoção deste protocolo, incluindo chamadas de atenção aos Estados-membros para

uma introdução rápida do mesmo. Todavia, como se trata de uma área onde a liderança deveria partir do sector privado, em particular dos ISP, há que esperar que estes comecem a fazer migrar todas as suas redes para IPv6.

Trata-se, todavia, de uma área onde os governos podem e devem ter um papel activo, através de políticas de aquisição de equipamentos e redes, que sejam compatíveis com o IPv6, e da implementação de políticas activas de procura, que solicitem o IPv6. Nesta área, os países do Extremo Oriente, em particular o Japão, a Coreia do Sul e a China têm estado bastante activos na migração das redes e dos seus serviços para IPv6.

Se bem que se anteveja que a exaustão dos endereços IPv4 só se verifique dentro de 20 anos, quanto mais rápida for a introdução do IPv6 mais preparadas estarão as instituições para as vantagens na Internet de nova geração.

CAPÍTULO

3

O NÍVEL APLICACIONAL NA INTERNET

OBJECTIVOS

- A camada superior da arquitectura da Internet é a aplicacional. É esta camada que é mais visível ao utilizador comum e aquela que lhe fornece os serviços que usamos no nosso dia-a-dia.
- São analisadas as principais aplicações usadas nas organizações e os pressupostos subjacentes à sua utilização.

PONTO DA SITUAÇÃO

Uma das razões do sucesso da Internet é a superior qualidade dos protocolos nucleares da rede, o TCP/IP, e a sua capacidade de adaptação aos diferentes meios de telecomunicações que vão sendo disponibilizados, fruto da evolução tecnológica.

Contudo, são as aplicações que são relevantes para os utilizadores finais. A simplicidade e flexibilidade destas aplicações têm tornado possível a sua implementação em sistemas muito diferentes, desde computadores de grande porte, aos computadores pessoais e até a computadores de bolso e telemóveis.

Neste capítulo são apresentadas as principais aplicações e, nalguns casos, como estas são integradas nos sistemas de informação e nas redes das organizações.

3.1. O NÍVEL APLICACIONAL NA INTERNET

Como vimos no capítulo anterior a Internet baseia-se em duas camadas protocolares fundamentais, o IP e o TCP, sobre os quais se suportam as aplicações.

O protocolo IP trata do envio de datagramas através da Internet de um modo eficiente mas não fiável, podendo dar-se o caso da perda de datagramas, ou então eles chegarem fora de ordem. Por esta razão costuma dizer-se que a Internet funciona sob o paradigma do **melhor esforço** (*best effort* na terminologia anglo-saxónica), ou seja, na Internet todos os elementos intervenientes tentam fazer levar os datagramas da origem ao destino de um modo muito eficiente mas isso nem sempre é garantido. Uma situação que por vezes acontece, impedindo que os datagramas transitem pela Internet de modo fiável, é quando há situações de congestionamento da rede.

O protocolo TCP tenta remediar as particularidades do IP introduzindo mecanismos que permitem recuperar estas situações.

Na realidade há um outro tipo de protocolo de transporte que é usado na Internet, o UDP (*User Datagram Protocol*). Este protocolo apresenta algumas semelhanças funcionais com o TCP mas não garante entrega fiável dos dados entre dois computadores que comunicam através da Internet. Esta situação pode parecer estranha para o utilizador comum mas existem aplicações em que a entrega de dados com garantia não é o mais relevante (por exemplo, numa videoconferência) e o que é importante é a eficiência do protocolo e, neste aspecto, o UDP é mais eficiente que o TCP. Todavia, neste texto não aprofundaremos este pormenor por não ser crucial para a compreensão global do funcionamento das redes e dos sistemas de informação.

3.1.1. AS APLICAÇÕES

O número de aplicações que se suportam na Internet é muito vasto mas a compreensão da sua natureza e da sua arquitectura pode ser entendida estudando unicamente um conjunto limitado destas.

Em meados da década de 80, quando os principais protocolos aplicacionais da Internet começaram a ser desenvolvidos, foi dada uma grande ênfase à simplicidade dos mesmos. Esta decisão teve por base o facto de os computadores da altura não serem muito poderosos do ponto de vista computacional. Assim, considerava-se necessário fazer protocolos simples de modo a não absorverem muitos recursos. Esta decisão veio a mostrar-se fundamental para a evolução da Internet. Sem dúvida que os computadores vieram a tornar-se mais avançados, mas o facto de os protocolos aplicacionais serem simples facilitou a sua implementação numa grande diversidade de sistemas. Em particular, permite que estes protocolos possam, hoje em dia, ser postos a funcionar em sistemas tão simples como, por exemplo, um PDA (*Personal Digital Assistant*) ou um telemóvel.

Assim iremos analisar alguns dos principais protocolos aplicacionais da Internet abordando também, conforme adequado, o modo como é concretizada a sua utilização nas organizações.

3.1.1.1. Correio electrónico

O correio electrónico foi uma das primeiras aplicações das redes de dados e ainda hoje é uma das aplicações mais usadas. É também, em muitos casos, a aplicação que muitas pessoas começam a utilizar quando se iniciam na Internet.

Para usar o correio electrónico há actualmente dois modos de o utilizar.

Num dos casos recorre-se a um programa chamado **agente utilizador** que recebe e envia todo o correio, através de um servidor de correio electrónico; esta situação está representada na figura 3.1, onde se podem ver quatro computadores pessoais ligados a uma rede local à qual, por sua vez, também está ligado o servidor de correio electrónico. Quando no nosso computador pessoal, após termos preparado uma mensagem a enviamos, essa mensagem é encaminhada do computador pessoal ao servidor, o qual, através da Internet, procede o seu envio para o destinatário. No processo de recepção passa-se de forma inversa. Quando não temos o nosso computador pessoal ligado à rede e nos enviam correio electrónico, as mensagens vão sendo armazenadas no servidor. Ao ligarmos o nosso computador pes-

soal e ao activarmos o agente utilizador, então todas as mensagens que foram ficando armazenadas no servidor são trazidas para o nosso computador pessoal, onde as podemos tratar.

Para troca de mensagens entre o nosso computador pessoal e o servidor há protocolos específicos, sendo um dos mais populares o POP (*Post Office Protocol*).

No que se refere ao agente utilizador, onde está instalado o computador que usamos, há alguns muito populares como o Microsoft Outlook, Netscape, Mozilla, os quais têm funcionalidades semelhantes.

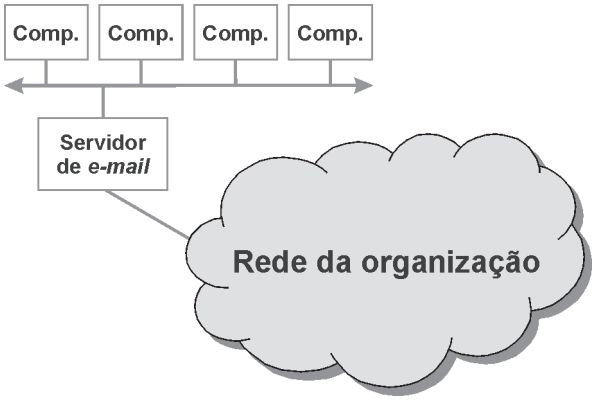

Figura 3.1 • Papel de um servidor de *e-mail* na Internet

Outra maneira de usar o correio electrónico é através do chamado Web-Mail. É um modo de uso do correio electrónico que foi popularizado pela WWW e que consiste, basicamente, em todo o correio electrónico estar guardado num servidor central que pode ser acedido por meio de um navegador da Internet, como o Internet Explorer ou o Netscape. Muitos utilizadores usam sistemas como o Hotmail.com, Yahoo.com ou o Megamail.pt, entre outros em que o correio electrónico funciona segundo este paradigma. Este sistema é vantajoso para o utilizador, uma vez que este pode aceder ao seu correio electrónico em qualquer sítio, necessitando apenas de ter acesso a um computados com ligação à Internet.

O sistema Web-Mail é muito vulgar para utilizadores que não têm um local fixo de acesso ao correio electrónico e que querem ter um mínimo de esforço na gestão do seu sistema de correio electrónico. O outro sistema é mais adequado a ambientes empresariais e tem a vantagem de que o correio pode ser tratado localmente no computador pessoal do utilizador, de modo mais avançado e mais flexível, mas obriga a uma gestão um pouco mais complexa do sistema.

Para transferir mensagens de correio electrónico entre servidores foi desenvolvido na Internet um protocolo específico, o SMTP (*Simple Mail Transfer Protocol*). Através deste protocolo as mensagens de correio electrónico são transformadas num formato específico e levadas do servidor de origem para o de destino.

ESTUDO DE CASO

Nos últimos anos o SPAM (correio electrónico não solicitado) tornou-se um dos maiores pesadelos dos utilizadores da Internet. Quando se abre a caixa do correio electrónico esta aparece «poluída» por enorme quantidade de mensagens de correio electrónico indesejáveis, na maioria das vezes com publicidade de produtos diversos mas, também, com ofertas enganosas de promessas de enriquecimento rápido. A famosa mensagem do comerciante de petróleo da Nigéria é, entre muitas outras, uma das que enchem as caixas de correio electrónico dos utilizadores da Internet. Como nos podemos resguardar do SPAM?

Não há uma receita universal para este efeito mas podem-se indicar algumas regras básicas no sentido de diminuir a probabilidade de sermos alvos de ataques do SPAM: i) não divulgar publicamente o nosso endereço de correio electrónico, de modo a evitar que este seja capturado e incluído nas listas de endereços que são alvo do SPAM; ii) instalar nos servidores da nossa organização e nos nossos programas clientes de correio electrónico filtros de SPAM; iii) nunca abrir mensagens de correio electrónico provenientes de um utilizador que não conhecemos ou em que o assunto nos parece suspeito, pois estas mensagens são também, com frequência, o meio de transporte de vírus e cavalos de Tróia, podendo causar sérios problemas de segurança.

No caso da Administração Pública, em que o correio electrónico já é equiparado a outros meios (carta, fax) para efeito de contactos com os utentes dos serviços públicos, há que dar formação aos funcionários de modo a ensiná-los os processos que conduzem à diminuição dos prejuízos do SPAM para o seu trabalho.

3.1.1.2. Transferência de ficheiros

A transferência de ficheiros foi a primeira grande aplicação que despertou o interesse dos engenheiros das primeiras redes de computadores. O objectivo das primeiras redes de computadores era transferir dados existentes num computador para outro, localizado num local distinto, de modo eficiente, evitando assim o transporte de dispositivos de armazenamento, como as bandas magnéticas.

Actualmente, esta aplicação ainda é muito usada, mas na maioria das situações é mascarada através de outros protocolos aplicacionais, como os que estão associados à WWW.

Trata-se de uma aplicação em que os ficheiros são directamente transferidos entre o computador que tem o ficheiro e o computador para onde o queremos copiar. É uma aplicação que se enquadra no paradigma par-a-par (*peer-to-peer*) e que foi vulgarizada, por exemplo, pelo programa Kazaa.

3.1.1.3. HTTP

O grande sucesso da Internet junto do grande público deveu-se à invenção da World Wide Web (WWW).

A WWW foi inventada no Centro Europeu para a Investigação Nuclear, o CERN, sedeado em Genebra por uma equipa chefiada por Tim Berners-Lee. O objectivo fundamental da equipa de investigação consistia em desenvolver um sistema que permitisse aos investigadores do CERN terem acesso a grandes e diversificados repositórios de informação contendo texto, imagens, vídeos, entre outro tipo de documentos, mas ocultando a complexidade da localização, tipo de informação e as especificidades da comunicação. Os utilizadores finais eram os investigadores do CERN que não queriam perder tempo com estes pormenores técnicos para se poderem concentrar no seu trabalho.

O sistema usa o paradigma cliente/servidor que vimos no Capítulo 1. Foi assim criado um sistema em que a informação à qual os cientistas queriam ter acesso estava distribuída por vários servidores e guardada num formato designado por HTML (*HyperText Markup Language*). Do lado do cliente era necessário dispor de um programa especial, a que actualmente designamos por *browser*, que contactava e trazia dos servidores a informação no formato HTML. Para concretizar a comunicação entre o *browser* e cada servidor foi desenvolvido um novo protocolo de comunicação, do nível aplicacional, designado por HTTP (*HyperText Transfer Protocol*) que basicamente analisa o primeiro ficheiro trazido do servidor e vai buscar os diferentes objectos necessários para representar uma página Internet.

A partir do momento em que os documentos HTML são trazidos do servidor para o cliente, este torna-se autónomo e todas as operações se tornam locais do lado do cliente. Por exemplo, operações de alteração da dimensão da janela e de impressão, entre outras, só contemplam processamento no lado do computador cliente, não sobrecarregando nem o servidor nem os circuitos de comunicação.

3.1.1.4. Os *URL*

Estamos habituados a ver indicações sobre sítios na Internet como:

http://www.dns.pt

Costuma designar-se por URL (*Uniform Resource Locator*) este conjunto de símbolos que permite identificar um recurso na Internet. A forma geral dos URL é um pouco complexa e a sua análise sai do âmbito deste manual. A sua forma mais comum, como a que apresentámos, destina-se a identificar um recurso, através da notação de domínios, e a identificar o protocolo usado para aceder a esse recurso, neste caso o protocolo http.

3.1.1.5. DNS

O DNS, sigla de *Domain Name System*, é um dos componentes da Internet crucial para o seu funcionamento. Sem a sua existência e estabilidade a FCCN como a conhecemos hoje não existiria.

Como vimos no capítulo anterior cada computador ligado à Internet tem de ter um endereço IP unívoco. Quando à Internet estavam ligados só alguns computadores era relativamente fácil memorizar os endereços IP dos computadores relevantes.

Contudo, à medida que mais computadores foram sendo ligados à Internet começou a constatar-se que seria necessário criar um sistema de identificação dos computadores mais intuitivo e fácil de memorizar.

Assim no início dos anos 80 no seio da comunidade Internet começou a ser desenvolvido um sistema que veio a ser conhecido por *Domain Name System* e que permitia a identificação dos computadores e outros recursos da Internet através de nomes simbólicos com a seguinte composição:

domínio.domínio.domínio-de-topo

ou seja, cada recurso na Internet pode ser identificado através de uma sequência de identificadores, chamados domínios, separados por um ponto. O nome de domínio mais à direita designa-se por domínio de topo. Tendo sido desenvolvido inicialmente nos Estados Unidos e face às características da língua inglesa, na construção dos nomes de domínios só eram permitidos os caracteres alfabéticos (sem distinção entre maiúsculas e minúsculas, sen-

do costume usar só letras minúsculas), os algarismos de 0 a 9 e alguns caracteres especiais.

