PRESIDÊNCIA DO CONSELHO DE MINISTROS

Resolução do Conselho de Ministros n.º 5/90

As presentes instruções têm como objectivo garantir a segurança nos sistemas informáticos.

A diversidade e evolução dos equipamentos e programas dos sistemas informáticos não se coaduna com o estabelecimento de normas rígidas que prevejam todas as situações. Entendeu-se, por isso, estabelecer um conjunto de regras suficientemente flexível, de forma a deixar à Autoridade Nacional de Segurança a possibilidade de, caso a caso, apreciar a oportunidade das medidas a aplicar.

A Autoridade Nacional de Segurança é a entidade responsável pela segurança nos sistemas informáticos, como resulta das competências que lhe são atribuídas, nomeadamente pelos SEGNACs 1 e 2, aprovados, respectivamente, pelas Resoluções n.os 50/88, de 3 de Dezembro, e 37/89, de 24 de Outubro.

Considerando que os sistemas informáticos tendem a tornar-se o principal suporte de certas actividades industriais, tecnológicas, administrativas e das investigações e que a falta de segurança de dados e programas pode influenciar, distorcendo, a acção competitiva nestas actividades;

Considerando que existem documentos, dados e programas relativos a essas actividades que, atendendo à sua especificidade, não foram ainda objecto de regulamentação própria;

Assim:

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

Aprovar, ao abrigo do disposto na alínea *d*) do n.º 2 do artigo 8.º da Lei n.º 20/87, de 12 de Junho, as instruções sobre a segurança informática, adiante designadas abreviadamente por SEGNAC 4, anexas a esta resolução e que dela fazem parte integrante.

Presidência do Conselho de Ministros, 28 de Setembro de 1989. — O Primeiro-Ministro, *Aníbal António Cavaco Silva.*

NORMAS PARA A SEGURANÇA NACIONAL, SALVAGUARDA E DEFESA DAS MATÉRIAS CLASSIFICADAS, SEGURANÇA INFORMÁTICA – SEGNAC 4

CAPÍTULO 1

Objecto

Artigo 1.º

Generalidades

Sem prejuízo das normas constantes dos regulamentos nacionais de segurança respeitantes à protecção de documentos, actividade industrial, tecnológica e de investigação e outros, a segurança informática tem como finalidade:

a) Garantir que o tratamento dos dados e programas esteja em conformidade com a classificação de segurança dos documentos que lhe deram origem, sempre que a salvaguarda dos interesses nacionais, de países aliados, organizações ou alianças de países de que Portugal faça parte justifique a sua aplicação;

b) Responsabilizar os directores dos estabelecimentos, empresas, organismos ou serviços pela protecção de dados e programas, instalações, material informático, do pessoal, das comunicações e de outras actividades contra quebras de segurança, comprometimentos e acções de sabotagem, espionagem e ainda pelo implemento de medidas que garantam a fiabilidade do equipamento e suportes lógicos, a integridade da informação e a continuidade dos trabalhos.

Artigo 2.º

Competências

1 — A responsabilidade pela coordenação, credenciação, fiscalização e controlo das normas de segurança estabelecidas para a segurança informática que diga respeito a elementos da Administração Pública será da competência das entidades e órgãos referidos no SEGNAC 1 — instruções sobre a segurança de matérias classificadas aprovadas pela Resolução do Conselho de Ministros n.º 50/88, de 3 de Dezembro.

2 — Quando não se trate de elementos da Administração Pública, aplicar-se-ão, com as devidas adaptações, as medidas constantes do SEGNAC 2 — instruções sobre a segurança industrial, tecnológica e de investigação, aprovadas pela Resolução do Conselho de Ministros n.º 37/89, de 24 de Outubro.

Artigo 3.º

Revisão

As propostas de revisão e de alteração às presentes instruções competem à Comissão Técnica do Sistema de Informações da República Portuguesa, em coordenação com a Autoridade Nacional de Segurança.

Artigo 4.º

Princípios básicos

1 — Todos os dados e programas devem ser convenientemente protegidos contra indiscrições, fugas, violações ou descuidos.

2 — Uma única medida de segurança não constitui, por via de regra, protecção suficiente, pelo que as medidas a aplicar têm de ser combinadas, de forma a obter-se uma sobreposição adequada.

Artigo 5.º

Estudo de ameaça e medidas de segurança

Na aplicação de medidas de segurança devem observar-se os seguintes princípios:

a) As medidas efectivas de segurança têm de se basear em estudos cuidadosos e contínuos das ameaças, especialmente respeitantes à segurança dos suportes informáticos, acessos lógicos, redes de comunicação e radiações electromagnéticas, pelo que se torna fundamental a coordenação entre as informações e a segurança;

b) As medidas de segurança devem ser planeadas de forma a incidirem principalmente sobre dados e programas classificados considerados essenciais;

c) Sempre que possível, devem concentrar-se os dados e programas classificados a proteger, por forma a poderem beneficiar de uma segurança mais eficaz;

d) O acesso aos dados e programas classificados deve restringir-se, exclusivamente, às pessoas credenciadas que tenham necessidade de os conhecer para cumprimento das suas missões ou tarefas;

e) As medidas de segurança física e manuseamento de documentos e programas classificados, por mais rigorosas que sejam, só são eficazes:

1) Se a idoneidade do pessoal credenciado para manusear dados e programas classificados estiver em permanente avaliação;
2) Se a sua instrução em matéria de segurança for também permanente;
3) Se as medidas de segurança física forem objecto permanente de revistas, rondas e inspecções, executadas por elementos credenciados e devidamente preparados para o efeito;

f) Na distribuição da classificação de segurança há que usar de maior prudência a fim de não ser atribuído um grau de classificação de segurança inferior ou superior ao requerido pelos dados e programas em análise.

Artigo 6.º

Disposições gerais

As normas constantes dos regulamentos de segurança em vigor são aplicáveis, com as devidas adaptações, às situações omissas ou não contempladas no presente regulamento, designadamente no que se aplica a:

a) Celebração de contratos;
b) Credenciação de pessoas e empresas;
c) Classificação, preparação e segurança das matérias classificadas;
d) Reprodução, transferência, controlo e destruição de matérias classificadas;
e) Medidas de segurança a adoptar em reuniões e conferências classificadas;
f) Quebras e violações de segurança e comprometimento das matérias classificadas;
g) Transporte internacional e nacional de material classificado;
h) Visitas internacionais.

Artigo 7.º

Tarefas e responsabilidades do pessoal técnico

Com observância do respectivo conteúdo funcional e níveis hierárquicos, deve o responsável pelo sistema informático atribuir as tarefas e responsabilidades do pessoal técnico de informática, nas áreas de concepção, desenvolvimento, sistema operativo e operação, segundo a legislação ou normas em vigor para esta matéria.

Artigo 8.º

Informatização de documentos

O processamento informático de documentos classificados de *Muito secreto* e *Secreto* só pode ter lugar desde que a entidade de origem não se tenha oposto à sua informatização.

Artigo 9.º

Microcomputadores

Não se abordam especificamente nestas normas a segurança e protecção dos dados e programas classificados, armazenados ou que se executam num microcomputador, por se considerar que estes últimos devem obedecer às mesmas regras enunciadas para equipamentos informáticos de maior porte.

Artigo 10.º

Definições

A definição de termos técnicos de informática e o glossário de termos de informações e segurança nacional constam de anexo A ao presente diploma, do qual faz parte integrante.

CAPÍTULO 2

Regime de segredo

Artigo 11.º

Credenciação

Os centros de informática do Estado ou privados e o seu pessoal, pertencentes aos estabelecimentos, empresas, organismos ou serviços, ou que funcionem isoladamente, que venham a desempenhar actividades a que tenham sido atribuídos um dos três graus de segurança — *Muito secreto, Secreto* e *Confidencial* — são obrigados, sempre que relacionados com essas actividades, a obter a credenciação adequada, à qual são aplicáveis as normas constantes dos SEGNAC 1 e 2, conforme se trate ou não de elementos ligados à Administração Pública.

Artigo 12.º

Extensão e duração da protecção do segredo

Os ministros ou os membros dos órgãos de governo próprio das regiões autónomas que tutelem as actividades a que tenha sido atribuída classificação de segurança, ouvida a Autoridade Nacional de Segurança, fixam a extensão e a duração das obrigações do estabelecimento, empresa, organismo ou serviço em matéria de protecção do segredo.

Artigo 13.º

Cumprimento das normas de segurança

1 — O cumprimento das normas de segurança estabelecidas deve ser inspeccionado com regularidade, de acordo com o estabelecido nos SEGNAC 1 e SEGNAC 2, respectivamente.

2 — A Autoridade Nacional de Segurança poderá, quando o entender, dispensar parte das exigências contidas no presente regulamento.

CAPÍTULO 3

Segurança física das instalações

Artigo 14.º

Generalidades

O presente capítulo define as instruções para a garantia da protecção física dos centros de informática, de forma a garantir a segurança dos dados, programas e materiais classificados contra a espionagem, sabotagem, terrorismo, comprometimento e divulgação não autorizada, especialmente a captação de radiações electromagnéticas, introdução dos vulgarmente denominados «vírus informáticos» e violação dos acessos lógicos.

Artigo 15.º

Áreas de segurança

1 — As áreas ocupadas pelo equipamento informático e seus periféricos obedecem à classificação das áreas de segurança definidas, respectivamente, nos SEGNAC 1 e SEGNAC 2.

2 — Existem áreas de segurança de classe 1, classe 2 ou de classe 3, consoante a classificação dos dados e programas a preparar, digitalizar ou imprimir.

Artigo 16.º

Necessidades em matéria de segurança

1 — Para decidir qual o grau de protecção física a adoptar é necessário ter em conta os elementos em causa, nomeadamente:

a) O grau de classificação de segurança dos dados e programas a proteger;
b) O volume e a localização dos equipamentos a salvaguardar;
c) A credenciação de segurança e a necessidade de conhecer das pessoas;
d) A avaliação das ameaças que representam a actividade dos serviços de informações hostis, actividades terroristas e criminosas, tais como as referidas no artigo 14.º

2 — As medidas a aplicar devem ser concebidas tendo em vista principalmente:

a) Impedir qualquer intrusão nas áreas ou dependências onde são guardados dados e programas classificados, por acções encobertas (electrónicas ou não) ou pela força;
b) Desencorajar, detectar e impedir acções de pessoal desleal, susceptível de actuar em proveito de organizações hostis;

c) Indigitar, de entre as pessoas credenciadas, aquelas que têm acesso à informação classificada, segundo o princípio da necessidade de conhecer;
d) Assegurar, em todas as circunstâncias, o perfeito controlo, quer dos dados e programas classificados, quer das chaves e combinações de segredo dos dispositivos de segurança dos respectivos móveis de segurança e casas-fortes.

Artigo 17.º

Localização e estrutura das instalações

1 — A localização do centro de informática deve ter as seguintes características:

a) Não existir índice acentuado de poluição atmosférica;
b) Não ter interferências electromagnéticas, como linhas de alta tensão, emissores de rádio, etc.;
c) Não existir intensa vibração, designadamente por linhas férreas, metropolitano, etc.

