

TRIBUNAL DE CONTAS



**RELATÓRIO N.º
26/02-2ªS**

**AUDITORIA AOS
SISTEMAS DE ATRIBUIÇÃO E
CONTROLO DE PENSÕES**

**LISBOA
JUNHO/2002**



Índices

Geral

	<u>Pág.</u>
ABREVIATURAS UTILIZADAS	4
FICHA TÉCNICA.....	6
I SUMÁRIO	7
II CONCLUSÕES E RECOMENDAÇÕES	9
II.1. CONCLUSÕES.....	9
II.1.1. <i>Processos de Atribuição e Controlo de Pensões</i>	9
II.1.1.1. Processo de Gestão de Requerimentos.....	9
II.1.1.2. Processo de Atribuição e Cálculo de Pensões.....	10
II.1.1.3. Processamento e Pagamento de Pensões	11
II.1.1.4. Maturidade e Eficiência dos Processos.....	11
II.1.2. <i>Processos de Gestão de Sistemas de Informação</i>	13
II.1.2.1. Processo de Planeamento e Estratégia de TI.....	14
II.1.2.2. Processo de Aquisição e Desenvolvimento de Sistemas.....	15
II.1.2.3. Processo de Operação do Ambiente de TI.....	16
II.1.2.4. Processo de Monitorização dos Processos de TI.....	18
II.2. SÍNTESE DAS RECOMENDAÇÕES.....	20
II.2.1. <i>Processos de Atribuição e Controlo de Pensões</i>	20
II.2.2. <i>Processos de Gestão de Sistemas de Informação</i>	24
III INTRODUÇÃO.....	28
III.1. OBJECTIVOS E ÂMBITO DA AUDITORIA	28
III.2. METODOLOGIA	28
III.3. EXERCÍCIO DO CONTRADITÓRIO	29
III.4. CONDICIONANTES E LIMITAÇÕES	30
IV. ENQUADRAMENTO JURÍDICO-FINANCEIRO E INSTITUCIONAL.....	31
IV.1. ENVOLVENTE SÓCIO-ECONÓMICA.....	31
IV.2. ENQUADRAMENTO JURÍDICO DAS PRESTAÇÕES DIFERIDAS.....	35
IV.3. DADOS FÍSICOS, FINANCEIROS E DE GESTÃO DAS PRESTAÇÕES RELATIVAS A PENSÕES.....	40
IV.3.1. <i>Dados Físicos</i>	40
IV.3.2. <i>Dados Financeiros</i>	41
IV.3.3. <i>Indicadores de Gestão</i>	43
IV.4. INSTITUIÇÕES DO SISTEMA DE SOLIDARIEDADE E SEGURANÇA SOCIAL.....	52
V. PROCESSOS E SISTEMAS DE ATRIBUIÇÃO E CONTROLO DE PENSÕES	54
V.1. IDENTIFICAÇÃO DOS PROCESSOS.....	54
V.2. OS PROCESSOS DE GESTÃO DE SISTEMAS DE INFORMAÇÃO	55
V.2.1. <i>As Principais Aplicações</i>	55
V.2.2. <i>As Principais Plataformas de Hardware</i>	56
V.2.3. <i>A Infra-estrutura de Redes</i>	57
VI. METODOLOGIA E RESULTADOS DA AUDITORIA INFORMÁTICA	59



Tribunal de Contas

VI.1.	METODOLOGIA DE AVALIAÇÃO DE RISCOS E CONTROLOS.....	59
VI.1.1.	<i>Definição de Conceitos.....</i>	<i>60</i>
VI.1.1.1.	Conceitos de Risco e Controlo	60
VI.1.1.2.	Conceitos de Avaliação de Processos	63
VI.1.1.3.	Conceitos da Maturidade de Processos	65
VI.1.2.	<i>Processos de Atribuição e Controlo de Pensões</i>	<i>68</i>
VI.1.2.1.	Testes aos Cálculos de Pensões.....	69
VI.1.2.2.	Testes de processos de Pensões calculados manualmente.....	71
VI.1.3.	<i>Sistemas e Tecnologias de Informação</i>	<i>74</i>
VI.1.3.1.	Testes ao Processo de Desenvolvimento.....	75
VI.1.3.2.	Testes à Segurança dos Sistemas de Informação.....	76
VI.2.	SÍNTESE DOS RESULTADOS DA AUDITORIA	78
VI.2.1.	<i>Processos de Atribuição e Controlo de Pensões</i>	<i>78</i>
VI.2.1.1.	Gestão de Requerimentos	78
VI.2.1.2.	Atribuição e Cálculo de Pensões	80
VI.2.1.3.	Processamento e Pagamento de Pensões	86
VI.2.2.	<i>Processos de Gestão de Sistemas de Informação.....</i>	<i>88</i>
VI.2.2.1.	Planeamento e Estratégia de Sistemas de Informação	90
VI.2.2.2.	Processo de Aquisição e Desenvolvimento de Sistemas	101
VI.2.2.3.	Processo de Operação do Ambiente de TI.....	104
VI.2.2.4.	Processo de Monitorização dos Processos de TI.....	111
VII	EMOLUMENTOS	112
VIII	DECISÃO	113
	ÍNDICE DOS ANEXOS	114



Tribunal de Contas

Tabelas

TABELA 1 -	AVALIAÇÃO DOS PROCESSOS DE ATRIBUIÇÃO E CONTROLO DE PENSÕES.....	12
TABELA 2 -	MATURIDADE E EFICIÊNCIA DOS PROCESSOS DE GESTÃO DE SISTEMAS DE INFORMAÇÃO.	15
TABELA 3 -	MATURIDADE E EFICIÊNCIA DO PROCESSO DE AQUISIÇÃO E DESENVOLVIMENTO DE SISTEMAS.....	16
TABELA 4 -	MATURIDADE E EFICIÊNCIA DO PROCESSO DE OPERAÇÃO DO AMBIENTE DE TI.....	17
TABELA 5 -	MATURIDADE E EFICIÊNCIA DO PROCESSO DE MONITORIZAÇÃO DOS PROCESSOS DE TI....	18

Quadros

QUADRO I -	EVOLUÇÃO DA POPULAÇÃO POR REGIME	40
QUADRO II -	EVOLUÇÃO DAS PENSÕES DE REFORMA POR REGIMES E EVENTUALIDADES	42
QUADRO III -	PROCESSOS ENTRADOS.....	44
QUADRO IV -	PROCESSOS CONCLUÍDOS.....	46
QUADRO V -	PROCESSOS PENDENTES POR EVENTUALIDADE.....	47
QUADRO VI -	PROCESSOS PENDENTES POR FASE DE TRAMITAÇÃO	48
QUADRO VII -	TEMPO MÉDIO DOS PROCESSOS CONCLUÍDOS	51
QUADRO VIII -	PRESSUPOSTOS	72
QUADRO IX -	AMOSTRA	73
QUADRO X -	TIPO DE EVENTUALIDADES.....	74

Gráficos

GRÁFICO 1 -	CSS – DESPESAS E TRANSFERÊNCIAS DOS PRINCIPAIS AGREGADOS (% PIB) – CONTINENTE E RA.....	33
GRÁFICO 2 -	CSS – DESPESAS COM PENSÕES, SUPLEMENTOS E COMPLEMENTOS POR TIPO DE MODALIDADE (PREÇOS CORRENTES) – CONTINENTE E RA.....	34
GRÁFICO 3 -	EVOLUÇÃO DA POPULAÇÃO POR REGIME	41
GRÁFICO 4 -	EVOLUÇÃO DOS GASTOS COM PENSÕES, POR REGIME.....	42
GRÁFICO 5 -	PROCESSOS ENTRADOS NO CNP EM 2000.....	45
GRÁFICO 6 -	PROCESSOS DA ÁREA NACIONAL.....	45
GRÁFICO 7 -	PROCESSOS NACIONAIS E INTERNACIONAIS AGREGADOS.....	49
GRÁFICO 8 -	DIAGRAMA DE FLUXO DE DADOS DE CONTEXTO	57
GRÁFICO 9 -	AMOSTRA POR EVENTUALIDADES.....	74
GRÁFICO 10 -	PRAZOS ENTRE A DATA DE GRAVAÇÃO E A DATA DE ENCERRAMENTO	85



Tribunal de Contas

ABREVIATURAS UTILIZADAS

Siglas	Descrição
BDR	Base de Dados Regional
BNDBU	Base Nacional de Dados de Beneficiários e Utentes
CDSSS	Centro Distrital de Solidariedade e Segurança Social
CGA	Caixa Geral de Aposentações
CNP	Centro Nacional de Pensões
CNPRP	Centro Nacional de Prevenção contra os Riscos Profissionais
CobIT	<i>Control Objectives for Information and Related Technology</i>
COSO	<i>Committee of Sponsoring Organizations of the Tradway Commission</i>
CRSS	Centro Regional de Segurança Social
CSS	Conta da Segurança Social
CTT	Correios de Portugal
CVIP	Comissão de Verificação de Incapacidades Permanentes
DL	Decreto-Lei
DPG	Departamento de Planeamento e Gestão
DSOPG	Direcção de Serviços de Organização, Planeamento e Gestão
FCR	Ficheiro central de Requerentes
FP	Ficheiro de Pensionistas
IGFSS	Instituto de Gestão Financeira da Segurança Social
IIES	Instituto de Informática e Estatística da Solidariedade
ISSS	Instituto de Solidariedade e Segurança Social
ONI	Organismo Nacional de Informática
PI	Pensão de Invalidez
PIB	Produto Interno Bruto
POCISSSS	Plano Oficial de Contabilidade das Instituições do Sistema de Solidariedade e Segurança Social



Tribunal de Contas

Siglas	Descrição
PS	Pensão de Sobrevivência
PV	Pensão de Velhice
RESSAA	Regime Especial de Segurança Social das Actividades Agrícolas
RG	Regime Geral
RNCE	Regime Não Contributivo e Equiparado
SAC	<i>System Auditability & Control</i>
SCML	Santa Casa da Misericórdia de Lisboa
SDLC	<i>System Development Life Cycle</i>
SI	Sistemas de Informação
SI	Sistema Informático
SRTC	Secção Regional do Tribunal de Contas
SSR	Serviço Sub Regional
SSSS	Sistema da Solidariedade e da Segurança Social
SVI	Serviço de Verificação de Incapacidades
TI	Tecnologias de Informação
UOPG	Unidade de Organização, Planeamento e Gestão



Tribunal de Contas

FICHA TÉCNICA

Sob a supervisão geral do Auditor-Coordenador *Dr. António Manuel Fonseca da Silva*, colaboraram neste trabalho os seguintes elementos:

Serviço	Função	Nome	Cargo / Categoria	Formação base
DA VII	Coordenação da Equipa	José Manuel Barbeita Pereira	Auditor-Chefe	Lic. Gestão de Empresas
	Execução	M. ^a Alexandrina Marina Fonseca	Auditora	Lic. Direito
		Vítor Manuel C. R. Domingos	Técnico Verificador Superior de 1 ^a Classe	Lic. Economia
	Assessoria jurídica	Gaspar Moreira Cardoso da Costa	Consultor	Lic. Direito

A execução da auditoria informática esteve a cargo de:

Ernst & Young	Consultor Externo	Rui Bastos	Coordenador da Equipa	Lic. Gestão de Empresas Lic. Sistemas de Informação
--------------------------	--------------------------	------------	-----------------------	--

Este trabalho contou, ainda, com a colaboração de:

SRTC Açores		Aida Sousa	Auditora	Lic. Gestão de Empresas
SRTC Madeira		Rui Rodrigues	Técnico Verificador Superior de 1 ^a Classe	Lic. Gestão de Empresas
		Luís Rodolfo Sousa	Técnico Superior de Informática de 1 ^a Classe	Lic. Engenharia Informática



Tribunal de Contas

I. SUMÁRIO

A auditoria realizada pelo Tribunal de Contas aos **Sistemas de Avaliação e Controlo de Pensões da Segurança Social**, e que contou com a colaboração da *ERNST&YOUNG* como consultor externo, centrou-se no respectivo Regime Geral (que, em 2000, ano de referência da auditoria, representou mais de 77% do total dos pensionistas e 84% do total das despesas com pensões) e visou analisar em que medida os seus processos oferecem, com o mínimo de riscos, as garantias necessárias para alcançar os objectivos estabelecidos pela legislação vigente.

A auditoria identificou, através de entrevistas com responsáveis do CNP, CDSSS, IGFSS e IIES, os processos principais existentes nesta área (gestão de requerimentos; atribuição e cálculo de pensões; processamento e pagamento de pensões), assim como os sistemas informáticos principais que os suportam, respectivas plataformas de *hardware* e infra-estruturas de redes. Considerou-se, por isso, conveniente proceder a uma avaliação dos processos de gestão de sistemas de informação.

Os conceitos base subjacentes aos modelos COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) e CobIT (*Control Objectives for Information and Related Technology*) foram utilizados extensivamente na avaliação dos processos de atribuição e controlo de pensões, enquanto o modelo CobIT foi utilizado, exclusivamente, na avaliação dos processos de gestão de sistemas de informação, conduzindo, em síntese, aos seguintes resultados:

a) Atribuição e Controlo de Pensões

A atribuição e o pagamento de pensões são efectuados, em grande parte, de forma correcta, assegurando que as pensões pagas são as devidas, nos termos das leis em vigor.

Existe, porém, necessidade de introdução de melhorias significativas no processo de gestão de requerimentos (que em 2000 foram mais de 190.000), designadamente em termos de maior integração e uniformização da informação e do reforço da aplicação relativa à validação da informação. Relativamente ao processo de atribuição e cálculo de pensões, verificou-se que, quanto aos regimes especiais, não existem os correspondentes programas de cálculo. Quanto ao processamento e pagamento de pensões, apesar de o respectivo processo estar razoavelmente controlado, existem ainda riscos significativos no tratamento e registo das devoluções de pensões, bem como ineficiências na reconciliação dos pagamentos efectuados.

Em termos de avaliação global, a pontuação atribuída à maturidade do processo, numa escala de 0 a 5, é de **3**.



Tribunal de Contas



Tribunal de Contas

b) Gestão de Sistemas de Informação

Foram analisados o planeamento e a estratégia de TI (a que foi atribuída a pontuação de **2**), a aquisição e desenvolvimento de sistemas (a que foi, igualmente, atribuída a pontuação de **2**), a operação do ambiente de TI (que foi pontuada com **1**) e a monitorização dos processos de TI (que se considerou como não existente, tendo-lhe sido, por isso, atribuída a pontuação de **0**).

Há, aliás, realidades muito diferentes nesta matéria nas diversas entidades do Sistema da Segurança Social abrangido pela auditoria, existindo várias actividades que ainda estão por implementar, algumas das quais são importantes para colmatar os riscos associados aos sistemas de informação.



Tribunal de Contas

II. CONCLUSÕES E RECOMENDAÇÕES

II.1. Conclusões

As conclusões que de seguida se apresentam, encontram-se agrupadas de acordo com as duas grandes áreas cobertas pelo âmbito desta auditoria, nomeadamente:

- Processos de Atribuição e Controlo de Pensões
- Processos de Gestão de Sistemas de Informação.

II.1.1. *Processos de Atribuição e Controlo de Pensões*

Os resultados da auditoria indicam que a atribuição e o pagamento de pensões são efectuados, em grande parte, de forma correcta, assegurando que as pensões pagas são as devidas, nos termos da lei em vigor. A aplicação da legislação na execução destes processos é, geralmente, bem executada, compensando algumas fraquezas no funcionamento do sistema; considera-se, no entanto, que são necessárias melhorias para assegurar uma melhor eficiência e um controlo mais efectivo destes processos.

II.1.1.1. PROCESSO DE GESTÃO DE REQUERIMENTOS

O processo de Gestão de Requerimentos, que começa com a recepção do requerimento de uma pensão, requer melhorias significativas, em termos do seu funcionamento e níveis de automatização. Os CDSSS, como as entidades mais próximas do público, devem ter a informação necessária para:

- prestar um atendimento eficiente ao público, e
- poder confrontar e validar a informação apresentada na recepção de um requerimento de pensão.

Para dar satisfação a estas necessidades, vai ser necessária uma maior integração dos sistemas dos CDSSS e do CNP, principalmente no que se refere à integração e validação da carreira contributiva e à identificação de contribuintes. Os atrasos na integração de informação proveniente dos CDSSS contribuem para uma carga administrativa adicional, que não é justificada. Estas medidas são fundamentais para reduzir os atrasos no processamento dos requerimentos e melhorar a qualidade dos serviços prestados ao público.



Tribunal de Contas

Existe, também, uma clara necessidade de reforçar a aplicação existente com funcionalidades ou controlos aplicativos interactivos que validem a informação registada e mantenham um rasto de alterações no sistema, de forma a que:

- os erros ou omissões sejam corrigidos no acto da sua introdução;
- parte da conferência e verificação da informação necessária para o deferimento de uma pensão seja automaticamente verificada;
- o envio de processos de requerimentos incompletos para o CNP seja minimizado;
- o processo seja monitorizável com maior facilidade; e
- se possa produzir indicadores de gestão adequados sobre o seu funcionamento.

Sem um nível de indicadores de gestão adequados e atempados sobre a eficiência deste processo, é difícil apontar as causas e instituir as medidas necessárias para a sua melhoria.

II.1.1.2. PROCESSO DE ATRIBUIÇÃO E CÁLCULO DE PENSÕES

De acordo com o trabalho realizado e com os pressupostos assumidos na avaliação dos processos de “atribuição e controlo de pensões”, tudo indica que o cálculo e o pagamento se encontram adequadamente controlados, não se afigurando a existência de erros materiais. Os resultados dos testes efectuados confirmam que existem controlos efectivos que detectam e corrigem a maioria dos potenciais erros.

Mesmo assim, identificou-se a ausência de uma segregação das funções efectiva, no que respeita ao deferimento de uma pensão, o que representa um factor adicional de exposição a riscos no processo de atribuição de pensões, pois que se trata de um requisito determinante para assegurar que somente as pensões válidas são processadas e pagas.

Considera-se que o processo de cálculo de pensões não está adequadamente suportado por aplicações informáticas, devido, principalmente:

- aos regimes especiais, para os quais não existem, ainda, programas de cálculo; e
- à necessidade de desenvolvimentos significativos para dar resposta a um novo regime.

Esta falta de suporte informático a este processo contribui significativamente para a ineficiência deste processo e para o atraso na atribuição de pensões.



Tribunal de Contas

II.1.1.3. PROCESSAMENTO E PAGAMENTO DE PENSÕES

O Processo de Processamento e Pagamento de Pensões está razoavelmente bem controlado, embora se reconheça que ainda existem riscos significativos no tratamento e registo das devoluções de pensões, bem como ineficiências na reconciliação dos pagamentos efectuados. Considerando que o ISSS está a promover o incremento de pagamento de pensões através dos bancos, será necessário melhorar a integração automática da informação recebida dos mesmos.

Dadas as limitações dos sistemas existentes, a longo prazo o ISSS deve seriamente considerar o redesenho dos sistemas, de forma que as alterações legislativas sejam parametrizáveis e não programadas. Os novos sistemas devem também contemplar a necessidade de um rasto de auditoria melhorado, para que a despistagem das alterações efectuadas aos processos seja facilitada.

Finalmente, considera-se que os impactes das alterações legislativas às pensões deverão ser minimizados, adoptando um processo de actualização mais estruturado, que considere, nomeadamente, um *timing* para a elaboração dos projectos legislativos, e a comunicação às entidades competentes antes da sua publicação.

II.1.1.4. MATURIDADE E EFICIÊNCIA DOS PROCESSOS

A avaliação da maturidade dos processos de “atribuição e controlo de pensões” pode ser resumida nos termos do quadro que segue:



Tribunal de Contas

Tabela 1 - Avaliação dos Processos de Atribuição e Controlo de Pensões

Nome do Processo e Actividades Associadas	Avaliação de Maturidade		Objectivos de Controlo Atingidos							
	Patamar de Evolução da Actividade	Pontuação	Classificado	Registado	Lançado	Sumariado	Real	Atempado	Eficiente	Eficaz
Gestão de Requerimentos										
Recepção e Registo do Requerimento	Repetitivo	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Identificação do Beneficiário	Gerido	4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Envio e Integração de Informação com o CNP	Repetitivo	2		<input checked="" type="checkbox"/>				<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Atribuição e Cálculo de Pensões										
A Conferência e Deferimento de Processos	Gerido	4		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
O Cálculo da Pensão	Definido	3		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Processamento e Pagamento de Pensões										
Actualização Periódica das Pensões	Repetitivo	2		<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Processamento Mensal das Pensões	Definido	3	<input checked="" type="checkbox"/>							
Pagamento de Pensões	Definido	3	<input checked="" type="checkbox"/>							
AVALIAÇÃO GLOBAL DO PROCESSO	DEFINIDO	3								

Legenda:

- Existem controlos que suportam o objectivo de controlo e os mesmos são efectivos
- Existem controlos que suportam o objectivo de controlo mas não são efectivos
- Não existem controlos que suportem o objectivo de controlo.

O processo de Atribuição e Controlo de Pensões está razoavelmente definido, embora apresentando áreas onde é possível efectuar melhorias, nomeadamente no que respeita à eficiência das actividades nele envolvidas. O potencial que a utilização mais intensiva dos Sistemas de Informação oferece, como ferramenta de controlo e desempenho do processo, não é adequadamente aproveitado, considerando-se que existem várias lacunas na integração e uniformização dos sistemas existentes, que resultam em:

- aumento desnecessário da carga administrativa inerente ao processo de atribuição de pensões;
- gestão detalhada do sistema, que seria facilitada pela interligação da informação operacional e financeira;
- aumento dos custos necessários para o funcionamento, gestão e manutenção dos processos; e



Tribunal de Contas

- inferior qualidade dos serviços prestados pelos funcionários do ISSS no contacto directo com o público, pela inadequação do nível de informação prestado pelo sistema às necessidades existentes.

Atendendo à realidade do SSSS, os objectivos de controlo sobre a eficácia e a eficiência dos processos devem ter um destaque especial. Neste contexto, devem merecer especial atenção todos os aspectos que contribuam para uma melhoria dos serviços prestados e para a diminuição da carga administrativa excessiva, associada aos processos operacionais. Para atingir este objectivo, terá que ser reforçada a automatização dos processos e integração de sistemas do SSSS.

Quanto à avaliação das aplicações que suportam todo o processo, observou-se que as aplicações existentes não oferecem uma cobertura suficiente para os regimes de pensões especiais, contribuindo, assim, para o elevado volume de processos cujo tratamento é manual; como factores de maior risco, refere-se que o desenho das aplicações:

- não oferece um rasto de alterações de dados suficiente para averiguar, com um nível de detalhe suficiente, o histórico de alterações;
- não facilita o confronto e validação automática da informação introduzida, aumentando o risco de ocorrência de problemas relacionados com a qualidade da informação produzida;
- não permite dar uma resposta atempada às inúmeras alterações provenientes da legislação, obrigando a esforços adicionais de produtividade dos elementos das Unidades Informáticas;
- não permitem a execução *online* de várias estatísticas e relatórios de controlo que permitiriam uma melhor gestão dos processos.

Detectou-se, por outro lado, a necessidade de uma maior integração da informação trocada entre os sistemas existentes nos CDSSS e os centralizadores de pagamentos (como os bancos).

II.1.2. Processos de Gestão de Sistemas de Informação

A arquitectura dos sistemas e tecnologias de informação do SSSS encontra-se numa fase de grandes transformações, que terão, previsivelmente, um impacte significativo sobre os seus processos, tecnologias e recursos humanos, tendo como principal objectivo a significativa melhoria qualitativa dos serviços prestados, bem como a obtenção de eficiências resultantes da informatização de processos.

O sucesso desta transformação e a realização das melhorias preconizadas para o sistema de atribuição e controlo de pensões depende de uma articulação detalhada das estratégias de



Tribunal de Contas

sistemas de informação a serem adoptadas, mas, também, das políticas e dos procedimentos necessários para dar efeito a essas estratégias.

II.1.2.1. PROCESSO DE PLANEAMENTO E ESTRATÉGIA DE TI

Os resultados da avaliação das actividades relacionadas com o processo de Planeamento e Estratégia de TI apontam para a necessidade de se definir vários aspectos para a gestão dos sistemas de informação do SSSS.

Os passos já tomados, em termos da estratégia estabelecida, requerem que as políticas e procedimentos necessários para dar efeito às mesmas sejam definidas e divulgadas a todo o universo de utilizadores do SSSS. Como parte integrante desta iniciativa, é importante que as Políticas e Procedimentos, ainda por desenvolver, providenciem uma maior cobertura dos aspectos de gestão da qualidade e dos riscos globais inerentes aos sistemas de informação.

A estratégia de sistemas de informação definida pelo IIES é um importante ponto de partida para esclarecer as suas necessidades, em termos da futura arquitectura e organização dos sistemas de informação do SSSS. Os passos já tomados requerem a definição de políticas e de procedimentos de segurança dos sistemas de informação, necessitando ainda de ser desenvolvidos e integrados os aspectos relacionados com a Avaliação de Riscos de TI e de Gestão de Qualidade.

II.1.2.1.1. MATURIDADE E EFICIÊNCIA DO PROCESSO

Os resultados da avaliação efectuada sobre as actividades que constituem o Processo de Planeamento e Estratégia de TI do SSSS são resumidos na tabela seguinte:



Tribunal de Contas

Tabela 2 - Maturidade e Eficiência dos Processos de Gestão de Sistemas de Informação

Nome da Actividade	Avaliação de Maturidade	Pontuação	Confidencialidade	Integridade	Disponibilidade	Eficácia	Eficiência	Cumprimento com Requisitos	Fiabilidade
Definição da Estratégia de TI	Repetitivo	2				D	P		
Definição de uma Arquitectura de Informação	Definido	2	P	P		D	P		
Definição da Direcção Tecnológica de TI	Repetitivo	2				D	P		
Definição da Organização de TI e outras Interdependências	Repetitivo	2				D	P		
Gestão dos Investimentos em TI	Definido	3				D	D		P
Comunicação das Orientações Estratégicas	Repetitivo	2				D		P	
Gestão dos Recursos Humanos	Principiante	1				D	D		
Cumprimento com Requisitos externos	Definido	3				D		D	P
Avaliação de Riscos de TI	Repetitivo	2	D	D	D	D	P	P	P
Gestão dos Projectos em Curso	Repetitivo	2				D	D		
Gestão da Qualidade	Repetitivo	2				D	D		P
AVALIAÇÃO GLOBAL	REPETTIVO	2							

Legenda:

D – A actividade tem um impacte directo sobre o objectivo de controlo.

P – A actividade tem um impacte indirecto sobre o objectivo de controlo.

II.1.2.2. PROCESSO DE AQUISIÇÃO E DESENVOLVIMENTO DE SISTEMAS

O processo de Aquisição e Desenvolvimento de Sistemas é fundamental para traduzir as necessidades, dos serviços de processamento de informação, em sistemas e aplicações. É necessário um efectivo controlo deste processo para que as estratégias de sistemas de informação e, indirectamente, as estratégias de “negócio”, sejam alcançadas.