Apresentam-se, na figura 3.2, três exemplos de identificadores de recursos na Internet.

arquivo.fccn.pt
xyz.test.global-name.info
www.alfa123.com

Figura 3.2 • Exemplos da notação de domínios

No primeiro exemplo o domínio de topo é **.pt,** no nível imediatamente inferior temos o domínio **fccn** e sob este último o **arquivo**.

A maioria dos domínios de topo da Internet correspondem aos códigos de dois caracteres dos países, como definidos pelo ISO, e cada um deles é gerido por uma organização responsável pelo registo (*registry*) desse país ou território.

Além destes domínios de países há outros de topo que não têm nenhuma associação geográfica. Desde o início da Internet foram criados domínios de topo como .com, .org, .net, .edu, .mil, .arpa, .int.

Recentemente o espaço de nomes da Internet viu serem acrescentados novos domínios de topo, que passaram a ser classificados como domínios genéricos (*gTLD – Generic Top-Level Domain*) e patrocionados (*sTLD – Sponsored Top-Level Domain*).

Como vimos, porém, cada computador é conhecido a nível do protocolo IP, através do seu endereço IP. Logo, é necessário fazer a associação entre o nome de um domínio, por exemplo www.fccn.pt, e um endereço IP específico, suponhamos 146.193.12.65. Para isto há servidores especiais na Internet, chamados como seria natural servidores DNS, que contêm tabelas que fazem estas associações.

Assim, quando um utilizador, por exemplo, através de um *browser* Internet, identifica um recurso como www.publico.pt é contactado o servidor DNS do utilizador, que faz a tradução e obtém um endereço IP como 201.34.64.12. É este o endereço do servidor associado ao nome de domínio www.publico.pt e a partir daqui é este endereço IP que é usado pelo protocolo HTTP para ir buscar ao servidor as páginas em HTML que depois representará no ecrã.

No caso de se tentar aceder a uma página Internet de outro domínio de topo, por exemplo, para ter acesso ao recurso www.bbc.co.uk de um domínio subordinado ao domínio de topo do Reino Unido (.uk) há, regra geral, que contactar vários servidores de DNS até obter o endereço IP que lhe corresponde. Estas operações são feitas de modo eficiente e o utilizador, em condições normais, não se apercebe do tempo que demora.

O sistema DNS é, portanto, concretizado a nível mundial como uma base de dados distribuída, que se mantém íntegra mediante uma série de servidores para todos os domínios de topo da Internet, devidamente coordenados. Trata-se de uma infra-estrutura de grande complexidade, crítica para o bom funcionamento da Internet mundial e que deve ter uma grande eficiência, fazendo traduções de nomes de domínios para endereços IP em fracções de segundo, de maneira que ela, para o utilizador comum, lhe pareça transparente.

Cada organização comum domínio sob um domínio de topo deve também dispor de um servidor para esse domínio. Por exemplo, a Universidade de Lisboa para o seu domínio ul.pt dispõe de um servidor DNS que resolve os endereços de toda a sua hierarquia (por exemplo, fc.ul.pt, fm,ul,pt, reitoria.ul.pt, entre outros). Muitas organizações não querem ter a complexidade técnica de gerir o servidor do seu próprio domínio, sendo, então, essa tarefa realizada pelo operador do seu acesso à Internet, o ISP.

3.1.1.6. O DNS em Portugal

Para cada domínio de topo da Internet há uma entidade que o gere, como vimos. Por razões técnicas só pode haver uma entidade gestora de todos os domínios de nível imediatamente inferior ao domínio de topo. Por outro lado, quando um domínio abaixo do de um de topo é atribuído a uma organização, esta torna-se responsável por ter um servidor para esse domínio de segundo nível, e assim sucessivamente, obrigando-se a manter a sua correcta operação técnica de modo a não perturbar o funcionamento da Internet global. As normas técnicas que devem ser seguidas na configuração e operação dos servidores de DNS são definidas pelo IETF.

Em Portugal o sistema DNS foi introduzido pela FCCN – Fundação para a Computação Científica Nacional para servir a comunidade de investigação e universitária, pioneiras na introdução da Internet em Portugal.

Numa fase inicial o número de domínios que existia era reduzido e o DNS era gerido de um modo simples e informal, baseado em regras muito simples.

Após 1995 quando a Internet comercial portuguesa começou a despontar foi necessário desenvolver estas regras e adaptá-las às necessidades nacionais.

Simultaneamente, a nível internacional, havia uma tentativa de harmonização de alguns aspectos internacionais da Internet. Foi então criada uma organização, o ICANN (*Internet Corporation for Assigned Names and Numbers*), para gerir a maioria dos aspectos de uma rede.

Neste contexto as regras aplicáveis ao registo de nomes na Internet portuguesa foram evoluindo e a última versão existe desde Fevereiro de 2001

(estas regras e toda a informação sobre o registo de domínios sob .pt pode ser obtida em www.dns.pt).

A estrutura do espaço de nomes do domínio Internet de Portugal, o .pt, está parcialmente representado na figura 3.3 e segue o modelo subjacente às regras de registo de domínios sob .pt.

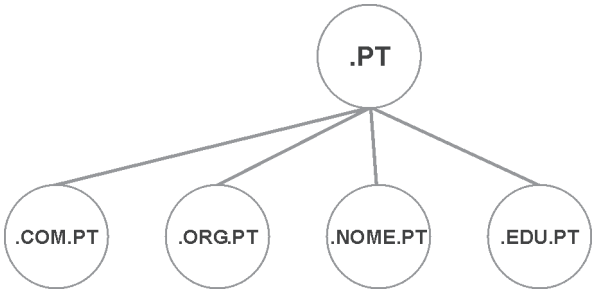

Figura 3.3 • Visão parcial da estrutura de domínios de .pt

Através da figura 3.3 podemos ver o domínio .pt, sob o qual as organizações e empresas podem registar os seus domínios. Existe ainda a possibilidade de registar domínios sob outros, chamados domínios classificadores, tais como: .com.pt, .org.pt, .nome.pt e .edu.pt, entre outros.

Esta estrutura do espaço de nomes foi evoluindo, tendo tomado a estrutura que acabamos de apresentar em 2001, com o intuito de acomodar as necessidades das várias classes de utilizadores.

Assim no nível imediatamente inferior a .pt podem ter nomes de domínios empresas e outras organizações com base no nome da empresa ou de marcas de que seja titular (por razões de espaço não é possível analisá-las com mais pormenor, estando disponíveis em www.dns.pt).

A seguir, temos o domínio classificador .nome.pt, destinado ao registo de nomes de domínios de pessoas físicas, como pedroveiga.nome.pt, o domínio classificador .org.pt, destinado ao registo de nomes de domínios de organizações não lucrativas.

O outro domínio classificador é o .com.pt. Este domínio foi criado, à semelhança de muitos países, para permitir o registo de nomes de domínios em linha. Qualquer pessoa pode registar o seu domínio sob .com.pt, por exemplo, batata.com.pt sem qualquer tipo de formalismo, pois trata-se de um processo feito exclusivamente através da Internet. O registante só tem de se assegurar que não viola um conjunto muito simples de regras, sob pena do domínio vir a ser removido *a posteriori*. Estas regras simples consideram motivo de remoção a violação de direitos de propriedade industrial de terceiros, geralmente associados a marcas notórias ou ao uso para o

nome do domínio de expressões que violem a legislação nacional (por exemplo, expressões ofensivas).

Na figura 3.4 podemos ver o modo como os registos de domínios foram evoluindo no domínio de topo de Portugal.

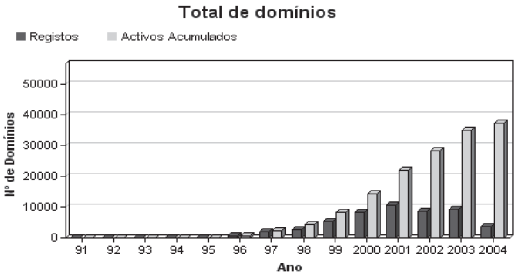

Figura 3.4 • Evolução dos domínios Internet em Portugal (dados fornecidos pela FCCN relativos a Jun/2004)

O ano com maior número de registos foi o de 2001, a partir daí tem-se mantido um volume de registo de domínios significativo, o que leva a que neste momento existam cerca de 40 000 domínios sob .pt e seus domínios classificadores.

ESTUDO DE CASO

Há cerca de dez anos a FCCN fez um conjunto de sugestões para que os nomes de domínios Internet para as Câmaras Municipais obedecessem a uma regra simples e eficaz. Em linhas simples o domínio Internet de uma Câmara Municipal deveria ser da forma: cm-autarquia.pt.

Muitas Câmaras criaram domínios desta forma, como cm-porto ou cm-palmela, tornando-se assim simples um cidadão obter o domínio do seu município.

Esta sugestão não foi universalmente adoptada, o que nem é grave pois entretanto surgiram na Internet modos alternativos de aceder aos sítios na Internet das autarquias – portais, motores de busca, por exemplo – o que nos parece fundamental é que cada autarquia reserve a sua presença na Internet portuguesa, registando o nome do seu domínio sob .pt.

O tecido económico ainda não se apercebeu da importância de registar sob .pt e respectivos domínios classificadores, em especial o .com.pt, o nome da empresa e dos produtos e marcas que detêm. Em países onde a economia digital está mais avançada os empresários têm uma enorme preocupação em preservar os seus direitos também na Internet, fazendo o registo de nomes de domínios para a empresa e para os seus produtos e marcas, mesmo que não

venham a usá-los de imediato. Conseguem, assim, proteger um património importante da sua empresa.

3.1.1.7. O Domínio .eu

Na sequência de esforços da União Europeia no sentido de obter uma identidade própria na Internet foi criado o seguinte registo do domínio de topo: **.eu**.

Entretanto, por regulamento do Parlamento Europeu e do Conselho do ano de 2000 foram definidas regras para a gestão e operação do domínio de topo da Internet, .eu.

Na sequência de um processo demasiado moroso, burocrático e complexo acabou por ser escolhida uma organização responsável pelo registo do domínio .eu e que conta com o auxílio de entidades registadoras, junto das quais os utilizadores finais farão os pedidos e registo dos seus domínios sob .eu. Prevê-se que este novo domínio de topo entre em funcionamento no final de 2004 ou início de 2005.

3.1.1.8. SNMP

Para que uma rede funcione bem é preciso que seja bem gerida. Gerir uma rede é observar o seu funcionamento e tomar decisões de manter ou alterar o seu estado de modo a que ela forneça aos seus utilizadores os serviços que eles necessitam.

Assim no seio do IETF foi definido um protocolo de gestão de recursos da Internet, designado por SNMP (*Simple Network Management Protocol*). O protocolo tem subjacente uma arquitectura de gestão, onde existem entidades, umas que fazem perguntas a um sistema central, e outras gestoras que fornecem informação às entidades geridas a respeito do seu modo e estado de funcionamento. O termo SNMP refere-se quer à arquitectura de gestão, quer ao protocolo usado para troca de informação entre o sistema gestor e os sistemas geridos.

Após o trabalho de normalização no seio do IETF começaram a surgir em quase todos os equipamentos que se podem ligar à Internet capacidades de gestão, isto é, os sistemas passaram a implementar as normas SNMP o que é muito vantajoso, pois podem ser geridos remotamente.

Além disso começaram a ser comercializados sistemas de gestão que seguem as normas do IETF e que, devidamente configurados, permitem a partir

de um ponto central conhecer as principais características de funcionamento de uma rede, dos seus equipamentos nucleares e dos sistemas a ela ligados.

Quando implementada a arquitectura de gestão da Internet é possível intervir e controlar a rede para que esta atinja os objectivos de operação definidos.

3.1.1.9. VoIP

VoIP, acrónimo para *Voice over IP*, designa um conjunto de tecnologias que permitem fazer chamadas de voz sobre a Internet. Esta ideia surgiu graças à crescente capacidade desta rede e à conveniência de reduzir custos de circuitos e de gestão de redes complexas.

Há diversos modos de implementar uma rede com facilidades de VoIP e apresentamos na figura 3.5 uma destas situações. Os telefones convencionais da organização podem ser ligados ao *router* da organização através de uma placa controladora específica. As chamadas de voz são passadas à forma digital, sob pacotes IP, os quais são enviados pela Internet até à rede de destino, que terá obrigatoriamente de suportar VoIP numa configuração semelhante.

Existe ainda uma outra alternativa, menos frequente por enquanto, que consiste em ter telefones IP, os quais são transformados, podendo ser directamente ligados à rede local da organização.

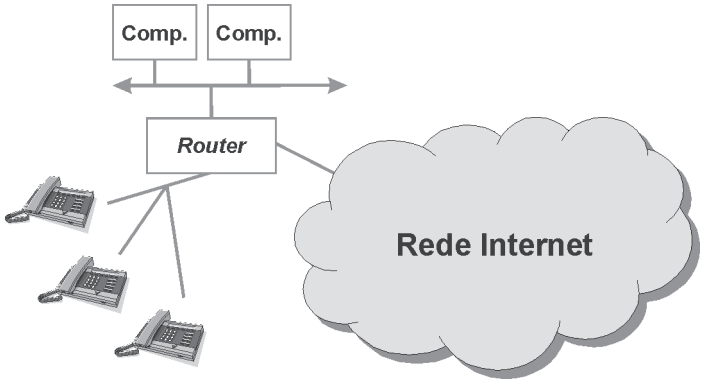

Figura 3.5 • Exemplo de integração de VoIP numa rede de uma organização

Há diversas vantagens e inconvenientes em usar VoIP, cuja discussão ultrapassa o objectivo deste manual, mas julgamos imprescindível juntar alguns aspectos relevantes:

- a partilha dos mesmos meios de comunicações para transmissão de voz e de dados pode permitir uma economia de custos, dependendo dos

volumes de voz e dos destinos mais usados; no caso de uma organização detentora de uma rede de dados, distribuída pelos diversos locais onde está implementada e com um elevado volume de chamadas internas, a economia de custos poderá atingir valores consideráveis;

- a introdução de VoIP exige que se invista em equipamento e que haja formação de pessoal técnico, como tal, os benefícios só serão visíveis a longo prazo;
- atendendo a que a transmissão de voz tem diversos requisitos relativamente à qualidade de serviço da rede, os perfis de tráfego de dados e de voz devem ser estudados, a fim de se avaliar se a transmissão de dados não prejudica a parte de voz

3.1.1.10. Videoconferência

Outra aplicação que se espera que venha a ter um significativo crescimento nos próximos anos é a videoconferência. Este processo consiste na colocação de dois ou mais utilizadores que comunicam por meio de voz e dados. No caso mais simples, quando existem dois utilizadores envolvidos na videoconferência, cada um deles deve ter um equipamento compatível com a norma relevante: a norma H.323. Esta norma define o modo como um sistema pode, simultaneamente, receber e enviar imagem e som para um outro sistema.

