PRESIDÊNCIA DO CONSELHO DE MINISTROS

Resolução do Conselho de Ministros n.º 47/88

A Lei n.º 30/84, de 5 de Setembro, que estabelece as bases gerais do Sistema de Informações da República Portuguesa (SIRP), prevê, no seu artigo 23.º, a possibilidade de os serviços que o integram disporem de centros de dados.

No que ao Serviço de Informações de Segurança (SIS) diz respeito, o Centro de Dados foi criado através do artigo 22.º da respectiva Lei Orgânica, constante do Decreto-Lei n.º 225/85, de 4 de Julho, estando, pois, criadas as condições para a sua efectiva instalação e início das respectivas funções.

Impõe-se, por isso, de acordo com o disposto no artigo 24.º daquela lei de bases e no artigo 23.º do diploma orgânico do SIS, estabelecer os critérios, normas técnicas e regulamentos que assegurem o funcionamento eficaz e seguro do Centro de Dados do SIS.

Isto, naturalmente, no estrito respeito por tudo quanto sobre a matéria dispõem quer a Constituição da República, designadamente no seu artigo 35.º, quer os diplomas legais referidos, e tendo, além disso, na devida conta o preconizado em documentos que sobre a matéria têm sido produzidos ao nível do Conselho da Europa e da OTAN.

Assim:

Nos termos das alíneas *f*) e *g*) do artigo 202.º da Constituição, o Conselho de Ministros resolveu aprovar os critérios, normas técnicas e medidas indispensáveis a garantir a segurança de informações processadas, necessários ao funcionamento do Centro de Dados do Serviço de Informações de Segurança (SIS), constantes do regulamento anexo a esta resolução e que dela faz parte integrante.

Presidência do Conselho de Ministros, 29 de Setembro de 1988. — O Primeiro-Ministro, *Aníbal António Cavaco Silva.*

Regulamento do Centro de Dados do Serviço de Informações de Segurança

CAPÍTULO I

Disposições gerais

1 — O presente Regulamento estabelece as medidas indispensáveis a garantir a segurança das informações processadas no Centro de Dados, adiante designado por Centro, do Serviço de Informações de Segurança (SIS), bem como os respectivos critérios e normas técnicas de funcionamento.

2 — Para efeitos do disposto no presente Regulamento consideram-se:

a) Ficheiro informático — conjunto de informações ou dados agrupados segundo determinado critério mantidos em suporte magnético ou óptico;
b) Periféricos — cada um dos equipamentos, designadamente impressoras, terminais e memórias externas, que actuam sob o comando da unidade central de processamento (CPU), constituindo o conjunto do computador;
c) Sala de exploração — sala em que se encontra a CPU, memórias secundárias e seus órgãos de comando;
d) Sistema de cópia de segurança — sistema de segurança consistente na duplicação de ficheiros (cópias) para fazer face aos casos de acidente ou avarias;
e) Palavras chave — código formado por um conjunto de símbolos, letras ou números que permite ao sistema central reconhecer o utilizador. Os termos «chaves de segurança», «código de acesso» e «senhas» são aplicados com a mesma finalidade;
f) Utilizador — toda a pessoa que utiliza o sistema informático.

3 — Todos os procedimentos adoptados no Centro devem ter em conta a estrita necessidade de eficazmente prevenir a divulgação, distorção ou destruição ilícitas das informações processadas.

4 — Os controles de segurança sobre equipamentos, pessoas, áreas de instalação do Centro e terminais obedecerão aos requisitos da mais elevada classificação.

5 — Periodicamente serão executados testes tendentes a aferir a eficácia das medidas de segurança em vigor no Centro.

6 — Sem prejuízo do disposto no número anterior, sempre que efectuada qualquer manutenção, reparação ou alteração importantes no Centro serão obrigatoriamente adoptados procedimentos tendentes a certificar que os dispositivos de segurança do sistema não foram modificados.

7 — Sempre que houver necessidade de transmitir informações classificadas, o seu encaminhamento deve ser efectuado de acordo com as normas nacionais de segurança.

8 — Ao pessoal será ministrada formação permanente e treino regular que assegure uma reacção pronta e eficaz a qualquer situação anómala.

9 — Sempre que se detectar qualquer quebra de segurança observar-se-á obrigatoriamente o seguinte procedimento:

a) Adopção de medidas prontas e decisivas tendentes à sua correcção;
b) Determinação rigorosa das causas, local e período durante o qual a quebra teve lugar;
c) Identificação dos responsáveis pela quebra de segurança.

