Resolução do Conselho de Ministros n.º 16/94

Nos termos das alíneas *d*) e *g*) do artigo 202.º da Constituição, o Conselho de Ministros resolveu:

Aprovar, ao abrigo disposto na alínea *d*) do n.º 2 do artigo 8.º da Lei n.º 20/87, de 12 de Junho, as instruções para a segurança das telecomunicações, adiante designadas abreviadamente por SEGNAC 3, anexas à presente resolução e que dela fazem parte integrante.

Presidência do Conselho de Ministros, 24 de Fevereiro de 1994. — O Primeiro-Ministro, *Aníbal António Cavaco Silva.*

Instruções para a segurança nacional – Segurança das telecomunicações – SEGNAC 3

CAPÍTULO 1

1 — Generalidades:

1.1 — Objecto:

1.1.1 — As presentes instruções definem princípios básicos, normas e procedimentos destinados a garantir a segurança protectiva das matérias classificadas no âmbito dos organismos do Estado, quando transmitidas por meios eléctricos e electrónicos.

1.1.2 — Excluem-se do âmbito destas instruções:

A segurança das matérias classificadas no âmbito das Forças Armadas;

A segurança das matérias classificadas que forem objecto de disposições especiais estabelecidas em acordos internacionais a que o nosso país tenha aderido.

1.1.3 — A revisão e as propostas de alteração às presentes normas competem à Comissão Técnica do Sistema de Informações da República Portuguesa, em coordenação com a Autoridade Nacional de Segurança.

1.2 — Princípios básicos:

Os utilizadores dos meios de comunicação, nos seus locais de trabalho, nas suas próprias residências ou noutros locais públicos ou privados, devem proceder ao cumprimento das medidas preconizadas nas presentes instruções, constituindo estas uma necessidade permanente de segurança ditada pela larga experiência de análise das vulnerabilidades dos diversos meios de telecomunicações.

1.2.1 — Finalidades:

Determinar a cada membro envolvido na comunicação de matérias classificadas a necessidade de uso de meios de telecomunicações pelo menos com o mesmo grau de classificação de segurança;

Instruir os membros directamente envolvidos na comunicação de matérias classificadas sobre os requisitos gerais de segurança de telecomunicações.

CAPÍTULO 2

2 — Meios de telecomunicação não seguros:

São os seguintes os principais meios de telecomunicação não seguros a que se reportam as presentes instruções:

I) Intercomunicador;
II) Telefone;
III) Radiotelefone — telemóvel;
IV) Telecópia — fax;
V) Telex;
VI) Teleconferência;
VII) Correio electrónico.

2.1 — Intercomunicador:

O intercomunicador é um meio de comunicação de voz, limitado a um número restrito de utilizadores e circunscrito a departamento ou edifício, cuja utilização está caindo em desuso. Devido à sua vulnerabilidade, é proibida a sua utilização para discussão e comunicação de matérias classificadas, devendo cada aparelho ter indicação de «Meio não seguro».

Se, apesar de tudo, se encontrarem intercomunicadores instalados em áreas de segurança das classes 1 e 2 (SEGNAC 1, capítulo 5), quando estiverem activados, deverão ter, bem visível, a indicação de tal situação. Pretende-se, assim, evitar que possam ser indevidamente escutadas no exterior dessas áreas conversações que ali decorram.

2.2 — Telefone:

2.2.1 — Âmbito de utilização:

Um telefone pode ter os seguintes acessos:

I) Rede telefónica pública;
II) Rede telefónica privada (PPCA), com ou sem acesso à rede telefónica pública ou a outras redes telefónicas privadas;
III) Ligação ponto a ponto.

a) Acesso à rede telefónica pública:

Normalmente designados «linhas de rede», os telefones ligados à rede telefónica pública permitem, através da marcação de um número telefónico, o acesso à universalidade dos seus assinantes.

b) Acesso a uma rede telefónica privada:

Normalmente designados «extensões», os telefones ligados a centrais telefónicas privadas permitem, através da marcação de um número de extensão, a ligação a qualquer das outras extensões dessa central.