Um sistema de videoconferência é composto, no mínimo, pelos seguintes componentes:

- câmara de vídeo, para captar a imagem local;
- microfone, para capturar o som local;
- ecrã de visualização da imagem remota;
- colunas de som para reprodução do som remoto;
- sistema de codificação do vídeo e do som (*codec – code /decoder*) para transformar o som e a imagem de modo a poderem ser transmitidos sob a forma de pacotes IP.

Existem no mercado muitos sistemas para fazer videoconferência com custos que dependem do número de opções e da qualidade dos sistemas de captura e reprodução do vídeo e do som.

Também se pode fazer videoconferência a partir de um simples computador com *software* de *codec*. Trata-se de uma solução bastante limitada, adequada apenas como solução de recurso para duas pessoas comunicarem.

A transmissão de vídeo e de som, para ter minimamente qualidade, exige largura de banda apreciável (aconselhamos um mínimo de 512 kbps). No entanto, continua a ser uma aplicação promissora, pois permite realizar sessões de trabalho entre pessoas localizadas em sítios distintos de modo eficiente e eficaz.

3.1.1.11. A convergência tecnológica

A evolução dos computadores e das redes, que analisámos neste capítulo e nos anteriores, veio introduzir várias novidades, a saber:

- podemos representar em formato digital dados (o uso inicial dos computadores), voz, imagem e vídeo;
- podemos armazenar todos estes tipos de informação de um modo compacto e económico;
- sobre a mesma rede e partilhando os mesmos circuitos de comunicações podemos transmitir dados, voz, imagem e vídeo.

Estes factos são a base da convergência tecnológica, um termo que designa o facto de no mesmo formato e usando os mesmos meios de comunicação ser possível capturar, processar e transmitir os diversos tipos de informação relevantes: texto, dados, voz, imagem e vídeo.

Deste modo as empresas, as organizações e as pessoas têm à sua disposição, de um modo simplificado e a custos moderados, acesso a um universo de opções que lhes permitem aceder à sociedade de informação.

CAPÍTULO

4

INTRODUÇÃO ÀS APLICAÇÕES E AOS SISTEMAS DE INFORMAÇÃO

OBJECTIVOS

- É feita uma abordagem sistémica dos actuais sistemas informáticos.
- São descritas abordagens e ferramentas de apoio para o desenvolvimento de aplicações e sistemas informáticos.
- São abordados diversos aspectos legais e éticos no uso de sistemas informáticos.

PONTO DA SITUAÇÃO

A complexidade dos sistemas de informação e das redes actuais tem levado à necessidade de criar modos expeditos e eficientes para os desenvolver. Por outro lado, a maturidade da indústria de *software* conduziu a que hoje em dia se consigam desenvolver de modo rápido e robusto aplicações de grande complexidade funcional.

O desenvolvimento de sistemas de informação obedece a uma diversidade de critérios, cuja análise é complexa e em que as decisões de concepção têm impacto. Para aumentar a eficiência do desenvolvimento e minimizar o trabalho associado de gestão e adaptação dos sistemas ao longo do seu ciclo de vida existem várias técnicas que são usadas: modularidade e abstracção. Estas técnicas são possíveis, graças ao tipo de tecnologias informáticas actualmente disponíveis em termos de linguagens, ferramentas computacionais e arquitecturas de concepção de sistemas informáticos.

4.1. INTRODUÇÃO ÀS APLICAÇÕES E AOS SISTEMAS DE INFORMAÇÃO

Desde que na década de 50 foi inventada a primeira linguagem de programação, o FORTRAN, foram dados passos notáveis nas técnicas e tecnologias de desenvolvimento de sistemas informáticos e respectivas aplicações.

Durante vários anos uma das principais preocupações dos investigadores e da indústria de *software* centrava-se no desenvolvimento de linguagens de programação com diferentes características:

- linguagens de programação especializadas em certos domínios aplicacionais, como por exemplo o COBOL, muito adequado às chamadas aplicações comerciais;
- linguagens de programação especialmente eficientes na execução para programar aplicações muito exigentes em termos de tempos de resposta, como a linguagem C;
- linguagens de programação universais, adequadas a todo o tipo de aplicações e que, segundo se esperava, poderiam simplificar o esforço de formação dos informáticos nas grandes organizações, como a linguagem ADA.

Esta tendência de desenvolvimento de linguagens de programação cada vez mais avançadas continuará a verificar-se, mas cremos que não será o centro da actividade de engenharia de *software*.

Nos anos recentes há uma preocupação crescente com outros aspectos. Sendo difícil explorar todas as tendências actuais da engenharia de *software*, podemos salientar dois pilares de acção, que, na nossa opinião, são fundamentais:

- a grande aposta na modularidade das aplicações, investindo-se muitos recursos no desenvolvimento de linguagens e sistemas que permitam a construção de aplicações e sistemas muito complexos pela «colagem» de módulos funcionais mais simples;
- o desenvolvimento de metodologias de desenvolvimento expedito que são necessárias para uma compatibilização com as necessidades de criação de novas aplicações com ciclos de vida muito curtos e com elevados níveis de robustez das soluções.

4.1.1. SISTEMAS DISTRIBUÍDOS

A informática inicial era centralizada. As plataformas informáticas mais avançadas eram desenvolvidas em torno de computadores centrais de grande porte ao qual os utilizadores tinham acesso através de terminais orientados ao carácter.

Com os desenvolvimentos verificados a partir de 1980 a informática tem vindo a evoluir para soluções distribuídas que podemos caracterizar de um modo simplificado, segundo os seguintes parâmetros:

- Os utilizadores têm normalmente um computador pessoal, com alta velocidade de processamento local e com capacidades gráficas e de armazenamento local avançadas;
- Funções específicas, que exigem recursos que se destinam a ser partilhados, são localizadas em sistemas informáticos mais ou menos dedicados, os servidores; aparecem assim servidores de armazenamento, servidores de impressão, servidores de base de dados, entre outros;
- A grande largura de banda disponível, especialmente em ambientes de rede local, torna quase irrelevante o modo como as aplicações complexas são distribuídas em termos de servidores e clientes, trazendo uma modularidade que permite uma evolução incremental e gradual das soluções informáticas e dos investimentos;
- A invenção da World Wide Web trouxe um modelo novo de apresentação de informação ao utilizador final, porque possui características que facilitam a interface com o utilizador final, o que leva à reengenharia das inter-

faces aplicacionais para que estas tenham uma coerência que seja transversal a todas as aplicações, o que facilita a aprendizagem dos utilizadores.

Deste modo, as soluções disponíveis às organizações são muito menos onerosas, em termos de *hardware*, do que se verificava há alguns anos. Por outro lado, tem vindo a aumentar, de modo significativo, os custos dos componentes de *software*, aplicações comuns e os esforços associados à sua adaptação aos requisitos de cada organização.

Os actuais sistemas são aqueles em que a capacidade de processamento e armazenamento já não está centralizada, mas sim distribuída. Com a crescente capacidade de velocidade das redes, mesmo em situações de redes alargadas (WAN), a deslocalização física dos servidores também se está a tornar uma realidade, tendo feito aparecer soluções em que uma organização pode ter os seus servidores principais alojados nas instalações de uma empresa especializada.

4.1.2. APLICAÇÕES

A indústria de *software* tem vindo a produzir sistemas cada vez mais complexos, de uso genérico, e onde a parametrização para servir as necessidades específicas de um certo cliente é o principal esforço a fazer.

Em muitas situações já não é necessário conceber uma aplicação de raiz, escrevendo e testando milhares de linhas de código. Para a maioria das situações há à disposição no mercado um leque alargado de aplicações genéricas, que só precisam de ser adaptadas ao contexto e às características e aos interesses da instituição.

Os sistemas de gestão de base de dados (SGBD) são um dos componentes dos actuais sistemas informáticos com maior maturidade, que assentam sobre o sistema operativo de modo a criarem uma plataforma flexível e sofisticada para concretizar um repositório de dados para cada organização.

Para outras áreas aplicacionais existem também múltiplas aplicações que, regra geral, cumprem a maioria dos requisitos das organizações. Assim basta adquirir a licença de uso da aplicação e proceder à sua parametrização para o ambiente específico onde vai estar inserida.

Podemos concluir que o desenvolvimento de aplicações de raiz não é necessário em muitas situações das organizações, a não ser que existam requisitos muito específicos a cumprir.

Mas retomando de novo o tema do desenvolvimento aplicacional e para os casos em que não existam aplicações que possam ser parametrizadas para

servir os interesses da instituição, neste caso há que recorrer ao desenvolvimento de aplicações à medida.

Nos últimos anos tem-se verificado alterações importantes no modo como podem ser desenvolvidas aplicações de modo expedito. Existem hoje ambientes de programação onde, a partir de especificações funcionais, é possível fazer a geração de aplicações de elevada complexidade e que geram códigos de alta qualidade e eficiência, aliando a isso a robustez e qualidade do código produzido.

ESTUDO DE CASO

Desenvolver uma aplicação à medida ou parametrizar uma aplicação *standard* do mercado. O que é mais acertado?

As aplicações necessárias para uma dada autarquia correspondem à concretização de processos administrativos ou burocráticos normais, com eventuais adaptações ao contexto de uso. Assim, e na maioria das situações, não se justifica o desenvolvimento de aplicações de raiz, mas antes a adaptação ou parametrização de aplicações existentes no mercado.

O desenvolvimento de aplicações de raiz é, na maioria das vezes, caro e traz muitos problemas de manutenção. Cria-se uma dependência quase total da empresa que faz o desenvolvimento e da sua capacidade em manter o suporte à aplicação ao longo da sua vida.

A parametrização de aplicações *standards* do mercado é, regra geral, a solução mais adequada, permitindo beneficiar da capacidade de manutenção da aplicação pela empresa que desenvolve esta aplicação para muitas entidades. Nestes casos também há várias empresas que podem prestar serviços de parametrização ou adaptação das aplicações, dando à autarquia uma maior margem negocial na obtenção das condições que mais se adaptam ao seu caso.

4.1.3. A PLATAFORMA COMPUTACIONAL

O diagrama esquemático, que apresentámos na figura 4.1 das camadas funcionais de um sistema operativo, pode ser visto de outro modo quando estamos mais preocupados com a colocação de aplicações que irão num computador. Nesta figura apresentamos uma outra visão possível de como os vários componentes de um sistema computacional interagem. Sobre o *hardware* é colocado o sistema operativo que for escolhido (por exemplo, Linux ou Windows) e podem ser adicionados outros subsistemas de *software* como um sistema de gestão de bases de dados, ou várias aplicações *standard*, que serão depois parametrizadas à medida, de modo a satisfazerem as necessidades da instituição.

Figura 4.1 • Arquitectura funcional de um sistema computacional

Dependendo de uma diversidade de opções tecnológicas, aspectos organizacionais da instituição e perspectivas de evolução da dimensão do sistema e das aplicações, esta arquitectura básica pode ser construída por meio de uma solução centralizada ou de uma solução distribuída. A selecção da concretização é normalmente feita com base numa série de factores bastante complexos, sendo uma actividade de engenharia informática que exige uma diversidade de competências alargada. Estas decisões são normalmente tomadas com base numa equipa multidisciplinar que envolve os «clientes» internos à instituição, os seus técnicos informáticos e os consultores das empresas fornecedores das soluções aplicacionais. Começa por um trabalho de análise que irá sendo refinado até se chegar a uma solução concreta.

4.1.3.1. O sistema operativo

Como já nos apercebemos, o sistema operativo tem um papel importante na concretização da plataforma computacional. Todos os sistemas operativos existentes actualmente dispõem de elevada qualidade e têm funcionalidades que os adequam a, virtualmente, qualquer tipo de ambiente aplicacional. Muitas vezes a decisão de se usar um sistema operativo A em detrimento de um outro B não se baseia em critérios estritamente técnicos.

Como plataforma aplicacional, actualmente, são muito populares o Linux™, o Solaris,™ o Windows™, entre outros. São sistemas bastante sofisticados e capazes de suportar qualquer aplicação. No que se refere às camadas funcionais acima do sistema operativo, como está representado na figura 4.1, os sistemas operativos variam de caso para caso. Assim a decisão sobre qual o sistema operativo a seleccionar depende do seu suporte às aplicações que pretendemos adquirir para servir os fins da instituição. Também se deve ter em consideração a capacidade do pessoal técnico da organização, qua(l)(is) o(s) sistema(s) operativo(s) que conhecem, bem como os custos de aquisição das licenças do sistema operativo, custos de manutenção e suporte.

ESTUDO DE CASO

Devemos optar por Windows ou LINUX? Esta é uma pergunta que, com alguma frequência, se coloca aos responsáveis de uma organização e cuja resposta não é trivial.

Em termos de funcionalidades oferecidas por cada uma destas plataformas computacionais, podemos dizer que são mais ou menos equivalentes para a maioria das situações, isto é, correm aplicações análogas, quer para uma, quer para outra existem sistemas de automatização de escritório, sistemas de gestão de bases de dados, aplicações gráficas, entre muitas outras, de excelente qualidade e robustez.

A nível de interface com o utilizador as duas plataformas podem ser consideradas idênticas, oferecendo funcionalidades ao utilizador equivalentes.

Então que tipo de aspectos se devem ter em conta para escolher entre um sistema operativo de base e outro?

Em nossa opinião devem ser tomados em consideração diversos aspectos, entre os quais salientamos: i) custo de aquisição das licenças para um sistema e para outro; ii) custo de manutenção das licenças nos anos seguintes ao da aquisição; iii) existência de pessoal técnico habilitado a dar apoio à plataforma escolhida quer dentro da autarquia, quer nas empresas que lhe prestam serviços; iv) custos de formação dos funcionários na plataforma e aplicações que vão estar disponíveis; v) complexidade das aplicações em termos de exigências de capacidade do *hardware* de suporte, na medida em que uma dada plataforma para uma dada aplicação pode exigir *hardware* potente, logo, dispendioso.

Em resumo, há uma diversidade de aspectos que, no seu conjunto, devem ser usados para tomar a decisão, olhando-se para todo o ciclo de vida dos sistemas e não só para os custos iniciais de aquisição.

