Working Paper nº 9

Segurança Informática
A Perspectiva da NATO

Alberto Mesquita

Working Paper nº9

ISSN: 0872 - 895X

Depósito Legal nº: 84532/94

Setembro 1994

Trabalho apresentado no âmbito do Mestrado em Estatística e Gestão de Informação, ano lectivo de 1993/94, na disciplina de Gestão de Informação.

Resumo

O problema da Segurança da Informação em ambientes informatizados tem vindo a crescer significativamente. Porém, verifica-se existirem diferentes perspectivas e abordagens à questão da Segurança Informática, raramente concordantes, nem mesmo no essencial, verificando-se alguma dificuldade em estabelecer um conjunto de pressupostos teóricos que permitam estruturar a análise da realidade.

Estas questões, preocupam os organismos ligados à Defesa, nomeadamente no âmbito da NATO, que tem vindo a divulgar uma série de documentos, não classificados, relativamente à sua perspectiva sobre o assunto, enunciando requisitos de segurança com vista a estabelecer padrões de orientação para os construtores de hardware e software de modo a que, após certificação, possam vir a ser usados militarmente. Esses requisitos constituem um referencial teórico, abstracto e organizado que pode servir de modelo aos desenvolvimentos práticos na área da Segurança das Tecnologias da Informação.
Esse modelo tem, no entanto, tido muito pouca divulgação no ambiente informático em geral, dificultada pelo grau de abstracção em que o problema é colocado, bem como pela terminologia utilizada.

Assim, os objectivos deste trabalho são os seguintes :
- divulgar a abordagem da NATO ao problema da Segurança Informática,
- fazer a ligação entre o nível abstracto em que o problema é colocado e as tecnologias actualmente existentes,
- efectuar uma tradução para português, quando possível, de uma terminologia própria,
- conjugar num só trabalho, conceitos provenientes de diferentes fontes,
- contribuir com algumas perspectivas pessoais.

Palavras chave: segurança informática, defesa militar, NATO, tecnologias da informação

Abstract

The importance of Information Security in computerised environments is growing significantly. Yet, there are several approaches and points of view with regard to Computer Security, rarely agreeing with each other, even in essential aspects, which leads to some difficulty in establishing a series of theoretical considerations which would allow a structured analysis of the reality.

This is a matter of concern for the Departments of Defence, specifically within NATO, which has been publishing some non classified documents containing its perspective on this issue, identifying security criteria that should be taken into consideration as guidelines by hardware and software developers so that their products can be used, after certification, in military establishments. These criteria establish a theoretical, abstract and organised reference that might serve as a model for practical developments.
Nevertheless, this model is almost unknown in the I.S. world, partly due to the level of abstraction as well as the kind of terminology used.

Thus, the objectives of this paper are as follows:
- to publish the approach of NATO to Information Security in Computerised Systems,
- to establish a link between the abstract level in which this issue is faced and existing technologies,
- where possible, to translate into Portuguese, the specific terminology used,
- to bring together items from different sources, in a single work
- to contribute some personal views.

Key words: computer security , military defence, NATO, information technology

ÍNDICE

1. INTRODUÇÃO

O tema da segurança informática tem vindo a ser, desde há já bastante tempo, objecto de discussão e análise nos diversos meios que de algum modo se encontram ligados às Tecnologias da Informação. Porém, verifica-se existirem diferentes perspectivas e abordagens ao problema, raramente concordantes, nem mesmo no essencial. Não só estão em causa diferentes sensibilidades, como existe também alguma dificuldade em estabelecer um conjunto de pressupostos teóricos que permitam estruturar a análise da realidade.

Frequentemente, evidenciam-se dificuldades em integrar conceitos como : segurança de hardware versus segurança de software, graus de credenciação de utilizadores dos sistemas informáticos, classificação de segurança de diferentes "objectos" informáticos (ficheiros, programas, dados, imagens, etc.), critérios de avaliação de risco físico e de outros tipos de risco, etc.

Este tipo dificuldades é em grande parte devido à evolução vertiginosa das Tecnologias da Informação, cujas transformações permanentes dificultam uma análise global de todas as suas implicações, nomeadamente no que diz respeito à segurança da informação que flui nesse ambiente. Enquanto que, no que diz respeito à informação residente em papel, se foi acumulando uma larga experiência, de séculos, quanto à forma de tratar a informação classificada, o mesmo não se passa quando essa mesma informação se encontra em suporte informático. Existe uma longa tradição de manuseamento de informação classificada, suportada por legislação nacional que refere pormenorizadamente, todos as questões a considerar sobre este assunto. O mesmo não se verifica em relação à que trata da segurança informática em computadores, legislação esta que embora forneça algumas orientações importantes, se encontra desajustada da actual realidade.

Este tipo de questões, tem vindo naturalmente a preocupar os organismos ligados à Defesa, nomeadamente no âmbito da NATO. Assim, nos últimos anos tem sido divulgada uma série de documentos, não classificados, relativamente à sua perspectiva sobre o assunto. Face às inúmeras dificuldades em tornar um sistema informático efectivamente seguro, a informação militar classificada tem, por via de regra, dificuldade em ser informatizada. O tipo de requisitos que seriam necessários para manter os níveis de segurança conseguidos relativamente a suportes tradicionais (papel, desenhos, fotografias, etc.), são de tal modo exigentes, que não existe actualmente qualquer sistema informático comercializado que os suporte na totalidade. Nesse sentido, a NATO tem vindo a divulgar esses mesmos requisitos com vista a estabelecer padrões de orientação para os construtores e que após certificação, poderão vir a ser usados militarmente.

Esta divulgação que a NATO tem vindo a fazer, apresenta porém algumas questões que importa considerar. Por um lado, apesar de os documentos não serem classificados, acabam por ter uma difusão restrita. Embora os grandes construtores estejam totalmente a par deste assunto e os seus produtos tenham vindo crescentemente a incorporar os requisitos propostos pela NATO, esta abordagem é muito pouco divulgada no ambiente informático em geral. Por outro lado, o grau de abstracção em que o problema é colocado, bem como a terminologia utilizada, dificultam bastante a sua divulgação. Tal facto é uma consequência do objectivo de colocar esses requisitos de segurança relativamente independentes da tecnologia actualmente disponível pois caso contrário teriam que ser constantemente revistos ou condicionariam o desenvolvimento de novas tecnologias.