No caso de acesso à rede telefónica pública, ou a outra rede telefónica privada, a marcação do respectivo número de telefone, ou do número da extensão, terá de ser antecedida por um número de acesso à respectiva rede.

c) Ligações ponto a ponto:

Este tipo de ligação só permite a comunicação directa entre dois interlocutores.

2.2.2 — Tipos de equipamento telefónico:

Os telefones podem ser de vários tipos:

Telefones simples;
Telefones com características especiais;
Telefones chefe/secretária e telefones intercomunicadores.

a) Telefone simples:

Telefone de marcador rotativo (disco), ou de teclas, não possuindo qualquer outro dispositivo ou características que lhe permitam outras operações para além de fazer e receber chamadas.

b) Telefone com características especiais:

Telefone que, além das funções descritas no número anterior, está preparado com outros dispositivo especiais ou permite outras funções, como sejam:

Alta voz — que possibilita a conversação sem utilizar o microtelefone, permitindo que várias pessoas, numa mesma sala, possam participar na conversação telefónica;
Memória/programação — que possibilita memorizar os números de telefone mais utilizados e de programar outras facilidades;
Telefone sem fios — telefone cuja ligação do microauscultador à base do aparelho é feita por via rádio (sem fios), permitindo fazer e receber chamadas distanciadas da base do aparelho.

c) Telefone chefe/secretária e telefone intercomunicador:

Telefone que permite a partilha de uma ou mais linhas de rede por dois ou mais locais distintos, através de um comutador, tendo também, como facilidade, a possibilidade de intercomunicação entre todos os postos.

2.2.3 — Vulnerabilidades:

As ligações dos telefones às centrais públicas ou privadas passam por uma sucessão de meios, quer dentro das instalações, quer no exterior, de fácil acesso, que podem permitir a intercepção das comunicações, em qualquer ponto do circuito, sem recurso a equipamentos sofisticados.

A própria linha telefónica é um inegável veículo de fornecimento de energia permanente aos mais variados equipamentos de escuta, que poderão ser colocados em qualquer parte do seu percurso.

Existem centrais telefónicas privadas onde é possível programar facilidades que permitem a escuta e corte de chamadas sem sinal de intervenção.

O próprio equipamento telefónico é susceptível de fáceis alterações, as quais podem ser um veículo de escuta permanente em determinada área e que não é detectável pelo utilizador.

2.2.4 — Conclusões:

Face ao exposto no número anterior, há que considerar o seguinte:

a) É proibida a utilização de telefones não seguros para discussão e comunicação de matérias classificadas. O mesmo se aplica a conversações que, embora não versando matérias classificadas, possam, em conjugação com outras, comprometer informações classificadas;
b) Em situações de excepção e quando a urgência na comunicação for absolutamente essencial e ou a informação já não possa ser explorada em tempo útil e não se dispuser de outros meios mais seguros, é da inteira responsabilidade do utilizador a discussão ou comunicação de matérias classificadas, bem como de matérias não classificadas, mas consideradas sensíveis, através de meios telefónicos. Nestas circunstâncias, a comunicação de matérias classificadas deverá utilizar os meios telefónicos que a seguir se indicam, por ordem de prioridade, que deve ser observada tanto no originador como no destinatário:

I) Postos públicos;
II) Extensão de central telefónica privada para acesso à rede pública;
III) Linha de rede pública telefónica;
IV) Ligação ponto a ponto.

Em caso algum matérias classificadas de *Muito secreto* poderão ser transmitidas em claro, através de meios de comunicação telefónicos;

c) A programação das centrais telefónicas privadas deve ser rigorosa e frequentemente controlada por pessoal especializado, com vista a evitar a utilização de facilidades que permitam a escuta e corte de comunicações;
d) No que respeita à utilização de telefone sem fios, as vulnerabilidades destes são acrescidas das descritas no n.º 2.3.2, para radiotelefones, pelo que deverão ser observadas as recomendações do n.º 2.3.3 sempre que sejam utilizados;
e) Os telefones equipados com alta voz não devem estar instalados em áreas de segurança das classes 1 e 2 (SEGNAC 1, capítulo 5). Mas, se tal vier a verificar-se, quando se encontrarem activados, deverão ter, bem visível, a indicação de tal situação. Pretende-se, assim, evitar que possam ser indevidamente escutadas, no exterior dessas áreas, comunicações que ali decorram;
f) Para alertar os utilizadores quanto às vulnerabilidades das ligações telefónicas, cada telefone deverá ter a indicação de «Meio não seguro».

