INSTITUTO DE ALTOS ESTUDOS MILITARES
CURSO DE ESTADO MAIOR

2000/2002

TRABALHO INDIVIDUAL DE LONGA DURAÇÃO

DOCUMENTO DE TRABALHO

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IAEM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DO EXÉRCITO PORTUGUÊS.

"A SEGURANÇA NOS SISTEMAS DE INFORMAÇÃO NO EXÉRCITO PORTUGUÊS"

"CONTRIBUTOS PARA A SUA DEFINIÇÃO"

João Batista Dias Garcia
Maj Tm (Eng)

INSTITUTO DE ALTOS ESTUDOS MILITARES

“A Segurança nos Sistemas de Informação no Exército Português”

“Contributos para a sua Definição”

MAJ TM (ENG) JOÃO BATISTA DIAS GARCIA

Resumo

Neste trabalho são caracterizados os sistemas de informação existentes no Exército quanto ao seu objectivo, finalidade e à temática do desenho que lhe está associada.

É discutida a necessidade de ser construído um modelo inicial de segurança que sirva de apoio à definição de segurança nos sistemas de informação. Neste sentido é apresentada uma proposta de metodologia para a implementação de segurança dos sistemas de informação e que percorra verticalmente a hierarquia do Exército. Esta proposta assenta essencialmente nas actividades que irão permitir definir os documentos orientadores da construção do modelo tais como a política de segurança da informação, a análise de riscos, a definição de uma política de segurança e os planos de contingência e recuperação.

Por fim é materializada a construção do modelo inicial de segurança com a calendarização das actividades e a respectiva atribuição de responsabilidades por actividade.

Palavras-chave: Política de segurança da informação; análise de riscos; política de segurança; planos de contingência e recuperação; auditorias; criptografia; sistemas de segurança.

Para a Eva e Lilita.

AGRADECIMENTOS

Não podia deixar de expressar os meus sinceros agradecimentos àqueles que contribuíram decisivamente para a concretização deste trabalho. A sua realização só foi possível devido à extrema disponibilidade de todos quanto foram alvo de entrevistas durante a fase de investigação.

Deixo a minha gratidão a todos os amigos e àqueles que contribuíram com os seus conhecimentos, proporcionando um excelente complemento para o trabalho.

Pela atenção disponibilizada, agradeço ao Gabinete Nacional de Segurança, ao Estado Maior do Exército nomeadamente à Divisão de Informações Militares e à Divisão de Comunicações e Sistemas de Informação, à Direcção dos Serviços de Transmissões, ao Centro de Informática do Exército e ao Batalhão de Informações e Segurança Militar.

Não podia deixar de referir a Caixa Geral de Depósitos e o Instituto das Tecnologias de Informação da Justiça pela sua disponibilidade e atenciosa contribuição.

GLOSSÁRIO DE ABREVIATURAS

Abreviatura	Descrição
ADME	Assistência na Doença aos Militares do Exército
ATCCIS	Army Tactical Command and Control Information System
BD	Bases de Dados
CA	*Certification Authority*
CAL	Comando Administrativo-Logístico
CEME	Chefe do Estado Maior do Exército
CFin	Centros de Finanças
CGLG	Centro de Gestão de Logística Geral
CIE	Centro de Informática do Exército
CmdLog	Comando da Logística
COFT	Comando Operacional das Forças Terrestres
DAMP	Direcção de Administração e Mobilização de Pessoal
DASP	Direcção de Apoio de Serviços de Pessoal
DCSI	Divisão de Comunicações e Sistemas de Informação
DES	*Data Encryption Standart*
DSF	Direcção do Serviço de Finanças
EME	Estado-Maior do Exército
EMGFA	Estado-Maior General das Forças Armadas
EPR	Entidade Primariamente Responsável
FA	Forças Armadas
GINET	Gestão da Instrução em Rede

Abreviatura	Descrição
LAN	Local Area Network
OTAN	Organização do Tratado do Atlântico Norte
PCR	Plano de Contingência e Recuperação
PKI	*Public Key Infrastructure*
RELCOI	Relatórios de Como Ocorreu a Instrução
RFW	Recursos Financeiros para Windows
RH	Recursos Humanos
RHW	Recursos Humanos para Windows
RRING	Redes Regimentais de Informação de Gestão
SI	Sistema de Informação
SIAPE	Sistema de Informação de Administração do Pessoal do Exército
SICCE	Sistema de Informação para o Comando e Controlo do Exército
SICOM	Sistema de Comunicações
SIILOG	Sistema Integrado de Informação Logística
SINFLOG	Sistema de Informação Logístico
SITEP	Sistema Integrado de Telecomunicações do Exército
SITMAT	Situação do Material do Exército
TI	Tecnologias de Informação
TILD	Trabalho Individual de Longa Duração
U/E/O	Unidades, Estabelecimentos e Órgãos
WAN	Wide Area Network

ÍNDICE

J - Algoritmos mais utilizados

K - O protocolo TCP

L - Características do SecNet

M - Gestão do controlo de acesso por password

N - Lista de política de segurança de informações

O - Guião das entrevistas

INTRODUÇÃO

Diariamente somos confrontados com questões de segurança. Desde o descer das escadas ou do elevador até ao percurso para o local do trabalho, a preocupação em nos protegermos de algo imprevisível é constante, e com o passar do tempo essa preocupação passa a fazer parte da nossa rotina e não se lhe dá a importância devida, até ao momento em que alguma coisa acontece que nos obriga a despertar para o problema.

Nas organizações, a primeira prioridade são os principais objectivos a atingir. Estes são programados, planeados e desenvolvidos com a finalidade de que todos os elementos da organização tenham disponível a informação necessária para o cumprimento das tarefas. Surge, desta forma, a necessidade de nos interrogarmos de que servirá a informação disponibilizada em todos os níveis da organização se não temos a certeza que ela é autêntica, confidencial, que a sua integridade não foi comprometida e que está disponível quando for necessária.

A resposta poderá estar, relativamente à informação, na segurança que a organização pode proporcionar ou que está disposta a investir, e para isso são necessários muitos recursos, elevados investimentos e uma definição exacta de uma política de segurança perceptível e difundida por todos quanto estejam envolvidos no Sistema de Informação (SI) da mesma.

Numa dinâmica de evolução, marcada por avanços tecnológicos, nem sempre passível de ser acompanhada pelos utilizadores de forma avaliativa e de sólida consciencialização, é decisivo minimizar os riscos com origem em desconhecimentos ou no desvirtuar da exploração de meios pouco controlados. Pelo que se impõe a definição de um conjunto de requisitos de segurança de sistemas que desvaneça receios, com ou sem fundamento, criando condições para a utilização dos SI com as garantias necessárias na sua aplicabilidade.

Os SI estão implícitos em todas as organizações, constituindo-se como um conjunto de meios, tecnológicos ou não, e procedimentos com a finalidade de assegurar informação onde é necessária. Face aos vasto campo que os SI abarcam, foi necessário limitar a definição a recursos que utilizam os meios informáticos, tendo em vista as aplicações utilizadas como veículo para a disseminação da informação.

A segurança aplicada no campo da informática alcança um campo muito vasto, não chega dizer que estamos seguros, quando temos todas as condições para realizar as nossas funções. É necessário estudar toda a envolvente interna e externa da organização para atingirmos um estado

de segurança aceitável[1]. A segurança que se procura tratar, neste trabalho, resulta da forma como os SI processam a informação e de que forma podemos controlar os acessos. Para isso vamos fazer uma análise sobre os sistemas de segurança associados ao controlo de acessos aos SI e sobre a forma como a informação é enviada pelos sistemas de comunicações.

A segurança total é impossível de concretizar, mas podemo-nos aproximar o mais possível daquilo que é essencial proteger face aos riscos que corremos derivados da análise das ameaças, o que implica uma atitude de alerta constante e de resposta imediata a situações não previstas.

Pretende-se ainda com este trabalho, para além de identificar e clarificar as actividades principais de uma organização face aos problemas de segurança dos SI, apresentar a segurança que está a ser desenhada nos sistemas e contribuir para a definição de um modelo inicial de segurança dos SI do Exército Português desenvolvidos, em fase de desenvolvimento ou projectados para o futuro.

Para isso propomo-nos verificar se existe segurança nos SI do Exército e contribuir para a definição de segurança nos sistemas de informação, pretendemos, também, levantar que tipo de segurança existe nos controlos de acesso e no transporte da informação dos SI existentes e, por fim, contribuir na área de segurança, com os conhecimentos adquiridos, para a construção de um primeiro modelo de segurança para os projectos futuros.

A abordagem do tema do trabalho conduziu a duas questões que servirão de guia para a investigação e julgamos que correspondem ao desafio a que nos propusemos:

1. Que segurança existe nos SI do Exército?
2. Que alteração a implementar no desenho dos SI no Exército, de forma a proporcionar-lhes segurança?

Com base no referido, a condução da investigação baseou-se na seguinte metodologia:

- consulta de bibliografia diversa que aborda conceptualmente a problemática da segurança;
- análise de legislação, directivas e demais documentos que apresentem dados sobre os SI existentes e em projecto no Exército;
- condução de entrevistas, realizadas no Gabinete Nacional de Segurança (GNS), no Estado Maior do Exército (Divisão de Informações Militares (DIM) e Divisão de Comunicações e Sistemas de Informação (DCSI)), no Centro de Informática do Exército (CIE) e no Batalhão de Informações e Segurança Militar (BISM).

Neste contexto, afigura-se-nos adequado apresentar o trabalho em cinco capítulos.

[1] Entende-se por segurança aceitável o estado de protecção de um determinado sistema após terem sido analisados as ameaças e as vulnerabilidades e terem sido tomadas as medidas adequadas para proteger os objectivos principais da organização.

Nos primeiros dois capítulos, francamente preliminares, são apresentados os conceitos fundamentais para um melhor enquadramento do estudo a desenvolver. Ainda no segundo capítulo são apresentados os conceitos relacionados com esta temática e os instrumentos que contribuem para a segurança e que se constituirão como pontos de reflexão e de futura comparação para o levantamento que nos propomos fazer no capítulo seguinte.

No terceiro capítulo pretendemos apresentar os SI de gestão e operacionais existentes e em desenvolvimento no Exército, abordando a sua finalidade e objectivo, e apresentar os sistemas de segurança implementados para a sua utilização como suporte à tomada de decisão e difusão por todos quanto a necessitem. No final deste capítulo julgamos estar em condições de dar a resposta à primeira questão colocada: “Que segurança existe nos SI do Exército?”

Após o levantamento dos sistemas existentes que contribuem para a segurança e sendo conhecedores dos indicadores de segurança dos SI de gestão e operacionais no Exército, no quarto capítulo vamos responder à segunda questão: “Que alteração a implementar no desenho dos SI no Exército, de forma a adoptar uma política de segurança?”. Neste capítulo, serão apresentados os contributos que podem ser proporcionados ou implementados para apoiar o desempenho das actividades de gestão e operacional. Vamos ainda, auxiliados com exemplos práticos reais, e apoiados na legislação em vigor, contribuir com indicadores e soluções concretas a situações que aguardam uma alteração urgente.

Por fim, vamos concluir o estudo com alguns pontos de reflexão e concretizar o que nos propusemos responder e apresentar no quarto capítulo. No quinto e último são apresentadas as propostas que irão contribuir para que o Exército desenvolva uma política de segurança da informação e dos SI.

1. ENQUADRAMENTO CONCEPTUAL

1.1 A IMPORTÂNCIA DA INFORMAÇÃO

"A informação tem que ser cuidadosamente adquirida, gerida e usada, como uma vantagem em relação às outras organizações"[2]. As organizações, actualmente, apresentam a informação como um valor primordial e que é universalmente aceite, constituindo, senão o mais importante, pelo menos um dos recursos cuja gestão e aproveitamento mais influencia o sucesso das mesmas. Ter acesso à informação tem feito a diferença entre os homens, Estados e governos. Como fonte de poder, a informação transformou-se no mais cobiçado e valioso bem da actualidade, passando a merecer tratamento especial no seio das organizações.

A informação, para além de ser vista como qualquer outro recurso, é também considerada e utilizada em muitas organizações como um factor que concorre para a definição da estrutura organizacional e como um instrumento de gestão, a par de poder ser utilizada como uma arma estratégica indispensável para a obtenção de vantagens competitivas. "Hoje a informação é uma arma preciosa, só que em excesso cria imobilismo"[3].

Motivadas pelas constantes mudanças, as organizações têm de se adaptar a novas situações, por isso assiste-se, actualmente, a uma crescente adopção de novos processos de desenho e funcionamento organizacional. Os novos processos implicam um aumento na valorização do papel da informação e da infra-estrutura que a suporta no seu desenho e funcionamento. Essa valorização é sentida pelas fortes apostas em investimentos em Tecnologias de Informação (TI) e na influência que tem na estrutura de custos das organizações modernas. O forte investimento em TI por parte da generalidade das organizações é certamente uma consequência das características económicas manifestadas pelas TI.

A gestão das TI, tem polarizado a atenção das organizações, talvez por se pensar, erradamente, que o facto de adquirirem TI e a explorarem com uma boa gestão é suficiente para a obtenção das vantagens que esta possa proporcionar. Por outro lado, a gestão da informação, ou a gestão do sistema responsável pela sua funcionalidade (do SI), não tem beneficiado do mesmo crescendo de interesse e reconhecimento por parte da grande generalidade das organizações. É comum pensar-se que a gestão dos SI é uma consequência da gestão de outros recursos (como, por exemplo, o financeiro ou o humano) ou o resultado marginal de projectos de reorganização administrativa. Contudo, a informação, como qualquer outro dos recursos vitais

[2] RASCÃO, José Poças, *Análise Estratégica – Sistema de Informação para a Tomada de Decisão*, pg. 158.
[3] VARAJÃO, João Eduardo Quintela, *A Arquitectura da Gestão de Sistemas de Informação*, pg. 53.

para a organização, deve ser gerida de forma a constituir-se como o cerne de uma área funcional da gestão da organização a que normalmente se designa por gestão da informação. A sua principal função motora é a de manter uma visão global dos dados da organização, de modo a satisfazer as suas necessidades de informação. A satisfação dessas necessidades passa essencialmente pela determinação de quais, onde e quando devem os dados estar presentes na vida da organização de forma a poderem ser utilizadas eficientemente.

1.2 CONCEITO DE SISTEMA DE INFORMAÇÃO

Os SI podem ser considerados como um meio para atingir a missão da organização, tendo como ideia que a "Missão" é a razão fundamental ou o propósito que justifica, em última análise, a sua existência e não uma finalidade em si, o que levanta a questão da definição da missão do SI como um dos sistemas organizacionais.

Após uma leitura de autores que abordam assuntos relacionados com os SI, facilmente se chega à ideia da existência de uma problemática de definição do conceito. Porém, relativamente à aceitação do termo "sistema", está bem objectivada nas definições encontradas, em que se entende que um sistema é um conjunto de elementos de um determinado tipo agrupados de forma a se constituírem como um todo.

As ideias que estão subjacentes na construção da definição de SI é que este apresenta a informação para o apoio à decisão, que engloba a combinação de procedimentos, informação, pessoas, métodos de trabalho e TI, e que combina o computador e os seus utilizadores para a transformação e armazenamento dos dados e da informação[4].

Um aspecto importante que surge na definição do conceito de SI é o da utilização do computador ou outros processos manuais, porém o segundo não vai ser incluído no nosso trabalho, pelo que não será espelhado na nossa definição, teremos sim presente que os SI são constituídos pelos "seguintes elementos:

- recolha de dados – factos, figuras ou rumores;
- arquivo dos dados – no computador ou em ficheiros manuais;
- selecção dos dados – seleccionar os dados segundo critérios apropriados;
- tratamento dos dados – manipular e agregar os dados;
- análise dos dados – analisar segundo a perspectiva pretendida;

[4] A diferença entre dados e informação é que os primeiros são factos, imagens ou sons que podem ser pertinentes para o desempenho de uma tarefa, mas que por si só não permitem compreender determinado facto ou situação; informação é um conjunto de dados úteis que permitem a sua utilização na tomada de decisão.

- apresentação da informação – proporcionar o uso da informação na forma mais conveniente"[5].

A definição que vamos apresentar e que vamos seguir durante todo o trabalho vai envolver não só as TI como elo de progresso e actualização, mas também, a informação, as pessoas da organização, bem como a própria organização. Assim, vamos considerar que o SI é o sistema responsável pela introdução, processamento, armazenamento e distribuição da informação na organização com o propósito de facilitar o planeamento, o controlo, a coordenação, a análise e a tomada de decisão ou a acção da organização. Por conseguinte, é um sistema de actividade humana que envolve o uso de TI.

Numa perspectiva estritamente tecnológica, as TI são o conjunto de equipamentos e suportes lógicos (hardware e software) que permitem executar tarefas como aquisição, transmissão, armazenamento, recuperação e exposição de dados. Por essa razão as TI são o conjunto de recursos disponíveis para o desenvolvimento, suporte e manutenção de SI.

Actualmente é quase impossível imaginar o SI de uma organização sem a sua adopção, pois as TI são um factor crucial para um melhor desempenho em termos da competitividade, incluindo o redireccionamento, a inovação e o redesenho de processos. As TI foram, e continuam a ser, potenciadoras de transformações capazes de adicionar vantagens nos fluxos da informação das organizações, funcionando assim como um factor diferenciador.

As TI estão a transformar o modo de funcionamento das organizações, e ao mesmo tempo a influenciar a sua estrutura interna. As facilidades para a transmissão de informação provocaram alterações nas estruturas das organizações tornando-as mais flexíveis, aproximando, em coordenação, fornecedores e clientes. As TI provocaram um grande impacto nas organizações impondo largas reformas, conduzindo ao desenvolvimento de novos negócios e de novos meios de comunicar, para além de aumentarem a eficiência e diminuírem as despesas[6].

Vimos até aqui a relação existente entre os SI e as TI, mas, é necessário relembrar que este trabalho assenta, principalmente, nas preocupações de segurança dos SI referentes às aplicações informáticas e nas implicações que envolvem a sua protecção. Com uma observação atenta à figura 1[7] podemos verificar que os SI que definimos estão localizados em termos de modelos de arquitectura por camadas[8], acima da camada de transporte ao nível da camada aplicação. Se associarmos, ainda, o facto de um sistema de comunicações ser um conjunto constituído por um emissor um canal de transmissão e um receptor utilizado para o transporte da informação,

[5] RASCÃO, José Poças, op. cit., pg. 25.
[6] Não se contabilizam os investimentos iniciais em novas TI, mas sim, o decréscimo das despesas para realizar a mesma tarefa antes do investimento.
[7] A figura 1 encontra-se na página A-2 do anexo A.
[8] Caso do modelo Open System Interconnetion (OSI).

podemos deduzir que os gestores dos SI não têm na sua responsabilidade os canais de comunicações, como as redes de telecomunicações ou as redes de dados, ficando apenas com as responsabilidades inerentes ao tratamento da informação até ao seu encaminhamento para os sistemas de comunicações e posteriormente na recepção.

É neste contexto que vamos dedicar a nossa atenção, nos próximos capítulos deste trabalho, à problemática da segurança nos SI associada à introdução, processamento, armazenamento, distribuição e apresentação da informação.

1.3 A SEGURANÇA EM AMBIENTES DE CARÁCTER INFORMÁTICO

Os sistemas informáticos têm um papel significativo nos sistemas de informação, tornando-se o principal suporte de todas as actividades, sejam elas industriais, tecnológicas ou administrativas para além das de investigação. É neste contexto que todas as organizações devem prestar maior atenção à problemática da segurança quer seja dos dados ou das aplicações informáticas.

O termo "segurança" aplicado aos sistemas informáticos é extremamente lato. Podemos considerar que um sistema seguro é aquele que permite aos utilizadores a realização do seu trabalho nas condições desejadas.

Um facto que veio enfatizar a necessidade de segurança nos sistemas de informação foi sem dúvida a globalização em que a industria se viu forçada a entrar. Neste sentido, a explosão da internet, como a conhecemos hoje, derrubou as barreiras que existiam na partilha e disponibilização de informação por todas as organizações do mundo, possibilitando a aproximação de culturas de organizações diferentes, e proporcionando a tendência de fusão entre grandes organizações internacionais. Com o objectivo de partilhar, ou apenas consultar toda a informação, organizações e particulares utilizam a internet colocando, sem intenção ou por negligência, em risco a sua estrutura interna.

A diversidade e evolução dos equipamentos e aplicações dos sistemas informáticos não se coaduna com o estabelecimento de normas rígidas que prevejam todas as situações criminosas; entendeu-se, portanto, criar um conjunto de regras suficientemente flexíveis, de forma a deixar aos responsáveis pela segurança a possibilidade de, caso a caso, apreciar a oportunidade das medidas a aplicar.

A aposta em novas TI é realmente um factor preponderante no desenvolvimento e crescimento de uma organização, mas essas apostas podem-se tornar insignificantes, duvidosas e destruidoras se não forem acompanhadas por fortes investimentos na segurança.

Actualmente, as organizações incluem os SI na sua estrutura organizacional. Este facto se por um lado, os torna mais competitivos e potenciam a exploração dos seus recursos, por outro lado, podem tornar a organização e a tomada de decisão dependente desses SI. O que implica depositar muita confiança e ter credibilidade nos SI da organização, e isto só é possível se os decisores tiverem a certeza que os sistemas são seguros.

Tem-se pensado muito que as ameaças à segurança vêm principalmente do exterior das organizações. No entanto, os maiores perigos e os que provocam danos superiores aos sistemas são aqueles que surgem no interior da organização, por pessoas internas, por causa da má formação ou mesmo por descuido ou desconhecimento.

A finalidade da segurança é proteger os bens das organizações, garantir e assegurar a continuidade das suas actividades, reduzindo o efeito das possíveis ameaças através da minimização dos impactos decorrentes das quebras de segurança.

O conceito de segurança quando se fala de informação não é simples visto que envolve muito mais que a simples protecção dos dados a nível lógico, pois para proporcionar uma segurança real temos que tomar em consideração múltiplos factores, tanto internos como externos. Um dos primeiros passos a dar é o de caracterizar o sistema que vai ser o depositário e que vai processar a informação, para serem posteriormente identificadas as ameaças.

Para desfazer qualquer tipo de más interpretações no decorrer do trabalho e para que fique claro que conceito de segurança adoptamos, tendo em consideração o que entendemos por SI e o quadro de relações abordado no ponto anterior, definimos segurança num contexto que nos permita garantir a protecção da informação processada nos SI desde o seu armazenamento até à sua apresentação.

Para que uma organização tenha uma boa postura em relação à segurança necessita ter grandes preocupações relativamente aos riscos que corre e à gestão desses mesmos riscos. Um risco é uma possibilidade de perda ou qualquer característica, objecto ou acção que está associado com essa possibilidade. Pode, ainda, ser associado com probabilidade, pois existe incerteza do resultado e com perda pois poderá prejudicar ou negar metas ou expectativas das pessoas, grupos ou da própria organização.

Para finalizar, apresentam-se os conceitos de ameaças, vulnerabilidades e nível de riscos. Assim uma ameaça[9] é uma força potencial que pode degradar a confidencialidade, a integridade, ou a negação dos serviços prestados pelos sistemas ou uma possibilidade potencial de uma tentativa deliberada sem autorização para ter acesso à informação, manipular a informação ou

[9] O conceito de ameaça aqui apresentado, apesar de não ter a mesma conotação da definição utilizada na estratégia (como uma capacidade por uma intenção), pode ser equiparado por ter um resultado muito semelhante quando da sua aplicação.

tornar um sistema incerto ou mesmo inutilizável. As ameaças podem surgir devido ao factor humano (e serem intencionais ou não intencionais) ou por causas naturais colocando assim em causa a segurança.

Entende-se por vulnerabilidade uma condição conhecida ou suspeita falha do sistema permitindo a sua exposição a penetrações, mostrando as suas fraquezas. Essa condição de fraqueza cria uma oportunidade para ser explorada por uma ou mais ameaças.

O nível de risco é determinado analisando a relação entre as ameaças e as vulnerabilidades. Um risco existe quando uma ameaça tem uma vulnerabilidade correspondente, mas até mesmo áreas de alta vulnerabilidade não terão nenhuma consequência se não existir a ameaça.

A verificação da inter-relação entre o objecto que se pretende segurar, as ameaças, as vulnerabilidades, e as contra-medidas para determinar o nível de risco é designada por análise de riscos[10]. O nível de risco que fica depois de terem sido analisadas todas as contra-medidas, o nível de vulnerabilidades, e as ameaças detectadas é chamado de risco residual. É com este risco residual que temos de trabalhar aceitando-o ou então, no mínimo, tentando reduzi-lo até ao ponto onde pode ser aceite.

[10] Na figura 2 no Anexo A são apresentados esquematicamente os conceitos relacionados com análise de riscos.

2. MEDIDAS DE SEGURANÇA

Este capítulo pretende apresentar os pontos principais que consideramos serem importantes para que uma organização disponha de SI com requisitos de segurança. Por isso, torna-se imprescindível referir quais as principais preocupações para o apoio ao primeiro passo da gestão dos SI (a Gestão dos SI é dividida em três actividades: o planeamento, o desenvolvimento e a execução dos SI)[11], o planeamento. Assim, considera-se que o responsável por planear a segurança para os SI deve seguir os seguintes passos:

a. analisar os riscos, estudar possíveis, quantificar as consequências desses riscos face à informação e contabilizar os custos totais;
b. analisar as medidas de protecção, definir as diferentes medidas de protecção tanto quantitativamente como na facilidade de utilização e velocidade de acesso;
c. decidir as medidas adequadas, comparar as duas análises das alíneas anteriores e decidir pela solução que amortize os riscos;
d. definir uma política de segurança, adaptar a forma de trabalho da organização às novas medidas de segurança;
e. manter continuamente as medidas de segurança bem como actualizar o desenho às novas realidades de potencial em informações;
f. elaborar planos de contingência e recuperação para eventuais riscos críticos que se detectem.

O facto de se seguirem estes passos, considerados gerais, é a garantia que, durante o planeamento, não se descuraram os aspectos de segurança. No entanto, é de primordial importância relembrar que, para proteger a informação, é necessário confrontarmo-nos com os seis problemas que são colocados à segurança e que se consideram como os objectivos principais da segurança dos SI. Estes são:

- a autenticação: assegurar que o utilizador e a informação sejam correctamente identificados;
- o controlo de acessos: proteger a informação contra intrusos;
- a confidencialidade: ocultar os dados de observadores não desejados;
- a integridade: comprovar que a informação não tenha sido alterada ou se modificada apenas por quem está autorizado;

[11] VARAJÃO, João Eduardo Quintela, *A Arquitectura da Gestão de Sistemas de Informação*, pg. 73.

- o não-repúdio: evitar que uma entidade autorizada seja rejeitada ao aceder à informação;
- a disponibilidade: assegurar que todos os recursos estejam disponíveis sempre que uma entidade autorizada o solicite.

Para a análise de segurança dos SI que pretendemos tratar, partimos das premissas que estamos a trabalhar em redes não seguras, da definição de SI, referida no capítulo anterior, e da segurança que pretendemos proporcionar-lhe, assim, vamos concentrar a nossa atenção sobre alguns considerandos relativos a aspectos que são de extrema importância para a definição da segurança nos SI de uma organização. Deste modo, aborda-se-à a necessidade da existência de uma política de segurança da informação e a importância da análise e gestão de riscos, indispensável para o sucesso no desenho de sistemas de segurança. De seguida, abordar-se-ão os métodos existentes relacionados com o acesso dos utilizadores aos SI e com a troca da informação entre utilizadores em redes não seguras, onde o recurso à criptografia (no Anexo B é apresentada uma perspectiva de evolução dos sistemas criptográficos) é, desde há muito tempo, fundamental para satisfazer os requisitos de segurança e confiança desejados. Por fim, apresentar-se-ão as medidas de segurança passivas que mais contribuem para os aspectos ligados com a segurança dos SI.

2.1 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A maioria dos órgãos executivos das organizações está consciente da necessidade da criação e cumprimento de uma política de segurança da informação, que envolva a formulação de directrizes (função estratégica), normas (função de gestão) e finalmente procedimentos e instruções de trabalho (função operacional), no entanto, é necessário fazer um grande esforço para que as diversas áreas de responsáveis pela segurança possam lançar mão dos principais recursos para a sua criação e manutenção.

A política de segurança de uma organização é, provavelmente, o documento mais importante num sistema de gestão de segurança da informação. Esta política deve ter como principal objectivo servir de base para o estabelecimento de normas, práticas e procedimentos de segurança da organização. Isto significa que deve ser simples, objectiva, de fácil compreensão e aplicação por todos os elementos da organização.

O controlo de segurança de um modo geral, e a política em particular, devem ser definidos para garantir um nível de segurança coerente com os objectivos da organização, contudo não deve prejudicar ou estrangular o seu funcionamento.

Entre os pontos abordados no documento que define a política de segurança de informações, deve constar a definição de segurança da informação sob o ponto de vista da organização, a definição das responsabilidades sobre os documentos existentes, as sanções que deverão ocorrer em casos de falha na segurança, uma visão geral sobre os controlos que estão (ou serão) implementados, e finalmente, deve referir a necessidade da existência do plano de contingência e de recuperação dos sistemas da organização.

Para a persecução dos objectivos na definição de uma política de segurança da informação, as organizações devem adoptar instrumentos e recursos tecnológicos de forma a assegurar a confidencialidade, a integridade e a autenticidade dos dados e informações classificadas, eliminar a dependência do exterior em relação a sistemas e equipamentos relacionados com a segurança da informação e promover a formação dos seus recursos humanos para o desenvolvimento da competência científico-tecnológica em segurança da informação.

Ao ser definida uma política de segurança da informação devem ter-se em consideração os quatro paradigmas básicos da sua composição: a integridade, a confidencialidade, a disponibilidade e a legalidade. A primeira diz respeito à condição na qual a informação ou os recursos da informação são protegidos contra modificações ou substituições não autorizadas, a segunda prevê que as propriedades de certas informações não possam ser difundidas ou divulgadas sem autorização prévia, a terceira é a característica da informação que se relaciona directamente com a possibilidade do acesso por parte daqueles que a necessitam para o desempenho de suas actividades e a última significa que deve obedecer a preceitos legais de acordo com a legislação em vigor.