Assim, os objectivos deste trabalho são os seguintes :

- divulgar a abordagem da NATO ao problema da segurança informática,

- fazer a ligação entre o nível abstracto em que o problema é colocado e as tecnologias actualmente existentes e a legislação portuguesa sobre este assunto,

- efectuar uma tradução para português, tão correcta quanto possível, e quando possível (por vezes existem termos que não convém traduzir), de uma terminologia específica e pouco divulgada,

- conjugar num só trabalho, conceitos provenientes de diferentes fontes não classificadas,

- contribuir com algumas perspectivas pessoais.

2. DESCRIÇÃO DA SITUAÇÃO ACTUAL

2.1 Panorâmica Geral

A segurança da informação foi até ao aparecimento dos computadores um problema importante, mas de solução relativamente simples. A flexibilidade e accessibilidade que são, em geral, características desejáveis de um sistema informático são porém, inimigas da segurança. No passado, as pessoas ou empresas limitavam-se em proteger fisicamente os objectos (papeis, fotografias, etc.) que consideravam sensíveis. Não havia pois, necessidade de abordar este problema de uma forma estruturada e formal em parte devido também ao facto de , exceptuando a perspectiva nacional ou governamental, o fluxo deste tipo de informação se encontrar restringido ao ambiente da própria pessoa ou empresa. O advento dos computadores acrescentou toda uma nova dimensão ao problema.

Poder-se-á até prever que, num futuro próximo, o problema da segurança da informação em ambientes informatizados se venha a pôr com mais veemência. À medida que mais pessoas vão possuindo maior "know-how" informático, que os sistemas de informação envelhecerem e que mais informação vital venha a ser armazenada informaticamente, maior será o número de casos divulgados de fuga de informação e menor será a credibilidade desses sistemas. Muitos são já os casos conhecidos deste tipo, mas o seu conjunto não assumiu ainda a dimensão de um verdadeiro problema que preocupe realmente as chefias da maioria das organizações.

Quando tal vier a acontecer, será naturalmente desejável que exista um referencial teórico, abstracto e organizado que dê suporte aos desenvolvimentos práticos de todos quantos estão envolvidos no crescimento das tecnologias da informação. Tentemos pois, enunciar algumas questões às quais seria conveniente poder dar uma resposta, tanto quanto possível, concreta :

- Quão seguro é um determinado equipamento informático e de que modo este se integra num sistema informático mais global, em termos de segurança ?

- Qual o nível de segurança que uma determinada organização deve exigir do seu sistema informático face à realidade específica em que opera, considerando a importância da informação que possui, do tipo de pessoas que aí trabalham, da sua disponibilidade financeira, etc. ?

- Quais os requisitos de segurança que os construtores de hardware e software devem cumprir para que os sistemas que produzem possam ser classificados em termos do nível de segurança que apresentam ?

- Como avaliar o nível de segurança de um sistema já instalado, quais os seus pontos fracos e quais as medidas a tomar ?

Naturalmente que será pouco provável que se venha a encontrar um modelo perfeito que responda a todas estas questões. A realidade é sempre bastante mais complexa do que as ferramentas de que poderemos vir a dispôr para a analisar no entanto, seria pelo menos conveniente que existisse uma linguagem comum entre os diversos intervenientes e uma ou pelo menos um número restrito de metodologias de abordagem ao problema.

Convém também ter presente a distinção entre dois diferentes cenários relativamente à forma como o problema da segurança da informação, numa perspectiva genérica, é colocado. Pondo de momento de lado, as questões específicas como por exemplo, o segredo de justiça, o segredo profissional ou segredo militar, torna-se possível distinguir a perspectiva da segurança de um ponto de vista nacional, da segurança de um ponto de vista pessoal ou empresarial.

Uma primeira fonte que poderia constituir um referencial para quem de algum modo está relacionado com este tipo de questões, poderia ser a legislação existente. Porém, a situação mais natural é a de esperar que esta questão se desenvolva em duas principais vertentes, distintas mas interligadas : por uma lado uma abordagem académica e teórica ao problema da segurança informática e por outro, uma produção comercial em termos de hardware, software e serviços.

2.2 A Legislação

Conforme referido, torna-se de certo modo legítimo, esperar que o pacote de legislação existente, cumpra a missão de simultaneamente constituir uma base doutrinária e pragmática para o problema da segurança em geral, e da segurança informática em particular. Pode-se considerar que a legislação nacional, constitui uma abordagem mais ou menos genérica e integrada ao problema da segurança da informação numa perspectiva nacional, assumindo a forma de uma série de normas, instruções e recomendações, nalguns casos um pouco vagas, noutras didácticas, noutras ainda, bastante concretas e bem explicitadas. Porém isto só é verdade para a informação residente nos suportes tradicionais (papel, fotografias, etc.).

O SEGNAC 1 contém "Instruções para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas" relativamente às matérias classificadas de âmbito governamental com vista a combater acções de sabotagem e espionagem e a evitar falhas humanas susceptíveis de ocasionar comprometimentos e quebras de segurança. O SEGNAC 2, contém igualmente um conjunto de normas e instruções, mas desta vez relativas à segurança industrial, tecnológica e de investigação, igualmente numa perspectiva nacional mas em que as empresas são igualmente consideradas como tendo responsabilidades nesta matéria. O SEGNAC 3 refere-se especificamente à segurança das telecomunicações de uma forma global e finalmente o SEGNAC 4 trata da segurança informática e assentando em grande parte, nas linhas gerais definidas pelos SEGNAC 1 e 2.

Poder-se-ia afirmar que caso os computadores não existissem, os SEGNAC's 1 e 2 constituiriam uma base sólida e funcional quer em termos teóricos quer em termos práticos para as questões da segurança da informação. Com certeza que a sua adaptação a situações específicas, nomeadamente ao ambiente empresarial, careceria de uma análise concreta dessas mesmas especificidades, mas o problema encontrava-se à partida, controlado.