2 — Em termos de estrutura, para obter um bom nível de segurança é necessário que a sala ou salas destinadas ao computador e seus periféricos sejam dotadas das seguintes características:

a) Não ficarem nem no piso térreo nem no último piso;
b) Não possuírem janelas para o exterior, sendo a iluminação toda artificial;
c) Disporem de uma única entrada para o centro;
d) Possuírem saídas de emergência, com portas a abrir para o exterior da sala e que se abram exclusivamente por dentro;
e) Estarem isoladas de calor e poeiras;
f) Existir uma sala para a unidade central, consolas, unidades de controlo, *modems*, unidades de banda e de disco, colocando as impressoras e demais equipamentos que lidam com papel noutra sala;
g) Instalar os equipamentos de recolha em sala própria;
h) As salas onde se instalam os equipamentos deverão ter chão ou tecto falsos, para permitir a passagem dos cabos de energia e de ligação, bem como a instalação de condutas e saídas para o ar condicionado;
i) As superfícies primárias a que se apuserem chão e tecto falsos devem ser pintadas com tinta antipoeira.

Artigo 18.º

Energia eléctrica

1 — A alimentação da energia eléctrica possui influência considerável no funcionamento dos equipamentos informáticos, pelo que deve haver especiais diligências no seu projecto e instalação.

2 — No caso de equipamentos de médio e grande porte, muito sensíveis, mesmo a pequenas variações, há que procurar uma potência adequada, uma qualidade e uma estabilidade que permitam um trabalho contínuo indispensável, se forem utilizados processamentos em tempo real.

3 — Os construtores de equipamentos informáticos fornecem geralmente um conjunto de especificações sobre o tipo e características da rede de energia eléctrica a instalar, de forma a maximizar o rendimento desses equipamentos, pelo que estas instruções devem ser sempre tomadas em consideração.

4 — A alimentação eléctrica deve possuir sistemas de regulação autónoma (estabilizadores), para além de eventuais sistemas de segurança adicionais, tais como geradores de corrente eléctrica e sistemas *no-break*.

5 — Um centro de tratamento automático de dados tem necessidade de energia eléctrica para além da utilizada no equipamento informático, nomeadamente a relacionada com o consumo dos sistemas de climatização, de iluminação e dos sistemas de alarme contra icêndios e intrusão, devendo ser usadas fases distintas para os vários sistemas, que devem ser comutadas, permitindo um balanceamento das cargas.

6 — Numa instalação eléctrica do tipo a que se refere o número anterior devem ser seguidos os regulamentos de segurança de instalações de utilização de energia eléctrica.

7 — A instalação eléctrica corresponderá a circuitos claros com separação dos cabos por tensão e separação dos cabos de telecomunicações e blindagem e todos os cabos devem estar etiquetados, por código a definir caso a caso.

8 — Os planos de passagem dos cabos e a tabela de correspondência das etiquetas devem estar guardados em local seguro e sempre actualizados.

Artigo 19.º

Climatização

1 — Quase todos os médios e grandes equipamentos requerem um sistema de climatização que garanta não só um determinado nível de temperatura, com valor médio de 22°C, com um certo grau de humidade, na ordem dos 50%, sendo de toda a conveniência que estes valores sejam estáveis.

2 — Devem ainda ser tomados em consideração os valores padrão fornecidos pelo construtor do equipamento, uma vez que os limites aceitáveis dependem do equipamento.

3 — Embora os pequenos sistemas não tenham uma tão grande exigência de temperatura e humidade, devem, no entanto, enquadrar-se nos padrões ambientais normais.

4 — Num centro de informática devem beneficiar do sistema de climatização as salas do computador e seus periféricos.

5 — Para que o sistema de climatização esteja adequado às necessidades do centro é necessário dimensioná-lo, levando em linha de conta os seguintes factores:

a) Difusão do ar por condutas ou directamente;
b) Humidificação do ar;
c) Filtragem do ar.

6 — Em todos os sistemas de climatização deve existir um sistema automático de segurança que garanta a estabilidade das condições exigidas e que detecte qualquer anomalia, de modo a permitir uma rápida correcção da mesma.

Artigo 20.º

Protecção contra incêndios

1 — O incêndio é um dos riscos mais graves, uma vez que os centros atingidos por um incêndio não conseguem retomar a sua actividade normal em tempo útil, obrigando a recorrer a complicados e onerosos processos de *back-up* para substituição.

2 — Todos os centros de informática devem estar dotados de sistemas de detecção de incêndios, providos de alarmes sonoros ou visuais que permitam uma rápida actuação no sentido de os combater logo no seu início.

3 — A escolha do tipo de detector dependerá do local a proteger e a instalação dos detectores de incêndio não se deve resumir às salas de exploração, mas ser alargada aos locais adjacentes.

4 — Para além dos meios de detecção, devem existir meios de combate a incêndio.

5 — O sistema de detecção e combate a incêndios deve ser um sistema semiautomático, de forma que só seja accionado o sistema de combate um certo tempo após o sistema de detecção o ter sido.

6 — Devem ser tomadas em conta as seguintes medidas específicas de protecção contra incêndios:

a) Isolamento das salas dos equipamentos com paredes resistentes ao fogo de, pelo menos, seis horas;
b) Não utilização de materiais inflamáveis na decoração dessas salas;
c) Não armazenamento dentro dessas salas de materiais inflamáveis, designadamente papel e cartões;
d) Manutenção das salas limpas;
e) Colocação de extintores manuais em todo o centro de informática;
f) Aquisição de um sistema de detecção de incêndios para equipar o centro;
g) Realização de inspecções periódicas do estado de funcionamento destes sistemas de detecção;
h) Treino regular do pessoal, de forma a dotá-lo de uma boa capacidade de resposta em situações de emergência.

Artigo 21.º

Protecção contra radiações electromagnéticas

1 — Um equipamento de tratamento eléctrico ou electrónico de dados emite radiações detectáveis a grande distância, o que induz sinais eléctricos, que se propagam pelas linhas de transporte de energia eléctrica ou de transmissão, pelo que a existência de circuitos vizinhos ou condutores estranhos funcionam como sondas na zona sensível e captam sinais que comprometem o segredo das informações.

2 — A utilização de métodos paralelos de transferência de dados a grande velocidade possibilita que as radiações emitidas por esse material possam ser captadas.

3 — Finalmente, os dispositivos de entrada e de saída funcionando em série, tais como os leitores de cartões e as teleimpressoras, emitem radiações cujo diagrama se aproxima intimamente do texto em bruto dos dados tratados.

4 — Tendo em vista a eliminação das radiações emitidas e quando o grau de classificação dos dados e programas a proteger o justifique, a instalação do centro de informática deve obedecer aos seguintes requisitos:

a) A instalação deve estar o mais próximo possível do centro do edifício ou do sector controlado, a fim de que a área de segurança — onde podem ser tomadas medidas positivas contra uma escuta clandestina — tenha um alcance máximo;
b) Devem ser instalados filtros nas linhas eléctricas e de transmissão do equipamento;
c) O material deve estar rodeado de uma zona livre de qualquer elemento metálico, para que nenhum sinal, por contacto ou indução, seja transmitido através de estruturas metálicas exteriores, tais como os móveis, condutas, canalizações e armaduras metálicas;
d) Os circuitos, cabos e outros materiais não essenciais devem ser retirados, designadamente telefones, sistemas de intercomunicadores e campainhas, e os circuitos essenciais devem estar isolados por filtros e ou elementos de separação física;
e) Todas as estruturas metálicas condutoras, tais como de ventilação, canalizações, tubos pneumáticos, e outras que entram na área de irradiação, devem ser interceptadas por um elemento não condutor, instalado nos pontos de saída e de entrada da área de irradiação;
f) A sala de exploração, a das impressoras e as dos terminais devem estar dotadas de um sistema tipo «gaiola de Faraday»;
g) Os vidros das janelas existentes devem ser duplos e laminados com estrutura metálica.

Artigo 22.º

Manutenção das infra-estruturas

1 — Para garantir a funcionalidade do centro de informática, os equipamentos não informáticos devem estar sujeitos a operações periódicas de manutenção que incluam aspectos como a limpeza do equipamento e a substituição de peças usadas.

2 — Consideram-se sistemas não informáticos, entre outros, os seguintes:

a) Sistema de climatização;
b) Estabilizadores de corrente;
c) Sistema *no-break;*
d) Sistema de detecção e combate a incêndios.

Artigo 23.º

Controlo de entradas e saídas

1 — As medidas de protecção e controlo de acessos físicos abarcam uma vasta gama de possibilidades, que vão desde o reforço do número de encarregados de segurança até ao implemento de mecanismos electrónicos, devem nomeadamente:

a) Ser identificados os pontos de acesso, fazendo-se listas que assegurem que nenhuma área vulnerável foi negligenciada;
b) Recorrer a dispositivos de controlo de acessos personalizados, permitindo obter mapas detalhados das entradas/saídas nas instalações;
c) Atender a que a profundidade de protecção varia com o grau de segurança dos dados e programas e o seu estudo deve ser feito caso a caso.

Artigo 24.º

Responsável de segurança

O responsável do centro de informática deve designar um responsável pela segurança informática, quando este não exista, a quem competirá especialmente a aplicação e verificação das medidas de segurança que estiverem em vigor.

Artigo 25.º

Pessoal de segurança

A vigilância das entradas e saídas do centro de informática deve ser confiada a pessoal devidamente credenciado e instruído, cuja missão é limitar o acesso unicamente às pessoas autorizadas e assegurar a protecção física das matérias classificadas, não devendo qualquer forma de protecção física ser considerada eficiente se não for sujeita permenente ou periodicamente à fiscalização por meios humanos.

Artigo 26.º

Rondas

Fora das horas normais de serviço, a área do centro de informática deve ser rondada pelos elementos da segurança e todas as rondas devem ter a responsabilidade de verificar se:

a) A temperatura e humidade se encontram dentro dos limites impostos;
b) Não houve violação às normas estipuladas neste regulamento ou a outras emanadas pelo centro de informática para a sua segurança.

Artigo 27.º

Contentores e móveis de segurança

Os móveis de segurança destinados à guarda de discos, *disquettes,* bandas magnéticas, *cassettes* e listagens que contenham dados e programas classificados dividem-se em três classes:

a) Classe A — contentores e móveis de segurança para a guarda de dados e programas classificados de *Muito secreto;*
b) Classe B — contentores e móveis de segurança para a guarda de dados e programas classificados de *Secreto* e *Confidencial;*
c) Classe C — contentores e móveis de segurança para a guarda de dados e programas classificados de *Reservado.*

Artigo 28.º

Casas-fortes

As casas-fortes são salas de trabalho que, no seu todo, oferecem protecção igual à de um móvel de segurança, de classe equivalente, pelo que as suas paredes, soalho, tecto, portas e fechaduras deverão ser construídos de modo a conferir o grau de segurança necessário.

Artigo 29.º

Fechaduras e cadeados

As fechaduras ou cadeados dos móveis de segurança que servem para guardar dados e programas classificados devem ser padronizados conforme a seguir se indica:

a) Grupo A — fechaduras ou cadeados para móveis de segurança que devem usar códigos electrónicos;
b) Grupo B — Fechaduras ou cadeados para móveis de segurança que devem usar combinações por processos mecânicos;
c) Grupo C — Fechaduras ou cadeados para móveis de segurança que utilizem um sistema normal de chaves.

