Aula nº 2 - Higiene e Segurança

Sumário:

1. Cuidados com o equipamento informático

Todo o equipamento informático é frágil e possui normas de utilização:

Portátil: saco de protecção almofadado para o transporte; cuidado com o écran de cristais líquidos (LCD) - não dobrar demasiado, limpar com pano de flanela húmido (não molhado), não fechar o écran com coisas (e.g. caneta) pousada no teclado; nunca devemos desligar o portátil sem fazer *shutdown* porque existem acções pendentes que podem levar à perda de informação - quando o computador "encrava" (bloqueia) devemos pressionar uma única vez as teclas CTRL+ALT+DEL e esperar que apareça uma caixa de diálogo que nos permite terminar a execução do programa que "encravou" o computador; devemos fazer uma manutenção periódica do disco duro do portátil, ou seja, devemos eliminar (apagar) os ficheiros e/ou aplicações que já não utilizamos (libertando assim mais espaço de disco necessário para outras aplicações) e devemos proceder também periodicamente à desfragmentação do disco para melhorar o seu desempenho e diminuir a possibilidade de erros.

Bateria: devemos carregar a bateria até ao máximo na primeira vez que a utilizamos e devemos evitar descargas acentuadas da bateria, aumentando assim a sua longevidade; a descarga da bateria depende da luminosidade do écran, do número de acessos aos disco e ao leitor de disquetes; periodicamente (meses) devemos efectuar uma descarga total da bateria seguida de uma carga total;

Disquetes: como em todos os suportes magnéticos devemos ter o cuidado de não os aproximar de campos magnéticos que possam apagar a informação aí armazenada; as disquetes são frágeis e devem ser transportadas numa caixa dura juntamente com o portátil num saco almofadado; não devemos tocar na película magnética das disquetes; não devemos expor as disquetes ao sol nem à água.

2. Cópias de segurança

Devemos ter sempre consciência da vulnerabilidade dos sistemas informáticos contra falhas de hardware, falhas de software, vírus informáticos, assim como de falhas humanas de utilização. Assim sendo, devemos fazer sempre cópias de segurança - **backups** - dos programas de software (são permitidas cópias de software como arquivos de reserva) e de trabalhos e/ou relatórios. Devemos travar (abrir a patilha de segurança) das disquetes originais que têm os programas e os trabalhos efectuados.

Também devemos possuir sempre uma disquete de arranque e se possível com um programa anti-vírus, ou seja, uma disquete com sistema operativo que nos permita arrancar com o computador e solucionar os problemas se alguma coisa acontecer ao disco ou se o computador estiver com problemas de vírus.

3. Vírus informáticos

Os vírus informáticos são programas em geral muito pequenos, que se podem acoplar automaticamente a outros programas e que efectuam acções desagradáveis nos nossos computadores - "*estragam*" (alteram) ou "*destruem*" (apagam) a informação e os programas. São programas feitos com o intuito de prejudicar o nosso computador (dados e programas) e que têm a particularidade de se autocopiarem (efeito reprodutor), ou seja, os vírus copiam-se a si próprios para o disco ou acoplam-se a outros programas e são executados de forma incógnita (e.g. apagam trabalhos e programas; formatam os disco

apagando toda a informação). Os vírus propagam-se/transmitem-se através de acções de cópia ou execução de programas "infectados".

Para evitar os vírus devemos instalar e manter actualizado no nosso computador um escudo anti-vírus recente, evitar emprestar e trocar programas (e.g. jogos) com os colegas; se o fizermos devemos proteger as disquetes contra escrita (abrir a patilha de segurança da disquete) e passá-las por um programa anti-vírus sempre que as emprestarmos. Existem diferentes tipos de vírus:

- **Vírus residentes**: são vírus que estão em memória (correm quando se liga o computador) e se autocopiam para ficheiros executáveis (*.exe) antes de qualquer programa correr (ser executado);
- **Vírus não residentes**: são vírus que não estão em memória e só podem copiar-se na altura em que corremos (executamos) um programa infectado;
- **Vírus de Boot**: no sector de arranque (sector 0) do disco duro ou da disquete há um programa que é executado quando o computador arranca; este programa carrega o sistema operativo para a RAM. Os vírus de Boot autocopiam para este sector 0 e quando o sistema arranca o primeiro programa a ser executado é o vírus mesmo antes do sistema operativo. Este vírus também se autocopiam para o sector 0 das disquetes se não estiverem travadas.

Devido aos efeitos nefastos resultantes das acções destes pequenos "diabretes" temos que tomar os devidos cuidados para evitar a contaminação (proteger o computador com um anti-vírus e travar as disquetes) e manter cópias de segurança de toda a informação que temos no disco do computador (trabalhos e programas).

4. Licenças de software

Os programas de computador, designados por aplicações de ***software*** (programas vendidos juntamente com uma licença de utilização e com um número limitado de instalações), caracterizam-se pelo tipo de utilização que os seus fabricantes permitem. Existem no entanto outros tipos de programas: ***freeware*** (programas de acesso e utilização grátis), ***shareware*** (programas de acesso grátis mas para serem utilizados durante um período curto bem determinado, com o objectivo de testar o programa; estas versões dos programas designadas por *demos* (demonstrações) possuem por vezes muitas das suas características bloqueadas).

Todos as aplicações comerciais de software são vendidas com um número limitado de instalações e uma **licença** de utilização que oferece algumas vantagens como por exemplo a recepção de novas versões (com alterações significativas) ou de versões actualizas (com alterações pontuais) do software. A utilização de instalações não licenciadas são passíveis de **acção judicial**.