II.1.2.2.1. MATURIDADE E EFICIÊNCIA DO PROCESSO

A tabela a seguir apresenta um resumo da avaliação efectuada relativamente às actividades inerentes a este Processo.



Tribunal de Contas

Tabela 3 - Maturidade e Eficiência do Processo de Aquisição e Desenvolvimento de Sistemas

Nome da Actividade	Avaliação de Maturidade	Pontuação	Confidencialidade	Integridade	Disponibilidade	Eficácia	Eficiência	Cumprimento com Requisitos	Fiabilidade
Identificações de Soluções	Repetitivo	2				D	P		
Aquisição e Manutenção de Aplicações	Repetitivo	2		P		D	D	P	P
Aquisição e Manutenção da Arquitectura de Tecnológica	Principiante	1		P		D	D		
Desenvolvimento e Manutenção de Procedimentos de TI	Principiante	1		P		D	D	P	P
Instalação e Certificação de Sistemas	Repetitivo	2		P	P	D			
Gestão da Mudança	Repetitivo	2		D	D	D	D		P
AVALIAÇÃO GLOBAL	REPETITIVO	2							

Legenda:

D – A actividade tem um impacte directo sobre o objectivo de controlo.

P – A actividade tem um impacte indirecto sobre o objectivo de controlo.

Os resultados da avaliação das actividades relacionadas com o processo de aquisição e desenvolvimento de sistemas de TI indicam que existem várias actividades com um nível de maturidade razoável; no entanto, considera-se que as entidades auditadas carecem dos seguintes controlos:

- a adopção de uma metodologia formal e *standard* na execução de trabalho de desenvolvimento de sistemas através das várias fases do seu ciclo de vida (*System Development Life Cycle - SDLC*);
- a definição formal dos requisitos mínimos para o teste e aprovação de qualquer desenvolvimento ou alteração aos sistemas de informação do SSSS.

A manutenção de procedimentos de TI dependerá, em parte, da definição das políticas e procedimentos anteriormente referidos.

II.1.2.3. PROCESSO DE OPERAÇÃO DO AMBIENTE DE TI

II.1.2.3.1. MATURIDADE E EFICIÊNCIA DO PROCESSO

A tabela seguinte apresenta um resumo das avaliações das actividades inerentes a este Processo.



Tribunal de Contas

Tabela 4- Maturidade e Eficiência do Processo de Operação do Ambiente de TI

Nome da Actividade	Avaliação de Maturidade	Pontuação	Confidencialidade	Integridade	Disponibilidade	Eficácia	Eficiência	Cumprimento com Requisitos	Fiabilidade
Definição dos Níveis de Serviço	Não existente	0	P	P	P	D	D	P	P
Gestão dos Serviços Prestados por Terceiros	Definido	3	P	P	P	D	D	P	P
Gestão da Performance e da Capacidade	Repetitivo	2			P	D	D		
Assegurar a Continuidade dos Serviços Prestados	Repetitivo	2			D	D	P		
Gestão da Segurança dos Sistemas	Principiante	1	D	D	P			P	P
Identificação e afectação dos custos	Não existente	0					D		D
Prestação de Apoio e Formação aos Utilizadores	Principiante	1				D	P		
Apoiar e aconselhar os Clientes	Principiante	1				D	D		
Gestão da Configuração	Principiante	1			P	D			P
Resolução e Gestão de Problemas de TI	Principiante	1			P	D	D		
Gestão dos Dados	Principiante	1		D					D
Gestão das Instalações Físicas	Principiante	1		D	D				
Gestão das Operações	Principiante	1		P	P	D	D		
AVALIAÇÃO GLOBAL	PRINCIPIANTE	1							

Legenda:

D – A actividade tem um impacto directo sobre o objectivo de controlo.

P – A actividade tem um impacto indirecto sobre o objectivo de controlo.

A avaliação das actividades inerentes ao processo de Operação do Ambiente de TI evidenciou uma alta dependência das entidades do SSSS relativamente aos colaboradores de cada um dos serviços/unidades de Sistemas de Informação, resultado da não formalização e da não sistematização dos procedimentos para execução das actividades inerentes a este processo. A formalização de procedimentos e rotação de tarefas permitirá sistematizar e reduzir esta dependência.

Adicionalmente, a inexistência de políticas de segurança aumenta o risco de os colaboradores do SSSS, não tendo consciência das suas responsabilidades, como utilizadores e administradores dos SI, poderem pôr em causa a confidencialidade, integridade e disponibilidade da informação.

Existem várias oportunidades de melhoria, através da automatização das tarefas em cada uma das seguintes actividades, nomeadamente:



Tribunal de Contas

- Gestão da Performance e da Capacidade;
- Gestão da Segurança dos Sistemas;
- Gestão da Configuração; e
- Gestão das Operações.

Finalmente, como forma de gerir melhor a continuidade dos serviços de Sistemas de Informação, entende-se ser necessário impor, como prioridade, a definição de planos de *disaster recovery* para os SI, devendo, entre outros aspectos, ser determinados procedimentos de salvaguarda de cópias de segurança fora das instalações de processamento.

II.1.2.4. PROCESSO DE MONITORIZAÇÃO DOS PROCESSOS DE TI

II.1.2.4.1. MATURIDADE E EFICIÊNCIA DO PROCESSO

A tabela apresenta um resumo das avaliações das actividades inerentes ao Processo em causa.

Tabela 5 - Maturidade e Eficiência do Processo de Monitorização dos Processos de TI

Nome da Actividade	Avaliação de Maturidade	Pontuação	Confidencialidade	Integridade	Disponibilidade	Eficácia	Eficiência	Cumprimento de Requisitos	Fiabilidade
Monitorização dos Processos de TI	Não existente	0	P	P	P	D	D	P	P
Avaliação do controlo interno de TI	Principiante	1	P	P	P	D	D	D	P
Certificação de Serviços e Sistemas	Não existente	0	P	P	P	D	D	D	P
Execução de Auditorias Independentes	Não existente	0	P	P	P	D	D	D	P
AVALIAÇÃO GLOBAL	NÃO EXISTENTE	0							

Legenda:

D – A actividade tem um impacto directo sobre o objectivo de controlo.

P – A actividade tem um impacto indirecto sobre o objectivo de controlo.

Os resultados da avaliação efectuada ao modo de Monitorização dos Processos de TI indicam que não existem, nas entidades do SSSS, actividades suficientemente definidas para, de forma adequada, a poderem assegurar.



Tribunal de Contas

Em conclusão, reconhecem-se os significativos esforços efectuados por parte das várias entidades do ISSS para assegurar a correcta atribuição e controlo de pensões, existindo, ainda assim, diversas áreas que exigem uma maior atenção. Assim, a reestruturação e melhoria de sistemas de informação deve:

- assegurar também uma melhoria de controlos nos processos informatizados;
- ser efectuada de forma controlada para assegurar a qualidade dos sistemas disponibilizados;
- considerar de forma integrada as melhorias necessárias relativas aos aspectos relacionados com recursos humanos, para que os benefícios dos novos sistemas sejam alcançados.



Tribunal de Contas

II.2. Síntese das Recomendações

Os processos de atribuição e controlo de pensões têm um único objectivo, nomeadamente a prestação de um serviço ao público que seja:

- ☑ Eficiente na atribuição e deferimento de uma pensão, sem prejudicar o requerente com atrasos significativos na avaliação do seu requerimento;
- ☑ Efectuado de forma controlada, para que a pensão atribuída e paga seja correcta e devida em termos da legislação aplicável; e
- ☑ Eficaz na utilização de recursos humanos e informáticos para efectuar a prestação desse serviço.

Esta caracterização é importante para estabelecer o patamar de qualidade desejado para este serviço, permitindo também que as recomendações apresentadas vão ao encontro deste objectivo.

As recomendações que de seguida se apresentam encontram-se agrupadas¹ de acordo com as duas grandes áreas cobertas pelo âmbito desta auditoria, a saber:

- ☑ Processos de Atribuição e Controlo de Pensões;
- ☑ Processos de Gestão de Sistemas de Informação.

Esta síntese é um resumo das recomendações principais deste relatório – detalhadas, por processo, no **Anexo C – Recomendações Detalhadas** – as quais deverão ser encaminhadas, pelas entidades visadas, às unidades orgânicas a que dizem respeito.

II.2.1. *Processos de Atribuição e Controlo de Pensões*

Integração de Sistemas

Os processos abordados representam a última fase do ciclo de vida de um beneficiário/utente do Regime Geral de Pensões e, como tal, já dependem de informação proveniente de processos anteriores, devendo estar devidamente integrados com estes.

¹ Face à complexidade dos sistemas auditados e para evitar repetições desnecessárias.



Tribunal de Contas

Deste modo, o processo de gestão de requerimentos tem que começar com a maior integração da informação entre os vários sistemas informáticos que suportam a identificação de beneficiários, bem como o registo da sua carreira contributiva. Uma maior integração destes sistemas permitirá que:

- ☑ Os elementos de informação inerentes a um requerimento de pensão sejam disponibilizados, a fim de:
 - Permitir a validação da informação apresentada no requerimento no momento em que é apresentado no CDSS;
 - Reduzir o volume de informação introduzido no sistema com a apresentação do requerimento; e
 - Reduzir o volume de correspondência necessária para esclarecer eventuais dúvidas.

- ☑ O cálculo das pensões seja automático, minimizando a intervenção humana, necessária, neste momento, para inserir informação omissa no cálculo.

- ☑ A informação financeira inerente ao processamento de pensões seja integrada automaticamente no sistema financeiro do ISSS (integração directa com o SAP R/3).

- ☑ A execução dos pagamentos seja efectuada e reconciliada electronicamente com os bancos “centralizadores”, permitindo, assim, uma gestão mais eficiente das tesourarias do IGFSS.

- ☑ Uma maior informação de gestão seja disponibilizada para permitir avaliar o desempenho dos seus processos, bem como outros aspectos relacionados com as responsabilidades do SSSS.

Uma Presença *Online*

A integração destes sistemas também pode oferecer outros benefícios. Numa situação de integração desta informação, o ISSS teria a opção de utilizar a sua presença na Internet para mais do que simplesmente a divulgação de legislação e outra informação. Com os devidos mecanismos de segurança implementados, é também possível disponibilizar, através da Internet, a cada beneficiário/utente a capacidade de:

- ☑ Validar o seu histórico de contribuições;

- ☑ Actualizar outras informações, como moradas e detalhes de contas bancárias;

- ☑ Efectuar simulações de cálculos, com base no seu histórico de contribuições;



Tribunal de Contas

- Preparar e, eventualmente, apresentar requerimentos de pensão, e
- Comunicar com o ISSS.

A apresentação das declarações de contribuições em formato electrónico por parte das empresas vai permitir reduzir os atrasos no registo da carreira contributiva, possibilitando, assim, ao contribuinte/beneficiário validar os seus registos de contribuições e os seus dados pessoais de forma quase imediata. A possibilidade de apresentação de um requerimento *online* permitirá que:

- A carreira contributiva do requerente possa ser validada pelo próprio antes de apresentação do requerimento;
- A validação automática da informação declarada no requerimento;
- O requerente/beneficiário/utente tenha um meio de actualizar os seus dados pessoais como morada e detalhes bancários;
- O volume de informação introduzido pelos elementos do CDSSS seja significativamente reduzido;
- A recepção do requerimento sirva somente para confrontar a declaração efectuada pelo conferente com os documentos apresentados;
- O status do requerimento seja visível ao requerente quando acede via Internet, poupando assim tempo e custos de deslocações aos CDSSS;
- As simulações de pensões prováveis sejam efectuadas *online*, reduzindo assim o volume de requerimentos manuseados pelos CDSSS e pelo CNP; e
- O requerente possa imprimir uma cópia do seu requerimento preenchido para eventual apresentação, com a documentação comprovativa necessária, ao respectivo CDSSS.

Dado que nem todos os requerentes terão acesso à Internet, será ainda necessário disponibilizar outras formas de apresentação dos requerimentos de pensão; mas, as maiores eficiência e eficácia associadas à apresentação de requerimentos *online* permitirão uma maior disponibilidade, por parte dos CDSSS, para dar resposta a um volume de requerimentos cada vez maior.

Esta solução pouparia tempo e custos, ao Estado e ao requerente, no processo de recepção e processamento do requerimento de uma pensão, dando também resposta a outro aspecto apontado neste relatório – a falta de diferenciação, em termos de prioridade, entre o tratamento dado a cálculos prováveis de pensão e a cálculos efectivos.



Tribunal de Contas

Definição de Prioridades

Considera-se que um cálculo provável de pensão representa a prestação de um serviço de informação para que o requerente possa avaliar se deve ou não reformar-se. O cálculo provável não tem que conferir o direito a uma pensão, mas oferecer uma simulação da pensão que um beneficiário poderá receber no momento de reforma. Uma simulação efectuada *online*, com os dados reais do beneficiário, ofereceria uma resposta mais atempada sem a carga administrativa (e eventuais atrasos) associada a um requerimento de pensão efectivo.

Na medida do possível, o ISSS deve também desenvolver os conhecimentos e as competências necessárias para que os cálculos de pensões prováveis sejam efectuados nos CDSSS, dando assim uma resposta mais imediata ao público e reduzindo o volume de requerimentos que têm que ser processados e enviados para o CNP para eventual deferimento. Esta diferenciação permitirá:

- Dar prioridade ao deferimento de requerimentos de pensão definitivos;
- Criar mais conhecimentos e competências nos CDSSS, no que se refere ao deferimento de pensões; e
- Reduzir os prazos de resposta médios do ISSS aos requerimentos apresentados.

Flexibilidade de Cálculo

A legislação inerente ao deferimento e cálculo de pensões não é estática. Assim, considera-se que os sistemas e programas que dão apoio ao cálculo das pensões têm que ser suficiente flexíveis para dar resposta a uma legislação dinâmica.

Deste modo, recomenda-se que o programa de cálculo de pensões seja parametrizável, de forma que qualquer alteração no cálculo da pensão necessite somente da alteração da parametrização da fórmula e não da alteração dos programas que efectuam os cálculos.

O CNP já efectua a codificação do tipo de pensão consoante o tipo de regime aplicável à pensão. Recomenda-se, por isso, que a fórmula de cálculo seja parametrizável consoante código da pensão, de forma a impedir a alteração do programa de cálculo cada vez que um cálculo de pensão novo tenha que ser introduzido.

Também a validação do cálculo, por parte do conferente, deve ser efectuada com um programa *online*, que permita essa validação e a impressão do verbete no momento em que o cálculo é



Tribunal de Contas

efectuado. Este aspecto permitirá reduzir o nível de manuseamento de requerimentos e o prazo necessário para o deferimento de um requerimento.

Os programas utilizados devem também assegurar que todos os dados introduzidos no cálculo são gravados e fazem parte do respectivo registo no sistema. Em situações onde o cálculo da pensão é efectuado mais do que uma vez, todos os cálculos que originem uma alteração ao valor de pensão a pagar devem ficar registados como parte do histórico do requerimento, para assegurar o rasto das alterações.

II.2.2. Processos de Gestão de Sistemas de Informação

Estratégia de Sistemas de Informação

Para alcançar o objectivo de uma arquitectura de sistemas de informação integrada, que suporte de forma efectiva os processos do ISSS, é necessário ter:

- Uma estratégia de sistemas de informação de médio/longo prazo bem definida e estruturada em termos de projectos distintos, com prazos de execução bem definidos;
- Uma arquitectura applicacional que apresente uma visão detalhada das funcionalidades informáticas que serão necessárias para dar resposta às necessidades dos processos do ISSS;
- Um modelo de informação e de dados detalhado.

O IIES já tomou os primeiros passos neste sentido, com a definição do Novo Sistema de Informação para o SSSS, mas recomenda-se que o Conselho Consultivo do IIES seja constituído o mais rapidamente possível, para acelerar a concretização desse projecto.

Arquitectura Tecnológica e Aplicacional

Como parte integrante do projecto para o Novo Sistema de Informação do SSSS será necessário reflectir sobre a arquitectura tecnológica actual. Uma maior uniformidade das plataformas tecnológicas existentes no ISSS permitiria:

- Maior integração entre os sistemas do ISSS;
- Maior redundância de sistemas, oferecendo, assim, maior segurança e estabilidade na prestação de serviços informáticos;



Tribunal de Contas

- ☑ Melhor aproveitamento das funcionalidades inerentes às novas tecnologias;
- ☑ Redução dos custos inerentes à gestão e à manutenção das variadíssimas plataformas utilizadas, bem como do custo da manutenção das várias versões de uma aplicação;
- ☑ Redução dos recursos necessários para dar apoio aos utilizadores dos vários sistemas e aplicações;
- ☑ Maior flexibilidade na resposta a alterações na legislação com impacte nos sistemas;
- ☑ Mudança para uma única plataforma tecnológica, com custos mais baixos por unidade de processamento;
- ☑ Redução da dependência do ISSS em relação aos escassos recursos com competências técnicas para gerir certos sistemas; e
- ☑ Redução do risco associado à provável obsolescência de certas plataformas no médio prazo.

De facto, a uniformização de plataformas permitirá ao ISSS focar os seus recursos (limitados) na maior informatização dos seus processos e menos na manutenção e gestão dos mesmos. Esta melhoria só é possível com a definição de uma estratégia de sistemas de informação que vise a uniformização e integração dos vários sistemas e contemple a avaliação dos requisitos necessários para efectuar a transição para esta nova realidade.

Controlo da Qualidade

A transição dos sistemas existentes para o Novo Sistema de Informação vai exigir um rigor e controlo significativos, associados:

- ☑ Ao desenvolvimento de novos sistemas e aplicações para que cumpram com os requisitos funcionais dos processos do ISSS;
- ☑ À migração de informação e dados dos sistemas existentes para os novos.

O nível de aceitação, bem como a compreensão dos benefícios que novos sistemas podem apresentar, estão directamente relacionados com a capacidade do ISSS para controlar a execução destes projectos e gerir a qualidade da informação transitada. Neste sentido, o ISSS deve considerar um maior acompanhamento no processo de controlo de qualidade de desenvolvimentos, que monitorize e assegure:

- ☑ A execução controlada e atempada dos projectos em curso;



Tribunal de Contas

- O cumprimento dos requisitos funcionais estabelecidos;
- A implementação, nas novas aplicações, de controlos financeiros e operacionais suficientes, que validem a informação introduzida, garantindo a integridade da informação processada; e
- A integridade da informação migrada entre sistemas.

Segurança de Sistemas de Informação

Num ambiente em que os processos do ISSS estão cada vez mais informatizados, é fundamental que a segurança dos sistemas e da informação que é processada seja salvaguardada. Esta segurança deve ser abordada de forma integrada. O IIES está a tomar os primeiros passos, mas recomenda-se que seja considerada a concepção e implementação de uma arquitectura de segurança integrada para o ISSS.

Esta arquitectura de segurança tem que:

- Ter o apoio e aceitação de todas as entidades do ISSS que assumem responsabilidades pela gestão de sistemas de informação;
- Ser baseada numa avaliação dos riscos inerentes aos sistemas de informação do ISSS;
- Considerar e classificar a informação do ISSS, bem como os requisitos de segurança inerentes à informação mais sensível ou crítica;
- Definir as políticas de segurança que minimizem ou reduzam possíveis impactos negativos destes riscos; e
- As políticas de segurança têm que ser traduzidas em configurações de sistemas seguras e em procedimentos de administração e monitorização direccionados às plataformas tecnológicas.

Como parte desta arquitectura de segurança, o ISSS deve também contemplar a definição de um ou vários Planos de Contingência de Sistemas de Informação, para assegurar a continuidade dos seus sistemas mais críticos, e a redundância de competências e recursos humanos para efectuar a sua recuperação.

A uniformidade de plataformas e sistemas contribuirá significativamente para a redução do esforço necessário para definir e manter uma arquitectura de segurança que dê resposta aos riscos do ISSS.



Tribunal de Contas

Monitorização

A monitorização dos processos de gestão de sistemas de informação é um processo fundamental para assegurar:

- A melhoria do desempenho dos mesmos; e
- A identificação e minimização dos riscos inerentes a um ambiente de sistemas de informação cada vez mais complexo, integrado e crítico para o funcionamento do ISSS.



Tribunal de Contas

III. INTRODUÇÃO

III.1. Objectivos e Âmbito da Auditoria

O Tribunal de Contas, reconhecendo a importância da área das pensões da Segurança Social, inscreveu no seu Programa de Fiscalização para 2001 – Departamento de Auditoria VII – a realização de uma auditoria ao sistema de atribuição e controlo de pensões, com vista a avaliar em que medida os seus processos oferecem as garantias necessárias para alcançar os objectivos estabelecidos pela legislação vigente e consequente análise dos procedimentos a eles subjacentes que visam a minimização dos riscos inerentes.

Dado que uma componente significativa destes processos está informatizada, o Tribunal de Contas considerou importante avaliar também a infra-estrutura informática que os suporta. Este documento serve para relatar as conclusões da auditoria efectuada aos processos de atribuição e controlo de pensões, bem como aos processos de gestão de sistemas de informação que os suportam.

O fenómeno da transição destes sistemas para o EURO alargou o âmbito inicial dos trabalhos, dado que os riscos associados a esta transição poderiam ter um impacto profundo sobre os processos de atribuição e controlo de pensões. Para assegurar um relato atempado sobre os riscos associados ao Euro foi elaborado, em Dezembro de 2001, um documento, no qual se encontram inscritas as conclusões e recomendações então emitidos.

III.2. Metodologia

Atendendo ao peso que as pensões do Regime Geral têm no total da despesa com as prestações diferidas, foi determinado que o objectivo central desta auditoria fosse o levantamento e avaliação do sistema de atribuição e controlo das pensões do Regime Geral, em duas vertentes distintas:

- ◆ tramitação processual, quer administrativa, quer financeira; e
- ◆ consequente análise do tratamento automático da informação e do respectivo processamento, pagamento e controlos efectuados.

Nesse sentido, a auditoria foi dividida em duas fases distintas:

- A **primeira** foi desenvolvida com o objectivo de fornecer ao consultor externo na área dos sistemas de informação, um documento² de suporte, no sentido de lhe proporcionar uma visão transversal relativamente ao universo envolvido no trabalho a realizar, dando-

² Vide Anexo E – Levantamento dos Circuitos e da Arquitectura Informática.



Tribunal de Contas

se um especial destaque ao levantamento dos processos envolvidos e à descrição das tramitações a eles inerentes, tendo-se, para tal, procedido ao levantamento dos circuitos implementados respeitantes, designadamente:

- tramitação processual e administrativa relativa à atribuição das prestações;
 - processamento e pagamento das prestações atribuídas;
 - controlo inerente aos procedimentos anteriores;
 - levantamento exaustivo das aplicações no âmbito deste sistema;
- Na segunda, já com a participação do consultor externo, efectuou-se uma análise dos sistemas informáticos e das respectivas aplicações que suportam os processos de atribuição e controlo de pensões. Para enquadrar o âmbito desta auditoria informática no contexto do SSSS, considerou-se importante identificar e caracterizar:
 - os principais processos de atribuição e controlo de pensões;
 - a arquitectura informática, nomeadamente as aplicações, plataformas e redes informáticas que suportam os mesmos; e
 - os processos de gestão de sistemas e tecnologias de informação que os suportam.

Embora a análise incida sobre os processos na sua forma actual, o universo tratado foi limitado aos processos deferidos no ano de 2000, relativos, exclusivamente, às pensões do Regime Geral – Invalidez/ Velhice e Sobrevivência.

III.3. Exercício do Contraditório

De harmonia com o disposto no art.º 13.º da Lei n.º 98/97, de 26 de Agosto, foram ouvidas, para, querendo, alegar o que houvessem por conveniente acerca do relato de auditoria, as seguintes entidades:

- Gabinete do Ministro do Trabalho e da Solidariedade;
- Instituto da Solidariedade e Segurança Social;
- Instituto de Informática e Estatística da Solidariedade;
- Instituto de Gestão Financeira da Segurança Social.



Tribunal de Contas

Destas, remeteram alegações³ dentro do prazo determinado o Instituto da Solidariedade e Segurança Social e o Instituto de Informática e Estatística da Solidariedade.

Todos os comentários recebidos foram objecto de análise, tendo eventuais citações e os respectivos comentários sido introduzidos no **Anexo B – Detalhe dos Resultados da Auditoria**, nos pontos pertinentes, em tipo de letra diferente, projectando-se as eventuais alterações, sempre que se revelou adequado, no texto do relatório.

III.4. Condicionantes e Limitações

O desenvolvimento desta acção foi sujeita às seguintes limitações e condicionantes:

- A análise dos programas de cálculo revelou que os valores de pensões calculados e registados no ficheiro de pensionistas são gravados por cima dos registos existentes, eliminando o rasto das pensões anteriormente pagas, o que inviabilizou a sua validação directa;
- Relativamente às diferenças detectadas e embora a entidade responsável pelo cálculo e processamento das pensões pretendesse analisá-las exaustivamente, as limitações de tempo para a execução desse trabalho não permitiram que tal objectivo pudesse ser alcançado.

Destaque-se, por último, o facto de num trabalho com as características e complexidade do presente, em que estão envolvidas diversas entidades e onde foram contactados diferentes dirigentes e técnicos de vários organismos, se obteve, de todos eles, uma colaboração cordial e colaborante, consubstanciada no fornecimento de todos os elementos solicitados e na prestação de todas as informações pretendidas, necessários à realização desta auditoria.

³ Incluídas no **Anexo F**.



Tribunal de Contas

IV. ENQUADRAMENTO JURÍDICO-FINANCEIRO E INSTITUCIONAL

IV.1. Envolvente Sócio-Económica

Desde o fim da Segunda Guerra Mundial, o modelo de segurança e protecção social europeu passou a representar um elemento fundamental para a estabilidade e coesão social e uma componente importante do moderno contrato social. Desde meados dos anos setenta, em consequência de um vasto conjunto de factores sócio-económicos desfavoráveis, os modelos de sistemas públicos de segurança social europeus têm sido sujeitos a um processo de reavaliação crítica pelas sociedades europeias. Entre esses factores desfavoráveis, que afectam, tanto os sistemas públicos, como os complementares, figuram:

- **A Tendência para a Acentuação do Envelhecimento Demográfico**

O envelhecimento da população europeia obriga a acelerar a adaptação dos sistemas de reforma. Simultaneamente, o aumento do número de pessoas muito idosas vem aumentar as necessidades em matéria de cuidados de saúde e de serviços sociais. O desafio futuro consiste na conciliação da satisfação destas necessidades e o controlo dos custos que este apoio social implica.

- **Os Efeitos do Fenómeno do Desemprego e as Alterações no Mercado de Emprego**

O trabalho está a mudar de natureza: tem-se tornado cada vez mais independente, qualificado e variado. O conceito de uma carreira linear, que marcou o século XX, tem vindo a desaparecer progressivamente. Quanto maior for a flexibilidade da vida profissional, mais os cidadãos exigirão apoio ao sistema de protecção social.