Artigo 30.º

Abertura de casas-fortes, contentores e móveis de segurança e seu registo

1 — Todas as casas-fortes ou contentores e móveis de segurança contendo matérias classificadas de qualquer grau devem possuir uma etiqueta de grandes dimensões com a palavra «Aberto» em fundo encarnado de um lado e a palavra «Fechado» em fundo verde no outro, para que permita alertar, claramente, os responsáveis para a situação em que se encontram aquelas casas-fortes ou móveis de segurança, e no exterior, parte superior, ou gaveta superior dos mesmos deve ser colocada uma relação dos nomes, endereços e telefones particulares de todas as pessoas que devem ser avisadas na eventualidade de serem encontrados abertos ou violados.

2 — Para além desta etiqueta, as casas-fortes ou contentores e móveis de segurança da classe A devem ter fixado, do lado exterior, um registo, conforme MOD. SEG. 1 em anexo, no qual a pessoa que proceder à respectiva abertura ou encerramento inscreva a data e a hora em que esta se efectuou e a sua rubrica.

Artigo 31.º

Controlo das chaves e combinações

1 — As pessoas não estão autorizadas a conservar as chaves dos móveis de segurança fora das horas normais de serviço.
2 — As combinações dos segredos das casas-fortes ou contentores e móveis de segurança devem ser retidas em memória pelas pessoas com necessidade de as conhecer.
3 — Os duplicados das chaves e um registo escrito de cada combinação de segredo devem ser conservados em envelopes lacrados e confiados à guarda dos encarregados de segurança, apenas para utilização em situações de emergência.
4 — As chaves e os registos das combinações de segredo das casas-fortes ou móveis de segurança devem beneficiar de uma protecção tão rigorosa quanto a das matérias nelas contidas.
5 — O número de pessoas que têm conhecimento das combinações do segredo das casas-fortes ou contentores e móveis de segurança deve ser limitado ao mínimo indispensável.
6 — As combinações devem ser mudadas:

a) Quando da recepção do dispositivo de segredo do fornecedor;
b) No mínimo todos os seis meses;
c) Sempre que haja mudança de pessoal que as conheça;
d) Quando se tenha verificado qualquer quebra de segurança ou se suspeite dessa possibilidade.

Artigo 32.º

Dispositivos de detecção de intrusos

1 — Sempre que forem utilizados sistemas de alarme, TV em circuito fechado ou outros dispositivos idênticos para protecção dos dados e programas classificados, a energia deverá ser fornecida permanentemente, através de um cabo principal exterior de fácil verificação ligado a um acumulador de reserva recarregável.
2 — Qualquer defeito de funcionamento ou qualquer tentativa de neutralização deste sistema deve accionar um outro sistema de alarme ou de advertência do pessoal de segurança.

Artigo 33.º

Protecção contra a observação

Devem ser tomadas as medidas julgadas necessárias, tanto durante o dia como durante a noite, para proteger os dados e programas classificados que corram o risco de ser observados.

Artigo 34.º

Protecção contra a escuta

Os gabinetes e as áreas onde é regularmente discutida informação com elevado grau de classificação devem ser protegidos contra as escutas, passiva e activa:

a) A protecção contra a escuta passiva exige inspecções de segurança técnica e requer a insonorização das paredes, portas, janelas, tectos e soalhos;
b) A protecção contra a escuta activa exige a inspecção de segurança técnica de toda a estrutura do compartimento em causa, do seu mobiliário, decoração, equipamento, material de escritório, máquinas e meios de telecomunicações.

Artigo 35.º

Áreas protegidas do ponto de vista técnico

1 — As áreas protegidas contra a escuta devem ser objecto de uma inspecção técnica pelo menos uma vez por ano e sempre que as pessoas não habilitadas ou não vigiadas ali tenham penetrado por quaisquer razões, designadamente manutenção ou decoração.
2 — As áreas a que se refere o número anterior devem ser designadas por áreas protegidas do ponto de vista técnico e ter à entrada um controlo de segurança especial, devendo ser fechadas à chave logo que deixem de estar ocupadas, e as chaves consideradas como chaves de segurança.
3 — Nenhum móvel ou material novo deve ser colocado nas áreas protegidas sem que tenha sido inspeccionado e aprovado pelo serviço de segurança.
4 — Nas áreas a que se refere o número anterior deve ser evitada a colocação de telefones e, se absolutamente necessário, devem ter protecção criptofónica.

Artigo 36.º

Medidas complementares de segurança

1 — As presentes instruções não impedem que sejam aplicáveis aos centros de informática, sempre que pela sua natureza o justifiquem, outras medidas complementares de segurança que as entidades responsáveis pela protecção do segredo achem dever implementar.
2 — A Autoridade Nacional de Segurança será obrigatoriamente informada das novas medidas tomadas.

CAPÍTULO 4

Segurança de suportes físicos

Artigo 37.º

Generalidades

O presente capítulo disciplina os requisitos a que devem obedecer os equipamentos informáticos, de forma a garantir a protecção dos dados e programas classificados contra a espionagem, a sabotagem, o comprometimento e a divulgação não autorizada.

Artigo 38.º

Controlo de circulação dos suportes informáticos

Uma vez que os dados e programas classificados residem em suportes informáticos, quer magnéticos quer de papel ou outros, deve o responsável do centro de informática obrigar a que as normas para a sua segurança, nomeadamente no que se refere a todos os procedimentos relativos ao arquivo, requisições ao arquivo, destruição, utilização e circulação dos referidos suportes, sejam cumpridas rigorosamente.

Artigo 39.º

Suportes magnéticos e ópticos

Os suportes magnéticos ou ópticos, quer se trate de discos, bandas, *cassettes*, ou outros, revestem-se de características especiais que obrigam a alguns cuidados no seu manuseamento e arquivo, impondo-se que:

a) Na utilização e arquivo dos suportes magnéticos ou ópticos devem ser tomadas em consideração todas as indicações dadas pelo fornecedor;
b) O arquivo de suportes magnéticos ou ópticos deve localizar-se em sala distinta da sala do computador, devendo possuir as mesmas condições ambientais que a sala do computador, bem como as mesmas restrições de acesso;
c) Sempre que o grau de classificação dos dados e programas o justifiquem, deve existir um segundo arquivo de suportes magnéticos ou ópticos fisicamente distinto do primeiro, situado noutro andar do mesmo edifício ou noutro edifício;
d) O arquivo de suportes magnéticos ou ópticos deve utilizar armários à prova de fogo;
e) Os suportes devem estar devidamente identificados e catalogados, devendo proceder-se a testes periódicos de verificação de compatibilidade entre o conteúdo e as respectivas etiquetas;
f) Todos os movimentos e utilizações dos suportes devem ser registados, designadamente o utilizador, a data e a hora de utilização, e analisados periodicamente;
g) O transporte dos suportes magnéticos ou ópticos deve ser apenas efectuado em caixas concebidas para esse fim, devido à sua vulnerabilidade perante o calor excessivo, os choques e a proximidade de campos magnéticos.

Artigo 40.º

Outros suportes

1 — Por outros suportes entende-se todo e qualquer suporte informático não magnético, incluindo, nomeadamente, papel contínuo corrente, pré-impressos, cartões, fichas e microfichas.

2 — Estes suportes carecem igualmente de cuidados na sua utilização e arquivo, impondo-se que:

a) O arquivo destes suportes deve localizar-se em sala distinta da sala de computador;
b) A sala de arquivo destes suportes deve estar equipada com extintores de incêndio;
c) Deve ser efectuado um controlo de humidade para estes suportes;
d) Os suportes de papel contendo informações classificadas devem ser previamente destruídas antes de deitados ao lixo, utilizando máquinas próprias;
e) O consumo de suportes de papel com pré-impressão específica deve ser controlado, de molde a evitar qualquer utilização fraudulenta;
f) O acesso aos arquivos destes suportes deve ser controlado, evitando possíveis desvios de material.

Artigo 41.º

Protecção contra radiações electromagnéticas

1 — Para impedir a emissão de radiações provocadas pelo material eléctrico e electrónico e, caso a Autoridade Nacional de Segurança entenda que os dados e programas a proteger o exijam, deve o equipamento informático obedecer às especificações «Tempest».
2 — Na ausência das especificações «Tempest» em equipamento de médio e grande porte, nomeadamente nas unidades de disco e banda, também a Autoridade Nacional de Segurança pode impor a utilização para aquele equipamento de «gaiolas de Faraday».
3 — Quando os dados classificados de *Muito secreto* e *Secreto* sejam transmitidos por cabo que permita interferências não autorizadas no circuito, deve ser utilizado cabo de fibra óptica para a interligação dos equipamentos central e periféricos.
4 — As medidas enunciadas constituem alternativas às alíneas *f*) e *g*) do n.º 4 do artigo 21.º deste regulamento.

Artigo 42.º

Generalidades sobre a segurança das redes de comunicação

A descentralização dos locais de utilização, processamento e armazenamento dos dados intensifica as trocas de informação, permite uma maior rapidez de acesso e multiplica os pontos de vulnerabilidade do sistema, impondo-se a adopção das medidas de segurança e protecção constantes dos artigos seguintes.

Artigo 43.º

Medidas de segurança nas comunicações

Nas comunicações devem ser respeitadas as seguintes medidas de segurança e protecção:

a) Verificar a não existência de interferências electromagnéticas;
b) Elaborar e manter actualizado um plano de passagem dos cabos de telecomunicações;
c) Utilizar cabos blindados;
d) Verificar periodicamente as linhas de comunicações para detectar derivações das mesmas;
e) Instalar os repartidores e *modems* em locais de acesso restrito.

Artigo 44.º

Outras medidas de segurança das redes de comunicação

As medidas anteriores não são exaustivas, devendo todas as interligações entre os elementos da instalação ou as interligações com o exterior (utilizando linha comutada, linha privada ou redes públicas de dados) obedecer às normas pertinentes em matéria de segurança das transmissões.

Artigo 45.º

Generalidades sobre a manutenção do equipamento informático

1 — Para garantir a funcionalidade do equipamento informático deve ser efectuado um contrato de manutenção com o fornecedor do equipamento e que contemple dois tipos possíveis de manutenção, respectivamente:

a) Manutenção preventiva;
b) Manutenção correctiva.

2 — A manutenção preventiva deve ser sistemática e planificada pelo fornecedor, incluindo aspectos como a limpeza do equipamento, a efectivação dos testes de funcionalidade ao equipamento e a substituição de peças usadas, sendo necessária a manutenção correctiva sempre que surja uma avaria.
3 — Deve ser mantido um inventário do equipamento informático, com a sua identificação, número de série e localização, devendo uma cópia desse inventário ser guardada em local seguro.
4 — A mudança de qualquer equipamento informático das suas instalações deve ser comunicada por escrito ao encarregado de segurança informática.

Artigo 46.º

Contrato de manutenção

Em termos gerais, os contratos de manutenção devem contemplar:

a) Prazos para a intervenção em caso de avaria, e segundo o tipo de avaria;
b) Duração máxima de indisponibilidade do equipamento;
c) Determinação da periodicidade da manutenção preventiva;
d) Substituição de peças;
e) Acompanhamento por parte do fornecedor, sempre que haja mudança de local do equipamento;
f) Definição de responsabilidades na ligação a outros equipamentos;
g) Delimitação das responsabilidades e obrigações do utilizador e do construtor.

Artigo 47.º

Diários de manutenção

1 — Deve o responsável do sistema informático manter um diário detalhado de reparações, com indicação do tipo de incidente, data e hora, diagnóstico, lapso de tempo entre o contacto com a firma responsável pela manutenção e a intervenção efectiva desta, identificação do técnico, duração total da interrupção e medidas tomadas, e outros elementos que entenda necessário registar.
2 — Também deve ser mantido um diário detalhado de intervenções de revisão, do qual conste o objecto da revisão, a data, a identificação do técnico e as medidas tomadas.