2.3 — Radiotelefone — telemóvel:

2.3.1 — Âmbito de utilização:

Um radiotelefone é um meio de comunicação de voz sem fios, integrado numa rede rádio privativa, que pode ser fixo, portátil ou instalado em viatura, permitindo ou não o acesso a redes telefónicas.

2.3.2 — Vulnerabilidades:

Todas as redes rádio são passíveis de ser escutadas com relativa facilidade, sem qualquer possibilidade de tal facto ser detectado. Qualquer simples receptor pode, inadvertida ou propositadamente, captar a emissão destas redes rádio, desde que estejam reunidas determinadas condições técnicas, tais como proximidade física, condições especiais de transmissão, etc.

Esta vulnerabilidade é agravada quando as redes rádio partilham os meios de telecomunicações com outras entidades com acesso aos mesmos canais e, inevitavelmente, ouvem todas as comunicações que por lá passam.

2.3.3 — Conclusões:

Deste modo, há que considerar o seguinte:

a) É proibida a utilização de radiotelefones para tratamento e comunicação de matérias classificadas. O mesmo se aplica a conversações que, embora não versando matérias classificadas, possam, em conjugação com outras, comprometer qualquer informação classificada;
b) Em situações de excepção e quando a urgência na comunicação for absolutamente essencial e a informação já não possa ser explorada em tempo útil e não se disponha de outros meios mais seguros, é da inteira responsabilidade do utilizador a discussão e comunicação de matérias classificadas, bem como de matérias não classificadas, mas consideradas sensíveis, através de meios de comunicação radiotelefónicos.

Em caso algum matérias classificadas de *Secreto* e *Muito secreto* poderão ser transmitidas em claro através de meios de comunicação radiotelefónicos;

c) Com a finalidade de advertir os utilizadores das vulnerabilidades das ligações rádio, cada radiotelefone, desde que não esteja instalado em viatura, deverá ter indicação de «Meio não seguro».

2.4 — Telecópia — fax:
2.4.1 — Âmbito de utilização:
É um meio de comunicação de documentos através de redes telefónicas, utilizando para o efeito um telecopiador acopulado a um telefone.
A sua capacidade de acesso é a mesma que para os telefones, conforme descrito no n.º 2.2.1
2.4.2 — Vulnerabilidades:
Para além das vulnerabilidades do telefone descritas no n.º 2.2.3, acrescem as devidas à possibilidade de mistificação dos documentos.
A mistificação consiste em deturpar e alterar os documentos, o que pode ser feito através de um outro equipamento que se introduza, com fins fraudulentos, no circuito.
2.4.3 — Conclusões:
Deste modo, há que considerar o seguinte:

a) À semelhança de outras formas de circulação e distribuição de documentos, deverá existir um sistema de controlo de todas as entradas e saídas de documentos, com especificação, designadamente, de originador, destinatário e grupo data/hora;
b) Quando da comunicação de matérias classificadas, deverão ser respeitados os procedimentos referentes à distribuição e transferência de documentos classificados constantes no n.º 7.2 do SEGNAC 1;
c) É proibida a utilização de telecópia para comunicação de matérias classificadas.
Em situações de excepção e quando a rapidez de comunicação for absolutamente essencial e a informação já não possa ser explorada em tempo útil e não se disponha de outros meios mais seguros, as matérias classificadas poderão ser transmitidas em claro. Este procedimento apenas poderá ser adoptado com autorização expressa, caso a caso, do chefe de escalão envolvido, que será inteiramente responsável pelo facto.
Em caso algum matérias classificadas no grau de *Muito secreto* poderão ser transmitidas em claro;
d) As vulnerabilidades da utilização da telecópia poderão ser diminuídas se forem utilizadas, quer pelo originador, quer pelo destinatário, as prioridades estabelecidas para os meios telefónicos para ligação das telecópias indicadas no n.º 2.2.4, alínea *b*);
e) Para alertar os utilizadores quanto às vulnerabilidades da utilização da telecópia, cada equipamento deverá ter a indicação de «Meio não seguro».