4.1.4. ASPECTOS LEGAIS

Quem gere o sistema de informação de uma organização deve ter em conta uma série de aspectos e obrigações legais no que diz a respeito às opções e decisões a tomar.

A legislação portuguesa tem-se preocupado com diversos aspectos ligados à utilização da informática e da Internet. A legislação cobre diversos aspectos dos quais realçamos os que julgamos de maior importância para o leitor:

- Cibercrime;
- Direitos do Consumidor;
- Contratação Informática;
- Protecção de Direitos de Autor;
- Protecção de Dados Pessoais e Privacidade.

Os aspectos legais da utilização de sistemas informáticos e os que se referem à Internet são um tema extenso e, infelizmente, não muito divulgado em Portugal.

Não sendo possível no contexto deste manual abordar em profundidade todos estes aspectos, realçamos todavia alguns dos que consideramos particularmente importantes.

4.1.4.1. Cibercrime

Nos últimos anos tem crescido o número de crimes em que a informática é um instrumento fundamental. Um dos exemplos de crimes cometidos com recurso ao computador é a intercepção de códigos de acesso a contas, ou números de cartões de crédito, com uso posterior destes dados para cometer crimes de furto ou uso abusivo.

No Capítulo 5 analisaremos algumas técnicas e tecnologias para evitar a intercepção de códigos.

A lei de criminalidade informática prevê punições para estes actos mas o número de casos até agora investigados e julgados é reduzido, pela complexidade da sua detecção e investigação mas, também, porque os casos que têm sido detectados e identificados não têm sido alvo de publicidade por razões de segurança e confiança dos utilizadores.

4.1.4.2. *Software* pirata

Os programas de computador são alvo de protecção jurídica específica, pelo Decreto-Lei n.º 252/94, sendo ilegal instalar *software* não licenciado (*software* pirata), fazer cópias ilegais ou vender *software* licenciado pertencente a terceiros.

ESTUDO DE CASO

O *software* de base, isto é, o sistema operativo e as bases de dados, bem como os aplicativos são normalmente fornecidos com base numa licença de utilização que tem de ser renovada periodicamente.

Além de ser uma exigência legal para se poderem usar os sistemas operativos e as aplicações, o pagamento das licenças e das renovações garante que se pode ter acesso a versões mais recentes dos produtos.

Em muitas organizações os funcionários, por desconhecimento, têm, muitas vezes, tendência para instalar produtos de *software* nos computadores sem dispor das licenças adequadas. Estas situações, além de representarem problemas de segurança, podem trazer responsabilidade criminal aos dirigentes das organizações por violação da lei de criminalidade informática.

É da responsabilidade do dirigente máximo de uma organização assegurar-se de que todo o *software* que está instalado tem licenças e que estas estão actualizadas.

4.1.4.3. Registo de bases de dados

A legislação portuguesa obriga ao registo das bases de dados que contenham dados pessoais. Este registo deve ser feito junto da Comissão Nacional de Protecção de Dados (www.cnpd.pt).

Uma entidade que detenha uma base de dados deste tipo deve notificar a Comissão Nacional de Protecção de Dados da sua existência, dando pormenores sobre o tipo de informação que contém e o destino a dar ao seu uso.

ESTUDO DE CASO

Uma parte significativa das bases de dados, existentes numa autarquia, possui informações tanto de carácter pessoal como sensíveis.

É da responsabilidade dos dirigentes autárquicos o registo das bases de dados sob sua tutela, sendo este um processo relativamente simples e eficiente.

Toda a informação sobre os passos a seguir está disponível no sítio da Internet da Comissão Nacional de Protecção da Dados, em www.cnpd.pt.

4.1.4.4. Outros aspectos

Além da legislação nacional específica, a nível da União Europeia têm sido produzidas diversas Directivas que têm sido transpostas para a legislação nacional. Limitamo-nos, aqui, a referenciar alguma legislação nacional e comunitária que consideramos importante:

- Lei n.º 109/91, Lei da Criminalidade Informática;
- Decreto-Lei n.º 252/94, relativo à protecção jurídica dos programas de computador;
- Lei n.º 67/98, Lei de Protecção de Dados Pessoais;
- Decreto-Lei n.º 122/2000, relativo à protecção jurídica das bases de dados e que transpõe uma Directiva comunitária de 1996;
- Decreto-Lei n.º 290-D/99, relativo à assinatura digital;
- Decreto-Lei n.º 375/99, relativo à factura electrónica;
- Directiva 97/7/CE, relativa à protecção de consumidores em matérias de contratos a distância.

CAPÍTULO

5

SEGURANÇA INFORMÁTICA: TECNOLOGIAS E SUA APLICAÇÃO

OBJECTIVOS

- São apresentados os fundamentos das tecnologias de segurança e como estas podem ser usadas.
- Analisam-se as linhas de orientação organizacionais de modo a garantir a segurança nos sistemas de informação e nas redes das nossas organizações.

P O N T O D A S I T U A Ç Ã O

A crescente importância que os sistemas de informação e as redes têm para a nossa sociedade e para o nosso bem-estar obriga, naturalmente, a que tenhamos de ter confiança no seu uso.

Existem actualmente muitas tecnologias que, se forem bem aplicadas, ajudam a garantir a segurança e a confiança de que podemos usar quer os sistemas de informação, quer as redes.

Porém, na área da segurança informática, como aliás em todas as áreas onde a segurança é um factor relevante, a tecnologia só resolve os nossos problemas se estiver integrada numa política de segurança bem definida, concebida de modo rigoroso, bem implementada e cuja aplicação deve ser auditada de modo independente.

5.1. SEGURANÇA INFORMÁTICA: TECNOLOGIAS E SUA APLICAÇÃO

A crescente importância que os sistemas de informação e as redes têm para o nosso dia-a-dia, para o nosso bem-estar e para o nosso desenvolvimento económico traz, naturalmente, um conjunto de preocupações relativas à estabilidade e à segurança desta infra-estrutura fundamental. O nível de uso da Internet pelos cidadãos, empresários e dirigentes das organizações só crescerá se a rede for segura e tiver elevados graus de qualidade dos serviços.

O desenvolvimento científico e tecnológico na área da segurança tem sido grande, permitindo garantir condições e níveis de segurança elevados, mas só se as tecnologias forem devidamente aplicadas é que elas podem desempenhar bem o seu papel. Por outro lado, para a nossa sociedade quanto mais crucial é o uso da Internet, maior é o risco de ser alvo de tentativas de perturbação do seu funcionamento por quem o quer prejudicar, por exemplo, tentando causar falhas na rede, ou destruindo informação ou ainda usando as redes como veículo de crimes.

5.1.1. TECNOLOGIAS CRIPTOGRÁFICAS

A base da maioria das tecnologias de segurança informática são as tecnologias criptográficas. Estas técnicas consistem, em termos gerais, na aplica-

ção de uma função matemática para transformar uma mensagem M numa outra M' usando um código K designado por chave criptográfica:

$$f(M, K) = M'$$

Se a chave K for bem escolhida, quem não a conhecer não consegue obter a mensagem M mesmo que tenha acesso a M'. Assim, por exemplo, se dois indivíduos quiserem trocar informação confidencial basta que ambos partilhem uma dada chave K e, entre si, troquem as mensagens cifrando-as com a função f(). A esta técnica dá-se o nome de criptografia simétrica, pois os dois interlocutores usam a mesma chave para comunicarem de modo seguro.

Na figura 5.1 representamos, de modo esquemático, o uso da criptografia para troca de mensagens seguras entre dois indivíduos A e B. Se o utilizador A pretende enviar uma mensagem para B, através de um canal, e garantir a sua confidencialidade, mesmo que seja alvo de intercepção durante a transferência de A para B, então deve cifrar a mensagem antes de a submeter ao canal de transmissão. Deveria ter, antecipadamente, comunicado a chave criptográfica ao utilizador B de modo seguro. Só este, porque dispõe da chave, consegue decifrar a mensagem. Se esta mensagem for interceptada não é possível decifrá-la, pois não se dispõe da chave necessária para o efeito.

Figura 5.1 • Troca de mensagens cifradas entre dois interlocutores

A criptografia assimétrica é uma variante das tecnologias criptográficas de grande utilidade. Tem algumas semelhanças com a tecnologia simétrica descrita, mas agora existem duas chaves para cada um dos intervenientes numa comunicação segura. Uma das chaves designa-se por chave privada e a outra por chave pública. As mensagens que são cifradas por uma são decifradas pela outra, e vice-versa (as duas chaves estão intimamente ligadas uma à outra). Nesta situação quando queremos enviar uma mensagem confidencial, cujo conteúdo só queremos que seja acessível a um destinatário, temos de cifrar a mensagem com a chave pública do destinatário. Só este a poderá ler usando a sua chave privada para ter acesso à mensagem. De modo

inverso, se nos quiserem enviar uma mensagem privada, basta que seja cifrada com a nossa chave pública e, assim poderemos decifrá-la com a nossa chave privada que só nós conhecemos.

Assim o processo de criptografia baseia-se nos seguintes elementos fundamentais:

- algoritmos criptográficos;
- chaves criptográficas;
- modo seguro de guardar as chaves criptográficas pelos emissores;
- modo seguro de entregar as chaves criptográficas aos destinatários.

Actualmente existem diversas tecnologias para garantir os aspectos acabados de referir, que se baseiam nas tecnologias criptográficas simétricas e/ /ou assimétricas, associadas a procedimentos rigorosos e seguros de concretização das aplicações e políticas de segurança.

5.1.2. FILTRAGEM DE TRÁFEGO

Uma rede informática se estiver isolada não é susceptível a intrusões. Porém, não se trata de uma situação normal, pois, na maioria dos casos, as organizações estão interessadas em ter a sua rede, ou parte dela, ligada a outras redes, e à Internet em particular.

Em quase todas as situações em que uma organização liga a sua rede à Internet deve fazer-se filtragem de tráfego nos dois sentidos, de modo a garantir a segurança. Da Internet para a rede da organização de modo a garantir que o tráfego que entra está devidamente autorizado e corresponde às políticas de segurança da organização. É uma situação equivalente ao controlo de acesso nas entradas de um edifício, só entra quem tem autorização. No sentido contrário, também é necessário controlar o tráfego que sai, designadamente para garantir que só flui da rede interna para o exterior tráfego devidamente autorizado de modo a evitar uma utilização que ultrapasse os objectivos da organização (por exemplo, evitando um gasto desnecessário de recursos) ou impedindo a transferência não autorizada de informação para fora da organização (por exemplo, o envio pela rede de informação confidencial).

Os equipamentos que permitem efectuar filtragem no tráfego entre a rede de uma organização e a Internet recebem a designação de *firewalls*. São, basicamente, sistemas que analisam cada datagrama dos protocolos da Inter-

net (de modo simplista, os datagramas IP e TCP) e deixam-nos passar ou não consoante as políticas de filtragem de tráfego para que foram preparados.

Protegendo uma rede com um *firewall*, como está representado na figura 5.2, é possível um controlo bastante rigoroso dos fluxos de informação entre a rede da organização e a Internet. Por exemplo, podem ser filtrados datagramas de potenciais utilizadores da Internet que queiram violar a rede interna da organização.

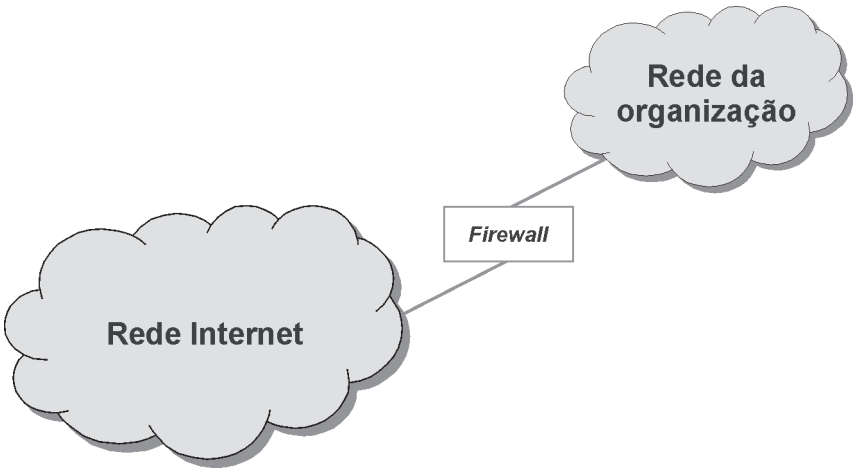

Figura 5.2 • Inclusão de um *firewall* para protecção de uma rede

A filtragem de tráfego é uma das primeiras técnicas que deve ser usada por uma organização que se liga à Internet e que deve estar associada a mecanismos adicionais de segurança, cuja complexidade e dimensão depende quer dos recursos a proteger, quer dos recursos que se querem investir na protecção. Este processo deve ser feito após uma análise de risco sobre quais os recursos a proteger e o seu valor para a organização.

5.1.3. VÍRUS E CAVALOS DE TRÓIA

Outros desafios de segurança para os sistemas de informação são os vírus e os cavalos de Tróia. Estes são programas informáticos que podem ser introduzidos num computador por vários meios e que têm como objectivo prejudicar o bom funcionamento dos sistemas ao destruir informação, degradando o desempenho do sistema ou capturando informação que depois é enviada para o exterior.

Um vírus é um programa que uma vez instalado num sistema de informação efectua um conjunto de operações que podem ir desde a destruição de informação, passando pela perturbação do bom funcionamento do sistema ou simplesmente a realização de operações mais ou menos inofensivas. Durante este processo o programa procura replicar-se noutros sistemas da rede em que o sistema inicialmente atacado está integrado. Daí a designação de vírus informático por analogia aos vírus que afectam a humanidade. Actualmente o modo mais usual de introdução dos vírus numa organização efectua-se através das mensagens de correio electrónico ou de *software* que é instalado sem uma origem devidamente certificada.

Um dos modos de proteger um computador ou um sistema de informação dos vírus é instalar e manter actualizado *software* antivírus específico. Além disso convém ter cuidado no tratamento de mensagens de correio electrónico que não são conhecidas, nunca procedendo à sua abertura e apagando-as de imediato. O *software* antivírus deve ser instalado quer em cada computador, quer nos sistemas servidores centrais da organização e deve ser aplicado segundo as políticas de segurança definidas. Neste caso todo o *software* que flui do exterior para a organização é previamente filtrado de vírus antes de ser armazenado no servidor de correio. Mensagens «infectadas» com vírus podem ser destruídas logo à entrada e, assim, nunca chegam a afectar a rede da organização. Contudo, para isto ser eficaz é preciso ter o cuidado constante de manter actualizadas as tabelas dos vírus detectados, já que há uma constante actividade de produção e propagação de vírus.