CAPÍTULO 5

Segurança lógica

Artigo 48.º

Generalidades

Para além das medidas de segurança física expostas nos capítulos 3 e 4, devem também ser implementadas medidas de segurança que protejam os recursos lógicos, de modo que fique claramente definido que só pode ter acesso à informação quem esteja devidamente autorizado.

Artigo 49.º

Procedimentos de prevenção para controlo lógico de acessos

A aquisição ou o desenvolvimento de suportes lógicos de base tais como o sistema operativo ou um *software* específico de segurança devem estar dotados de mecanismos que permitam:

a) Associação de uma *password* a um utilizador (ou grupo de utilizadores) do sistema informfico;
b) Não impressão e não visualização da *password;*
c) Mudança periódica da *password,* por processos automatizados ou não;
d) Invalidação do terminal, após um número preestabelecido de tentativas de procura de uma *password* que dê acesso ao sistema;
e) Identificação do utilizador com os respectivos postos de trabalho, nomeadamente terminais e impressora, responsabili-

zando o utilizador da visualização e impressão de dados e programas por pessoas não autorizadas;
f) Invalidação do posto de trabalho (terminal) ao fim de um certo período de inactividade;
g) Invalidação automática do terminal fora das horas normais de trabalho;
h) Programação, após cada utilização, do próximo horário de acesso;
i) Definição para qualquer ficheiro (dados ou programas) dos privilégios de acesso para leitura escrita e execução que cada utilizador tem sobre ele.

Artigo 50.º

Procedimentos de detecção posteriores para controlo lógico de acessos

1 — A confidencialidade de um sistema informático passa:

a) Pela análise e detecção de anomalias ou infracções às regras de acesso;
b) Pela existência obrigatória de procedimentos que registem num relatório diário os acessos realizados ao sistema informático.

2 — Nos relatórios diários devem ficar registados não só todos os acessos correctos ao sistema e ficheiros, como também a identificação detalhada de todas as tentativas de violação.
3 — A verificação e leitura dos relatórios diários deve constituir uma tarefa diária do responsável do sistema informático.

Artigo 51.º

Generalidades sobre controlo dos dados

1 — A grande percentagem de erros de um sistema informático é de origem acidental, ocorrendo durante a manipulação dos dados, quer por factores humanos, quer por deficiências do próprio equipamento ou *software* existente.
2 — A utilização de medidas e controlos incidindo sobre o pessoal e sobre os dados é obrigatória.
3 — Para além da formação específica do pessoal em relação ao trabalho a desempenhar, este é ainda obrigado ao cumprimento das normas constantes do SEGNAC 2.

Artigo 52.º

Recolha e processamento dos dados e divulgação dos resultados

Relativamente aos dados, e para as fases de recolha, processamento e divulgação, devem ser implementados os seguintes procedimentos, automatizados ou não:

a) Recolha de dados:

1) Verificação e validação dos dados de entrada;
2) Aceitação das transacções (ou operações) devidamente identificadas e autorizadas;
3) Correcção dos dados errados;

b) Processamento dos dados:

1) Detecção de processamentos incompletos ou duplicados;
2) Reposição dos ficheiros a um estado congruente (*roll-back* e *fowar-back*);
3) Recuperação de ficheiros e ou registos erradamente destruídos;
4) Controlos internos às aplicações, de forma a garantir a coerência dos dados entre si e entre o que foi definido na própria aplicação;
5) Verificação do estado dos ficheiros e impedimento de processamento de ficheiros que estejam num estado incorrecto;
6) Comparação dos resultados obtidos com os resultados esperados;
7) Actualização do modo de funcionamento dos programas, devido a mudanças do sistema operativo, compilador ou outras ferramentas informáticas;

c) Divulgação dos resultados:

1) Assegurar o correcto encaminhamento dos dados enviados por teleprocessamento aos destinatários;
2) Assegurar o transporte correcto dos dados, por meios tradicionais;
3) Destruição de resultados (listagens) já obsoletos.

Artigo 53.º

Generalidades sobre segurança dos suportes lógicos

Qualquer que seja o tipo de *software* a adquirir, deve este:

a) Garantir que o *software* obedece a um mínimo de normas e de requisitos de segurança;
b) Assegurar a não redundância ou proliferação do *software;*
c) Proteger o *software* de roubo ou utilização abusiva;
d) Assegurar que o *software* é utilizado de acordo com os termos do contrato, o que impedirá os centros de informática de serem penalizados por uso indevido.

Artigo 54.º

Segurança no desenvolvimento de suportes lógicos

O desenvolvimento de projectos informáticos, devido à sua importância, requer medidas especiais de protecção e controlo, pelo que os responsáveis e técnicos dos centros de informática devem:

a) Definir a metodologia de desenvolvimento para cada projecto, com indicação dos passos mínimos a cumprir, qualquer que seja a sua dimensão;
b) Identificar claramente os objectivos a atingir;
c) Testar individualmente cada programa de aplicação em desenvolvimento, e, após estes testes, proceder ao teste geral da cadeia, cobrindo toda a aplicação;
d) Efectuar, sempre que possível, os testes de uma nova aplicação com os dados reais das mesmas;
e) Preparar documentação pormenorizada das aplicações desenvolvidas;
f) Providenciar para que o utilizador principiante tenha facilidades que o auxiliem a contactar com o sistema, como funções de *help,* ensino programado ou exemplos simples de utilização;
g) Estabelecer prazos para revisão dos projectos.

Artigo 55.º

Segurança na aquisição de suportes lógicos

A aquisição de *software* deve obedecer a normas de segurança que garantam a adequação e a manutenção desse mesmo *software,* bem como as relações futuras com o fornecedor, pelo que o responsável do sistema informático deve:

a) Definir os requisitos funcionais para a aplicação, realizando um estudo de oportunidade;
b) Preparar um documento contendo as indicações de todas as funções necessárias a realizar pelo produto, descrevendo os controlos que devem ser efectuados por ele;
c) Fazer um estudo do mercado dos produtos que contemplam o ponto anterior e avaliar as suas vantagens e inconvenientes;
d) Sempre que haja necessidade de adquirir um produto, contactar os respectivos fornecedores para verificar as capacidades de manutenção, custos do produto e da sua manutenção, possibilidade de adaptações a fazer pela firma fornecedora e cláusulas contratuais;
e) Comparar os resultados dos pontos anteriores, de modo a obter as melhores soluções;
f) Requerer demonstrações dos *packages,* de preferência com dados reais, ou obter um período de teste utilizando um conjunto representativo de dados que reflictam casos gerais e também situações pouco frequentes;
g) Obter referências financeiras e grau de confiança, bem como a avaliação do grau de eficiência, em relação às firmas fornecedoras, nas condições definidas no SEGNAC 2;
h) Seleccionar a firma e realizar o contrato, com o apoio do sector jurídico da entidade compradora;
i) Assegurar que é fornecida informação detalhada, formação necessária e apoio técnico;
j) Dar especial atenção às restrições legais de uso e cópia, de modo a impedir a divulgação a terceiros pelos contratantes.

Artigo 56.º

Documentação dos suportes lógicos

1 — Tanto em equipamentos de grande porte como em micros, as aplicações necessitam de estar bem documentadas, sem correr o risco de dependerem apenas de uma pessoa para o seu bom funcionamento.

2 — A documentação do *software* deve assegurar a formação dos utilizadores, o manter da continuidade de utilização no caso de mudança de pessoal e o correcto funcionamento em tempo útil.

Artigo 57.º

Medidas a aplicar à documentação dos suportes lógicos

Para cumprir os objectivos referidos no artigo anterior, impõe-se a implementação das seguintes medidas:

a) Estabelecimento de normas, indicando o mínimo de documentação que deverá obrigatoriamente existir em cada aplicação, incluindo:

1) Sumário das funções e objectivos;
2) Manual do utilizador;
3) Documentação de análise e de programação;
4) Manual de operação;
5) Documentação sobre os controlos internos, segurança e auditoria;
6) Manutenção e modo de fazer modificações sem perturbar o bom funcionamento do sistema;
7) Listagens dos programas;

b) Cópias da documentação, que serão guardadas noutro local, fora do centro de informática;
c) Divulgação da documentação apenas entre pessoal credenciado e com necessidade de a conhecer;
d) Manutenção de toda a documentação actualizada, sendo indicado conferir a responsabilidade das actualizações ao responsável pelo *software;*
e) Cometimento ao responsável da segurança informática da distribuição das novas versões e recolha das anteriores que estejam em poder dos vários utilizadores, bem como a manutenção das cópias da documentação;
f) Preparação, classificação e protecção dos documentos inerentes a uma aplicação informática, nos termos das normas constantes dos SEGNAC 1 e SEGNAC 2.

Artigo 58.º

Manutenção dos suportes lógicos

1 — Para garantir a integridade e a continuidade dos trabalhos informáticos é necessário que o *software* se encontre em perfeitas condições de operacionalidade.

2 — É obrigatória a celebração de um contrato de manutenção do *software* de base que defina, nomeadamente:

a) Obrigatoriedade de correcção de anomalias detectadas;
b) Definição da responsabilidade de implementação e adaptação do *software;*
c) Fornecimento de documentação clara e actualizada a acompanhar as alterações efectuadas;
d) Garantias de implementação de novas versões.

3 — É de considerar também a existência da manutenção do *software* específico ou aplicações informáticas que inclua as correcções de imperfeições e as modificações, em função de novas necessidades e ou alterações de procedimentos, devendo todas estas alterações estar devidamente documentadas.

4 — Deve ser mantido um diário detalhado de anomalias, semelhante ao indicado para o equipamento.

Artigo 59.º

Plano de recuperação

1 — O plano de segurança obriga à criação de cópias de toda a informação relevante, designadamente ficheiros, bases de dados, bibliotecas de programas, que devem ser estabelecidos pelo responsável do sistema informático, devendo constar as seguintes menções:

a) Periodicidade das protecções;
b) Número de exemplares de protecção;
c) Localização do arquivo de suportes magnéticos;
d) Procedimentos de reposição.

2 — Deve ser efectuado controlo periódico da correcta aplicação dos procedimentos.

3 — Cada aplicação em exploração normal deve possuir o seu esquema de cópias de segurança, indicando:

a) Os ficheiros a copiar;
b) O momento em que deve ser efectuada a sua cópia;
c) Como efectuar a recuperação da informação, de modo que seja possível refazer os processamentos em caso de erro não detectado em tarefas anteriores ou avaria de discos ou do próprio sistema.

4 — Deve o responsável do sistema informático definir a periodicidade quanto à execução dos seguintes quatro tipos de cópias de segurança *(back-ups):*

a) *Back-ups* diários — efectuam-se no final de cada período de trabalho, excepto no último dia da semana, e devem ser copiados os ficheiros permanentes criados no período diário e os ficheiros permanentes que foram alterados;
b) *Back-ups* semanais — efectuam-se no último dia da semana. Serão copiados todos os ficheiros permanentes. Estes *back-ups* terão a duração de, pelo menos, uma semana;
c) *Back-ups* mensais — correspondem ao *back-up* semanal da última semana do mês e terão, pelo menos, a duração de um mês;
d) *Back-ups* anuais — são os *back-ups* mensais efectuados no mês de Dezembro, que terão obrigatoriamente a duração de, pelo menos, um ano.