2.5 — Telex:
2.5.1 — Âmbito de utilização:
É um meio de telecomunicação de textos através da rede telegráfica nacional ou em ligação ponto a ponto, utilizando para o efeito normalmente um teleimpressor.
2.5.2 — Vulnerabilidades:
Do mesmo modo que para o telefone, a ligação dos teleimpressores à rede telegráfica nacional passa por uma sucessão de meios, quer dentro das instalações, quer no exterior, de fácil acesso, que podem permitir a intercepção das comunicações em qualquer ponto do circuito através de um outro equipamento que se lhe introduza com fins fraudulentos.
Para além disso, acrescem, do mesmo modo que para a telecópia, as vulnerabilidades devidas à possibilidade de mistificação dos textos que podem ser deturpados ou alterados.
2.5.3 — Conclusões:
Deste modo, há que considerar o seguinte:

a) À semelhança de outras formas de circulação e distribuição de documentos deverá existir um sistema de controlo de todas as entradas e saídas de documentos, com especificação, designadamente, de originador, destinatário e grupo data/hora;
b) Quando da telecomunicação de matérias classificadas, deverão ser respeitados os procedimentos referentes à distribuição e transferência de documentos classificados constantes no n.º 7.2 do SEGNAC 1;
c) É proibida a utilização de telex para telecomunicação de matérias classificadas.
Em situações de excepção e quando a rapidez de telecomunicação for absolutamente essencial e a informação já não possa ser explorada em tempo útil e não se disponha de outros meios mais seguros, as matérias classificadas poderão ser transmitidas em claro. Este procedimento apenas poderá ser adoptado com autorização expressa, caso a caso, do chefe de escalão envolvido, que será inteiramente responsável pelo facto.
Em caso algum matérias classificadas no grau *Muito secreto* poderão ser transmitidas em claro;
d) Para alertar os utilizadores quanto às vulnerabilidades da utilização do telex, cada equipamento deverá ter indicação de «Meio não seguro».

2.6 — Teleconferência:
2.6.1 — Âmbito de utilização:
A teleconferência ou videoconferência é um meio de comunicação de voz e imagens efectuado através de canais de alta capacidade em ligações por cabo ou radiodifusão.
Esta forma de transmissão permite pôr em contacto um número limitado de participantes colocados em salas especiais equipadas com microfones, câmaras e *écrans* de televisão.
Desta forma podem todos os intervenientes ver e ouvir-se uns aos outros, bem como utilizar meios de apoio à exposição (mapas, diagramas, gráficos, etc.).
2.6.2 — Vulnerabilidades:
Apesar de, para efeitos de optimização de transmissão, a videoconferência pressupor a digitalização e codificação dos sinais, quando o meio de ligação utilizado é a radiodifusão (por circuito de satélite ou não), as suas vulnerabilidades são muito semelhantes às do radiotelefone.
Quando o meio físico de transmissão é o cabo blindado ou fibras ópticas, as vulnerabilidades são menores, mas, mesmo assim, é fundamental o bom acondicionamento e segurança electromagnética e acústica das salas de teleconferência.
2.6.3 — Conclusões:

a) Em caso algum matérias classificadas como *Secreto* e *Muito secreto* poderão ser transmitidas em claro através da teleconferência em circuitos não seguros. O mesmo se aplica a conversações que, embora não versando matérias classificadas, possam, em conjugação com outras, comprometer informações classificadas;
b) Em situações de excepção e quando a urgência na comunicação for absolutamente essencial e ou a informação já não possa ser explorada em tempo útil e não se dispuser de outros meios seguros, é da inteira responsabilidade do utilizador a discussão ou comunicação de matérias classificadas, bem como de matéria não classificada, mas consideradas sensíveis, através da teleconferência.