Uma das áreas que deve ser tratada pela política de segurança da informação é a das ameaças. As principais ameaças que podem ser levantadas são as seguintes:

- integridade, devido a ameaças de ambiente (fogo, enchente, tempestade, etc.), a erros humanos, a fraudes e a erro de processamento;
- indisponibilidade, motivada por falhas em sistemas ou nos diversos ambientes computacionais;
- divulgação da informação, por duas ordens de razões, premeditada e acidental;
- alterações não autorizadas, causadas por acções premeditadas ou acidentais.

2.2 GESTÃO E ANÁLISE DE RISCOS

As medidas de segurança não proporcionam cem por cento de protecção contra todos os tipos de ameaças possíveis de serem levantados. A análise de riscos ajuda a estabelecer uma definição de segurança e a gestão de riscos permite que isso aconteça.

A análise de riscos, que se pode definir como o processo de avaliar ameaças e vulnerabilidades de um sistema, é uma parte essencial de qualquer programa de gestão de riscos. O processo de análise permite identificar as prováveis consequências ou riscos associados às vulnerabilidades e constituírem-se como uma base para estabelecer um bom programa de segurança. Utiliza-se a gestão de riscos como um processo de implementar e manter as contra-medidas necessárias de forma a proporcionar uma redução dos efeitos dos riscos para um nível aceitável.

O processo de análise de riscos dá a informação necessária para que seja possível fazer julgamentos relativos à segurança da informação. Este processo permite identificar os controlos de segurança existentes, o cálculo de vulnerabilidades e avaliar o efeito das ameaças nas diversas áreas de vulnerabilidades.

Na maioria dos casos, o procedimento de análise de riscos procura encontrar um equilíbrio económico entre o impacto que os riscos podem provocar e o custo das soluções de segurança que se podem planear para os evitar.

O custo associado ao controlo de qualquer risco não deve ultrapassar os custos das perdas máximas a ele associadas. Mas, nem todos os casos podem ser analisados desta forma, a decisão para implementar (ou não implementar) contra-medidas também pode ser tomada pela importância do sistema e dos dados armazenados, ou mesmo não tendo em conta os custos associados aos riscos que possamos correr. Em qualquer caso, deve ser sempre considerada a soma total dos riscos evitados pelo simples facto de apenas, com uma simples contra-medida, reduzir outros riscos associados.

As considerações referidas anteriormente formam a base para determinar as medidas de protecção mais apropriadas[12]. Com informação sobre as perda antes de e depois da aplicação das contra-medidas, podemos avaliar o custo-eficácia da decisão que foi tomada na prevenção dos riscos.

Após a identificação das medidas de protecção que deverão ser implementadas, deve ser dada primazia aos riscos maiores. A metodologia de análise de riscos seleccionada proporcionará

[12] Na figura 3 no Anexo A apresenta-se um gráfico que exemplifica o controlo dos riscos e as medidas que podem ser tomadas face às perdas.

o uso de indicadores de custo provável ou denominadores comuns que funcionam para identificar a solução de segurança com um óptimo custo-eficácia.

Uma política de segurança requer a criação de um planeamento de gestão de informação contínuo, processo que inclui planeamento para a segurança da informação de cada organização. A gestão de riscos é um programa contínuo dinâmico que permite estabelecer e manter uma solução de segurança dos sistemas de informação num nível aceitável. Uma vez que se atinja esse nível de segurança, a actividade de monitorização de gestão de riscos deve ser seguida de uma forma continua e diária. Em muitos casos, as regras, regulamentos, ou políticas que definem os programas de segurança da informação devem estipular quando deve ser feita uma análise de riscos.

Os passos que devem ser seguidos para a gestão de riscos passam por ordenar e localizar as acções correctivas necessárias de forma a reduzir o risco residual para níveis aceitáveis e monitorizar continuamente a política de segurança seguida.

Uma análise de riscos é um procedimento para estabelecer estimativas de risco sobre o objecto a proteger e o que podemos perder devido a um determinado número de ameaças. O primeiro procedimento determina o nível de vulnerabilidade do que pretendemos proteger identificando e avaliando o efeito das contra-medidas tomadas. Este nível de vulnerabilidade do objecto que pretendemos proteger face ao conjunto de ameaças, apenas é determinado pelas contra-medidas tomadas na altura da análise de riscos.

De seguida, com as informações obtidas, determina-se o significado das vulnerabilidades. Isto inclui, como o objecto a proteger é (ou será) utilizado, os níveis da sensibilidade dos dados, o fim a que se destinam e a sua inter-conectividade. E, por fim, o impacto negativo (ou perdas esperadas) é calculado examinando várias combinações nas áreas de ameaças e vulnerabilidades.

O que se referiu até aqui mostra bem a importância dos factores essenciais associados com a análise de riscos para a segurança, que são a definição do objecto a proteger, as ameaças, as vulnerabilidades, as contra-medidas e as perdas esperadas. O relacionamento entre estes factores é determinante para se perceber a problemática de uma análise de riscos.

Uma análise de riscos permite definir o ambiente actual e obter indicações sobre futuras acções correctivas se o risco residual for inaceitável. É ainda uma parte vital de qualquer programa de gestão de riscos e de uma segurança contínua. O processo da sua análise deve ser conduzido com a regularidade suficiente para assegurar que a gestão de riscos sobre a informação de objectos a proteger nas organizações seja uma resposta realista face aos riscos actuais.

2.3 ACESSO À INFORMAÇÃO POR ENTIDADES AUTORIZADAS

Para a selecção das entidades que podem ter acesso aos SI deve existir uma identificação única do utilizador ou grupo de utilizadores. Actualmente existem três métodos de identificar estes utilizadores:

- utilização de um segredo, com recurso à utilização de uma password;
- características físicas dos indivíduos, com recurso aos sistemas biométricos;
- da utilização de um objecto.

Actualmente, o método mais utilizado é o recurso a uma password, os sistemas biométricos, ainda muito recentes, estão a desenvolver-se rapidamente apesar de existirem contrariedades para o seu desenvolvimento tais como o preço dos equipamentos utilizados, conceitos éticos e a pouca divulgação de utilização, entre outros. A posse de objectos é desde há muito tempo conhecida, no entanto, o facto de implicar custos adicionais nos identificadores de objectos transforma-a num método pouco utilizado, actualmente estão a ser desenvolvidos acessos por sistemas criptográficos designados por certificados digitais.

Futuramente estes sistemas (o uso de uma password, de um objecto e da impressão digital por exemplo) vão ser complementares para aumentar a segurança; a utilização de um único não será suficiente para ter acesso à informação.

Passemos de seguida a analisar cada um dos sistemas.

2.3.1 UTILIZAÇÃO DE UMA PASSWORD

A maioria das organizações baseia o acesso aos SI na utilização de uma password para autenticar entidades e atribuir-lhe privilégios devido ao facto de serem os mais simples, populares e testados. Mas continuam a ser o ponto mais débil dos sistemas de segurança, pois é este método que normalmente se utiliza para proceder à autorização de acesso aos sistemas. O recurso excessivo a esta forma de controlo de acessos provoca situações de descontrolo de sigilo de password se a organização não tiver uma política de formatação, distribuição e controlo de acessos.

O principal problema dos sistemas de autenticação de utilizadores por password é o próprio utilizador. Este raramente está prevenido para os aspectos de segurança, quebrando-a quando cede a sua password a outro, quando a escreve num papel e quando utiliza uma password igual ao "*login*"[13], ou palavras/nomes relacionados com o utilizador.

[13] Nome utilizado pelo sistema para identificar um utilizador.

2.3.2 SISTEMAS BIOMÉTRICOS

Estes sistemas[14] utilizam uma característica física ou comportamental dos indivíduos para a sua identificação automática. A característica deve ser única nas pessoas e não se alterar com o tempo ou com as circunstâncias (estado de animo, temperatura, iluminação), como é o exemplo das impressões digitais, voz, retina, íris, reconhecimento da face, emissão de calor, análise de assinatura, geometria da mão e outras técnicas. Estes sistemas são muito mais seguros que o anterior e são de grande interesse em áreas onde é realmente importante verificar com exactidão a identidade de um indivíduo.

A utilização da biometria trouxe muitas vantagens aos sistemas de segurança. Os sistemas biométricos não permitem ser transferíveis, não necessitam que o utilizador faça gestão de utilização, como guardar objectos ou recordar frases, e são muito seguros contra qualquer tipo de ataque, evitando serem duplicados, roubados, esquecidos ou perdidos.

No entanto, também apresentam desvantagens como o de necessitar de tecnologia adicional para realizar leituras de imagens, tornando o sistema mais caro. A tecnologia actual não está muito desenvolvida, existe uma certa rejeição pelo utilizador motivada pela exposição física a sensores, levantam-se ainda questões de moral devido à exposição pública das características físicas e implicar estar cadastrado para toda a vida.

2.3.3 UTILIZAÇÃO DE OBJECTOS

2.3.3.1 OBJECTOS FÍSICOS

O controlo de acessos por este processo pode ser feito pela utilização de objectos que são transportados pelo utilizador onde são guardadas as password, ou são equipamentos electrónicos que utilizam um algoritmo de criação de password única por sessão ou que permita gerar um protocolo com o sistema de identificação. Estes sistemas podem ser cartões magnéticos, que permitem o registo em memória da password, cartões com *chip*, utilizados em contacto[15] ou à distância, ou calculadoras programáveis que permitem a programação de algoritmos.

Estes sistemas podem ser utilizados para complementar qualquer método de identificar pessoas, reforçando a segurança pelo factor posse de um objecto.

[14] Em Anexo C são descritos alguns exemplos dos métodos utilizados nestes sistemas.
[15] O exemplo mais comum são os cartões utilizados nos telemóveis para ter acesso às operadoras das redes móveis.

2.3.3.2 OBJECTOS LÓGICOS

Este sistema[16] utiliza criptografia para dar ao utilizador um objecto lógico. Assim, o utilizador tem que possuir uma chave privada dum algoritmo assimétrico[17] e um certificado digital com a chave pública, par da privada, assinado digitalmente pelo servidor (ou terceira entidade).

Os algoritmos assimétricos funcionam com duas chaves, com uma cifra-se, a outra é utilizada para decifrar, não existe a possibilidade de cifrar e decifrar com a mesma chave. Assim, uma chave é privada e somente a possui o seu utilizador, a excogitação com sucesso desta chave rompe todo o sistema de segurança, a outra é transmitida antecipadamente através de um certificado digital, este é um código contendo:

- o nome e dados do utilizador;
- a chave pública do utilizador;
- dados e informações de caracter geral;
- a assinatura digital[18] de uma terceira entidade.

É esta terceira entidade que assegura que a chave pública é de quem diz pertencer-lhe, assim, a segurança é baseada na confirmação da assinatura digital da terceira pessoa.

A assinatura digital é efectuada utilizando um resumo do texto e cifrando-o com a chave privada. No processo de decifração com a chave pública e comparação com o resumo calculado, pode-se comprovar que o texto não foi modificado porque os resumos coincidem e que a assinatura é do utilizador que tem a chave privada par da pública utilizada para decifrar.

O sistema está protegido contra roubo, extravios e duplicações devido ao processo de acesso implicar um protocolo de validação.

2.4 TROCA DE INFORMAÇÃO EM SEGURANÇA

A informação pode ser enviada com segurança através de qualquer tipo de canal de comunicações, para isso, actualmente, utiliza-se a infra-estrutura de chaves públicas (*Public Key Infrastructure* ou PKI), que consiste em serviços, protocolos e aplicações utilizados para a gestão de chaves públicas e certificados, provendo serviços de criptografia de chave pública[19] e assinatura digital, para permitir a interacção segura entre utilizadores e aplicações.

[16] No Anexo D é explicado em pormenor o funcionamento deste sistema.
[17] No Anexo F é descrito o funcionamento dos algoritmos simétricos e a forma como as chaves públicas e privadas são utilizadas.
[18] Uma assinatura digital, é um documento digital que identifica uma entidade e é baseada nos sistemas criptográficos assimétricos, no Anexo E pode-se verificar o seu funcionamento.
[19] No Anexo F são apresentados alguns conceitos importantes para a compreensão dos sistemas PKI.

Os serviços oferecidos por uma solução PKI podem variar desde um registo de chaves, emitindo novos certificados para uma chave pública, renovação ou cancelamento de certificados, obtenção de chaves públicas de uma autoridade certificadora até à validação de confiança, verificando se o certificado é válido e quais as operações a que está autorizado.

O facto do PKI usar a criptografia de chave pública, cuja utilização mais comum é a de ser utilizada para assinaturas digitais, torna-o como um sistema seguro que garante os seguintes serviços de segurança:

- Autenticação: identificar os utilizadores e/ou terminais;
- controle de acesso: controlar o acesso a informações e a realização de operações;
- confidencialidade e privacidade: assegurar que as comunicações sejam privadas mesmo em redes não seguras;
- integridade: garantir que a informação não é alterada;
- não-repúdio: adoptar um método de assinatura digital das informações e operações.

Desta forma, a solução PKI desenvolve um sistema em que os utilizadores, na troca de informação electrónica entre si, podem verificar inequivocamente a identidade de todos os utilizadores, garantir que a informação trocada não foi alterada por terceiros e que se mantém privada.

O conceito é inovador e permite expandir a esfera da segurança até às aplicações. Contudo, é necessário definir as necessidades com clareza, para depois especificar uma solução PKI.

Uma pergunta essencial que podemos fazer acerca do PKI é de que forma podemos ter a certeza que as chaves públicas encontradas correspondem à entidade a que se diz pertencerem e essa não foi falsificada. A resposta está em que o PKI estabelece níveis de confiança entre os seus utilizadores com a criação de uma Autoridade de Certificação (*Certification Authority* ou CA)[20]. A sua função básica é a de verificar a identidade das entidades que solicitam os certificados digitais[21], criar certificados e listas de revogações quando estes expirarem o prazo.

A utilização de algoritmos baseados em criptografia assimétrica, CA e certificados digitais permite que um grupo de utilizadores, dentro uma rede não segura, transmita dados entre eles de uma forma segura.

[20] No Anexo F apresenta-se a função das CA e a criação de uma estrutura hierárquica.
[21] Um certificado tem que conter, de uma forma estruturada, informação acerca da identidade do seu titular, a sua chave pública e a CA que o emitiu.

2.5 SEGURANÇA PASSIVA

Contribuem também para a segurança todas as acções e medidas consideradas importantes mas que não estão relacionadas directamente com os SI. No entanto, a segurança passiva é importante por contribuir a curto ou longo prazo para a diminuição de eventuais incidentes e das respectivas consequências relacionadas com as quebras de segurança. Desta forma, considera-se que é fundamental para uma organização ter a percepção do valor dos planos de contingência e recuperação em caso de desastres, das actividades de auditoria e das actividades relacionadas com a formação dos seus recursos humanos.

2.5.1 PLANOS DE CONTINGÊNCIA E RECUPERAÇÃO

Um Plano de Contingência e Recuperação (PCR) tem como finalidade identificar processos críticos para a continuidade da actividade da organização e dos recursos necessários para manter um nível aceitável de actividade, para proteger esses recursos e preparar procedimentos para assegurar a sobrevivência da organização aquando da ocorrência de acidentes; e visa repor, da maneira mais rápida possível, a capacidade da organização de continuar a realizar as suas actividades mesmo que aconteça um acidente nos seus processos críticos.

De uma forma geral, um PCR descreve as medidas que uma organização deve tomar para assegurar a continuidade das suas actividades essenciais no caso de existirem ameaças ao seus sistemas, deve ser desenvolvido para ambientes de situações em que as regras normais de segurança podem falhar, e deve ser concebido e testado antes da ocorrência da eventualidade para o qual foi elaborado. Um PCR, deve também, permitir antecipar todos os cenários susceptíveis de porem em causa o funcionamento da organização ou o bem estar das pessoas[22].

2.5.2 AUDITORIAS DE SEGURANÇA

As auditorias são de extrema importância para a avaliação do cumprimento dos objectivos, políticas, normas, regulamentos e planos de segurança desenhados para a organização. Através das auditorias pode ser verificado se o documento elaborado sobre a política de segurança é o

[22] O PCR deve ser desenvolvido por equipas pluridisciplinares, envolvendo equipas fortes e adequadamente lideradas e englobando todas as áreas a que o plano diz respeito. Isto quer dizer que a elaboração do plano não é da exclusiva responsabilidade dos técnicos e responsáveis pela segurança, deve também envolver a organização para ser testado periodicamente, actualizado sempre que necessário e estar em local seguro, mas de fácil acesso ao pessoal e equipas de recuperação.

adequado e se eventualmente é necessário proceder a algum tipo de alteração ou correcção no seu conteúdo.

"O objectivo das auditorias de segurança é controlar a observância das medidas de segurança"[23] de forma a assegurar que os planos de segurança aprovados bem como a legislação em vigor estão a ser cumpridos. Permite rever e avaliar os procedimentos internos, pela verificação da eficiência da utilização de recursos materiais e humanos, constatar a eficácia, verificando se os sistemas estão adequados às necessidades dos utilizadores e testar a segurança abrangendo as vertentes física, lógica e de comunicações.

2.5.3 FORMAÇÃO DOS RECURSOS HUMANOS

Os ataques à segurança são maioritariamente perpetrados por pessoas da organização, que podem praticar determinadas acções colocando a segurança em causa, como ter acesso indevido à informação de outros ou passar-se por outra pessoa para imputar responsabilidade, validar informação de forma maliciosa, afirmar ter recebido ou enviado informação, modificar indevidamente os direitos de outros, esconder a existência de informações, monitorizar indevidamente o tráfego da informação, alterar indevidamente uma função de software e provocar falhas aparentes no funcionamento normal dos SI.

"Os actos praticados pelas pessoas da organização constituem-se como cerca de 80% dos ataques aos sistemas"[24], podendo ser motivados por várias razões, como a obtenção de benefícios pessoais ou sofrer do síndroma de Robin Hood[25], e ainda o nutrir ódio pela organização, sofrer de perturbações mentais, ser desonesto e ter problemas financeiros.

Para diminuir as ameaças provocadas pelo factor humano devem-se motivar as pessoas desenvolvendo métodos de participação activa que obriguem a reflectir sobre o significado de segurança e do risco, assim como sobre o seu impacto na organização, nas funções ou nas pessoas. Todos os responsáveis nas diversas áreas devem ser capacitados a fim de conhecerem e entenderem a relação entre segurança, riscos e informação, e as suas implicações na organização, de forma a serem detectadas as debilidades e potencialidades da organização face aos riscos.

[23] FERREIRA, Jorge, *Normas Técnicas de Segurança dos Sistemas e Tecnologias de Informação*, pg. 62.
[24] Referido por Luís Sousa Cardoso, durante a palestra "*Os sistemas de informação - análise de riscos"*, no seminário sobre a segurança e protecção da informação.
[25] Sindroma relacionado com as pessoas que julgam que com a sua acção, sobre um determinado sistema, podem dar solução a um problema.

3. QUE SEGURANÇA NOS SISTEMAS DE INFORMAÇÃO DO EXÉRCITO

A informação que é produzida, com o auxílio dos SI do Exército, circula pelos meios de comunicação disponíveis nas Forças Armadas (FA), nomeadamente pelo Sistema Integrado de Telecomunicações do Exército (SITEP)[26], pelas redes de dados (Local Area Network - LAN, cabelagem estruturada e equipamento activo) das U/E/O, pelas interligações à Wide Area Network (WAN) do Exército (com acessos por circuitos militares e circuitos civis) e também por diversos circuitos do Sistema de Comunicações (SICOM)[27] da responsabilidade do Estado-Maior General das Forças Armadas (EMGFA). Todos estes sistemas de comunicações são considerados não seguros para a transmissão de documentos classificados, pelo que urge definir estratégias de segurança ao nível dos sistemas de informação para a rentabilização destes sistemas em toda a sua plenitude. A opção de tornar os sistemas de comunicações seguros é muito dispendiosa, pelo que não é praticável nem aconselhável face às verbas envolvidas e às sucessivas restrições orçamentais para as FA.

A estrutura organizacional do Exército desenvolve-se segundo duas linhas ortogonais (ver a figura 4[28]), uma, por convenção, horizontal, ao nível dos órgãos centrais de administração e direcção e outra, vertical, que se estende ao longo dos órgãos de implantação territorial.

Desta estrutura matricial deriva a arquitectura adoptada pelo CIE que apresenta igualmente duas componentes, as Grandes Aplicações Informáticas do Exército (GAIDES) que materializam o universo que abrange, segundo a direcção horizontal, todas as actividades relevantes para cada órgão central de administração e direcção; na componente vertical, as aplicações das Redes Regimentais de Informação de Gestão (RRING) que constituem o universo de integração das actividades de vários órgãos de implantação territorial.

As GAIDES, que correm sobre o sistema central, foram reforçadas por redes locais, onde cada grupo de utilizadores, contemplado por uma rede local, se encontra conectado a um servidor de dados no qual reside uma réplica da parte para si relevante da Base de Dados (BD) central sobre a qual realizam diariamente o seu trabalho sem sofrer as perturbações resultantes do acesso concorrente por parte de outros grupos de utilizadores, à mesma capacidade de processamento e à mesma BD.

[26] Em Anexo G é apresentado este sistema de comunicações da responsabilidade da DST.
[27] Em Anexo H é apresentado este sistema de comunicações da responsabilidade do EMGFA.
[28] A figura 4 encontra-se no Anexo A.

Esta arquitectura teve, no passado, uma só dimensão, a das actividades funcionais, visto que as Unidades que dispunham de alguma informática a manuseavam duma forma desagregada do contexto global.

Os SI militares foram desde muito cedo divididos em duas grandes categorias, os SI de gestão e os SI operacionais ou de comando e controlo, os primeiros englobam os sistemas que processam a informação necessária ao apoio da decisão dos órgãos centrais da administração e direcção do Exército, de forma a identificarem as insuficiências e as soluções para se atingirem altos níveis de eficácia. Nos segundos estão agrupados os sistemas de apoio à tomada de decisão em termos de Comando e Controlo da actividade operacional. São os SI destas duas categorias que vamos apresentar neste capítulo fazendo uma breve caracterização geral e focando os aspectos de segurança que eles englobam.

Por fim, faremos a apresentação de uma aplicação criptográfica para comunicações seguras em rede, desenvolvida no BISM.

3.1 OS SISTEMAS DE INFORMAÇÃO DE GESTÃO

Os SI de gestão do Exército que actualmente estão a ser utilizados, foram desenhados para apoiarem os órgãos centrais de administração e direcção nas áreas de pessoal, logística, finanças e instrução e estão agrupados na componente das GAIDES; as aplicações para as mesmas áreas disponibilizadas para as U/E/O foram agrupadas no projecto RRING.

Vamos, a seguir, fazer uma breve descrição dos SI utilizados nas áreas referidas das duas componentes do CIE e levantar algumas características relativas à segurança que possuem ou aos riscos de insegurança que representam. Como os SI da componente GAIDES apresentam uma estrutura e implementação de segurança semelhante e comum a todos, os aspectos mais significativos serão tratados posteriormente em conjunto no ponto 3.1.5 "Aspectos comuns de segurança".

3.1.1 ÁREA DE PESSOAL

O Sistema de Informação para a Administração do Pessoal do Exército (SIAPE) é o SI principal da área de pessoal, onde estão centralizadas, numa Base de Dados Única de Pessoal (BDUP), as notas de assentos e a ficha biográfica de todos os militares do Exército. Esta BD talvez seja o maior desafio para a segurança, devido ao cumprimento necessário da lei da protecção dos dados pessoais, quanto ao seu tratamento e à sua circulação pelos circuitos de comunicações. Para além de, obrigatoriamente, ter de terminar com as duplicações de BD

existentes em outros locais como é o caso da BD utilizada pela Direcção de Apoio de Serviços de Pessoal (DASP) e uma outra BD utilizada pela área das finanças, sem contabilizar as múltiplas pequenas BD existentes nos regimentos e hospitais do Exército, sem estarem sujeitas a qualquer tipo de controlo centralizado.

No âmbito do SIAPE funcionam vários processos automatizados que a Direcção de Administração e Mobilização de Pessoal (DAMP) e as suas repartições de pessoal permanente, não permanente e civil utilizam para efeitos de colocações, promoções, produção de fichas biográficas, listas de antiguidade, avaliação de mérito, edição da Ordem do Exército, etc.. No Estado-Maior do Exército (EME) encontram-se informatizadas as funções das Divisões de Pessoal e Operações relacionadas com a elaboração dos quadros orgânicos de pessoal.

Na DAMP e no EME estão implementados ambientes descentralizados com redes locais e com réplicas parciais da informação contida no sistema central que corresponde às respectivas áreas de interesse que, entre outras facilidades, facultam a obtenção imediata de respostas a interrogações agregadas segundo diferentes critérios e ordenações.

O SIAPE é composto por diversos subsistemas, correspondentes com as várias direcções do comando de pessoal, supostamente todas ligadas à BDUP. Como o SIAPE não se encontra totalmente implementado, devido aos vários subsistemas não estarem terminados (como se pode verificar no Anexo I) e não se encontrarem interligados, não permite o cruzamento da informação entre os vários subsistemas.

Entre os subsistemas do SIAPE, pelo desafio que representam no futuro destacam-se, o Sistema Informático Para as Operações de Recrutamento Geral (SIPORG) que será a adaptação das alterações introduzidas na lei de serviço militar no desafio de recrutamento para as FA e o Sistema Informático de REcrutamento de MIlitares Contratados (SIREMIC) que vai permitir a gestão de vagas RV/RC em tempo real, dando resposta aos pedidos de solicitação de informações sobre contratações face às necessidades e vagas existentes no Exército.

3.1.2 ÁREA DA LOGÍSTICA

Inicialmente na área da Logística estava previsto ser desenvolvido um vasto conjunto de aplicações que constituiriam o Sistema Integrado de Informação Logística (SIILOG) de forma a servirem as entidades gestoras logísticas e os depósitos no controlo e actualização de:

- processos de obtenção, catalogação, reabastecimento e manutenção de várias classes de artigos da cadeia logística;
- situação dos materiais orgânicos principais de cada Unidade;

- grau de apetrechamento das Unidades do Sistema de Forças do Exército.

O SIILOG surge inicialmente com o princípio de se constituir como o SI único da logística de todos os órgãos do Exército, e a sua finalidade é a de integrar o conhecimento logístico numa perspectiva informática com uma BD central, de forma a permitir a gestão centralizada dos recursos e a uniformizar procedimentos, contendo um conjunto de "ferramentas" para auxiliar a gestão do reabastecimento, a gestão do transporte, a gestão da manutenção, a gestão da obtenção, a catalogação, o sistema de forças e respectiva situação de material operacional e a gestão de códigos.

O SI de apoio à área da logística estará a funcionar plenamente quando for apoiado pelos suportes informático e de catalogação. Os suportes informáticos deverão permitir recolher e processar toda a informação e possibilitar a ligação ao Comando da Logística (CmdLog), através do Centro de Gestão de Logística Geral (CGLG). Este estará ligado às Direcções de Serviços, aos Depósitos Gerais e ao Comando Administrativo-Logístico (CAL), que tem a missão de prestar o apoio logístico às forças do Comando Operacional das Forças Terrestres (COFT) empenhadas em operações através do seu Centro de Gestão de Material.

O objectivo do SIILOG era ser um sistema único de informação para todos os órgãos logísticos. Decorrente da demora no desenvolvimento do SIILOG, e devido à necessidade de sistematização e integração da informação de âmbito logístico, o CGLG, desenvolveu o Sistema de Informação da Situação do Material (SITMAT), com a finalidade de implementar um SI que permitisse a consulta e actualização contínua e permanente da situação dos materiais no Exército referente a quantitativos existentes, à sua distribuição e respectivo estado de operacionalidade. Este sistema disponibilizava a informação aos vários escalões de planeamento, decisão e execução, designadamente do EME, do CmdLog, do COFT e das grandes Unidades de natureza territorial, permitindo apoiar os processos de decisão.

Como o SITMAT era um SI em que a introdução dos dados seria feita *on line*, e que estava dependente do desenvolvimento do Projecto RRING, e este projecto ainda não está aplicado em todas as U/E/O, levou a que fosse abandonado por se tornar pouco útil para atingir os objectivos para os quais foi desenhado.

Com a intenção de permitir, no quadro da logística operacional[29], efectuar uma adequada e oportuna gestão, e sem prejudicar a funcionalidade de integração entre as logísticas operacional e de produção[30], o CmdLog desenvolveu uma iniciativa que lhe permite ter a capacidade de gerir os materiais e infra-estruturas. Para isso, servindo como base o SITMAT, o CmdLog pretende

[29] A logística operacional ou de consumo estuda os problemas que se apresentam ao nível das forças operacionais.
[30] A logística de produção, económica ou de alto nível estuda os problemas logísticos que se apresentam à escala nacional ou governamental e corresponde à faceta industrial da logística.

integrar as aplicações existentes ao nível das Direcções Logísticas e incrementar o funcionamento da catalogação. A iniciativa desenhada para este novo sistema "intermédio" parece ser bastante audaz e válida, no entanto, tem um senão, pela análise da directiva inicial que lhe deu origem, verifica-se que não foi dada a missão de preocupação em proteger os dados e a respectiva BD processada por este sistema, colocando a segurança da informação processada num plano com pouco significado.

Actualmente, está em processo de desenvolvimento o Sistema de Informação Logístico (SINFLOG) que vai integrar todas as possibilidades e potencialidades definidas para os SIILOG e SITMAT, apresentando novos módulos e uma nova estrutura.