No SEGNAC 3 não é feita qualquer referência ao ambiente informático. Quanto ao SEGNAC 4, constitui uma referência obrigatória sobre o tema da segurança informática, contendo um conjunto alargado de definições e procedimentos. Embora apresente alguns conceitos muito úteis e até didácticos, não satisfaz as questões acima enunciadas. A título de exemplo : distingue entre programas e dados, referindo um conjunto de técnicas de classificação de programas, mas não o faz para os dados nem refere sequer a intervenção nesse processo, dos sistemas de gestão de bases de dados ou dos sistemas operativos.

Relativamente à legislação comunitária, já a situação é diferente. O assunto tem vindo a ser alvo de uma atenção crescente e em Fevereiro deste ano foi publicado o "Livro Verde sobre a Segurança dos Sistemas de Informação", Proposta da Comissão Europeia de Fevereiro de 94, existindo ainda duas outras referências obrigatórias nomeadamente, o "Information Technology Security Criteria", ITSEC, de Junho de 91 e o "Information Technology Security Evaluation Manual", ITSAM, de Setembro de 93. Seria de todo o interesse analisar exaustivamente a perspectiva comunitária sobre a segurança informática, mas tal encontra-se fora do âmbito deste trabalho.

Conforme referido, para além das fontes legislativas, surge a tendência para encarar o problema da Segurança Informática segundo duas outras vertentes : uma abordagem académica e outra em função dos sistemas comerciais (hardware e software) existentes.

2.3. Abordagem Teórica

Por razões que não valerá a pena desenvolver muito, a segurança informática não tem sido uma questão muito privilegiada pelas pessoas de algum modo ligadas à investigação científica. Talvez por ser uma área que embora se encontre nitidamente dentro do âmbito científico e tecnológico, exija uma metodologia de abordagem teórica, mais próxima da utilizada pelas Ciências Sociais. Trata-se de encarar uma questão, de certo modo abstracta, sem números, fórmulas ou equipamentos de medição, mas para a qual os investigadores das Ciências Sociais não se encontram motivadas por possuir uma forte componente tecnológica. O tema encontra-se, de facto, interligado com diferentes áreas, nomeadamente as da Organização e Planeamento, a da Gestão dos Recursos Humanos, a da Engenharia de Software, a do Hardware e da Electrónica e outras.

O ambiente universitário, não é também um meio onde a segurança da informação assuma um papel vital. No dia-a-dia de uma Universidade, não se faz sentir grandemente a necessidade de manter especialmente segura a informação que aí circula. As eventuais fugas de informação não se traduzem directamente em perdas financeiras ou de posição face à concorrência, antes pelo contrário, quanto maior for a difusão da informação, maior será a produção científica. Esta será possivelmente uma outra razão para um um certo alheamento relativamente a estas questões.

As intervenções científicas sobre este assunto têm sido efectuadas mais numa perspectiva concreta dos equipamentos, do software, dos algoritmos criptográficos, ou ainda dos modelos de avaliação do risco físico ou de medidas concretas a tomar em determinadas situações específicas. Raramente se tentam integrar os diferentes subsistemas que constituem o problema global. A literatura existente por sua vez, sofre, por vezes, de uma problema muito comum em informática : ao fim de 2 ou 3 anos torna-se obsoleta. Não só não tem, evidentemente, em consideração as especificidades dos novos sistemas que vão surgindo como principalmente, não fornece uma estrutura de raciocínio que as permita analisar.

Assim, das abordagens teóricas conhecidas, nenhuma conseguiu ser globalmente aceite ou sequer, alcançar uma posição de destaque. Recentemente têm surgido algumas novidades. As referências ao tema têm vindo a aumentar e nalguns casos são propostos modelos de análise de âmbito um pouco mais vasto.

2.4. Abordagem Comercial

Conforme referido anteriormente, a segurança informática tem sido uma questão eminente prática pelo que em termos gerais se pode afirmar que existe um sem número de diferentes produtos e serviços, cada um encarando o problema de uma forma particular. Convém por isso começar por distinguir entre produtos e serviços e dentro dos produtos, os principais "ambientes" : Mainframes, Sistemas UNIX, redes locais Novell e DOS/Windows em Pc's isolados. Esta divisão pode ser muito questionável, mas parece ser apropriada dentro deste contexto. Além disso, serão referências obrigatoriamente superficiais embora exista campo para grande desenvolvimento mas que não está no âmbito deste trabalho, servindo apenas como ilustração da enorme diversidade e consequente necessidade de estruturação.

Comecemos pelo ambiente de mainframes. É neste ambiente que tradicionalmente, mais se faz sentir o problema da segurança informática. Quer em termos nacionais quer a nível mundial e apesar de uma tendência constante para o "downsizing", os mainframes estão omnipresentes nas grandes empresas coexistindo com ligações periféricas a sistemas de menor porte encontrando-se geralmente a informação vital, dita "corporativa", nesses mainframes. Por outro lado, dá-se o facto de as grandes companhias, incluindo as administracões públicas, serem precisamente aquelas cujo prejuízo (em sentido lato) é maior em caso de acidentes em matéria de segurança informática. Os grandes bancos, companhias de seguros e outras empresas, em especial as que estão espalhadas por uma grande diversidade geográfica, são as

que de mais perto sentem esta preocupação e por isso, as que maiores investimentos estão dispostos a fazer e consequentemente, é este o ambiente em que existe uma melhor oferta de produtos e serviços.

Quanto aos sistemas operativos que aí operam, possuem diferentes predisposições para a implementação de sistemas de segurança uma vez que as suas diferenças estruturais são significativas. A título de exemplo : enquanto que no sistema operativo MVS da IBM os utilizadores utilizam uma mesma aplicação carregada apenas uma vez em memória, em VM cada utilizador possui uma máquina virtual carregando em memória a aplicação que utiliza independentemente de outro utilizador a estar ou não a usar simultaneamente. Qualquer um destes sistemas operativos, é geralmente considerado bastante robusto, incorporando desde logo na sua versão de base, susbsistemas de segurança relativamente potentes.

Em termos de segurança física e de organização existe nestes ambientes como que uma "escola", com evidentes repercussões positivas. Os diferentes intervenientes no funcionamento do sistema informático encontram-se geográfica e funcionalmente separados e os procedimentos de organização geralmente bem definidos.