5 — Ao efectuar estes *back-ups* nunca se deverá destruir a cópia imediatamente anterior, mas sim proceder à rotação dos suportes, de modo a garantir uma efectiva reposição da informação.

6 — O número de gerações que se deverá manter depende, nomeadamente, do carácter estratégico da informação, do seu volume, da frequência de actualização e da necessidade dos utilizadores em matéria de rapidez de reposição, após detecção de uma situação de erro ou avaria.

7 — Para ficheiros contendo informação classificada deve-se efectuar *back-ups* duplos, pois é sempre possível durante uma recuperação de informação ocorrer o mesmo incidente ou ocorrer um outro incidente que destrua a protecção.

8 — O arquivo de suportes magnéticos ou ópticos que contém uma das cópias de segurança deve estar junto à sala do computador.

9 — Se existir outra cópia de segurança, deve localizar-se fora do perímetro do centro de informática.

10 — Deve ser elaborado um manual com os procedimentos a seguir, de modo a recuperar a informação a partir das cópias de segurança.

11 — Deve verificar-se periodicamente se os suportes contendo os *back-ups* se encontram em condições físicas de ser utilizados e se o esquema de cópia e procedimentos estabelecidos permitem a recuperação efectiva em caso de avaria ou acidente grave.

12 — Deve ser efectuado um controlo periódico, para verificar o cumprimento das normas estabelecidas para a protecção da informação.

Artigo 60.º

Plano de reposição

1 — Devem existir normas pormenorizadas que permitam repor o bom funcionamento do sistema, sempre que tenha ocorrido uma interrupção ou avaria, de forma a reduzir ao mínimo os danos do equipamento e a não provocar grandes perturbações aos utilizadores.

2 — Deve recorrer-se a essas normas sempre que surjam incidentes do seguinte tipo:

a) Avarias no equipamento;
b) Avarias de climatização ou de energia eléctrica;
c) Avarias ou erros nas telecomunicações;
d) Erros de programação ou de exploração;
e) Destruição de ficheiros;
f) Ausência de pessoal.

3 — Os procedimentos que integram as normas de reposição estão geralmente descritos nos *dossiers* de exploração das rotinas e nos manuais de exploração e referem-se, nomeadamente:

a) À recuperação após cancelamento de um programa;
b) À reposição de um ficheiro, recorrendo a uma cópia *(back-up)* em banda;
c) À modificação da configuração do equipamento, por avaria de uma das impressoras;

d) À reconfiguração da rede de teleprocessamento, devido a avaria num terminal ou num controlador de terminais;
e) À recuperação de movimentos por erro na transmissão.

CAPÍTULO 6

Classificação, preparação e segurança de dados e programas classificados

Artigo 61.º

Objectivos

1 — Dada a descentralização dos postos de trabalho de um sistema informático, considera-se que a classificação e preparação dos dados não é tarefa específica dos centros de informática, pelo que são aplicadas à classificação e preparação dos dados todas as regras enunciadas a esse respeito nos SEGNAC 1 e SEGNAC 2.
2 — A elaboração de programas é tarefa própria do centro de informática e à segurança técnica no seu desenvolvimento é aplicável o disposto no artigo 54.º

Artigo 62.º

Definição

A orientação em matéria de classificação de segurança dos programas visa assegurar que estes apenas sejam classificados quando tal for necessário, que o grau de classificação atribuído seja o mais adequado e que só seja mantido enquanto se tornar imprescindível.

Artigo 63.º

Responsabilidades

Os directores dos estabelecimentos, empresas, organismos ou serviços são responsáveis pela manutenção da classificação de segurança dos programas.

Artigo 64.º

Classificação dos programas

1 — Deve ser evitada toda a classificação excessiva ou insuficiente, por inconvenientes sob o ponto de vista de segurança.
2 — Cada programa deve ser classificado apenas em função dos dados que trata e não de acordo com a classificação de qualquer outro programa ou subprograma a que se refira.
3 — As referências a programas classificados não devem, só por isso, ser também classificadas, a menos que contenham ou revelem informações classificadas e, para se não correr o risco de comprometer o sigilo das informações ou matérias classificadas, estas referências devem ser reduzidas ao mínimo.

Artigo 65.º

Generalidades sobre a preparação de programas classificados

1 — Os programas classificados com grau igual ou superior a *Confidencial* devem ser desenvolvidos e digitalizados somente por pessoas credenciadas e com acesso autorizado, pelo menos, para o nível de segurança desses programas.
2 — Para efeitos desta última exigência, devem as pessoas em causa estar previamente inscritas nas listas de acesso.

Artigo 66.º

Segurança dos materiais utilizados na preparação de programas classificados

1 — As pessoas encarregadas do desenvolvimento e digitalização de programas classificados ficam responsáveis pelo destino ulterior dos manuscritos utilizados para aqueles fins.
2 — Os manuscritos ou listagens obsoletos que permitam a revelação de informações classificadas devem beneficiar das medidas de protecção de segurança correspondentes ao grau de classificação atribuído àquelas informações a ser destruídos logo que possível.
3 — Todos os restantes materiais utilizados na preparação de programas classificados que, pela sua natureza, não sejam de destruir devem ser protegidos em conformidade com o grau de classificação correspondente.

Artigo 67.º

Identificação dos suportes magnéticos ou ópticos

1 — Todos os suportes informáticos, tais como bandas magnéticas, discos magnéticos, discos ópticos, *disquettes* e *cassettes*, onde ficam registadas matérias classificadas devem trazer claramente indicado o grau de classificação da informação mais classificada dos dados e programas ali contidos.
2 — A classificação a que se refere o número anterior deve ser mantida até os suportes serem desgravados por métodos seguros, devendo elaborar-se um certificado de destruição da gravação da matéria classificada.
3 — Também devem estar bem legíveis outras indicações ou instruções julgadas necessárias, nomeadamente as relacionadas com a reclassificação e desclassificação de dados e programas.
4 — São aplicáveis a esta matéria todas as normas estabelecidas no SEGNAC 2.

Artigo 68.º

Marcação de programas classificados

Todos os programas classificados devem ter, em comentário, as seguintes indicações:

a) Classificação — a qual indica o grau de classificação do programa: *Muito secreto, Secreto, Confidencial ou Reservado;*
b) Número de referência — o qual identifica o programa para a segurança;
c) Datas de revisão — as quais indicam as datas de eventuais revisões globais ulteriores, número do exemplar e indicação de ser o original ou qual o número da cópia;
d) Nome do programa — o qual indica o nome do programa ou subprograma;
e) Descrição sobre a funcionalidade do programa ou subprograma; tratando-se de um subprograma, deve ser indicado o nome do programa do qual ele é subprograma;
f) Autor — nome do responsável pelo desenvolvimento do programa;
g) Notas — as quais configuram indicações relevantes para a utilização de programas por terceiros, como, por exemplo, opções de compilação ou *linkagens* necessárias;
h) Historial — esta secção documenta as modificações feitas ao código original. Por cada alteração significativa deve existir uma entrada nesta zona que descreva sucintamente as modificações introduzidas. Cada entrada consta de três campos:

1) Autor — autor da modificação;
2) Data — data em que a modificação foi feita;
3) Comentário — breve descrição da modificação efectuada.

Artigo 69.º

Classificação da documentação de programas

1 — A documentação de programas classificados deve ter uma classificação igual à dos respectivos programas.
2 — As regras sobre documentação classificada, enunciadas nos SEGNAC 1 e SEGNAC 2, aplicam-se a toda a documentação de programas classificados.

Artigo 70.º

Generalidades sobre acesso a dados e programas classificados

A aplicação, total ou parcial, dos procedimentos de prevenção e detecção posteriores, descritas no artigo 49.º, deve ser decidida pelo responsável do sistema informático.

Artigo 71.º

Privilégios de acesso

Os privilégios de acesso para leitura, escrita e ou execução de programas ou dados classificados devem ser exclusivamente atribuídos aos utilizadores credenciados e com necessidade de conhecer, devendo qualquer tentativa de violação dos privilégios ser automaticamente registada.

Artigo 72.º

Reclassificação e desclassificação de programas

1 — Todos os programas classificados estão sujeitos a um processo sistemático de revisão, com vista à sua baixa de classificação ou des-

classificação, a fim de que o sistema de segurança global não fique saturado de documentação, cujo conteúdo não mais justifica o grau de classificação inicial.

2 — Tal revisão torna-se, porém, desnecessária nos casos em que a entidade de origem tenha previsto, para determinados programas classificados, a baixa de classificação automática, devendo, nestes casos, os programas em causa e sua documentação conter tal indicação.

3 — Sempre que possível, a entidade de origem de programas classificados de *Muito secreto* ou de *Secreto* deve indicar o prazo em que a classificação atribuída se mantém, com a indicação de quando deve ser reclassificada ou baixada de grau.

4 — Para tal fim pode ser fixada uma data, acontecimento ou facto limite daquele prazo, que deve constar de uma anotação a escrever, em comentário, no programa e na sua documentação.

5 — No caso de ser impossível a determinação da data ou facto que ditará no futuro a baixa de classificação ou desclassificação de programas classificados, pode ser utilizado, quando julgado pertinente, o seguinte comentário:

> Baixa de classificação/desclassificação não pode ser, neste momento, determinada.

6 — No que se refere aos programas classificados recebidos, apenas poderá ser alterada ou anulada a sua classificação com prévia autorização do organismo de origem ou, caso haja sido extinto, do que o substitui ou, ainda, da entidade que lhes é hierarquicamente superior.

7 — Sempre que uma entidade detentora de programas admita que o grau de classificação respectivo é excessivo ou insuficiente, deve chamar a atenção da origem, solicitando-lhe autorização para fazer a alteração necessária.

Artigo 73.º

Reclassificação ou desclassificação de programas de origem estrangeira ou pertencentes a organizações internacionais

A classificação dos programas originados em países estrangeiros aliados, ou com os quais se mantenham boas relações, ou pertencentes a organizações internacionais de que Portugal faça parte, não poderá ser alterada sem autorização expressa daqueles países ou organizações.

Artigo 74.º

Marcação de programas a reclassificar

1 — Sempre que um programa tiver de ser reclassificado, deve ser escrita, em comentário, uma das seguintes indicações:

> Reclassificado/desclassificado... (nova classificação) por ordem de.../por... (categoria, nome e cargo da pessoa que fez a alteração) em... (data) ou;
> Reclassificado/desclassificado... (nova classificação) em conformidade com... (documento que autoriza a alteração) por... (categoria, nome e cargo da pessoa que fez a alteração) em... (data).

A documentação do programa deve ser actualizada com as mesmas indicações que foram dadas ao programa.

2 — A documentação de programas reclassificados deve ser marcada com o carimbo correspondente, e não dactilograficamente, no cimo e no pé de todas as páginas, e a classificação anterior riscada a vermelho.

3 — Após a sua marcação, os documentos devem ser arquivados e guardados em conformidade com as medidas de segurança exigidas pelo seu novo grau de classificação.

4 — Os programas obsoletos ou desactualizados continuarão a beneficiar das medidas de segurança correspondentes à sua classificação, enquanto esta se mantiver.

CAPÍTULO 7

Reprodução, transferência, controlo de segurança e destruição de dados e programas classificados

Artigo 75.º

Reprodução de dados e programas classificados

1 — Podem ser feitas cópias de dados e programas classificados, desde que tal se reconheça necessário e na estrita observância da necessidade de conhecer.