3.1.3 ÁREA DAS FINANÇAS

É na área das finanças que a interligação entre as GAIDES e as aplicações do RRING foi concretizada. Assim, as U/E/O utilizam a aplicação Recursos Financeiros para Windows (RFW) do RRING e enviam um ficheiro, previamente cifrado utilizando o algoritmo simétrico *Data Encryption Standart* (DES)[31], através da rede ou recorrendo a uma disquete, para os Centros de Finanças (CFin) dos comandos territoriais, estes utilizam a "aplicação dos CFin" desenvolvida pelas GAIDES. A Direcção dos Serviços de Finanças (DSF) recebe os relatórios em formato ficheiro dos CFin dos comandos territoriais, mas, neste caso os ficheiros não são cifrados o que denota uma falta de coordenação de procedimentos de segurança entre as duas componentes do CIE.

A maioria das Secções Financeiras das U/E/O e dos CFin dispõe de um sistema informático que lhes permite executar de modo automático e metódico um vasto conjunto de operações como:

- elaborar planos orçamentais;
- efectuar registos de tesouraria;
- controlar encargos;
- prestar contas;
- pagar comparticipações da Assistência na Doença aos Militares do Exército (ADME);
- coligir elementos que originam alterações ao vencimento de cada militar.

Estes processos geram informação que é enviada posteriormente para vir a ser utilizada por outros processos de entidades externas a cada Unidade. São receptores deste fluxo proveniente das U/E/O diversos organismos como a DSF, os Serviços Sociais das Forças Armadas (SSFA), a

[31] Em Anexo J é apresentado o algoritmo DES e outros tipos de algoritmos mais utilizados em alternativa a este.

Caixa Geral de Aposentações (CGA), a DASP, a Direcção-Geral de Protecção Social aos Funcionários e Agentes da Administração Pública, as Oficinas Gerais de Fardamento e Equipamento (OGFE) e a Chefia de Abonos e Tesouraria (ChAT).

No caso da ChAT, aí residem as aplicações para processamento dos vencimentos que dependem fortemente dos dados oriundos das U/E/O e que têm uma importância vital não apenas pelo cálculo dos vencimentos em si, mas também porque constituiem uma fonte de informação sobre pessoal, mais actualizada do que qualquer outra BD por força da sua natureza e sensibilidade. Esta informação, depois de enviada para os registos da BDUP, permite ser utilizada por outras aplicações do SIAPE.

3.1.4 ÁREA DA INSTRUÇÃO

A área da Instrução apoia-se sobre o sistema de Gestão da Instrução em Rede (GINET) através do qual os centros de instrução elaboram ficheiros no acto da incorporação e no final da preparação militar geral e da preparação complementar dos cursos de formação de oficiais, sargentos e praças e ainda das escolas de cabos.

Esses ficheiros contêm informação sobre a identidade dos militares incorporados, o modo como decorreu a incorporação e sobre as aptidões dos instruendos e as diversas classificações obtidas nos circuitos de avaliação, no tiro de espingarda e pistola, na educação física militar e no mérito pessoal. É com base na informação contida nesses ficheiros que é efectuada a distribuição dos militares pelas U/E/O.

A partir desses ficheiros são organizados os Relatórios de Como Ocorreu a Instrução (RELCOI) para envio, via disquete, aos Quartéis Generais e Comando da Instrução e outros relatórios de instrução para envio, também via disquete, ao CIE e inserção na BDUP à qual acede, por sua vez, a DAMP que tem assim possibilidade de explorar a informação originada nos Centros de Instrução para efeito de eventual convocação e mobilização de pessoal.

Dos cursos de formação, promoção e qualificação do pessoal do Quadro Permanente são também extraídas das respectivas Fichas de Controlo da Instrução e registadas na BDUP as relações de frequência e aproveitamento que passam a constituir elementos de informação para alimentar pesquisas com objectivos variados.

Toda a informação processada nesta área é transportada via disquete, para posteriormente ser inserida na BDUP, e não é difícil prever as consequências que podem daí advir se não forem tomadas providências muito ajustadas sobre o manuseamento e tratamento dessa informação.

3.1.5 ASPECTOS COMUNS DE SEGURANÇA

As GAIDES, em termos de segurança, têm, na sua globalidade, um tratamento muito semelhante para a generalidade das aplicações. Foi esta a razão que levou ao agrupamento, neste ponto, dos considerandos sobre os aspectos de segurança dos SI descritos nos pontos anteriores, com a excepção do ponto "3.1.3 Área das finanças" por ter um tratamento diferenciado como se referiu.

Em termos gerais, o controlo de acessos aos SI é feito em três níveis, o primeiro diz respeito ao controlo de acesso do utilizador à rede de dados do Exército[32] ou ao sistema central, feito através das potencialidades permitidas pelos respectivos sistemas operativos, o segundo é accionado pelo método do acesso por máquina entre a aplicação do SI instalada na estação de trabalho e o servidor[33], e o terceiro nível de segurança é o acesso às BD.

O controlo de acesso às BD apresenta uma particularidade que, em termos de acessos, pode ser considerada uma óptima solução de segurança, em que o utilizador, após ter acesso à rede de dados através do sistema operativo, no seu posto de trabalho, encontra disponível a aplicação do SI que opera. O processo de acesso à BD não exige a intervenção do utilizador, a autorização de troca de informação entre o SI e a BD é feita de uma forma transparente para o utilizador, isto é, o SI tem um módulo de segurança incorporado, com as características do posto de trabalho do utilizador e os respectivos certificados de acesso às áreas da BD. No entanto, tanto os registos na BD como a informação trocada entre a aplicação e a BD não é cifrada por qualquer tipo de algoritmo, apesar de existir essa capacidade.

Para controlar a actividade de registos nas BD, feita por utilizadores autorizadas, foi criado um sistema de controlo pós actividade, ou seja, quando um utilizador autorizado executa uma operação de alteração, modificação ou inserção de novos dados na BD é guardado o registo anterior ("ficheiro primário", antes das alterações) e criado um registo de alterações ("ficheiro de alterações") contendo informação sobre o autor da operação, quando a executou e que tipo de acção foi tomada. De seguida, pessoas credenciadas fazem a comparação entre o ficheiro de alteração e o ficheiro inicial e verificam a validade das operações efectuadas. Este processo constituí-se como a única medida passiva de segurança dos SI da responsabilidade das GAIDES.

[32] Iremos nos referir a este controlo de acessos quando se abordar mais à frente o projecto RRING.
[33] Esta forma de controlo de acessos não foi abordada neste trabalho.

3.1.6 PROJECTO RRING

O Projecto RRING, para além do fornecimento de Computadores Pessoais (*Personal Computer* - PC) com software de série, tem um outro grande esforço dirigido directamente às Unidades, com o desenvolvimento de software para resolver problemas pontuais. O seu objectivo é suportar, de uma forma global e integrada, o sistema de informação de uma unidade de escalão regimento e dotá-la de funcionalidades adequadas à sua vida interna.

A finalidade deste projecto centra-se no apoio à acção de comando, de forma a permitir que os vários escalões de comando tenham acesso em tempo real à informação necessária nas áreas de pessoal, informações, logística, segurança, finanças, justiça, etc., para além de se centrar na implementação da doutrina, das normas e regulamentos em vigor, na normalização dos dados e tabelas para todo o Exército, na automatização dos processos e partilha dos dados, fundamental para a partilha de dados entre as várias áreas funcionais das U/E/O, na uniformização de procedimentos e relatórios, ao padronizar as aplicações para todas as unidades e na simplificação da formação e treino, conseguida porque se adoptou como norma o interface *Windows da Microsoft* que é actualmente o Sistema Operativo (SO) mais utilizado e conhecido e, por conseguinte, de fácil aprendizagem e compreensão.

A informatização proporcionada pelo projecto RRING consiste em vários módulos correspondentes às áreas funcionais de regimento, instalados numa rede de PC e apoiados por uma BD local com possibilidade de estar ligada à BD central.

Cada Regimento, para além dos módulos nucleares (comando, recursos financeiros, secretaria, etc.) terá a possibilidade de adicionar os módulos que, não sendo os normalizados, sejam necessários à sua missão específica (mobilização, instrução, etc.).

Os módulos desenvolvidos partilham uma mesma BD local, intercomunicam entre si de acordo com a funcionalidade de um regimento e ligam-se de forma transparente à BDUP do Exército e através delas às GAIDES. Esta funcionalidade só está disponível para a área das finanças, como se referiu anteriormente.

Para além do software de série que equipa todas as estações de trabalho e faculta todas as facilidades vulgarmente designadas de automatização de escritório, existe ainda o software aplicacional constituinte dos módulos que permite automatizar áreas como a gestão de recursos financeiros, a gestão de pessoal, cargas e a produção de relatórios para o escalão superior. As actividades de secretaria, de mobilização e de justiça, e algumas funções introduzidas nos módulos incluem ou irão incluir:

- o registo digital de fotografias para o controlo de movimentos e emissões de cartões de acesso nas portas de armas;
- o fornecimento, numa estação "pública" (ao alcance de todo o pessoal) com écran sensitivo, de informações gerais sobre cada Unidade, tais como a planta, a localização de bocas de incêndio, o plano de uniformes, a Ordem de Serviço (OS), as Normas de Execução Permanentes, as efemérides e o historial de cada unidade;
- o envio automático de mensagens em ficheiro de cada posto de trabalho para o centro de mensagens.

As características deste projecto centram-se na modularidade de cada área funcional das U/E/O (Pessoal, Finanças, etc.), na integração a vários níveis entre aplicações, na conectividade, devido ao facto da tecnologia adoptada ser a mesma em todas as aplicações do projecto RRING, na flexibilidade, pois as aplicações são concebidas para multiutilizador o que permite instalar diversos postos de trabalho, na integridade e segurança, em que nas várias aplicações os utilizadores são autenticados por password duas vezes (a primeira no acesso à rede de dados e a segunda por mecanismos das próprias aplicações) e no facto de ser utilizado o *Transmisson Control Protocol* (TCP)[34] para o encaminhamento de pacotes[35] através da WAN do Exército o que potencia a segurança da transmissão dos dados, e finalmente, na administração centralizada, característica imposta, devido a não existir capacidade local nas U/E/O para administrar todos estes sistemas.

A situação actual do projecto RRING está numa fase bastante avançada, tem duas aplicações principais que permitem informatizar a área financeira através da aplicação RFW[36], e a aplicação Recursos Humanos para Windows (RHW) que informatiza a área do pessoal.

O projecto RRING tem ainda outras aplicações e serviços que permitem informatizar algumas rotinas nos Regimentos como a OS, a Lista Telefónica Militar (LTefEx), a Gestão de Cargas (GCargas), a Gestão de Cargas, saltos e Pára-quedas (GParaq), a Lista de Antiguidades do Exército (LAE) e, uma última recentemente desenvolvida, a Legislação Militar (LegMil). Possui também uma *intranet*, a nível do Exército, e uma componente de correio electrónico para troca de informação não oficial entre os utilizadores da WAN do Exército, e simultaneamente de e para fora dela, sendo essa última possibilidade através do recurso à Internet.

Como se referiu, em todas as aplicações o controlo de acesso dos utilizadores é feito duas vezes por password, a primeira no acesso à rede de dados e a segunda pelas próprias aplicações.

[34] Em Anexo K apresenta-se o protocolo TCP e as características principais da sua utilização em rede.
[35] Conjunto de bits agrupados de comprimento fixo, resultado da divisão em partes semelhantes de um determinado grupo de dados que se pretendem transmitir.
[36] Esta aplicação está disponível em duas versões, uma que permite o seu funcionamento num computador isolado e outra versão para U/E/O com ligação à WAN do Exército.

As password são fornecidas automaticamente ao utilizador. Este tem a possibilidade de escolher o tamanho e o conteúdo que quiser para a sua password, isto pode ser traduzido da seguinte forma, o utilizador pode escolher o tamanho de um caracter, por exemplo a letra "a" se associarmos a isto o facto do *login*[37] ser o número mecanográfico do utilizador, a probabilidade de uma pessoa não autorizada ter acesso aos recursos que a rede de dados proporciona, através da descoberta da password, é muito elevada, conseguindo essa proeza no tempo recorde de um segundo.

A informação está registada em BD de forma estruturada e o acesso é sempre feito pelas aplicações respectivas sem intervenção do utilizador. O acesso às aplicações está condicionado, por isso, só é possível através de utilizadores credenciados para o efeito; esta credenciação é feita pelo utilizador que acede ao módulo do chefe no caso da RFW ou pelo utilizador que é definido como chefe da secção de pessoal no caso da RHW. São estes utilizadores credenciados que definem quais são os utilizadores que trabalham com as aplicações e em que módulos das mesmas.

3.2 OS SISTEMAS DE INFORMAÇÃO OPERACIONAIS

Estes SI permitem o relacionamento entre os dados (oriundos da área de pessoal, informações, operações e logística) e o terreno representado em cartas topográficas.

Os SI operacionais é o sistema que permite o tratamento, arquivo e apresentação da informação necessária à condução das operações militares. Com o surgimento das TI estes SI tiveram um grande impacto, permitindo automatizar a obtenção, armazenamento e processamento da informação, colocar à disposição do comandante o resultado desse processamento e difundir as ordens.

Vamos de seguida apresentar o sistema que está a projectado para o apoio ao comando e controlo no Exército.

3.2.1 O PROJECTO SICCE

Actualmente, as operações militares caracterizam-se por uma tendência crescente para operações conjuntas e combinadas e pela existência de problemas de interoperabilidade no interior e entre os Ramos, forças e países. É neste contexto que foi levantada a necessidade do comprometimento do Exército, num projecto audaz e de cooperação, para o desenvolvimento de um SI táctico para o Sistema de Forças Nacional, o Sistema de Informação para o Comando e

[37] Identificação ou nome do utilizador.

Controlo do Exército (SICCE), não deixando de ser aplicável no apoio da actividade normal dos órgãos de implantação territorial, constituindo-se assim, num verdadeiro sistema de informações de comando e controlo (Command and Control Information System - CCIS) integrado ao nível táctico e estratégico.

O projecto SICCE, está a ser desenvolvido por uma equipa constituída em parceria entre o Exército e o INESC[38], e desde logo, procurou participar activamente no grupo de estudos ATCCIS[39].

O projecto SICCE que visa essencialmente permitir o desempenho de tarefas essenciais, em especial as operacionais, nas principais funções de planeamento e de Estado-Maior, visa também ter permanentemente actualizada a apresentação da situação táctica (terreno e unidades) como base essencial para a avaliação da situação e permitir a transmissão dos planos e ordens a todos os intervenientes de uma forma rápida e eficiente, garantindo ao mesmo tempo, não só um alto nível de interoperabilidade, já que se baseia nos princípios das especificações ATCCIS mas também, permitir ser um sistema em permanente evolução, por forma a proporcionar apoio ao comando e controlo conjunto e combinado no futuro.

O projecto na área do CCIS táctico contemplará a componente do sistema de informação, através do desenvolvimento de aplicações operacionais com interface simples e amigável com os utilizadores correspondentes às células de Estado-Maior, bem como um mecanismo de réplica da informação e respectiva gestão e controlo e ainda a componente do transporte da informação através dos sistemas de comunicações tácticos.

O SICCE responderá aos requisitos de flexibilidade, para poder adaptar-se facilmente às mudanças tecnológicas, de modularidade, de modo a poder adaptar-se a níveis pretendidos e a facilitar posteriores upgrades de hardware e software, de fiabilidade, de forma a garantir eficácia e qualidade adequadas ao tratamento e transporte da informação de forma integrada, de estandardização, não só para garantir a compatibilidade e integrabilidade entre os diversos elementos constitutivos do sistema, bem como a interoperabilidade com outros sistemas nacionais e da Organização do Tratado do Atlântico Norte (OTAN). Apresenta também o requisito de segurança, de forma a permitir isolar, em termos físicos e lógicos, as aplicações e sistemas de utilizadores não autorizados.

Quanto a este último requisito, não foi possível encontrar, nos documentos a que tivemos acesso, o desenho de segurança para o projecto SICCE, obtendo-se apenas a informação de que não está previsto o desenvolvimento de qualquer módulo de segurança, o que nos leva a pensar

[38] Instituto de Engenharia de Sistemas e Computadores.
[39] Army Tactical Command and Control Information System.

que, mais uma vez, o planeamento de um novo projecto fica desmembrado do desenho de sistemas de segurança.

Levanta-se, assim, a grande dúvida colocada inicialmente, se um SI é desenhado para o apoio à gestão ou à tomada de decisão, que garantias dá aos decisores a informação tratada por esses SI, se não obedece aos princípios gerais de segurança. E obriga a questionar, se não será necessário definir desde já que política de segurança seguir para os SI do Exército, deixando de dar azo a planeamentos desprovidos da área de segurança.

3.3 UMA APLICAÇÃO CRIPTOGRÁFICA PARA COMUNICAÇÕES SEGURAS

No BISM foi desenvolvida uma Aplicação Criptográfica, designada por "*Security Network*" (SecNet), que disponibiliza ao utilizador uma ferramenta que permite a transmissão segura de dados em redes não seguras. Esta aplicação vem tornar possível o encaminhamento da informação classificada por circuitos não seguros e, ao mesmo tempo, utilizar algoritmos de cifra como ferramenta fundamental para concretizar os objectivos da segurança.

O SecNet é baseado na estrutura PKI para a troca de informação segura entre utilizadores e apresenta como característica principal ser uma aplicação que satisfaz os objectivos de segurança para além de implementar um esquema de certificação digital (em Anexo L são apresentadas as características desta aplicação). Esta característica torna a aplicação de extrema utilidade para servir como base para a troca de informação classificada entre os centros de comunicações do Exército, e pode também ser estendido aos Ramos das FA e proporcionar-lhes uma integração total dos serviços de comunicações.

O grande entrave à utilização desta aplicação é a inexistência de um processo de acreditação dos SI ou aplicações desenvolvidas ou adquiridas para o Exército, que certifique os SI desenvolvidos ou adquiridos de forma a serem enquadrados legalmente.

4. CONCLUSÕES - CONTRIBUTOS PARA A DEFINIÇÃO DE SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO NO EXÉRCITO

Da pesquisa realizada e das entrevistas efectuadas, facilmente se chegou à conclusão da forma como a segurança dos SI é tratada (ou não é tratada). Assim, podemos claramente referir que a segurança que está desenhada para os SI no Exército é insuficiente e muito pouco fundamentada, principalmente nos pontos que foram focados na abordagem teórica nos capítulos um e dois comparativamente com a segurança existente nos SI descrita no capítulo três. Se atendermos, ainda, que as soluções encontradas para a definição dessa segurança se devem fundamentalmente às potencialidades e vulnerabilidades do SO adquirido à *Microsoft Corporation* (o *Windows NT*), somos levados a referir que a segurança nos SI simplesmente não existe.

Para além do referido foi detectado que não existe uma estratégia de segurança que percorra hierarquicamente, de cima para baixo, a estrutura do Exército, isto é, não existe ao mais alto nível da hierarquia a definição de normas e procedimentos quanto ao tratamento e manuseamento da informação em formato digital em segurança e do nível de responsabilidades atribuídas aos escalões subordinados, para que esses, nas suas áreas de actuação, procurem desenvolver esforços na mesma direcção e de acordo com os objectivos de segurança definidos superiormente.

Neste contexto, surge a segunda questão formulada inicialmente "Que alteração a implementar no desenho dos SI no Exército de forma a proporcionar-lhe segurança?" Assim, pretende-se neste capítulo apresentar as principais ideias que concorrem para a construção de um potencial modelo ou desenho arquitectural de forma a proporcionar requisitos de segurança aos SI no Exército. Na certeza de que, para a construção de um desenho de segurança de um sistema, é necessário percorrer várias fases e que estas se relacionam entre si, algumas fases não poderão ser iniciadas e concretizadas antes do fim da fase anterior.

Desta forma, estabelecem-se os seguintes passos considerados como fundamentais para a construção de um modelo inicial de segurança:

- definição de uma política de segurança da informação;
- análise de riscos;
- formulação de uma política de segurança;
- adopção de medidas indispensáveis de segurança passiva.

4.1 DEFINIÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A tarefa primordial a desenvolver, face às novas realidades do campo da informática, face ao progresso das tecnológicas de informação existentes e aos novos meios de armazenamento da informação, é a reformulação e actualização do único documento existente sobre a segurança de matérias classificadas, as Instruções para a Segurança Militar (SEGMIL-1, elaborado pelo EMGFA em 1986), que trata da salvaguarda e defesa de matérias classificadas e define os princípios básicos, normas e procedimentos considerados fundamentais para garantir a protecção das matérias classificadas.

Actualmente a informação, não só está registada em documentos em formato papel, como também em outros tipos de meios que, pelas suas características, podem constituir-se como um meio de armazenamento, nos quais a informação pode ser registada ou exibida. Estes meios podem ser os dispositivos magnéticos, como são os exemplos de disquetes, cassetes video, *Hard disk*, os discos removíveis e *cartridges*, os filmes registados em vários formatos ou dispositivos, o registo em fontes ópticas, onde podem ser armazenadas grandes quantidades de informação como é o caso dos discos compactos, do *cd-rom*, do *laser disks* e do *optical disks*.

Após a reformulação e actualização do documento orientador da política de segurança da informação, este deve ser dado a conhecer a todos os elementos da organização, através da distribuição do próprio documento escrito ou através de outros meios de armazenamento referidos, palestras, acções de formação ou individualmente caso seja necessário.

A elaboração do documento oficial que define a política de segurança da informação para as FA permite prosseguir para os passos seguintes da construção de um modelo inicial de segurança, perfeitamente enquadrados com os objectivos e finalidades da segurança da informação para a organização.

4.2 ANÁLISE DE RISCOS

Com o conhecimento sobre a orientação a seguir relativamente ao tratamento da informação, parte-se para a tarefa mais agreste do percurso de definição de segurança: a elaboração de um relatório de análise de riscos que tem como objectivo principal identificar e especificar as protecções recomendadas para os recursos de SI existentes, ou seja, identificar as vulnerabilidades e ameaças que possam colocar em risco o ambiente que envolve as TI e avalizar recomendações de segurança que possam aumentar o nível de confidencialidade, disponibilidade e integridade das informações. Com este relatório pretende-se definir que áreas de informação devem ser protegidas, quem são os responsáveis por protegê-las, e como devem ser protegidos

estes recursos.

O primeiro passo a dar na análise de riscos é definir quais os objectos a proteger, esta definição é fundamental para os estudos subsequentes pois é a partir destes que se parte para o levantamento de ameaças e vulnerabilidades. Cada objecto definido deve ser estudado e analisado individualmente, de forma a analisar as ameaças externas e as internas à organização, as físicas (face à destruição, roubo, modificação) e as técnicas (de ataques a BD e de simuladores) e serem analisadas as vulnerabilidades relativamente a defeitos, funcionamentos incorrectos[40], sistemas de segurança inadequados ou desactualizados e sistemas operativos desactualizados ou desadaptados. Determinadas as ameaças e as vulnerabilidades, é com a sua conjugação que se obtêm os riscos com que temos que lidar, o objectivo é minimizá-los de forma a não descurar a segurança, não esquecendo que existem sempre os riscos residuais e é com estes que temos de continuar a trabalhar.

Atingir uma situação em que as vulnerabilidades e os riscos sejam nulos é impossível, pelo que se recomenda uma definição do grau de tolerância a intrusões, abranger uma capacidade apropriada na detecção das ameaças mais críticas e dispor de capacidades de reacção e de recuperação conciliáveis com as ameaças mais perigosas detectadas. A tónica de segurança deve ser colocada na prevenção, no sentido de serem estudados os ataques e de colmatar, continuamente, as vulnerabilidades.

4.3 FORMULAÇÃO DE UMA POLÍTICA DE SEGURANÇA

O maior desafio colocado à segurança é a definição de a quem e onde a informação deve ser disponibilizada, o que nos induz a pensar que a segurança é um problema relacionado com as pessoas pois são estas que utilizam os SI e têm acesso às áreas críticas.

A base de uma política de segurança é a definição do comportamento autorizado para todos os elementos que interagem com um determinado sistema. O objectivo básico de uma política de segurança é informar esses elementos do que devem fazer e proteger em relação aos recursos tecnológicos e de informação da organização; essa prática de segurança deve deixar claros os mecanismos através dos quais isso pode ser conseguido, bem como explicar como configurar, manter e avaliar sistemas para que essa política se mantenha consistente. Assim, a política de segurança define o que é, e o que não é permitido em termos de segurança, durante a vida útil de um dado sistema.

[40] Do inglês *bugs.*

A política de segurança deve incluir regras detalhadas, definindo o modo como as informações e recursos da organização devem ser manipulados ao longo de seu ciclo de vida, ou seja, desde o momento que passam a existir no contexto da organização até ao momento em que deixam de existir. Esta política deve servir como instrumento de comunicação e informar sobre o que é necessário fazer quando se tiver que tomar decisões que envolvam aspectos de segurança, por isso é importante que a política seja explícita e clara sobre o porquê das decisões que foram tomadas e definir expectativas e responsabilidades entre todos os elementos da organização de forma a que todos tenham conhecimento do que se espera de cada um.

A implementação de uma política de segurança baseia-se na aplicação de regras que limitam o acesso de uma entidade às informações e recursos, com base na comparação do seu nível de autorização relativo a essa informação ou recurso, na designação da sensibilidade da informação ou recurso e na forma de acesso utilizada.

Um sistema é considerado seguro em relação à política de segurança, caso garanta o cumprimento das leis, regras e práticas definidas nessa política. A definição de uma política de segurança é fundamental; a inexistência deste documento traduz a ausência de linhas gerais estratégicas referentes à problemática da segurança dos SI, reflectindo-se de forma negativa nos desenvolvimentos de sistemas que são efectuados revelando-se estes, após um curto prazo de tempo, ineficazes para os objectivos da organização.

O documento a elaborar sobre a implementação de uma política de segurança deve abranger os objectivos, condutas, normas e métodos de actuação e distribuição de responsabilidades de forma a englobar tipicamente as áreas que têm maior impacto na rotina do utilizador, correio electrónico, serviços internet, vírus informáticos, classificação de documentos, arquivo de informação, acesso físico, acesso lógico, níveis de responsabilidades dos utilizadores, etc.. Em cada uma destas áreas devem ser definidas políticas de utilização, bem como as medidas necessárias no sentido de garantir os níveis de segurança pretendidos. Por isso, o documento deve contemplar a definição de princípios gerais de segurança, de normas e procedimentos e de um plano de monitorização (apoiado em listas de itens a serem verificadas).

A introdução deste tipo de documentos na organização deverá ser feita de uma forma faseada. Assumindo que a inexistência deste documento reflecte uma tolerância total de utilização das infra-estruturas, a sua implementação coloca restrições aos hábitos dos utilizadores, pelo que a implementação por fases diminuirá o impacto dessas restrições, ainda desta forma, será possível obter resultados mais rapidamente.

Apresentamos a seguir os contributos, com base no trabalho de campo, que são mais prementes não só para a elaboração do documento definidor da política de segurança, mas

também face à urgência que se descortinou para alteração no controlo de acessos implementado actualmente nos SI[41].

A forma como a informação é transmitida entre utilizadores requer também que se teçam alguns comentários correctivos para melhorar a sua performance, o que nos permite avançar com uma proposta de utilização da aplicação "SecNet" para o tratamento da informação em segurança em qualquer tipo de redes.

4.3.1 ACESSOS LÓGICOS

O controlo de acesso às aplicações e dados deverá continuar a ser feito pela utilização de uma ou mais password, pois este sistema é o mais económico e é o que actualmente o SO proporciona. No entanto, a gestão de password[42] deverá cumprir os seguintes requisitos:

- ter um mínimo de seis caracteres de comprimento;
- ser uma mistura de caracteres alfanuméricos, com a utilização de maiúsculas e minúsculas e caracteres gráficos disponibilizados pelos teclados standard[43];
- ser alterada todos os três meses, pelo menos;
- ser facilmente substituída quando for comprometida a sua segurança;
- as password não serão compartilhadas ou divulgadas a pessoas sem autorização ou expostas em qualquer tipo de ocasião;
- palavras conhecidas, nomes, aniversários etc. não devem ser usadas como password.

Para cada sistema que envolva mais do que um utilizador, deverá existir um responsável nomeado pelos restantes utilizadores de forma a ser aquele a autorizar o acesso. As password, sempre que possível, devem ser memorizadas e não serem escritas. Deve existir um duplicado das password das actividades críticas, este deve ser lacrado num envelope, este envelope deverá ser guardado em lugar seguro e deverá ter o mesmo nível de segurança que o nível mais alto dos dados envolvidos nessas actividades.

Relativamente ao controlo de acesso dos administradores, estes deverão ter pelo menos dois sistemas de identificação complementares. A utilização de acesso por objecto lógico e a utilização de uma password parece a mais racional[44], o primeiro por não envolver posse de

[41] O facto de serem apresentados baseados em informações resultantes de investigação, não inviabiliza que se efectuem estudos, à *posteriori*, para a sua aceitação e viabilidade seguindo os passos apresentados para a construção de um modelo inicial de segurança.
[42] Em Anexo M – "Gestão do controlo de acesso por password" são abordados mais considerandos que complementam a gestão de password.
[43] Na tabela A ou na figura 5 em Anexo A apresentam-se os resultados obtidos para a comparação e escolha do número de caracteres da Password.
[44] Racional na medida em que não foram feitos estudos de custo-eficácia que permitissem referir com exactidão qual o custo dos sistemas de segurança adequados face à informação que se pretende proteger.

qualquer objecto ou recurso a equipamentos adicionais (normalmente muito caros) e a segunda por ser disponibilizada pelos SO actualmente comercializados. As password deverão ser limitadas e controladas na medida das necessidades básicas de ter conhecimento, mudadas mensalmente, escritas e lacradas num envelope que deverá ser disposto num nível de protecção proporcional com a classificação mais alta da informação a que está autorizado. E, quando praticável, os administradores devem ter uma password de utilizador comum, para o trabalho de rotina, permitindo-lhe ter acesso a áreas ou aplicações necessárias ao seu trabalho do dia a dia.

4.3.2 TRANSMISSÃO DA INFORMAÇÃO EM SEGURANÇA

Durante o trabalho de campo foi detectado que a informação pode ser enviada através de qualquer tipo de canal de comunicações ou ser transportada manualmente utilizando disquetes, por isso, julgamos ser necessário apresentar alguns comentários para colmatar problemas de segurança que possam surgir.