Os cavalos de Tróia são programas cuja introdução nos computadores é feita em moldes semelhantes aos dos vírus, se bem que existam muitas variantes cuja descrição sai do âmbito deste manual. Ao contrário dos vírus informáticos a sua presença pretende passar despercebida, tendo, na maioria das vezes, como objectivo a captura de informação sensível dentro do computador e proceder ao seu envio para o exterior de um modo não perceptível. Trata-se de uma situação bastante grave, pois pode, por exemplo, estar a ser capturada informação confidencial, como códigos de acesso a contas bancárias, que posteriormente são enviadas para o exterior para serem usadas em diversos tipos de crimes informáticos.

Os cavalos de Tróia podem propagar-se por métodos semelhantes aos dos vírus mas há outras variantes que é preciso ter em atenção. Um modo infelizmente frequente de entrada de cavalos de Tróia nos computadores é quando o utilizador é convidado a visitar um sítio na Internet e copiar para o seu computador um programa que efectua alguma actividade que julgamos útil, como carregar uma música, um utilitário que dá informações sobre o tempo ou que nos mostra uma imagem de um lugar aprazível. Alguns destes programas não são mais do que um artifício para instalação do cavalo de Tróia

que depois se instala no nosso computador com os resultados atrás descritos e que podem ser mais ou menos graves.

ESTUDO DE CASO

A segurança informática é uma das áreas onde há, muitas vezes, tendência para ser deixada em último lugar nas opções dos investimentos informáticos, porque implementar mecanismos de segurança custa dinheiro e os orçamentos nem sempre são suficientes, ou então, por vezes não há qualquer preocupação com a segurança. Por outro lado os técnicos, por falta de formação, não alertam os responsáveis para a necessidade de proteger os seus sistemas informáticos.

No caso particular das autarquias, onde a informação pública deve ser protegida pelos responsáveis aos vários níveis, deve haver a preocupação de considerar a segurança como algo a introduzir, logo desde o início, nos sistemas informáticos.

Relativamente aos vírus e cavalos de Tróia é necessário instalar *software* de protecção, instalando as licenças dos produtos de protecção nos postos cliente e nos servidores. Posteriormente, é fundamental manter actualizadas as licenças dos produtos para serem instaladas todas as novas versões destes sistemas.

A ignorância destas situações traz, infelizmente e com elevada frequência, prejuízos muito maiores do que representaria o investimento inicial. Com efeito, e como exemplo, um ataque de vírus pode tornar os computadores e os servidores inoperacionais, o que pode conduzir à perda ou deterioração da informação. Os custos de repor o estado normal dos computadores e recuperar os dados a partir de cópias de segurança, quando isso é possível, são normalmente muito mais elevados do que custaria o investimento inicial em bons sistemas de segurança e protecção informática.

A formação dos utilizadores, em particular dos funcionários da Administração Pública, é uma responsabilidade que deve ser reconhecida logo desde o início da informatização autárquica e que pode contribuir para uma concretização eficaz de políticas de segurança. Há um conjunto de regras elementares de segurança informática, que podem ser ensinadas de modo rápido e eficiente, e que são um contributo decisivo para redes mais seguras e, logo, sem as elevadas perdas que são causadas pelas falhas de segurança informática.

5.1.3.1. Servidor *Proxy*

Chamam-se *proxies*, procuradores ou agentes intermediários, os sistemas que concentram e processam todos os pedidos relativos a um certo protocolo entre uma rede e o exterior. A sua aplicação pode estar inserida numa política de segurança de uma organização e visa fazer passar por um único sistema todo o tráfego de um certo tipo.

Na figura 5.3 mostramos esquematicamente como um *proxy* pode ser integrado numa rede de uma organização. O *proxy* pode ser inserido na

rede da organização como qualquer outro computador. Vamos exemplificar o seu funcionamento numa situação muito comum: um *proxy* para o protocolo **http**.

O computador que aloja o servidor de *proxy* é dotado de um *software* específico, o qual recebe pedidos http dos outros computadores da rede interna, reenviando-os posteriormente para o exterior. Quando a resposta ao pedido de http é recebida, esta recepção também é feita pelo *proxy*, que depois encaminha o resultado para o computador que originou o pedido inicial.

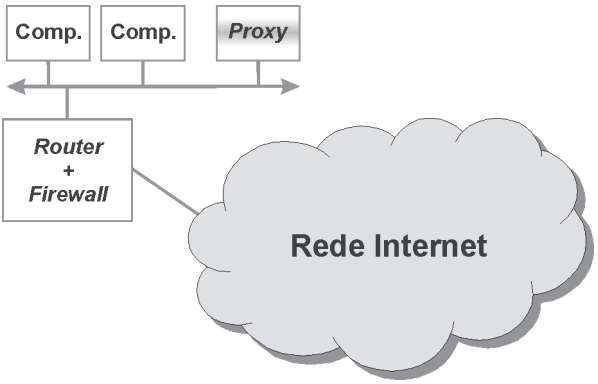

Figura 5.3 • Exemplo do uso de um servidor *proxy*

Ou seja, todo o tráfego do protocolo http é feito exclusivamente com recurso ao servidor de *proxy*. Neste caso o *firewall* é programado para filtrar todo o tráfego http de todos os computadores, internos e externos, excepto o que se destina ao servidor *proxy*. Consegue-se, assim, evitar ataques à segurança dos computadores da rede interna, devendo concentrar-se todo o investimento em garantir a segurança do servidor *proxy*. Os computadores da rede têm de ser parametrizados para usar o servidor *proxy*; se tal não for feito pura e simplesmente não conseguem aceder à WWW pois o *firewall* impede todos os acessos.

A existência deste tipo de servidor tem outras vantagens indirectas:

- pode-se fazer contabilização centralizada de todos os acessos ao WWW feitos pelos computadores da rede interna;
- os servidores de *proxy* podem guardar as páginas Internet que são trazidas do exterior, durante um certo intervalo de tempo; se, por exemplo, uma certa página Internet foi pedida pelo utilizador de um computador, porém, esta mesma página foi solicitada por um outro utilizador então o servidor *proxy* identifica esta situação e devolve a página que estava armazenada, evitando assim ir buscar de novo essa página ao servidor

onde a página estava alojada, o que diminui o tráfego na rede e melhora os tempos de resposta vistos pelos utilizadores da rede.

5.1.4. REDES VIRTUAIS PRIVADAS

As redes virtuais privadas (VPN – *Virtual Private Networks*) são soluções tecnológicas que usam tecnologias criptográficas para cifrar a informação que atravessa uma rede pública, como a Internet, garantindo elevados padrões de segurança.

Na figura 5.4 representa-se uma organização que tem as suas instalações distribuídas por três locais físicos e que usa a Internet para as interligar.

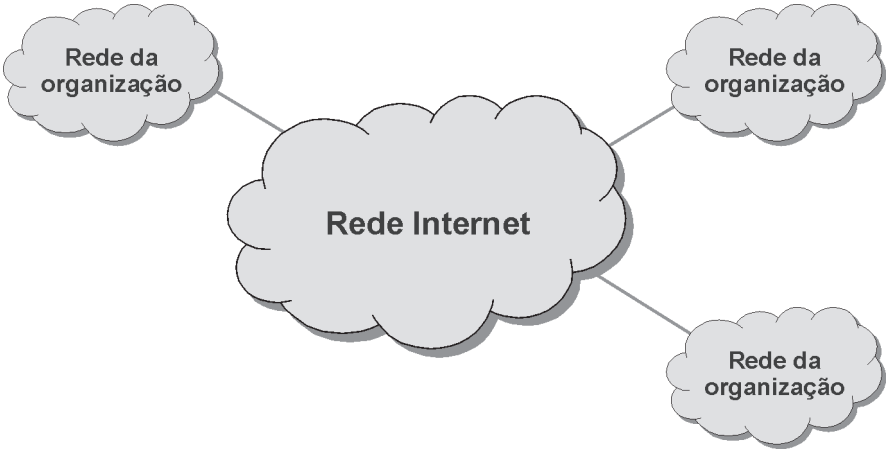

Figura 5.4 • Rede virtual privada

Para ligar estes três locais físicos a organização pode proceder ao aluguer de circuitos dedicados para os interligar. No entanto, esta situação pode sair cara, porque exige que estes circuitos dedicados se liguem a locais distantes entre si.

Este problema pode ser resolvido se for usada uma rede pública como a Internet para ligar os três locais. Contudo as redes públicas podem ser alvo de intercepções se não houver diversos cuidados. É aqui que uma rede virtual privada pode ter um papel importante. Basicamente a rede virtual privada é concretizada cifrando todos os datagramas que são enviados para a rede. Por exemplo, quando se envia uma mensagem de correio electrónico entre dois locais através da VPN todos os datagramas IP que transportam a mensagem são cifrados antes de serem enviados para a Internet. No destino, estes

datagramas são decifrados. Se houver uma intercepção no meio da rede Internet, o agente que a realizou não consegue ter acesso ao conteúdo de cada datagrama individual, pois todos são cifrados.

Hoje em dia é possível criar VPN mesmo a partir de postos de trabalho isolados, como por exemplo um computador pessoal. Um teletrabalhador pode ligar-se à rede da sua empresa através de uma VPN, tendo assim elevados níveis de segurança para efectuar o seu trabalho remoto.

ESTUDO DE CASO

Quando uma autarquia está distribuída por vários locais geográficos e é preciso interligar as várias redes locais, como já vimos, uma das soluções possíveis e com custos de gestão moderados são as VPN.

Uma alternativa ao uso de VPN é a instalação de redes privadas alugando os circuitos aos operadores, sendo a rede criada e gerida pelos próprios técnicos da autarquia. Esta solução é mais flexível mas tem custos de investimento e de exploração que devem ser avaliados face à solução da VPN.

Os operadores de telecomunicações disponibilizam hoje soluções que se podem adaptar às necessidades da maioria das situações de interligação das redes de uma autarquia, em termos de velocidades, qualidade de serviço e tudo isto aliado a elevados níveis de segurança. Tendo os operadores equipas e meios redundantes, conseguem-se obter com as VPN níveis de disponibilidade da rede muito elevados, evitando interrupções de serviço sempre indesejáveis e com prejuízos significativos.

5.1.5. ASSINATURAS DIGITAIS

Uma assinatura digital é um conjunto de informações que é adicionado a um documento de modo a garantir a sua associação a uma pessoa física, assim como a assinatura confirma que um documento está associado a uma dada pessoa.

As tecnologias criptográficas são a base da realização das assinaturas digitais. Assinar digitalmente um documento é um processo que consiste nos seguintes passos elementares:

1. A partir de um documento em formato digital, por exemplo, um ficheiro de texto com o original de um contrato, deverá ser tratado de modo a obter um **sumário** do documento. O sumário consegue-se através de um algoritmo matemático e visa detectar qualquer alteração ao documento original. Se for feita qualquer alteração a este

(por exemplo, uma adulteração) o sumário gerado a partir do documento é diferente;

2. Cifrar o sumário do documento através da chave privada de quem o assina;
3. Enviar o documento e o seu sumário cifrado para o destinatário.

Após estes três passos quem recebe o documento começa por decifrar o sumário deste com a chave pública do emissor, isto é, quem assinou o documento. De seguida calcula o sumário do documento recebido com o mesmo algoritmo matemático e compara-o com o sumário recebido. Se forem iguais pode concluir o seguinte:

Que o documento original é uma cópia fiel daquele que foi enviado, ou seja, entre o emissor e o receptor não existiu qualquer tipo de alteração pois, se tal acontecesse, os dois sumários não poderiam ser iguais;

Que quem assinou o documento é o detentor da chave privada usada para cifrar o sumário recebido, pois ele pode ser decifrado através da chave pública que lhe corresponde.

Estas técnicas são extremamente robustas do ponto de vista computacional, podendo dizer-se que é impossível adulterar um documento sem este facto ser detectado (ou seja, não é possível alterar um documento após ele ter sido assinado digitalmente) e, também, que é possível associar o autor do documento a uma pessoa, aquela que usou a sua chave privada para assinar digitalmente o sumário do documento. Como curiosidade refira-se, por exemplo, que quando assinamos um contrato em papel temos de rubricar todas as páginas do documento e assinar a última. No processo de assinatura digital apõe-se uma assinatura a todo o documento, sendo um processo conceptualmente mais perfeito.

5.1.5.1. Autoridades de certificação

Para um indivíduo poder usar os meios atrás expostos precisa de ter uma chave privada e uma chave pública. Além disso precisa de guardar a sua chave privada de um modo muito seguro e, também, necessita que a sua chave pública seja divulgada do modo mais alargado possível para esta ser acessível a quem quiser (por exemplo, para poderem confirmar a origem dos documentos por si assinados, por exemplo).

As autoridades de certificação são, geralmente, empresas que efectuam as tarefas de gerar uma chave privada e uma chave pública para uma pessoa, certificar a identidade dessa pessoa e dar-lhe de modo seguro e confidencial

a sua chave privada. Além disso distribuem na Internet a sua chave pública. São, assim, um elemento essencial para a criação de uma infra-estrutura de comunicação segura e confiável, mesmo entre entidades que não se conhecem, mas que confiam na autoridade de certificação.

5.1.6. POLÍTICAS E AUDITORIA DE SEGURANÇA

Os instrumentos tecnológicos que analisámos nas secções anteriores são um componente fundamental na protecção e no uso seguro dos sistemas de informação e das redes. Contudo, como qualquer tecnologia não resolve os problemas se não for devidamente aplicada.

Deve ser obrigação dos dirigentes de cada organização a definição das políticas de segurança a que deve obedecer a sua rede e os sistemas de informação pelos quais é responsável.

Este trabalho deve ser feito por técnicos especializados com base nas orientações recebidas dos gestores da organização. Estas políticas de segurança devem estar contidas num documento, que deve ser validado pela gestão de topo da organização, e cujas partes não confidenciais devem ser divulgadas por todo o pessoal da organização. A divulgação da política de segurança informática de organização pelo seu pessoal é muito importante para: i) se saber que existe uma política de segurança informática na organização; ii) consciencializar o pessoal para a importância de preservar um dos valores mais importantes de qualquer organização, a sua informação; iii) evitar que se cometam erros básicos que podem comprometer quer a segurança da informação da organização, quer o seu normal funcionamento.