- **As Novas Realidades Sociais**

O novo equilíbrio laboral entre os sexos a nível profissional entra em conflito com as políticas familiares tradicionais, sendo necessário encontrar novas fórmulas para, designadamente:

- não penalizar as mulheres que não tiveram uma actividade remunerada;
- facilitar a cobertura às crianças e às pessoas idosas.



Tribunal de Contas

▪ A Necessidade de Adaptar os Modelos Tradicionais de Financiamento da Protecção Social

As despesas de protecção social representam 28% do PIB bruto da União Europeia, compreendidas entre 16% e 35% ⁴ consoante o Estado-Membro. Estas despesas desempenham um papel fundamental na estabilidade política, na coesão social e no progresso económico. Apesar das necessidades fundamentais serem as mesmas, o contexto sócio-económico mudou e a necessidade de adaptar os sistemas é cada vez mais urgente.

Em Portugal, a conta da Segurança Social representa, em 2000, aproximadamente 12% do PIB nacional ⁵ e a sua sustentação apresenta-se, cada vez mais, como um desafio significativo para a economia do país, dado que o sistema público de segurança social tem acumulado várias insuficiências quanto:

- aos níveis de protecção social prestados aos seus cidadãos;
- a défices de equidade quanto ao modo de realização dessa protecção; e
- a défices de eficácia na organização e gestão desse sistema.

Em face da evolução demográfica, social e económica, acima descrita, é cada vez mais urgente gerir o equilíbrio financeiro e melhorar a eficiência e eficácia do sistema público de segurança social a curto, médio e longo prazos, alcançando, simultaneamente, os objectivos de melhoria de protecção, através da actualização de pensões e do melhoramento do poder de compra das mesmas.

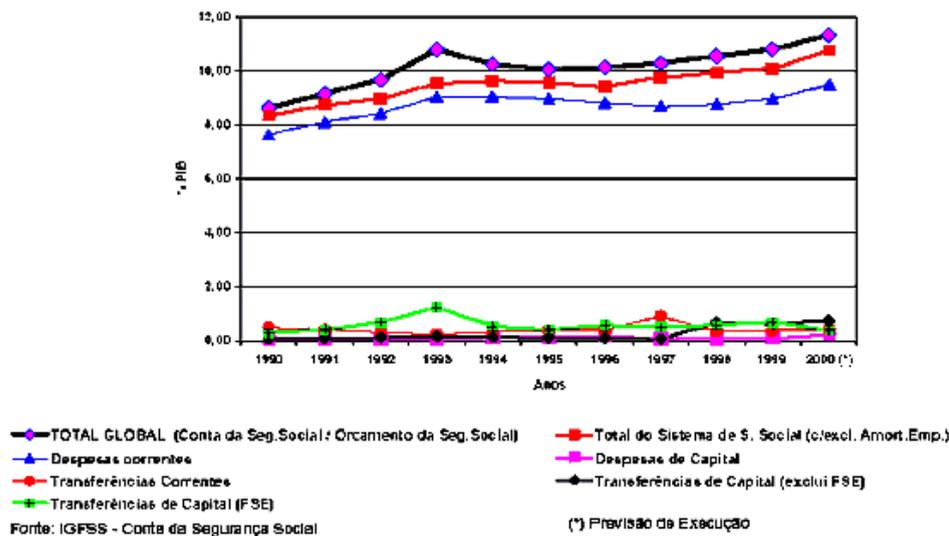
⁴ Fonte: europa.eu.int; não é mencionado o ano de referência.

⁵ Fonte: www.seg-social.pt.



Tribunal de Contas

Gráfico 1- CSS – Despesas e transferências dos Principais Agregados (% PIB) – Continente e RA

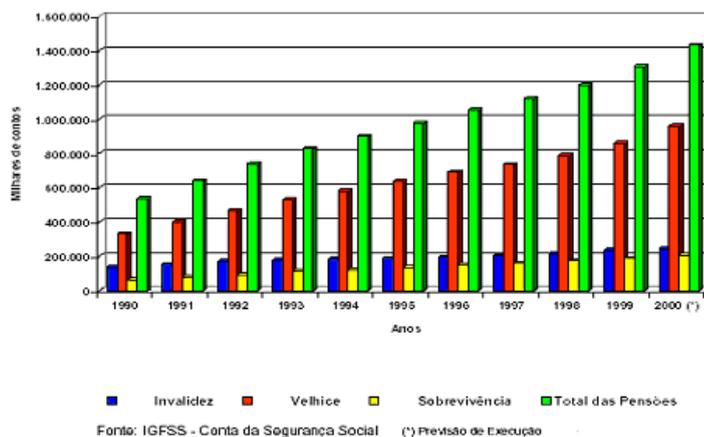


A Lei n.º 17/2000, de 8 de Agosto, veio introduzir na filosofia do sistema de segurança social uma série de transformações que visam a substituição do paradigma assistencialista por um novo modelo de protecção social com o objectivo de promover a *“melhoria das condições e dos níveis de protecção social e o reforço da respectiva equidade”*, a *“eficácia do sistema e a eficiência da sua gestão”* e a *“sustentabilidade financeira (...)”* do Sistema de Solidariedade e Segurança Social (SSSS) cujas despesas sofreram no último decénio um forte crescimento retratado no gráfico seguinte:



Tribunal de Contas

Gráfico 2 - CSS – Despesas com Pensões, Suplementos e Complementos por tipo de modalidade (preços correntes) – Continente e RA



O alcance dos supracitados objectivos, bem como a melhoria dos problemas existentes no sistema público de segurança social, requerem uma melhor gestão dos seus recursos financeiros. A melhoria significativa exigida na gestão dos recursos financeiros existentes e futuros é possível através de um maior e melhor aproveitamento dos sistemas de informação para promover a eficiência dos processos principais do SSSS, bem como uma melhoria da qualidade da informação disponível para gestão da mesma.

Uma maior e melhor informatização do SSSS permitirá:

- uma maior eficiência no atendimento e seu relacionamento com o público;
- uma maior celeridade e capacidade de resposta no tratamento de processos de requerimentos e processamento de pensões;
- uma maior eficiência na sua interligação com outras entidades, como a banca e outras repartições do Estado; e
- uma maior disponibilidade de informação sobre o seu desempenho.

Uma maior disponibilidade de informação inerente aos processos do SSSS contribuirá para:

- melhorar o entendimento existente das capacidades e responsabilidades financeiras do sistema público de segurança social;
- a melhor definição, planeamento e execução de uma estratégia de equilíbrio financeiro do sistema a médio longo prazos;
- suportar as decisões estratégicas do sistema público de segurança social com informação fiável e atempada; e



Tribunal de Contas

- melhorar a fiscalização da recolha de contribuições e do pagamento de benefícios, através da utilização dos sistemas de informação como um dos meios importantes do combate à fraude.

O Estado Português reconhece também esta necessidade, no *Acordo sobre a Modernização da Protecção Social* de Novembro de 2001, que prevê, entre outras medidas:

- *“A melhoria da eficácia de gestão e qualidade do desempenho do sistema de solidariedade e segurança social;*
- *O combate à fraude e evasão contributiva e prestacional; e*
- *Um sistema de informação”.*

IV.2. Enquadramento jurídico das Prestações Diferidas

Relativamente às prestações⁶ propriamente ditas, nas quais se incluem as pensões⁷ de invalidez, velhice e morte, quer do subsistema previdencial, quer do de protecção social de cidadania, elencam-se no quadro seguinte a legislação em vigor, âmbito, condições de atribuição, montante ou cálculo e respectiva duração das mesmas.

⁶ Utilizou-se como base de referência para os termos legais utilizados neste relatório o *Dicionário Técnico e Jurídico de Protecção Social*, de **Ilídio das Neves**, Coimbra Editora, Coimbra, 2001.

⁷ Designa-se por Pensão a prestação pecuniária mensal, de atribuição continuada, a suprir a ausência de rendimentos decorrentes de diversas eventualidades, das quais as mais significativas, em termos de despesa, são a morte (pensão de sobrevivência), a invalidez e a velhice (pensão de velhice).



Tribunal de Contas

Tabela 6 - Prestações Diferidas – Enquadramento Jurídico

Prestações/ Legislação em vigor	Destinatários /Âmbito	Condições de atribuição	Montante ou Cálculo	Duração
<p>Complemento social*</p> <ul style="list-style-type: none"> DL n.º 329/93, de 25 de Setembro 	<ul style="list-style-type: none"> Beneficiários cuja pensão estatutária se situa abaixo do montante garantido 	<ul style="list-style-type: none"> Sem condições de recurso 	<ul style="list-style-type: none"> Valor necessário para perfazer o montante mínimo garantido 	<ul style="list-style-type: none"> Mensal
<p>Pensão de invalidez</p> <ul style="list-style-type: none"> DL n.º 329/93, de 25 de Setembro; Portaria n.º 272/98, de 29 de Abril 	<ul style="list-style-type: none"> Trabalhadores por conta de outrem; Trabalhadores independentes; Clero. 	<ul style="list-style-type: none"> Situação de incapacidade permanente física ou mental¹ de causa não profissional, determinante da impossibilidade de auferir na sua profissão mais de 1/3 da remuneração correspondente ao exercício normal. Prazo de garantia: ** Em formação: 5 anos civis seguidos ou interpolados com registo de remunerações superiores a 120 dias; ou 1095 dias de doença. 	<p>Fórmula de cálculo: $P=(2/100xn) \times RR$.</p> <p>Assim a pensão é igual ao produto da</p> <ul style="list-style-type: none"> Taxa Global (2/100xn), i e, 2% (taxa anual) vezes o número de anos com 120 dias com remunerações, no mínimo de 30% e máximo de 80% pela Remuneração de referência (RR) (R 10/14X10) – remunerações dos melhores 10 anos dos 15 últimos revalorizados e divididos por 140. 	<p>14 prestações mensais no ano</p> <ul style="list-style-type: none"> Até ao termo da incapacidade, ou Até à convalidação em pensão de velhice (na idade de reforma por velhice)
<ul style="list-style-type: none"> DL n.º 40/89, de 1 de Fevereiro 	<ul style="list-style-type: none"> Seguro social voluntário 	<p>Prazo de garantia:</p> <ul style="list-style-type: none"> 72 meses de contribuições 	<ul style="list-style-type: none"> Valores fixos para grupos especiais de beneficiários (ex: agrícolas ***) 	
<ul style="list-style-type: none"> Lei 1/89, de 31 de Janeiro; Dec. Regulamentar n.º 25/90, de 9 de Agosto 	<ul style="list-style-type: none"> Trabalhadores com paramiloidose e doença do Machado 	<p>Prazo de garantia:</p> <ul style="list-style-type: none"> 36 meses de contribuições 	<ul style="list-style-type: none"> taxa de formação de pensões: 3%; Remuneração de referência: S/36 	
<p>Pensão de orfandade*</p> <ul style="list-style-type: none"> DL n.º 160/80, de 27 de Maio; Dec. Regulamentar n.º 71/80, de 12 de Novembro 	<ul style="list-style-type: none"> Órfãos até à maioridade ou emancipação 	<p>Condição de recurso:</p> <p>Rendimento <i>per capita</i> de 40% da rmm (remuneração mínima nacional) geral com o limite máximo para o agregado familiar de 1 vez e meia aquela remuneração</p>	<ul style="list-style-type: none"> 20, 30 ou 40% da pensão social fixada anualmente conforme se trate de 1, 2 ou mais órfãos de pai ou mãe. 14 prestações anuais. 	<ul style="list-style-type: none"> Mensal

¹ Presume-se que não recuperará dentro de 3 anos subsequentes a capacidade de auferir, no desempenho da profissão, mais de 1/3 da remuneração correspondente ao seu exercício normal;

* Prestação do regime não contributivo;

** Prazos de garantia cumpridos:

✓ Até 12/73: 5 anos de inscrição e 30 meses de contribuições ou 5 anos de contribuições;

✓ Até 12/79: 3 anos de inscrição e 24 meses de contribuições;

✓ Até 9/84: 36 meses de contribuições;

✓ Até 12/93: 60 meses de contribuições.

*** 29 550\$00 (desde Dezembro de 2000)



Tribunal de Contas



Tribunal de Contas

Prestações/ Legislação em vigor	Destinatários /Âmbito	Condições de atribuição	Montante ou Cálculo	Duração
<p>Pensão de sobrevivência</p> <ul style="list-style-type: none"> DL n.º 322/90, de 18 de Outubro; Dec. Regulamentar n.º 1/94, de 18 de Janeiro 	<ul style="list-style-type: none"> Cônjuges e ex -cônjuges com direito a alimentos; União de facto há mais de 2 anos titulares de direito a alimentos; Descendentes ou equiparados. <p>Na falta destes:</p> <ul style="list-style-type: none"> Ascendentes a cargo; Parentes, afins e equiparados em linha recta e até ao 3.º grau em linha colateral a cargo 	<ul style="list-style-type: none"> 36 meses de contribuições 	<ul style="list-style-type: none"> Cônjuge ou ex -cônjuge : 60 ou 70% (se for 1 ou mais) da pensão do beneficiário; Filhos adoptados plenamente: 20, 30 ou 40% se se tratar de 1, 2 ou mais com cônjuge ou ex -cônjuge com direito e o dobro daquela percentagem sem cônjuge; Outros parentes a cargo na falta de cônjuge ou filhos: 30, 50 ou 80%, conforme forem 1, 2 ou mais. 	<p>Cônjuges e ex -cônjuges:</p> <ul style="list-style-type: none"> Com mais de 34 anos: sem limite; Com 34 anos ou menos: durante 5 anos: excepto com filhos a cargo ou invalidez. <p>Descendentes:</p> <ul style="list-style-type: none"> Até aos 18 anos: sem condições; Dos 18 aos 25: curso secundário ou superior; Até aos 27: mestrado, pós-graduação e estágio.
<p>Pensão Social*</p> <ul style="list-style-type: none"> DL n.º 160/80, de 27 de Maio; DL n.º 464/80, de 13 de Outubro; Portaria 1141-A/2000, de 30 de Novembro 	<ul style="list-style-type: none"> Residentes nacionais não abrangidos por regimes contributivos. 	<p>Condição de recursos:</p> <ul style="list-style-type: none"> rendimentos iguais ou inferiores a 30% da rmm (remuneração mínima nacional) ou 50%, tratando-se de casal; 65 anos para a velhice; a partir dos 18 anos em caso de invalidez para toda e qualquer profissão. 	<p>Geral:*****</p> <ul style="list-style-type: none"> 26.250\$00 mensais; Invalidez na paramiloidose (e doença do machado): 36.000\$00; 14 prestações mensais. 	<ul style="list-style-type: none"> Mensal
<p>Pensão de Velhice</p> <ul style="list-style-type: none"> Portaria de 18 de Dezembro de 1975; Dec. Regulamentar n.º 40/86, de 12 de Setembro; DL n.º 392/90, de 10 de Dezembro; DL n.º 195/95, de 28 de Julho; DL n.º 329/93, de 25 de Setembro; Portaria n.º 272/98, de 29 de Abril 	<ul style="list-style-type: none"> Trabalhadores por conta de outrem ; Trabalhadores independentes; Trabalhadores agrícolas; Clero. 	<p>Prazo de garantia:</p> <p>Em formação:** 15 anos civis seguidos ou interpolados com registo de remunerações igual ou superior a 120 dias.***</p> <p>Idade legal de reforma:</p> <ul style="list-style-type: none"> 65 anos – geral; 50 anos – mineiros; 50 ou 55 – pescadores; 55 – comercio de longo curso; 55 ou 60 – desempregados; 60 – pilotos da aviação civil; <p>Idade antecipada convencionalmente para os beneficiários que o requeiram.</p>	<p>Fórmula de Cálculo:</p> $P = (2/100 \times n) \times RR.$ <p>Assim a pensão é igual ao produto da</p> <ul style="list-style-type: none"> Taxa Global (2/100 x n), i e, 2% (taxa anual) vezes o número de anos com 120 dias com remunerações, no mínimo de 30% e no máximo de 80%, pelas Remunerações de Referência (RR) (R 10/14 x 10) – remunerações dos melhores 10 anos dos 15 últimos revalorizados e divididos por 140; Valores fixos para grupos especiais de beneficiários (ex: agrícolas****) 	<ul style="list-style-type: none"> Mensal

* Só previsto no regime não contributivo;

** Prazos de garantia cumpridos:

✓ Até 12/73: 10 anos de inscrição e 60 meses de contribuições ou 10 anos civis de contribuições;



Tribunal de Contas

- ✓ Até 12/79: 3 anos de inscrição e 24 meses de contribuições;
 - ✓ Até 9/87: 60 meses de contribuições;
 - ✓ Até 12/93: 120 meses de contribuições.
- *** Para o seguro social voluntário: 144 meses;
- **** Desde Dezembro de 2000: 29.550\$00. em Julho de 2001: 32.300\$00;
- ***** Desde Dezembro de 2000. Em Julho 2001: com 70 anos ou mais: 31.250\$00; com menos de 70 anos: 28.750\$00



Tribunal de Contas

Prestações/ Legislação em vigor	Destinatários /Âmbito	Condições de atribuição	Montante ou Cálculo	Duração
Pensão de Viuvez* <ul style="list-style-type: none">• Dec. Regulamentar n.º 52/81, de 11 de Novembro;• Dec. Regulamentar n.º 92-B/94, de 28 de Dezembro	<ul style="list-style-type: none">• Cônjuge Sobrevivo (ou união de facto) que por si não tenha direito a qualquer pensão;	Condição de recursos: Rendimentos iguais ou inferiores a 30% da rmm (remuneração mínima nacional)	•60% da pensão social (15.750\$00)	•Mensal
Prestação do Rendimento Mínimo *; ** <ul style="list-style-type: none">• Lei n.º 19-A/96, de 29 de Junho;• DL n.º 164-A/97, de 27 de Junho;• DL n.º 196/97, de 31 de Julho	Maiores; Menores: <ul style="list-style-type: none">• grávidas;• com outros menores a cargo.	<ul style="list-style-type: none">• Residência em Portugal;• Condição de recursos:<ul style="list-style-type: none">✓ 100% da pensão social por cada maior até ao 2.º;✓ 70% da pensão social por cada maior além do 2.º;✓ 50% da pensão social por cada menor.	Diferença entre: <ul style="list-style-type: none">• o rendimento mínimo do agregado nos termos da condição de recurso e• o rendimento do agregado	•12 meses renováveis
Subsídio por morte <ul style="list-style-type: none">• DL n.º 322/90, de 18 de Outubro;• Dec. Regulamentar n.º 1/94, de 18 de Janeiro	<ul style="list-style-type: none">• Cônjuges e ex-cônjuges;• União de facto ;• Descendentes ou equiparados;• Na falta destes: ascendentes a cargo; parentes, afins e equiparados em linha recta e até ao 3.º grau da linha colateral a cargo.	Condição de recursos: Para os ascendentes, parentes, afins e equiparados em linha recta e até ao 3.º grau da linha colateral a cargo: Rendimento não superior à pensão social	<ul style="list-style-type: none">• 6 vezes a remuneração de referência, considerando-se para base de cálculo os 2 melhores anos civis dos últimos 5 sendo a remuneração de referência igual a 1/24 desse valor.• Por inteiro ao cônjuge ou aos descendentes; e• ½ se houver uns e outros.	•Prestação única

* Só previsto no regime não contributivo;

** Pode adicionar compensação pelas despesas de habitação



Tribunal de Contas

IV.3. Dados Físicos, Financeiros e de Gestão das Prestações Relativas a Pensões

IV.3.1. Dados Físicos

O Quadro I apresenta a evolução dos dados físicos no triénio 1998-2000, relativamente à população abrangida pelos vários regimes de pensões:

Quadro I - Evolução da População por Regime

(em milhares)

Regimes	1998	1999	2000	Variação	
				1998/99	1999/2000
Regime Geral	1.810	1.863	1.928	2,9	3,5
Sobrevivência	475	490	504	3,2	2,9
Invalidez	307	311	301	1,3	(3,2)
Velhice	1.028	1.062	1.123	3,3	5,7
RESSAA	498	466	446	(6,4)	(4,3)
Sobrevivência	93	91	92	(2,2)	1,1
Invalidez	41	36	22	(12,2)	(38,9)
Velhice	364	339	332	(6,9)	(2,1)
RNCE	123	112	106	(8,9)	(5,4)
Sobrevivência	4	4	3	0,0	(25,0)
Invalidez	50	46	47	(8,0)	2,2
Velhice	69	62	56	(10,1)	(9,7)
Totais	2.431	2.441	2.480	0,4	1,6

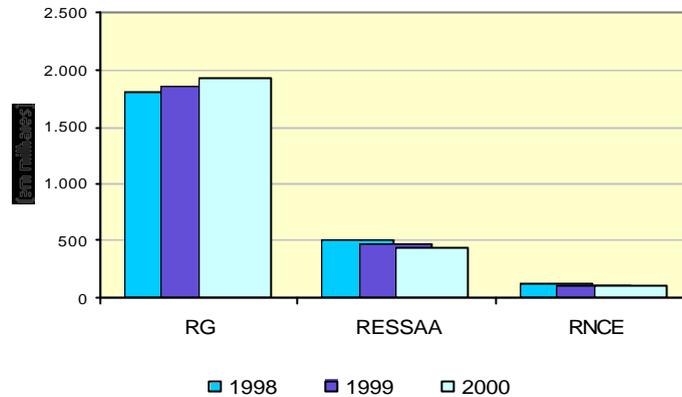
Fonte: CSS/99 e Boletim Estatístico do IIES

A expressão gráfica dos dados reflectidos no quadro anterior é a seguinte:



Tribunal de Contas

Gráfico 3 - Evolução da População por Regime



Como se pode observar, os pensionistas do Regime Geral são largamente maioritários, representando, em 2000, cerca de 77,7% do universo e, contrariamente ao que acontece com os dois outros regimes, apresentam uma dinâmica de crescimento positiva, tendo até, relativamente a 1999, acelerado esse crescimento.

IV.3.2. Dados Financeiros

Relativamente aos dados financeiros, o Quadro II mostra as despesas efectuadas no triénio 1998/2000:



Tribunal de Contas

Quadro II - Evolução das Pensões de Reforma por Regimes e Eventualidades

(em milhares de contos)

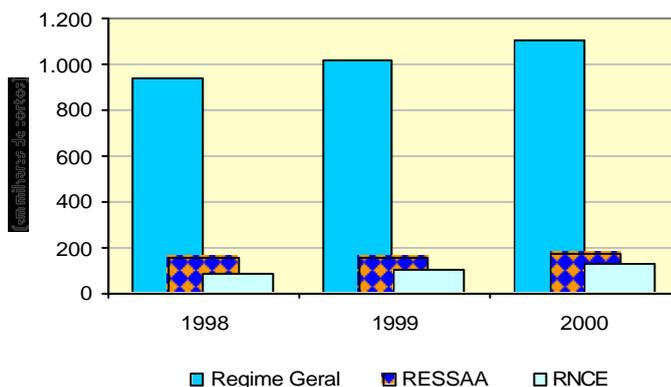
	Eventualidades	1998	%	1999	%	2000	%	1998/99	%	1999/2000	%
Regime Geral	Sobrevivência	152.955	13,0	166.349	13,0	180.632	12,9	13.394	8,8	14.283	8,6
	Invalidez	171.596	14,6	183.992	14,4	188.102	13,4	12.396	7,2	4.110	2,2
	Velhice	605.528	51,4	665.405	52,0	740.891	52,7	59.877	9,9	75.486	11,3
	Subtotal	930.079	79,0	1.015.746	79,3	* 1.109.625	79,0	85.667	9,2	93.879	9,2
RESSAA	Sobrevivência	17.089	1,5	18.118	1,4	20.118	1,4	1.029	6,0	2.000	11,0
	Invalidez	14.978	1,3	14.558	1,1	12.991	0,9	(420)	(2,8)	(1.567)	(10,8)
	Velhice	127.971	10,9	127.227	9,9	136.436	9,7	(744)	(0,6)	9.209	7,2
	Subtotal	160.038	13,6	159.903	12,5	169.545	12,1	(135)	(0,1)	9.642	6,0
RNCE	Sobrevivência	3.404	0,3	4.604	0,4	6.042	0,4	1.200	35,3	1.438	31,2
	Invalidez	29.134	2,5	35.002	2,7	40.498	2,9	5.868	20,1	5.496	15,7
	Velhice	54.856	4,7	65.315	5,1	79.400	5,7	10.459	19,1	14.085	21,6
	Subtotal	87.394	7,4	104.921	8,2	125.940	9,0	17.527	20,1	21.019	20,0
Totais	1.177.511	100,0	1.280.570	100,0	1.405.110	100,0	103.059	8,8	124.540	9,7	

Fonte: IGFSS

* - Este valor difere do constante na Conta Geral do Estado (1.109.610), mencionado no capítulo XII do Parecer do Tribunal de Contas sobre a CGE/2000 – designadamente no quadro XII.41 –, sendo aqui utilizado dado ser a única desagregação, por eventualidades, existente.

Graficamente:

Gráfico 4 - Evolução dos gastos com Pensões, por Regime





Tribunal de Contas

Relativamente aos dados financeiros expostos no quadro anterior salienta-se o seguinte:

- **As pensões afectas ao regime geral representam 79 % do total dos gastos com estas prestações**, tendo-se registado, no seu crescimento relativo, uma estagnação de 1999 para 2000;
- As pensões do RESSAA denotaram, em 2000, um crescimento de 6%, contrariando a tendência anteriormente registada;
- Finalmente, no que respeita ao RNCE, onde se inclui o *Complemento Social*, verificou-se, em 2000, relativamente a 1999, um aumento de cerca de 20% no total das despesas com este regime.

IV.3.3. Indicadores de Gestão

Apresenta-se, de seguida, alguns elementos informativos, recolhidos a partir dos relatórios internos de acompanhamento, produzidos pela Unidade de Organização Planeamento e Gestão, desenvolvidos com o objectivo de se obter uma imagem sobre a dimensão e evolução procedimental das actividades do CNP.

O conjunto de quadros e gráficos abaixo expostos relacionam os processos⁸ entrados, concluídos e pendentes, em termos de volume físico anual e média mensal e tempos médios de execução, discriminados de acordo com as áreas e eventualidades inerentes ao regime de segurança social em apreço, que subjazem à organização de tarefas e distribuição de responsabilidades dentro do CNP.

Os dados relativos ao número de processos entrados encontram-se sintetizados na tabela infra:

⁸ Trata-se aqui de processos administrativos, não devendo confundir-se com os processos de natureza informática ou organizacional mais adiante referidos no presente relatório.