Relativamente à informação quer transportada via disquetes quer enviada através do SITEP impõe-se a utilização de um algoritmo de cifra aplicado aos ficheiros que contêm essa informação, pelo que se impõe a certificação do algoritmo a ser utilizado no Exército.

O transporte das disquetes implica certos cuidados de manuseamento, pelo que deve ter-se em atenção a credenciação dos responsáveis pelo transporte, a forma como a disquete é entregue e os respectivos protocolos de entrega.

O correio electrónico e a emissão de documentos electrónicos deve ser estimulado. Para que a sua transmissão se opere em segurança devem ser introduzidas modalidades de assinatura digital produzidas através de técnicas criptográficas.

Em complemento desse estímulo pode-se recorrer à utilização de uma PKI para criar um sistema de troca de informação electrónica para as FA em geral e para o Exército em particular. Neste caso, a utilização da aplicação SecNet, apresentada anteriormente, pode-se constituir como a solução ideal para a concretização dessa PKI.

Para que esta solução seja possível é necessário que se cumpram duas condições, a primeira é a existência de uma entidade certificadora (conforme o Dec-Lei n.º 290-D/99 de 2 de Agosto), pelo que é necessário elaborar um pedido a apresentar à autoridade credenciadora de assinaturas digitais, o Instituto das Tecnologias de Informação da Justiça (ITIJ) que exerce as funções de autoridade credenciadora (conforme o Dec-Lei n.º 234/2000, de 25 de Setembro) permitindo constituir-se uma entidade certificadora de assinaturas digitais para as FA, de forma a exercer a actividade num quadro legal e serem reconhecidos em termos jurídicos os documentos

digitais e as chaves criadas e de forma que os certificados digitais emitidos cumpram os requisitos legais em vigor (em virtude de falta de legislação e da necessidade de existirem reuniões entre os Ramos para uma definição da entidade certificadora não é possível apresentar uma solução sobre este assunto). A segunda condição é a criação de uma autoridade de acreditação de sistemas.

4.4 MEDIDAS DE SEGURANÇA PASSIVA

As medidas de segurança passivas que foram abordadas no presente estudo[45], podem ser colocadas em prática em determinadas alturas do desenho arquitectural de segurança.

A fase da formação dos RH não é imperiosamente activada no final de uma outra fase qualquer, esta poderá ser realizada a qualquer altura, durante o processo de construção do modelo, pelo que poderemos referir que se trata de uma etapa de sensibilização de segurança de todos os elementos da organização, como é o caso da fase de definição de uma política de segurança da informação em que a necessidade de dar formação ou sensibilizar os RH em certas áreas pode ser indispensável. O mesmo não se passa relativamente à formação de técnicos de segurança, neste caso apenas se podem determinar as áreas específicas de formação necessárias após a elaboração do documento da política de segurança.

Em relação às auditorias de segurança, apesar de estas se tornarem mais eficazes a partir do momento da aceitação do documento sobre a política de segurança definida para os sistemas em estudo e da colocação em prática do preconizado no documento, as auditorias poderão tornar-se úteis se forem executadas durante as fases de implementação do desenho de segurança, exercendo um controlo de execução durante as fases de implementação.

Relativamente aos PCR, estes devem fazer face a qualquer evento fatal ou sucessão de eventos que coloquem em risco os processos vitais para a consecução dos objectivos principais da organização. Por isso é necessário prever o restabelecimento da actividade dos sistemas críticos, mesmo que parcialmente, no caso do desastre se efectivar. A ausência ou desactualização de um PCR contribui para um menor nível de qualidade nos SI na eventualidade de, em caso de desastre, não se conseguir recuperar a informação na totalidade, nem colocar os sistemas operacionais no mais curto espaço de tempo.

Ao diminuir as consequências dos acidentes, estão-se a diminuir as eventuais perdas advindas da paragem do SI. A avaliação das potenciais consequências de um acidente deverá ser

[45] Os planos de contingência e recuperação, as auditorias de segurança e a formação dos RH.

sistémica, isto é, devem-se procurar avaliar os efeitos nas diferentes áreas críticas da organização e equacionar todo o tipo de consequências, incluindo as de ordem ética e legal.

Dada a impossibilidade de prever acidentes que possam provocar a interrupção dos SI, a eficácia de um PCR depende consideravelmente da sua constante actualização em função das alterações efectuadas nos respectivos SI devendo ser encarado de uma forma dinâmica, nunca como um produto acabado.

Para a elaboração do PCR, é necessário que sejam levantados alguns itens básicos, como os:

- sistemas críticos que garantem a continuidade da actividade principal da organização;
- recursos de hardware, software e infra-estrutura de que esses sistemas dependem;
- levantamento e actualização da documentação dos sistemas mais críticos;
- definição e tipificação dos dispositivos de *backup*;
- decisões pós-desastre e a forma de evitar novos prejuízos executando os procedimentos de emergência;
- procedimentos indispensáveis para a recuperação dos sistemas afectados.

Deste modo o PCR apenas poderá ser elaborado quando forem percorridos os caminhos para alcançar os objectivos de segurança dos sistemas. Assim, a sua elaboração ou inclusive a decisão de quantos PRC, repartidos pelas áreas críticas, serão necessários, só é possível após a detecção e análise dos riscos, o estabelecimento e definição da política de segurança, a execução da política de segurança e o respectivo acompanhamento de implementação, a avaliação dos resultados face aos objectivos traçados e a validação dos objectivos da política de segurança.

5. PROPOSTA DE UMA METODOLOGIA PARA A IMPLEMENTAÇÃO DE SEGURANÇA NOS SISTEMAS DE INFORMAÇÃO

Neste capítulo, complementar do anterior, apresentam-se os subsídios para a implementação da segurança dos SI. Seguindo o racional das medidas preconizadas anteriormente, este capítulo tem como objectivo formular ideias conducentes à alimentação das incitações descritas nos pontos do capítulo anterior.

Por conseguinte, socorrendo-nos do racional seguido ao longo do trabalho, impõe-se que, para a construção do modelo inicial de segurança, sejam referidas qual ou quais as entidades que encabeçarão as responsabilidades pela persecução das tarefas principais em cada passo do modelo, isto é, qual a Entidade Primariamente Responsável (EPR). Assim, vão ser focados os seguintes aspectos:

- a reformulação das instruções para a segurança militar;
- a elaboração da política de segurança, que envolve as responsabilidades da análise de riscos, a área dos sistemas de segurança a implementar e os PCR;
- o estabelecimento de auditorias de segurança;
- a criação de uma autoridade de acreditação no Exército.

Terminaremos o trabalho de investigação com a apresentação de um calendário das actividades a desenvolver que reflicta os passos apresentados para a construção do modelo inicial de segurança.

5.1 PROPOSTA DE REFORMULAÇÃO DAS INSTRUÇÕES PARA A SEGURANÇA MILITAR

A reformulação do SEGMIL-1 é quase uma imposição que a estrutura superior das FA tem que integrar no seu planeamento, pelo que, a constituição de um grupo de trabalho que envolva os Ramos (Marinha, Exército e Força Aérea) é uma exigência para a elaboração deste projecto.

No que diz respeito ao Exército, e comummente aos outros Ramos, o EME deve designar para integrarem o grupo de trabalho a Divisão de Pessoal (DP) a DIM e a DCSI com o intuito de representarem as áreas de interesse que concorram para a segurança dos SI no Exército, nomeadamente, nas áreas de instrução e segurança da informação classificada, segurança do pessoal, segurança física, segurança informática e dos SI e segurança das comunicações.

5.2 PROPOSTA DE ELABORAÇÃO DA POLÍTICA DE SEGURANÇA

A política de segurança para os SI no Exército deve ser definida pela entidade cuja responsabilidade de desenvolver estudos dos SI, sob o ponto de vista informático, recai no seio do Exército, pelo que o CIE será a entidade que terá a competência de elaborar o relatório de análise de riscos, definir as regras de segurança para cada sistema, que se constituirão como princípios gerais, estudar as normas ou especificações técnicas para cada uma dessas regras e desenvolver processos de verificação dessas regras e normas de forma a possuir todos os indicadores para elaborar o documento da política de segurança para os SI no Exército.

Uma outra área que foi considerada neste estudo como medida de segurança passiva, a elaboração de PCR, não será responsabilidade apenas de uma entidade, pelo que devem ser desenvolvidos esforços para que nas áreas onde os SI possam considerar-se críticos sejam elaborados PCR. No entanto, o CIE deve constituir-se como a EPR neste processo, não só na elaboração dos PCR de cada sistema em utilização, como também junto das entidades que são apoiadas pelos SI desenvolvidos ou adquiridos, na responsabilidade sobre a elaboração de PCR das diversas actividades críticas nas áreas de pessoal, logística, finanças e instrução.

As competências e responsabilidades impostas ao CIE, conjugadas com a falta de uma repartição ou secção de segurança de sistemas na sua estrutura, para poder em tempo colaborar no desenvolvimento e acompanhamento de projectos e de elaborar pareceres técnicos sobre segurança de sistemas, podem constituir-se como o grande entrave à preparação do modelo inicial de segurança. Essa repartição ou secção deve ser criada e ter uma participação activa nas áreas de segurança e reger-se pelos seguintes princípios básicos:

- aprovar as exigências de segurança de SI;
- planear as actividades relativas à segurança dos SI;
- participar na credenciação, que é o processo da aceitação dos sistemas que obedecem ao quadro legal e exigências de segurança definidos;
- aprovar ligações com o exterior das instalações, serviços ou organizações;
- inspeccionar, examinar e medir o desempenho dos planos de segurança;
- aconselhar sobre os riscos à segurança durante o processo de elaboração dos projectos dos SI;
- monitorizar e analisar os ataques à segurança do SI;
- investigar quebras de segurança detectadas ou suspeitas.

5.3 PROPOSTA DE CRIAÇÃO DE UMA AUTORIDADE DE ACREDITAÇÃO

As potencialidades da aplicação criptográfica "SecNet" são inúmeras, podendo transformar-se na solução procurada para terminar com a definição e diferenciação entre Centros Criptos e Centros de Mensagens, há já muito tempo que se pensa na sua integração mas, até hoje, com resultados pouco práticos (o que se fez actualmente foi apenas a sua integração física).

O aproveitamento das potencialidades desta aplicação na reformulação dos circuitos de troca de informação classificada entre entidades pode ser a chave para terminar com a duplicação de tarefas dos serviços (que zelam pelos documentos classificados e não classificados) que estão incumbidos do encaminhamento da informação no Exército.

Para isso, é necessário que exista uma entidade de acreditação de sistemas. Essa autoridade, que terá a designação de Autoridade de Acreditação e Segurança no Exército (AASE), terá a competência de aprovar e acreditar os SI no Exército, a autoridade será representada pelo Vice-Chefe do Estado-Maior do Exército (VCEME), este por seu lado, terá um órgão para avaliar tecnicamente os sistemas, designado por Comissão Técnica de Segurança (CTES). Este órgão terá a competência de emitir os certificados dos SI para serem submetidos à AASE.

A CTES deverá ter a seguinte composição: a DIM e a DCSI do EME, o Subdirector da DST, o Subdirector da DSE, o Director do CIE e o Comandante do BISM. O apoio técnico deve ser garantido pelos órgãos sobre a sua dependência ou a criar na sua falta, como é o caso do CIE. Devido aos estudos e experiências técnicas que terão de se efectuar, devem ser criadas condições para a possibilidade de existirem acordos com universidades e empresas que trabalhem em estudos técnicos em áreas específicas da segurança, estas entidades deverão estar certificadas pelo Gabinete Nacional de Segurança (GNS).

5.4 PROPOSTA DE ESTABELECIMENTO DE AUDITORIAS DE SEGURANÇA

Ao ser definida a política de segurança, a sua colocação em prática obriga a que existam mecanismos para apoiar os elementos da organização no desempenho das suas actividades. Para isso será indispensável a criação de um núcleo de auditorias de forma a proporcionar análises, avaliações, recomendações, assessoria e informação correspondente às actividades examinadas.

A missão dessa equipa de auditoria[46] será a de proporcionar um serviço de avaliação construtiva de todas as actividades da organização, por conseguinte, deverá seleccionar as

[46] Em Anexo N é apresentada uma lista-tipo de verificação do plano de segurança.

operações e actividades que serão submetidas à auditoria e que potencialmente possam beneficiar com as acções de auditoria efectuadas.

O produto final da auditoria é informar, com base em evidências, os responsáveis pelas áreas sujeitas a estudo sobre se os seus sistemas de segurança são eficientes e efectivos, assim como oferecer um conselho ou assessoramento documentado de como conseguir que ditos sistemas o sejam. Assim, pelo tipo de actividades desenvolvidas e pela especificidade das áreas a serem tratadas, a equipa de auditorias deverá ser constituída por elementos específicos a nomear pela DCSI/EME que se constituirá como a EPR neste processo.

5.5 PROPOSTA DE CALENDARIZAÇÃO

Para finalizar este trabalho apresenta-se o mapa onde são representadas as actividades que concorrem para a construção do modelo inicial de segurança no Exército. A representação gráfica vai ser apresentada em termos de data de início e de fim de actividades escalonadas ao longo do eixo horizontal; no plano das ordenadas são apresentadas as actividades e, quando aplicável, as respectivas EPR pelas mesmas.

Data / Actividades	Meses: 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Política de segurança da informação	EMGFA[47]
Análise de riscos	CIE
Política de segurança	CIE
Controlo de acessos	CIE
Formação de RH	Actividades de formação[48] e sensibilização[49]
Auditorias	Constituição de equipas (DCSI)
PCR	CIE[50]
Criação da CTES	DCSI[51]

[47] Grupo de trabalho constituído por equipas do EMGFA e dos Ramos com a representação da DP, DIM e DCSI do EME.
[48] O Comando de Instrução deve promover e desenvolver esforços para que a formação em segurança seja programada.
[49] Todos os elementos das U/E/O devem ter iniciativas neste campo nomeadamente as entidades responsáveis pelas áreas de instrução.
[50] O CIE deve constituir-se como a EPR neste processo; os Comandos de Pessoal, Logística e Instrução têm à sua responsabilidade a elaboração dos PCR das respectivas áreas de competência.
[51] A DCSI deve coordenar a constituição da comissão técnica com DIM, o Subdirector da DST, o Subdirector da DSE, o Director do CIE e o Comandante do BISM.

5.6 CONSIDERAÇÕES FINAIS

Com este trabalho podemos constatar que tipo de segurança está desenhada nos SI de gestão e operacionais do Exército e as grandes lacunas existentes no tratamento da informação, no controlo de acessos e no transporte dessa informação.

Face ao grande hiato encontrado no desenho de segurança existente nos actuais sistemas de segurança implementados, fomos levados a apresentar um modelo inicial de segurança que permite estabelecer as actividades principais a desenvolver e as respectivas autoridades responsáveis pela sua concretização.

Finalmente, esperamos que a DCSI desenvolva esforços para que seja possível ver concretizado o modelo que se apresentou e que, após os dois anos que se prevê para o término das actividades, seja possível dizer que existe segurança nos SI no Exército.

BIBLIOGRAFIA

1. Livros

- ARIMA, Carlos H., Metodologia de Auditoria de Sistemas, Érica Editora, 1994.
- FEGHHI, J. e P. Williams, *Digital Certificates Applied Internet Security*, Addison Wesley, 1999.
- FERREIRA, Jorge, *Normas Técnicas de Segurança dos Sistemas e Tecnologias de Informação,* Instituto de Informática, SIG Lda, 1995.
- PEREIRA, José Luís, *Tecnologias de Informação*, *Tecnologias de Bases de dados*, 3ª Edição, FCA – Editora de Informática, Outubro de 1998.
- RASCÃO, José Poças, *Análise Estratégica – Sistema de Informação para a Tomada de Decisão*, Lisboa, Edições Sílabo, 2000.
- STALLINGS, William, *Cryptography and Network Security*, *Principles and Practice*, Prentice Hall, 1999.
- VARAJÃO, João Eduardo Quintela, *A Arquitectura da Gestão de Sistemas de Informação*, Lisboa, FCA – Editora de Informática, Agosto 1998.

2. Documentação institucional

- MINISTÉRIO DA CIÊNCIA E TECNOLOGIA, Decreto-Lei n.º 290-D/99 de 2 de Agosto de 1999: *aprova o regime jurídico dos documentos electrónicos e da assinatura digital*.
- MINISTÉRIO DA DEFESA NACIONAL, Decreto Regulamentar n.º 43/94 de 2 de Setembro de 1994: *Estabelece as atribuições, organização e competências do Estado-Maior do Exército.*
- MINISTÉRIO DA DEFESA NACIONAL, Decreto Regulamentar n.º 47/94 de 2 de Setembro de 1994: *Estabelece as atribuições, organização e competências dos comandos territoriais, do Comando das Tropas Aerotransportadas, das unidades, estabelecimentos e órgãos territoriais e dos campos de instrução.*
- MINISTÉRIO DA DEFESA NACIONAL, Decreto-Lei n.º 217/97 de 20 de Agosto de 1997: C*ria o Gabinete Nacional de Segurança (GNS) e determina as suas competências*.

- NORTH ATLANTIC COUNCIL, Document AC/322-D/30: NATO INFOSEC technical and implementation directive for the interconnection of communication and information system, de 2 de Fevereiro de 2000.
- NORTH ATLANTIC COUNCIL, Document AC/35-D/1017: *Guide lines for ADP security risk analysis*, de 17 de Novembro de 1993.
- O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA, Directiva 1999/93/CE de 13 de Dezembro de 1999: *quadro legal comunitário para as assinaturas electrónicas*.
- PRESIDÊNCIA DO CONSELHO DE MINISTROS, Resolução de Conselho de Ministros n.º 94/99 de 25 de Agosto de 1999: *aprova o Documento Orientador da Iniciativa Nacional para o Comércio Electrónico*.

3. Outros trabalhos

- ALVES, Carlos António, *Sistemas e Informação Tácticos no Exército Português, situação actual e perspectivas futuras*, TILD CSCD 2000/2001, IAEM, Lisboa, 2000.
- AUGUSTO, Cordeiro, *As informações militares e a sua inserção no sistema de informações nacional, que adaptações a introduzir*, TILD CEM 96/98, IAEM, Lisboa, 1997.
- REBELO, José António Coelho (Major), *Sistemas de Informação no Exército*, TILD CEM 95/97, IAEM, Lisboa, 1996.
- RIJO, Fonseca, Pardal dos Santos e Oliveira Ribeiro, *Medidas a implementar com vista ao total aproveitamento das possibilidades da internet*, Estudos Parcelares CEM 98/00, IAEM, Lisboa, 2000.

4. Artigos de revistas

- BIROS, David P. e Todd Eppich, "Human element key to intrusion detect", in *SIGNAL AFCEA's International Journal*, Agosto de 2001, pp. 31-33.
- CORREIA, Alberto José, "Segurança Informática. A perspectiva da OTAN", in *ANAIS do Clube Militar Naval*, Vol CXXIV, Tomo 10 a 12, Lisboa, Clube Militar Naval, Out a Dez de 1994, pp. 749-775.
- KENYON, Henry S., "Fusion center unites diverse research groups", in *SIGNAL AFCEA's International Journal*, Agosto de 2001, pp. 35-37.

- KENYON, Henry S., "New tricks for old threats", "Cyberwarfare blurs rules of engagement", in *SIGNAL AFCEA's International Journal*, Janeiro de 2001, pp. 43-46.
- LOWLOR, Maryann, "For security, the eyes have it", in *SIGNAL AFCEA's International Journal*, Março de 2001, pp. 56-59.
- SILVA, Álvaro, "Biometria", in *Informação & informática*, nº 25, 2000, Lisboa, Instituto de Informática, SIG Lda, pp. 34-43.
- VEIGA, Pedro M. Barbosa e Maria Dulce Domingues, "A segurança informática e as autoridades de certificação", in *Informação & informática*, n.º 24, 1999, Lisboa, Instituto de Informática, SIG Lda, pp. 47-51.

5. Conferência

- ALMEIDA, João Carreira, *Os sistemas de informação, o cidadão e o futuro, catões de identificação de acesso*, Seminário sobre "A actividade informática" "As ameaças à segurança" e a "protecção dos sistemas de informação", Instituto de Defesa Nacional, 16 e 17 Dezembro de 1999.
- TOMÁS, Nelson Manuel e José Gomes de Almeida, *A segurança da informação nas Grandes Organizações*, Instituto de Defesa Nacional, Seminário sobre "A actividade informática" "As ameaças à segurança" e a "protecção dos sistemas de informação", Instituto de Defesa Nacional,16 e 17 Dezembro de 1999.
- CUNHA, Alberto, "As tecnologias de informação – perspectivas de evolução", seminário sobre a segurança e protecção da informação, Instituto de Altos Estudos Militares, 15 e 16 de Outubro de 2001.
- CARDOSO, Luís Sousa, "Os sistemas de informação - análise de riscos", seminário sobre a segurança e protecção da informação, Instituto de Altos Estudos Militares, 15 e 16 de Outubro de 2001.
- MIRA da SILVA, Miguel, "A certificação digital - Aspectos técnicos", seminário sobre a segurança e protecção da informação, Instituto de Altos Estudos Militares, 15 e 16 de Outubro de 2001.

6. Internet

- AFCEA Internacional, http://www.afcea.org/, de 18 de Setembro de 2001.
- ANCAP, http://www.ancap.com.uy/portugues/auditor1.htm, de 5 de Setembro de 2001.

- BALTIMORE, Global E-security, http://www.baltimore.com/library/pki-es/index.html, de 10 de Setembro de 2001.
- BALTIMORE, Global E-security, http://www.baltimore.com/library/pki-es/pki-security.html, de 10 de Setembro de 2001.
- BALTIMORE, Technologies, http://www.baltimore.ie/unicert/pki/index.html, de 15 de Julho de 2001.
- BANESTO, http://www.banesto.es/banesto/certificacion/castella/c.htm, de 6 de Outubro de 2001.
- Brad Biddle's Home Page, http://www.acusd.edu/~biddle/, de 13 de Outubro de 2001.
- CERTIPOR, http://www.certipor.com/legislacao.html, de 10 de Setembro de 2001.
- Commonwealth of Massachusetts, Information technology Division, http://www.state.ma.us/itd/legal/pki.htm, de 15 de Julho de 2001.
- Computer Emergency Response Team - Rio Grande do Sul (CERT-RS), http://www.cert-rs.tche.br/docs_html/autentic.html, de 18 de Julho de 2001.
- CRIPTONOMICÓN, http://www.iec.csic.es/criptonomicon/articulos/criptologia.html, de 18 de Setembro de 2001.
- CRIPTONOMICÓN, http://www.iec.csic.es/criptonomicon/articulos/expertos74.html, de 18 de Setembro de 2001.
- CRIPTONOMICÓN, http://www.iec.csic.es/criptonomicon/articulos/expertos73.html, de 18 de Setembro de 2001.
- CRIPTONOMICÓN, http://www.iec.csic.es/criptonomicon/seguridad/default.html, de 18 de Setembro de 2001.
- DIGITO, *Segurança* biométrica, http://www.digito.pt/tecnologia/artigos/tecart61.html, de 10 de Setembro de 2001.
- Distributed Systems Technology Centre, Queensland University of Technology: PKI Project, http://www.dstc.qut.edu.au/MSU/projects/pki/index.html, de 15 de Julho de 2001.
- EUROPA Home Page, http://europa.eu.int/scadplus/leg/pt/lvb/l24121.htm, de 20 de Julho de 2001.
- GeP - Consultoria de Sistemas de Informação, http://www.gep.pt/, de 6 de Outubro de 2001.
- Grupo de Securidad y Criptografía, http://www.um.es/si/ssl/PKI/pki.html, de 6 de Outubro de 2001.

- Harvard Law School Center for Law & Information Technology, http://www.law.harvard.edu/groups/center_law/, de 18 de Julho de 2001.
- INFOJUR, http://ute.edu.ec/~mjativa/ce/seguridad.html, de 18 de Julho de 2001.
- Instituto das Tecnologias de Informação na Justiça, http://www.itij.mj.pt/default.asp, de 18 de Setembro de 2001.
- Intelligence Resourse Program, http://www.fas.org/irp/program/process/echelon.htm, de 18 de Setembro de 2001.
- International Biometric Group, Biometric Technology Offerings, http://www.biometricstore.com/a_biometrics_42/biometric_technology_offerings.asp, de 15 de Julho de 2001.
- ITL Bulletin, http://www.itl.nist.gov/lab/bulletns/archives/july97bull.htm, de 15 de Julho de 2001.
- JAIN, A.; Kulkarini, Y. A Multimodal Biometric Sustem Using Fingerprint, Face, and Speech, http://web.cps.msu.edu/, de 15 de Julho de 2001.
- JIMENEZ. Jose Alfredo, *Evaluación Seguridad de un Sistema de Información*, http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml, de 20 de Julho de 2001.
- KESSLER, G. Passwords - Strengths and Weaknesses, de 18 de Julho de 2001.http://www.hill.com/library/password.html, de 15 de Julho de 2001.
- Legal Information Institute (Cornell), http://www.law.cornell.edu/, de 18 de Julho de 2001.
- LÓPEZ, Manuel J. Lucena, *Criptografía y Seguridad en Computadores*, Tercera Edición (Versión 1.00), Junio de 2001, livro integral retirado de http://wwwdi.ujaen.es/~mlucena, de 16 de Junho de 2001.
- METHODUS, Parte integrante, http://www.methodus.pit.com.br/auditorias_sistemas.htm
- Missão para a Sociedade da Informação, http://www.missao-si.mct.pt, de 15 de Julho de 2001.
- MODULO E-security, http://www.modulo.com, de 18 de Julho de 2001.
- NIST, http://www.itl.nist.gov/lab/bulletns/archives/july97bull.htm, de 18 de Setembro de 2001.
- NIST's Computer Security Resource Clearinghouse: Public Key Infrastructure, http://csrc.nist.gov/pki/, de 5 de Setembro de 2001.
- NSI, http://www.nsi.org/, de 6 de Outubro de 2001.

- Revista Sistemas de Informação, http://www.apsi.pt/Revista/InfoRev/revista.html, de 18 de Setembro de 2001.
- REZENDE, Pedro António Dourado de, *Certificados Digitais, Chaves Púbicas e Assinaturas*, http://www.cic.unb.br/docentes/pedro/trabs/cert.htm, de 20 de Julho de 2001.
- ROB, McMillan, *Site Security Policy Development*, http://secinf.net/info/policy/AusCERT.html, de 19 de Julho de 2001
- RSA Data Security Inc., The most trusted name in e-Security, http://www.rsasecurity.com/, de 6 de Outubro de 2001.
- RSA Data Security, Inc. "*Frequently Asked Questions about Today's Cryptography"*, http://www.rsa.com, de 5 de Setembro de 2001.
- SEGURIDAD, Foro de profissionales latinoamericanos de seguridad, http://www.seguridad-la.com/, de 10 de Setembro de 2001.
- Shan Computers, Segurança Informática, http://www.shancomputers.com/security/apr.htm?183,165, de 13 de Outubro de 2001.
- Treasury Board of Canada Secretariat, http://www.cio-dpi.gc.ca/pki-icp/index_e.asp
- WINDERMERE, Information Assurance Division, http://iw.windermeregroup.com/infosec.html, de 13 de Outubro de 2001.