2 — As operações de reprodução de dados e programas classificados não se poderão dissociar das operações concernentes à sua preparação, pelo que as disposições referidas no capítulo anterior e no SEGNAC 2 devem ser observadas.

3 — A fim de se assegurar a devida protecção dos originais classificados, deve observar-se o seguinte:

a) As cópias que contêm extractos desta natureza devem ser classificadas pelo menos com o grau mais elevado que aparecer entre os dados e programas originais;
b) No caso de os extractos, só por si, não justificarem o mesmo grau de classificação do original, os dados e programas que os contiverem podem receber outra classificação de segurança, desde que a origem, ou a entidade que a substitui, no caso de ter sido extinta, ou, ainda, a entidade que lhes for imediatamente superior, assim o autorize.

4 — Os dados e os programas copiados em número elevado devem ser convenientemente protegidos, para o que a entidade que encomendou a sua reprodução deve tomar as necessárias medidas para que não fiquem cópias ou exemplares na posse de pessoas não autorizadas.

5 — Sempre que seja necessário recorrer a particulares para serem feitas cópias de dados e programas classificados, devem estes requerer previamente a sua credenciação.

6 — A reprodução, transferência e destruição de dados e programas classificados implica a reprodução, transferência e destruição da respectiva documentação, nos termos das normas constantes do SEGNAC 1.

Artigo 76.º

Reprodução de dados e programas classificados de *Muito secreto* e *Secreto*

1 — Se um destinatário necessitar de dados e programas classificados de *Muito secreto* e *Secreto*, deve tentar obtê-los, em primeira instância, por solicitação directa à entidade de origem.

2 — Em casos excepcionais, porém, em que tal não seja possível e em que um destinatário tenha efectivamente necessidade de fazer cópias, parciais ou totais, de dados e programas classificados de *Muito secreto* ou *Secreto*, tais cópias podem ser efectuadas, observados os seguintes requisitos:

a) Sejam autorizadas pela entidade de origem ou pela entidade que legalmente a substitui, a quem deve ser formulado o pedido, informando-a da finalidade a atingir e do número de cópias ou extractos a fazer;
b) Sejam expressamente ouvidos os directores dos estabelecimentos, empresas, organismos ou serviços a quem os dados e programas a reproduzir se encontram confiados;
c) Contenham, em comentário, a classificação e o número da cópia dos programas originais, bem como a indicação da entidade que lhes deu origem e da que as reproduziu;
d) Contenham, em comentário, um número de referência localmente atribuído pela entidade que procedeu à reprodução do programa;
e) Sejam registadas e relacionadas nas folhas de controlo dos dados e da documentação de programas classificados de *Muito secreto* (MOD. SEG. 2), bem como relacionadas nos respectivos inventários anuais, como se se tratasse de documentos originais;
f) Sejam reproduzidas apenas por pessoas credenciadas e com acesso autorizado à informação classificada de *muito secreto* ou *Secreto*;
g) O número de cópias autorizado seja limitado ao número correspondente às necessidades;
h) As cópias que já não haja necessidade de conservar sejam cuidadosamente destruídas em conformidade com o que se encontra estabelecido.

3 — Se a entidade que deu origem a um programa classificado de *Muito secreto* ou *Secreto* deseja conservar o controlo exclusivo da sua reprodução, deve expressá-lo de forma bem visível através da seguinte indicação, aposta em comentário no programa e na respectiva documentação:

> É proibida a reprodução deste programa, no todo ou em parte, sem prévia autorização da origem.

4 — A nível superior ao da origem, as cópias podem ser feitas mediante simples autorização do responsável desse nível, devendo, no entanto, a origem ser informada.

Artigo 77.º

Reprodução de dados e programas classificados de *Confidencial*

1 — Os dados e programas classificados de *Confidencial* podem ser reproduzidos sem autorização da origem, a menos que esta o tenha expressamente proibido.

2 — Para os programas nas condições referidas no número anterior deve existir, nos programas e respectiva documentação, a indicação referida no n.º 3 do artigo 76.º

3 — A atribuição de um número de referência a cada cópia e o seu registo são obrigatórios e o número total de cópias efectuadas deve ser limitado ao mínimo correspondente às necessidades do serviço.

4 — Em todos os exemplares de programas reproduzidos deve figurar, em comentário, a classificação do programa original.

Artigo 78.º

Reprodução de dados e programas classificados de *Reservado*

Os dados e programas classificados de *Reservado* podem ser reproduzidos sem autorização da origem, devendo-se limitar, todavia, o número de cópias ao indispensável para as necessidades.

Artigo 79.º

Distribuição e transferência de dados e programas classificados

1 — A segurança das matérias classificadas deve ser assegurada não só quando as mesmas estão armazenadas ou a ser trabalhadas, mas também quando se encontram em trânsito, diferindo os procedimentos respectivos em função do grau de classificação da matéria a proteger e, consoante a transferência se processe de um departamento para o outro, dentro de um mesmo edifício ou complexo de edifícios diferentes, dentro do território nacional, ou entre parcelas diferentes do mesmo, ou ainda para além fronteiras.

2 — Dentro de um mesmo edifício ou complexo de edifícios, a transferência dos suportes magnéticos, ópticos ou outros que contenham dados e programas classificados e o seu transporte far-se-á por um elemento credenciado.

3 — A transmissão, por meios electrónicos, de dados e programas classificados obedece às normas ou instruções estabelecidas para o efeito.

4 — Deve ter-se presente, como princípio geral, que o transporte dos suportes contendo dados e programas classificados só deve ser confiado a pessoas credenciadas para o mesmo grau de classificação.

5 — No caso em que se pretenda assegurar que somente determinada individualidade tenha acesso aos suportes transportados, deve ser aposta, adicionalmente, na embalagem interior, a seguinte indicação:

> Para ser aberto unicamente por ... (nome do destinatário ou seu substituto autorizado).

Artigo 80.º

Distribuição e transferência de dados e programas classificados de *Muito secreto*

1 — São os seguintes os processos autorizados para a transferência de suportes contendo dados e programas classificados de *Muito secreto:*

a) Contacto directo das pessoas a quem as mesmas estiverem confiadas;
b) Por funcionários/empregados nomeados especificamente para tal função, munidos de certificado (MOD. SEG. 3 e MOD. SEG. 4);
c) Por mensageiro credenciado, munido de certificado (MOD. SEG. 3 e MOD. SEG. 4)

2 — A transferência interna, temporária ou definitiva, ou entre estabelecimentos, empresas, organismos ou serviços de dados e programas classificados de *Muito secreto* far-se-á, obrigatoriamente, pelo sistema de duplo invólucro e deve obedecer às especificações referidas na alínea *g*) do artigo 39.º deste regulamento.

3 — O invólucro exterior conterá apenas:

a) Endereço do estabelecimento, empresa, organismo ou serviço e, sempre que conhecido, o destinatário directamente interessado, evitando-se assim, tanto quanto possível, que outro destinatário tenha de abrir antecipadamente o envelope exterior antes que o conjunto atinja o destino;
b) Número de expedição;
c) Data de expedição.

4 — Quando se pretenda que determinado suporte seja apenas transferido por mão própria, o invólucro exterior deve conter, ainda, a seguinte indicação:

> A transportar somente por correio especial devidamente credenciado.

5 — O invólucro interior deve ser lacrado ou fechado com selo de segurança e deve ter impresso, de forma bem visível, ou marcada a carimbo, a classificação de *Muito secreto.*

6 — Os invólucros dos suportes que contêm dados e programas classificados de *Muito secreto* devem ser abertos apenas pelo pessoal credenciado inscrito nas listas de acesso e nomeado para o efeito.

Artigo 81.º

Certificados de transferência

1 — A transferência interna em estabelecimentos, empresas, organismos ou serviços de dados e programas classificados de *Muito secreto* far-se-á sempre mediante a elaboração, em duplicado, de um certificado de transferência (MOD. SEG. 5), que seguirá junto ao suporte, dentro do invólucro interior.

2 — O certificado de transferência deve identificar perfeitamente o expedidor, o destinatário e o suporte a que diz respeito, constituindo, normalmente, um documento «Não classificado» quando isolado, não devendo, para efeitos do disposto no número anterior, revelar o assunto respectivo, por transcrição do título ou qualquer outra referência à matéria tratada.

3 — O original do certificado de transferência será sempre assinado pelo destinatário directo ou pelo responsável pela segurança informática e devolvido à origem, por forma que não haja dúvidas quanto à identidade da pessoa que recebeu a matéria transferida.

4 — Aos dados e programas classificados de *Muito secreto,* produzidos em mais de um exemplar, dever-se-á anexar um documento contendo uma lista de distribuição, na qual serão indicados os números dos exemplares atribuídos a cada uma das entidades nas mesmas mencionadas, incluindo aqueles que se destinam a arquivo.

5 — Os dados e programas classificados de *Muito secreto* requerem a existência de um sistema contínuo de registo de recepção e de expedição que esteja sujeito a um mínimo de alterações.

6 — Cada estabelecimento, empresa, organismo ou serviço que detenha dados e programas classificados de *Muito secreto* estabelecerá medidas de controlo interno, nas quais estarão compreendidas inspecções periódicas e outras medidas tidas por convenientes que assegurem o controlo e o registo pormenorizado das referidas matérias.

7 — Na transferência entre estabelecimentos, empresas, organismos ou serviços, ou entre estes e outros além-fronteiras, a entrega de cada duplo invólucro será sempre controlada por um sistema de recibo (MOD. SEG. 6).

8 — Os portadores de suportes contendo dados e programas classificados de *Muito secreto* não podem, em caso algum, separar-se dos mesmos, a menos que estes fiquem protegidos nos termos do SEGNAC 2.

9 — Aos portadores de suportes contendo dados e programas classificados de *Muito secreto* deve ser dado a assinar, antes da partida, um formulário conforme MOD. SEG. 7, em que atestem terem tomado conhecimento das instruções nele contidas.

Artigo 82.º

Distribuição e transferência de dados e programas classificados de *Secreto, Confidencial* e *Reservado*

Os processos autorizados para a transferência de suportes contendo dados e programas classificados de *Secreto, Confidencial* e *Reservado* são os aplicáveis às matérias classificadas no SEGNAC 1 e no SEGNAC 2.

Artigo 83.º

Controlo de segurança

1 — Para além dos procedimentos especificamente ligados às operações de produção, reprodução, distribuição e transferência de matérias classificadas, existem ainda outros procedimentos que, nuns

casos, complementam as medidas já enunciadas e, noutros, regulam aspectos particulares do seu manuseamento.

2 — Em tudo o que estiver omisso neste regulamento sobre controlo de segurança são aplicáveis as normas estabelecidas nos SEGNAC 1 e SEGNAC 2.

3 — A saída de suportes contendo dados ou programas classificados das instalações do serviço em que se encontram depositados deve obedecer aos seguintes requisitos:

a) Nenhum suporte contendo dados e programas classificados de *Muito secreto, Secreto* e *Confidencial* poderá ser levado para fora das instalações em que se encontra depositado com a finalidade de ser trabalhado em casa ou por quaisquer outras razões;
b) Os suportes contendo dados e programas classificados de *Reservado* poderão ser levados para fora dos estabelecimentos, empresas, organismos e serviços, desde que autorizados pelos respectivos directores;
c) As pessoas autorizadas a deter os suportes nas condições atrás expressas assegurarão que, enquanto em seu poder, os mesmos serão resguardados, devendo ser elaborado registo do nome da pessoa a quem o suporte foi confiado, data da saída e data da devolução.