2.7 — Meios de telecomunicações não seguros em áreas de segurança das classes 1 e 2:
Qualquer equipamento de telecomunicações, antes de ser instalado numa zona de segurança da classe 1 (SEGNAC 1, capítulo 5), deverá ser rigorosamente verificado. Depois de instalado, deverá ser sujeito a inspecções rigorosas e frequentes, por forma a assegurar que estranhos ou pessoas não autorizadas possam ter acesso à informação classificada, através desse mesmo equipamento, no exterior dessas áreas.
2.8 — Correio electrónico:
2.8.1 — Âmbito de utilização:
O correio electrónico é um meio de transmissão de documentos sob a forma electrónica que se assemelha ao serviço postal.
2.8.2 — Vulnerabilidades:
Este meio de comunicação apresenta como principais vulnerabilidades:

a) Nas linhas de transmissão de dados, quer públicas, quer privadas, poderão ser colocados equipamentos que permitam a intercepção das telecomunicações;
b) Os pontos onde as mensagens são temporariamente guardadas até chegarem ao seu destino — sistemas informáticos — poderão ser acedidos por pessoal não credenciado.

As consequências destas vulnerabilidades poderão ser a quebra de confidencialidade ou de integridade de matérias classificadas.
2.8.3 — Conclusões:

a) Para proteger efectivamente as matérias classificadas relativamente às vulnerabilidades apontadas, os documentos devem ser mantidos cifrados desde a sua emissão até à sua recepção;
b) A transmissão de matérias classificadas via correio electrónico só poderá ser feita de modo cifrado;
c) Os documentos classificados só poderão existir em claro nos sistemas informáticos enquanto se encontrarem em trabalho; ao terminar a sua produção ou consulta, todos os documentos em claro deverão ser cifrados;
d) Deverão ser respeitados todos os restantes procedimentos referentes à preparação, transferência e consulta de documentos constantes do SEGNAC 1;
e) Deverão ser cumpridas, quando da transmissão de dados por meios informáticos, as normas constantes do SEGNAC 4.

CAPÍTULO 3

3 — Meios de comunicação seguros:

3.1 — Comunicação por meios seguros:

Consideram-se seguras as comunicações por meios eléctricos e electrónicos sempre que:

a) O circuito, embora não protegido por equipamento de cifra, esteja aprovado especificamente pela Autoridade Nacional de Segurança, até um determinado grau de classificação de segurança;

b) O circuito esteja protegido por equipamento de cifra que tenha merecido a aprovação específica e prévia da Autoridade Nacional de Segurança, bem como a sua instalação, até um determinado grau de classificação de segurança.

3.2 — Circuitos aprovados:

Considera-se que um circuito é aprovado para comunicação em claro sempre que todo o seu traçado reúna condições de segurança que lhe permitam transmitir informações classificadas até um determinado grau de classificação de segurança.

Compete à Autoridade Nacional de Segurança a sua aprovação na fase de projecto e inspecção na fase de instalação e utilização.

Os graus de classificação de segurança a atribuir aos circuitos aprovados são os mesmos que se utilizam nas matérias classificadas conforme o n.º 3 do SEGNAC 1.

Os terminais servidos por estes circuitos e postos à disposição dos utilizadores deverão ter a indicação de «Meio seguro» para comunicação por voz, para comunicação de textos e documentos por telecópia e para comunicação por telex.

3.3 — Segurança cripto:

3.3.1 — Equipamento cripto:

Os equipamentos cripto destinam-se a cifrar ou codificar as comunicações que não podem ser transmitidas em claro, sendo necessária, para o efeito, a utilização de chaves de cifra.

Para o telefone, radiotelefone e telecópia e telex são utilizados equipamentos cripto, acopulados directamente às linhas ou equipamentos de transmissão — *on line*.

O telex também é utilizado para transmitir textos já cifrados e que, em oposição ao sistema anterior, se designa por *off-line*.

Os graus de classificação de segurança a atribuir aos equipamentos de cifra são os mesmos que se utilizam nas matérias classificadas conforme o n.º 3 do SEGNAC 1.

Os terminais postos à disposição dos utilizadores que dispõem de equipamentos cripto acopulados — *on-line* — devem ter a indicação de «Meio seguro».

3.3.2 — Chaves de cifra:

Os equipamentos critpo devem permitir a utilização de diferentes chaves de cifra, as quais deverão ser preparadas por um organismo dependente do Ministério da Defesa Nacional e alteradas segundo as regras a fixar para cada caso.