ANEXOS

A - Figuras

B - Evolução dos sistemas de criptografia

C - Os sistemas biométricos

D - Controlo de acesso por certificado digital

E - Funções *hash*

F - A criptografia como suporte da segurança

G - Sistema Integrado de Telecomunicações do Exército Português

H - Sistema de Comunicações

I - Situação dos projectos da responsabilidade do CIE

J - Algoritmos mais utilizados

K - O protocolo TCP

L - Características do SecNet

M - Gestão do controlo de acesso por password

N - Lista de política de segurança de informações

O - Guião das entrevistas

ANEXO A

FIGURAS

FIGURAS

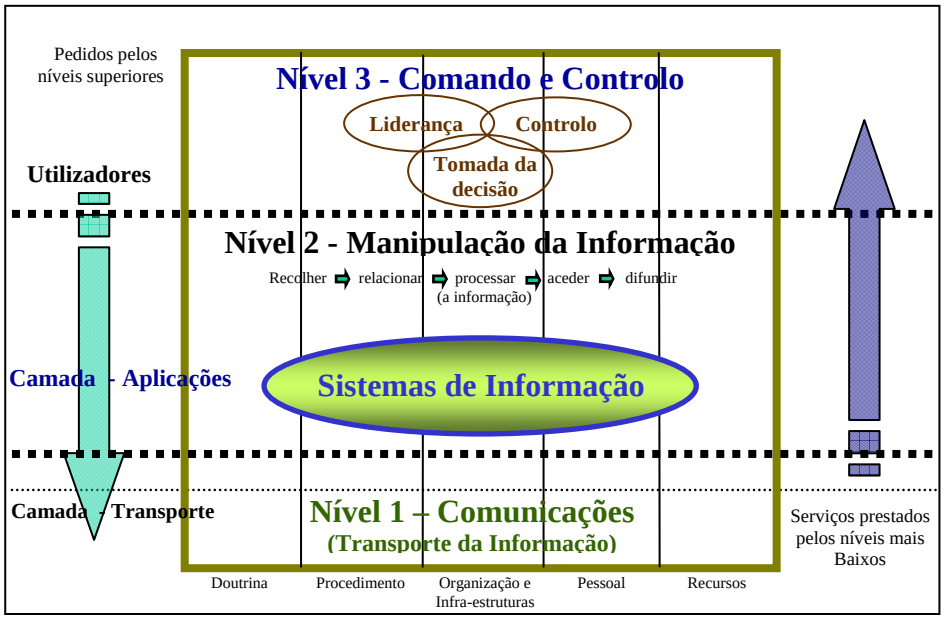


Figura 1 - Arquitectura de Sistemas de C2

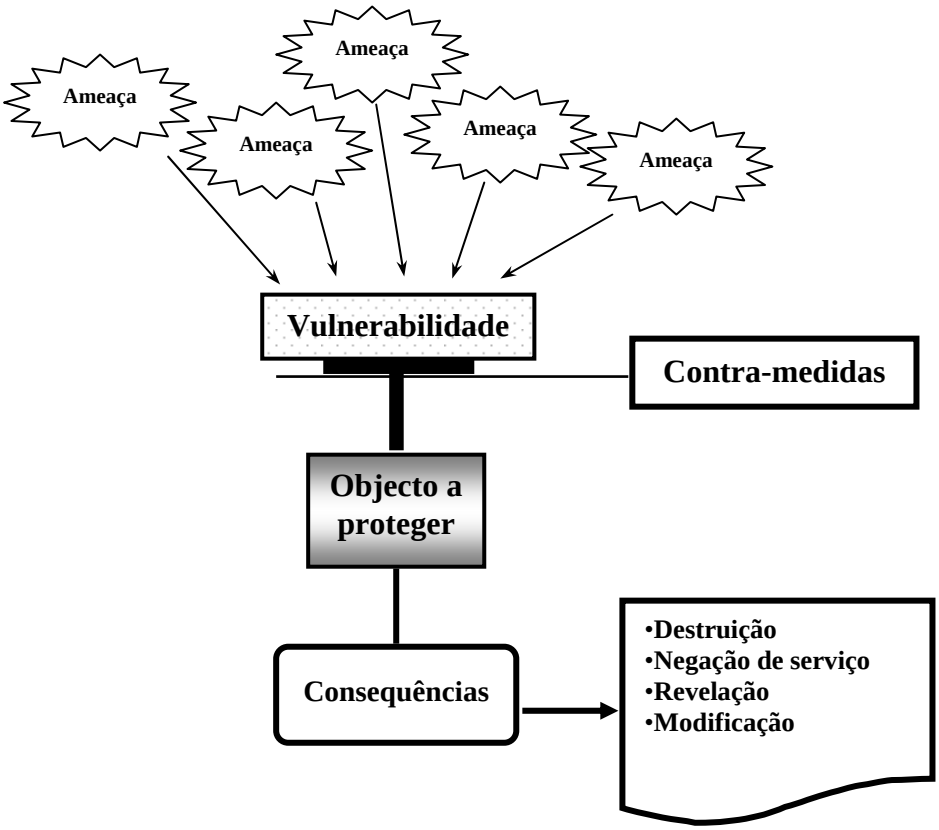


Figura 2 – Análise de riscos

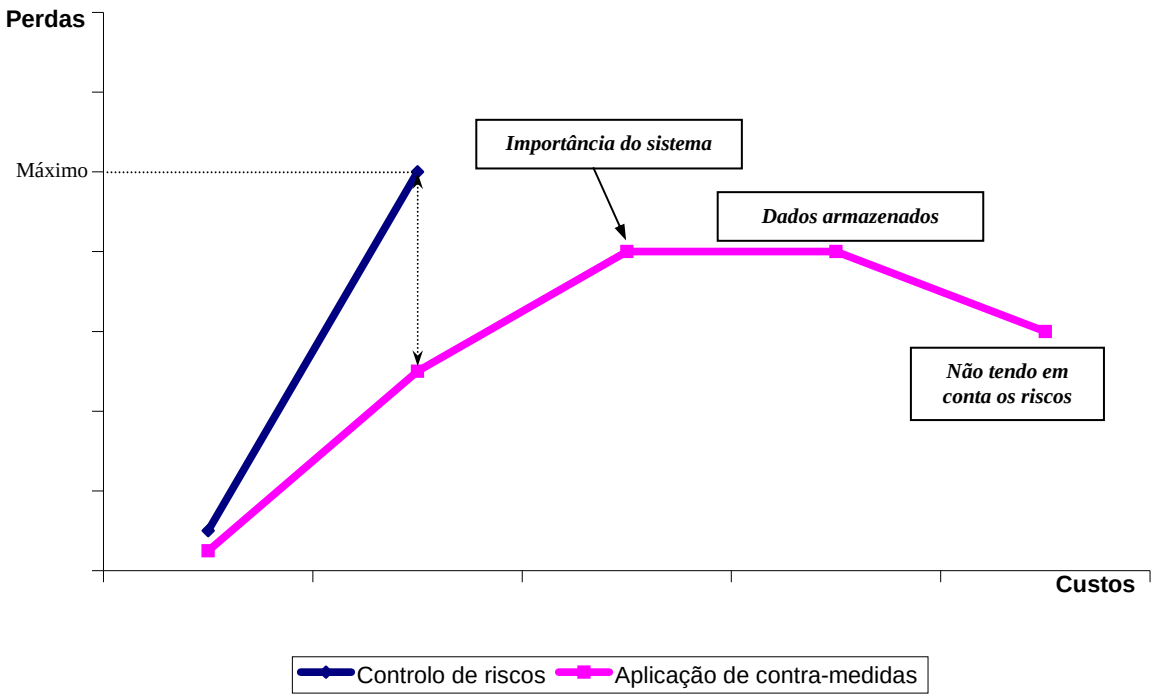


Figura 3 – Controlo de riscos versus contra-medidas

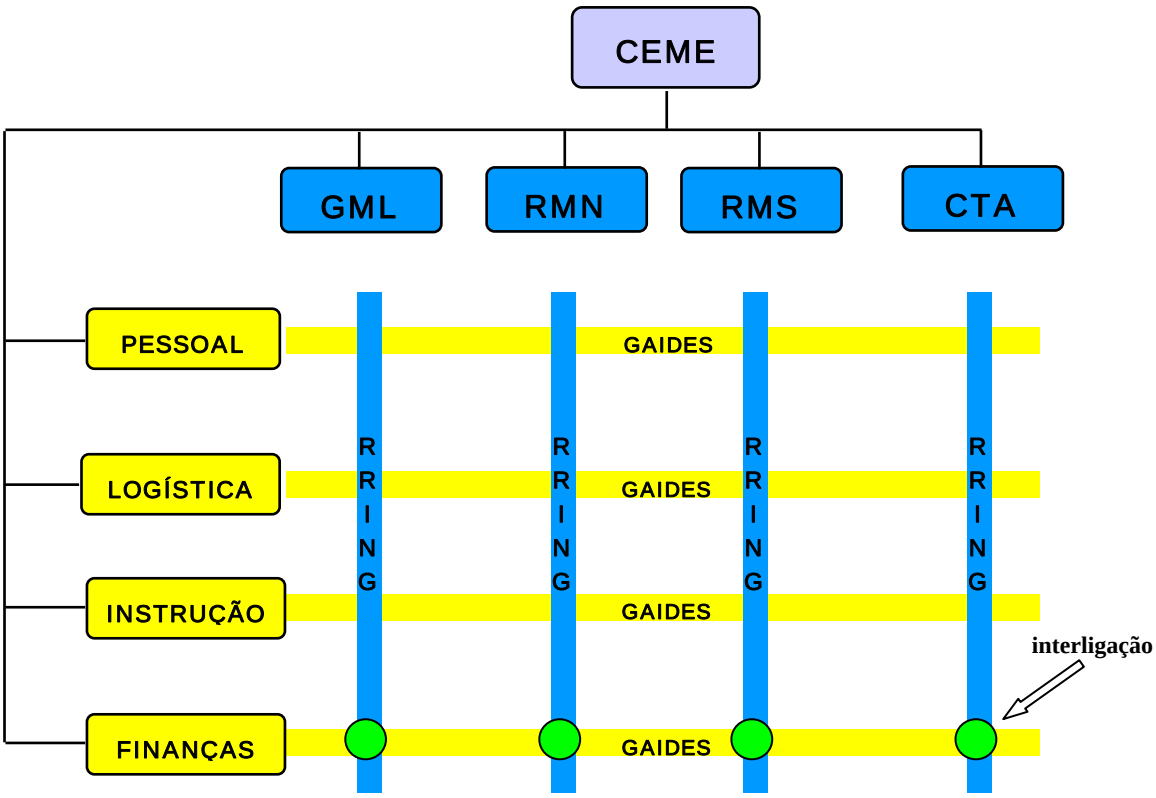


Figura 4 - A estrutura organizacional do Exército

	Número de caracteres da Password					
	1	**4**	**6**	**8**	**9**	**12**
A	10	10.000	1.000.000	1E+08	1E+09	1E+12
B	26	456.976	3,1E+08	2,1E+11	5,4E+12	9,5E+16
C	62	14.776.336	5,7E+10	2,2E+14	1,4E+16	3,2E+21
D	100	1E+08	1E+12	1E+16	1E+18	1E+24

Tabela A – Comparação do número de caracteres de password.

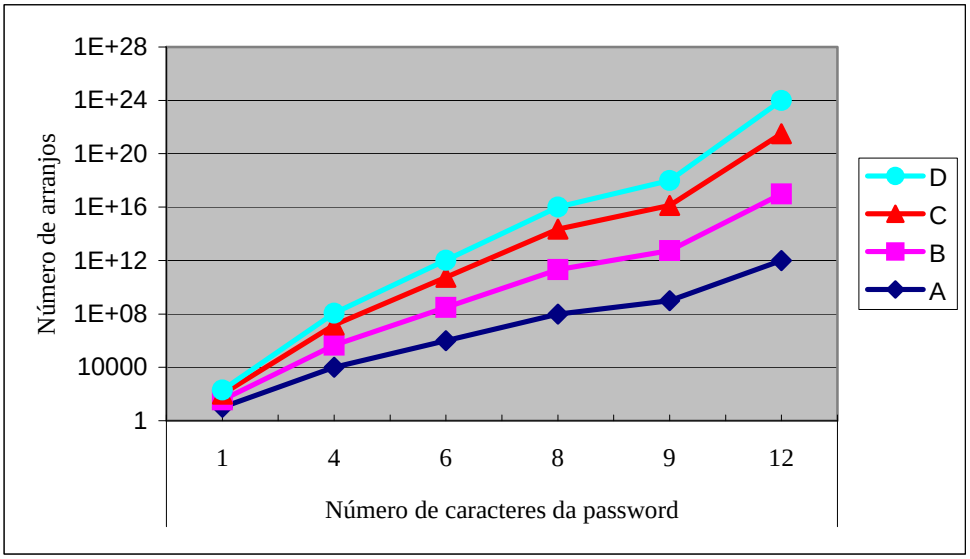


Figura 5 – Visualização gráfica comparativa do n.º de caracteres versus n.º de arranjos

A - Utilização de números
B - Utilização alfanumérica
C - Utilização de alfanumérica (c/ diferenciação de maiúsculas e minúsculas)
D - Utilização de maiúsculas e minúsculas e caracteres gráficos disponibilizados pelos teclados standard

ANEXO B

EVOLUÇÃO DOS SISTEMAS DE CRIPTOGRAFIA

EVOLUÇÃO DOS SISTEMAS DE CRIPTOGRAFIA

Neste Anexo pretende-se apresentar a evolução da criptografia, retratando alguns sistemas que se destacaram pela sua importância e influência para os actuais métodos de algoritmos criptográficos e ressaltando os métodos tradicionais mais antigos para aqueles que passaram a utilizar uma palavra como chave para cifrar.

1. OS PRIMÓRDIOS DA CRIPTOLOGIA

1.1 MÉTODO DE JÚLIO CÉSAR

É da época de Júlio César que aparecem os primeiros relatos de que uma língua, o latim, tenha sido tão popularizada como forma de comunicar através da escrita.

Com a utilização do latim na forma escrita pelos militares, surgiu a necessidade de esconder a informação que os papiros transportavam, desta forma aparece Júlio César com a ideia de distorcer a informação, para o destinatário posteriormente a voltar a colocar em ordem, ainda hoje esta ideia se considera como o primeiro criptograma conhecido.

O sistema, que é muito simples consiste em substituir cada letra por uma outra situada três posições mais à frente no alfabeto.

Por exemplo o E é substituído pelo H e o X substituído pelo A, no caso da seguinte frase:

INSTITUTO DE ALTOS ESTUDOS MILITARES

ficaria

MQVWMWYWR GH DOWRV HVXYGRV PMOMWDUHV

2. AS PRIMEIRAS PALAVRAS CHAVE

2.1 SISTEMAS MONOALFABÉTICOS

Neste sistema, cada letra é substituída por uma outra que ocupa a mesma posição num alfabeto desordenado, deste modo, é possível conseguir tantas formas de cifrar quantas possibilidades de constituir uma nova ordem para o alfabeto.

É um método mais evoluído que o de Júlio César e tem a hipótese de formar tantas chaves quantas as possibilidades de formar um alfabeto desordenado.

Este método tem um grave problema que é como relembrar a ordem do novo alfabeto desordenado. Para isso, recorre-se ao uso de uma palavra de utilização comum, permitindo criar

um alfabeto desordenado. Na prática não é construído um novo alfabeto, mas sim, a utilização de palavras comuns como chave do criptograma.

O sistema funciona da seguinte maneira:

a. procura uma palavra (chave) fácil de relembrar e retiram-se as letras repetidas;
   MILITARES ---- MILTARES
b. acrescentam-se no final da palavra, sem repetições, as restantes letras do alfabeto;
   MILTARESBCDFGHJK ..... XYZ
c. ordena-se uma matriz cuja primeira linha é a palavra chave

M	I	L	T	A	R	E	S
B	C	D	F	G	H	J	K
N	O	P	Q	U	V	W	X
Y	Z						

d. o novo alfabeto é constituído por colunas, ficando da seguinte forma
   MBNYICOZLDPTFQAGURHVEJWSKX

2.2 *PLAYFAIR*

O sistema *Playfair* foi inventado em 1854 por um britânico chamado *Sir Charles Wheastone*. É um sistema baseado em grupos de duas letras que utiliza uma palavra chave e uma matriz de 5x5. Vejamos um exemplo para melhor compreender este sistema:

CHAVE: MILITARES ---- MILTARES

Matriz 5x5:

M	I/J	L	T	A
R	E	S	B	C
D	F	G	H	K
N	O	P	Q	U
V	W	X	Y	Z

em que o I e a J compartem a mesma casa.

O método segue as seguintes regras para cifrar:

a. normalmente baseia-se na substituição de uma letra pela correspondente da mesma fila da coluna da outra, no caso da palavra PE ficaria OS;
b. as palavras separam-se em diagramas, estes nunca podem ter duas letras repetidas, nesse caso põe-se uma a separá-las (X), por exemplo a palavra DISSE antes de ser cifrada ficaria DI SX SE;
c. se duas letras estão seguidas na mesma linha da matriz, são substituídas pela seguinte da direita num esquema de continuidade circular, por exemplo a palavra NOTA cifrada ficaria OPAM;
d. se duas letras estão na mesma coluna da matriz substitui-se pela imediatamente inferior num esquema de continuidade circular, por exemplo a palavra FOCA cifrada ficaria OWKC.

Este sistema tem a vantagem de utilizar um diagrama de 676 símbolos (26*26) e de ser muito difícil de identificar uma palavra isolada; foi considerado durante muito tempo como inquebrável. A marinha inglesa e a marinha do EUA utilizaram este sistema durante a segunda guerra mundial.

2.3 SISTEMAS POLIALFABÉTICOS

Estes tipos de sistemas são utilizados para trocar as estatísticas do criptograma. A cada letra corresponde-lhe um alfabeto, isto implica que, para ser ideal, utilizaria uma chave de alfabetos aleatórios, o que é muito difícil de memorizar e transmitir. Por isso, são utilizadas uma tabela de alfabetos e uma palavra chave.

O sistema mais conhecido designado pela tabela de *Vigenère*, nome do seu autor alquimista, matemático e criptólogo, data de 1586.

A tabela é formada da seguinte maneira:

	a	b	c	d	..	..	..	..	x	y	z
a	A	B	C	D					X	Y	Z
b	B	C	D	E					Y	Z	A
c	C	D	E	F					Z	A	B
d	D	E	F	G					A	B	C
:											
:											
:											
:											
x	X	Y	Z	A					U	V	W
y	Y	Z	A	B					V	W	X
z	Z	A	B	C					W	X	Y

Os alfabetos formam as colunas e começam sempre pela letra da abcissa.

O método segue as seguintes regras:

a. procura-se uma palavra chave fácil de memorizar;
b. escreve-se a palavra chave por baixo do texto em claro, forma-se um conjunto de caracteres de igual comprimento que o texto em claro, repetindo a palavra chave quantas as vezes necessárias;
c. cada letra do texto em claro é codificada com a letra encontrada resultante do cruzamento do alfabeto da tabela e a letra da palavra chave repetida correspondente.

Vejamos um exemplo clarificador:

Chave: MILITAR

Texto em claro: INSTITUTO DE ALTOS ESTUDOS
Chave repetida: MILITARMI LI TARMI LITARMI

Criptograma: UVDAATLFW ON TLKAA PZMUUAA

2.4 SISTEMA DE PERMUTA

Este sistema é baseado na desordenação de caracteres, bits, etc.. Neste caso, não são trocados os símbolos mas sim a sua situação no texto. Um exemplo da utilização deste sistema é o método das colunas que segue as seguintes regras:

a. escolhe-se uma palavra chave simples de decorar, com esta, forma-se a primeira linha de uma matriz;
b. debaixo desta acrescenta-se o texto em claro preenchendo a matriz da esquerda para a direita;
c. trocam-se as colunas de posição, a nova posição da coluna segue a ordenação da palavra chave por ordem alfabética;
d. o novo texto, criptografado, escreve-se com as letras das colunas de baixo para cima.

Para melhor esclarecermos este método vamos exemplificar com um texto simples em claro e uma chave simples:

Chave: TROPAS

Texto em claro: TRABALHO DE INVESTIGAÇÃO

T	R	O	P	A	S
T	R	A	B	A	L
H	O	D	E	I	N
V	E	S	T	I	G
A	C	A	O		

Para ordenar a nova matriz coloca-se a palavra chave por ordem alfabética ficando desta forma:

AOPRST

A matriz reordenada terá o seguinte aspecto:

A	O	P	R	S	T
A	A	B	R	L	T
I	D	E	O	N	H
I	S	T	E	G	V
	A	O	C		A

O criptograma seria transmitido desta forma: IIA ASDA OTEB CEOR GNL AVHT

ANEXO C

OS SISTEMAS BIOMÉTRICOS

OS SISTEMAS BIOMÉTRICOS

1. ORIGEM DA BIOMETRIA

A tecnologia envolvida na Biometria tem evoluído rapidamente nos últimos anos, não só pelo aumento das capacidades de processamento, como pelo desenvolvimento e aperfeiçoamento dos "periféricos" (como câmaras e/ou um scanner) que têm tornado viável (física e economicamente) o desenvolvimento de aplicações e dispositivos biométricos.

Como isto tudo começou, é a questão que nos surge de imediato, quando abordamos este assunto. Isto leva-nos a pensar sobre a biometria como uma tecnologia futurista que deveríamos utilizar como é o caso dos carros a energia solar, pílulas de alimentação e outros tipos de equipamentos futuristas num futuro próximo. Esta imagem sugere produtos do final do século XX, na era dos computadores. Na verdade, os princípios básicos da verificação biométrica foram compreendidos e aplicados um pouco antes. Centenas de anos antes, no Vale do Nilo empregava-se a verificação biométrica num grande número de situações diárias de negócios.

Existem diversas referências sobre indivíduos identificados por características físicas e parâmetros como cicatrizes, critérios de medida física ou a combinação de características mais complexas como cor dos olhos, altura e outra características. Estas seriam frequentemente utilizadas no sector da agricultura onde grãos e provisões seriam armazenados numa central de reposições e aguardavam para movimentações futuras, após identificação dos proprietários. É evidente que eles não possuíam sistemas biométricos e redes de computadores e, certamente, não estavam a lidar com o mesmo número de indivíduos de hoje, mas os princípios básicos eram similares.

Mais tarde, no século XIX houve um pico de interesse em pesquisa de crimes na tentativa de relacionar características físicas com tendências criminais. Isto resultou numa variedade de dispositivos para medir características físicas. Os resultados não foram conclusivos, mas a ideia de medir características físicas individuais continuou, e os desenvolvimentos paralelos com as impressões digitais, estas já vulgarmente utilizadas, tornaram-se métodos internacionalmente empregues pelas autoridades governamentais para a identificação e verificação de pessoas.

Com os conhecimentos adquiridos, não foi surpresa que, por muitos anos, o fascínio tenha ocupado a mente de pessoas e de organizações com a possibilidade de utilização de equipamentos electrónicos e de dispositivos de microprocessadores para automatizar a verificação de identidades pelos militares e no sector comercial.

Foram iniciados vários projectos para verificar o potencial da biometria. Inicialmente foi desenvolvido um leitor da geometria da mão, este serviu para motivar os seus autores e continuar a sua concepção. Mais tarde, uma pequena empresa especializada criou uma unidade, e um leitor mais aprimorado da geometria da mão tornando-se o princípio da industria biométrica actual.

Os equipamentos biométricos que trabalham com impressões digitais são utilizados em numerosos projectos biométricos por todo o mundo. Paralelamente, estão a ser desenvolvidos outros métodos biométricos melhorados e refinados até ao ponto em que se tornem realidades comerciais.

2. SISTEMAS BIOMÉTRICOS

A identificação biométrica tem inúmeras aplicações, uma das mais significativas nos próximos anos será sem dúvida, a sua introdução nas caixas multibanco, uma vez que muitos bancos americanos têm já planos para implementar estes sistemas nas máquinas de levantamentos. Muitas organizações têm sistemas destes em funcionamento, os exemplos mais popularizados são descritos a seguir.

2.1 RECONHECIMENTO DE IMPRESSÕES DIGITAIS

Um scanner diferencia a luz reflectida pelos padrões das impressões digitais de um dedo, identificando o seu possuidor. É o sistema mais barato e popular dos sistemas biométricos, sendo também bastante seguro. O único inconveniente é que não pode ser utilizado para controlar grandes quantidades de utilizadores.

2.2 RECONHECIMENTO DA ÍRIS

Uma câmara reconhece os círculos e padrões da íris humana identificando assim o utilizador. É o sistema que proporciona a maior segurança pois é difícil reproduzir a íris da vista humana de forma a enganar este sistema. É bastante prático e cómodo pois não implica um contacto físico do utilizador com a câmara, mas têm o inconveniente de ser o sistema mais caro. Os peritos recomendam este sistema em prisões de alta segurança e em centrais nucleares ou bases militares.

2.3 RECONHECIMENTO FACIAL

As câmaras ajudam a medir e a reconhecer as fisionomias e os traços do rosto humano através de pontos de referência (olhos, nariz, etc.). Não requer o contacto físico, pode mesmo ser utilizado sem o conhecimento de quem está a ser sondado. Embora muito falível tem grandes potencialidades, nomeadamente em aeroportos. Este método é um dos sistemas de biometria mais caros.

2.4 RECONHECIMENTO DE VOZ

Os microfones ajudam na análise da voz e das ondas sonoras de forma a identificar o utilizador. É o ideal para o controlo de acesso num computador e é relativamente barato. No entanto, é bastante falível e se o utilizador tiver alterada a sua voz por rouquidão ou por uma constipação pode não ser identificado.

ANEXO D

CONTROLO DE ACESSO POR CERTIFICADO DIGITAL

CONTROLO DE ACESSO POR CERTIFICADO DIGITAL

O sistema de controlo de acesso por certificado digital apresenta as seguintes fases (acompanhar com a figura da página seguinte):

- o utilizador autorizado recebeu um certificado digital com o seu nome e a sua chave pública assinada pelo servidor que pretende aceder. Também recebeu, por um processo seguro, a sua chave privada;
- para ter acesso ao sistema envia o seu certificado;
- o servidor comprova a assinatura do certificado e guarda a chave pública;
- o servidor envia um número aleatório ao utilizador;
- o utilizador cifra o número aleatório com a sua chave privada e envia o resultado para o servidor;
- o servidor decifra e comprova que a chave privada é par da pública que foi enviada com o certificado.

Este processo pode complicar-se, no entanto, deve basear-se sempre nos seguintes princípios:

- a posse do certificado digital correctamente assinado implica que o utilizador tenha a chave privada par da pública indicada e que a recebe do servidor;
- a possibilidade de cifrar com a chave privada indica que o utilizador que enviou o certificado é quem diz ser, evitando-se os roubos de certificados.

Os certificados podem ser retirados ou anulados aos seus utilizadores utilizando-se para esse efeito a data de caducidade no certificado e construindo uma lista de renovações de certificados.

Os certificados são como os bilhetes de identidade das pessoas, o que implica muita gestão do servidor. Assim, se o servidor quer activar um grupo de utilizadores com os mesmos privilégios não se pode utilizar um único certificado, deve ser criado um para cada utilizador.

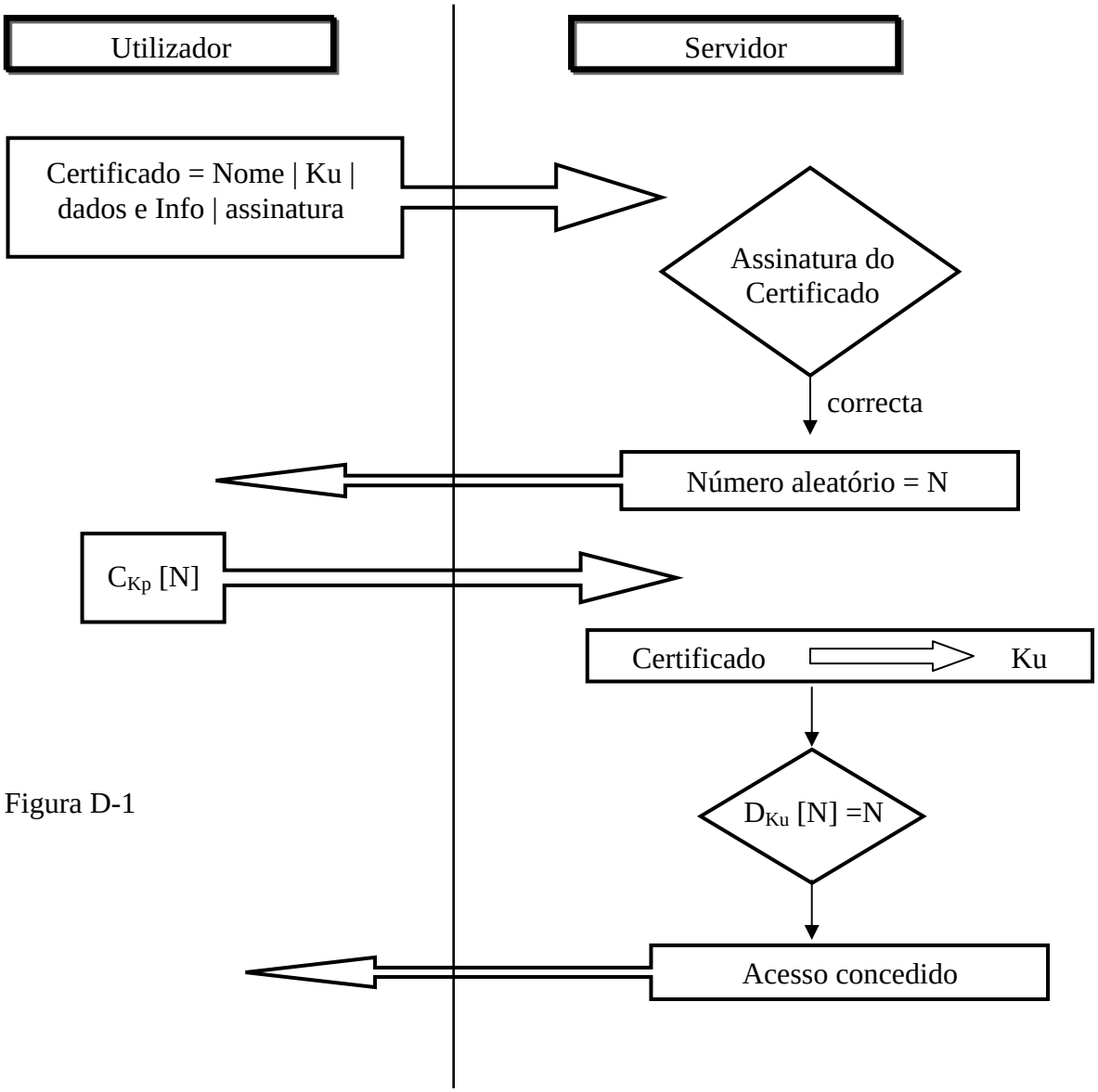


Figura D-1

Legenda:

C – cifrar
D – Decifrar
Ku – Chave pública do utilizador
Kp – Chave privada do utilizador
Assinatura: C_{Kp} do servidor [certificado]

ANEXO E

FUNÇÕES *HASH*

FUNÇÕES *HASH*

O objectivo principal da utilização das funções *Hash* é o de comprimir um texto num bloco de comprimento fixo, estas funções são utilizadas em autenticação e em assinaturas digitais com os seguintes propósitos:

- não ter que cifrar todo o texto nos serviços de autenticação e assinatura digital, pois este processo é muito lento nos algoritmos assimétricos. O resumo serve para comprovar se a chave privada do emissor é autêntica, não sendo necessário cifrar todo o texto se não se pretende a sua confidencialidade (ver figura abaixo);
- para se poder comprovar automaticamente a autenticidade. Ao se cifrar um texto na sua totalidade, quando se decifra, só é possível comprovar a sua autenticidade, verificando se o resultado é inteligível, este processo tem evidentemente de realizar-se de uma forma manual. Utilizando o processo de resumo do texto pode-se comprovar se é autêntico comparando o resumo efectuado no receptor com o decifrado;
- para comprovar a integridade do texto, pois este pode ser transmitido com erros ou ser danificado na recepção, neste caso não coincidirá com o resumo do texto decifrado.