Em termos de software, quer os programas-produto (SGBD's, Linguagens, etc.) quer as aplicações, apresentam um conjunto relativamente vasto de ferramentas na área da segurança. Existem sistemas de criptografia e softwares de segurança bastante sofisticados. De entre estes, merece especial relevância o RACF como sendo o produto que mais extensamente implementa os requisitos do modelo NATO que adiante será descrito.

O ambiente UNIX, frequentemente associado a instalações de média dimensão, apresenta grandes diferenças em relação ao anterior. O facto de ser um sistema aberto, não proprietário e bem conhecido de muitos programadores, contém em si próprio o dilema da segurança ou seja, flexibilidade versus segurança. Tal como anteriormente referido, o facto de este ambiente estar ligado em termos gerais a instalações de dimensão mais reduzida e cujo valor médio da informação é menor, o panorama geral é mais preocupante e o assunto nem sequer é muito abordado. Apesar de existir um grande número de softwares de segurança disponíveis no mercado, o problema põe-se logo ao nível do próprio sistema operativo que apresenta fraquezas relativamente a ameaças por parte de utilizadores, programadores de sistema e vírus de proveniência externa.

A questão mais relevante no entanto, relativamente à inexistência de uma filosofia global de segurança está relacionada com o facto de não ser um sistema proprietário. Assim, este sistema apresenta um grande número especificidades de acordo com cada uma das versões em que é comercializado (Unix, Ultrix, Aix, Xenix). Essas especificidades assumem maiores proporções no que diz respeito à administração do sistema, que é precisamente a área que mais está relacionada com a sua segurança. É pois um ambiente, em termos de segurança, com pontos fracos de origem e grande heterogeneidade.

Quanto às redes locais Novell, é frequente ouvirem-se opiniões muito diversas. Tal facto deve-se provavelmente à disparidade dos termos de comparação. Tomando como referência Pc's isolados ou outros softwares de redes locais ou mesmo o ambiente UNIX, o Netware 3.11, e com certeza que também o 4.0 (com o qual o autor não se encontra familiarizado), são bastante seguras. A robustez e segurança deste software constituem até uma das suas bandeiras. Quando comparados porém com o ambiente de mainframes IBM por exemplo, os problemas são semelhantes aqueles que foram referidos para o ambiente UNIX, com excepção do que resulta de serem comercializados exclusivamente pela Novell. Independentemente de serem ou não seguras, há que referir no entanto, que a filosofia que presidiu ao seu desenvolvimento, ou não se encontra bem definida, ou pelo menos não tem sido apropriadamente divulgada.

Quanto aos microcomputadores a operar em stand-alone correndo DOS, com ou sem Windows, o problema põe-se muito claramente. Ou bem que o Pc se encontra num local fisicamente protegido e atribuído a uma única pessoa, obviamente com direito a aceder a toda a informação que nele está contida, ou então a segurança simplesmente não existe, qualquer que seja o padrão de referência. O DOS com ou sem Windows, não só não apresentam nenhuma filosofia de segurança, como não permitem implementar quaisquer medidas de protecção eficazes. Mesmo na situação descrita, em que o Pc se encontra fisicamente protegido, a utilização por mais do que um utilizador, ainda que estejam todos autorizados a aceder à informação, verificam-se problemas de segurança pela dificuldade em implementar os requisitos mínimos definidos pelo modelo NATO, como se verá.

Após uma referência genérica, se bem que superficial, sobre os diferentes produtos/ambientes, resta fazer uma análise da mesma natureza sobre a oferta de serviços na área da Segurança Informática. Assim, poder-se-ia pôr a hipótese de que apesar da grande diversidade de produtos e sistemas de segurança existentes, fosse possível encontrar empresas prestadoras de serviços, tipicamente empresas de consultoria, que dispusessem de metodologias e técnicas que dessem resposta às grandes questões enunciadas anteriormente. Tal não é porém o caso, uma vez que este tipo de empresas tem uma perspectiva eminentemente comercial sobre o assunto e conforme foi já referido, a procura deste tipo de serviço não é, actualmente, suficientemente significativa por forma a despoletar uma abordagem genérica e integrada ao problema. A procura que existe é muito específica, geralmente grandes empresas como por exemplo, bancos. Para esse tipo de situações existem de facto empresas disponíveis mas que não só se fazem pagar excelentemente pelo serviço personalizado que prestam, como não têm qualquer interesse, antes pelo contrário, em divulgar as metodologias que utilizam.

3. O MODELO NATO

O tema da Segurança em termos gerais é, naturalmente, uma preocupação das Forças Armadas e dos Organismos ligados à Defesa, desde longa data. Existe uma vasta experiência acumulada durante muitos anos, sendo especialmente relevantes aqueles que se referem ao período da Guerra Fria em que este assunto assumia um carácter relevante. Assim, foi-se desenvolvendo uma filosofia global bem como uma "Escola", que se traduz numa vastíssima literatura sobre o assunto, sendo no entanto de referir que, neste trabalho, se entra em linha de conta apenas estritamente com informação que pode ser obtida em documentos não classificados.

Fazendo Portugal parte da NATO desde a sua origem, é também público que o seu conceito de Defesa tem que ser entendido não apenas numa perspectiva nacional mas também, profundamente articulada com a da NATO. Assim, em matérias que não digam especificamente respeito a Portugal, torna-se obrigatório efectuar uma referência permanente aos conceitos e procedimentos utilizados nesse ambiente. O tema da segurança informática é tipicamente um desses assuntos.

Embora o tema em causa seja o da segurança informática, esta não se pode dissociar do âmbito mais vasto que é a Segurança em geral. Tal como anteriormente referido em relação à legislação nacional em que o SEGNAC 4 assenta em conceitos definidos nos SEGNAC 1 e 2, também os documentos NATO relativos a questões informáticas, assentam em conceitos definidos noutras publicações, desde documentos oficiais até artigos publicados numa grande diversidade de revistas da especialidade. Essa enorme quantidade de referências bibliográficas existente não será especificada por ser excessivamente longa.