As regras de gestão das chaves de cifra dos equipamentos cripto são estabelecidas pela Autoridade Nacional de Segurança.

A destruição das chaves de cifra far-se-á segundo o n.º 7.4 do SEGNAC 1, ou segundo quaisquer outras normas que venham a ser estabelecidas pela Autoridade Nacional de Segurança.

3.3.3 — Localização dos equipamentos:

A segurança física dos locais onde se encontram localizados os equipamentos cripto é estabelecida por regras emanadas da Autoridade Nacional de Segurança, com base no preconizado no capítulo 5 do SEGNAC 1.

3.3.4 — Publicações cripto:

Com a designação «publicações cripto» deve considerar-se toda a documentação associada a um sistema cripto, tal como instrução de operação, manuais para os utilizadores, manuais de instalação e manutenção, instruções de segurança cripto e todo o restante material cripto impresso, com excepção das «chaves de cifra».

3.3.5 — Aprovação dos equipamentos cripto:

Existindo actualmente no mercado grande número de sistemas e equipamentos cripto, cujas características técnicas e de segurança interessa analisar, e ainda com vista a garantir o seu máximo aproveitamento, compatibilidade e atribuição do respectivo grau de segurança, impõe-se que:

a) A Autoridade Nacional de Segurança proceda ao estudo e definição das redes e equipamentos cripto a instalar em cada um dos organismos do Estado, de modo a permitir a sua compatibilização e máximo aproveitamento, tendo em atenção os vários níveis de segurança em que terão necessidade de operar;

b) A Autoridade Nacional de Segurança aprove, específica e previamente, cada tipo de equipamento, bem como a sua instalação, até um determinado grau de segurança.

CAPÍTULO 4

4 — Centro de comunicações:

4.1 — Finalidade:

É uma área onde, além dos serviços de recepção, transmissão, registo e distribuição de documentos e textos, classificados ou não, se pretende que estejam reunidos todos os equipamentos e meios de telecomunicações postos ao serviço de uma determinada entidade ou organismo.

4.2 — Meios:

O centro de comunicações deverá, sempre que possível, centralizar todas as infra-estruturas de telecomunicações (v. n.º 5) do departamento ou departamentos que serve.

No domínio dos equipamentos telefónicos, o centro de comunicações deve incluir as centrais das redes telefónicas privadas (PPCA) e respectivos operadores, centrais radiotelefónicas e ainda os equipamentos criptofónicos, se estes forem partilhados por mais de uma extensão.

No domínio da telecópia e do telex, os respectivos terminais, bem como os equipamentos cripto, se os houver, deverão ficar igualmente instalados nesta mesma área.

4.3 — Funcionamento do centro de comunicações:

Sempre que a dimensão do centro, em termos de meios e volume de tráfego de telecomunicações, o justifique, deverá aquele dispor de pessoal próprio devidamente credenciado, habilitado com curso ou estágio sobre «segurança cripto», podendo os originadores dos textos ou documentos, ou funcionários em quem eles deleguem, utilizar os meios disponíveis naquele centro sempre que as circunstâncias o justifiquem.

Nas situações em que não se justifique a existência de pessoal próprio, a utilização do centro deverá ser sujeita às regras de acesso próprio da área de segurança da classe 1 (SEGNAC 1, capítulo 5).

Deverão existir registos de todos os textos e documentos entrados e saídos de acordo com os modelos constantes do SEGNAC 1. Quando os textos e documentos forem classificados, deverão seguir-se as regras aplicáveis e relativas ao manuseamento de matérias e documentos classificados conforme o n.º 7 do SEGNAC 1.

4.4 — Segurança do centro de comunicações:

4.4.1 — Segurança da exploração:

A responsabilidade pela segurança da exploração do centro de comunicações é da competência dos gabinetes e núcleos de segurança dos respectivos organismos (SEGNAC 1, capítulo 2), que providenciarão no sentido de garantir o funcionamento do mesmo, dentro das regras de segurança das comunicações regulamentadas nas presentes instruções e das emanadas da Autoridade Nacional de Segurança.