Artigo 84.º

Controlo dos suportes contendo dados e programas classificados de *Muito secreto*

No controlo dos suportes contendo dados e programas classificados de *Muito secreto* e da sua documentação devem ainda ser observadas as seguintes medidas de controlo adicional:

1) Folha de controlo dos suportes contendo dados e programas classificados de *Muito secreto* e da sua documentação (MOD. SEG. 2)

a) A folha de controlo destina-se ao registo dos nomes e rubricas das pessoas que tiverem acesso à documentação e suportes contendo dados e programas classificados de *Muito secreto,* com a data em que efectuaram o respectivo manuseamento;
b) Um exemplar da folha de controlo da documentação e suportes classificados de *Muito secreto* acompanhá-los-á quando estes forem transferidos, ficando no organismo que os enviou cópia da mesma e registada a identificação de quem os copiou, expediu, arquivou ou por qualquer outra razão participou da preparação dos mesmos e a eles teve acesso;
c) Quando um suporte e documentação classificados de *Muito secreto* forem destruídos, a folha de controlo respectiva será removida e apensa ao certificado de destruição conforme MOD. SEG. 8 em anexo, sendo destruída somente quando estes últimos o forem e caso a entidade que recebeu o suporte e documentação proceder à distribuição de exemplares, cópias ou extractos aos organismos subordinados, deverá tal facto ficar devidamente registado na folha de controlo respectiva;
d) Para além das responsabilidades geralmente definidas para esta categoria de classificação, compete ainda ao encarregado pela segurança informática verificar se ficaram efectivamente registados nas folhas de controlo respectivas o nome e as rubricas das pessoas a quem foi dado conhecimento dos suportes e documentação classificados de *Muito secreto,* com as datas em que tal conhecimento teve lugar.

2) Inventário dos suportes contendo dados ou programas classificados de *Muito secreto* e da sua documentação:

a) Em todos os organismos onde existam suportes classificados de *Muito secreto* o responsável pela segurança informática deve assegurar que os mesmos sejam inventariados em Janeiro de cada ano, segundo o estipulado nos artigos 38.º e 56.º deste regulamento;
b) O inventário será referido a 31 de Dezembro do ano anterior e deve estar permanentemente disponível para ser examinado pelas inspecções de segurança, conforme MOD. SEG. 9 em anexo.

3) Substituição de funções:

a) Quando a pessoa a cuja guarda estão confiados os suportes e documentação classificados de *Muito secreto* for substituída nas funções que exerce, estiver ausente por um período superior a 30 dias ou, por qualquer outro motivo, não possa continuar com tal responsabilidade, deve fazer entrega daqueles suportes e documentação à pessoa nomeada para a substituição, mediante recibo feito por esta última;
b) Compete ao responsável pela segurança informática assegurar que tal medida é cumprida antes de a pessoa a substituir abandonar o cargo.

Artigo 85.º

Controlo dos suportes contendo dados e programas classificados de *Secreto, Confidencial* e *Reservado*

Ao controlo dos suportes contendo dados e programas classificados de *Secreto, Confidencial* e *Reservado* são aplicáveis todas as medidas de controlo mencionadas para matérias classificadas de *Muito secreto,* com excepção da necessidade de manutenção de um folha de controlo para os suportes e documentação com aquele grau de classificação.

Artigo 86.º

Generalidades sobre destruição de dados, programas e suportes classificados

1 — Para evitar acumulações desnecessárias, serão apagados periodicamente, e logo que conveniente, todos os dados e programas dos suportes já substituídos ou de que se presume não haver mais necessidade.

2 — Deverá evitar-se manter em arquivo suportes contendo dados e programas classificados e sua documentação com mais de cinco anos cuja necessidade ou interesse histórico não seja reconhecido.

Artigo 87.º

Destruição de dados e programas classificados

1 — Sempre que o detentor de suportes classificados julgue que o conteúdo dos mesmos se tornou inútil deve proceder em conformidade com as normas estabelecidas nos SEGNAC 1 e SEGNAC 2 no que respeita à destruição de documentos classificados.

2 — A reutilização de suportes classificados na mesma instalação não necessita de procedimentos especiais, a menos que o responsável do sistema informático julgue conveniente, devendo, no entanto, os referidos suportes manter a categoria de classificação dos dados e programas originais.

3 — A reutilização dos suportes magnéticos classificados noutras instalações implica a destruição total do seu conteúdo, podendo tal destruição ser efectuada pela reescrita, total no suporte, de dados não classificados ou por outros procedimentos que o responsável pelo sistema informático julgue conveniente.

Artigo 88.º

Destruição de suportes classificados

1 — Em caso algum devem ser entregues aos fornecedores, para reparação, suportes magnéticos ou outros contendo dados ou programas classificados.

2 — Os suportes magnéticos ou outros contendo informação classificada e considerados irrecuperáveis para leitura ou escrita de dados e programas devem ser destruídos, utilizando métodos apropriados.

3 — A destruição de suportes que se encontrem nas condições descritas no número anterior obedece às normas estabelecidas no SEGNAC 2 sobre destruição de matérias classificadas.

4 — Considerando-se que os dados e programas contidos em suportes considerados irrecuperáveis para leitura foram destruídos, deve proceder-se nos termos do n.º 1 do artigo 87.º

Artigo 89.º

Planos de evacuação e destruição de emergência

Nos planos de evacuação e destruição de emergência devem seguir-se as normas constantes dos SEGNAC 1 e SEGNAC 2.

Presidência do Conselho de Ministros.

SEGNAC 4
(MOD.SEG. 1)

_____
(Est., Emp., Org. ou Serviço)

REGISTO DE ABERTURAS E ENCERRAMENTOS

Repartição _____ Mês _____ Ano _____

Número de série do móvel _____

ABERTURAS			ENCERRAMENTOS		
DATA	HORA	RUBRICA	DATA	HORA	RUBRICA

SEGNAC 4
(MOD.SEG. 2)

_____
(Est., Emp., Org. ou Serviço)

FOLHA DE CONTROLO DE DOCUMENTOS E SUPORTES INFORMATICOS

CLASSIFICADOS DE MUITO SECRETO

1. Assunto			2. Origem	3. Nº de referência
4. Data do documento ou suporte informático	5. Nº do exemplar	6. Nº de Registo de entrada	7. Data da entrada	8. Processo

CONHECIMENTO / CIRCULAÇÃO

ENTIDADE	REGISTO DE SAÍDA			REGISTO DE DEVOLUÇÃO		
	Data-hora da saída	Rubrica de quem entrega	Rubrica de quem recebeu	Data-hora da entrada	Rubrica de quem devolveu	Rubrica de quem recebeu

SEGNAC 4
(MOD.SEG. 3)

CERTIFICADO DE CORREIO ESPECIAL Nº ____

PARA TRANSPORTE NACIONAL EM MÃO DE DOCUMENTOS E SUPORTES INFORMATICOS CLASSIFICADOS.

1. Certifica-se que o portador _____
nascido em ___/___/___, em _____ (país)
natural de _____ (localidade) detentor do Passaporte/B.I.Nº _____
emitido por _____ em ___/___/___ e empregado no _____ (Est., Emp., Org. ou Serviço) está autorizado a transportar o seguinte material:
_____ volume(s), peso de cada volume _____, dimensões de cada volume _____, outros dados de identificação _____.

2. No decurso da sua viagem entre _____ e _____ executada no período de ___/___/___ a ___/___/___ o portador viaja em execução de funções oficiais e é acreditado como correio oficial, sendo assim autorizado a transportar _____ volumes, contendo documentos e suportes informáticos protegidos pelo competente selo oficial.

3. Todos os funcionários dos serviços aduaneiros nacionais são solicitados no sentido de não submeterem aos seus serviços normais de fiscalização os volumes acima referidos, dispensando ao portador todas as demais facilidades aduaneiras compatíveis com os seus regulamentos.

Válido até ___/___/___

_____, _____ de _____ de 19__

_____
(Estabelecimento, Empresa, Organismo ou Serviço)

_____ (Entidade tutelar)

_____ (Autoridade Nacional de Segurança)

SEGNAC 4
(MOD.SEG. 4)

CERTIFICADO DE CORREIO ESPECIAL Nº _____

PARA TRANSPORTE INTERNACIONAL EM MÃO DE DOCUMENTOS E SUPORTES INFORMATICOS CLASSIFICADOS.

Certifica-se que o portador _____ (nome completo)
nascido em ___/___/___, em _____ (país), natural de _____ (localidade)
detentor do Passaporte/B.I.Nº _____, emitido por _____ em ___/___/___ e empregado no _____ (Est., Emp., Org. ou Serviço) está autorizado a transportar durante a viagem abaixo descrita, o seguinte material:
_____ volume(s), peso de cada volume _____, dimensões de cada volume _____, outros dados de identificação _____.

Chama-se a atenção das Alfândegas, Polícia e/ou funcionários da Emigração para o seguinte:
- O material transportado é classificado.
- Solicita-se que o material não seja inspeccionado por outras pessoas que não as devidamente autorizadas ou aquelas que tenham permissão especial; Sendo necessária a inspecção, deve ser efectuada num local próprio e na presença do correio especial.
- Solicita-se que o volume, se for aberto para a inspecção, seja marcado depois de novamente fechado, assinalando a abertura por meio de carimbo e assinatura e anotando nos documentos de embarque (se os houver) que o material foi aberto.
- Solicita-se aos funcionários das Alfândegas, Polícia e/ou Emigração dos países de trânsito, de chegada ou de saída que prestem o auxílio necessário para assegurar a entrega do material em boas condições e em segurança.

Início da viagem ____ / ____ / ____

De: _____ (país de origem) Para: _____ (país de destino)

Através de: _____ (países intermédios) Paragens autorizadas: _____ (Indicar os locais)

Válido até ___ / ___ / ___

_____, ___ de _____ de 19__

_____
(Estabelecimento, Empresa, Organismo ou Serviço)

_____ (Entidade tutelar)

_____ (Autoridade Nacional de Segurança)

SEGNAC 4
(MOD.SEG- 5)

(Est., Emp., Org. ou Serviço)

CERTIFICADO DE TRANSFERÊNCIA INTERNA Nº _____

DE: CLASSIFICAÇÃO:

PARA: DATA:

Designação do doc. e suporte informático	Data do Sup./Doc.	Número de Exemplares	Número dos Exemplares	Obs.

Declaro que transferi o material mencionado	Declaro que recebi o material mencionado
Assinatura:	Data _____/_____/_____
(nome e cargo legível)	Assinatura:
	(nome e cargo legível)

SEGNAC 4
(MOD.SEG. 7)

D E C L A R A Ç Ã O

(Nome de família e nome próprio)

de _____
(Estabelecimento, Empresa, Organismo ou Serviço)

(Cargo no Estabelecimento, Empresa, Organismo ou Serviço)

Declaração

O Encarregado de Segurança do _____
(nome do Est., Emp., Org. ou Serviço)

entregou-me as notas relativas ao tratamento e custódia dos documentos/ suportes informáticos classificados a serem transportadas por mim. Li e compreendi o conteúdo das mesmas.

Conservarei permanentemente durante a viagem os documentos/suportes informáticos classificados e não abrirei o invólucro a não ser que tal me seja exigido pelas autoridades alfandegárias.