Assim, a principal referência será a chamada "Rainbow Series" ou "Série Arco-Íris" bem como uma série de outros documentos que lhe estão associados, geralmente sobre a forma de auxiliares de interpretação. Esta série de publicações que inclui os vulgarmente designados "Nato Orange Book", "Nato Red Book" e "Nato Yellow Book" e ainda, o "Nato Light Blue Book" constitui um conjunto bem integrado de conceitos e filosofias de acção mas em que o primeiro assume uma posição de relevo. Para além da estrutura fundamental que irá ser apresentada, a "Rainbow Series" bem como uma série de outros documentos dispersos, abordam um grande número de questões concretas que incluem conceitos sobre criptografia, sistemas de identificação sofisticados (reconhecimento de impressões digitais ou de voz, smart cards, etc) reflexões com cariz pragmático sobre sistemas existentes, formas de implementação da estrutura teórica, etc..

A estrutura dos capítulos seguintes porém, é estritamente pessoal e corresponde certamente em muitos casos a uma visão personalizada do assunto, em grande parte motivada pela necessidade de tornar o tema mais simples. Por outro lado essa estrutura será também afectada pelo facto de estarmos interessados apenas no que diz respeito à segurança informática. Tendo permanentemente em consideração este facto, irão ser analisados os principais items em questão, tentando conferir uma certa coerência ao esquema global.

3.1. A Classificação

A primeira noção a ter em conta é a de que todos os objectos em sentido lato devem ser passíveis de serem classificados. Embora este conceito pareça extremamente simples, irá constituir uma questão central de toda a análise. Comecemos por definir "objectos" e "classificação".

Por objectos entende-se naturalmente, papéis, documentos, fotografias, quadros, etc., mas não só. Num ambiente informático, este conceito pode e deve ser amplamente alargado na medida em que diferentes objectos informáticos embora semelhantes, têm implicações muito diferentes em termos de segurança. Em termos de software podem-se distinguir os seguintes :

- Ficheiro contendo o código-fonte de um programa,
- Ficheiro contendo dados em claro,
- Sistema de Gestão de uma Base de Dados em que os dados não são facilmente separáveis de outros blocos de software que operam sobre esses dados,
- Programa compilado,
- Ficheiro fazendo parte de um sistema operativo ou de programas-produto

e outros. Sai deste âmbito o aprofundamento das suas especificidades servindo apenas para evidenciar a grande diversidade de situações possíveis o que permite antever alguns dos problemas que surgem.

Relativamente ao hardware o problema não se põe da mesma forma uma vez que este ocupa uma localização geográfica concreta.

Quanto à classificação existem, como referência fundamental, as seguintes divisões :

- Não Classificado
- Reservado
- Confidencial
- Secreto
- Muito Secreto

Para além destas divisões, utilizadas também em termos nacionais, não ligadas à Defesa, existe ainda uma série de variantes que não valerá a pena considerar.

Surge desde logo a questão de como entender esta classificação em termos mais pessoais ou empresariais. Desde a conversão numa escala de "Valor da Informação" de 1, 2, 3, etc. até outras mais elaboradas, todas elas se devem adaptar ao ambiente para que são criadas e não constituem um facto relevante para a estrutura global. Pode no entanto referir-se um sistema de classificação que pode tornar-se útil num meio empresarial, a título de exemplo :

Secreto - Informação considerada de natureza estratégica. A sua exposição pode causar perdas significativas para a organização, afectando a sua posição financeira e acarretando perdas de mais de 5% dos lucros totais.

Confidencial - Informação a que só deve ter acesso a administração ou gestão. Em mãos alheias pode ser prejudicial para a imagem da empresa e levar a perdas de 1 a 5% do total de lucros.

Reservado - Informação respeitante a negócios que não deve ser do conhecimento de pessoas estranhas à organização. É informação relativa à ética empresarial, privacidade individual, etc..

Não classificado - Toda a restante informação.

3.2. Pessoas e Credenciação

Curiosamente, um dos aspectos que tem vindo recentemente a aparecer com alguma intensidade, é o da importância das "Pessoas" num sistema global de segurança. O título de um artigo recentemente publicado numa revista da especialidade é o seguinte : "Information systems security isn't a computer problem, it is a people problem". Nos ambientes ligados à Defesa, este é um aspecto absolutamente essencial. Um sistema informático por mais seguro que seja, fica totalmente comprometido se as pessoas autorizadas a aceder à informação não oferecerem a adequada credibilidade.

Nesse sentido, existe em termos nacionais e não apenas da Defesa, a Autoridade Nacional de Segurança, cujas funções são, entre outras, as de avaliar com rigor, da seriedade, credibilidade, em termos gerais, do grau de credenciação que pode ser atribuído a um determinado indivíduo. Existe um processo individual, com necessidade de renovação periódica, onde consta informação considerada relevante para essa avaliação. Uma vez analisado esse processo individual, é atribuído a esse mesmo indivíduo uma credenciação correspondente a um determinado grau de classificação. Por exemplo : Sr. António Silva, credenciado "Secreto".

Em termos empresariais, a conversão é imediata. Por exemplo : O Director-Geral ou Administração, atribuem a cada funcionário um grau de credenciação de

acordo com a escala de classificação que escolheram e segundo critérios de confiança que entenderam.

Esta credenciação implica que, **um indivíduo credenciado num determinado grau só pode ter acesso a objectos classificados com grau igual ou inferior ao que lhe foi atribuído.**

3.3 Need-to-know

Um princípio fundamental da Segurança é o bem conhecido conceito de Need-to-know. Torna-se fundamental referi-lo explicitamente uma vez que será um elemento determinante na avaliação de um sistema informático, face à possibilidade ou não de o implementar.

Consiste em estabelecer que o facto de um indivíduo estar credenciado para aceder a informação classificada, não lhe dá o direito, por princípio, de efectivamente tomar conhecimento de toda ela, mas tão-somente daquela que necessitar para o exercício das suas funções.

Para que se possa aferir a importância deste conceito quando aplicado à segurança informática, pode imaginar-se a dificuldade de um determinado software de segurança não só controlar o acesso de um indivíduo a determinada informação em função do seu grau de credenciação mas também, entrando em conta com a classificação concreta de um determinado objecto específico e da sua necessidade em o conhecer.

3.4. Grau de Risco

Conforme anteriormente referido, é posta uma grande ênfase nas pessoas, considerando-as como o principal factor crítico no que diz respeito à segurança informática. Assim, uma das principais características que este modelo apresenta, reside na convicção de que **o nível de segurança que um sistema informático deve possuir, está directamente dependente da disparidade que possa existir entre o grau de credenciação das pessoas que nele operam e o grau de classificação dos objectos que contém**. Tal não significa que não possam coexistir, mas sim que quanto maior for a sua diferença maior serão os requisitos de segurança exigidos. A determinação concreta desse grau de risco segue um conjunto de regras com uma série de pormenores mas que dá basicamente origem a umas tabelas que serão adiante exibidas.