Tribunal de Contas

Quadro III - Processos Entrados

Áreas	N.º de processos			Média mensal		
	1998	1999*	2000	1998	1999	2000
Nacional e Internacional	176.611	199.667	190.637	14.718	16.639	15.886
P. Invalidez	57.151	62.309	52.004	4.763	5.192	4.334
P. Velhice	36.188	49.797	55.812	3.016	4.150	4.651
P. Sobrevivência**	43.030	44.154	42.002	3.586	3.680	3.500
Despesas de funeral	40.242	43.407	40.819	3.354	3.617	3.402
Nacional	153.564	173.597	166.000	12.797	14.466	13.833
P. Invalidez	48.364	52.184	43.708	4.030	4.349	3.642
P. Velhice	26.978	39.193	44.907	2.248	3.266	3.742
P. Sobrevivência**	38.738	39.691	37.441	3.228	3.308	3.120
Despesas de funeral	39.484	42.529	39.944	3.290	3.544	3.329
Internacional	23.047	26.070	24.637	1.921	2.173	2.053
P. Invalidez	8.787	10.125	8.296	732	844	691
P. Velhice	9.210	10.604	10.905	768	884	909
P. Sobrevivência**	4.292	4.463	4.561	358	372	380
Despesas de funeral	758	878	875	63	73	73

* Os dados disponibilizados, relativos ao ano de 1999, inseridos nos relatórios de 2000 e 1999, apresentam contradições.

** Integra o subsídio por morte.

Fonte: Centro Nacional de Pensões – UOPG (ex-DSOPG/DPG).

O número de processos entrados revela um comportamento oscilatório ao longo do triénio. Depois de um acréscimo, de 1998 para 1999, na ordem dos 23.000 processos, em 2000 o número de processos entrados baixou para um volume total à volta das 190.000 unidades. Este tipo de dinâmica reflecte-se em quase todos os elementos desagregados, com excepção da pensão de velhice que revelou um crescimento, embora em desaceleração, ao longo do período (no agregado nacional e internacional, a pensão de velhice cresceu, em 1999 e 2000, 37,6% e 12,1% respectivamente).

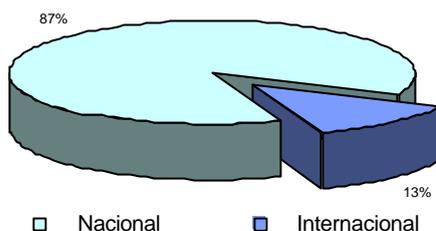
Registe-se, igualmente, a evolução da posição relativa do volume dos processos por eventualidade. A pensão de velhice que, no agregado nacional e internacional, em 1998, ocupava a última posição (20,5% dos processos entrados), inverteu, em 2000, essa posição, passando a liderar o número de processos entrados, com 29,3% do volume global, sobretudo em detrimento da pensão de sobrevivência.



Tribunal de Contas

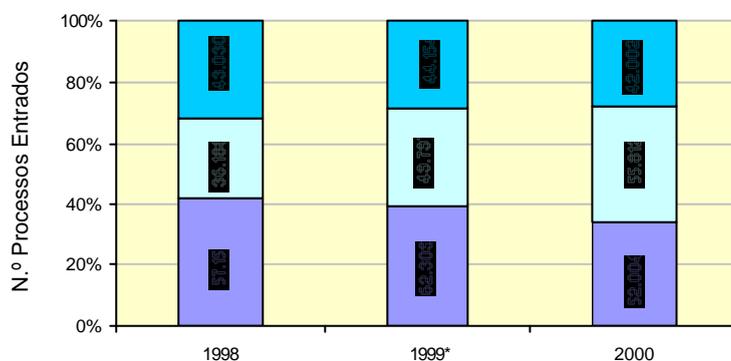
Os processos com origem no território nacional são largamente majoritários, representando cerca de 87% do total dos requerimentos entrados no CNP. O gráfico abaixo demonstra a distribuição dos processos entrados por origem:

Gráfico 5 - Processos entrados no CNP em 2000



A expressão gráfica da distribuição dos processos entrados da área nacional por tipo de eventualidade é a seguinte:

Gráfico 6 - Processos da Área Nacional



* Os dados disponibilizados, relativos ao ano de 1999, inseridos nos relatórios de 2000 e 1999, apresentam contradições

■ P.Invalidez □ P.Velhice ■ P.Sobrevivência

Corroborando a tendência atrás constatada, relativa ao cúmulo nacional e internacional, também no âmbito restrito à área nacional é notório o ganho de importância relativa, em volume, das pensões de velhice, ao longo do período, com ganho da liderança no número de processos entrados e, paralelamente, a perda de posição dominante da pensão de sobrevivência.

Relativamente aos processos concluídos no triénio 1998/2000 e a respectiva média mensal, veja-se o quadro seguinte:



Tribunal de Contas

Quadro IV - Processos Concluídos

Áreas	N.º de processos			Média mensal		
	1998	1999*	2000	1998	1999	2000
Nacional e Internacional	177.024	190.153	192.902	14.752	15.846	16.075
P. Invalidez	57.427	58.649	54.079	4.786	4.887	4.507
P. Velhice	36.533	44.785	57.772	3.044	3.732	4.814
P. Sobrevivência*	42.890	43.525	41.117	3.574	3.627	3.426
Despesas de funeral	40.174	43.194	39.934	3.348	3.600	3.328
Nacional	154.546	166.423	168.102	12.879	13.869	14.009
P. Invalidez	48.918	49.633	45.559	4.077	4.136	3.797
P. Velhice	27.292	35.450	46.730	2.274	2.954	3.894
P. Sobrevivência*	38.861	39.029	36.736	3.238	3.252	3.061
Despesas de funeral	39.475	42.311	39.077	3.290	3.526	3.256
Internacional	22.478	23.730	24.800	1.873	1.978	2.067
P. Invalidez	8.509	9.016	8.520	709	751	710
P. Velhice	9.241	9.335	11.042	770	778	920
P. Sobrevivência*	4.029	4.496	4.381	336	375	365
Despesas de funeral	699	883	857	58	74	71

* Os dados disponibilizados, relativos ao ano de 1999, inseridos nos relatórios de 2000 e 1999, apresentam contradições.

** Integra o subsídio por morte.

Fonte: Centro Nacional de Pensões – UOPG (ex-DSOPG/DPG).

Destaca-se dos dados observados, o crescimento constante ao longo do triénio do volume de processos concluídos – 7,4%, de 1998 para 1999 e 1,5%, de 1999 para 2000. Recorde-se que, relativamente aos processos entrados, havia-se registado oscilações ao longo do período.

Verifica-se também uma alteração da posição relativa das diferentes prestações no período. Em 2000 (1998) a proporção das diferentes eventualidades, nos agregados nacional e internacional, era a seguinte: invalidez 28,03% (32,44%), velhice 29,95% (20,64%), sobrevivência 21,31% (24,23%) e despesas de funeral 20,7% (22,69%).

Confrontando os dados do quadro em análise com os relativos aos processos entrados, verifica-se que o índice de cobertura⁹ dos processos concluídos em relação aos entrados, em termos globais, foi, ao longo do triénio, muito elevado, situando-se próximo da unidade. Não obstante, de 1998 para 1999 houve uma ligeira quebra deste indicador, de 1 para 0,95; enquanto em

⁹ Índice de cobertura = n.º processos concluídos/n.º processos entrados.



Tribunal de Contas

2000 o índice passou para o valor de 1,01, o que revela, para este último ano, um ganho de eficiência na produção.

A quebra no índice de cobertura em 1999 verificou-se, sobretudo, tendo em conta os valores agregados das áreas nacional e internacional, nas eventualidades velhice e invalidez, com valores, respectivamente, de 0,90 e 0,94. E, procedendo-se à sua desagregação por áreas, os valores mais baixos registaram-se também naquelas eventualidades mas na área internacional, atingindo, respectivamente, leituras de 0,88 e 0,89; enquanto que na área internacional os valores replicaram o índice agregado.

Relativamente aos dados dos processos entrados e ainda não concluídos, veja-se os quadros abaixo:

Quadro V - Processos Pendentes por Eventualidade

Áreas	N.º de processos			Variação (%)	
	Dez-98	Dez-99	Dez-00	1999/1998	2000/1999
Nacional e Internacional	46.827	52.674	51.236	12,5	(2,7)
P. Invalidez	31.059	31.205	29.948	0,5	(4,0)
P. Velhice	9.232	15.668	13.092	69,7	(16,4)
P. Sobrevivência*	6.536	5.801	8.196	(11,2)	41,3
Nacional	36.347	42.247	40.942	16,2	(3,1)
P. Invalidez	24.394	25.060	23.971	2,7	(4,3)
P. Velhice	6.300	12.185	9.747	93,4	(20,0)
P. Sobrevivência*	5.653	5.002	7.224	(11,5)	44,4
Internacional	10.480	10.427	10.294	(0,5)	(1,3)
P. Invalidez	6.665	6.145	5.977	(7,8)	(2,7)
P. Velhice	2.932	3.483	3.345	18,8	(4,0)
P. Sobrevivência*	883	799	972	(9,5)	21,7

* Os dados disponibilizados, relativos ao ano de 1999, inseridos nos relatórios de 2000 e 1999, apresentam contradições.

** Integra o subsídio por morte.

Fonte: Centro Nacional de Pensões – UOPG (ex-DSOPG/DPG)

Em relação aos processos pendentes e sua evolução no triénio, verifica-se que, após um andamento negativo de 1998 para 1999 (os pendentes cresceram 12,5%), se procedeu a uma ligeira recuperação em 2000, decréscimo nos pendentes em 2,7%. O crescimento dos processos pendentes, em 1999, foi mais significativo no conjunto da área nacional, com destaque para a pensão de velhice (+93,4%).

A melhoria registada em 2000 deriva sobretudo da recuperação entretanto efectuada nos pendentes referentes à pensão de velhice (-20% na área nacional). Esta tendência positiva, embora



Tribunal de Contas

embora seja generalizada a quase todas as eventualidades, não abarcou a pensão de sobrevivência, onde se constatou um acréscimo significativo de pendentes de 41,3%.

Para se obter uma imagem mais detalhada das pendências apresenta-se, no quadro seguinte, a decomposição dos processos pendentes por fases de tramitação, a saber: nos CDSSS, em trânsito e no CNP.

Quadro VI - Processos Pendentes por Fase de Tramitação

Nacional e Internacional	N.º de processos			Variação (%)	
	Dez-98	Dez-99	Dez-00	1999/1998	2000/1999
Nos CDSSS	21.834	21.745	20.955	(0,4)	(3,6)
P. Invalidez	16.634	15.385	15.652	(7,5)	1,7
P. Velhice	3.363	5.335	4.369	58,6	(18,1)
P. Sobrevivência/Desp. Funeral	1.837	1.025	934	(44,2)	(8,9)
Em Trânsito	3.102	3.413	5.030	10,0	47,4
P. Invalidez	1.084	1.018	1.569	(6,1)	54,1
P. Velhice	600	943	1.293	57,2	37,1
P. Sobrevivência/Desp. Funeral	1.418	1.452	2.168	2,4	49,3
No CNP	21.891	27.516	25.251	25,7	(8,2)
P. Invalidez	13.341	14.802	12.727	11,0	(14,0)
P. Velhice	5.269	9.390	7.430	78,2	(20,9)
P. Sobrevivência/Desp. Funeral	3.281	3.324	5.094	1,3	53,2
Total	46.827	52.674	51.236		

Fonte: Centro Nacional de Pensões

Conforme resulta da leitura dos dados observados, pode-se ainda precisar que:

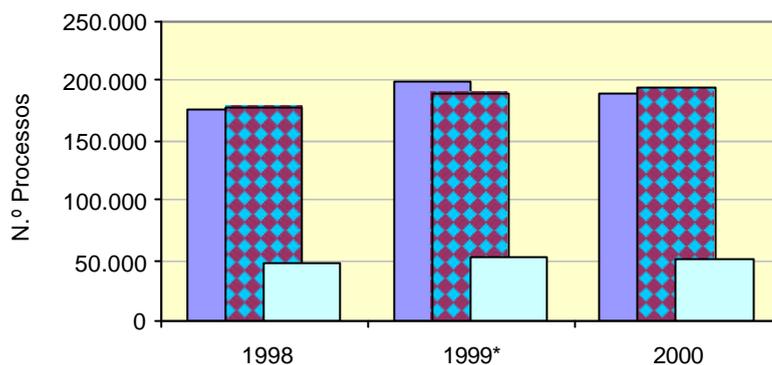
- Para a evolução verificada em 1999, que tinha na pensão de velhice o seu elemento principal, contribuíram os atrasos verificados ao longo das diferentes fases da tramitação, assim:
 - nos CDSSS: (+58,6%);
 - em trânsito: (+57,2%); e
 - no CNP: (+78,2%).
- Em relação à melhoria constatada em 2000, que teve também na pensão de velhice o elemento com melhores valores, constata-se que aquela se deveu principalmente a melhores desempenhos nos CDSSS (-18,1%) e no CNP (-20,9%), apesar da regressão em relação à fase de trânsito (+37,1%).



Tribunal de Contas

Para uma melhor percepção das correlações que se estabelecem entre os três grupos de dados analisados – processos entrados, concluídos e pendentes – apresenta-se, como síntese, o Gráfico 7 que ilustra a evolução em paralelo daqueles três universos ao longo do triénio.

Gráfico 7 - Processos Nacionais e Internacionais Agregados



* Os dados disponibilizados, relativos ao ano de 1999, inseridos nos relatórios de 2000 e 1999, apresentam contradições

■ Proc. Entrados ■ Proc. Concluídos □ Proc. Pendentes

Na imagem gerada são perfeitamente perceptíveis as considerações anteriormente expostas, constatando-se que:

- o número de processos entrados apresentou um crescimento de 1998 para 1999, invertendo-se essa tendência em 2000;
- os processos concluídos cobriam, em 1998, os processos entrados. Em 1999, o índice de cobertura ficou abaixo da unidade, para, em 2000, a superar ligeiramente;
- os processos pendentes, em 1999, apresentaram um crescimento com algum significado, verificando-se, em 2000, uma ligeira descida dos mesmos.

Em relação a este último ponto é importante fazer uma observação final. Assim, apesar dos processos pendentes, em volume, demonstrarem um comportamento oscilatório, a sua relação com o número de processos entrados manteve-se praticamente constante ao longo do período, apresentando valores na casa dos 26%.



Tribunal de Contas

Um outro parâmetro importante acerca dos processos que correm junto do CNP é o tempo de execução dos mesmos. O quadro abaixo reflecte os tempos médios observados pelos processos concluídos.



Tribunal de Contas

Quadro VII - Tempo Médio dos Processos Concluídos

(em meses)

Nacional e Internacional		Períodos Homólogos				
		Dez-98	Dez-99	Dez-00	Variação (%)	
					1999/1998	2000/1999
Nacional	Invalidez	7,1	7,4	7,7	4,2	4,1
	Nos CRSS	4,8	5,0	5,1	4,2	2,0
	Em Trânsito	0,2	0,2	0,3	0,0	50,0
	No CNP	2,1	2,2	2,3	4,8	4,5
	Velhice	3,5	3,8	4,1	8,6	7,9
	Nos CRSS	2,3	2,4	2,6	4,3	8,3
	Em Trânsito	0,2	0,2	0,2	0,0	0,0
	No CNP	1,0	1,2	1,3	20,0	8,3
	Sobrevivência e Morte	2,0	2,3	2,7	15,0	17,4
	Nos CRSS	1,1	1,2	1,4	9,1	16,7
	Em Trânsito	0,3	0,3	0,2	0,0	(33,3)
	No CNP	0,6	0,8	1,1	33,3	37,5
Internacional	Invalidez	12,5	12,8	12,2	2,4	(4,7)
	Velhice	5,8	5,9	6,5	1,7	10,2
	Sobrevivência e Morte	4,3	5,2	5,9	20,9	13,5

Fonte: Centro Nacional de Pensões

Da leitura dos elementos inseridos na tabela, constata-se que:

- os processos da área internacional são, em média, mais morosos que os da área nacional;
- o ordenamento decrescente das eventualidades, por tempo médio necessário para a conclusão de um processo, é o seguinte: invalidez, velhice e sobrevivência e morte;
- em regra, a comparação dos tempos médios de execução, dentro de um período homólogo ao longo do triénio, indicia que o tempo de execução necessário tem-se alargado; e que, na área nacional, o crescimento do tempo médio necessário, foi mais acentuado nas prestações de sobrevivência e morte e invalidez;
- na área nacional, o maior consumo do tempo médio despendido, regista-se nos CDSSS – sempre acima dos 50% do tempo global de execução;



Tribunal de Contas

- em relação à área nacional, o crescimento do tempo médio de execução necessário, ao longo do período em análise, ocorrido no CNP, foi maior que a média de crescimento total.

IV.4. Instituições do Sistema de Solidariedade e Segurança Social

A organização institucional do Sistema de Solidariedade e Segurança Social (SSSS), assenta nos seguintes institutos de âmbito nacional, alguns dos quais dispõem de delegações regionais e distritais:

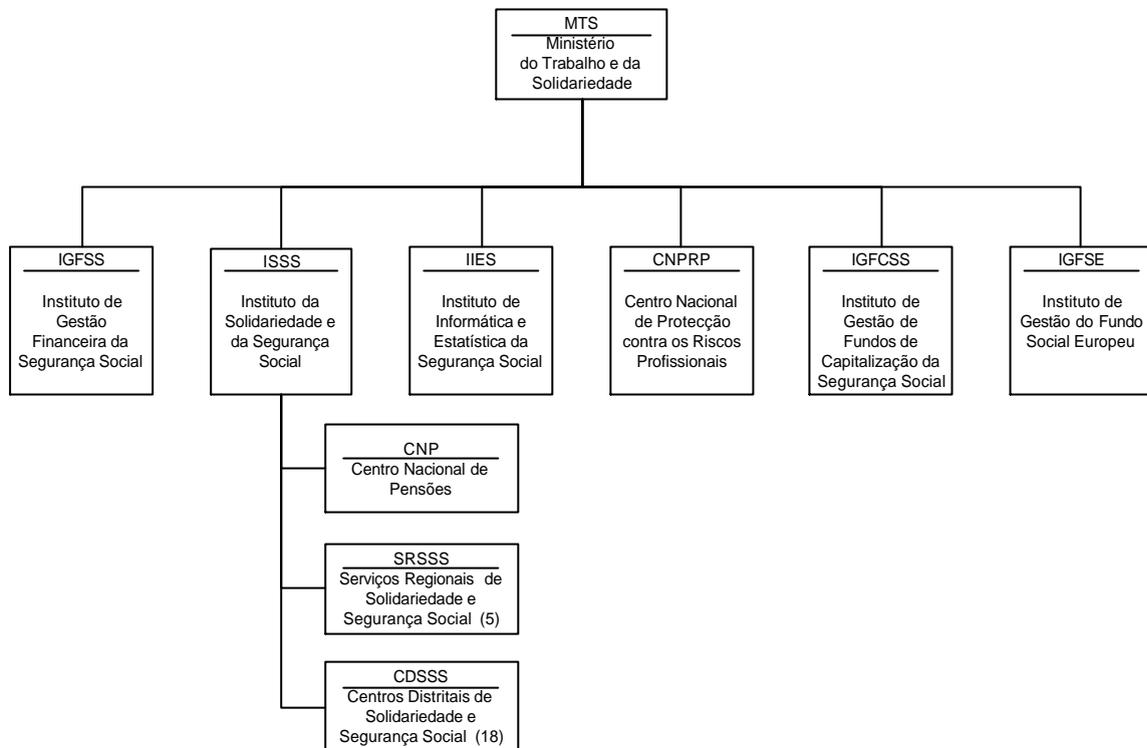
- **Instituto de Gestão Financeira da Segurança Social (IGFSS)**, ao qual compete a gestão financeira unificada dos recursos económicos consignados no orçamento da segurança social;
- **Instituto de Solidariedade e Segurança Social (ISSS)**, que tem por objectivo a gestão das prestações do SSSS;
- **Instituto de Informática e Estatística da Solidariedade (IIES)**, ao qual cabem a concepção, definição, implementação e avaliação do sistema de informação nas áreas de solidariedade e segurança social, bem como as políticas de informática e estatística;
- **Centro Nacional de Prevenção contra os Riscos Profissionais (CNPRP)**, tendo como objectivo desenvolver actividades nos domínios da prevenção, tratamento, reparação e recuperação de doenças ou incapacidades resultantes de riscos profissionais;
- **Instituto de Gestão de Fundos de Capitalização da Segurança Social**, com o objectivo da gestão de fundos de capitalização;
- **Instituto de Gestão do Fundo Social Europeu**, responsável pela gestão nacional do Fundo Social Europeu.

Em termos de organigrama, esta organização institucional apresenta-se como segue:



Tribunal de Contas

O SISTEMA DE SOLIDARIEDADE E SEGURANÇA SOCIAL



Nos termos do Decreto-Lei n.º 45-A/2000, de 22 de Março, o Instituto da Solidariedade e Segurança Social (ISSS) agregou, em matéria de prestações, as atribuições e competências cometidas anteriormente às instituições de âmbito regional e distrital (CRSS – Centros Regionais de Solidariedade e Segurança Social e SSR – Serviços Sub-Regionais) e, também, ao Centro Nacional de Pensões (CNP). Dos seis institutos acima mencionados, os primeiros quatro são os que se encontram mais directamente envolvidos no sistema que suporta a atribuição e controlo de pensões. Porém, considerando que o CNPRP foi já objecto de auditoria autónoma por parte do Tribunal de Contas¹⁰, bem como as particularidades das prestações por cuja atribuição é responsável, optou-se por excluir este Centro da presente auditoria.

¹⁰ Veja-se o Relatório n.º 57/01-2ªS, disponível para consulta em www.tcontas.pt.



Tribunal de Contas

V. PROCESSOS E SISTEMAS DE ATRIBUIÇÃO E CONTROLO DE PENSÕES

V.1. Identificação dos Processos

Os processos principais do SSSS foram identificados e levantados através de entrevistas com os responsáveis dos vários Serviços e Unidades do CNP, CDSSS, IGFSS e IIES. Com base no levantamento efectuado e na documentação apresentada pelo CNP e pelos CDSSS, os processos principais que constituem o sistema de atribuição e controlo das pensões abrangidas pelo âmbito desta auditoria são os seguintes:

- **Gestão de Requerimentos**¹¹ – Tem início com a recepção do requerimento de pensão (velhice, invalidez ou sobrevivência) num CDSSS (ou no CNP, no caso de ser um requerimento recebido do estrangeiro) e termina, sendo caso disso, com a transferência do mesmo para o CNP, após verificação de que todos os elementos necessários foram apresentados e integrados no processo;
- **Atribuição e Cálculo de Pensões**¹² – Inicia-se com a recepção, pelo CNP, dos requerimentos enviados pelos CDSSS (ou no CNP, no caso de ser um requerimento recebido do estrangeiro) e termina, em caso de deferimento, com a realização do cálculo da pensão ou, caso contrário, com o indeferimento e/ou arquivamento do processo;
- **Processamento e Pagamento de Pensões**¹³ – Inicia-se com o processamento mensal das pensões calculadas e termina com a reconciliação dos pagamentos efectuados aos beneficiários e a emissão de estatísticas relativas a estas prestações.

É importante entender que o processo de Gestão de Requerimentos não representa o início do ciclo da vida de um contribuinte/beneficiário no SSSS, sendo apenas a última fase do seu envolvimento no sistema. Assim, o primeiro processo considerado no âmbito deste trabalho já depende de outros processos que asseguram o registo da identificação do contribuinte/beneficiário, bem como da sua carreira contributiva.

¹¹ Vide descrição detalhada destes processos no **Anexo E – Levantamento dos Circuitos e da Arquitectura Informática**.

¹² Idem.

¹³ Ibidem.



Tribunal de Contas

V.2. Os Processos de Gestão de Sistemas de Informação

Os processos inerentes à atribuição e controlo de pensões foram, e continuam a ser, suportados pelos processos que dependem dos sistemas de informação. A gestão destes sistemas assegura que as tecnologias de informação utilizadas funcionam de forma correcta e fiável. Os principais processos de gestão de sistemas de informação do SSSS foram identificados e levantados, também, através de entrevistas com os responsáveis dos vários Núcleos e Unidades do CNP, CDSSS, IGFSS e IIES. Com base no levantamento efectuado e na documentação apresentada pelas entidades mencionadas, os principais processos de gestão de sistemas de informação são os seguintes:

- Planeamento e Estratégias de Sistemas de Informação;
- Desenvolvimento e Aquisição;
- Operação dos Ambientes de Sistemas de Informação;
- Monitorização.

Os processos de Desenvolvimento e Aquisição de Sistemas de Informação, bem como os processos de Operação dos Ambientes de Sistemas de Informação tiveram uma ênfase acrescida no decorrer deste trabalho, dado que afectaram, de forma mais directa, os processos inerentes à “atribuição e controlo de pensões”.

V.2.1. As Principais Aplicações

Durante o ano 2000, os processos relativos à “atribuição e controlo de pensões” foram suportados por quatro sistemas informáticos principais, a saber:

- o Sistema de Identificação de Beneficiários e Utentes (BNDBU);
- os Sistemas de Requerimentos (FCR);
- o Sistema de Pensões (FP); e
- o Sistema de Contabilidade Financeira – CONTICO.

Os sistemas de Identificação de Beneficiários e Utentes, de Requerimentos e de Pensões são sistemas *proprietários* do CNP, centralizados em Lisboa, e assentam numa base de dados gerida pela plataforma UNISYS, sendo a sua utilização partilhada entre o CNP e os CDSSS, o que possibilita que ambas as entidades possam partilhar informação sobre Beneficiários e Requerimentos de Pensões.

O sistema financeiro mais importante para o “sistema de atribuição e controlo de pensões” assenta no sistema CONTICO, gerido pela Unidade Financeira do CNP. No início do corrente



Tribunal de Contas

ano, para poder dar resposta às exigências do EURO e do novo POCISSSS, este sistema informático foi substituído pelo sistema SAP R/3. Dado que o âmbito do trabalho contempla somente o ano 2000, o sistema SAP R/3 não foi aqui considerado.

O levantamento efectuado revelou que, embora cada tipo de pensão implique um tratamento de dados distinto, as transacções de introdução e de consulta de dados que estão a ser utilizadas para registar os vários tipos de requerimentos de pensões do Regime Geral são, na maior parte dos casos, idênticas. No caso do cálculo e processamento de pensões do Regime Geral, a maioria dos programas utilizados no sistema do CNP para os efectuar é comum.

V.2.2. As Principais Plataformas de Hardware

O sistema do CNP, que se configura como a peça central do SSSS no que respeita à atribuição e controlo de pensões, reside numa plataforma *UNISYS ClearPath IX*. Este sistema é alimentado por vários sistemas distritais, assentes em diferentes plataformas, designadamente:

- *IBM S/390* – CDSSS – Lisboa;
- *IBM AS/400* – CDSSS – Setúbal, Vila Real, Bragança, Viseu, Castelo Branco, Aveiro, Guarda e Coimbra;
- *ICL Series 39* – CDSSS – Porto, Braga, Leiria, Santarém, Beja, Açores e Madeira;
- *UNISYS XR6* – CDSSS – Faro.