Uma outra actividade importante que deve complementar os aspectos que temos vindo a referir é a auditoria de segurança informática. É um processo fundamental que consiste, de um modo simplificado, em verificar se as políticas de segurança definidas para a organização estão a ser aplicadas de modo correcto e adequado. Como resultado desta auditoria será produzido um documento que deve ser analisado pela gestão da organização para poder verificar a boa adequação das políticas de segurança informática definidas e a sua adequada concretização pelos técnicos. Como boa prática esta auditoria deve ser realizada por auditores externos à organização. Acresce que é conhecido que muitos problemas de segurança das organizações têm origem no seu interior, o que torna ainda mais importante o recurso a meios externos à organização para efectuar esta auditoria.

ESTUDO DE CASO

A quem compete definir a política de segurança na minha autarquia?

Sem dúvida que a responsabilidade última é da presidência da autarquia, que deve pedir ajuda a especialistas de informática internos ou externos, para a produção de um documento com as linhas orientadoras de toda a política de segurança da informação e dos sistemas informáticos. Esta política deve incluir muitos aspectos: i) segurança e confidencialidade da informação, incluindo a segurança lógica e física das instalações e equipamentos; ii) políticas de cópias de segurança e sua salvaguarda; iii) definição das funções e dos serviços disponíveis a cada funcionário dependentemente da sua função; iv) orientações de formação do pessoal técnico e não técnico sobre a segurança, incluindo regras de manipulação e salvaguarda de códigos de acesso, como o correio electrónico deve ser tratado de modo a evitar intrusões de vírus ou cavalos de Tróia; v) planeamento de medidas periódicas de monitorização da adequada concretização das políticas de segurança, etc.

5.1.6.1. A segurança dos sistemas operativos e das aplicações

Uma das funções de qualquer sistema operativo, como vimos, é introduzir mecanismos de segurança e de protecção. Estas funções destinam-se a garantir a integridade do sistema, para que este possa desempenhar as suas funções na íntegra mas, também, que proteja o sistema contra uso indevido.

Por outro lado, a dinâmica do sector da informática leva a que os fabricantes estejam constantemente a produzir novas versões dos seus sistemas operativos, dos gestores de bases de dados, dos compiladores e das aplicações.

Por fim e face ao desenvolvimento da informática, verifica-se que nos últimos anos os sistemas operativos e as aplicações se tornaram cada vez mais complexos, sendo constituídos por milhões de linhas de código. Cada versão que é produzida por estes sistemas, apesar do enorme esforço de teste que os seus criadores lhes dedicam, há sempre algumas falhas residuais, as quais são, frequentemente, aproveitadas por indivíduos que pretendem violar a segurança dos sistemas de informação e das redes.

É necessário estar consciente da actual fase de evolução da informática para se poder compreender a necessidade de cuidados especiais na gestão dos sistemas operativos e aplicações actuais, e de como estes cuidados devem ser integrados na política de segurança de uma organização.

Todos os actuais sistemas operativos têm falhas ou erros de concepção ou de implementação, de maior ou menor dimensão. Os seus fabricantes estão atentos a esta situação e têm permanentemente equipas que identifi-

cam estas debilidades de segurança, as quais produzem soluções para a sua correcção. Uma das fontes de conhecimento das falhas que existem resultam de ataques que são efectuados por piratas informáticos, a outra é a base de utilizadores.

Quando é identificada uma falha num sistema operativo, num período de tempo mais ou menos curto, o seu fabricante disponibiliza soluções para a sua correcção sob a forma de alterações ao código do sistema operativo e que recebem a designação de *patches* (remendos). É muito importante que os administradores dos sistemas informáticos procedam à instalação frequente destes remendos para garantir que as falhas de segurança conhecidas para a versão do sistema operativo em uso na instituição estão devidamente instaladas. Como é fácil de perceber estes procedimentos devem fazer parte da política de segurança da instituição.

CAPÍTULO

6

eGOV: EXEMPLOS DE SOLUÇÕES TECNOLÓGICAS

OBJECTIVOS

- São apresentados alguns exemplos simples de plataformas tecnológicas para suporte de soluções de governo electrónico.
- Analisam-se soluções com crescentes níveis de funcionalidade e complexidade.

P O N T O D A S I T U A Ç Ã O

A maturidade dos países em termos de Sociedade da Informação é medida por vários indicadores. Dentro de um vasto conjunto de indicadores os que se referem ao nível de desenvolvimento do Governo Electrónico (eGov) são os mais relevantes por permitirem observar até que nível o país beneficia das vantagens das TIC na disponibilização de serviços em linha para os cidadãos e para as empresas.

Portugal tem, desde 1997, vindo a dar passos importantes para a disponibilização de serviços de eGov, mas o mesmo acontece com os nossos parceiros da União Europeia. Urge aumentar o ritmo da nossa Administração Pública no sentido de disponibilização dos serviços em linha. Para este efeito as autarquias podem dar uma ajuda decisiva, pois são entidades que têm uma forte interacção com os cidadãos e, assim, podem ser importantes agentes de mudança nesta área.

6.1. eGOV: EXEMPLOS DE SOLUÇÕES TECNOLÓGICAS

O termo eGov, acrónimo para Governo Electrónico, refere-se a um conjunto de tecnologias e soluções para disponibilização de serviços aos cidadãos e às empresas pelos vários níveis da Administração Pública.

Na realidade a definição e delimitação rigorosa do âmbito e contornos do eGov tem sido alvo de muito estudo e discussão. Neste trabalho como nos preocupamos mais com a apresentação de aspectos tecnológicos usaremos esta definição simples de eGov que é, em nossa opinião, suficientemente abrangente para os objectivos da apresentação de como as tecnologias abordadas nos capítulos anteriores podem ser utilizadas na construção de diferentes plataformas tecnológicas.

Sendo objectivo central das interacções entre a Administração Pública, por um lado, e os cidadãos e as empresas, pelo outro, a troca e disponibilização de informação é de esperar que as Tecnologias da Informação e Comunicação (TIC) possam ser um veículo de eleição para agilizar estas interacções. Por outro lado as evoluções nas tecnologias da Internet poderão, se devidamente utilizadas, contribuir para um significativo aumento da eficiência na disponibilização dos serviços da Administração Pública e que poderá estar associada à redução de custos de exploração, como se tem verificado, por exemplo, no sector bancário.

6.1.1. NÍVEIS DE EGOV

Nas interacções com a Administração Pública podemos, de modo simples, diferenciar níveis de crescente complexidade da solução. Em geral soluções mais complexas correspondem a níveis mais aprofundados de interacção entre Administração e utentes, com ganhos crescentes mas, de igual modo, com complexidades crescentes de concretização.

Se bem que entre os vários autores que se têm debruçado sobre esta matéria tenham modos diversos de classificar os níveis de complexidade das soluções de eGov, aqui introduzimos um modelo de três níveis, que consideramos suficiente para analisar as linhas gerais das soluções tecnológicas que são fundamentais para nós nesta obra. Assim podemos ter os seguintes níveis de desenvolvimento de soluções:

- Acesso à informação da Administração Pública através de canais de comunicação suportados em TIC;
- Acesso à informação da Administração Pública através de canais de comunicação suportados em TIC e comunicação de informação ou efectivação de pedidos à Administração através destes mesmos canais;
- Realização de transacções entre a Administração Pública e os utentes que com ela interagem (cidadãos ou empresas).

O nível de complexidade tecnológica e organizativa de cada uma destas soluções é crescente mas traz vantagens para os diferentes utentes que são, de igual modo crescentes. Estas vantagens são visíveis e mensuráveis em termos de eficiência da solução para os vários utentes envolvidos, dos ganhos de exploração do sistema e da disponibilidade da solução.

A concepção destas várias soluções tem o mesmo conjunto básico de componentes que são um servidor Internet (servidor WWW) e um sistema de informação da Administração.

Nos diferentes cenários, os serviços instalados em cada um destes componentes, o modo como os funcionários e os utentes dos serviços da Administração interagem com o sistema de informação e os mecanismos de segurança variam significativamente, como veremos. Além disso para se poder atingir o nível mais sofisticado de concepção, sistema com transacções, há que efectuar uma reengenharia dos «processos de negócio» da Administração quer do ponto de vista processual, quer do ponto de vista de novas práticas de actuação pelos serviços e pelos funcionários da Administração. Esta reengenharia é aconselhável para permitir a necessária adaptação dos processos e dos objectivos da Administração a um tratamento completamente automati-

zado e disponibilizado numa base permanente (o modelo 24*7, ou seja, 24 horas por dia e 7 dias por semana). Muitos processos da Administração estão presentemente estruturados em torno de múltiplas intervenções humanas, muitas vezes desnecessárias, penalizadoras da eficiência e que inviabilizam a informatização e, além disso, desnecessárias e só existentes pela carência de um efectivo esforço para o seu redesenho.

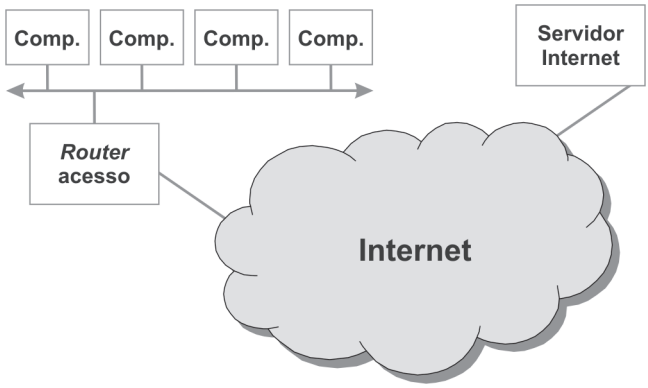

Figura 6.1 • Configuração genérica

Na configuração genérica que apresentamos na figura 6.1 representamos uma organização (da Administração Pública) que dispõe de uma rede local e de um servidor Internet. Pelo menos um dos computadores da sua rede local pode ser um servidor onde está armazenada toda a informação da organização.

A interacção e troca de informação entre o servidor local e o servidor Internet, implementada através do *software* aplicacional, que pode ser extremamente complexo nos casos mais avançados de eGov, é a base dos serviços que são prestados pelo organismo. Para podermos expor as vantagens destas soluções vamos, de seguida, proceder à análise de três cenários que correspondem, *grosso modo*, aos três níveis de complexidade que referimos.

6.1.2. CENÁRIO DE DISPONIBILIZAÇÃO DE INFORMAÇÃO

Como foi já referido trata-se do cenário mais simples em que é disponibilizada informação aos cidadãos e às empresas pela Administração.

Trata-se de uma utilização das novas tecnologias da comunicação (TIC) para aumentar a abrangência e eficiência na disponibilização de informação de carácter público. Com as possibilidades que a Internet traz de dar acesso à informação de modo permanente e global, os vários níveis da Administração podem criar um sítio na Internet onde disponibilizam documentos com a informação relevante.

A solução tecnológica para esta situação pode ser concretizada como se representou na figura 6.1 mas cuja versão mais adequada a este caso se mostra na figura 6.2.

Há um servidor Internet que concretiza o sítio de um organismo da Administração. Os conteúdos para o sítio são transferidos pelos funcionários usando um conjunto de ferramentas informáticas disponíveis para o efeito (aquilo que podemos designar pelo *backoffice* – retaguarda – do sítio da Internet). Informações, avisos públicos, notícias, podem ser divulgados a comunidades muito alargadas a custos muito moderados.

Quando comparado com outros métodos, baseados em papel (por exemplo, um folheto periódico), conseguem-se custos de produção reduzidos com a possibilidade de actualizações frequentes. Com efeito podem-se ter actualizações diárias, ou mesmo várias vezes ao dia, com custos de produção muito reduzidos.

Referindo-nos de novo à representação esquemática da figura 6.2 aqui os funcionários da organização estão a trabalhar nos computadores ligados à rede local do organismo. Em cada um destes postos de trabalho deverá ter sido instalado *software* cliente que permite inserir ou actualizar informação no servidor Internet de modo transparente. Este *software* de *backoffice* autentica o utilizador que fica, a partir deste momento, autorizado a agir sobre todo o sítio na Internet do organismo ou numa parte sua, por exemplo, a parte do sítio na Internet pela qual o funcionário é responsável.

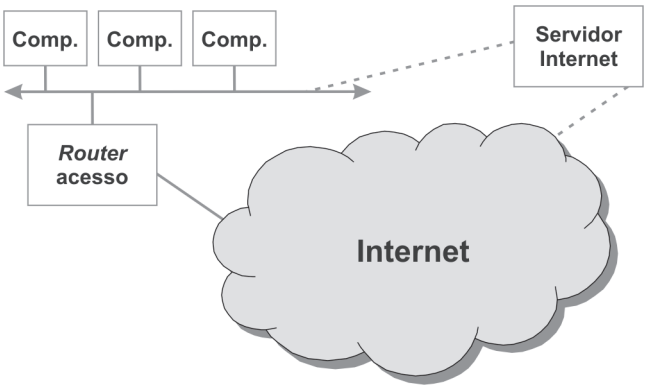

Figura 6.2 • Cenário de disponibilização de informação

Os sítios na Internet de organismos que primam pela qualidade e abrangência da informação disponibilizada, da sua utilidade para os públicos alvo, da regularidade da sua utilização e da ergonomia da sua interface gráfica designam-se por portais desses organismos.

Este é um cenário já muito usado em diversas autarquias que dispõem do seu portal na Internet. Na figura 6.3 vemos um exemplo do portal na Internet de uma Câmara Municipal (www.cm-grandola.pt). Este portal disponibiliza diversos serviços de informação para os seus utentes. Além destes disponibiliza ainda serviços tais como pedidos de certidões que são, todavia, serviços que já classificamos no nível seguinte de interacção entre a Administração e os seus utentes, como veremos.

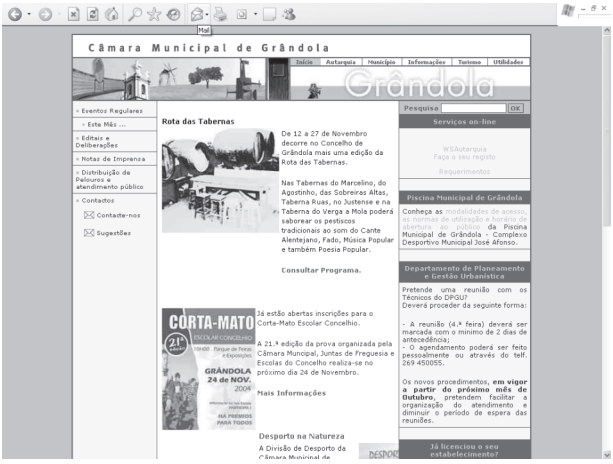

Figura 6.3 • Exemplo do portal na Internet de uma Câmara Municipal

Mas centrando-nos ainda na solução tecnológica para este caso e recorrendo de novo à figura 6.2, aqui representámos o servidor Internet que acolhe as páginas do portal como podendo estar ligado à rede interna da organização ou à Internet.