10 — Da situação de quebra será dado imediato conhecimento ao director do SIS, ao qual serão transmitidas, no mais curto prazo, as conclusões e respectiva fundamentação do procedimento previsto no número anterior, para acção regulamentar, estatutária, disciplinar ou judiciária.

CAPÍTULO II

Segurança das informações processadas

SECÇÃO I

Da segurança física

11 — A segurança física do Centro compreende a protecção das instalações, do equipamento e o controle de acesso.

12 — O acesso ao Centro é feito por uma única entrada.

13 — No interior do Centro são estabelecidas zonas de circulação restrita com acesso limitado ao pessoal devidamente credenciado, criando-se para esse efeito um sistema de entrada controlado automaticamente ou não.

14 — O acesso à sala de exploração é limitado ao pessoal devidamente credenciado em estrita razão de serviço, devendo sempre ser por ele preenchido o livro de entradas e saídas caso não exista controle automático orientado para essa finalidade.

15 — O pessoal responsável pela manutenção de equipamentos é obrigatoriamente acompanhado, à vista, por um funcionário do SIS credenciado para a área onde a manutenção é feita.

16 — Os documentos, instalações e equipamentos serão protegidos contra incêndios, inundações e outros agentes físicos ou químicos, designadamente contra agressões ou tentativas de acesso por meios eléctricos, electrónicos, magnéticos ou de radiação.

SECÇÃO II

Da segurança dos dados

17 — A segurança dos dados consiste no conjunto de medidas e procedimentos destinados a impedir o acesso, a alteração ou a destruição da informação de uma forma não prevista ou não autorizada.

18 — Será criado um sistema de cópias de segurança que apenas podem ser manuseadas pelo pessoal credenciado para trabalhar na sala de exploração, sujeito a registo rigoroso de movimentação.

19 — Ao pessoal de informática serão atribuídas responsabilidades relativas à total integridade estrutural e protecção de dados, ficheiros e programas.

20 — A atribuição de responsabilidades e a sujeição às correspondentes sanções serão feitas quer a nível de credenciação quer a nível de conteúdo funcional pelo responsável do Centro.

21 — O acesso aos dados impõe a criação de palavras chave, alteráveis sempre que se julgue necessário, e a definição de níveis de segurança a atribuir aos utilizadores credenciados para o efeito.

22 — Ao pessoal do Centro está vedado o conhecimento das informações reais existentes em suporte magnético; nos casos em que se verifiquem anomalias, os técnicos do Centro, para tanto habilitados, prestarão o apoio necessário, sempre em presença do utilizador dessa área.

23 — Todos os trabalhos de programação e testes serão executados com base em dados fictícios.

24 — Será criado um inventário dos suportes de dados e dos programas existentes com toda a documentação necessária à manutenção das aplicações e equipamento.

25 — Para prevenir o tratamento inadequado ou abusivo de informações, todas as operações consideradas tecnicamente delicadas serão obrigatoriamente feitas com a presença de, pelo menos, dois técnicos.

26 — O acesso ao arquivo de suportes magnéticos será feito, pelo menos, por dois técnicos credenciados para o efeito.

27 — As cópias de segurança dos ficheiros e dos programas serão feitas sempre na presença de, pelo menos, dois técnicos autorizados para o efeito.

28 — As aplicações a desenvolver possuirão chaves de segurança próprias que condicionarão tanto o acesso a elas mesmas como o acesso a partes de informação que manipulem, segundo identificação do utilizador e o seu nível de credenciação.

29 — Sempre que haja necessidade de desenvolvimento ou alteração de aplicações, o respectivo pedido deverá obedecer ao preenchimento de um formulário, que indicará, obrigatoriamente, a identificação do utilizador, o que pretende, quais os ficheiros a manipular e qual ou quais os níveis de segurança a serem atribuídos, bem como a classe ou classes de utilizadores que a ela poderão ter acesso.

30 — Os utilizadores do sistema informático são responsáveis pela protecção dos respectivos terminais e áreas de trabalho, bem como pela integridade do conteúdo.

31 — Todas as saídas de trabalhos para os periféricos de impressão são obrigatoriamente controladas pelos utilizadores aos quais se destinam.

32 — Serão elaboradas estatísticas do nível de utilização do sistema, englobando informações referentes à identificação dos utilizadores, tempo de utilização e sua localização física e lógica.

CAPÍTULO III

Critérios e normas técnicas de funcionamento do Centro de Dados

33 — O Centro deve permitir guardar e processar, simultaneamente, informações de diferentes níveis de classificação, incluindo as não classificadas, permitindo o acesso selectivo e simultâneo a essas informações por indivíduos com «necessidade de conhecer» e com credenciação eventualmente diferentes.