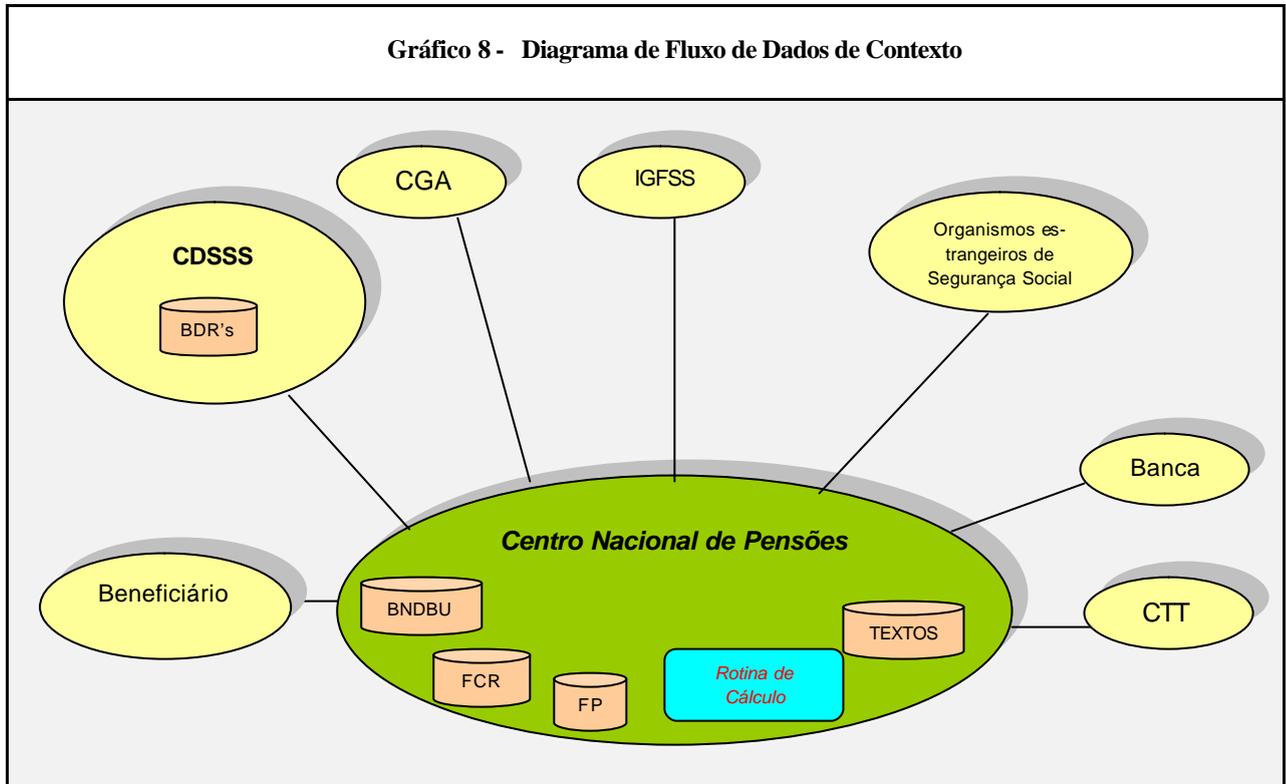
Existem, ainda, outras plataformas em UNIX, que são importantes para a transferência de dados e informação entre os vários interlocutores deste sistema.

Funcionalmente, o CNP organiza e implementa formas de protecção social relativas aos eventos de invalidez, velhice, morte e outras prestações que com elas se relacionem ou sejam determinadas pelo mesmo facto.

A fim de proporcionar uma visão mais geral do sistema de informação em causa, o diagrama a seguir representa o contexto do Centro Nacional de Pensões com as entidades externas com as quais interage.



Gráfico 8 - Diagrama de Fluxo de Dados de Contexto



V.2.3. A Infra-estrutura de Redes

Os sistemas informáticos do SSSS estão interligados através de uma rede *ethernet*, baseada no protocolo TCP-IP, que liga todos os sistemas e instalações principais do ISSS.

A estrutura de redes do SSSS é baseada num troço principal, com nós centrais no IIES e no CNP, e com ligações entre as seguintes regiões:

- Lisboa e Vale do Tejo;
- Norte;
- Centro;
- Alentejo;
- Algarve;
- Açores; e
- Madeira.

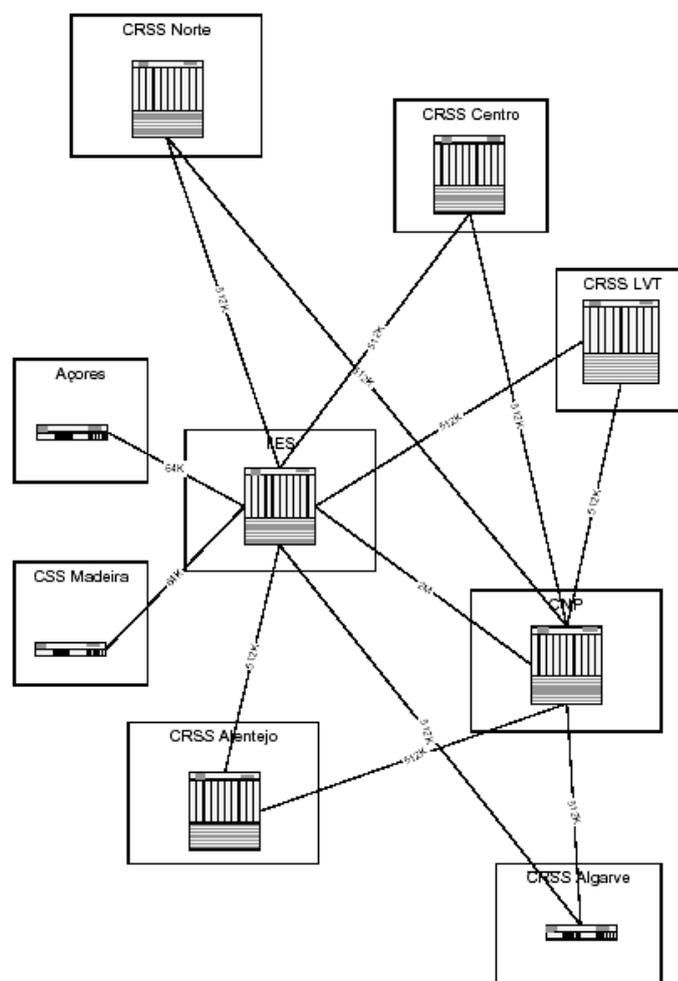
Os troços principais foram desenvolvidos com alguma redundância de ligações entre os vários sistemas regionais, tendo, cada um destes (com a exceção da Madeira e dos Açores), pelo menos duas ligações indirectas ao IIES e ao CNP. Dado que os sistemas do CNP são os sistemas críticos para o funcionamento da atribuição e pagamento de pensões do SSSS agregado



Tribunal de Contas

pelo ISSS, o CNP tem um número significativo de ligações de rede com os centros distritais. A largura de banda no troço de ligação com os Açores foi entretanto aumentada para suportar a introdução do sistema SAP R/3.

A cada CDSSS foi atribuída uma classe de endereços de IP específicos, tendo, cada um deles, uma rede local com pelo menos um domínio de Windows NT que suporta os clientes de rede. Cada domínio tem um servidor de *e-mail* (MS-Exchange) e pelo menos um *Backup Domain Controller* que replica a informação de segurança necessária para a autenticação dos utilizadores. Neste momento não existe nenhuma segmentação da rede global, permitindo, assim, a livre circulação de dados entre as várias redes locais.



Fonte: IIES



Tribunal de Contas

VI. METODOLOGIA E RESULTADOS DA AUDITORIA INFORMÁTICA

VI.1. Metodologia de Avaliação de Riscos e Controlos

O âmbito desta auditoria e os objectivos nela estabelecidos incidem, fundamentalmente, sobre os processos relativos ao sistema de “atribuição e controlo de pensões” e sobre os processos de gestão dos sistemas de informação inerentes aos mesmos.

A metodologia adoptada direccionou-se para uma visão global dos riscos e controlos subjacentes aos processos e sistemas que constituem a “atribuição e controlo de pensões”, podendo ser resumida nas seguintes fases:

- levantamento da Arquitectura de Sistemas e Tecnologias de Informação de Suporte;
- levantamento dos Processos Principais de Atribuição e Controlo de Pensões;
- levantamento dos Processos de Gestão de Sistemas e Tecnologias de Informação;
- identificação e análise dos riscos mais significativos associados aos processos de atribuição e controlo de pensões bem como dos sistemas e tecnologias de informação que os suportam;
- identificação e avaliação dos controlos existentes para gerir os impactes dos riscos identificados;
- execução de Testes aos Controlos; e
- relato das carências de Controlo detectadas e identificação das possíveis melhorias de controlo.

Assim, a abordagem desta auditoria foi delineada, não só no sentido de se obter um conhecimento detalhado dos processos envolvidos no referido sistema, como para permitir a compreensão dos processos de gestão de sistemas e tecnologias de informação do SSSS e, assim, possibilitar um adequado conhecimento dos impactes que os riscos do sistema de informação poderão ter neste processo.

Atendendo a que os vários processos enquadrados no âmbito desta auditoria são suportados por sistemas de informação e dado que a auditoria foi iniciada na fase de preparação da introdução do EURO (vital para a estabilidade do SSSS), considerou-se necessário, neste âmbito, caracterizar, não apenas a arquitectura informática subjacente, mas também, o processo de gestão de sistemas de informação responsável para o efectivo controlo dos mesmos.

O modelo de processos aqui definido apenas contempla a sua discriminação até ao nível da actividade, sendo dado um maior detalhe aos processos de TI (Tecnologias de Informação) que têm aqui maior ênfase. A articulação de cada um destes processos e actividades consta do **Anexo E – Levantamento dos Circuitos e da Arquitectura Informática**. Esta articulação foi necessária, quer para confirmar o entendimento do funcionamento das várias actividades do



Tribunal de Contas

processo de atribuição e controlo de pensões do SSSS, quer para identificar os riscos e controlos manuais e/ou informáticos inerentes aos processos enquadrados no âmbito desta auditoria.

VI.1.1. Definição de Conceitos

VI.1.1.1. CONCEITOS DE RISCO E CONTROLO

Para facilitar a interpretação, na leitura deste relatório, importa definir, à partida, os conceitos de risco e controlo, aqui utilizados num contexto específico de auditoria à gestão de sistemas e tecnologias de informação.

Assim, **RISCO** é definido como qualquer evento ou omissão de acção que impossibilite o alcance de um objectivo de uma Organização. Esta definição é muito abrangente e deve ser considerada, para o efeito deste trabalho, de uma forma mais restrita, em termos dos riscos associados à gestão das pessoas, processos e tecnologias de sistemas de informação que enformam o sistema de atribuição e controlo de pensões da segurança social.

A definição de **CONTROLO** contempla qualquer actividade, tarefa, processo, estrutura organizacional ou mecanismo implementado por uma Organização como parte integrante de seu processo, de modo assegurar o alcance dos seus objectivos e salvaguardar os seus activos¹⁴.

É geralmente aceite que a Administração de uma Organização é responsável pela gestão dos riscos que possam afectar o alcance dos seus objectivos. A gestão *pró activa* destes riscos requer a sua identificação atempada e a definição de um sistema de controlo que minimize o seu impacte. Um sistema de controlo efectivo deve, designadamente:

- responder aos riscos inerentes aos seus processos de “negócio”;
- ser parte integrante dos processos de “negócio”;
- ser capaz de responder a riscos internos ou externos; e
- ser capaz de identificar e reportar fraquezas de controlo significativas.

Um processo que seja bem controlado terá que alcançar estes objectivos, mas, também, ser capaz de demonstrar e medir a sua conformidade com os mesmos.

¹⁴ *Turnbull Report.*



Tribunal de Contas

Existem vários modelos de controlo [**COSO**¹⁵, **CobIT**¹⁶ e **SAC**¹⁷] que estabelecem objectivos de controlo para os processos de uma Organização.

O modelo de controlo interno pela COSO (que incide principalmente sobre os processos operacionais de “negócio”) requer que um sistema de controlo interno efectivo alcance cinco objectivos fundamentais:

- Fiabilidade e Integridade de Informação;
- Cumprimento e Conformidade com Requisitos Legais em vigor;
- Salvaguarda de Activos;
- Eficácia e Eficiência de Processos Operacionais; e
- Alcance dos Objectivos e Metas Estabelecidas para os vários Processos Operacionais.

Estes objectivos de controlo, traduzidos no contexto de um processo, requerem:

- uma correcta segregação de funções;
- a salvaguarda de recursos utilizados;
- uma correcta gestão de erros; e
- que as transacções inerentes ao processo sejam:
 - **autorizadas** – assegurando que todas as transacções são devidamente aprovadas por pessoas autorizadas, de acordo com as regras estabelecidas pela Organização ou outra regulamentação relevante, antes de serem registadas ou executadas;
 - **válidas** – assegurando que todas as transacções registadas representam a realidade económica dos acontecimentos, que respeitam as leis relevantes e que foram executadas de acordo com as exigências estabelecidas pela Organização;
 - **completas** – assegurando que todas as transacções válidas são registadas nos sistemas contabilísticos ou operacionais da Organização;
 - **correctas** – assegurando que todas as transacções válidas são correcta e atempadamente registadas de forma consistente com os dados originais da transacção.

A definição de um controlo, no contexto dos processos de “negócio”, contempla todas as actividades, tarefas e configurações técnicas implementadas para assegurar o alcance dos seguintes objectivos de controlo, para cada um dos processos avaliados:

¹⁵ *COSO – Committee of Sponsoring Organizations of the Treadway Commission*

¹⁶ *CobIT- Control Objectives for Information and Related Technology*

¹⁷ *SAC - System Auditability & Control*



Tribunal de Contas

- **registado** – todas as transacções inerentes ao processo foram devidamente registadas;
- **lançado** – todas as transacções registadas são replicadas para todos os sistemas que necessitam ou dependem da informação introduzida;
- **sumariado** – os cálculos e resumos efectuados sobre as transacções registadas são efectuados correctamente;
- **real** – todas as transacções registadas são transacções verdadeiras e não duplicadas;
- **atempado** – todas as actividades associadas ao processo são efectuadas dentro dos prazos estabelecidos para a sua execução;
- **classificado** – todas as transacções registadas são devidamente categorizadas de forma a permitir a sua correcta análise e resumo;
- **eficiente** – todas as actividades associadas ao processo são efectuadas de uma forma que utilize o mínimo de tempo e recursos; e
- **eficaz** – existe uma optimização dos recursos atribuídos ou utilizados pelo processo.

O modelo CobIT, desenvolvido posteriormente ao modelo COSO, aprofundou os objectivos de controlo para os processos de gestão de sistemas e tecnologias de informação. Estes objectivos pretendem assegurar a fiabilidade da informação processada pelos sistemas e tecnologias de informação inerentes a um processo operacional, assegurando:

- **confidencialidade** – a preocupação com a protecção de informação sensível contra a sua divulgação não autorizada;
- **integridade** – a preocupação com a exactidão e representação da totalidade da informação, assim como com a sua validação em termos de valores e expectativas da Organização;
- **disponibilidade** – a preocupação com a disponibilidade da informação e os sistemas que a garantem sempre que ela é requerida pelos processos de “negócio”;
- **eficiência** – a disponibilização de informação através de uma afectação óptima dos recursos;
- **eficácia** – a informação é relevante e pertinente para os processos de “negócio” e, ao mesmo tempo, é disponibilizada atempada e correctamente, de uma forma consistente e utilizável; e



Tribunal de Contas

- **cumprimento de requisitos legais** – a preocupação com o cumprimento da legislação, regulamentos e compromissos contratuais a que os processos de “negócio” estão sujeitos.

Os referidos modelos de controlo são complementares, tendo ambos como objectivo o correcto funcionamento de um processo de “negócio” para possibilitar o alcance dos objectivos definidos pela Organização. Os conceitos base subjacentes aos modelos COSO e CobIT foram utilizados extensivamente na avaliação dos processos de atribuição e controlo de pensões, enquanto o modelo CobIT foi utilizado, exclusivamente, na avaliação dos processos de gestão de sistemas de informação.

VI.1.1.2. CONCEITOS DE AVALIAÇÃO DE PROCESSOS

Para a abordagem desta matéria foi necessário definir, *a priori*, os processos que se enquadram dentro do âmbito estabelecido para este trabalho, designadamente:

- identificação dos principais processos inerentes à atribuição e controlo de pensões;
- definição e uniformização de uma visão das actividades que constituem os processos de atribuição e controlo de pensões;
- identificação das interdependências dos processos relativamente aos sistemas de informação subjacentes;
- interligação dos riscos e controlos identificados no decorrer do trabalho, permitindo, assim, avaliar os mesmos no contexto dos respectivos processos afectados;
- comparação do modelo de processos existente com outros modelos de processos de referência, como o modelo CobIT, no caso dos processos de Gestão de Sistemas de Informação; e
- delimitação do âmbito do trabalho a efectuar.

Um modelo de processos define as actividades principais de uma organização, independentemente do departamento funcional responsável pela sua execução, ou do tipo de produto ou serviço que é tratado. Para efeito deste relatório, o modelo de processos define três níveis hierárquicos, a saber:

- ***Actividade***

Uma actividade representa um conjunto ou agrupamento de tarefas ou unidades de trabalho distintas mas indissociáveis. Uma actividade tem um ciclo de vida que enquadra várias tarefas necessárias para atingir um objectivo mensurável.

- ***Processo***



Tribunal de Contas

Um processo representa um conjunto de actividades com um objectivo comum, mas com limites ou fronteiras naturais. Um processo principal é hierarquicamente superior a um processo, que agrega várias actividades.



Tribunal de Contas

- **Mega-Processo**

A um nível mais elevado, um mega-processo representa um conjunto de processos principais com um objectivo e ciclo de gestão comum. O modelo CobIT atribui o nome de domínio a um mega – processo.

VI.1.1.3. CONCEITOS DA MATURIDADE DE PROCESSOS

A maior parte dos gestores já foi confrontada com decisões de investimento para o controlo dos seus processos operacionais e da sua infra-estrutura de sistemas de informação. Apesar do reconhecimento, manifestado por uma grande maioria, da necessidade de algum investimento na gestão dos riscos associados, é notória a dificuldade em avaliar até que ponto o seu custo é justificado pelos benefícios daí resultantes. Para responder a esta questão é necessário definir um mecanismo de avaliação dos processos em questão, para aferir, nomeadamente:

- a situação actual do processo;
- a evolução desejada para o processo; e
- um mecanismo de avaliação que permita compreender as melhorias alcançadas mediante os objectivos estabelecidos para o processo.

Um modelo de maturidade oferece um mecanismo que permite avaliar e definir o nível de desenvolvimento de um processo e a gestão dos riscos inerentes ao mesmo. O nível de maturidade correcto para um processo depende:

- das necessidades e objectivos da Organização;
- da sua dependência relativamente aos sistemas e tecnologias de informação; e
- do valor atribuído à sua informação.

Um modelo de maturidade permite à Administração de qualquer Organização avaliar os processos actuais e identificar os aspectos necessários para os desenvolver até ao ponto de evolução desejado, sendo que um aumento de maturidade e capacidade de um processo é sinónimo de uma melhor gestão dos riscos que lhe estão associados e de uma maior eficiência do mesmo. O modelo de maturidade escolhido para este trabalho foi baseado no *Capability Maturity Model* definido pelo *Institute of Software Engineering* e adoptado pelo modelo CobIT. Esse modelo define os vários níveis de evolução de um processo com a pontuação respectiva numa escala de 0 a 5, como segue:



Tribunal de Contas

- **0 – Não Existente**

Não existe uma actividade identificável e a entidade ou organização não reconhece a sua necessidade.

- **1 – Principiante**

Existe evidência de que a organização reconhece a necessidade de uma actividade definida mas não existe qualquer padronização do processo. Existem abordagens pontuais e individuais que são aplicadas caso a caso. A abordagem de gestão do processo é desorganizada.

- **2 – Repetitivo**

A actividade já evoluiu até ao ponto em que pessoas diferentes seguem procedimentos similares para a mesma tarefa. Não existe formação ou comunicação dos procedimentos ou normas estabelecidas, deixando ao critério de cada pessoa envolvida a execução da actividade. Existe um alto nível de dependência sobre os conhecimentos de cada pessoa envolvida no processo, e, por isso, a existência de erros é provável.

- **3 – Definido**

A actividade está padronizada, documentada e comunicada através de formação. A responsabilidade de cumprir os procedimentos definidos é da pessoa envolvida. Não existem mecanismos para avaliar os desvios em relação aos procedimentos estabelecidos. Os procedimentos em si não são sofisticados mas existe a formalização dos procedimentos existentes.

- **4 – Gerido**

É possível monitorizar e medir o cumprimento dos procedimentos estabelecidos para possibilitar medidas correctivas onde o processo não é efectivo. Os processos sofrem melhorias constantes e constituem boas práticas, no entanto o processo não é automatizado, ou adequadamente suportado, pela utilização eficiente das ferramentas existentes.

- **5 – Optimizado**

A actividade está optimizada ao ponto de ser considerada melhor prática, resultado das melhorias constantes efectuadas e na comparação com outras organizações. As tecnologias de informação são utilizadas de uma forma integrada, automatizando os processos de trabalho, melhorando o nível de qualidade e eficiência do processo e permitindo uma rápida adaptação do processo à mudança.



Tribunal de Contas

A tabela seguinte apresenta as práticas necessárias para a evolução de um processo, nos seguintes aspectos:

Tabela 7 - Práticas Necessárias para a Evolução de um Processo

Nível	Entendimento e Consciência	Formação e Comunicação	Processo e Práticas	Técnicas e Automação	Cumprimento	Conhecimentos Especializados
1	Reconhecimento do processo	Comunicação pontual sobre assuntos relacionados com o processo	Abordagem pontual ao processo e às práticas em vigor			
2	Maior consciência do próprio processo.	Comunicação global dos assuntos e das suas necessidades	Existência de um processo intuitivo mas comum	Existência de algumas ferramentas comuns	Monitorização inconsistente sobre assuntos pontuais	
3	Reconhecimento da necessidade de actuar sobre o processo	Formação informal que suporta iniciativas individuais	Práticas definidas, padronizadas e documentadas permitindo a partilha de melhores práticas	Estão disponíveis e é utilizado um conjunto de ferramentas padronizadas	Monitorização inconsistente, medição do processo iniciado, análise de causas é intuitiva	Envolvimento pontual de especialistas de TI nos processos do “negócio”
4	Entendimento total dos requisitos do processo	Formação formal suporta a gestão do processo	Responsabilidades pelo processo estão definidas, o processo está completo e as melhores práticas internas são utilizadas	Técnicas estabelecidas são utilizadas, e a utilização de ferramentas padronizadas é cumprida, mas verifica-se uma utilização limitada da tecnologia	Monitorização consistente em função de um conjunto de indicadores de gestão estabelecidos, com a análise de causas padronizada	Envolvimento de especialistas internos do processo.
5	Visão e entendimento pró-activo do processo	Formação e comunicação suportam a utilização de melhores práticas externas utilizando conceitos de ponta	São aplicadas as melhores práticas externas	Técnicas sofisticadas são implementadas e o uso extensivo de tecnologia é optimizado	Monitorização global em função de um conjunto de indicadores de gestão estabelecidos, a análise de causas é padronizada e as excepções são analisadas e as acções de melhoria necessárias são tomadas	Utilização de especialistas externos e líderes da indústria para definir melhorias no processo

A avaliação efectuada dos processos de gestão das tecnologias de informação do SSSS é baseada nos níveis de maturidade estabelecidos nos termos deste modelo. É importante reconhecer que a evolução de um processo implica um maior investimento de recursos na sua monitorização e gestão. Por outro lado, considerando o custo/benefício associado à gestão de uma activi-



Tribunal de Contas

uma actividade, nem sempre é viável, para uma Organização, evoluir a maturidade de todos os seus processos para níveis otimizados.

VI.1.2. Processos de Atribuição e Controlo de Pensões

A avaliação dos riscos e controlos associados aos processos relativos à “atribuição e controlo de pensões” baseou-se na realização de entrevistas com os responsáveis dos departamentos directamente envolvidos nestas matérias, bem como na observação e inspecção de documentos e outras evidências electrónicas, que permitiram confirmar o seu entendimento e posterior identificação dos riscos e dos controlos existentes para os colmatar.

A avaliação de riscos pretendeu, essencialmente, avaliar se os procedimentos existentes asseguravam:

- uma correcta segregação de funções entre os vários elementos envolvidos na execução do processo;
- uma correcta aplicação dos requisitos legais estabelecidos;
- a salvaguarda adequada de recursos financeiros;
- um funcionamento eficiente e eficaz do processo; e
- a fiabilidade e integridade da informação produzida no processo.

Na sequência do trabalho desenvolvido, foram definidos, para os processos onde se identificaram riscos com maior probabilidade de ocorrência de erros (nos processos de atribuição, cálculo e pagamento de pensões), testes específicos para avaliar a eficácia dos controlos existentes, sendo, para esse efeito, considerados apenas os **processos de pensão do Regime Geral “puro”¹⁸ deferidos em 2000**. A natureza destes testes pode ser resumida nas seguintes categorias:

¹⁸ Optou-se por designar de “puro” o regime base constante dos Decreto-Lei nº 329/93, de 25 Setembro, e Decreto Lei nº 322/90, de 18 de Outubro, e demais legislação complementar.



Tribunal de Contas

VI.1.2.1. TESTES AOS CÁLCULOS DE PENSÕES

Uma vez que a maior parte do cálculo de pensões se encontra informatizado, avançou-se para o recálculo das pensões com base nos pressupostos legais estabelecidos, sendo as dúvidas, entretanto surgidas, colmatadas através de entrevistas tidas com os responsáveis do CNP. Paralelamente, efectuaram-se levantamentos sobre a informação disponível e relevante para este trabalho. Quanto aos testes sobre o cálculo automatizado de pensões foi necessário desenvolver um entendimento dos dados existentes nos sistemas do CNP e da natureza dos processamentos efectuados. Este trabalho inicial permitiu a identificação dos dados informáticos principais para os recálculo e testes das pensões, tendo sido, subsequentemente, requisitados três grupos de ficheiros que serviriam de base para a efectivação dos testes:

- **Ficheiros de Cálculo** – servem de base aos cálculos automáticos efectuados para as pensões do Regime Geral deferidas em 2000;
- **Ficheiros de Requerimentos** – possuem toda a informação inserida no sistema informático sempre que é dada entrada a um requerimento;
- **Ficheiros de Pensionistas** – possuem os dados necessários para o processamento de pensões, desde a identificação do beneficiário, incluindo os valores de pensão efectivamente processados e recebidos e as características da pensão em causa. Este ficheiro representa ao mesmo tempo o âmbito do trabalho a efectuar (pensões deferidas e processadas durante o ano de 2000) e o valor a validar, para cada parcela de pensão.

Os primeiros três grupos de ficheiros foram recebidos em meados de Novembro de 2001. Após importação, leitura, análise e validação dos totais de controlo enviados pelo CNP, foi dado início ao trabalho de recálculo automático. Os testes de recálculo requereram a concepção e execução de programas em SAS (uma ferramenta de *Data Mining*) para simular o cálculo efectuado pelos sistemas do CNP, utilizando os dados fornecidos pelo mesmo. Estes programas permitiram a comparação dos respectivos resultados com os obtidos pelos sistemas do CNP. Desta forma foi possível, não só identificar as excepções nos cálculos efectuados, mas também confirmar que os cálculos executados pelos sistemas do CNP estão de acordo com a legislação e a regulamentação aplicáveis. As diferenças identificadas permitiram analisar a razoabilidade das razões pelas divergências à regulamentação estabelecida.