Porém, torna-se necessário começar por fazer uma distinção importante entre um "Sistema Aberto" e um "Sistema Fechado". De referir que estes conceitos não correspondem aos vulgarmente utilizados em informática.

Sistema Fechado - Um sistema fechado caracteriza-se por se verificarem simultaneamente as seguintes duas condições : 1ª - Os programadores de aplicações bem como os encarregados da sua manutenção estão devidamente credenciados, ao nível da classificação máxima da informação residente nesse sistema, pelo que é assumido de que não existe o risco de introduzirem nesse sistema, software corrupto ou corrompido ("malicious logic"). 2ª - As aplicações que correm nesse sistema estão protegidas, elas próprias, quanto à possibilidade de o sistema operativo ou outro software de base as poder corromper.

Sistema Aberto - Um sistema aberto existe, quando qualquer uma das duas condições se verifique : 1ª - Os programadores de aplicações e os encarregados da sua manutenção não estão devidamente credenciados. 2ª - As aplicações não estão protegidas quanto à possibilidade de virem a ser corrompidas pelo sistema operativo ou pelo software de base.

Os quadros que irão ser apresentados em seguida são uma adaptação dos originais retirando alguns pormenores dispensáveis para a compreensão do seu princípio de funcionamento.

MATRIZ DE SEGURANÇA PARA SISTEMAS FECHADOS

	Máximo Grau de Classificação da Informação				
	NCLAS	RESERV	CONF	SECRETO	MTOSEC
NCLAS	C1	B1	B2	B2	A1
RESERV	C1	C2	B1	B2	B3
CONF	C1	C2	C2	B1	B2
SECRETO	C1	C2	C2	C2	B2
MTOSEC	C1	C2	C2	C2	C2
Credenciação Mínima dos Utilizadores					

MATRIZ DE SEGURANÇA PARA SISTEMAS ABERTOS

	Máximo Grau de Classificação da Informação				
	NCLAS	RESERV	CONF	SECRETO	MTOSEC
NCLAS	C1	B1	B2	B3	*
RESERV	C1	C2	B2	B2	A1
CONF	C1	C2	C2	B1	B3
SECRETO	C1	C2	C2	C2	B2
MTOSEC	C1	C2	C2	C2	C2
Credenciação Mínima dos Utilizadores					

Conforme se pode constatar da análise destes dois quadros, **do cruzamento entre o valor máximo da informação residente no sistema com a credenciação mínima dos seus utilizadores, resulta um conjunto de "Classes" que se caracterizarão por uma série de requisitos que os sistemas informáticos deverão possuir para que possam ser considerados seguros.**

Na realidade, por trás destes quadros estão cálculos de índices de risco que não é, neste momento, oportuno esclarecer mas que vale a pena referir apenas como justificação para o facto de este tipo de quadros poderem ser alterados por forma a incluírem outros critérios de risco.

Os asterisco significa que face ao estado actual da tecnologia não se torna possível definir requisitos para um sistema com tão elevado grau de vulnerabilidade.

3.5 As "Classes"

Da análise dos quadros anteriores surge imediatamente a necessidade de caracterização das Classes enunciadas. Antes porém, convém referir que esta é a parte mais complexa de todo o modelo, em que se torna imprescindível definir uma terminologia própria, bem como introduzir alguns conceitos fora do vulgar, num contexto em que pequenas diferenças nessa terminologia podem significar conceitos significativamente diferentes.

A descrição das diferentes Classes será extremamente resumida face a toda a informação contida nos documentos de base servindo apenas para uma compreensão global do modelo. De referir que este trabalho tem apenas fins ilustrativos e nunca poderia constituir uma base de referência para qualquer implementação prática.

As Classes formam 4 Grupos representados pelas letras A, B, C e D em que o número que se lhe encontra associado, indica que pertence a esse Grupo. A sua ordenação relativa vai de A a D em que A é o Grupo de Classes com maiores exigências em termos de requisitos de segurança e inversamente, o Grupo D o que apresenta menores requisitos de segurança. Dentro de cada Grupo, o número indica a posição relativa das diferentes classes e o menor número, o 1, refere-se à Classe que menores requisitos de segurança possui, face às Classes contendo os números que se lhe seguem. Em termos gerais, pode-se afirmar que uma determinada Classe apresenta todos os requisitos de segurança da Classe que a precede e acrescenta alguns de novo. Explicitando : A1 > B3 > B2 > B1 > C2 > C1 > D

Para que uma Classe possa ser caracterizada, foram criados 6 diferentes Requisitos de avaliação, constituindo áreas de análise que poderão ser especificadas tanto quanto venha a ser necessário, podendo os sistemas implementá-los em maior ou menor grau, permitindo deste modo distingui-las umas das outras. Embora esta seja a metodologia que os documentos NATO usam para caracterizar exaustivamente as Classes, a que aqui irá ser feita, constará apenas de um resumo dessas mesmas características. É porém importante entender esses Requisitos como elemento fundamental deste modelo.

REQUISITOS FUNDAMENTAIS DE SEGURANÇA

- **Política de Segurança** : Um sistema deve possuir uma Política de Segurança bem definida e explícita, que o próprio sistema obriga a cumprir. Os requisitos de protecção devem ser definidos em termos das ameaças, riscos e objectivos da organização que se traduzem numa adequada Política de Segurança. Considera-se normalmente que essa Política de Segurança resulta de leis, regulamentos e regras externas, independentemente do uso de um computador. Uma Política de Segurança deve ser um reflexo da Política Geral de Segurança da qual emana.

- **Marcação** : Os objectos devem possuir "rótulos" (labels) com a sua classificação de segurança, que se lhes encontram intrinsecamente associados e/ou, os modos de acesso (criar, alterar, apagar, consultar, e outros mais específicos) por parte dos potenciais utilizadores.