Quando chegar entregarei os documentos/suportes informáticos classificados à entidade receptora, contra recibo

(Local e data)

(Assinatura do correio especial)

Atestado por: _____
(Encarregado de Segurança do Est., Emp., Org. ou Serviço)

SEGNAC 4
(MOD.SEG- 6)

(Est., Emp., Org. ou Serviço)

RECIBO DE DOCUMENTOS E SUPORTES INFORMÁTICOS Nº ___

- TRANSFERENCIA EXTERNA -

Ao _____

enviam-se para _____

os materiais ou documentos abaixo mencionados:

CLASSIFICAÇÃO _____

Designação de Sup./ Docum.	Data do Sup./Docum.	Número de Exemplares	Número do Exemplar	Obs.

Em ___ de _____ de 19___

O ENCARREGADO DE SEGURANÇA

_____

DESTACAR PELO TRACEJADO E DEVOLVER

Recebi os suportes ou documentos relacionados no Recibo Nº ____ de ___/___/___ da _____
(Carimbo)

_____, ___ de _____ de 19__

_____

SEGNAC 4
(MOD.SEG. 8)

(Est., Emp., Org. ou Serviço)

C E R T I F I C A D O D E D E S T R U I Ç Ã O

Nº _____ DATA ___/___/_____

REFERÊNCIA DO SUPORTE OU DOCUMENTO	Nº DO SUP./DOCUM.	Nº DE EXEMPLARES	Nº DE REGISTO DE INVENTÁRIO	CLASSIFICAÇÃO DE SEGURANÇA	OBSERVAÇÃO

Declaro que foi destruído suporte/docum. acima mencionado

Assinatura _____

Nome e categoria (bem legível ou dactilografado) _____

Declaro que assisti à destruição do suporte/docum. acima mencionado

Assinatura _____

Nome e categoria (bem legível ou dactilografado) _____

Declaro que assisti à destruição do suporte/doc. acima mencionado

Assinatura _____

Nome e categoria (bem legível ou dactilografado) _____

SEGNAC 6
(MOD. SEG. 9)

_____
(Est., Emp., Org. ou Serviço)

INVENTARIO DE SUPORTES INFORMATICOS OU DOCUMENTOS CLASSIFICADOS DE MUITO SECRETO

O ENCARREGADO DE SEGURANÇA

_____
Assinatura

(Nome e categoria dactilografados)

Folha Nº _____

Iniciada em _____/_____/_____

1	2	3	4	5	6	7	8	9		10		11
								Arquivado		Redistribuído		
Designação do sup./doc.	Data do suporte ou documento	Origem	Nº de Exemplares	Nº Exemplar	Nº de Registo de Inventário	Recebido de: (Entidade)	Data	Processo	Nº do Exemplar	Entidade	Nº do Exemplar	Data da Destruição

GLOSSÁRIO DE TERMOS DE INFORMAÇÕES E SEGURANÇA NACIONAL

Acesso lógico. — Método de entrada por programação, num sistema informático.

Aplicação informática. — Conjunto de programas usados como um todo para a solução informática de um problema concreto.

Auditoria. — O meio pelo qual os acessos ao sistema, processos e transacções podem ser vigiados e registados de modo que as quebras e tentativas de acesso possam ser detectadas.

«BACK-UP». — Sistema de segurança que consiste na cópia de ficheiros informáticos para suportes magnéticos suplementares.

Centro de informática. — Área onde estão instalados sistemas informáticos e onde são feitos a concepção de desenvolvimento das aplicações.

Classificação. — Atribuição de um grau de segurança a um documento, ficheiro de dados, programa ou suporte informático que impede que este seja acedido por alguém cuja credenciação seja menor do que a do referido documento.

Comprometimento. — É o conhecimento, parcial ou total, de matérias classificadas por parte de pessoas não autorizadas, isto é, pessoas sem a adequada credenciação ou sem acesso autorizado às referidas matérias. Considera-se ter havido comprometimento sempre que matérias classificadas tenham estado sujeitas ao risco de divulgação a pessoas não autorizadas ou tenham estado perdidas, ainda que temporariamente, no exterior de uma área de segurança. Considera-se também ter havido comprometimento sempre que matérias classificadas não sejam localizadas nas conferências periódicas ou que tenham sido perdidas, ainda que temporariamente, no interior de uma área de segurança, até que uma investigação de segurança venha provar o contrário.

Configuração. — Grupo de dispositivos e programas integrados entre si de forma a operarem como um sistema único de processamento de dados.

Credenciação. — Determinação ou reconhecimento feito pela Autoridade Nacional de Segurança no sentido de que, sob o ponto de vista de segurança, um determinado indivíduo, empresa, estabelecimento, organismo ou serviço está apto a assegurar a protecção à informação de uma certa categoria de classificação e de todas as restantes categorias inferiores.

Documento. — É todo e qualquer registo gráfico ou de outra natureza de qualquer assunto, nomeadamente:

Manuscritos, cartas, notas, actas, relatórios, memorandos, mensagens, papéis taquigrafados, impressos, apontamentos e listagens de computador;

Planos, esboços, *croquis*, desenhos, plantas e cartas topográficas;

Registos fotográficos ou cinematográficos de qualquer natureza (vídeos, por exemplo), cartões ou fitas perfurados e registos em banda magnética;

Composições gráficas, material litográfico, matrizes, zincogravuras, *stencil*, fitas de máquina de escrever, papel químico ou absorvente, ou qualquer outro material de reprodução de documentos.

Encarregado de segurança informática. — Responsável por todas as actividades de segurança informática, na dependência hierárquica dos núcleos e gabinetes de segurança.

Escuta (activa/passiva). — Termo genérico que designa a intercepção não autorizada de notícias ou informações difundidas por qualquer meio sonoro ou electromagnético.

Espionagem. — Actividade que visa a recolha de notícias ou informações por métodos clandestinos.

«Foward back». — Possibilidade de um sistema informático repor, em caso de falha durante o processamento, a situação no ponto em que se encontrava quando a falha ocorreu, ainda que a meio da transacção.

Função de «Help». — Conjunto de instruções destinadas a ajudar um utilizador na execução de uma determinada aplicação, podendo ser consultadas em simultâneo com essa aplicação.

Gabinete de segurança. — Órgão do canal técnico funcionando na dependência directa dos ministérios e governos das regiões autónomas, destinado a apoiar no campo de segurança estas entidades, de acordo com as normas do presente regulamento.

Gaiola de Faraday. — Revestimento interior de uma sala com uma malha metálica que impede a captação do exterior da radiação electromagnética.

«Hardware». — Termo usado para expressar de forma genércia o equipamento informático (unidades de disco, unidade central, terminais, impressoras, etc.).

Indução eléctrica. — Efeitos das tensões de linhas eléctricas sobre os condutores vizinhos.

Informação. — É o produto resultante da análise das notícias obtidas pelos serviços que constituem o SIRP, no desempenho das missões que lhes sejam cometidas.

«Linkagem». — Ligação de dois ou mais programas (ou subprogramas) distintos, acopulando-os, de modo a formarem um todo.

Matéria classificada. — É toda a informação, notícia, material ou documento que, se for do conhecimento de indivíduos não autorizados, pode fazer perigar a segurança nacional dos países aliados ou de organizações de que Portugal faça parte.

Material. — É todo o documento, substância, elemento de máquina, de qeuipamento ou de arma, fabricado, em curso de fabricação, ou em estudo, bem como construções ou instalações, nomeadamente:

Matérias-primas e manufacturadas;
Modelos, montagens, cunhos, matrizes, chancelas e selos brancos;
Trabalhos, edifícios e instalações;
Armamento, munições e equipamento;
Dados, programas, aplicações informáticas.

Núcleo de segurança. — Órgão do canal técnico, funcionando na dependência directa dos directores dos estabelecimentos, empresas, organismos ou serviços, destinado a dar apoio em todas as atribuições na área da segurança, de acordo com as presentes normas.

«Package». — Programa ou conjunto de programas concebidos para resolver problemas genéricos, comercializados como produto acabado.

«Password». — Conjunto de caracteres que permite ao utilizador o acesso a sistemas, dados ou programas. Deve ser pessoal e intransmissível.

Periférico. — Componentes de *hardware* através dos quais os utilizadores comunicam com o sistema informático, terminais, impressoras, *scanner,* sintetizador de voz, etc.

Processamento em tempo real. — Modo de funcionamento de um sistema informático em que as informações provenientes dos periféricos são imediatamente processadas, actualizando os ficheiros.

Protecção criptofónica. — Protecção resultante da conversão de linguagem clara para linguagem ininteligível, destinada a proteger as comunicações contra intercepção não autorizada.

Quebra de segurança. — É toda a acção contrária ou omissa aos regulamentos de segurança em vigor que faça perigar ou possa comprometer as matérias classificadas.

Responsável do sistema informático. — Pessoa a quem compete gerir o sistema informático. Basicamente, faz parte das suas atribuições a implantação da metodologia para exploração dos equipamentos informáticos e desenvolvimento de projectos informáticos.

«Roll back». — Reposição dos dados na sua situação inicial, após erro ou avaria durante a execução de uma transacção.

Sabotagem. — É a destruição, ruína ou avaria intencional de equipamento ou parte do equipamento, material ou instalações por elementos hostis ou a favor destes.

Segurança. — Um estado que se alcança quando a informação classificada, o pessoal, as instalações e as actividades estão protegidas contra a espionagem, sabotagem, terrorismo e subversão, bem como contra perdas ou acesso não autorizado. O termo também se aplica às medidas necessárias para se conseguir aquele estado e às organizações responsáveis por estas medidas.

Segurança física. — A parte de segurança que se preocupa com as medidas físicas destinadas a salvaguardar o pessoal e prevenir acessos não autorizados a informações, materiais e instalações, contra a espionagem, sabotagem, danificação e roubo, tanto nos locais de fabrico ou armazenagem como durante deslocações.

Segurança informática. — Salvaguarda dos sistemas de processamento automático e prevenção da divulgação, distorção ou destruição ilícita das informações classificadas.

Sistema informático. — Conjunto formado por equipamentos informáticos, instruções, normas, procedimentos, pessoal e meios de transmissão de tal modo organizado e interligado que permita trabalhar e comunicar informações.

Sistema «No break». — Unidade que garante o fornecimento ininterrupto de energia ao equipamento, em caso de falha no abastecimento do exterior.

Sistema operativo. — Conjunto de programas que fazem a gestão dos recursos de um sistema informático.

«Software». — Termo utilizado para indicar programas ou conjuntos de programas. Pode ser traduzido por suporte lógico.

«Software-house». — Empresa dedicada à realização de programas.

«Software» de base. — Conjunto de programas geralmente fornecidos com o equipamento, tais como o sistema operativo, subsistemas, compiladores, etc.

Subversão. — Acção destinada a enfraquecer o potencial militar, económico e político de uma nação, minando o moral, a lealdade e a confiança dos seus cidadãos.

Suporte informático — Discos magnéticos ou ópticos, bandas magnéticas, *disquettes, cassettes* ou *cartridges,* sobre os quais se podem registar dados.

Teleprocessamento. — Transmissão à distância da informação emitida ou recebida por um sistema informático, devidamente codificada e sem alterar o seu significado.

«Tempest». — Equipamento informático que não emite radiações nem emana sinais eléctricos ou electromagnéticos para o exterior.

Violação de segurança. — O mesmo que quebra de segurança.

Vírus informático. — Programas propositadamente inseridos no sistema informático com intenção de impedir ou dificultar o seu funcionamento. Alguns tipos de virus estão programados de modo a corromper a integridade dos dados.