A população a analisar centrou-se no ficheiro de pensionistas, ou seja, o ficheiro com os dados de pensões de Sobrevivência, Velhice e Invalidez, do Regime Geral, deferidas durante o ano de



Tribunal de Contas

2000. Das várias parcelas¹⁹ que constituem uma pensão, somente foram consideradas as parcelas referentes às Pensões do Regime Geral, que apenas incluem:

- Pensão Estatutária – Parcela 01
- Actualização de Pensão – Parcela 02
- Complemento Social – Parcela 11
- Complemento de Dependência de Primeiro Grau – Parcela 22
- Complemento de Dependência de Segundo Grau – Parcela 42

Da análise efectuada da legislação e dos dados recebidos concluiu-se que uma pensão, considerada como pertencente ao Regime Geral “puro”, requer a codificação informática de três aspectos que devem ser cumpridos simultaneamente:

1. Código de Pensão Especial = 0;
2. Código de Situação Especial = 0;
3. Parcelas de Pensão:
 - 01 – Pensão Estatutária;
 - 02 – Actualizações de Pensões;
 - 11 – Complemento Social;
 - 22 – Complemento de Dependência de 1º Grau;
 - 42 – Complemento de Dependência de 2º Grau.

Foi efectuada o recálculo das pensões, para cada uma destas parcelas, e compararam-se os resultados com os obtidos pelo CNP. Em consonância com o tratamento dado pelo CNP, todos os arredondamentos foram feitos para a dezena de escudos superior. Identificaram-se, assim, todas as diferenças entre os resultados do cálculo de teste e o cálculo efectuada pelo CNP e analisaram-se estas diferenças, de acordo com os seguintes limites:

- Parcela 01 – Pensão estatutária – todas as diferenças superiores a PTE 1000;
- Restantes Parcelas – todas as diferenças superiores a PTE 10

Nos casos de existência de pensão por antecipação da idade (para efeitos de pensão de velhice), é aplicado um factor específico de redução aquando do cálculo da pensão. Estas pensões, dadas as especificidades do seu cálculo, não foram consideradas no âmbito do recálculo automático de pensões, mas foram consideradas na população de pensões de cálculo “manual”.

¹⁹ Referente às diferentes fracções que compõem a totalidade do valor da pensão.



Tribunal de Contas

Os testes efectuados consistiram na criação de programas específicos que, com o apoio da legislação e dos próprios colaboradores do CNP (pela sua larga experiência nestas matérias), visaram validar os resultados obtidos pelos programas existentes no CNP. A interpretação da legislação em vigor com impacte nos cálculos efectuados foi discutida com os responsáveis do CNP, para assegurar a sua correcta consideração nos testes informáticos realizados e a avaliação da sua compatibilidade com os programas utilizados por este organismo.

A avaliação da integridade e fiabilidade dos programas de cálculo baseia-se nos testes efectuados sobre o cálculo de pensões. Utilizando ferramentas próprias para o efeito, simulou-se o cálculo automático das pensões processadas no ano 2000 no âmbito do Regime Geral “puro”. Foram identificadas preliminarmente as pensões objecto de cálculo “manual”, tendo-lhes sido dado um tratamento alternativo.

VI.1.2.2. TESTES DE PROCESSOS DE PENSÕES CALCULADOS MANUALMENTE

Os testes sobre a atribuição de pensões incidiram principalmente na verificação do cumprimento da legalidade e, concomitantemente, na observação da correcção financeira dos cálculos efectuados, destacando-se os seguintes pontos:

- correcção do ponto de vista da organização processual, designadamente, da documentação legalmente prevista para cada tipo de processo – Invalidez (PI), Velhice (PV) e Sobrevivência (PS);
- correcção da documentação interna do CNP, nomeadamente, dos despachos de deferimento e outros documentos auxiliares da instrução do processo (verbetes resumo das transacções a efectuar e efectuadas);
- verificação do enquadramento legal de cada processo e correcta aplicação das respectivas normas;
- verificação do prazo de garantia e da carreira contributiva dos pensionistas;
- verificação da correcção dos cálculos efectuados manualmente.

Dado que o cumprimento destes requisitos depende da existência de documentos comprovativos, e não existindo nenhum registo electrónico que indique o estado de cumprimento dos requisitos legais de cada requerimento, a avaliação da atribuição de pensões foi efectuada manualmente, sobre uma amostra seleccionada para o efeito.



Tribunal de Contas

VI.1.2.2.1. DEFINIÇÃO DA AMOSTRA

Devido ao tratamento informático dos sistemas que suportam o cálculo de pensões, foi necessário tratar um processo como uma instância única de um beneficiário com um sufixo de sobrevivência. Deste modo, para a análise da atribuição do cálculo de pensões, o conceito de “processo” é baseado nesta definição.

O universo de requerimentos do Regime Geral, deferidos durante o ano 2000, foi de cerca de 135 000. Deste universo, foram identificados processos "manuais", que resultaram da comparação do ficheiro de pensões com o ficheiro de cálculo, como anteriormente referido.

Dos 2571 processos calculados “manualmente”, foi seleccionada uma amostra aleatória com base em cálculos estatísticos sobre a população total dos processos “manuais”. A selecção desta amostra foi efectuada recorrendo a técnicas estatísticas de amostragem de modo a assegurar que fosse possível projectar as percentagens de erro ou inconformidades no universo de processos manuais. O quadro abaixo resume os pressupostos utilizados nestes cálculos:

Quadro VIII - Pressupostos	
População – Processos com cálculos manuais	2.571
Erro Tolerável (em PTE)*	2.571.000
Key Item Cut Off (em PTE)	175.000
Avaliação do Risco	Moderada
Conforto de outros Testes	Algum
Grau de Confiança	95%

* Considerando tolerável um erro de 1000 escudos por processo

Como parte dos critérios de selecção de amostra, foi estabelecido um valor mínimo de pensões (*Cut Off* = PTE 175.000) que determinaria todos os *Key Items*, ou seja, assegurando-se que todas as pensões de montante superior ao valor predeterminado seriam automaticamente seleccionadas.

VI.1.2.2.2. CARACTERIZAÇÃO DA AMOSTRA

A amostra seleccionada representa cerca de 15,8% do universo em causa, tendo sido ligeiramente reduzida no decorrer dos trabalhos, visto existirem, em alguns casos, dois ou mais processos separados relativos ao mesmo beneficiário, referentes a eventualidades distintas



Tribunal de Contas

(pensão de velhice/invalidez e de sobrevivência) que foram considerados conjuntamente. O quadro seguinte evidencia os resultados da selecção efectuada:

Quadro IX - Amostra	
<i>Cut Off</i> (PTE)	175.000
<i>Key Items</i>	74
Amostra Aleatória Representativa	331
Total de Processos Seleccionados	405

Sendo esta população extraordinariamente heterogénea²⁰ do ponto de vista legal – muitas vezes causa suficiente para o seu tratamento manual –, que implica, amiúde, a aplicação conjugada de várias leis e diplomas regulamentares e obriga a inúmeras considerações e raciocínios – seu enquadramento jurídico; contagem do tempo relevante da carreira contributiva do beneficiário; prazo de garantia (variável consoante o ano de referência²¹); efectivação do cálculo da pensão que resulta, nestes casos, da consideração de diversas variáveis – depreende-se a complexidade implícita ao tratamento destes processos e o nível de risco de ocorrência de erros associado à determinação do valor da pensão a pagar.

O quadro e o gráfico abaixo tipificam os tipos de eventualidade, demonstrando, também, o facto de que existem processos em que se conjugam várias eventualidades relativas ao mesmo beneficiário razão da diferença entre o total evidenciado no quadro anterior e o reflectido no seguinte:

²⁰ Ver glossário de legislação utilizada na análise dos processos (**Anexo A1**).

²¹ Prazos de Garantia:

- **Invalidez**

- ✓ Regra geral: 5 anos civis com registo de remunerações (n.º 1 do art.º 16.º do DL 329/93, de 25 de Setembro)
- ✓ Até Dezembro de 1973: 5 anos de inscrição e 30 meses com entrada de contribuições ou 5 anos civis com entrada de contribuições;
- ✓ Até Dezembro de 1979: 3 anos de inscrição e 24 meses com entrada de contribuições;
- ✓ Até Setembro de 1984: 36 meses com entrada de contribuições;
- ✓ Até Dezembro de 1993: 36 meses com entrada de contribuições.

- **Velhice**

- ✓ Regra geral: 15 anos civis com registo de remunerações (art.º 21.º do DL 329/93, de 25 de Setembro);
- ✓ Até Dezembro de 1973: 10 anos de inscrição e 60 meses com entrada de contribuições ou 10 anos civis com entrada de contribuições;
- ✓ Até Dezembro de 1979: 3 anos de inscrição e 24 meses com entrada de contribuições;
- ✓ Até Setembro de 1984: 60 meses com entrada de contribuições;
- ✓ Até Dezembro de 1993: 120 meses com entrada de contribuições.



Tribunal de Contas



Tribunal de Contas

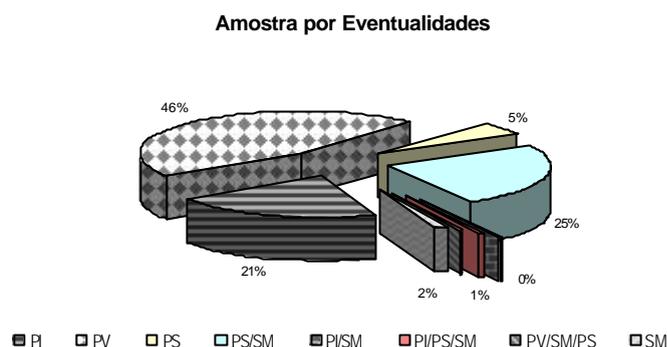
Quadro X - Tipo de Eventualidades

Tipo de Eventualidade	Total
PI	83
PV	182
PS	19
PS/SM	99
PI/SM	1
PI/PS/SM	3
PV/SM/PS	1
SM	6
Total Global	394

Legenda:

PI – Pensão de Invalidez;
PV – Pensão de Velhice;
PS – Pensão de Sobrevivência;
SM – Subsídio por morte.

Gráfico 9 - Amostra por Eventualidades



Assim, cerca de 46% dos processos dizem respeito a Pensões de Velhice, sendo o segundo grupo mais significativo, com cerca de 25% da amostra, respeitante àquele onde se conjugam a Pensão de Sobrevivência e o Subsídio por Morte.

VI.1.3. Sistemas e Tecnologias de Informação

A avaliação dos riscos e controlos inerentes aos processos de gestão de sistemas de informação foi efectuada recorrendo ao confronto do modelo de processos de CobIT com o modelo de processos do SSSS, de forma a definir os processos principais de gestão dos sistemas e tecnologias de informação. Com esta abordagem, foi possível identificar actividades e controlos que não constam da realidade do SSSS, cuja omissão pode ter riscos para a mesma, bem como áreas onde o SSSS pode melhorar as actividades já existentes.

O modelo CobIT é reconhecido e aceite mundialmente como o modelo de referência para a avaliação de riscos e controlos dos processos de tecnologias de informação (TI). O modelo oferece uma estrutura de processos inerentes a um departamento ou direcção de sistemas de informação com os seus respectivos pontos de controlo e de acordo com as *melhores práticas*. O modelo CobIT que foi adoptado para a avaliação dos processos e actividades de sistemas e tecnologias de informação do SSSS define 34 actividades para um ambiente de sistemas e tecnologias de informação, tendo, cada uma dessas actividades, entre 3 e 30 pontos de controlo específicos,



Tribunal de Contas

específicos, para responder aos riscos do mesmo. A escolha deste modelo de melhores práticas na gestão de processos de TI permite avaliar, de forma global, a gestão dos processos de TI do SSSS; no entanto, visto que se trata de comparar um modelo teórico com os processos existentes numa realidade concreta, é possível que, decorrente de decisões estratégicas tomadas no passado, vários processos previstos no referido modelo não existam no contexto do SSSS.

A verificação dos riscos inerentes aos processos de gestão de sistemas de informação pretendeu, essencialmente, avaliar se os procedimentos existentes asseguravam:

- confidencialidade;
- integridade;
- disponibilidade;
- eficiência e eficácia; e o
- cumprimento dos requisitos legais,

da informação processada pelos sistemas de informação do SSSS. Por outro lado, para avaliar em que medida os riscos identificados resultavam em erros ou inconformidades nos processos de gestão de sistemas de informação, foi necessário formular e efectuar testes sobre os controlos considerados mais importantes para o funcionamento dos processos de desenvolvimento/implementação de sistemas e aplicações, bem como sobre os processos de gestão de segurança.

Visto que não é possível analisar os controlos existentes no ano de 2000 (ano a que se reportam os dados sobre os quais incidiram os testes efectuados), a avaliação recaiu sobre os processos de gestão de sistemas de informação existentes durante o ano 2001.

VI.1.3.1. TESTES AO PROCESSO DE DESENVOLVIMENTO

Durante o ano de 2001, os desenvolvimentos mais significativos aos sistemas que suportam os processos de “atribuição e controlo de pensões” estiveram directamente relacionados com a sua preparação para o EURO.

Os testes ao processo de desenvolvimento foram conjugados com os testes efectuados ao Projecto EURO, de forma a otimizar a sua cobertura, tendo sido realizados com base, quer na documentação existente do projecto, quer em entrevistas aos responsáveis directamente envolvidos na execução, desenvolvimento e conversão dos sistemas para o EURO. Os testes realizados concentraram-se na entrevista dos elementos envolvidos nos desenvolvimentos efectuados e no teste destes, bem como na inspecção de evidência documental ou electrónica, caso existisse, que comprovasse a execução de pontos de controlo essenciais a um ciclo de desenvolvimento. As práticas de controlo identificadas foram comparadas com as melhores



Tribunal de Contas

práticas estabelecidas pelo modelo CobIT nesta área, bem como com outras referências sobre o controlo de projectos de desenvolvimento de sistemas.

Esta abordagem permitiu, não só uma avaliação do nível de preparação do SSSS para a entrada do EURO, como também, simultaneamente, a avaliação dos processos de desenvolvimento e implementação de sistemas. Os testes aos processos de desenvolvimento incidiram sobre as plataformas mais significativas do SSSS e sobre as várias realidades que existem no mesmo, tendo os respectivos resultados sido atempadamente comunicados.

VI.1.3.2. TESTES À SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO

Os testes à segurança de sistemas de informação consistiram na avaliação dos procedimentos de segurança adoptados pelas várias instituições abrangidas pelo âmbito deste trabalho.

Dada a grande variedade de plataformas e departamentos/unidades de sistemas de informação existentes no SSSS, efectuou-se a avaliação dos processos de gestão de sistemas de informação apenas para as seguintes entidades:

- Centro Nacional de Pensões – Plataforma UNISYS Clearpath IX;
- Centro Distrital de Solidariedade e Segurança Social de Lisboa – Plataforma IBM S/390;
- Centro Distrital de Solidariedade e Segurança Social do Porto – Plataforma ICL Series 39;
- Centro Distrital de Solidariedade e Segurança Social de Setúbal – Plataforma AS/400;
- Instituto de Informática e Estatística da Segurança Social – Rede Windows NT.

A selecção destes sistemas permitiu uma visão global dos processos de gestão dos sistemas de informação adoptados pelo SSSS, incidindo sobre os sistemas e as aplicações mais críticas para os processos de atribuição e controlo de pensões. Para cada um destes ambientes informáticos foi definido um plano de auditoria específico, consoante as características tecnológicas de cada plataforma abordada, tendo a sua execução sido devidamente suportada pela utilização de ferramentas de auditoria informática para a obtenção de evidências sobre o estado da segurança lógica dos sistemas auditados.

O plano de auditoria definido para cada uma das plataformas auditadas exigiu:

- A realização de entrevistas com os responsáveis (e outros elementos do ISSS ou IESS) pelos vários sistemas de informação enquadrados no âmbito deste trabalho;



Tribunal de Contas

- a análise das configurações das aplicações, dos sistemas operativos, bases de dados e ou tecnologias de telecomunicações, com base na extracção de relatórios ou outra informação de configuração inerentes à tecnologia em questão; e
- a utilização de ferramentas de análise de segurança de sistemas de informação (Como *CyberCop*, *DumpACL*, *DumpSec* e várias outras) para validar e testar as configurações dos sistemas auditados.

As entrevistas realizadas tiveram como objectivo obter um entendimento detalhado dos procedimentos de controlo, em vigor nas várias instituições, relacionados com:

- A Gestão da Segurança Física – i.e., existência de controlos manuais ou informáticos que salvaguardem os sistemas e os dados de ameaças físicas, como, por exemplo, cortes de energia, acesso físico a sistemas, condições ambientais inadequadas, etc.
- A Gestão de Segurança Lógica - i.e., a existência de controlos manuais ou informáticos que assegurem que o acesso à informação (bem como a sua alteração ou eliminação) estava devidamente controlada, em termos da configuração das aplicações, das bases de dados, dos sistemas e das redes e mecanismos de telecomunicações que contribuem para segurança e integridade da informação, etc.
- A Gestão de Desenvolvimentos e Alterações a Sistemas - i.e., a existência de controlos manuais ou informáticos que assegurem que as alterações aos sistemas não afectam a integridade da informação existente e não resultam na omissão de informação.

Este entendimento foi cruzado e confirmado com a evidência obtida através da análise efectuada às configurações dos sistemas, mencionada acima. Estas análises permitiram confirmar as constatações verbais com os controlos implementados nos sistemas e evidentes nas configurações dos mesmos. As análises das configurações foram efectuadas *in loco* com os vários elementos, permitindo, assim, esclarecer quaisquer dúvidas e transmitir os impactos das deficiências de controlo detectadas.



Tribunal de Contas

VI.2. Síntese dos resultados da auditoria

Um dos princípios fundamentais de controlo interno estabelece que qualquer processo deve colmatar os seus riscos inerentes com a implementação de controlos adequados e efectivos. A avaliação dos processos que se apresenta foi efectuada com base na identificação e avaliação dos riscos e controlos existentes em cada uma das actividades que compõem um processo, bem como na execução de testes de auditoria para confirmar o funcionamento efectivo dos controlos mais significativos identificados. Dada a extensão e variedade dos temas abordados nesta auditoria, foi necessário resumir os resultados obtidos. Assim, apresenta-se no **Anexo B – Detalhe dos Resultados da Auditoria** o detalhe dos resultados discutidos e resumidos neste capítulo. Esse anexo deve ser considerado como parte integral deste relatório, sendo fundamental para um entendimento completo e detalhado dos resultados obtidos.

Para facilitar a leitura e interpretação dos resultados principais, resume-se de seguida os resultados da avaliação dos vários processos e actividades que integram o “sistema de atribuição e controlo de pensões”, bem como o processo de gestão de sistemas de informação que suporta os sistemas e as aplicações inerentes aos processos, no âmbito deste trabalho.

VI.2.1. Processos de Atribuição e Controlo de Pensões

Os resultados da avaliação dos processos de “atribuição e controlo de pensões” apontaram para os seguintes aspectos:

VI.2.1.1. GESTÃO DE REQUERIMENTOS

Os procedimentos relativos a este processo estão adequadamente detalhados (em termos do Manual de Procedimentos elaborado pelo ISSS) e as responsabilidades dos intervenientes estão razoavelmente bem definidas (em termos do Decreto Lei n.º 316-A/2000, de 7 de Dezembro). É da responsabilidade dos CDSSS a execução das medidas necessárias para o reconhecimento de direitos de atribuição e pagamento de pensões, com a excepção das medidas que são da competência do CNP.



Tribunal de Contas

VI.2.1.1.1. EFICIÊNCIA DO PROCESSO

O processo de registo de requerimentos está bastante informatizado, mas, dado que a recepção do requerimento continua a ser registada manualmente, é difícil controlar, de forma eficaz, a omissão do registo de requerimentos no sistema. O registo da carreira contributiva depende, neste momento, da integração desta informação, proveniente de vários sistemas, sedeados nos CDSSS. Devido a atrasos no carregamento automático nos sistemas do CNP, esta informação está a ser carregada manualmente pelos CDSSS e pelos elementos do CNP no sistema informático deste Centro. Este “carregamento” manual tem resultado em atrasos significativos no processamento de requerimentos, dado que uma quantidade significativa de processos é enviada para o CNP sem que estejam completamente registados no sistema. Neste momento, cabe ao CNP carregar, na maioria dos casos, os últimos anos de contribuições, dado que o seu sistema ainda não possui estes dados. Estes atrasos ocorrem devido a problemas relacionados com:

- incompatibilidade dos sistemas dos CDSSS com o do CNP;
- atrasos no carregamento de ficheiros no sistema do CNP; e
- atrasos no carregamento de carreiras contributivas nos CDSSS.

Presentemente, não existe nenhum procedimento que assegure que os requerimentos enviados ao CNP estejam completos, em termos da informação necessária para o deferimento do processo, e que esta informação esteja totalmente carregada nos sistemas do CNP. Durante a avaliação deste processo, não foi constatada a existência de estatísticas, por parte do CNP ou dos CDSSS, que reflectissem a situação atrás descrita, sendo difícil, sem este tipo de informação, avaliar os impactos e apontar as causas inerentes aos atrasos verificados. Estes atrasos têm vindo a ser recuperados, mas, à data do trabalho de campo desta auditoria, o CNP ainda se encontrava a carregar manualmente os últimos anos de carreira contributiva no seu sistema.

O processo actual não distingue em termos da prioridade do requerimento. Deste modo, um requerimento para um cálculo provável tem a mesma prioridade e segue os mesmos trâmites que um cálculo definitivo. Constatou-se que os cálculos prováveis representam um volume significativo de processos tratados, principalmente no que se refere às pensões de velhice. Considera-se que, para melhorar os tempos de resposta do sistema, deve haver uma distinção entre o tratamento daqueles processos.

VI.2.1.1.2. INTEGRIDADE DO PROCESSO

Quanto à integridade da informação introduzida, observou-se que o carregamento de informação nos sistemas sofre de várias deficiências. Foram encontrados vários campos, principalmente campos de datas, que não são adequadamente validadas, para assegurar que a informação



Tribunal de Contas

introduzida seja fiável. Esta situação dificulta a identificação e monitorização de requerimentos, com atrasos significativos no seu processamento e deferimento.

Os testes efectuados sobre a fiabilidade da informação de identificação de beneficiários indicam que não existem beneficiários duplicados, mas que é possível que o mesmo beneficiário possua mais que um número na BDNBU; mesmo assim, não se detectaram situações de requerimentos deferidos não adequadamente suportados em termos de documentação comprovativa.

VI.2.1.2. ATRIBUIÇÃO E CÁLCULO DE PENSÕES

VI.2.1.2.1. INTEGRIDADE DO PROCESSO

Este processo, tal como definido, requer a existência de uma segregação de funções clara entre o organizador, o conferente e o responsável pelo deferimento do processo (normalmente o Chefe de Secção ou Chefe de Divisão). Assim, nos procedimentos internos do CNP, o deferimento de um requerimento só pode ser efectuado pelo Chefe de Secção/Divisão visto que, por delegação de competências, são eles os únicos possuidores das necessárias competências para o efeito.

Os testes efectuados sobre a amostra dos processos “manuais”, deferidos em 2000, apontaram para uma percentagem significativa de situações onde esta segregação de funções não teria sido respeitada, em virtude de os despachos de deferimento terem sido, aparentemente, exarados por pessoas sem competência para o efeito.

Já em sede de contraditório, o ISSS vem informar que “...*não pode, de modo algum, confirmar-se que haja pedidos de pensão com deferimento efectuado por conferente ou por assistente administrativo especialista*”, referindo que “*Esse “despacho” ou consta directamente do suporte de informação elaborado para cada processo ou consta duma relação elaborada para o efeito e cuja existência o relato constata.*”

Cumprir referir que, no decurso dos trabalhos, em entrevista com responsáveis com competência delegada para o deferimento, estes, confrontados com as situações detectadas, referiram que, não sendo o procedimento usual, essa eventualidade poderia ter ocorrido face à falta ocasional de recursos humanos disponíveis para dar resposta a um volume crescente de processos a tratar. Não foi, na altura, feita referência ao facto de os processos em causa poderem ter sido deferidos por relação.

Em 9% dos casos não se encontraram evidências do despacho proferido pela pessoa competente para o efeito, tratando-se, na maior parte destes casos, de pensões “unificadas”, portanto pensões com parcelas atribuídas pela Caixa Geral de Aposentações (CGA). Note-se que, nos casos em que a CGA é o último regime do beneficiário, e apesar de o deferimento ser por ela efectua-



Tribunal de Contas

efectuado, considera-se ser sempre necessário o parecer conclusivo e vinculativo do CNP sobre a decisão a tomar, relativo à atribuição e pagamento da prestação. Por outro lado, os testes efectuados identificaram que, em 26% dos processos, não existe evidência de que os mesmos tenham sido conferidos pelo chefe da unidade, sendo, segundo os responsáveis do CNP, consequência da falta de recursos humanos especializados para dar resposta a um volume crescente de processos tratados.

A avaliação efectuada do processo de atribuição e cálculo de pensões apontou para os seguintes aspectos que carecem de alguma melhoria:

- A análise dos programas de cálculo revelou que os valores de pensão calculados e registados no ficheiro de pensionistas são gravados por cima dos registos existentes, eliminando o rasto das pensões pagas anteriormente. Por esse motivo, não foi possível validar directamente a pensão calculada anteriormente. Apesar disso, reconhece-se que é possível, ao CNP, identificar o valor anteriormente pago.
- Os programas utilizados para esta actividade não registam os salários omissos da carreira contributiva, que são introduzidos no sistema no acto do cálculo. A futura integração dos salários omissos poderá criar algumas inconsistências, caso os registos das carreiras contributivas recebidos dos centros distritais não coincidam com os valores introduzidos manualmente no cálculo.
- Embora se tenha conseguido simular e comparar a quase totalidade das pensões calculadas informaticamente, encontraram-se algumas situações em que foi necessário o esclarecimento por parte dos responsáveis do CNP. Estas situações resultam da complexidade e variedade de requisitos legais inerentes ao cálculo. Os testes efectuados indicam que o cálculo efectuado pelo sistema funciona correctamente. Considera-se, contudo, que não existe documentação suficientemente detalhada para:
 - discriminar todas as especificidades inerentes ao cálculo; e
 - permitir guardar um rasto adequado das alterações efectuadas.

Se estas especificidades não forem adequadamente documentadas e sistematizadas, poderão originar, no futuro, algumas dificuldades quanto à eficiente transmissão destes conhecimentos sobre os sistemas.