- **Identificação** : Os sujeitos devem poder ser individualmente identificados. Cada acesso à informação deve ser condicionado em função de quem está a aceder a essa informação e qual o seu grau de credenciação. Esta identificação e autorização devem ser mantidas de uma forma segura pelo sistema e encontrarem-se associadas com todo e qualquer elemento activo que efectue alguma acção relevante em termos de segurança nesse sistema.

- **Sistema de Auditoria** : Deve existir um sistema de auditoria que registe e mantenha a informação, de uma forma selectiva e segura, sobre as acções que afectem a segurança do sistema, de modo a que estas possam ser investigadas e reconstituídas. Um sistema seguro deve poder registar todas as ocorrências relevantes em termos de segurança. A capacidade de seleccionar os eventos a serem auditados torna-se necessária por forma a reduzir o seu peso e permitir uma análise mais eficiente. Essa informação deve ainda estar protegida de eventual modificação ou destruição não autorizada que impedisse uma investigação sobre violações de segurança.

- **Mecanismos de Segurança** : Um sistema informático deve conter um conjunto de mecanismos de hardware e de software que possam ser avaliados independentemente quanto à sua capacidade para assegurar o cumprimento dos items anteriores. Estes mecanismos estarão tipicamente englobados no âmbito do sistema

operativo e serão encarregados de cumprir as tarefas que lhes são atribuídas, podendo ser avaliados de uma forma positiva e independente através de documentação clara.

- **Protecção Contínua** : Os Mecanismos de Segurança anteriormente definidos devem ser continuamente protegidos contra intromissão (tampering) e/ou alterações não autorizadas. Nenhum sistema informático pode ser considerado verdadeiramente seguro se os mecanismos básicos de hardware e software que asseguram o cumprimento da Política de Segurança estiverem eles próprios sujeitos a modificações não autorizadas ou subversivas. A Protecção Contínua tem implicações directas ao longo de todo o ciclo de vida do sistema informático.

Torna-se igualmente útil definir o conceito de TCB em inglês, Trusted Computing Base, que se poderia traduzir por "Sistema de Segurança Informática". Trata-se de um conceito amplamente divulgado no ambiente NATO pelo que não irá ser traduzido e que se pode caracterizar como sendo :

TCB - um conjunto de mecanismos de validação que poderão ser desde um sistema operativo, até um equipamento de segurança específico ou mesmo o sistema informático em toda a sua globalidade. O TCB é pois o "coração" de um sistema informático seguro que contém todos os elementos desse sistema encarregados de suportar a Política de Segurança e a separação entre os diversos objectos (dados e programas) em que se baseia a protecção de uma forma global. As fronteiras desse TCB são designadas geralmente por "perímetro de segurança". Um TCB deve ser tão simples quanto possível e consistente com as funções que é chamado a desempenhar. Assim, um TCB inclui, normalmente, partes de hardware e de software, considerados críticos para a protecção sendo designados e implementados por forma a que todos os componentes do sistema que se encontrem fora desse perímetro de segurança, não necessitam de ser seguros nem, que lhes seja assegurada protecção. Assim, a identificação dos interfaces e dos elementos de um TCB bem como a verificação do seu correcto funcionamento, constituem as principais bases de avaliação de um qualquer sistema informático.

A diferença entre os conceitos de "**Discricionário**" e de "**Mandatório**" constitui também um elemento central deste modelo. Por Segurança Discricionária entende-se aquela que permite condicionar o acesso à informação a um indivíduo em função do conceito de need-to-know . Por Segurança Mandatória entende-se aquela que se baseia directamente na comparação entre a credenciação de um determinado indivíduo e a classificação do objecto a que pretende aceder e indirectamente, em considerações de ordem física e ambiental. São dois conceitos distintos que se podem ou não sobrepor. Nenhum deles substitui o outro e um sistema realmente seguro deve implementá-los simultaneamente. Nesse caso, para que um indivíduo acedesse a uma determinada informação, não só teria que ser considerado digno de confiança face ao objecto a que pretendia aceder (Mandatório) como também esse acesso ser necessário para o exercício das suas funções (Discricionário).

Para que se possa ficar com uma imagem mais viva de como estes conceitos se traduzem na prática imagine-se a seguinte descrição informal de um sistema que implemente medidas de segurança mandatórias e discricionárias :

O sistema começa por identificar um determinado indivíduo positivamente ou seja, tentando garantir que a pessoa que está em contacto com o sistema é efectivamente quem afirma ser. Isto é geralmente obtido a partir de um login e de uma password o que no entanto em sistemas mais seguros pode não ser suficiente. Uma vez feita a identificação, importa determinar qual o grau de credenciação que essa pessoa possui. Seguidamente, quando essa pessoa pretende aceder a uma determinada informação, há que verificar qual o grau de classificação dessa mesma informação. Caso seja igual ou inferior ao da sua credenciação, está satisfeita uma primeira condição para que esse acesso se possa vir a fazer. Porém há que verificar ainda uma outra condição : que tem necessidade de conhecer a informação que vai consultar, no âmbito das suas funções. Só caso tal se verifique, é que o acesso se pode realmente efectuar. A determinação do need-to-know pode ser também implementado através de uma password, imaginando o seguinte esquema : frequentemente as passwords de acesso a determinados objectos ou grupos de objectos (eventualmente associadas ao seu suporte físico) são obrigatoriamente mudadas e a sua divulgação não pode ser feita de forma automática aos seus habituais utilizadores. Tal obrigará a que esses utilizadores tomem a acção de obter essas passwords, altura em que é determinada a sua necessidade de conhecer a informação, não se correndo o risco de um utilizador, só porque num determinado momento necessitou de aceder a uma determinada informação, mantenha esse privilégio por tempo indefinido.

Conforme referido, irá proceder-se à descrição resumida dos diversos Grupos e Classes e que caso se optasse por uma versão mais alargada, seria feita em função dos 6 Requisitos anteriormente definidos.

Grupo D - Protecção Mínima

Este Grupo contém apenas uma Classe. Está reservado para aqueles sistemas que tenham sido avaliados mas que não tenham cumprido os requisitos exigidos a uma Classe mais elevada.

Grupo C - Protecção Discricionária

As Classes deste Grupo providenciam uma Protecção baseada numa Segurança Discricionária e num Sistema de Auditoria aos sujeitos e às acções que estes executarem.