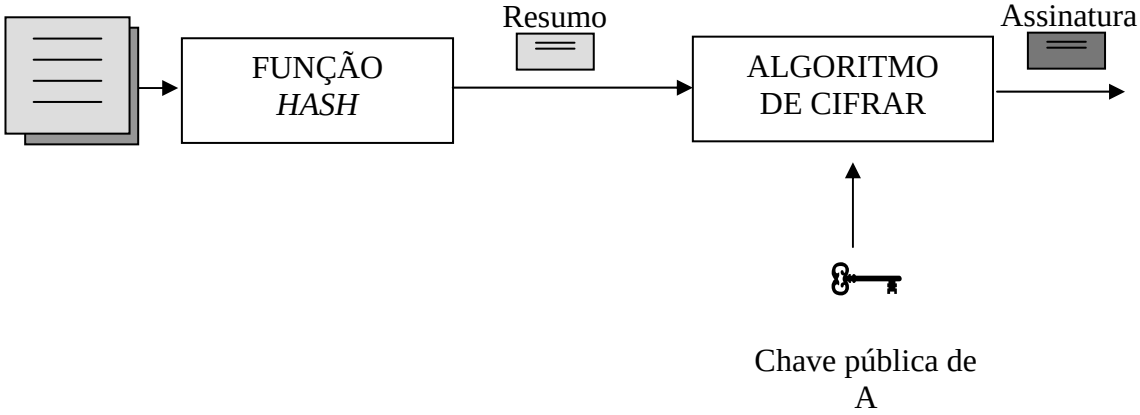


Figura E - 1

As funções *Hash* são públicas e irreversíveis, não cifram, apenas comprimem os textos em blocos de comprimento fixo, estas funções são muito diferentes das funções clássicas de compressão de textos como o ZIP, V-42, RAR e outros, que são funções reversíveis e apenas tentam eliminar a informação redundante de um texto mantendo o texto original intacto.

Com a utilização das funções *Hash* o texto original não pode ser recuperado através do resumo, para isso devem-se cumprir as seguintes condições:

- transformar um texto de comprimento variável num bloco de comprimento fixo;
- ser irreversível;
- conhecido um texto e a sua função *Hash* deve ser impossível encontrar outro texto com a mesma função *Hash*;
- ser impossível de inventar dois textos cuja função *Hash* seja a mesma.

Os algoritmos mais utilizados são:

- o MD5, inventado em 1992 por *Rivest*, o comprimento dos blocos é de 128 bits, é comercializado livremente;
- o SHA, inventado em 1994 pela agência norte americana NIST, o comprimento do bloco é de 160 bits e a sua comercialização está sob autorização dos EUA.

ANEXO F

A CRIPTOGRAFIA COMO SUPORTE DA SEGURANÇA

A CRIPTOGRAFIA COMO SUPORTE DA SEGURANÇA

1. CONCEITO DE CRIPTOGRAFIA

Podemos definir criptografia como uma técnica de converter um texto inteligível (texto em claro), num outro, a que se chama criptograma, em que a informação contida nele é igual ao anterior mas, só pode ser compreendido por entidades autorizadas.

Assim, para aplicar esta técnica, devem ser bem definidas as entidades que devem conhecer os algoritmos e chaves utilizadas na transformação de textos (no Anexo B "Evolução dos sistemas de criptografia" explica-se o significado de chave usada nas técnicas de criptografia), com a utilização de algoritmos secretos (figura F-1) ou algoritmos públicos que utilizam uma chave secreta (figura F-2), apenas conhecida por entidades autorizadas.

Actualmente os sistemas utilizam algoritmos públicos e chaves secretas porque proporcionam o mesmo nível de segurança, e porque é mais seguro e fácil transmitir as chaves que os algoritmos e, por outro lado, os algoritmos públicos podem ser produzidos em série

Figura F - 1

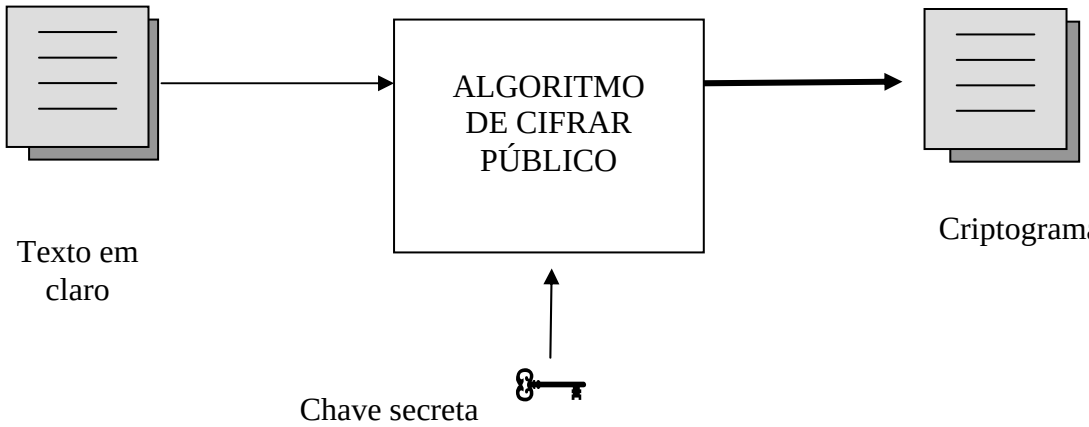


Figura F - 2

(tornando o seu fabrico bastante rentável), tanto em *chips* de hardware como em aplicações lógicas (software), tornando-os mais apelativos para a comunidade cientifica, pois tem a possibilidade de os testar e tentar encontrar possíveis falhas ou buracos detectáveis.

2. TIPOS DE CHAVES UTILIZADAS

Actualmente existem dois tipos de chaves usados pelos sistemas de criptografia modernos, que vamos de seguida aprofundar mais detalhadamente para um melhor esclarecimento de opções a tomar no futuro.

2.1 A CHAVE PRIVADA

É sem duvida o sistema de criptografia mais antigo, utilizado desde o tempo de Júlio César, esta técnica é também conhecida por criptografia simétrica, caracteriza-se por a mesma chave ser utilizada pelo emissor e pelo receptor para cifrar e decifrar textos.

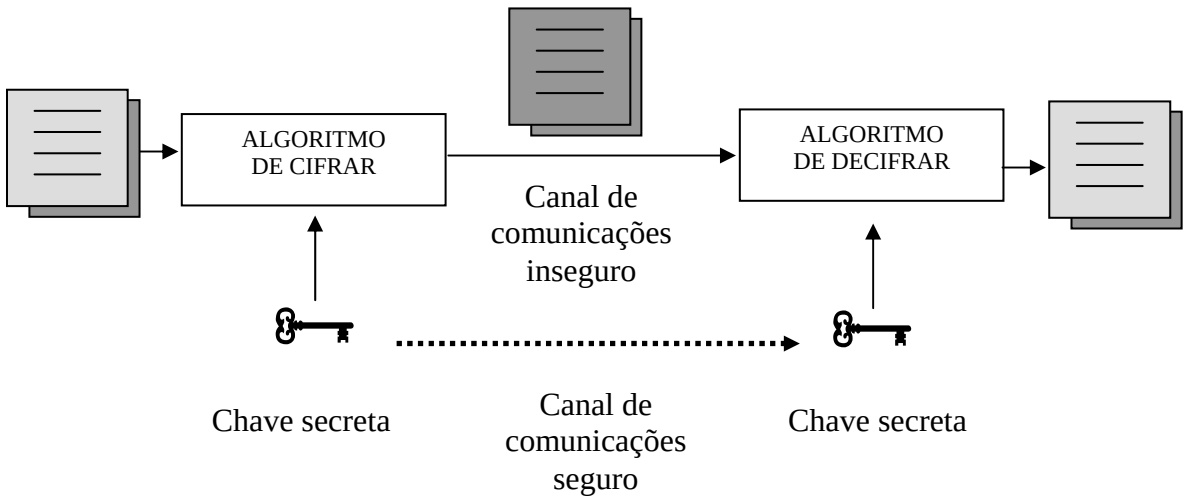


Figura F - 3

A segurança deste sistema está totalmente baseada na privacidade da chave secreta. A transmissão da chave é feita por um sistema de comunicações seguro para todas as entidades autorizadas a receber mensagens, o que constitui o maior problema para os sistemas simétricos. Actualmente utilizam-se os sistemas assimétricos para resolver o problema da transmissão de chaves privadas simétricas.

Estes sistemas só permitem confidencialidade, não permitem a autenticação nem a assinatura digital.

2.2 A CHAVE PÚBLICA

A utilização da criptografia de chave pública, também designada por criptografia assimétrica, iniciada em 1976 por *Diffie e Hellman*, veio revolucionar a criptografia em geral. A ideia veio permitir resolver o problema da distribuição simétrica de chaves e permitir utilizar a confidencialidade (da mesma forma que os sistemas simétricos), a autenticação, e a assinatura digital na transmissão de textos em claro.

Para cada tipo de serviço é utilizada uma forma diferente de cifrar:

- Para a confidencialidade, o emissor cifra o texto com a chave pública do receptor e este decifra-o com a sua chave privada. Desta forma, qualquer utilizador pode enviar uma mensagem cifrada, mas só o receptor que tem a chave privada e o emissor, que criou a mensagem, podem decifrar o conteúdo desta, na figura F-4 ilustra-se este processo.
- Para a autenticação, é cifrada uma mensagem ou um resumo desta com a chave privada e qualquer utilizador pode comprovar a sua procedência utilizando a chave pública do emissor. A mensagem é autêntica porque só o emissor verdadeiro pode cifrar com a sua chave privada (confrontar com o esquema da figura F-5).
- Para a assinatura digital é utilizado um processo igual à autenticação, mas o que se cifra é sempre um resumo da mensagem em que o criptograma utilizado é a assinatura do emissor. Assim, o emissor não pode negar a procedência pois foi utilizada a sua chave privada. Por outro lado, o receptor não pode modificar o conteúdo da mensagem porque o resumo seria diferente e facilmente seria detectada a alteração, pois não coincidiria com a decifração da assinatura. No entanto, o receptor pode comprovar que o resumo coincide com a assinatura decifrada para comprovar se é autêntico, isto é, a assinatura implicitamente garante a autenticação, este processo pode-se ver através da figura F-6.

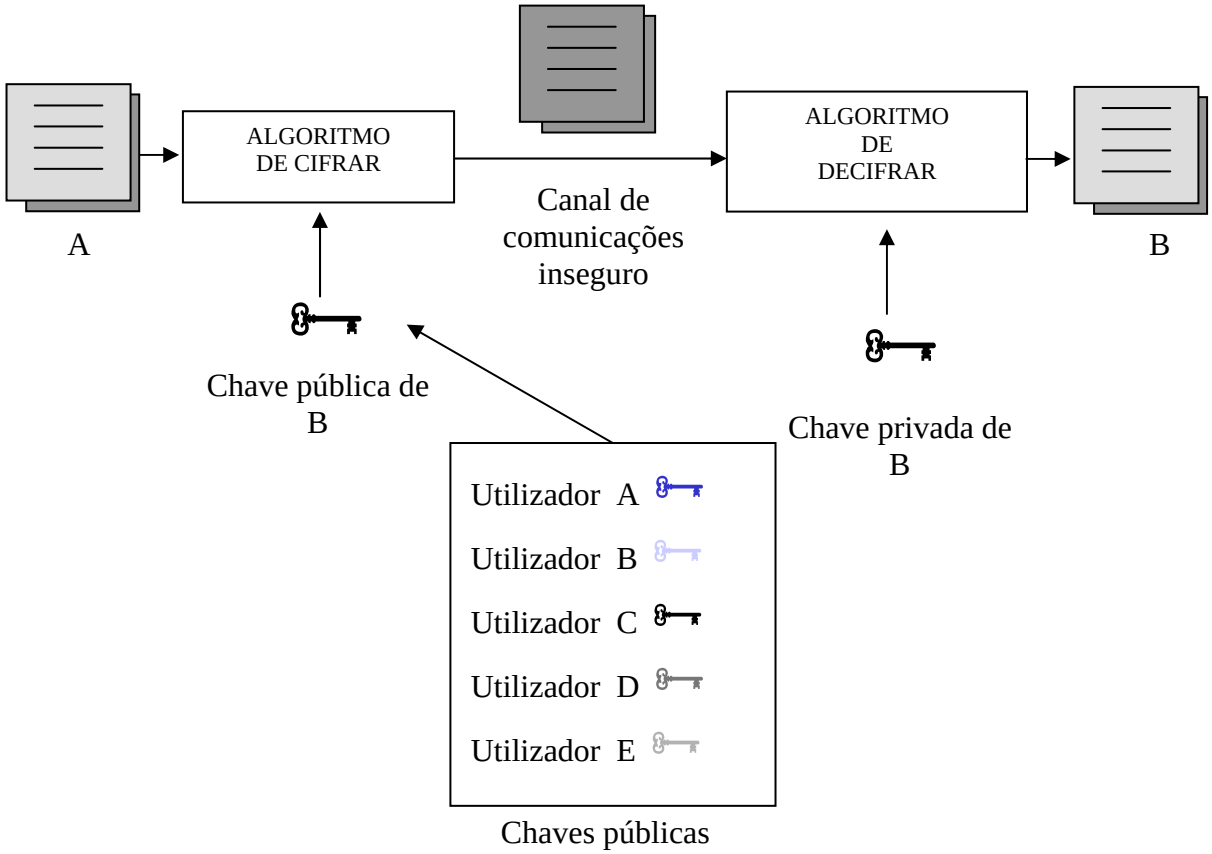


Figura F - 4

Os algoritmos assimétricos são baseados em funções matemáticas fáceis de resolver mas cujo processo inverso é muito complicado de descobrir, como é o exemplo da utilização da potência e do logaritmo. As chaves privadas e públicas estão relacionadas matematicamente, devem ser bastante complexas para evitar que sejam descobertas, por isso, as chaves privadas e públicas não são escolhidas pelo utilizador mas sim calculadas por um algoritmo, sendo normalmente extensas.

O algoritmo de chave pública deve obedecer a três requisitos fundamentais:

- conhecido o criptograma não se pode decifrar o texto nem adivinhar a chave;
- conhecido o texto e o criptograma é mais caro (em termos de tempo e/ou custos) decifrar a chave que o valor da informação;
- conhecida a chave pública e o texto não se pode gerar um criptograma com chave privada.

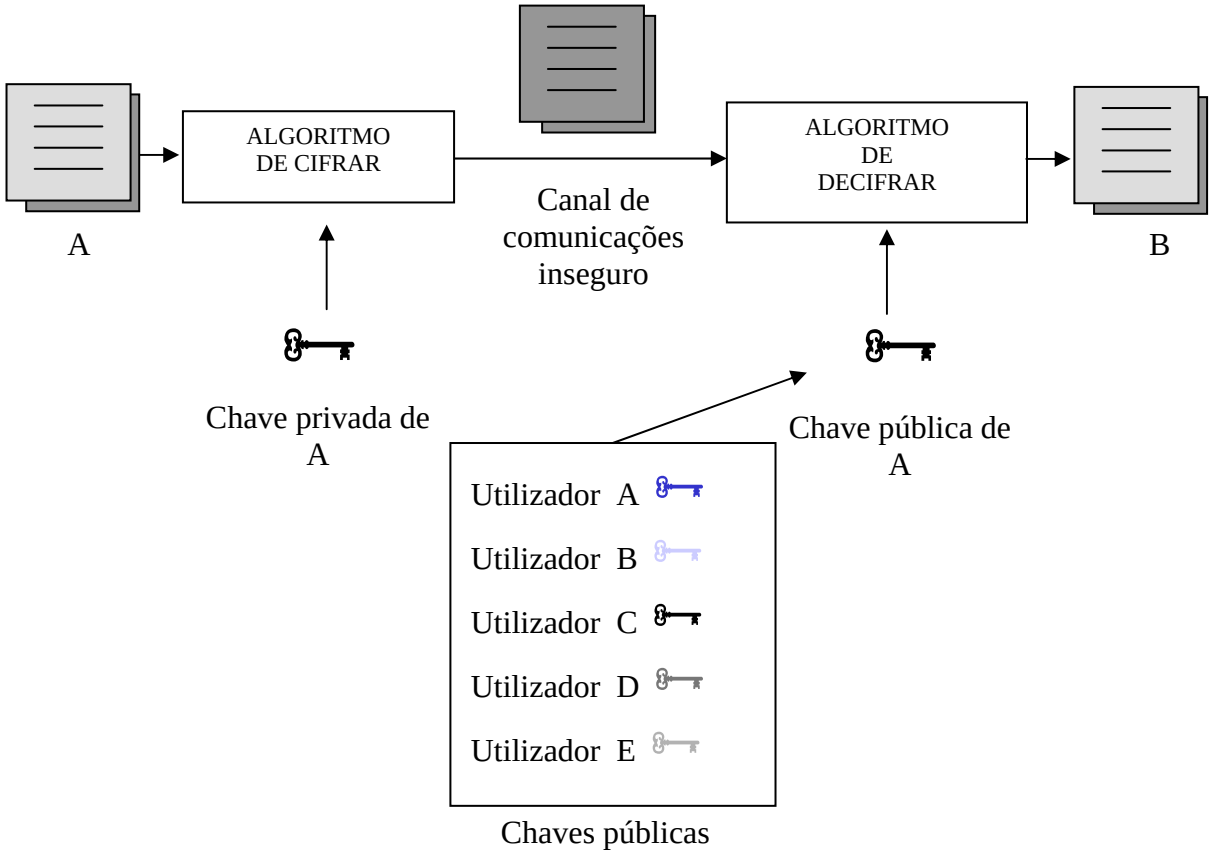
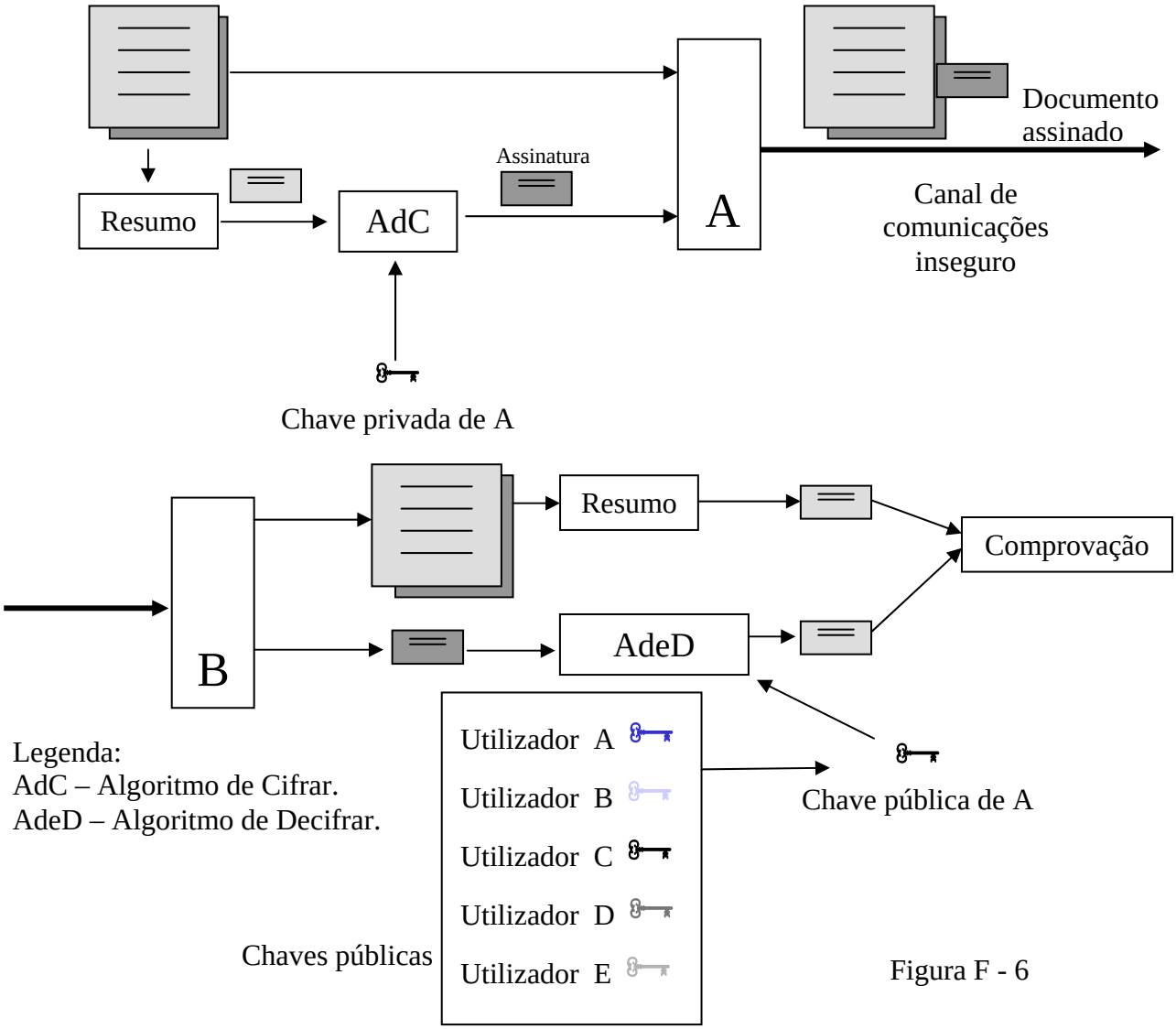


Figura F - 5

O grande inconveniente destes sistemas é a dificuldade de serem implementados e a lentidão do processo.

A grande vantagem é que implementam serviços de autenticação e assinatura digital, para além de não causarem o problema da distribuição de chaves (a chave pública pode ser visível para todos mas a privada nunca se transmite).



Legenda:
AdC – Algoritmo de Cifrar.
AdeD – Algoritmo de Decifrar.

Figura F - 6

3. CERTIFICADOS DIGITAIS[1]

3.1 A TRANSMISSÃO DE CHAVES

Um dos problemas da utilização da criptografia simétrica é a transmissão das chaves, pois se eventualmente a chave é descoberta, o sistema é quebrado e consequentemente desacreditado. O problema tem a solução, como já foi referido, de se adoptar por uma opção de enviar as chaves cifradas por um sistema assimétrico.

As chaves privadas nunca são transmitidas, por isso, são seguras e confidenciais. No entanto, quando se pretende transmitir uma chave pública, surgem desde logo dois riscos, o primeiro é o de a chave ser enviada por uma entidade falsa, falsificando a assinatura de outra entidade, o segundo risco é o de estar a trocar textos confidenciais com um interlocutor fictício, fazendo-se passar por uma entidade conhecida.

O problema, de um elemento estranho se poder fazer passar por uma entidade autorizada, pode ser solucionado com a utilização de certificados de chave pública, este certificados normalmente têm os seguintes dados dos utilizadores:

- o nome do utilizador;
- a chave pública de um outro utilizador;
- informações e dados gerais;
- a assinatura digital de uma terceira entidade de confiança.

É através da autenticidade da assinatura digital desta terceira entidade (necessariamente terá que ser de confiança) que existe a confiança nas chaves públicas que circulam entre os utilizadores de qualquer rede, tornado-se credíveis e passíveis de não pertencerem a uma entidade falsa.

Por isso, todo o software produzido deve estar preparado para receber certificados, verificar a sua autenticidade e permitir dar ao utilizador a autenticidade ou não do texto recebido.

Resolvido o problema da transmissão de chaves públicas, evitando que um estranho se possa passar por uma entidade autorizada, surge de imediato um outro, o de ter a total confiança na terceira entidade que assina os certificados. O problema pode ser resolvido por dois métodos, um não poderá necessariamente substituir o outro, mas são muito utilizados actualmente, o método dos níveis de confiança do *Pretty Good Privacy* (PGP) e o das Autoridades de

[1] São também designados por certificados de chaves públicas.

Certificação (CA), esta sigla vem de *Certification Autorities,* é o que nos propomos a descrever nos pontos a seguir.

3.2 CERTIFICADO DO PGP

Os certificados do sistema de correio PGP baseiam o seu funcionamento em níveis de confiança. Este sistema só seria perfeito se todos os certificados chegassem assinados aos interessados mediante um comprovativo da chave pública, mas nem sempre é assim, isto, porque uma chave sem certificado só é de confiança se transmitida pessoalmente ou através de meios de comunicação seguros.

Neste sistema, de PGP, são distinguidos dois níveis de confiança a cada chave pública da base de dados:

- confiança própria, a confiança da chave pública é calculada segundo o percurso que fez pelos vários utilizadores da rede, podendo chegar directamente e ter confiança máxima ou chegar via certificado e a confiança dependeria da assinatura da terceira entidade;
- confiança para assinar certificados, uma chave pública pode ter uma confiança própria muito alta porque foi transmitida por um sistema seguro, mas podemos ser levados a desconfiar da assinatura do certificado desse utilizador, porque este pode assinar qualquer certificado de outro utilizador sem confirmar a procedência.

Os certificados próprios e de confiança para assinar são criados entre os utilizadores da rede, cada utilizador tem estes dois níveis de confiança como parâmetros, e quando um novo utilizador envia um texto pela rede é um utilizador já possuidor dos dois parâmetros que vai assinar os seus níveis de confiança. Desta forma, cada novo utilizador é certificado por um outro possuidor dos dois níveis de confiança.

Como podemos facilmente verificar, este sistema apenas serve para um certo número de utilizadores numa rede, mas se o número de utilizadores é substancial (como é o caso dos utilizadores da internet) este sistema não se mostra fiável porque os utilizadores não poderão certificar-se entre si. Para além disso, para o sistema PGP ser utilizado em sistemas oficiais como os governamentais, judiciais, militares, etc., em que a procedência de uma assinatura tem que ser comprovada, este processo de certificação torna-se num problema de difícil resolução.

3.3 AUTORIDADE DE CERTIFICAÇÃO

Os problemas que surgiram no sistema de certificação anterior foram colmatados pela criação das Autoridades de Certificação.

As CA são entidades públicas ou privadas cuja função é oferecer a confiança necessária aos certificados que assinam. Estas entidades geram chaves públicas e certificados para utilizadores sob o seu domínio, para além de darem a conhecer as suas chaves públicas para as comprovações. Os utilizadores devem identificar-se pessoalmente para pedir um certificado a uma CA. O sistema é semelhante ao processo de pedido do bilhete de identidade, onde existe uma entidade governamental responsável, entidade de confiança do Estado, que concebe o documento necessário para que todos os organismos públicos ou privados aceitem o documento como verdadeiro e de confiança.

A gestão das CA pode ser descentralizada com a criação de uma estrutura hierárquica a nível mundial, para isso podem ser criadas CA Locais para se responsabilizarem por um grupo restrito de utilizadores e, num nível superior a essas CA Locais, são criadas outras CA que terão a responsabilidade de certificar as CA Locais, acima destas poderá existir uma CA Principal, que se responsabilizará por todas, como se mostra na figura F - 7 em baixo.

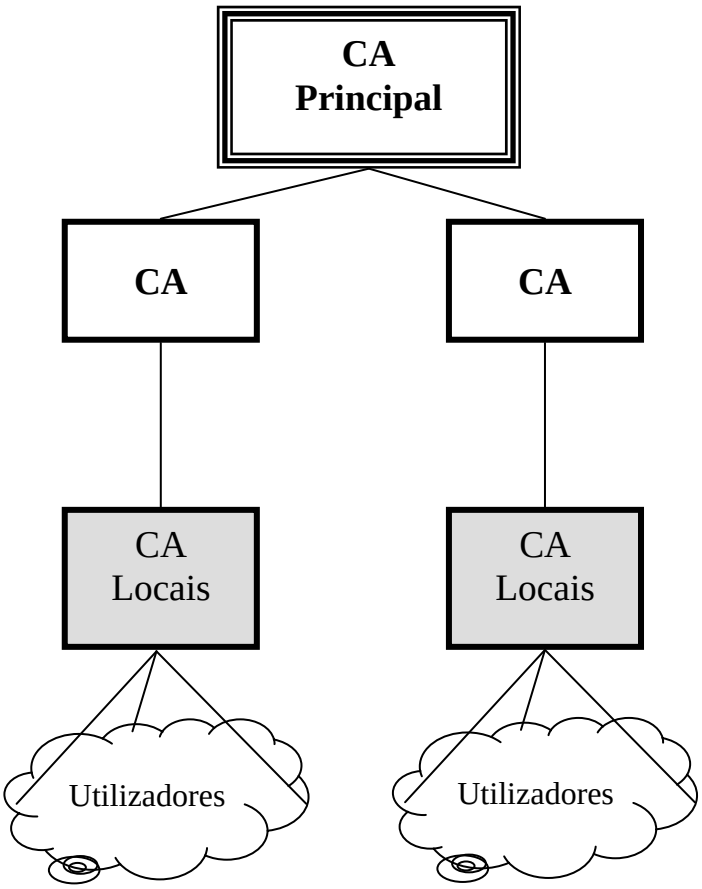


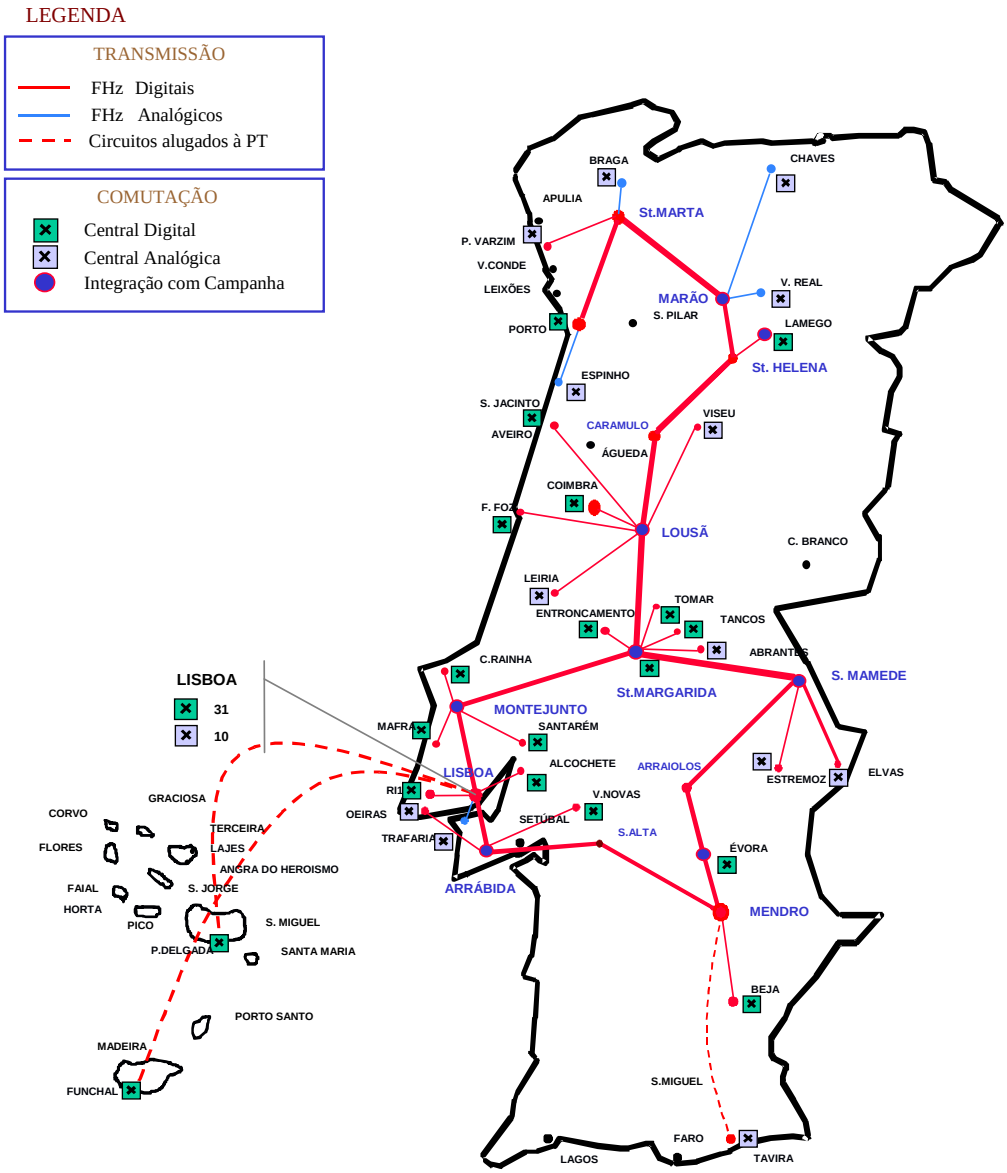
Figura F - 7

As CA de ordem superior certificam as inferiores e assim se podem juntar certificados desde a CA Principal até à chave do utilizador, permitindo que os utilizadores comuniquem entre si de maneira segura, com apenas uma condição, que conheçam a chave pública da CA Principal que podem obter de uma CA Local qualquer.