VI.2.1.2.2. INTEGRIDADE DOS CÁLCULOS DE PENSÕES

A maior parte dos cálculos é efectuada automaticamente, com base na informação registada nos sistemas do CNP, existindo, ainda assim, um volume significativo de cálculos “manuais” que, em grande parte dos casos, dizem respeito a pensões que não se enquadram no Regime Geral



Tribunal de Contas

“puro”. Esta situação é indicativa de que o sistema existente no CNP não consegue dar resposta a muitas situações onde o conjunto de legislação a considerar no cálculo da pensão se desvia significativamente do Regime Geral “puro”.

Para confirmar que os cálculos de pensões atribuídas estavam correctos, foi efectuado um recálculo informático das pensões deferidas em 2000. A tipificação das diferenças identificadas neste recálculo resumem-se na tabela abaixo:

Tabela 8 - Resultados do Recálculo das Pensões

Resultado do Recálculo das Pensões	Parcela 01 Pensão Estatutária		Parcela 02 Actualizações	Parcela 11 Complemento Social	Parcela 22 Complemento Dependência 1º Grau	Parcela 42 Complemento Dependência 2º Grau
	Beneficiário Não Pensionista	Beneficiário Pensionista (*)				
Total de Processos	109.135	25.734	38.750	67.211	1.266	472
Dos quais:						
Cálculos sem Diferenças	85,60%	49,93%	50,47%	71,70%	91,5%	93,2%
Cálculos com Diferenças:						
Suspensos	1,30%	7,01%	1,95%	4,09%	8,5%	6,6%
Pensões Especiais	9,09%	2,25%	28,72%	15,97%		
Fora do Regime Geral “puro”:						
Contribuições no Estrangeiro	1,25%	8,97%	13,15%	6,78%		0,2%
Contribuições para a CGA	0,02%	0,20%		0,01%		
Processos “Manuais”	2,70%			0,40%		
Cálculos com Diferenças Não Conciliadas	0,05%	31,64%	5,72%	1,06%	0,0%	0,0%
TOTAIS	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%

(*) Pensões de sobrevivência cujo beneficiário era já pensionista à data de falecimento.

De acordo com os resultados obtidos no recálculo automático das pensões, pertencentes ao Regime Geral “puro”, não se considera que as diferenças detectadas sejam materialmente relevantes.

As diferenças não reconciliadas mais significativas estão relacionadas com pensões de sobrevivência, nas situações em que o falecido (“produtor” da pensão) era já pensionista à data do falecimento. Nestes casos, a pensão é calculada pela mera repartição da pensão existente, que podia ou não ser do Regime Geral, ponderada pelos sobreviventes; não existem dados suficientes nos ficheiros informáticos recebidos para suportar o cálculo das mesmas, sendo apenas efectuado o recálculo dos coeficientes e consequentes valores de pensão, atribuídos aos sobreviventes.

Embora o CNP pretendesse examinar exaustivamente e explicar todas as diferenças detectadas, as limitações de tempo para a execução desta auditoria não permitiram o esclarecimento de todas as diferenças encontradas. Nos testes efectuados, as “diferenças” identificadas resultam de



Tribunal de Contas

pequenas desconformidades no tratamento de arredondamentos. Refira-se que a maioria destas favorece o pensionista.

Relativamente a esta matéria, o ISSS veio, no exercício do direito de contraditório, esclarecer que *“Dado que o recálculo das pensões de sobrevivência, de beneficiários falecidos na situação de pensionistas, foi efectuado com base nos salários introduzidos para cálculo do Subsídio por Morte em vez da utilização da pensão do produtor, cujo montante se encontra devidamente actualizado, os resultados tiveram que ser obviamente diferentes...”*

Na análise das outras diferenças encontradas, observou-se a existência de situações onde os dados existentes sobre a carreira contributiva, nos sistemas e nos ficheiros recebidos, eram insuficientes para suportar o valor da pensão deferida. A identificação de diferenças nestes casos pode ter a sua origem nas pensões com referência a países estrangeiros ou a pensões cujo beneficiário apresentou contribuições para a CGA. Estes casos foram identificados por:

- código de país, no caso das pensões cujos beneficiários fizeram contribuições no estrangeiro;
- código de parcela específico (87), no caso das pensões cujos beneficiários efectuaram descontos para a CGA; e
- código de suspensão, no caso de pensões suspensas, por motivos vários, à data da extracção dos dados.

Nestes casos, as diferenças detectadas entre os recálculos efectuados e os valores processados pelo CNP foram identificadas, mas não foi possível assegurar que essas diferenças fossem exclusivamente provenientes destes factores.

Quanto aos processos manuais, os erros detectados nos cálculos de pensões tinham por base, fundamentalmente: os designados “erros por simpatia”; deficiente aplicação de factores definidos em tabelas práticas; ou deficiente contagem da carreira contributiva, não derivando, na esmagadora maioria, de um incorrecto entendimento do processo e da legislação. Nos 394 processos analisados detectaram-se 14 erros de cálculo, o que corresponde a cerca de 3,5% da amostra analisada. A tipificação destas ocorrências consta no **Anexo D – Diferenças Detectadas nos Cálculos Manuais**.

Dos catorze erros detectados apenas os relativos a seis casos tiveram como efeito que fossem pagas pensões cujo valor é superior ao efectivamente devido, requisito necessário ao preenchimento da figura de “pagamentos indevidos”, prevista no art. 59.º da Lei n.º 98/97, de 26 de Agosto.



Tribunal de Contas

A violação desta norma consubstancia a prática de uma infracção financeira, uma vez que se tratam de pagamentos ilegais, que, por não ter havido contraprestação efectiva, causaram dano para o Estado, nos termos do n.º 2 do supra citado artigo.

Havendo, eventualmente, lugar a responsabilidade financeira reintegratória, nos termos do n.º 1 do art.º 61.º da mesma lei; salienta-se, no entanto, que se tratam de montantes baixos que decorreram de meros erros de cálculo, que parecem afastar a culpa do responsável, conforme o disposto no n.º 5 do art. 61.º da mesma Lei.

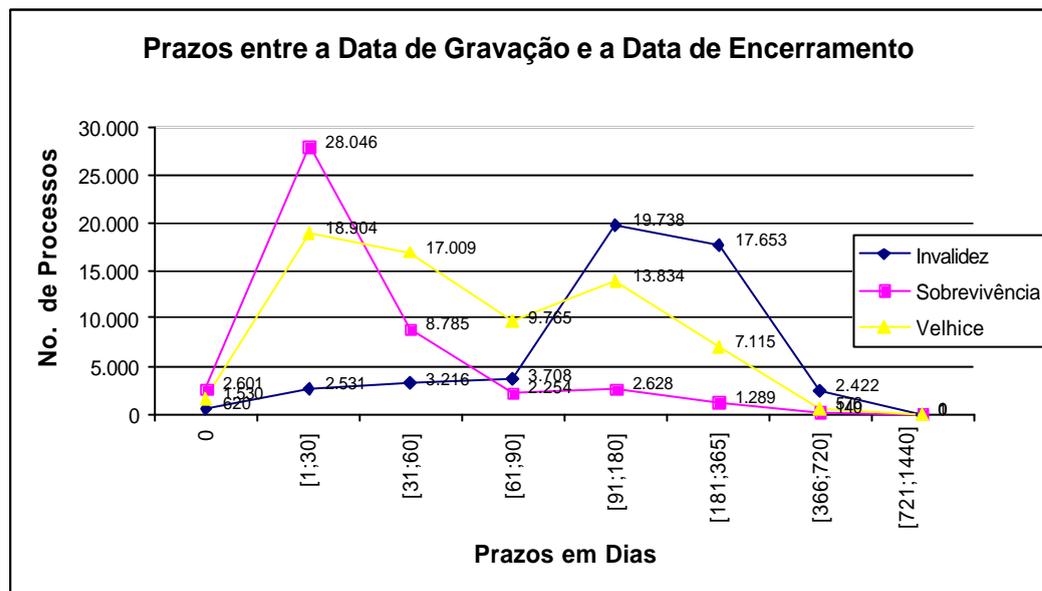


Tribunal de Contas

VI.2.1.2.3. EFICIÊNCIA DO PROCESSO

Como parte da análise deste processo avaliou-se os prazos médios de deferimento dos processos, observando-se a seguinte situação:

Gráfico 10 - Prazos entre a Data de Gravação e a Data de Encerramento



A avaliação efectuada à eficiência deste processo demonstrou que os prazos de deferimento das pensões estão directamente relacionados com a natureza do requerimento. O gráfico anterior confirma que o ISSS demora, em média, cerca de 30 dias para deferir um requerimento para atribuição de uma pensão de sobrevivência. Este prazo poderá ser justificado por, no caso de requerimentos deste tipo de pensão, a maior parte da informação necessária já existir nos sistemas do CNP, associada à pensão de velhice paga ao beneficiário antes deste falecer. Um requerimento para uma pensão de invalidez demora, em média, mais de 90 dias até ser deferido. Este prazo está directamente relacionado com o período de espera pela Certidão de Invalidez, emitida pelo CVIP. O prazo necessário ao deferimento de uma pensão de velhice pode estender-se de um mês a um ano. Considera-se que as causas prováveis para esta extensão do prazo estejam relacionadas com o envio, por parte dos CDSSS, de quantidades significativas de processos incompletos, em termos de carreira contributiva, e com a existência de variados pensionistas com rendimentos no estrangeiro, implicando a obtenção de comprovativos junto de entidades externas.



Tribunal de Contas

VI.2.1.3. PROCESSAMENTO E PAGAMENTO DE PENSÕES

VI.2.1.3.1. INTEGRIDADE DO PROCESSAMENTO DE PENSÕES

A integridade do processamento de pensões está directamente relacionada com a capacidade do CNP em gerir o volume de alterações que requerem um controlo adequado para assegurar a exactidão das pensões pagas. Estas alterações podem ser divididas em duas grandes categorias:

➤ **Alterações introduzidas por legislação**

As alterações introduzidas por legislação podem resultar das seguintes situações:

- actualização anual ou específica das pensões;
- introdução de novos regimes ou categorias de pensão; e
- alteração das regras de aplicação de um regime existente.

As actualizações anuais ou pontuais dos valores das pensões são suportadas por programas que as executam de forma quase automática. Verificou-se que a maioria das alterações são testadas e validadas pela Unidade Informática do CNP, sem recurso aos elementos das outras Unidades. Salienta-se, no entanto, que não foram encontrados indícios de que tenham existido problemas na execução desta actividade no passado, resultado, em grande medida, do significativo esforço efectuado pelo CNP nesta área.

➤ **Alterações aos dados inerentes ao processo**

A alteração dos dados inerentes a uma pensão resulta, por um lado, no seu recálculo e, por outro, no cálculo dos valores atrasados inerentes às referidas alterações. O pagamento dos valores em atraso deriva, muitas vezes, de situações onde o direito à pensão foi reconhecido, mas, em consequência de informação omissa, não foi possível determinar, num primeiro momento, o valor real da pensão à qual o beneficiário tinha direito, sendo a diferença posteriormente reposta. Este procedimento, protegendo o pensionista ao conceder-lhe uma pensão assim que lhe é reconhecido o direito à mesma, é resultado, em muitos casos, de atrasos administrativos a que este é alheio.

Em face do atrás descrito, diligenciou-se no sentido de efectuar testes à actualização dos cálculos das pensões. Constatou-se, porém, a existência de um obstáculo à sua realização, dada a impossibilidade de estabelecer, no final de 2000, a data efectiva da última actualização do cálculo das pensões; isto, porque o programa de cálculo substituiu os valores anteriormente registados no



Tribunal de Contas

ficheiro de pensionistas cada vez que um cálculo/recálculo é realizado. O sistema actual regista a existência de uma alteração efectuada a uma pensão mas não regista o detalhe suficiente para estabelecer o seu conteúdo. Ainda assim, os testes efectuados não indicaram quaisquer situações onde as alterações às pensões tivessem resultado em erros nas pensões pagas.

VI.2.1.3.2. EFICIÊNCIA DO PROCESSAMENTO DE PENSÕES

A introdução de novos regimes de pensão e a alteração das regras de aplicação de um regime existente podem resultar em novos programas de cálculos da pensão. Dado que a filosofia dos programas desenvolvidos não oferece muita flexibilidade em termos da sua parametrização, qualquer alteração desta natureza pode exigir um esforço significativo de programação para dar efeito a uma alteração legislativa no cálculo de uma pensão.

Este aspecto é agravado com os atrasos na comunicação de alterações legislativas, os prazos estabelecidos para a implementação das alterações daí resultantes e a natureza dos seus impactes sobre os programas existentes, que dificultam, por vezes, o processo, resultando num maior risco da não detecção atempada de problemas ou erros de cálculo.

VI.2.1.3.3. INTEGRIDADE DO PROCESSO DE PAGAMENTO

Historicamente, a maioria dos pagamentos de pensões tem sido efectuada através de vales de correio. Esta tendência irá, provavelmente, ser invertida, havendo, por parte do ISSS, um esforço substancial na promoção dos pagamentos por transferência bancária directa, não só por se tratar de uma forma mais expedita e segura de efectuar os pagamentos, como por razões de natureza financeira, já que o pagamento por vales de correio é mais dispendioso.

O CNP não tem, neste momento, capacidade de confirmar, de forma sistemática, que os pagamentos de pensões efectuados pelos bancos são de facto recebidos pelos beneficiários. Este aspecto é muito importante para assegurar que o CNP não está a pagar pensões indevidas a beneficiários já falecidos e para assegurar que não foi debitado duas vezes o mesmo pagamento. No caso de beneficiários falecidos, o CNP recebe, do Ministério da Justiça, uma banda com registos de falecimentos, mas não tem capacidade de efectuar o cruzamento dessa informação com base num Número de Bilhete de Identidade ou um Número de Contribuinte, o que não facilita a sua identificação, resultando esta situação na incapacidade de, atempadamente, controlar os pagamentos efectuados indevidamente aos mesmos.

Os pagamentos efectuados pelos bancos, bem como as devoluções recebidas, são reconciliados contabilisticamente. Na análise das reconciliações bancárias constatou-se que os registos contabi-



Tribunal de Contas

contabilísticos são registados somente no fim do mês, criando uma situação onde só é possível estabelecer a posição contabilística correcta dos bancos centralizadores, também, no fim do mês.

VI.2.1.3.4. EFICIÊNCIA DO PROCESSO DE PAGAMENTO

Dado que, por um lado, não existe a possibilidade de integrar os ficheiros de extracto de conta bancária e, por outro, subsiste uma grande dificuldade em identificar pensões individuais devolvidas, sucede:

- uma carga administrativa adicional significativa com a imputação desta informação;
- um desfasamento de dois meses, em média, na reconciliação das contas bancárias; e
- uma lista de pendentes significativa em cada mês.

VI.2.2. Processos de Gestão de Sistemas de Informação

Os resultados da avaliação efectuada dos processos de gestão de sistemas de informação apontaram para a existência de realidades muito distintas neste plano. Em termos da realidade encontrada, o processo de Planeamento e Estratégia de Sistemas de Informação é da inteira responsabilidade do IIES. As responsabilidades de gestão dos processos de Aquisição e Desenvolvimento de Soluções de TI e Operação dos Ambientes de TI são partilhados entre o IIES, o CNP e os CDSSS, que têm um papel fundamental na manutenção e operação dos sistemas existentes. O processo de Monitorização de Processos de TI ainda não está formalmente definido como sendo da responsabilidade do IIES ou de qualquer outra entidade do SSSS.

Por outro lado, nem todos os processos de gestão de sistemas de informação existiam na realidade do SSSS. A tabela apresentada abaixo espelha a cobertura dos processos de gestão de sistemas de informação, propostos pelo modelo CobIT, pelas entidades do SSSS enquadradas no âmbito deste trabalho.



Tribunal de Contas

Tabela 9 - Cobertura dos Processos de Gestão de TI pelos Organismos do SSSS

Processo	Descrição da Actividade	IIES	CNP	CDSSS
Planeamento e Estratégia de Sistemas de Informação				
	Definição da Estratégia de TI	v		
	Definição de uma Arquitectura de Informação	v		
	Definição da Direcção Tecnológica de TI	v		
	Definição da Organização de TI e outras Interdependências	v	v	v
	Gestão dos Investimentos em TI	v		
	Comunicação das Orientações Estratégicas	v		
	Gestão dos Recursos Humanos	v	v	v
	Cumprimento de Requisitos Externos	v	v	v
	Avaliação de Riscos de TI	v	v	v
	Gestão dos Projectos em Curso	v	v	v
	Gestão da Qualidade	v		
Desenvolvimento e Implementação de Soluções				
	Identificação de Soluções	v		
	Aquisição e Manutenção de Aplicações	v	v	v
	Aquisição e Manutenção da Arquitectura Tecnológica	v		v
	Desenvolvimento e Manutenção de Procedimentos de TI	v	v	v
	Instalação e Certificação de Sistemas			
	Gestão da Mudança	v		
Operação dos Ambientes de TI				
	Definição dos Níveis de Serviço			
	Gestão dos Serviços Prestados por Terceiros	v	v	v
	Gestão da <i>Performance</i> e da Capacidade	v	v	v
	Assegurar a Continuidade dos Serviços Prestados	v	v	v
	Assegurar a Segurança dos Sistemas	v	v	v
	Identificação e Afectação dos Custos			
	Prestação de Apoio e Formação aos Utilizadores	v		
	Apoiar e aconselhar os Clientes			
	Gestão da Configuração			
	Resolução e Gestão de Problemas de TI	v	v	v
	Gestão dos Dados	v	v	v
	Gestão das Instalações Físicas	v	v	v
	Gestão das Operações	v	v	v
Monitorização dos Processos de Gestão de TI				
	Monitorização dos Processos de TI			
	Avaliação do Controlo Interno de TI			
	Certificação de Serviços e Sistemas			
	Execução de Auditorias Independentes.			



Tribunal de Contas

Em termos da realidade encontrada, existem várias actividades que ainda estão por ser implementadas, algumas das quais são importantes para colmatar riscos associados aos sistemas de informação do SSSS. De seguida apresenta-se um resumo dos resultados obtidos em cada uma das actividades abordadas.

VI.2.2.1. PLANEAMENTO E ESTRATÉGIA DE SISTEMAS DE INFORMAÇÃO

VI.2.2.1.1. DEFINIÇÃO DA ESTRATÉGIA DE SISTEMAS E TECNOLOGIAS DE INFORMAÇÃO

Na avaliação do Processo de Definição da Estratégia de Sistemas e Tecnologias de Informação, identificaram-se três riscos significativos, a saber:

➤ **A Estratégia do Legislador versus a Estratégia de Sistemas de Informação**

A estratégia de sistemas de informação de qualquer Organização depende directamente e deve estar sempre alinhada com a estratégia de “negócio”. A estratégia de sistemas de informação, definida pelo IIES, depende directamente dos objectivos estabelecidos pela legislação em vigor, podendo sofrer alterações periódicas consoante as orientações políticas que afectem, directa ou indirectamente, a estratégia de “negócio” do SSSS. Este fenómeno obriga a que a execução da estratégia de sistemas de informação esteja sempre atrasada face às necessidades estabelecidas pelo Estado. A redução do desfasamento temporal entre as necessidades estabelecidas pelo Estado e a implementação de sistemas que dêem resposta a essas necessidades é, muitas vezes, um factor crítico para o alcance atempado dos objectivos estabelecidos. Assim, considera-se que a efectiva implementação da estratégia de sistemas de informação contribuiria fortemente para uma significativa melhoria do SSSS, designadamente nos seguintes aspectos:

- qualidade dos serviços prestados ao público;
- maior eficácia do sistema;
- melhor planeamento financeiro dos recursos;
- redução dos custos de administração do sistema;
- maior confiança na informação produzida pelos sistemas de informação.

O IIES e o CNP têm acompanhado a evolução da legislação e têm avaliado os impactes da mesma na sua estratégia e nos seus sistemas de informação. No entanto, afigura-se que este acompanhamento é, por vezes, posterior à publicação das alterações legislativas. Existe, por isso, o risco de os impactes sobre os sistemas de informação do SSSS, relativos às



Tribunal de Contas

alterações à legislação, não serem devida e atempadamente considerados antes da sua entrada em vigor.



Tribunal de Contas

➤ **Actualização da Estratégia de Sistemas de Informação**

O SSSS encontra-se numa fase de tomada de decisões estratégicas sobre investimentos de longo prazo em tecnologias de informação. É fundamental que, para tal, haja uma clara definição da estratégia de sistemas de informação a médio prazo, para assegurar que os investimentos efectuados em projectos anuais de sistemas de informação sejam os mais adequados e estejam de acordo com os objectivos a médio/longo prazo definidos para o SSSS. A linha geral destas estratégias não tem mudado significativamente desde 1998, mas as políticas para a sua execução têm sido ajustadas por cada Conselho Directivo do IIES. Constatou-se que o plano existente, datado de 1998, poderá requerer uma actualização para reflectir as novas decisões entretanto tomadas, considerando-se, por outro lado, fundamental a existência de uma clara definição dos prazos e das prioridades da estratégia de sistemas de informação e a sua actualização periódica, sem a qual é difícil avaliar, de modo independente, em que medida estas estão a ser alcançadas e se os recursos e os prazos necessários para atingir os objectivos estabelecidos são adequados.

Em sede de contraditório, o IIES informa que só será possível clarificar e definir a estratégia dos sistemas de informação a médio e curto prazo após a constituição formal do Conselho Consultivo, embora tenha vindo a efectuar os indispensáveis levantamentos que servirão de base a todo este processo.

➤ **Horizonte Temporal da Estratégia de Sistemas de Informação**

A transformação e a informatização de qualquer sistema com a dimensão e complexidade do SSSS exigem um horizonte temporal alargado. Para assegurar a qualidade e a integridade desta transição, é necessário assegurar que:

- os requisitos dos processos existentes sejam adequadamente considerados no desenvolvimento dos novos sistemas; e
- a interpretação das especificidades dos dados históricos garanta uma transição correcta para os novos sistemas.

VI.2.2.1.2. DEFINIÇÃO DA ARQUITECTURA DE INFORMAÇÃO

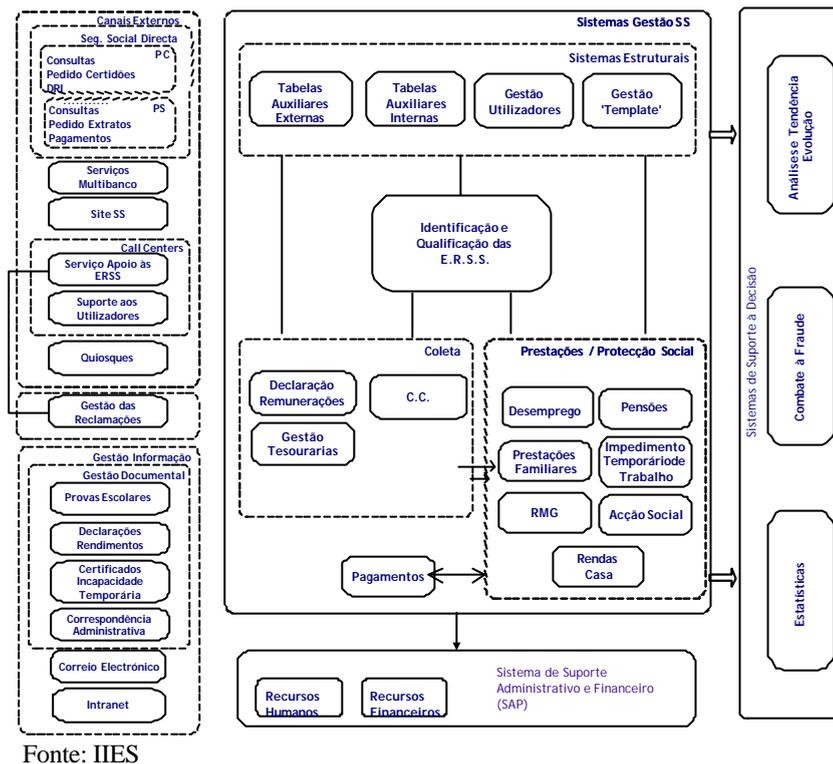
A arquitectura de informação existente no SSSS resulta de uma variedade de sistemas, com modelos de dados diferentes, de acordo com a plataforma tecnológica implementada ao longo dos anos nos vários centros distritais e no CNP. A realidade da arquitectura de sistemas de informação existente é representativa de ilhas de informação com pouca ou nenhuma interligação



Tribunal de Contas

entre os vários sistemas e com interpretações diferentes da informação gerida. O IIES está consciente dos problemas associados a esta realidade e está a tomar passos concretos no sentido de definir uma arquitectura de informação integrada e abrangente que cubra todo o SSSS.

Arquitectura Global do Sistema Informação



Fonte: IIES

A arquitectura global de sistemas de informação, acima apresentada e proposta pelo IIES, requer uma significativa reformulação da existente, para que o SSSS consiga:

- dar resposta às necessidades de informação, cada vez mais exigentes;
- melhorar a qualidade dos serviços prestados ao público português;
- melhorar a qualidade da informação sobre o SSSS; e
- disponibilizar sistemas de suporte à decisão, transversais aos sistemas operacionais do SSSS.

Dado que muitas das aplicações inerentes a esta arquitectura ainda não foram desenvolvidas ou estão, actualmente, em desenvolvimento, os modelos de dados subjacentes ainda não se encontram finalizados. A classificação de informação, em termos de categorias de segurança, também ainda não foi totalmente definida.

A arquitectura de sistemas de informação proposta pelo IIES pretende centralizar a informação do SSSS onde possível, alargando a sua disponibilização a todas entidades, através de uma rede



Tribunal de Contas

informática nacional. De sublinhar, relativamente a esta matéria, uma acrescida preocupação por parte dos responsáveis do IIES no sentido de se assegurar a integridade da informação a transitar para os novos sistemas.

VI.2.2.1.3. DEFINIÇÃO DA DIRECÇÃO TECNOLÓGICA DE TI

Até recentemente, as entidades do SSSS tinham alguma liberdade para escolher as plataformas tecnológicas que pretendiam implementar, resultando daí que a direcção tecnológica não fosse definida de forma consistente, o que acarretou as seguintes consequências:

- um investimento significativo em tecnologias e recursos humanos sem o benefício de economias de escala, dada a diversidade de plataformas;
- ineficiências na modificação e manutenção de sistemas, pelo mesmo motivo; e
- incompatibilidades entre plataformas, dificultando a integração da informação e criando um esforço administrativo adicional.

Entretanto, o IIES tem vindo a ganhar uma influência cada vez maior nesta actividade, começando a ter uma intervenção mais directa na negociação e compra de novos sistemas e soluções tecnológicas e na integração dos mesmos, sendo esta intervenção particularmente evidente na recente implementação das redes informáticas que visam a interligação dos vários sistemas do SSSS.

VI.2.2.1.4. DEFINIÇÃO DA ORGANIZAÇÃO DE TI E SUAS INTERDEPENDÊNCIAS

A prestação dos serviços de TI está a ser realizada por cada uma das entidades do SSSS, existindo, em cada CDSSS e no CNP, um serviço ou unidade responsável pelos serviços de sistemas de informação que suportam as suas plataformas tecnológicas. O IIES, como entidade coordenadora, assume responsabilidade pelas infra-estruturas de redes e pelas infra-estruturas que suportam as novas plataformas.