34 — Com observância do respectivo conteúdo e níveis funcionais, ao director do Centro compete a atribuição das tarefas e responsabilidades ao pessoal de informática, nas áreas de concepção e desenvolvimento, sistemas e operação.

35 — Sem prejuízo do disposto no número anterior e das demais atribuições e competências fixadas em lei ou regulamento interno, o director do Centro, em coordenação com os utilizadores, pode definir quais os ficheiros a utilizar no sistema informático, elaborando documentação referente à identificação desses ficheiros, sua classificação de segurança, código de acesso e identificação do utilizador, bem como a respectiva credenciação de segurança.

36 — Na área de concepção e desenvolvimento é efectuada a análise funcional, análise orgânica e programação.

37 — Os técnicos que integram a área de concepção e desenvolvimento estão especialmente obrigados:

a) A zelar pela manutenção das aplicações, programas e rotinas por si desenvolvidos;

b) A elaborar a respectiva documentação e proceder à sua entrega ao director do Centro; da documentação constará obrigatoriamente a identificação do responsável e seu nível de credenciação, qual ou quais os serviços para quem foi desenvolvida, quais os dados que manipula e qual a sua classificação de segurança.

38 — Para viabilizar o cumprimento das obrigações referidas no número anterior e o desenvolvimento das tarefas correspondentes, o director do Centro atribuirá aos técnicos da área de concepção e desenvolvimento áreas de trabalho no sistema informático, sendo-lhes vedada a utilização de quaisquer outras não superiormente autorizadas.

39 — Na área de sistemas é efectuada:

a) A programação do sistema;
b) A gestão dos recursos do sistema no que diz respeito a memórias, suportes magnéticos, periféricos e utilizadores, desencadeando e controlando todos os procedimentos tendentes ao bom funcionamento do mesmo;
c) A coordenação da implementação da segurança dos acessos ao sistema, bem como tarefas de classificação de ficheiros segundo as especificações dadas pelos utilizadores, resolvendo quaisquer anomalias técnicas que ocorram no sistema.

40 — Sem prejuízo do disposto no número anterior, a área de sistemas deve assegurar as ligações de carácter técnico com os fornecedores do sistema informático, seguindo para o efeito as normas constantes deste Regulamento.

41 — À área de operação incumbe predominantemente:

a) Assegurar a realização dos trabalhos de processamento de dados já em execução ou que tenham sido solicitados;
b) Efectuar o planeamento do trabalho em computador, definindo sequências e prioridades;
c) Controlar a utilização e rendimento do equipamento;
d) Documentar toda a actividade do sector de operação;
e) Zelar pela segurança do sistema e aplicações, tomando as medidas adequadas, designadamente diagnosticando as causas de interrupção de funcionamento do sistema e promovendo o reatamento e recuperação de ficheiros;
f) Manter e gerir a biblioteca de ficheiros e programas;
g) Accionar e manipular o equipamento informático, central e periférico, verificando o seu bom funcionamento;
h) Accionar os mecanismos para obtenção de cópias de segurança *(back up)*.

42 — Sem prejuízo do disposto na lei e no presente Regulamento, as normas internas de funcionamento do Centro, tendo designadamente em conta o disposto no n.º 3, devem obrigatoriamente prever medidas nos seguintes domínios:

a) Controle de transmissão dos dados;
b) Métodos a utilizar para mencionar a identificação e classificação em todos os suportes de informação;
c) Método de trabalho no interior do Centro e registos a manter para esse fim;
d) Controle, inventário e verificação periódica de todo o equipamento classificado existente no Centro;
e) Assegurar a integridade do *software;*
f) Precauções pormenorizadas a tomar antes e depois do tratamento ou preparação dos diferentes tipos de trabalho classificado, incluindo normas de rotina para limpar a memória principal, as secundárias, assim como as memórias associadas aos equipamentos periféricos;
g) Exame dos registos manuais e dos registos de computador a fim de verificar o cumprimento das instruções;
h) Procedimento a seguir em caso de avaria de um componente do sistema, falha de corrente ou outro incidente que possa comprometer a fidelidade e ou as características de funcionamento dos dispositivos de segurança do sistema;
i) Directivas aos utilizadores do Centro, como, por exemplo, preparação de dados de entrada que incluam requisitos de segurança, responsabilidade em matéria de classificação, protecção de identidade dos utilizadores e das senhas para acesso aos dados e comunicação de situações pouco usuais, que possam pôr em causa a segurança, tais como a recepção de saídas não pedidas;
j) Plano de destruição de todas as informações classificadas do Centro.

O Primeiro-Ministro, *Aníbal António Cavaco Silva.*