No primeiro caso a organização tem o servidor integrado na sua rede interna e os acessos a este servidor pelos utentes são feitos através da Internet pelo acesso à rede da organização. Estes acessos aumentam o tráfego desta ligação, a qual deve ser devidamente dimensionada para suportar o tráfego dos utentes. Se houver um dimensionamento insuficiente da largura de banda deste acesso isto pode ser apercebido pelos utentes como o portal «estar lento». Em especial se for usado um acesso usando a tecnologia ADSL, como esta disponibiliza uma largura de banda no sentido ascendente (organização/rede) mais baixa que no sentido inverso, pode haver sérias limitações ao desempenho do portal da perspectiva do utilizador deste. Assim,

caso o portal esteja alojado na rede interna da organização deve-se ponderar o uso de outras tecnologias de acesso à Internet em alternativa ao ADSL.

Centrando ainda a nossa atenção neste caso e como o servidor está inserido na rede da organização, é preciso ter em consideração um conjunto de políticas de segurança para protecção do servidor que alberga o portal. Isto passa por usar as tecnologias que vimos no capítulo anterior.

Passando agora para o segundo caso representado na figura 6.2 podemos ter o servidor ligado à Internet mas fora da rede da organização. Um cenário como este é frequente e consiste em ter este servidor alojado na rede de um ISP (*Internet Service Provider*, empresa que presta serviços de comunicações na área da Internet).

O modo como os funcionários da organização fazem as actualizações das páginas Internet do portal é em tudo semelhante ao caso anterior, isto é, estas actualizações são feitas através do *backoffice* de gestão de conteúdos do portal. Claro que para os funcionários poderem aceder à rede externa e actualizarem as páginas do portal há que implementar políticas de segurança adequadas.

Um outro exemplo de um portal informativo é o Programa Operacional Sociedade da Informação (POSI), acessível em www.posi.pcm.gov.pt e cuja página de entrada podemos ver na figura 6.4.

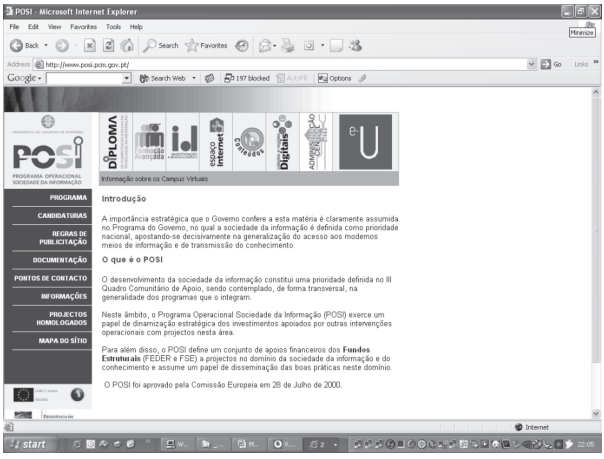

Figura 6.4 • Exemplo do portal na Internet do POSI

No portal do POSI é possível ter acesso a todas as informações sobre o Programa, tais como legislação aplicável, listagem de projectos aprovados, regras de publicitação, entre muitos outros conteúdos. Existem também disponíveis formulários que podem ser descarregados para o computador do utente para utilização. Neste portal já existem alguns servi-

ços um pouco mais avançados que permitem a um utente registar-se e, a partir daí, pode passar a receber determinados tipos de informação de um modo automático na sua conta de correio electrónico. É um modo excelente de um utente ser informado sobre o que acontece em relação a um determinado serviço da Administração sem ter de ter a preocupação de aceder periodicamente ao portal.

Em relação a estes dois cenários, em que se dispõe de um servidor Internet que alberga o portal num ISP podem ser concretizados de dois modos distintos, cada um deles com as suas vantagens e características: i) *housing* do servidor, ou ii) *hosting* do portal. Vamos analisar cada uma destas alternativas.

Quando a organização dispõe de um computador e servidor Internet que alberga as páginas do portal e este equipamento é colocado nas instalações de um ISP trata-se da situação de *housing*. A gestão do *hardware* e do *software* do servidor é, regra geral, da responsabilidade integral da organização que faz esta gestão remotamente a partir da sua rede local, se bem que outros modelos contratuais possam ser negociados.

Esta solução tem a vantagem de colocar o servidor do portal na rede do ISP que está ligada à Internet em alta velocidade. Deste modo o portal está acessível aos utentes em condições óptimas de velocidade.

Além disso esta rede tem uma disponibilidade muito maior que a rede da organização. Imagine-se, na situação em que o servidor está sedeado na rede da organização, e há uma avaria no circuito que concretiza o acesso da rede da organização. Durante o tempo em que este acesso estiver a ser reparado o portal da organização está indisponível, o que pode ser indesejável quando se pretende fornecer serviços de alta qualidade.

Passemos agora a analisar a situação de *hosting*. Neste caso a organização não necessita de adquirir o *hardware* e *software* para concretizar o portal. O ISP disponibiliza uma plataforma computacional onde as páginas que concretizam o portal podem ser alojadas. São da responsabilidade do ISP todas as actividades de gestão do *hardware* do servidor, do seu sistema operativo, do servidor WWW, dos serviços de segurança, etc. A organização faz um contrato com o ISP onde são definidas as características dos serviços oferecidos como espaço em disco para alojamento do portal, tipo de servidor WWW e serviços adicionais, disponibilidade, segurança, entre outros.

Do ponto de vista de uma organização que não pretenda ter encargos elevados de investimento com a plataforma computacional, com licenças de *software* e com o pessoal técnico para fazer a gestão do servidor, esta solução pode ser bastante vantajosa.

No caso do *housing* a actualização das páginas pode ser, também, feita a partir da rede da organização e podem ser implementados mecanismos de

segurança para garantir que este processo se faça com os mais elevados padrões de confidencialidade. Pode-se, por exemplo, estabelecer uma VPN entre a rede da organização e o servidor do ISP, para este efeito.

Um último exemplo que aqui apresentamos da aplicação desta tecnologia, em sistema de *housing*, utilizada por um elevado número de organismos, e que também é uma plataforma computacional que suporta muitos sítios na Internet, é o portal do Programa Espaços Internet do POSI, disponível em http://www.espacosinternet.pt.

O Programa Espaços Internet do POSI visa criar espaços públicos de acesso gratuito à Internet nas Câmaras Municipais. Ao abrigo deste programa já estão a funcionar quase duas centenas de Espaços Internet no país. Surgiu a necessidade de cada Espaço ter uma presença na Internet, obedecendo a um conjunto de critérios que garantissem uma certa uniformidade nesta presença. Assim nas páginas Internet de cada Espaço deveria estar informação institucional, horários de funcionamento, lista de actividades periódicas e ocasionais, notícias relevantes para a comunidade servida pelo Espaço Internet, entre outras.

Figura 6.5 • Exemplo de um sítio de um Espaço Internet alojado num servidor central em regime de *hosting*

Por outro lado o nível de conhecimentos dos técnicos responsáveis pela gestão de cada Espaços Internet variava muito de local para local do país. Nalguns existiam técnicos com um elevado nível de conhecimento de produção de páginas Internet, noutros os técnicos que foram recrutados não tinham conhecimentos sobre produção de páginas Internet, até porque tal não era necessário para a sua principal função nestes Espaços.

A solução para resolver esta situação consistiu em criar um servidor Internet central que aloja as páginas de todos os portais de todos os Espaços Internet. Este servidor está sedeado num local de facilmente disponível na

Internet. Assim qualquer pessoa que aceda ao sítio de um Espaço Internet tem uma velocidade de acesso muito grande.

O sistema de gestão de portais instalado neste servidor impõe a todos os Espaços Internet uma estrutura lógica e um aspecto gráfico de apresentação dos sítios comum e uniforme. Isto é muito vantajoso do ponto de vista dos utilizadores dos portais, pois dispõem de uma mesma estrutura de acesso à informação independentemente do portal a que acedem. Este aspecto é muito importante, em particular para utilizadores pouco experientes de uso da Internet, para os quais uma coerência lógica e estrutural da informação é uma condição para a simplicidade de acesso.

Para a actualização das páginas Internet de cada Espaço Internet foi disponibilizada uma aplicação de *back-office*. Esta aplicação permite aos técnicos de cada Espaço autenticarem-se e, a partir daí, actualizarem o «seu» portal de um modo simples, eficiente e, talvez mais importante, sem terem necessidade de conhecerem a linguagem HTML em que estão escritas as diferentes páginas de cada portal.

6.1.3. CENÁRIO EM QUE SÃO SUPORTADOS PEDIDOS

Do ponto de vista estritamente técnico e das tecnologias de suporte, a solução tecnológica necessária para suportar um cenário em que além de serem disponibilizados serviços de informação através do portal também se suportam pedidos dos utilizadores dos serviços do organismo é bastante idêntica à acabada de analisar.

Para concretizar esta solução são adicionadas às funcionalidades do portal que já vimos umas novas que permitem aos utentes do organismo efectuar pedidos. Numa análise atenta do exemplo que mostramos na figura 6.3 podemos ver que no canto superior direito do portal há uma secção designada «Serviços *on-line*».

Nos portais de organismos em que são suportados pedidos existe uma secção do portal em que o utente pode efectuar pedidos aos serviços desse organismo. O nível de serviços e o modo como são concretizados varia dentro de um leque muito diversificado de hipóteses.

No nível mais básico podemos considerar o simples envio de uma mensagem de correio electrónico para o organismo. Trata-se de substituir o método mais tradicional de ir a um balcão, fazer um telefonema ou enviar uma carta.

Na realidade a obrigatoriedade dos serviços públicos tratarem o correio electrónico em pé de igualdade com outros meios já está previsto na legislação nacional há alguns anos. Além dos organismos que integraram o correio electrónico no dia-a-dia do seu funcionamento há, infelizmente, duas situações que são indesejáveis: i) organismos que não obedeceram às orientações da legislação e nada fizeram; e ii) organismos que criaram a caixa de correio mas não criaram na sua estrutura organizativa os procedimentos necessários para que o correio electrónico fosse integrado no normal funcionamento do organismo; as mensagens que são enviadas para essa caixa de correio não são tratadas com a mesma periodicidade e diligência das comunicações por outros meios mais tradicionais.

O segundo caso acabado de referir, isto é, um organismo que cria um processo que poderia permitir que os utentes desse organismo pudessem passar a efectuar pedidos através da Internet, mas não o integra no seu funcionamento normal é um mau exemplo e é um dos principais desafios que existe para a implementação deste cenário de eGov.

Mas como podem os utentes concretizar os seus pedidos ao organismo? Além do método básico do correio electrónico podemos considerar dois casos:

- formulários disponíveis no sítio do organismo, que são descarregados para o computador do utente e aí preenchidos; depois de preenchidos são enviados por correio electrónico e assinado digitalmente para o organismo;
- formulários electrónicos disponíveis no sítio do organismo, que são preenchidos directamente pelo utente; quando o formulário está completamente preenchido é automaticamente enviado para o organismo.

O primeiro caso é ainda mais básico, corresponde em linhas gerais a substituir os tradicionais formulários em papel por um documento electrónico que é mais económico e que pode ser preenchido de uma maneira mais eficiente.

Um dos principais problemas desta situação reside no facto de não existirem normas para o formato destes documentos, acabando-se muitas vezes por usar documentos em formatos específicos de um certo tipo (documentos *Word*), o que é indesejável do ponto de vista de independência de plataformas computacionais.

A segunda situação é muito mais interessante, é já implementada por uma diversidade de organismos da nossa Administração Pública e é o que iremos analisar. Usaremos como base a funcionalidade de pedido de certidões disponível no Portal do Cidadão, acessível em:

http://www.portaldocidadao.pt

Após entrar neste portal pode-se aceder a um formulário electrónico para pedido de diversos tipos de certidões. Na figura 6.6 apresenta-se o exemplo do formulário para pedir uma certidão de registo civil.

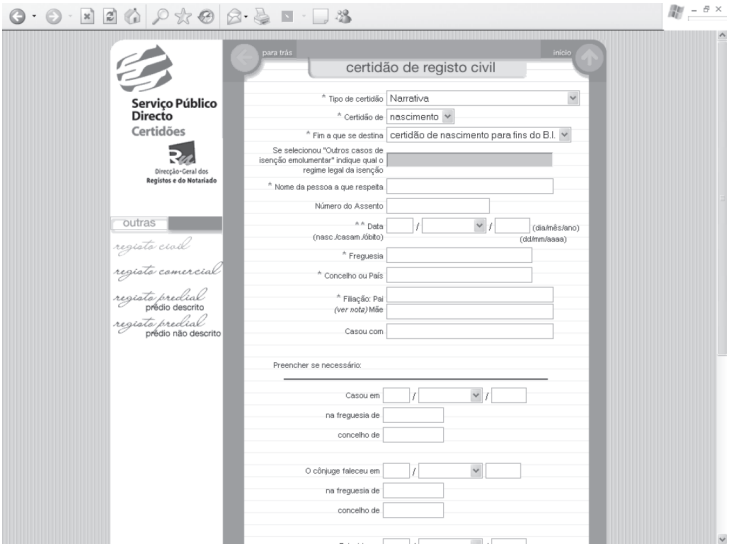

Figura 6.6 • Formulário para pedido de uma certidão de registo civil

Neste caso, como na maioria das situações em que existe um formulário electrónico para efectuar pedidos, o utente é confrontado com um ou com vários ecrãs onde vai sendo guiado por uma série de pedidos para balizar o que pretende exactamente. Este processo tem a vantagem de que o utente irá pedir uma certidão que corresponde à sua necessidade por ter sido guiado nas suas selecções.

No exemplo da figura 6.6 temos um exemplo onde começamos por aceder ao Portal do Cidadão, pesquisamos por «pedido certidão» e fomos imediatamente guiados à página inicial dos Pedidos de Certidão. Aqui seleccionamos uma certidão de nascimento, indicámos o distrito e concelho em causa e, após estas primeiras selecções apareceu-nos o ecrã que se reproduz nesta figura.

Para concretizar o pedido de certidão bastaria preencher os vários campos com os dados da pessoa a quem a certidão se refere e submeter o pedido. Preenchem-se de seguida, numa nova página Internet, os dados relativos à morada para onde a certidão deve ser enviada pelos serviços da Administração. O sistema efectua um cálculo do custo da certidão e da sua expedição e permite o pagamento de vários modos: à cobrança, por cartão bancário electrónico (*vulgo* Multibanco), cartão de crédito, etc.