Classe C1 : Protecção por Segurança Discricionária - O TCB de um sistema cumprindo os requisitos da Classe C1 deve cumprir os requisitos de Segurança Discricionária, providenciando a separação entre utilizadores e dados. Deve incorporar formas de controlo credíveis capazes de assegurar limitações no acesso à informação de uma forma individualizada. Essas formas de controlo devem ainda estar totalmente disponíveis por forma a permitir que os utilizadores possam proteger a sua informação, quer de natureza privada quer corporativa, evitando deste modo que outros utilizadores acidentalmente tomem conhecimento ou corrompam essa informação.

Classe C2 : Protecção por Acesso Controlado - Os sistemas desta Classe asseguram um controlo de acesso discricionário mais fino que os da Classe C1 tornando os utilizadores individualmente auditáveis nas suas acções, através de procedimentos lógicos, auditoria de eventos relevantes em termos de segurança e encapsulamento de recursos.

Grupo B - Protecção Mandatória

Um dos principais requisitos deste Grupo tem a ver com a noção de um TCB que preserva a integridade dos "rótulos" de classificação dos diferentes objectos e os utiliza para assegurar um conjunto de regras de controlo que executam uma Segurança Mandatória. Os sistemas incluídos nesta divisão transportam esse rótulos apenas juntamente com estruturas de dados de elevado nível. O construtor do sistema é quem fornece o modelo para a Política de Segurança em que o TCB se baseia e fornece igualmente as especificações para a constituição desse TCB. Tem ainda que conseguir demonstrar explicitamente que consegue implementar um mecanismo que medeie todos os acessos dos sujeitos aos objectos.

Classe B1 : Protecção Rotulada - Os sistemas da classe B1 devem suportar todos os requisitos definidos para a Classe C2. Adicionalmente, devem conter um modelo informal para a Política de Segurança, possibilidade de "rotulagem", e controlo de acesso mandatório entre objectos e sujeitos devidamente identificados.

Classe B2 : Protecção Estruturada - Nos sistemas da Classe B2, o TCB deve estar baseado num modelo de Política de Segurança formal, claramente definido e documentado que exige o cumprimento dos controlos de acesso mandatórios e discricionários tal como na classe B1 mas desta vez, extensível a todos sujeitos e objectos do sistema. O problema da intromissão através da análise das variações de campos electromagnéticos em canais de comunicações (covert channels) deve também ser considerado e apresentadas soluções. O TCB deve estar bem estruturado por forma ser possível identificar todos os elementos quanto à protecção de que necessitam. Os interfaces do TCB devem também estar perfeitamente definidos e o desenho e implementação desse TCB devem permitir que este possa ser sujeito a testes extensivos e completos. Os mecanismos de autenticação são mais exigentes e deve existir um conjunto seguro de facilidades à disposição do Administrador do Sistema e dos Operadores de Sistema impondo exigentes procedimentos de administração e operação. Este tipo de sistema é relativamente seguro à penetração.

Classe B3 : Domínios Seguros - Um TCB da classe B3 deve satisfazer o requisito de mediar todos os acessos de todos os sujeitos a todos os objectos, estar seguro contra a intromissão e ser suficientemente pequeno de modo a poder ser submetido a análises e testes completos. Tendo em vista este fim, o TCB deve estar estruturado por forma a que possa ser excluído todo o software de sistema que não seja essencial para a cumprimento da Política de Segurança, o que obriga a que o desenho e implementação desse TCB tenho sido efectuado num perspectiva de minimização da sua complexidade. Esta Classe obriga a que esteja prevista a existência de um Administrador de Segurança, que os mecanismos de auditoria sejam expandidos ao ponto de alertarem automática e imediatamente para eventos definidos

como violadores da segurança, e exista a possibilidade e procedimentos de recuperação (recovery) do próprio sistema. Este sistema é altamente resistente à penetração.

Grupo A - Protecção Verificada

Este Grupo, é caracterizado pela utilização de métodos formais de verificação da segurança de modo a assegurar que os mecanismos de controlo da segurança discricionária e mandatória utilizados pelo sistema permitem proteger efectivamente informação classificada guardada ou processada pelo sistema. É requerida uma extensa documentação para demonstrar que o TCB cumpre os requisitos de segurança em todos os aspectos relacionados com o seu desenho, desenvolvimento e implementação.

Classe A1 : Desenho Verificado - Os sistemas da Classe A1 são funcionalmente equivalentes aos da Classe B3, sem qualquer requisito adicional no que diz respeito às características da sua arquitectura ou Política de Segurança. O facto que a distingue, tem a ver com a análise das especificações formais do seu desenho e das suas técnicas de verificação bem como elevado grau de segurança no que diz respeito à sua implementação, incluindo a física.

3.6. Testes de Segurança e Avaliação Comercial

Para que o modelo apresentado faça globalmente sentido, e possa responder às questões enunciadas no início, os documentos NATO referidos apresentam linhas de orientação relativamente às condições em que os testes de segurança a um determinado sistema devem ser efectuados bem como no que diz respeito à avaliação de um determinado sistema comercial. Sai mais uma vez fora do âmbito deste trabalho explicitar todas essas condições para cada uma das Classes anteriormente descritas.

Importa porém saber quais as suas linhas principais. Mais uma vez é posta ênfase nas pessoas que vão efectuar esses testes pelo que para cada Classe, são definidas condições quer para os testes propriamente ditos, quer para as pessoas que os irão efectuar. Relativamente às pessoas que irão efectuar esse testes, por exemplo, é definido para cada Classe, o número de pessoas a envolver, durante quanto tempo (tempo total e horas de trabalho), quais as suas habilitações académicas mínimas, as áreas em que devem possuir experiência e o que se entende por experiência e ainda, o seu grau de credenciação.

Quanto ao processo de avaliação comercial, está prevista uma sequência de passos que começa por uma proposta de avaliação por parte do construtor do produto (hardware ou software), seguido de uma avaliação formal de acordo com a metodologia atrás apresentada e finalmente a sua inscrição e divulgação pública numa lista de produtos, referindo as suas características. Uma vez que se torna difícil de incluir requisitos de segurança em produtos numa fase adiantada do seu desenvolvimento, evidencia-se a necessidade de que a intervenção dos futuros avaliadores se inicie numa fase relativamente primária do processo.