4.4.2 — Segurança física:

A área do centro de comunicações deve ser considerada como área de segurança da classe 1 (SEGNAC 1, capítulo 5), sendo a responsabilidade da segurança física da competência dos gabinetes e núcleos de segurança dos respectivos organismos, conforme o fixado no capítulo 2 do SEGNAC 1, que providenciarão no sentido de garantir o funcionamento do mesmo dentro das regras de segurança das telecomunicações regulamentadas nas presentes normas e nas emanadas da Autoridade Nacional de Segurança.

Compete à Autoridade Nacional de Segurança a definição de subáreas para instalação dos equipamentos e documentos cripto, bem como a localização e segurança das respectivas chaves de cifra.

CAPÍTULO 5

5 — Infra-estruturas de telecomunicações:

5.1 — Instalações de telecomunicações:

As infra-estruturas de telecomunicações deverão, sempre que possível, estar centralizadas no centro de comunicações (n.º 4.2).

Contudo, sempre que tal não possa verificar-se, devido à sua vulnerabilidade, devem ser consideradas as seguintes medidas de segurança:

a) A localização das centrais telefónicas privadas e respectivos operadores deve ser considerada como área de segurança de classe 1 (SEGNAC 1, capítulo 5);

b) Todos os repartidores e caixas de distribuição devem estar protegidos com fechaduras ou cadeados da classe B (SEGNAC 1, n.º 5.7) ou com selos de inviolabilidade.

Qualquer infra-estrutura de telecomunicação das áreas de segurança das classes 1 e 2 (SEGNAC 1, capítulo 5) deverá ser sempre aprovada pela Autoridade Nacional de Segurança, na fase de projecto ou concurso, e regularmente inspeccionada, depois da sua entrada em funcionamento.

5.2 — Classificação da documentação das redes e meios de telecomunicações:

5.2.1 — Toda a informação de redes de telecomunicações que mostre a capacidade global de telecomunicações de um organismo, bem como documentos sobre aquelas redes que mostrem detalhes importantes, deve ser, no mínimo, classificada de *Secreto*.

5.2.2 — Toda a informação e dados relativos a telecomunicações cuja divulgação possa comprometer de algum modo os interesses do organismo deve ser, no mínimo, classificada de *Confidencial*

CAPÍTULO 6

6 — Comportamento de segurança nas telecomunicações:

6.1 — Generalidades:

Ainda como reforço dos procedimentos anteriormente indicados para garantia da segurança das telecomunicações, poder-se-á acrescentar a utilização de sistemas de autenticação.

6.2 — Autenticação:

A autenticação é uma medida de segurança destinada a proteger um sistema de telecomunicações contra possíveis mistificações.

Existem vários sistemas de autenticação, que poderão ser utilizados conforme as circunstâncias o aconselhem.

A Autoridade Nacional de Segurança poderá dar o seu apoio técnico nesta matéria.

6.3 — Quebras de segurança e comprometimentos:

Sempre que se verifiquem quebras de segurança das telecomunicações e ou comprometimentos, deverão ser observados os procedimentos constantes do capítulo 9 do SEGNAC 1.

Quando se trate de quebras de segurança ou comprometimentos de equipamentos critpo e respectivas chaves de cifra, deverá ser dado imediato conhecimento à Autoridade Nacional de Segurança, que actuará em conformidade com o estabelecido especificamente para este material.

6.4 — Destruição de equipamento de cifra em situações de emergência:

No que respeita à destruição de equipamento cripto e respectivas chaves de cifra em situações de emergência, dever-se-á proceder conforme o n.º 7.4.6 do SEGNAC 1 e ou segundo quaisquer outras normas que a Autoridade Nacional de Segurança ditar para esse efeito.

MINISTÉRIOS DAS FINANÇAS E DA AGRICULTURA

Despacho Normativo n.º 177/94

Considerando que em 1 de Agosto de 1992 cessou a comissão de serviço Edgar Manuel Madeira, à data chefe de divisão da ex-Direcção-Geral das Florestas;

Considerando o disposto no artigo 3.º do Decreto-Lei n.º 34/93, de 13 de Fevereiro, e nos n.ºs 6 e 8 do artigo 18.º do Decreto-Lei n.º 323/89, de 26 de Setembro, na redacção que lhe foi conferida pelo artigo 1.º daquele diploma:

Determina-se o seguinte:

1 — É criado no quadro de pessoal do Instituto Florestal, constante do mapa I anexo à Portaria n.º 781/93, de 6 de Setembro, um lugar de assessor, da carreira de engenheiro, a extinguir quando vagar.