ANEXO G

SISTEMA INTEGRADO DE TELECOMUNICAÇÕES DO EXÉRCITO PORTUGUÊS

SISTEMA INTEGRADO DE TELECOMUNICAÇÕES DO EXÉRCITO PORTUGUÊS

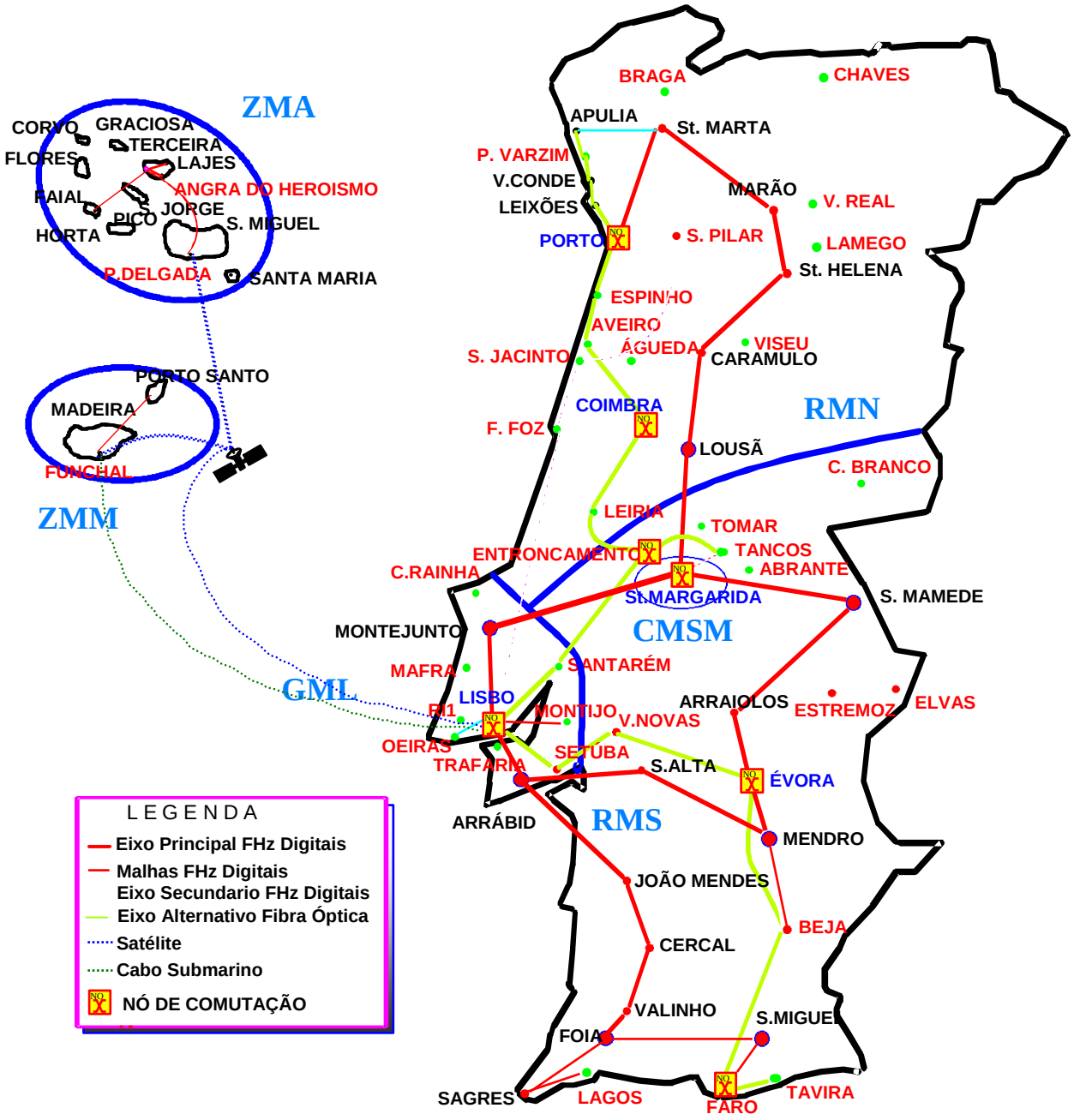


Fonte: Chefia das Telecomunicações Permanentes/DST

ANEXO H

SISTEMA DE COMUNICAÇÕES (SICOM)

SISTEMA DE COMUNICAÇÕES (SICOM)



Fonte: EMGFA

ANEXO I

SITUAÇÃO DOS PROJECTOS DA RESPONSABILIDADE DO CIE

SITUAÇÃO DOS PROJECTOS DA RESPONSABILIDADE DO CIE

O CIE entre 1999 e 2001 tinha ou tem em actividade alguns projectos em diversas fases de andamento que convencionalmente se distinguem em quatro categorias:

- os que se encontram ainda em fase de planeamento;
- os que se encontram em pleno progresso;
- os que foram realizados mas não foram ainda sujeitos à comprovação do seu desempenho;
- os já concluídos.

	PESSOAL (SIAPE)	
1	Informatização da DAMP - Colocações	CONCLUÍDO
2	Informatização da DAMP - Pessoal Civil	CONCLUÍDO
3	Informatização dos Quadros Orgânicos (3ªREP)	EM TESTES
4	Controlo Informático de Voluntários e Contratados	CONCLUÍDO
5	Informatização da Convocação e Mobilização	CONCLUÍDO
6	Back-Up da Aplicação de Vencimentos	EM PROGRESSO
7	Informatização do Serviço de Justiça	EM PROGRESSO
8	Cartões de Identidade	EM PROGRESSO
9	Implementação da Base de Dados Única de Pessoal	EM PLANEAMENTO
10	Transferência de Dados para o MDN	CONCLUÍDO
11	Migração para o Euro e Ano 2000	EM PROGRESSO
12	Informatização da DAMP - Promoções	EM PROGRESSO
13	Informatização da DAMP - Reserva e Reforma	EM PLANEAMENTO
14	Informatização da DAMP - Simulação de Carreiras	EM PLANEAMENTO

	PESSOAL (SIPORG)	
1	Informatização e Ligação dos CRs	CONCLUÍDO
2	Informatização e Ligação da DR	CONCLUÍDO
3	Informatização dos BIRMs e DIRMs	CONCLUÍDO
4	Optimização do SIPORG	EM PROGRESSO

	PESSOAL (INSTRUÇÃO)	
1	Gestão dos Cursos	EM PLANEAMENTO

	LOGÍSTICA (SINFLOG)	
1	Gestão do Reabastecimento	CONCLUÍDO
2	Redes Locais das Direcções Logísticas do Edifício Ceuta	CONCLUÍDO
3	Controlo Orçamental da DSM	CONCLUÍDO
4	Informatização do DGMG	EM PROGRESSO
5	Instalação da Rede Local do Comando da Logística	CONCLUÍDO

	RRING	
1	RRING: Aplicação de Recursos Humanos (RHW)	CONCLUÍDO
2	Informatização do COFT	CONCLUÍDO
3	MDN: INFOREC (Informação aos Recrutas)	EM PROGRESSO
4	RRING: Instalação da Aplicação das Sub Sec Fin nas UEO (RFW)	CONCLUÍDO
5	Conversão de Aplicações e HW dos CFin e DSF/ADME	EM TESTES
6	Informatização da Gestão de Tesouraria no Exército	EM PLANEAMENTO
7	Instalação de Quiosques Internet nos Estabelecimentos de Ensino	EM PROGRESSO

	GERAIS	
1	Instalação da Rede Local do CIE	CONCLUÍDO
2	Projecto Moçambique	CONCLUÍDO
3	Instalação da Rede Local do EME	CONCLUÍDO
4	Impacto da RAFE nas Aplicações Financeiras do Exército	EM PLANEAMENTO
5	Criação de um Domínio na Internet	EM TESTES
6	Informatização do PPA/POP	CONCLUÍDO

Fonte: CIE, informação actualizada em 2001

ANEXO J

ALGORITMOS MAIS UTILIZADOS

ALGORITMOS MAIS UTILIZADOS

1. ALGORITMOS SIMÉTRICOS

1.1 DATA ENCRYPTION STANDART

Inventado em 1971 pela IBM, recorrendo à aplicação de todas as teorias de criptografia conhecidas, ficou conhecido por LUCIFER. Mais tarde, os mesmos autores deste algoritmo, respondendo a um desafio lançado pelo *Nacional Bureau of Standart* (NBS) que procuravam um modelo padrão de criptografia para a transmissão de documentos oficiais em segurança, melhoraram o algoritmo inicial e designaram-no por *Data Encryption Standart* ou DES. Este algoritmo nunca foi quebrado por ninguém até a esta data, e mantém-se como o algoritmo padrão do *National Institute of Standards and Technology* (NIST), agência de padrões dos Estados Unidos da América (EUA).

Apesar de ser um algoritmo pouco comercializado no exterior dos EUA e de possuir uma chave muito curta, mantém-se como o algoritmo mais comercializado do mundo e mais resistente às ameaças de testes e ensaios das máquinas actuais.

Este algoritmo apresenta vantagens por ser o mais utilizado, sendo mais barato e o mais experimentado, até a esta data ainda não foi quebrado e é muito fácil e rápido de implementar.

1.2 TRIPLO DES

Numa tentativa de evitar o principal inconveniente do algoritmo DES, de possuir uma chave curta, e permitir continuar a utilizá-lo, arranjou-se um sistema baseado na aplicação do algoritmo de DES três vezes, ficando conhecido por Triplo DES ou TDES, que utiliza uma chave de 128 bits e é compatível com o DES simples.

A aplicação é muito simples, entre a aplicação de dois DES aplica-se um DES inverso, o que resulta numa função matemática de aplicação de um DES simples, aplicado três vezes. O facto de se utilizarem três algoritmos para cifrar poderia dar azo à utilização de três algoritmos diferentes, mas isso não sucede pois o principal motivo da utilização do TDES é o facto de se continuar a utilizar o DES simples.

1.3 INTERNACIONAL DATA ENCRYTION ALGORITHM

Em 1990 o *Swiss Federal Institute of Tecnology* criou um algoritmo que designou por *Internacional Data Encrytion Algorithm* (IDEA), este é um algoritmo livre de restrições e autorizações nacionais e está a ser distribuído livremente na internet, isto faz com que seja muito popular, principalmente fora dos EUA.

1.4 RC5

É um algoritmo muito recente, que derivou do RC4 cuja chave foi quebrada em 1996 por uma universidade francesa, o que colocou em dúvida a segurança que poderia proporcionar.

O seu funcionamento é muito simples, baseia-se num gerador de números aleatórios que são somados ao texto mediante um OR-Exclusivo. Este algoritmo tem a possibilidade de se configurar com muitos parâmetros como o número de iterações, o comprimento da chave e tamanho do bloco, permitindo que cada aplicação se adapte às necessidades de velocidade e/ou segurança.

2. ALGORITMOS ASSIMÉTRICOS MAIS UTILIZADOS

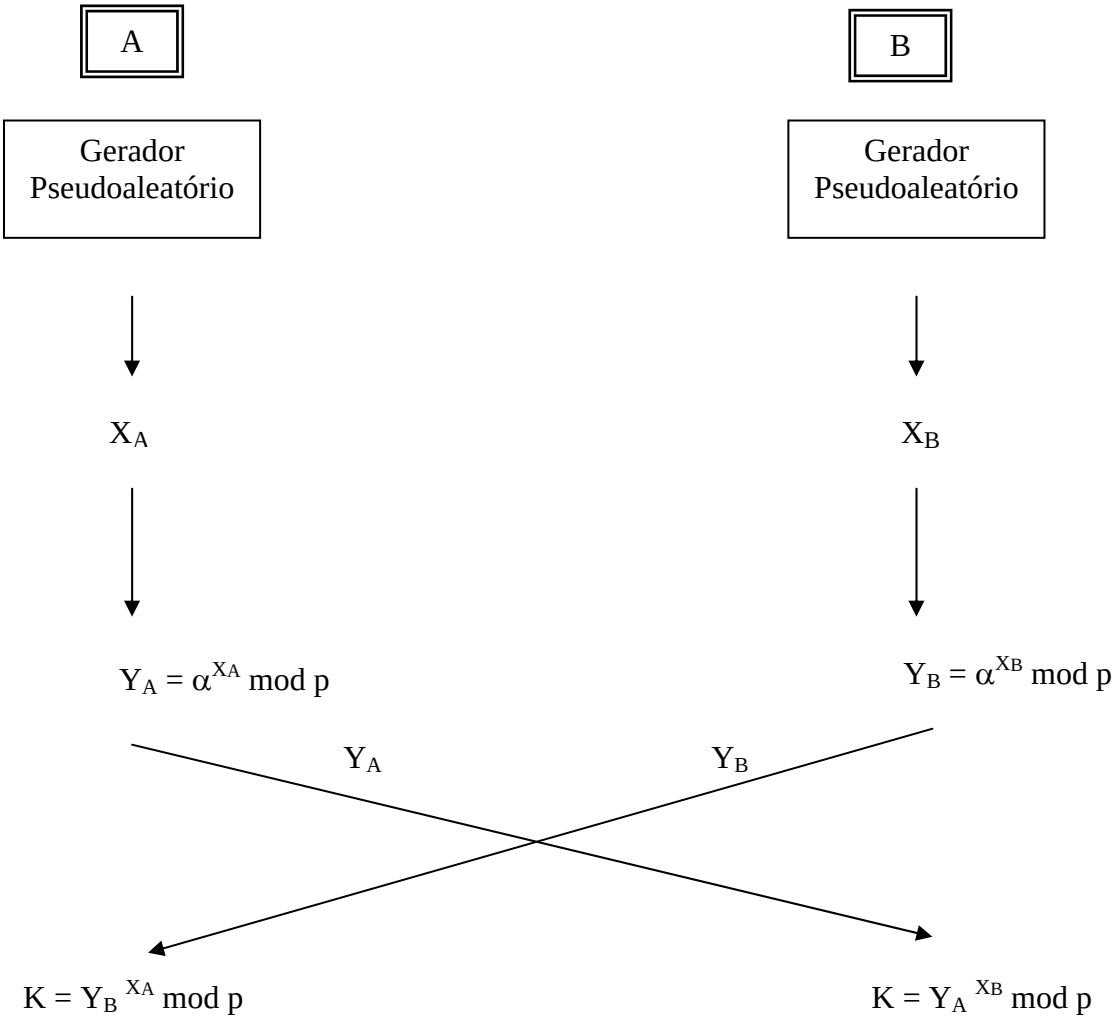
2.1 ALGORITMO DE DIFFIE-HELLMAN

Este foi o primeiro algoritmo assimétrico e começou por ser a primeira descoberta de *Diffie-Hellman* sobre a criptografia de chave pública.

O algoritmo apresenta um grande inconveniente de utilização, apenas é aplicado para trocar chaves simétricas, apesar dos algoritmos assimétricos serem utilizados principalmente para a troca de chaves simétricas entre utilizadores. Contudo, tornou-se o algoritmo mais utilizado em sistemas da internet na confidencialidade de chaves simétricas.

A segurança associada a este algoritmo depende essencialmente do cálculo de um logaritmo do tipo $Y = X^a \bmod p$. A geração de chaves públicas processa-se do seguinte modo:

- procura-se um número primo de grande extensão a que se designa por p;
- procura-se α raiz primitiva de p (para ser raiz primitiva deve ser calculado $\alpha \bmod p$, $\alpha^2 \bmod p$, $\alpha^3 \bmod p$, ..., $\alpha^{p-1} \bmod p$ e serem números diferentes);
- α e p são as chaves públicas.
- As chaves simétricas são compartilhadas segundo o processo que se apresenta na figura em baixo.



O número K é calculado pelos utilizadores e é igual para ambos, justificado pela propriedade distributiva desta forma:

$K = Y_B^{X_A} \bmod p = (\alpha^{X_B} \bmod p)^{X_A} \bmod p = \alpha^{X_B X_A} \bmod p = \alpha^{X_A X_B} \bmod p =$

$(\alpha^{X_A} \bmod p)^{X_B} \bmod p = Y_A^{X_B} \bmod p = K$

Quando se pretendem compartilhar chaves simétricas uma a uma num sistema de multiutilizadores, primeiro colocam-se todas as chaves Y_i disponíveis num servidor, quando se pretender enviar uma mensagem decifrada o processo é o seguinte:

- o emissor vai buscar a chave de Y_d (o destinatário da mensagem cifrada) ao servidor;
- o emissor calcula a chave K com o seu número secreto X_e;
- a mensagem decifrada é enviada com o valor K;

- o receptor, para calcular K, utiliza o seu número secreto X_r e vai buscar a chave de Y_e (chave do emissor).

2.2 RIVEST, SHAMIR AND ADLMAN

É um algoritmo que ganhou muita popularidade, para além de ser o mais utilizado dos algoritmos assimétricos, é o mais rápido e simples dos actualmente existentes. Este algoritmo foi inventado em 1978 por *Rivest, Shamir and Adlman* (RSA) que lhe deram o seu nome.

Este algoritmo utiliza as seguintes chaves:

- chave pública - dois números primos (a e b) de grande extensão (entre os 100 e os 300 dígitos);
- chave privada - um número (d), consequência dos anteriores.

O cálculo destas chaves é realizado em segredo no computador depositário da chave privada. O processo reveste-se de muita importância para a segurança do sistema. O processamento do algoritmo é o seguinte:

1. procuram-se dois números primos de grande extensão designados por **a** e **b**;
2. calcula-se **x** = (**a**-1)*(**b**-1) e **m** = **a***b;
3. procura-se **z** como um número sem múltiplos comuns a **x**;
4. calcula-se **k** = e^{-1} mod **x** (mod = resto da divisão por um inteiro);
5. Os números **m** e **z** são distribuídos, tornando-se as chaves públicas e guarda-se **k** para a chave privada, os números **a**, **b** e **x** são destruídos.

Este algoritmo tem todas as vantagens dos sistemas assimétricos, apesar de ter sido quebrado pela própria empresa utilizando muitos recursos para o efeito, actualmente aconselha-se a utilização de chaves de 1024 bits.

Os serviços de autenticação e assinatura digital apenas são implementados por estes sistemas, para a confidencialidade também se pode utilizar um dos sistemas simétricos descritos.

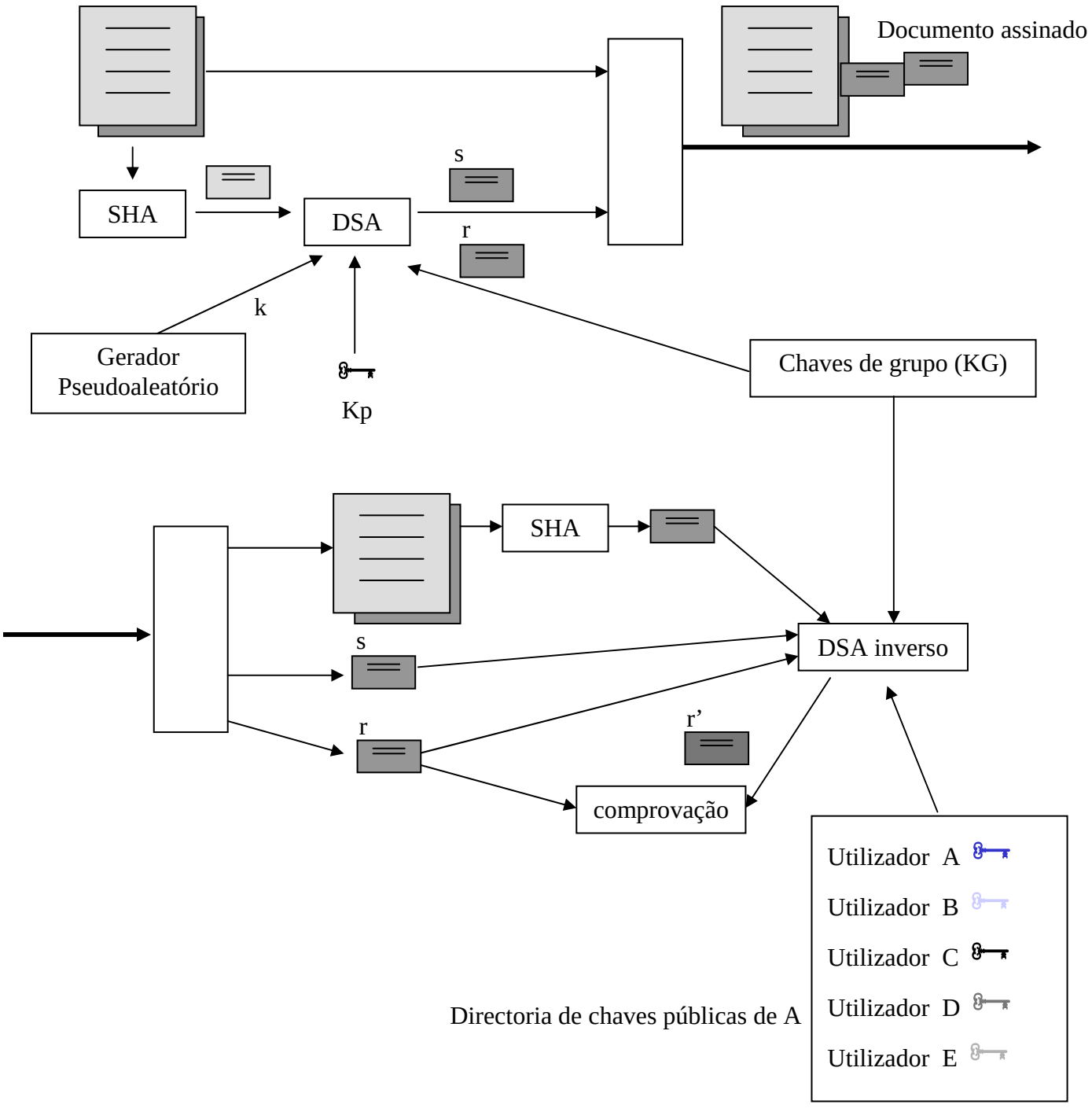
2.3 DIGITAL SIGNATURE STANDART

O NIST adoptou o sistema *Digital Signature Standart* (DSS) como padrão para os sistemas de assinatura digital. O seu funcionamento baseia-se na utilização da função *Hash* SHA e o algoritmo assimétrico *Digital Signature Algorithm* (DSA) (o DSA é um algoritmo assimétrico que apenas se utiliza com assinatura digital, mas como utiliza mais parâmetros que o RSA consegue-se um maior grau de segurança).

Os parâmetros utilizados no sistema DSS são os seguintes:

- chaves públicas de grupo (KG), são comuns e públicas num grupo de utilizadores;
- chave pública (KU), é gerada uma por cada utilizador a partir das KG e são tornadas públicas;
- chave privada (KP), é privada para cada utilizador e é gerada das anteriores;
- k é um número aleatório, gerado um por cada assinatura, não permite que seja criada uma mesma assinatura para o mesmo texto do mesmo utilizador;
- s e r, são duas palavras de 160 bits que formam a assinatura de um texto.

O número k não permite que para o mesmo texto, do mesmo utilizador, seja gerada uma mesma assinatura. Este processo de DSS pode ser apreciado na figura da página seguinte.


Documento assinado
SHA
DSA
s
r
k
Gerador Pseudoaleatório
Kp
Chaves de grupo (KG)
SHA
s
r
r'
DSA inverso
comprovação
Utilizador A
Utilizador B
Utilizador C
Utilizador D
Utilizador E
Directoria de chaves públicas de A

ANEXO K

O PROTOCOLO TCP

O PROTOCOLO TCP

1. DESCRIÇÃO GERAL

Não se pode falar de redes sem falar do TCP (*Transmission Control Protocol* ou Protocolo de Controlo de Transmissão). O conjunto de protocolos originalmente desenvolvido pela Universidade da Califórnia em *Berkeley*, sob contrato para o Departamento de Defesa dos EUA, tornou-se no conjunto de protocolos padrão das redes locais e remotas.

Mesmo antes da internet entrar no vocabulário de todo o mundo, o TCP já era o protocolo mais utilizado para as grandes redes, formadas por produtos de diferentes fornecedores, e tinha sido escolhido pela *Microsoft* como o protocolo preferencial para o *Windows NT*, devido às limitações técnicas do seu próprio conjunto de protocolos.

Entretanto, ao contrário dos protocolos proprietários para redes locais da *Microsoft* e da *Novell*, que foram desenhados para serem praticamente "*plug and play*", as necessidades que orientaram o desenvolvimento do TCP obrigaram ao estabelecimento de uma série de parametrizações e configurações que devem ser conhecidas pelos profissionais envolvidos na instalação, administração e supervisão de redes.

O TCP é um conjunto de protocolos utilizados na internet que inclui uma série de padrões que servem para especificar a forma como os computadores[2] se interligam de forma a permitir a criação de ligações nas redes e para o encaminhamento de pacotes através dessas ligações.

Os protocolos da internet são o resultado de um projecto da DARPA (*Defense Advanced Research Projects Agency*) sobre a problemática das ligações entre redes no final dos anos 70. Este tipo de protocolo foi utilizado em todas as redes de longa distância do sistema de Defesa dos EUA em 1983, mas não foi amplamente aceite até ser incorporado ao BSD (*Berkeley Software Distribution*). Os motivos porque o TCP vingou no mercado foram os seguintes:

- possui uma estrutura cliente-servidor robusta, o TCP é uma excelente plataforma cliente-servidor, especialmente em ambientes WAN.
- permite compartilhar informações; milhares de organizações militares, educacionais, científicas e comerciais partilham dados, correio electrónico (*e-mail*) e outros serviços na internet ou em *intranet* usando o TCP.
- grande disponibilidade, as implementações do TCP estão disponíveis praticamente em todos os sistemas operacionais conhecidos. O código fonte está amplamente

[2] Utilizamos o exemplo de computadores por melhor servir no exemplo de qualquer tipo de rede, se pretendermos extrapolar os conceitos para o caso específico da internet, esse poderia ser substituído por servidor.

disponível em várias implementações. Actualmente, os produtos apresentados pelos fabricantes, nomeadamente *bridges*, *routers* e analisadores de redes oferecem suporte para o TCP.

2. O MODELO TCP

É natural que se conheça, por leitura de revistas da especialidade, o "Modelo OSI[3] com as suas sete camadas". Todo o software de redes é baseado em alguma arquitectura de camadas, e normalmente refere-se a um grupo de protocolos criado para funcionar em conjunto como uma camada de protocolos[4]. Os protocolos de uma dada camada normalmente interagem somente com os protocolos das camadas imediatamente superior e inferior.

O modelo de camadas traz a vantagem de modularizar naturalmente o software de redes, permitindo a sua expansão com novos recursos, novas tecnologias ou aperfeiçoamentos sobre a estrutura existente, de forma gradual.

Entretanto, o Modelo OSI é um modelo conceptual, e não a arquitectura de uma implementação real de protocolos de rede. Mesmo os protocolos definidos como padrão oficial pela *International Standards Organization* (ISO), entidade criadora do modelo OSI, não foram projectados e construídos segundo este modelo.

O TCP foi desenhado segundo uma arquitectura de camadas, onde diversas camadas de software interagem somente com as camadas superior e inferior. Há diversas semelhanças com o modelo conceptual OSI da ISO, mas o TCP é anterior à formalização deste modelo e portanto possui algumas diferenças.

Visto superficialmente, o TCP possui quatro camadas, desde as aplicações de rede até ao meio físico que transporta os sinais eléctricos até o seu destino:

[3] *Open Sistem Interconetion.*

[4] Tradução do inglês, *protocol stack.*

CAMADAS	PROTOCOLOS
4. Aplicação	FTP, TELNET, HTTP, SMTP/POP3, etc.
3. Transporte	TCP, UDP
2. Rede	IP
1. Físico	Ethernet

Além das camadas propriamente ditas, temos uma série de componentes, que realizam a interface entre as camadas:

Aplicação / Transporte	DNS, *Sockets*
Rede / Ligação	ARP, DHCP

Apresenta-se de seguida uma descrição da função de cada camada do TCP:

Camada 1 - os protocolos de ligação têm a função de fazer com que as informações sejam transmitidas de um computador para outro, num serviço compartilhado ou numa ligação ponto-a-ponto (ex: modem). A preocupação destes protocolos é permitir o uso do meio físico que liga os computadores na rede e fazer com que os *bytes* enviados por um computador cheguem a um outro computador directamente, desde que exista uma ligação física directa entre si.