Este sistema particular tem tido, desde há anos, um apreciável sucesso pois permite a qualquer pessoa com acesso à Internet pedir uma certidão de modo simples e eficiente. A título de curiosidade refira-se que tem sido bastante usado por emigrantes portugueses residentes no estrangeiro que podem, em qualquer lugar do mundo, fazer pedidos de certidões.

Qual o suporte tecnológico para permitir estas funcionalidades?

Vamos então de seguida voltar a analisar as soluções tecnológicas para este cenário de eGov e, de seguida, iremos tecer algumas considerações sobre o impacto destas soluções tecnológicas no funcionamento do organismo.

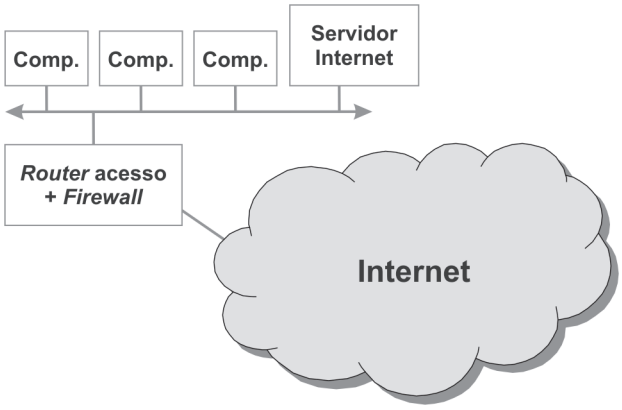

Figura 6.7 • Arquitectura para o sistema de eGov com suporte a pedidos

A representação da figura 6.7 e que é essencialmente semelhante a outras já analisadas, irá por nós ser usada para apresentar algumas soluções tecnológicas para este caso.

No servidor Internet do organismo, que supomos estar já integrado na sua rede local, é instalada uma aplicação que concretiza o formulário. Trata-se de uma das possibilidades da linguagem HTML a construção de formulários. Além disso os formulários podem ter associado um código que faz algumas validações ao que é inserido pelos utentes. Podemos considerar um formulário como sendo constituído por uma série de campos, que:

- podem ser preenchidos com texto livre (por exemplo, o nome de uma pessoa ou uma morada);
- podem conter texto ou números que podem ser validados pelo *software* que executa no servidor (por exemplo, validando o código postal ou verificando se o número de telefone tem o número de dígitos correcto);
- caixas de selecção múltipla que confrontam o utente com as várias hipóteses que podem ser escolhidas para esse campo do formulário (por

exemplo, se seleccionamos um certo distrito num campo e no seguinte temos de seleccionar um concelho, apenas aparecem para serem seleccionados os concelhos do distrito previamente escolhido).

Após finalizar o formulário o utente submete-o ao organismo.

Existem diversas soluções tecnológicas para tratar o formulário após a sua submissão. Uma solução interessante consiste em armazenar o formulário numa base de dados devidamente estruturada. Outra alternativa consiste em gerar um ficheiro com o conteúdo formatado correspondente ao formulário preenchido. Em qualquer dos casos o que se segue é o tratamento do formulário.

O tratamento ou processamento do formulário é feito pelo *back-office* do organismo. Trata-se de uma fase cuja complexidade e dificuldade dependem do modo como o organismo se preparou para suportar este tipo de pedidos. Regra geral o pedido do utente, independentemente da solução tecnológica usada para o seu armazenamento (base de dados ou ficheiro), é enviado a um funcionário que o deverá processar.

Do ponto de vista do utente trata-se de uma solução cómoda pois pode usar o sistema numa base 24*7 e pode fazer o pedido, por exemplo, desde sua casa.

Do ponto de vista do organismo esta solução também é eficiente pois, relativamente ao pedido do utente, há a garantia de que este já vem validado numa série de aspectos o que simplifica a sua resposta.

Passando agora à análise desta solução do ponto de vista tecnológico há um conjunto de características que queremos evidenciar.

Como o utente está ligado ao servidor do organismo através da Internet durante todo o tempo em que está a preencher o formulário podem verificar-se as seguintes duas situações incómodas:

- se o acesso à Internet do organismo não está devidamente dimensionada para o número de pedidos que se estima que sejam feitos em simultâneo, este parece «estar lento» do ponto de vista do utente, o que pode levar à sua desmotivação e abandono deste tipo de uso;
- se a ligação à Internet do utente for interrompida durante o preenchimento do formulário (por exemplo, se estava a ser usada uma ligação por *modem* e a ligação é interrompida) todo o trabalho que estava a ser feito perde-se, devendo o utente voltar a repetir todo o processo desde o início.

Analisados os diversos aspectos tecnológicos e de organização do organismo para suportar pedidos, podemos ver que é uma via interessante para concretizar soluções de eGov com esforço e custos moderados.

6.1.4. CENÁRIO EM QUE SÃO REALIZADAS TRANSACÇÕES

O nível mais aprofundado de eGov é o que vamos analisar de seguida. Atendendo às muitas alternativas tecnológicas não podemos considerá-las todas, indo centrar o nosso foco num tipo de solução que julgamos suficientemente poderosa para se compreender a extensão das suas vantagens e o seu nível de complexidade.

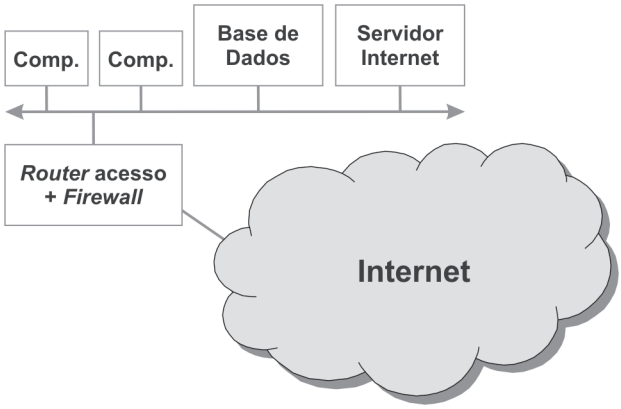

Figura 6.8 • Arquitectura para o sistema de eGov com suporte a transacções

Podemos analisar este caso através de uma primeira observação da figura 6.8, onde podemos evidenciar que além do servidor Internet existe um servidor com um gestor de bases de dados. Este tipo de arquitectura permite concretizar transacções, na medida em que o servidor Internet interage com o gestor de base de dados podendo haver apresentação de dados contidos na base de dados ou introdução de informação na base de dados pelo utente.

Para este tipo de interacção entre o utente e o organismo o processo deve iniciar-se por uma autenticação do utente. Após esta autenticação o utente fica autorizado a efectuar um certo conjunto de operações de consulta ou de inserção de dados na base de dados. Por exemplo, consideremos um caso simples em que um utente de um organismo quer actualizar informação sobre uma mudança do seu número de telemóvel de contacto. Poderia aceder ao portal do organismo e autenticar-se. Após esta fase seleccionaria uma opção de actualização de dados pessoais. O servidor Internet faria um acesso à base de dados e apresentaria ao utente uma página Internet com o conteúdo do seu registo na base de dados. O utente alteraria o campo que pretende e terminaria com uma confirmação da alteração. Neste instante e após valida-

ção da informação introduzida (por exemplo, verificar se o número de telefone está num formato correcto) o servidor Internet faz uma transacção na base de dados que fica actualizada.

Este exemplo que descrevemos, necessariamente simples para não tornar a exposição demasiado complexa e fastidiosa, descreve um processo que hoje em dia já é usado em muitas situações em que se a apresentação de dados e/ou a recolha e actualização de dados relativos aos utentes de um serviço é completamente automatizada. Deste modo é possível com uma economia de recursos humanos e com uma grande disponibilidade do serviço promover a interacção entre utente e organismo.

Vamos suportar a apresentação de um cenário onde se suportam transacções com um organismo que dispõe de um sistema totalmente informatizado para gerir o seu relacionamento com os seus utentes, descrevendo e apresentando alguns aspectos do funcionamento. Trata-se do sistema de registo *on-line* de domínios Internet em .com.pt, com o qual temos uma familiaridade grande. Apesar da FCCN não ser de um organismo público o facto de gerir um recurso de importância para a comunidade Internet nacional, procedemos aqui à sua breve análise. Este sistema pode ser usado através do portal:

https://online.dns.pt/site/publico

Note-se que o URL deste sítio se inicia por https em vez do normal http. O «s» final indica que se trata de um sítio onde toda a comunicação entre utente e servidor Internet é feita usando um protocolo seguro. Este facto, na maioria dos *browsers* Internet é confirmado aparecendo um pequeno cadeado na parte inferior direita.

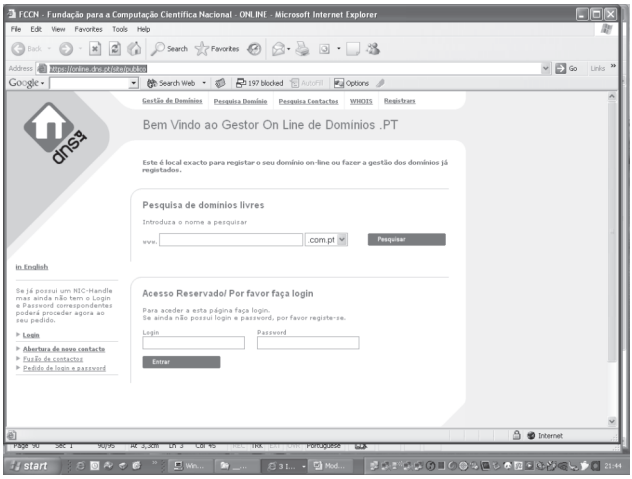

Figura 6.9 • Registo *on-line* de um domínio em .com.pt

Se o utente já se registou previamente, por exemplo por já ter anteriormente registado num domínio Internet, usa o seu *Login* e a sua *Password* para ser autenticado. Caso seja a primeira utilização preencherá um formulário electrónico com os seus dados e os códigos de acesso ser-lhe-ão enviados.

No caso de ser um utilizador já registado e após indicar e ter confirmação que o domínio que pretende está livre, o servidor Internet faz um acesso à base de dados onde está guardado o perfil do utilizador, não havendo necessidade de repetir esta informação.

Neste caso o utente, após registar o seu pedido de um novo domínio, pode fazer o pagamento pelos meios electrónicos tradicionais (Multibanco, Cartão de Crédito, entre outros).

Este sistema e outros que funcionam segundo o mesmo modelo, estão disponíveis numa base de funcionamento 24*7, não vinculando o utente a horários e pode ser usado a partir de qualquer sítio do mundo onde se possa estar ligado à Internet.

Uma última chamada de atenção que é imprescindível fazer em relação a este tipo de soluções refere-se à segurança. Estando a base de dados do organismo com a sua informação a ser acedida e actualizada de modo transaccional, há que garantir elevados padrões de qualidade na autenticação dos utentes e na atribuição de perfis de utilização que garantam que cada utente só acede à informação que lhe é específica. Assim os mecanismos de segurança postos em prática devem ser adequados à infra-estrutura disponível e ao modo como o servidor Internet e o sistema de gestão de base de dados estão implementados.

REFERÊNCIAS

Bibliografia

- Andew S. Tanembaum, *Modern Operating Systems,* Pearson Educatin, 2nd Edition, 2001.
- Andew S. Tanembaum, *Structured Computer Organization,* 4th Edition, Prentice-Hall.
- Andrew S. Tanenbaum, *Computer Networks*, 3th Edition, Prentice-Hall International Editions, 1996.
- Cricket Liu, *DNS and BIND Cookbook*, O'Reilly Associates.
- Dana Joy, *Protect Your Home PC: Hackers, Viruses and Privacy*, Gateway Press.
- Douglas Comer, *Internetworking with TCP/IP,* Prentice-Hall.
- Douglas Comer, *Internetworking with TCP/IP: Principles, Protocols and Architecture*, vol. 1*,* Prentice Hall, April 2000.
- Edmundo Monteiro, Fernando Boavida, *Engenharia de Redes Informáticas*, 3.ª Edição, FCA, 2000.
- L. Peterson, B. Davie, *Computer Networks: A Systems Approach,* 2nd Edition*,* Morgan Kaufmann Publishers, 2000.
- Olivier Hersent, *Beyond VoIP Protocols: Understanding Voice Technology and Networking Techniques for IP Telephony,* John Wiley and Sons.
- Paula Rainha, Sónia Queiroz Vaz, *Guia Jurídico da Internet em Portugal,* Centro Atlântico.
- Paulo Trezentos, António Cardoso, *Fundamental do Linux,* FCA.
- Ana Margarida Marques, Mafalda Anjos, Sónia Queiroz Vaz, *101 Perguntas e Respostas do Direito da Internet e da Informática*, Centro Atlântico.
- William Stallings, *Network Security Essentials*, US Imports & PHIPEs.

URL Recomendados

IETF – www.ietf.org

ICANN – www.icann.org

IEEE – www.ieee.org

World Wide Web Consortium – www.w3c.org

LINUX – www.linux.org

DNS em Portugal – www.dns.pt

Segurança – www.cert.pt

ANEXOS

A N E X O A

Lista de Acrónimos

ADSL – Asymmetrical Digital Subscriber Loop.
CAD – Computer Aided Design.
CD – Compact Disk.
CPU – Central Processing Unit.
CRT – Cathode Ray Tube.
DNS – Domain Name System.
DVD – Digital Versatile Disk.
GB – Giga Byte.
HTML – HyperText Markup Language.
HTTP – HyperText Tranfer Protocol.
IEEE – Institute of Electrical and Electronic Engineers.
IMAP – IIII Message Access Protocol.
IP – Internet Protocol.
IPv4 – Internet Protocol version 4.
IPv6 – Internet Protocol version 6.
ISM – Industrial, Scientific, Medical.
LAN – Local Area Network.
MAN – Metropolitan Area Network.
MB – Mega Byte.
Mbps – Mega bits per second.
PC – Personal Computer.
PDA – Personal Digital Assistant.
POP – Post Office Protocol.
POS – Point-of-Sale.
SCSI – Small Computer System Interface.
SIG – Sistema de Informação Geográfica.
SMTP – Simple Mail Transfer Protocol.
SNMP – Simple Network Management Protocol.
TCP – Transmission Control Protocol.
TFT – Thin Film Transistor.
UDP – User Datagram Protocol.
VPN – Virtual Private Network.
WAN – Wide Area Network.
WIFI – Wireless Fidelity.
WWW – World Wide Web.

Í N D I C E