2 — A criação do lugar referido no número anterior produz efeitos desde o dia 1 de Agosto de 1992, considerando-se tais efeitos como reportados ao quadro da ex-Direcção-Geral das Florestas até à entrada em vigor da portaria referida no número anterior.

Ministérios das Finanças e da Agricultura, 23 de Fevereiro de 1994. — Pelo Ministro das Finanças, *Norberto Emílio Sequeira da Rosa,* Secretário de Estado do Orçamento. — Pelo Ministro da Agricultura, *Álvaro dos Santos Amaro,* Secretário de Estado da Agricultura.

Despacho Normativo n.º 178/94

Considerando que em 7 de Abril de 1993 cessou a comissão de serviço Maria de Lurdes Trindade da Cunha de Serra Camilo, à data chefe de divisão do ex-Instituto de Qualidade Alimentar;

Considerando o disposto no artigo 3.º do Decreto-Lei n.º 34/93, de 13 de Fevereiro, e nos n.ºs 6 e 8 do artigo 18.º do Decreto-Lei n.º 323/89, de 26 de Setembro, na redacção que lhe foi conferida pelo artigo 1.º daquele diploma:

Determina-se o seguinte:

1 — É criado no quadro de pessoal do Instituto de Protecção da Produção Agro-Alimentar, constante do mapa I anexo à Portaria n.º 825/93, de 8 de Setembro, um lugar de assessor, da carreira de técnico superior, a extinguir quando vagar.

2 — A criação do lugar referido no número anterior produz efeitos desde o dia 7 de Abril de 1993, considerando-se tais efeitos como reportados ao quadro do ex-Instituto de Qualidade Alimentar até à entrada em vigor da portaria referida no número anterior.

Ministérios das Finanças e da Agricultura, 23 de Fevereiro de 1994. — Pelo Ministro das Finanças, *Norberto Emílio Sequeira da Rosa,* Secretário de Estado do Orçamento. — Pelo Ministro da Agricultura, *Álvaro dos Santos Amaro,* Secretário de Estado da Agricultura.

Despacho Normativo n.º 179/94

Considerando que em 7 de Abril de 1993 cessou a comissão de serviço Anabela Alves Pereira Lima Teixeira, à data chefe de divisão da ex-Direcção-Geral das Florestas;

Considerando o disposto no artigo 3.º do Decreto-Lei n.º 34/93, de 13 de Fevereiro, e nos n.ºs 6 e 8 do artigo 18.º do Decreto-Lei n.º 323/89, de 26 de Setembro, na redacção que lhe foi conferida pelo artigo 1.º daquele diploma:

Determina-se o seguinte:

1 — É criado no quadro de pessoal do Instituto Florestal, constante do mapa I anexo à Portaria n.º 781/93, de 6 de Setembro, um lugar de assessor, da carreira de engenheiro, a extinguir quando vagar.

2 — A criação do lugar referido no número anterior produz efeitos desde o dia 7 de Abril de 1993, considerando-se tais efeitos como reportados ao quadro da ex-Direcção-Geral das Florestas até à entrada em vigor da portaria referida no número anterior.

Ministérios das Finanças e da Agricultura, 23 de Fevereiro de 1994. — Pelo Ministro das Finanças, *Norberto Emílio Sequeira da Rosa,* Secretário de Estado do Orçamento. — Pelo Ministro da Agricultura, *Álvaro dos Santos Amaro,* Secretário de Estado da Agricultura.

MINISTÉRIO DAS OBRAS PÚBLICAS, TRANSPORTES E COMUNICAÇÕES

Portaria n.º 160/94

de 22 de Março

O Decreto-Lei n.º 329/90, de 23 de Outubro, que estabelece o regime de acesso e de exercício da actividade de prestação de serviços de telecomunicações de valor acrescentado, prevê, no seu artigo 3.º, a aprovação de regulamentos de exploração para esses serviços, tendo o primeiro sido aprovado pela Portaria n.º 428/91, de 24 de Maio.