Camada 2 - o protocolo de rede, é responsável por fazer com que as informações enviadas por um computador cheguem a outros computadores mesmo que eles estejam em redes fisicamente distintas, ou seja, não exista ligação directa entre eles. Como o próprio nome (internet) diz, o *Internet Protocol* (IP) realiza a ligação entre redes e é onde se encontra a capacidade da rede TCP se "reconfigurar" quando uma parte da rede está fora de serviço, procurando um caminho (rota) alternativo para a comunicação.

Camada 3 - os protocolos de transporte mudam o objectivo, que era ligar dois equipamentos, para ligar dois programas. Podem-se ter, num mesmo computador, vários programas a funcionarem simultaneamente com a rede, por exemplo um *browser Web* e um serviço de *e-mail*. Da mesma forma, um mesmo computador pode estar ligado ao mesmo tempo a um servidor *Web* e a um servidor POP3. O protocolo de transporte TCP atribui a cada

programa um número de porta, que é anexado a cada pacote de modo que o TCP saiba para qual programa entregar cada mensagem recebida pela rede.

Camada 4 - os protocolos de aplicação são específicos para cada programa que faz uso da rede. Desta forma existe um protocolo para a conversação entre um servidor *web* e um *browser web* (HTTP), um protocolo para a conversação entre um cliente *Telnet* e um servidor *Telnet*, e assim sucessivamente. Cada aplicação de rede tem o seu próprio protocolo de comunicação, que utiliza os protocolos das camadas mais baixas para poder atingir o seu destino.

Para melhor se compreender o protocolo TCP e as redes que o utilizam, apresentam-se de seguida alguns conceitos básicos que são importantes para o seu esclarecimento.

2.1 NÚMERO DE IP

Podemos fazer uma analogia entre computadores e telefones e o número de IP. Se o número IP for visto como um número de telefone com todos os números que se utilizam para se efectuar uma chamada internacional, isto significa que qualquer computador poderá contactar outro computador usando o número de IP, para isso apenas é necessário que exista um caminho entre os dois computadores. É evidente que todos os computadores de uma rede tem de ter um número de IP, e obrigatoriamente significa que dois computadores na mesma rede não podem ter o mesmo número de IP.

O número de IP tem 4 *bytes* de tamanho e tem um formato específico, exemplificado pode ser deste tipo: 248.541.345.07, em que cada grupamento de três algarismos só pode ir de 0 a 255 (pois essa é a capacidade de 1 byte).

2.2 MÁSCARA DE SUB-REDE

Numa rede TCP, cada computador (ou melhor, cada placa de rede, caso o computador possua mais do que uma) possui um endereço numérico formado por 4 *bytes*, geralmente escritos na forma w.x.y.z. Além deste Endereço IP, cada computador possui uma máscara de rede (*network mask* ou *subnet mask*), que é um número do mesmo tipo mas com a restrição que deve começar por uma sequência contínua de bits em 1, seguida por uma sequência contínua de bits em zero. Ou seja, a máscara de rede pode ser um número como 11111111.11111111.00000000.00000000 (255.255.0.0), mas nunca um número como 11111111.11111111.00000111.00000000 (255.255.7.0).

Existem 3 classes de endereços IP: classes A, B e C. A diferença entre as classes é a forma como o número de IP é interpretado. O número de IP é divido em duas partes: o endereço da

rede e o endereço da sub-rede. Considere o número IP da seguinte forma: w.x.y.z (ex: 248.541.345.07)

Classe	Número de IP	Indicador da rede	Indicador da Sub-rede	Número de redes disponíveis	Número de sub-redes disponíveis
A	1.126	w	x.y.z	126	16,777,214
B	128.191	w.x	y.z	16,384	65,534
C	192.223	w.x.y	z	2,097,151	254

Obs: O endereço 192.168 é reservado para uso em redes internas, o endereço 127 é utilizado para testes de *loopback* e os acima de 224 (inclusive) são reservados para protocolos especiais.

Uma sub-rede é uma rede que pode ser ligada a uma outra através de qualquer rede ligada à anterior. A rede que se pretende ligar recebe um número de IP, e distribui os números de IP dentro da sua sub-rede. As classes apenas definem quantas sub-redes um número de IP poderá ter. De acordo com a tabela, existem 126 números de IP da classe A e cada um deles pode ter 16.777.214 sub-redes. Para uma rede como a internet é fácil deduzir que não existem endereços classe A suficientes para abarcar todo o universo de utilizadores. Actualmente não existem endereços classe A e B disponíveis na internet, e os de classe C não chegam para as necessidades futuras, o *Internet Engenniering Task Force* (IETF) está a estudar a expansão desses números de forma a colmatar essas necessidades.

As máscaras de sub-rede identificam a classe do número de IP. À primeira vista isso parece desnecessário, pois basta olhar o primeiro número do número do IP para determinar a sua classe. Mas acontece que um número de IP classe A pode funcionar como um classe B ou classe C, dependendo da estrutura interna da sua sub-rede. Um caso prático: imagine-se uma empresa com 200 PC ligados entre si em rede. A matriz tem um número de IP classe A, por exemplo o 100 e distribui as suas sub-redes da seguinte forma:

100.1.0.0	Matriz
100.2.0.0	PC 1
100.3.0.0	PC 2
.....	
100.201.0.0	PC 200

Para os PC, o número de IP (ex: 100.201.0.0) é de classe B, pois só tem 16.384 sub-redes disponíveis. Para os restantes PC ainda é possível distribuírem-se em sub-redes, as quais teriam número de IP classe C.

Para que o encaminhamento funcione correctamente, os computadores precisam saber qual a classe do número de IP, e elas são as seguintes:

Classe	**Máscara de Sub-rede**
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

2.3 *GATEWAY* PADRÃO (DEFAULT *GATEWAY*)

O *gateway* padrão é um computador para quem pedimos ajuda quando não conseguimos encontrar outro computador na rede. O modo de funcionamento é o seguinte, quando uma computador na rede precisa de comunicar com outro, emite um pedido de ligação (esse pedido é feito através de *broadcasting*, ou seja, o computador envia um pedido a toda a rede, mas apenas o computador destino irá responder) e aguarda uma resposta. Se a resposta não vier, ela entra em contacto com o *gateway* padrão e solicita que o mesmo ligue com o computador destino. Se o *gateway* conseguir ligar-se ao computador destino, ele fica como "intermediador" dessa ligação, caso contrário ele avisa o computador requerente que não foi possível encontrar o computador destino.

Esse tipo de estrutura de procura visa diminuir o tráfego e aumentar a eficácia das redes. Se todas as solicitações de ligação realizadas na internet (e em todas as redes ligadas à internet) fossem enviadas para todos os computadores ligados à rede, provocariam um tráfego enorme.

Assim, durante o processo de transmissão, a procura vai ser repartida por níveis, primeiro na LAN, depois na WAN de cidade ou distrito, depois na WAN nacional até chegar à WAN internacional. Reduz-se desse modo todo o tráfego interno às WAN's e LAN's, aliviando as ligações.

2.4 *DOMAIN NAME SYSTEM* (DNS)

Para melhor percebermos este sistema vamos fazer novamente uma analogia com o telefone. Quando se pretende telefonar para o café da esquina, é necessário consultar a lista telefónica, encontrar o número telefone e ligar, isto é, não se consegue telefonar para lugar algum se não se souber o número de telefone. Nas redes baseadas no protocolo TCP acontece a mesma coisa, os utilizadores não decoram o número IP dos computadores, mas sim os seus nomes. Mas para se localizar um computador na rede, precisamos do seu número de IP. Para resolver isso, foi criado o DNS, um serviço disponível na rede que, dado um nome de um computador, ele devolve o número de IP do mesmo.

Uma particularidade destes casos, quando estamos numa rede local ligada a alguma outra, é recomendável que o servidor DNS (o programa que oferece o serviço DNS) seja executado no computador que interliga as duas redes (o *gateway*), para que no caso do nome requisitado não existir na rede local, o DNS possa pedir ao servidor DNS da outra rede para pesquisar o nome a procurar.

O Windows NT oferece um serviço semelhante, o WINS (*Windows Internet Name System*). A principal diferença entre os dois é que o DNS usa uma tabela estática, e o WINS usa uma tabela dinâmica.

2.5 *DYNAMIC HOST CONFIGURATION PROTOCOL* (DHCP)

Numa rede TCP, os computadores têm de ter um número de IP distinto. Isto significa que antes de colocar um novo computador na rede, o administrador teria de saber quais os números que estão a ser utilizados para poder escolher um número adequado para um novo computador.

Em pequenas redes isso é possível de ser feito, mas em grandes redes isso torna-se uma tarefa impraticável e sujeita a erros, para evitar isso, foi criado o DHCP. Quando um computador entra na rede a primeira tarefa é procurar o servidor DHCP (cujo número de IP foi previamente fornecido) e solicitar um número de IP. O servidor verifica qual o número disponível, informa o solicitante desse número e torna-o indisponível para futuros pedidos de IP, desta maneira, a

administração dos número de IP é feita automaticamente e não existem problemas de conflito. Quando o requerente sai da rede, o servidor DHCP disponibiliza novamente esse número de IP.

2.6 PORTAS

Uma porta pode ser vista como um canal de comunicações para um computador. Os pacotes de informações que chegam a um computador não são apenas endereçados ao computador, mas sim à porta de um determinado computador.

Entretanto, um computador geralmente não está a apontar a todas as portas disponíveis, ele aponta para algumas portas específicas, e não responde a um pedido que chegue a uma porta para a qual ele não esteja a apontar.

Existem uma série de portas predefinidas para certos serviços que são aceites universalmente, as principais são:

Serviço	Porta	Descrição
FTP	21	*File Transfer Protocol*
Telnet	23	Protocolo para se ligar remotamente a um servidor
SMTP	25	Para enviar um e-mail
Gopher	70	Browser baseado em modo texto
HTTP	80	Protocolo WWW - Netscape, Mosaic
POP3	110	Para receber *e-mail*
NNTP	119	Newsgroups
IRC	6667	*Internet Relay Chat*
Compuserve	4144	Compuserve WinCIM
AOL	5190	*America Online*
MSN	569	*Microsoft Network*

3. VISÃO GERAL DE UMA REDE TCP

Numa rede que utiliza o TCP pode-se encontar uma estrutura básica composta por um (ou mais) servidores utilizando servidores de DNS (ou WINS), DHCP, SMTP, POP3 e servidores de outros serviços (HTTP, *Gopher*, *Telnet*, etc.) e os computadores clientes solicitadores desses serviços. Para se interligar essa rede a uma outra rede TCP, é necessário o uso de um *gateway*[5] e da correcta configuração da rede. Existem 2 maneiras de se ligar a LAN à internet:

- Atribuindo-se um número de IP válido para cada computador na rede, o que pode ser impossível para redes com muitos computadores.
- Atribuindo-se um número de IP válido para o *gateway* e utiliza-se o número de IP 192.168.x.x internamente.

O segundo caso é o mais praticável, e de uma forma simplista podemos explicar que nenhum computador ligado directamente a uma rede tem um IP 192.168.x.x. Isso é necessário porque, como foi referido, nenhum computador pode ter um número de IP que já esteja a ser utilizado por um outro computador.

O *gateway* tem duas interfaces de rede, uma para se ligar à internet e outra para se ligar à LAN, à interface da internet atribuí-se o número de IP válido na internet e na da LAN o número de IP do tipo 192.168.x.x (normalmente 192.168.0.1). Nos computadores da LAN o número de IP é do tipo 192.168.x.x (em que o primeiro "x" é o mesmo do *gateway*) e o *gateway default* é o IP do *gateway* virado para a LAN (192.168.x.x). Dessa forma podemos ter até 16.384 computadores na internet por número de IP válido. Essa estrutura também facilita a adopção de medidas de segurança contra intrusos da internet, pois como todo o tráfego internet passa pelo *gateway*, basta protegê-lo para proteger toda a LAN.

4. PROTOCOLOS DO TCP

4.1 TCP E IP

O TCP e o IP são apenas dois elementos da família TCP. O IP é um protocolo que providencia a entrega de pacotes para todos os outros protocolos da família TCP e oferece um sistema de entrega de dados sem ligação. Isto é, não garante que os pacotes IP cheguem ao seu destino, nem que sejam recebidos na ordem em que foram enviados. Desta maneira, a

[5] Define-se gateway como um servidor que é utilizado para ligar duas ou mais redes distintas.

responsabilidade pelos dados contidos no pacote do IP (e sua sequência) é tarefa de protocolos de mais alto-nível.

Talvez o protocolo de alto nível do IP mais comum seja o TCP. O TCP oferece um bom serviço de protocolo baseado em ligações com encapsulamento no protocolo IP. O TCP garante a entrega dos pacotes, assegura a sequência dos pacotes, e providencia um "*checksum*" que valida tanto o cabeçalho como os dados do pacote. No caso da rede perder ou introduzir erros num pacote TCP durante a transmissão, o TCP efectua a retransmissão do pacote em falta ou com erros. Essa fiabilidade torna o TCP o protocolo escolhido para transmissões baseadas em sessões, aplicações cliente-servidor e em serviços críticos como correio electrónico.

Porém essa fiabilidade tem um preço, os cabeçalhos dos pacotes TCP requerem o uso de bits adicionais para assegurar a correcta sequência da informação, bem como um "*checksum*" obrigatório para garantir a integridade do cabeçalho e dos dados. Para garantir a entrega dos pacotes, o protocolo também requer que o destinatário informe que recebeu o pacote. O acto de informar do recebido (conhecido por ACK's, de *acknowledgments*) provoca tráfego adicional na rede, aumentando a fiabilidade em detrimento da taxa de transferência de dados. Para reduzir o impacto na performance, a maioria dos servidores envia um ACK após ter recebido todos os pacotes de um bloco de dados ou quando um ACK expira.

Em resumo, qualquer computador ligado a uma rede com o protocolo de rede TCP deve ser configurado pelo menos com três parâmetros, a saber: o seu endereço IP exclusivo, a sua máscara de rede (que deve ser a mesma utilizada por todos os computadores na mesma LAN) e o endereço IP do *default gateway*.

4.2 *USER DATAGRAM PROTOCOL* (UDP)

Se a confiabilidade não é essencial, o UDP, um complemento do TCP, oferece um serviço de transmissão de dados sem ligação que não garante nem a entrega nem a correcta sequência dos pacotes enviados (à semelhança do protocolo IP).

4.3 ARP E ICMP

Existem ainda dois outros protocolos da família TCP com importantes funções, embora essas funções não estejam directamente relacionadas com a transmissão de dados: ARP (*Address Resolution Protocol*) e ICMP (*Internet Control Message Protocol*). O ARP e o ICMP são protocolos de manutenção que mantêm a estrutura do IP e normalmente são invisíveis aos utilizadores e às aplicações.

Os cabeçalhos do IP contêm tanto o endereço IP da origem quanto o do destino, mas o endereço do hardware também tem de ser conhecido. O IP obtém um endereço de hardware de um determinado sistema e difunde-o pela rede num pacote especial de requisição (um pacote ARP de requisição) contendo o endereço IP do sistema com o qual se pretende comunicar. Todos os nós da rede local que tiverem o ARP habilitado detectam essa difusão, e o sistema que tem o número de IP em questão envia um pacote contendo o seu endereço de hardware para o computador que o solicitou. O endereço de hardware e o endereço IP do computador é armazenado no cache do ARP para futuras utilizações. Como a resposta ARP também é feita na forma de difusão, é normal que outros usem essa informação para actualizar os arquivos de ARP.

O ICMP permite que dois nós numa rede IP compartilhem o *status* do IP e a informação de erros. Esta informação pode ser usada por protocolos de alto nível para tratar problemas de transmissão ou para administradores de rede para detecção de problemas na rede. Embora esteja encapsulado em pacotes IP, o ICMP não é considerado um protocolo de alto nível (ele é necessário na implementação do TCP/IP). A aplicação "*ping*" faz uso do ICMP para determinar se um certo endereço IP na rede está operacional. Isto é útil para diagnosticar problemas em redes IP ou falhas em *gateways*.

4.4 OUTROS PROTOCOLOS

Além desses protocolos referidos, existem os protocolos de alto-nível, como o *Telnet*, FTP, http, etc.. Vamos apresentar de seguida uma breve descrição desses protocolos:

4.4.1 TELNET

É um protocolo que permite o *logon* em computadores remotos. Desta forma pode ser utilizado o computador remoto para realizar o processamento. No Windows NT existe o RAS (*Remote Access Service*) que tem os mesmos objectivos do *Telnet*.

4.4.2 FTP

File Transfer Protocol (protocolo de transferência de ficheiros), como o nome refere é utilizado para a transferência de ficheiros.

4.4.3 HTTP

Hyper Text Transfer Protocol é o protocolo utilizado na internet, onde se transmite textos, gráficos e qualquer outro tipo de arquivo (substituindo o FTP).

ANEXO L

CARACTERÍSTICAS DO SecNet

CARACTERÍSTICAS DO SecNet

A aplicação SecNet garante a confidencialidade, a integridade, a autenticação, o controlo de acessos, o não-repúdio e a assinatura digital da informação.

Esta aplicação foi desenvolvida para operar sobre plataforma Windows (95/98, 2000 e NT).

A aplicação SecNet baseia-se na estrutura PKI realizada com base na norma PKIX do *Internet Engineering Task Force* (IETF) e implementa os seguintes algoritmos:

- Triple Data Encryption Standard (TDES);
- Rivest Chamir e Adleman (RSA);
- Standard Hash Algorithm 1 (SHA-1);
- E a recomendação X.509v3 para certificados digitais.

A estrutura base foi implementada de forma a tornar a aplicação generalista, podendo a qualquer momento, se a conjuntura criptográfica se alterar ou apenas para personalizar a aplicação de acordo com a preferência do utilizador, ser actualizada com novos algoritmos e esquemas, não sendo necessário alterar a estrutura base.

Todos os processos e comandos são automatizados, de forma a que o utilizador apenas tenha de interagir com a aplicação cliente, fornecendo dados de confirmação às acções solicitadas pela aplicação. Aprofundar os fundamentos e funcionalidades desta aplicação é deveras mais difícil do que utilizá-la, porém, é importante que o futuro utilizador tenha conhecimento de algumas das capacidades que esta possui e quais os métodos que tem ao seu dispor para maximizar a componente segurança.

Esta aplicação implementa um esquema de Certificação Digital gerido por uma Entidade Certificadora, no qual os Certificados Digitais têm como objectivo garantir que todos os utilizadores estejam devidamente autenticados e autorizados. Os certificados contêm informação necessária para que se proceda à identificação do utilizador, tal como o nome, o n.º de série, a instituição e o endereço IP ou e-mail, o certificado é assinado pela entidade certificadora que o gerou e que o torna válido.

ANEXO M

GESTÃO DO CONTROLO DE ACESSO POR PASSWORD

GESTÃO DO CONTROLO DE ACESSO POR PASSWORD

Na gestão do controlo de acesso por password serão emitidos um identificador para cada utilizador, que continuará a ser o número mecanográfico, e a atribuição de uma password inicial. Posteriormente o processo de gestão deve ter em atenção o seguinte:

- o sistema será configurado de forma a que todos os utilizadores mudem as suas password pelo menos todos os três meses.
- os procedimentos para notificar os utilizadores da suas password serão os seguintes:
    - aos utilizadores com funções específicas serão entregues as password em envelopes lacrados, os restantes utilizadores serão informados, via secção de segurança, da activação do acesso;
    - a cada utilizador deve ser-lhe exigido que assine em documento próprio que tomou conhecimento da sua password inicial;
    - todas as password serão geradas e serão protegidas usando algoritmos aprovados e procedimentos de segurança.
- os utilizadores são responsáveis por manter o segredo da própria password e em caso de suspeita que a confidencialidade da sua password tenha sido comprometida devem alterar a sua password e informar imediatamente a secção de segurança da ocorrência;
- no caso de um utilizador esquecer a password será emitida uma nova com o procedimento referido;
- no caso de um utilizador ter um período de inactividade entre os 45 a 90 dias o acesso deve ser-lhe inibido;
- no caso de um utilizador ter um período de inactividade de 120 dias deve ser simplesmente "eliminado" da BD de acesso;
- no caso de um curto período de inactividade, uma estação de trabalho deverá ter uma protecção de forma a solicitar password para reentrar no sistema;
- o sistema encerrará a conta de um utilizador depois de várias tentativas sucessivas falhadas. O número permitido de tentativas falhadas sucessivas nunca deve ser mais do que cinco. Só os gestores do sistema é que devem ser autorizados a fechar contas;
- os utilizadores dos sistemas devem informar sobre todos os acontecimentos ou sobre uma suspeita de incidentes de segurança, devem manter uma consciência e concordância com os procedimentos de segurança definidos superiormente e com as exigências legais relativas ao tratamento da informação;

- todo o pessoal envolvido em projectos será esclarecido sobre o nível apropriado para a classificação de informação a que tem acesso;
- qualquer pessoa substituída ou suspensa de projectos, ou do cargo que ocupa ser-lhe-á negado o acesso imediatamente. As autorizações e os privilégios aos sistemas deverão ser-lhe imediatamente retirados.

ANEXO N

LISTA DE POLÍTICA DE SEGURANÇA DE INFORMAÇÕES

LISTA DE POLÍTICA DE SEGURANÇA DE INFORMAÇÕES

A lista que se apresenta neste anexo pode ser utilizada como uma lista de controlo, tanto pela gestão de segurança de sistemas, como pela equipa de auditoria. Para a gestão de segurança, esta lista pode servir como um conjunto de tarefas a serem realizadas na implementação da política de segurança na organização, para as equipas de auditoria podem servir como tarefas a cumprir na verificação da segurança traçada superiormente.

1. Elaborar, divulgar e manter actualizado o documento que descreve a política de segurança da informação.
2. Os órgãos de gestão da organização devem estar comprometidos com a política de segurança da informação, a qual deve ser implementada de acordo com o documento formal por ela aprovado.
3. Definir uma estrutura organizacional responsável pela segurança, a qual deve aprovar e revisar as políticas de segurança, designar funções de segurança e coordenar a implementação da política.
4. Estabelecer procedimentos de segurança de pessoas, com intuito de reduzir ou evitar erros humanos, uso inadequado dos recursos computacionais, fraude ou roubo, por meio de um processo rigoroso de recrutamento de pessoal e de controlo sobre acessos a informações classificadas.
5. Todos os elementos da organização devem ter conhecimento dos riscos de segurança da informação e das suas responsabilidades em relação a esse assunto. Devem promover-se treinos de segurança para difusão de práticas e padrões de segurança, criando uma cultura de segurança na organização.
6. Controlar e classificar os recursos computacionais de acordo com o grau de confidencialidade, prioridade e importância para a organização. Todos os recursos (hardware, software, dados, documentos, etc.) devem ser geridos por um responsável.
7. Definir padrões adequados de segurança física para prevenir acessos não autorizados, danos ou interferências em actividades críticas. Devem ser estabelecidos limites de acesso ou áreas de segurança com dispositivos de controlo de entrada. Todos os equipamentos e cabos de energia eléctrica e de telecomunicações devem ser protegidos contra intercepções, dano, falha de energia, picos de luz e outros problemas eléctricos.
8. Implementar o controlo de acesso lógico aos sistemas de forma a prevenir acessos não autorizados.

9. Gerir os recursos computacionais e as redes, seguindo requisitos de segurança previamente definidos.
10. Definir procedimentos de *backup* e de reposição dos sistemas computacionais para garantir a integridade e a disponibilidade de dados e software. A frequência de *backup* deve ser apropriada e deve ser guardada pelo menos uma cópia em local seguro. Os procedimentos de reposição devem ser periodicamente testados para garantir sua efectividade na eventualidade de serem necessários.
11. Investigar qualquer incidente que comprometa a segurança dos sistemas. Os registos desses incidentes devem ser mantidos e periodicamente analisados para detectar vulnerabilidades na política de segurança adoptada.
12. Após uma violação da política de segurança, tomar as medidas necessárias para a identificação das causas e agentes, para a correcção das vulnerabilidades e punição dos infractores.
13. Elaborar um plano de auditorias para serem verificados regularmente todos aspectos de segurança a fim de determinar se as políticas estão a ser efectivamente cumpridas ou se são necessárias modificações.

ANEXO O

GUIÃO DAS ENTREVISTAS

GUIÃO DAS ENTREVISTAS

1. AUTORIDADE NACIONAL DE SEGURANÇA

a. O GNS, em termos de responsabilidades de segurança nacional, quais as suas principais competências?

b. As organizações Internacionais têm pontos de vista semelhantes em termos dos documentos legais sobre segurança, ou seguem uma política de segurança da informação muito comum? Os documentos das OI (NATO/UEO/EU) são de alguma forma integrados?

c. Que tipo de responsabilidade tem o GNS sobre a Segurança dos SI, numa perspectiva de análise de riscos, política de segurança da informação e planos de contingência?

d. Existe uma política de segurança da informação a nível nacional? Qual o papel do GNS sobre o assunto?

e. Que tipo de colaboração é estabelecida com o Instituto de Informática do Ministério das Finanças? Que responsabilidades tem a ANS sobre o "*Manual Técnico da Segurança dos Sistemas e Tecnologias de Informação"*?

2. REPARTIÇÃO DE APOIO DO GNS

a. Existe alguma empresa, instituto ou universidade credenciada pelo GNS?
b. O GNS, como o responsável pelos documentos classificados OTAN, tem algum SI para tratamento da documentação em formato digital, recepção dos mesmos e posterior envio para os Sub-Registos OTAN?
c. O Sistema de Segurança Electrónica da Informação (SEIF) assenta o seu funcionamento em que tipo de estrutura?
d. A certificação do SEIF foi feita pela OTAN? Isso quer dizer que a PKI é aceite e certificada no seio da OTAN?
e. Quais os circuitos de comunicações por onde passa a informação tratada pelo GNS?

3. DIRECTOR DO CIE

a. Actualmente o CIE depende do VCEME. Quando está prevista a alteração da dependência hierárquica? E que vantagens poderá proporcionar ao Centro?

b. Existem directivas para o CIE seguir uma política de segurança dos SI para o Exército?

c. Que segurança está a ser implementada nos SI desenvolvidos?

d. Existe uma repartição responsável pela segurança dos SI desenvolvidos no CIE? Face à complexidade e exigência dos mecanismos de segurança, não será mais eficaz que exista uma secção independente das repartições que estude e planeie metodologias a aplicar nos SI e BD?

e. Existem alguns sistemas de monitorização de segurança accionados pelo CIE?

f. Que alterações deveriam ser realizadas para que o CIE desenvolva SI com a segurança desejável? Estão definidos requisitos mínimos de segurança para o processo de aquisição de equipamento ou aplicações?

4. CHEFE DA REPARTIÇÃO DE PROJECTOS DO CIE

a. Qual a entidade que toma a decisão da aplicação dos sistemas de segurança para os SI desenvolvidos ou a desenvolver no CIE?

b. Como são definidos os controlos de acesso aos SI e que tipo de controlo está a ser implementado?

c. A informação de e para as BD é processada através de algum algoritmo de cifra?

d. Existe formação dos utilizadores direccionada para questões de segurança? É feito algum plano de actualização/reciclagem para os utilizadores?

e. Que deve ser alterado para que os SI desenvolvidos tenham requisitos mínimos de segurança definidos?

f. Quais os problemas que devem ser ultrapassados para colmatar lacunas de segurança dos SI?

5. CHEFE DA REPARTIÇÃO DE REDES E PEQUENOS SISTEMAS DO CIE

a. Como são definidos os controlos de acesso aos SI e que tipo de controlo está a ser implementado?

b. A informação de e para as BD é processada através de algum algoritmo de cifra?

c. Existe formação dos utilizadores direccionada para questões de segurança? É feito algum plano de actualização/reciclagem para os utilizadores?

d. Que deve ser alterado para que os SI desenvolvidos tenham requisitos mínimos de segurança definidos?

e. Quais os problemas que devem ser ultrapassados para colmatar lacunas de segurança dos SI?

6. SOGRUPO, SI DA CAIXA GERAL DE DEPÓSITOS

a. Que tipo de controlo de acesso tem em funcionamento nos SI da CGD?

b. O sistema de segurança baseado nas password é definido pelos SO existentes? Que definições foram criadas para potenciar este tipo de controlo?

c. Como é que a informação é tratada quando do seu envio para os canais de comunicações? Como é que se processa o mecanismo de cifra e que tipo de algoritmo é utilizado? Esse algoritmo foi acreditado pela CGD?

d. A CGD tem algum mecanismo de acreditação de sistemas? Quais os elementos que compõem essa equipa interna?

e. O documento sobre a política de segurança foi elaborado segundo algum critério? De que é a responsabilidade pela sua elaboração?

f. Quem é que definiu a política de segurança dos sistemas de informação?

g. Que mecanismos de monitorização possuem para os controlo das operações efectuadas nos SI?

h. Existe alguma entidade ligada à CGD que seja responsável pelas auditorias de segurança?

i. De quem é a responsabilidade dos PCR e qual a razão pela qual foi decidido todas as áreas de sistemas críticos terem PCR para as respectivas áreas?

j. Que formação foi ministrada aos técnicos de sistemas?

k. Que tipo de responsabilidades distingue as funções dos técnicos de sistemas das dos técnicos de segurança?

7. INSTITUTO DAS TECNOLOGIAS DE INFORMAÇÃO DA JUSTIÇA

a. Quantas entidades certificadoras foram credenciadas pelo ITIJ?

b. Não existe nenhuma entidade certificadora para administração pública em geral?

c. Quais são as condições gerais que o auditor de segurança que é referido no artigo 16.º do Dec-Lei n.º 290-D/99tem de possuir para exercer a sua actividade?