Existe uma definição mínima de responsabilidades dos recursos humanos, nas várias entidades visitadas mas, em certas áreas (como, por exemplo, a gestão de redes), persiste alguma incerteza das responsabilidades partilhadas entre o IIES, os vários CDSSS e o próprio CNP. Há uma consciência da necessidade de reformular a estrutura organizacional de TI no ISSS, reconhecendo-se que a estrutura existente está demasiadamente fragmentada, adveniente de abordagens de gestão que variam de entidade para entidade. Com a centralização de sistemas será necessário, também, ponderar a abordagem mais adequada para a prestação de serviços de processamento de dados, bem como o apoio necessário aos utilizadores nas várias entidades do SSSS.



Tribunal de Contas

Nas suas alegações, o IIES veio acrescentar que: “... *é responsável pela totalidade da chamada “Rede Nacional de Dados da Segurança Social”, faz a sua monitorização de forma centralizada, detectando qualquer anomalia que se verifique na comunicação em qualquer ponto da rede, desde os “routers” locais até aos “nós” centrais. Actualmente, está a ser implementada uma ferramenta adicional que permitirá a monitorização das redes locais incluindo estações e impressoras padrão.*”

Quando considerada útil, a informação de monitorização pode e é disponibilizada ao ISSS e ao IGFSS”.

VI.2.2.1.5. GESTÃO DOS INVESTIMENTOS EM TI²²

A maioria dos grandes investimentos recentemente efectuados em TI implicou a subcontratação de serviços externos, estruturados em projectos específicos. Existem procedimentos de controlo orçamental para controlar desvios entre as despesas reais e as orçamentadas nos projectos em curso. A definição de orçamentos para projectos é feita caso a caso, com fundamento em propostas e orçamentos de fornecedores e prestadores de serviços, que servem de base para a justificação do custo dos projectos, sendo a justificação dos benefícios, na maioria dos casos, qualitativa, dado que a sua medição é difícil e complexa.

VI.2.2.1.6. COMUNICAÇÃO DAS ORIENTAÇÕES ESTRATÉGICAS

A responsabilidade pela definição de políticas de segurança tem sido partilhada entre o IIES e os vários CDSSS, tendo-se constatado, ainda assim, a inexistência de políticas consistentes e homogéneas nas várias entidades que compõem o SSSS, o que resulta em planos de segurança que variam de local para local. Embora não haja uma definição única das políticas e procedimentos de sistemas de informação para o SSSS, existe alguma documentação dos procedimentos de gestão e segurança de sistemas de informação para o IIES, o CNP e os CDSSS.

As políticas de administração de sistemas encontradas já contemplam alguns procedimentos de *backup* e protecção de dados, mas existem ainda várias áreas em que estas políticas necessitam de ser definidas e implementadas; por outro lado, existe pouca informação concreta sobre a implementação das políticas estabelecidas para as várias plataformas do SSSS e poucos mecanismos de monitorização para assegurar a conformidade com as políticas existentes. Tem-se efectuado, no âmbito do SSSS, alguns esforços para formalizar as políticas de segurança de

²² Esta vertente foi analisada, exclusivamente, na perspectiva e segundo os desígnios e necessidades do modelo CobIT, pelo que não foram adoptados procedimentos no sentido da verificação da legalidade, regularidade e correcção financeira dos contratos analisados para esse efeito.



Tribunal de Contas

sistemas de informação, estando a reavaliar-se, face à sua realidade tecnológica, não só as políticas, como os próprios procedimentos actualmente existentes. Enquanto decorria este trabalho, o IIES tinha em curso um projecto de segurança visando suprimir as carências existentes nesta área, aguardando-se, a curto prazo, a sua aceitação formal por parte dos utilizadores.

VI.2.2.1.7. GESTÃO DOS RECURSOS HUMANOS

O SSSS tem uma longa tradição na utilização de sistemas de informação e, em várias áreas, foi pioneiro na informatização dos serviços do Estado; no entanto, estes avanços tecnológicos não têm sido devidamente sustentados com o desenvolvimento contínuo dos recursos humanos afectos a esta área, criando uma situação de grande carência de conhecimentos em várias áreas relacionadas com as tecnologias de informação mais recentes.

O crescimento explosivo, nos anos 90, das tecnologias de sistemas de informação reduziu, progressivamente, a capacidade do SSSS para atrair e reter funcionários com um nível de conhecimentos informáticos adequados para sustentar a sua modernização. A responsabilidade pela gestão dos recursos humanos necessários para suportar sistemas e tecnologias de informação está partilhada entre as várias entidades que integram o ISSS. A constituição do IIES e a subcontratação de serviços de desenvolvimento e implementação de serviços têm colmatado alguns problemas nesta matéria, mas o problema continua a ser importante para as outras entidades que integram o SSSS. Dadas as especificidades dos sistemas desenvolvidos, o SSSS continua dependente de funcionários que detêm o conhecimento histórico dos sistemas e dos seus dados, sendo que o risco que advém desta dependência é substancialmente acrescido se tivermos em conta a idade média destes técnicos. Constatou-se, por outro lado, que não existe um plano de desenvolvimento de recursos humanos que prepare os recursos existentes para responder às necessidades dos futuros sistemas do SSSS.

Esta realidade tem criado situações em que não existem recursos humanos suficientes para dar resposta às necessidades de controlo de qualidade de sistemas e informação, bem como para providenciar uma adequada segregação de funções nos serviços de sistemas de informação das várias entidades, tendo-se verificado situações em que:

- os serviços de sistemas de informação são os “donos” efectivos dos sistemas, dado que nem sempre existe uma clara definição e separação de responsabilidades entre os utilizadores dos sistemas e os serviços informáticos;
- não existe uma segregação de funções entre a gestão de desenvolvimentos, a gestão de dados e a segurança dos sistemas;
- nas matérias de segurança de sistemas de informação, nem sempre existe uma clara definição de políticas e responsabilidades.



Tribunal de Contas

O recrutamento e promoção dos funcionários pertencentes aos vários serviços de sistemas de informação seguem os procedimentos adoptados pelo ISSS, com a excepção do IIES, que apresenta uma maior flexibilidade na contratação dos seus recursos humanos. Afigura-se não existir uma definição formal, pelo ISSS, das competências para suportar os sistemas de informação existentes e futuros, sendo, neste sentido, difícil de avaliar e identificar as necessidades de recrutamento ou de formação interna, o que resulta na necessidade de subcontratação de serviços e, assim, numa baixa utilização dos recursos existentes. Existem, pontualmente, necessidades específicas de formação, normalmente associadas à introdução de novos sistemas ou de alterações significativas aos existentes, para as quais são disponibilizadas verbas. Por outro lado, como consequência da introdução desses novos sistemas e tecnologias, tem surgido a necessidade de desenvolver competências nas áreas de gestão de redes e administração de sistemas e bases de dados, o que implica o aumento do nível de literacia informática necessária a um bom desempenho por parte dos utilizadores do ISSS.

A introdução dos novos sistemas previstos na estratégia de sistemas de informação avançada pelo IIES resultará numa situação em que as competências existentes nos serviços de sistemas de informação das várias entidades pertencentes ao SSSS estarão desajustadas, face às necessidades das novas tecnologias introduzidas, implicando a necessidade de que a estratégia traçada seja complementada com um Plano de Recursos Humanos que actualize os conhecimentos e competências existentes para poderem ser enquadrados na futura organização de sistemas de informação. Neste momento, muitos destes detalhes ainda estão por definir. Não existe, também, uma política clara sobre a rotação de tarefas e funções para assegurar a polivalência dos informáticos do ISSS.

Existem alguns procedimentos que asseguram a disponibilidade de elementos críticos para o funcionamento dos sistemas mais importantes; ainda assim, o SSSS está vulnerável aos impactes provocados pela eventual saída de funcionários chave dos vários serviços informáticos.

De facto, o SSSS enfrenta, neste momento, um desafio significativo relativamente à idade média dos seus quadros, começando muitos deles, a curto prazo, a entrar na idade de reforma. Esta situação é tão mais relevante quanto a estratégia definida, e hoje existente, poderá não ter ponderado a resolução atempada deste problema.

O IIES informou, nas suas alegações, que *“...tomou a iniciativa reunir com os interessados, de forma a que os mesmos sejam ouvidos e apresentem sugestões com vista à elaboração dum plano estratégico de recursos humanos da área informática. Em termos de preparação básica destes recursos, o IIES tem mesmo previsto, no seu plano de actividades para 2002, acções de formação vocacionadas para sistemas abertos.”*

VI.2.2.1.8. CUMPRIMENTO DE REQUISITOS EXTERNOS



Tribunal de Contas

Acrescendo à, já de si complexa, teia legal que envolve o universo em causa, as alterações legislativas ou o surgimento de nova legislação subjacente ao SSSS podem ter impactes profundos nos sistemas informáticos existentes, implicando a necessidade de efectuar desenvolvimentos aos seus programas para dar resposta às modificações ou novidades introduzidas. O CNP dispõe de uma Unidade Jurídica que interpreta os requisitos estabelecidos pela legislação, de modo a que se efectuem, correctamente, os desenvolvimentos ou alterações aos programas que forem afectados; no entanto, essas alterações legislativas exigem, por vezes, o registo ou processamento de elementos de informação que podem, ou não, existir nos actuais modelos de dados. Reconhece-se, assim, que o sucesso desta actividade é fundamental, não só para a atribuição e controlo de pensões, mas para todo o SSSS.

Neste momento, o cumprimento funcional das aplicações face às Leis da Segurança Social constitui a preocupação principal dos serviços de sistemas de informação, considerando-se, assim, importante alertar para a existência de outra legislação relacionada com sistemas de informação que também terá relevância para o SSSS: as Leis de Protecção de Dados, de Protecção de *Software* e da Criminalidade Informática.

Como o ISSS, através do CNP, processa dados pessoais referentes aos pensionistas do país, as bases de dados do CNP requerem o seu registo perante a Comissão Nacional para a Protecção de Dados. Esse registo foi já efectuado junto desta Comissão. As medidas especiais de segurança, estabelecidas no art.º 15.º da Lei de Protecção de Dados, são aplicáveis se uma entidade processa dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo dados genéticos. Com base nos dados existentes nos sistemas do CNP, considera-se que esta entidade tem responsabilidades acrescidas nos termos desta lei, dado que os seus sistemas de informação guardam e processam informação relacionada com o estado de saúde dos beneficiários.

Face a estas exigências, considera-se que existem alguns aspectos dos sistemas informáticos de controlo e pagamento de pensões que podem pôr em risco o cumprimento destes requisitos, nomeadamente:

- o sistema de autenticação do CNP efectua a validação do acesso aos dados de um requerimento com base na transacção executada. Verificou-se que muitas das transacções de consulta aos dados não requerem uma autenticação do utilizador, podendo pôr em causa a confidencialidade da informação de um beneficiário. Reconhece-se, ainda assim, que o acesso a esta informação requer a entrada num terminal com o devido emulador instalado;
- a transmissão de dados não é *encriptada* entre o sistema do CNP e os clientes de rede nem no seu transporte em bandas. Existem, também, troços da rede do ISSS que utilizam ligações via satélite. Dada a dimensão da rede, há sempre o risco de que o tráfego nas redes do ISSS possa ser escutado, comprometendo, assim, a confidencialidade dos dados por si geridos.



Tribunal de Contas

Nas alegações produzidas, o IIES informa, quanto à protecção dos dados detidos pelo SSSS, que “...*encetou diligências no sentido de providenciar a legalização dos mesmos, a nível da segurança social, em detrimento da abordagem por instituição*”.

Em relação à segurança na transmissão dos dados, confirma que “... *existe de facto o risco potencial de o tráfego na RNSS poder ser escutado, tal como existe em todas as redes sobre infra-estruturas de operadores públicos, pelo que estão a ser desenvolvidos projectos que visam melhorar a segurança da Rede, nomeadamente através da inclusão de mecanismos de encriptação e outros.*”

VI.2.2.1.9. AVALIAÇÃO DOS RISCOS DE TI

Esta actividade existe no ISSS, mas de forma muito limitada, não fazendo parte da metodologia de gestão global de sistemas de informação adoptada pelos serviços de sistemas de informação que integram o SSSS. Ainda assim, verificou-se que a análise de risco é efectuada formalmente, pelo IIES, ao nível de projectos de grande envergadura. Por outro lado, constatou-se que, relativamente aos projectos de preparação dos sistemas para o EURO, houve uma preocupação de incluir uma componente formal de avaliação de riscos, tendo esta sido discutida com os vários intervenientes no projecto e os riscos, identificados pró activamente, monitorizados para assegurar o sucesso.

Como referido, a avaliação de risco, como uma prática global abrangendo todos os sistemas e tecnologias do ISSS, ainda não é comum. A falta de políticas e procedimentos de segurança, baseados numa avaliação de riscos de sistemas de informação, não foi, ainda, definida. Considera-se, assim, que uma avaliação de riscos dos sistemas do ISSS, complementada por políticas e procedimentos de segurança, é importante no sentido da optimização dos investimentos realizados em mecanismos de controlo e segurança, nas áreas de maior risco para o ISSS. A conformidade com as políticas e procedimentos ainda por estabelecer deve ser suportada com auditorias realizadas para este efeito.

VI.2.2.1.10. GESTÃO DOS PROJECTOS EM CURSO

Constatou-se, aquando da avaliação desta actividade, que existem duas realidades distintas: a do CNP e a do IIES. O CNP gere e executa todos os seus projectos de sistemas de informação internamente, definindo as suas prioridades e o seu calendário de desenvolvimentos. Por outro lado, a maioria dos projectos de grande envergadura fora do CNP (como foi o caso da transição para o EURO), geridos pelo IIES no último ano, foram objecto de subcontratação a entidades



Tribunal de Contas

externas, dada a dimensão e complexidade dos trabalhos a efectuar, tendo a sua prioritização sido estabelecida pelo respectivo Conselho Directivo e, com excepção do CNP, o acompanhamento partilhado entre esta entidade, os CDSSS que representavam cada plataforma e a entidade subcontratada.

A subcontratação destes projectos foi sujeita à definição de um plano de implementação pelas entidades subcontratadas, com prazos adequadamente definidos, tendo a metodologia de gestão dos projectos variado conforme a entidade externa envolvida. Considera-se que, nos projectos analisados, houve uma metodologia de gestão razoavelmente definida, sendo, na maioria dos casos, os riscos financeiros inerentes, em parte, transferidos para os prestadores de serviços e, por outro lado, contemplada a gestão de riscos associados aos atrasos dos projectos ou incumprimento de expectativas. Neste sentido, o ISSS demonstrou uma grande preocupação com a gestão dos projectos em curso na área de sistemas de informação, implementando as medidas necessárias para assegurar o cumprimento dos prazos estabelecidos. A conformidade atempada do SSSS com o EURO demonstrou o esforço investido nesta actividade.

VI.2.2.1.11. GESTÃO DA QUALIDADE

Não está formalmente estabelecido um processo de gestão da qualidade para os serviços de sistemas de informação prestados mas, dada a dimensão dos serviços/unidades de sistemas de informação nos vários CDSSS, não seria viável ter esta função operacional em cada CDSSS. A gestão da qualidade de projectos varia de projecto para projecto, embora se tenha observado, nos projectos analisados, a existência de procedimentos mínimos de teste com o objectivo de assegurar a qualidade das funcionalidades implementadas. Constatou-se, na avaliação dos projectos, que a sua gestão não tinha como objectivo a retenção de evidências que demonstrassem a execução dos procedimentos de testes efectuados ou dos procedimentos de controlo de qualidade executados.

Na avaliação desta actividade, não foi possível identificar a definição formal dos requisitos mínimos de qualidade nem as métricas consistentes para demonstrar o seu funcionamento, tendo-se, no entanto, encontrado evidência de que estes foram efectuados. Existem abordagens distintas relativamente ao envolvimento de utilizadores no processo de gestão da qualidade dos projectos implementados. No caso do CNP, as responsabilidades de gestão de qualidade estão concentradas na Unidade Informática, enquanto que, em outros projectos analisados, existe alguma intervenção de utilizadores chave nos processos de gestão de qualidade dos sistemas desenvolvidos ou alterados. Em certos casos, a falta do envolvimento dos utilizadores finais não permite a segregação efectiva de funções para garantir que as alterações efectuadas respeitam os mínimos de qualidade estabelecidos.



Tribunal de Contas

VI.2.2.2. PROCESSO DE AQUISIÇÃO E DESENVOLVIMENTO DE SISTEMAS

VI.2.2.2.1. IDENTIFICAÇÃO DE SOLUÇÕES

Esta actividade é uma das responsabilidades do IIES, dado que esta entidade é responsável pela implementação da nova arquitectura de sistemas prevista para o SSSS. Dadas as necessidades especiais do ISSS, em termos das funcionalidades inerentes às novas aplicações, o IIES tem apostado no desenvolvimento de soluções “personalizadas” para dar resposta às necessidades do SSSS para os sistemas de identificação e qualificação de beneficiários e contribuintes. No caso dos sistemas administrativos e financeiros, o IGFSS teve um papel importante na identificação e selecção de uma nova aplicação que teria de dar resposta às necessidades do novo POCISSSS e ser compatível com o EURO.

Devido à plataforma tecnológica existente, no caso do CNP, esta actividade está direccionada para o desenvolvimento de programas para dar resposta às novas funcionalidades pretendidas, sendo a definição das necessidades estabelecida com os responsáveis das várias unidades.

VI.2.2.2.2. AQUISIÇÃO E MANUTENÇÃO DE APLICAÇÕES

Nenhuma das entidades auditadas utiliza uma metodologia formal e *standard*, adoptada pelo ISSS, na execução do trabalho de desenvolvimento de sistemas, através das várias fases que perfazem o ciclo de vida de desenvolvimento de sistemas. Verificou-se, ainda assim, que a metodologia do prestador de serviços de desenvolvimento foi, na maioria dos casos, adoptada, considerando-se aceitável esta abordagem, desde que o ISSS assegure que a metodologia apresentada respeita os requisitos mínimos de controlo e qualidade para um projecto de desenvolvimento; neste momento, a avaliação desses requisitos para o processo de desenvolvimento de sistemas é ainda intuitivo, dado que a definição destes mínimos requer uma adequada formalização.

Durante o processo de conversão dos sistemas e dos dados para o Euro foram adoptados alguns dos pressupostos desta metodologia; contudo, uma vez terminado, a sua aplicação continua a não ser sistemática.

VI.2.2.2.3. AQUISIÇÃO E MANUTENÇÃO DA ARQUITECTURA TECNOLÓGICA

Neste momento, o IIES encontra-se a definir uma arquitectura tecnológica para o SSSS, que passa pela centralização e padronização de plataformas tecnológicas. Existe um processo de administração das infra-estruturas que tem, até agora, sido realizado de forma descentralizada, o que resultou, relativamente aos investimentos efectuados nesta área, numa não padronização dos sistemas.



Tribunal de Contas

Com a excepção do IIES, nenhuma das entidades auditadas utiliza ferramentas na gestão da sua rede local e dos seus clientes de rede, de uma forma que lhe permita efectuar uma manutenção pró activa e mais eficiente do seu parque de tecnologias de informação; assim sendo, na maioria dos casos, esta manutenção é efectuada de forma reactiva. Por outro lado, ainda não foi estabelecido um Plano de Manutenção para o seu parque de Tecnologias de Informação, sendo corrente o recurso a *outsourcing* para a implementação e manutenção de várias componentes da sua infra-estrutura tecnológica, como forma de responder a problemas e reagir a necessidades de alteração; acresce, ainda, que este procedimento nem sempre resulta na transferência de conhecimentos para os funcionários que serão, futuramente, responsáveis pela administração dos sistemas e tecnologias implementadas.

As questões de continuidade das novas tecnologias implementadas começam a ser consideradas de uma forma integrada e concertada, com a participação do IIES.



Tribunal de Contas

VI.2.2.2.4. DESENVOLVIMENTO E MANUTENÇÃO DE PROCEDIMENTOS DE TI

Todas as entidades auditadas reconhecem a necessidade da existência de documentação para esta área, havendo mesmo, relativamente às Pensões, um Manual de Procedimentos, divulgado e de utilização corrente junto dos utilizadores, que oferece algum detalhe sobre as principais transacções inerentes a esses processos. A documentação relativa às operações de sistemas de informação é produzida ocasionalmente e de forma dispersa pelas várias unidades operacionais, afigurando-se, assim, inconsistente. Por outro lado, muitos dos procedimentos e documentação de suporte actuais estão desactualizados, consequência da falta de tempo para realizar as devidas correcções, sendo a sua manutenção efectuada esporadicamente, conforme as necessidades e disponibilidade de cada momento.

VI.2.2.2.5. INSTALAÇÃO E CERTIFICAÇÃO DE SISTEMAS

A instalação de novos sistemas tem vindo a ser executada por entidades externas contratadas para o desenvolvimento ou *customização* de uma solução informática, sendo a conversão de dados para os novos sistemas e a formação dos futuros utilizadores, usualmente, subcontratada à mesma entidade que desenvolve a nova solução, estando os utilizadores chave, geralmente, envolvidos na certificação das funcionalidades pretendidas. O teste dos aspectos de segurança da nova aplicação nem sempre é considerado como parte desta actividade.

É reconhecida a necessidade de verificar e confirmar se a solução implementada serve os objectivos, necessidades funcionais e padrões de qualidade pretendidos. Verificou-se que, normalmente, não são obtidas aprovações formais dos utilizadores antes do transporte de alterações do ambiente de teste para o ambiente de produção. As abordagens e a extensão dos testes efectuados variam, já que não é utilizada qualquer metodologia de testes estruturada.

Apesar de o IIES ter definida uma metodologia de gestão de projectos que contempla a certificação de sistemas, essa metodologia não é consistentemente aplicada por todas as entidades do ISSS.

VI.2.2.2.6. GESTÃO DA MUDANÇA

Existem duas realidades distintas nesta actividade: a do IIES – responsável pela gestão de mudança dos projectos de grande envergadura – e a dos CDSSS – que efectuam alterações aos sistemas existentes.



Tribunal de Contas

Há um reconhecimento, por parte de todas as entidades auditadas, de que as mudanças devem ser geridas e controladas, mas nem sempre é seguido um processo estruturado que parta de uma metodologia formal e *standard* na execução do trabalho de desenvolvimento de sistemas, através das várias fases do ciclo de vida desse desenvolvimento. Nos projectos de conversão para o EURO, constatou-se que houve a definição e categorização de prioridades e uma gestão e controlo de versões das aplicações alteradas. Mesmo assim, nem sempre foi possível assegurar a segregação dos ambientes de desenvolvimento e produção durante este processo.

A documentação sobre o processo de mudança é limitada ou inexistente. As alterações são efectuadas de uma forma que reduz a possibilidade de interrupções nos sistemas de informação, mas poderão ocorrer erros aliados a interrupções no ambiente produtivo, devido a uma gestão inadequada do processo de mudança em certas plataformas. No CNP e nos CDSSS de Porto e Setúbal, verificou-se que os desenvolvimentos e testes de novas aplicações ou novas funcionalidades são, em certos casos, efectuados directamente no ambiente produtivo.

VI.2.2.3. PROCESSO DE OPERAÇÃO DO AMBIENTE DE TI

VI.2.2.3.1. DEFINIÇÃO DOS NÍVEIS DE SERVIÇO

Neste momento, não existe uma definição formal dos níveis de serviço esperados de cada Unidade de SI e não está pensada a sua definição. A definição de um SLA necessitaria da determinação de medidas de avaliação de desempenho da prestação de serviços de cada Unidade de SI, não existindo, actualmente, os mecanismos necessários para os efectuar.

VI.2.2.3.2. GESTÃO DOS SERVIÇOS PRESTADOS POR TERCEIROS

O IIES é responsável pela gestão das relações com prestadores de serviços de TI, designando, quando é necessário recorrer à contratação de serviços, o responsável pelos Sistemas de Informação para iniciar a consulta a vários fornecedores. Os critérios de avaliação são identificados para cada projecto, mas não são antecipadamente formalizados, só o sendo nos casos da contratação de serviços e de alteração das condições contratuais. Existe um acompanhamento concomitante do fornecimento do serviço, não se podendo, contudo, considerar que este seja estruturado, uma vez que a sua sequência é intuitiva. Quanto aos aspectos legais dos contratos estabelecidos, existe um processo especialmente vocacionado para os assegurar.



Tribunal de Contas

VI.2.2.3.3. GESTÃO DA PERFORMANCE E DA CAPACIDADE

A responsabilidade pela monitorização do desempenho e gestão de capacidade dos sistemas de informação é partilhada entre o IIES, o CNP e os CDSSS. Actualmente, cada uma das entidades analisadas tem alguns procedimentos informais de monitorização de espaço em disco e processamento dos seus servidores. Dada a importância crítica do seu sistema, o CNP tem procedimentos que asseguram a monitorização constante dos seus sistemas principais. A monitorização do desempenho de rede é pontual, mas existem procedimentos de monitorização constante dos tempos de resposta da rede ou da sua capacidade, nos CDSSS.

A monitorização efectuada sobre os outros sistemas é reactiva, visto que só se consegue identificar problemas no momento em que acontecem ou posteriormente ao seu acontecimento. A implementação de quotas de espaço nos servidores serve, de certo modo, como um mecanismo de monitorização, já que os utilizadores são obrigados a contactar os administradores de sistema para obterem mais espaço em disco.

Não existem, actualmente, mecanismos ou procedimentos que permitam detectar e resolver, imediatamente, problemas de falta de capacidade de processamento dos sistemas de informação. Não se pode considerar que exista um planeamento de capacidade dos sistemas, considerando-se, apenas, a implementação de *upgrades* ou novas soluções, quando não existem alternativas susceptíveis de serem aplicadas ou se verifique, de facto, largos períodos de indisponibilidade dos sistemas.

VI.2.2.3.4. ASSEGURAR A CONTINUIDADE DOS SERVIÇOS PRESTADOS

Da avaliação efectuada desta actividade, constatou-se que nenhuma das entidades abordadas formalizou um Plano de Contingências para os seus sistemas de informação, tendo, apenas, cada uma das Unidades de Sistemas de Informação, um mínimo de procedimentos informais de segurança física e de salvaguarda de informação. Os procedimentos de salvaguarda de dados contemplam, em todos os casos, a realização de *backups* diários da informação armazenada nos seus servidores; contudo, não está definido – à excepção do CNP – um procedimento complementar que obrigue a guardar as cópias de segurança efectuadas fora das instalações de processamento. As entidades do SSSS que foram alvo desta auditoria não procederam a uma classificação da sua informação, em termos de confidencialidade e disponibilidade exigida, procedimentos que constituiriam o primeiro passo para perceber qual a informação crítica e quais as medidas necessárias a tomar para a sua salvaguarda.

As instalações físicas onde se encontram alguns dos sistemas de informação condicionam o nível de salvaguarda da informação, como acontece, por exemplo, no CDSSS de Setúbal, cuja sala de



Tribunal de Contas

processamento não oferece a protecção física adequada aos sistemas de informação, nomeadamente, porque:

- existe diverso material combustível na sala de processamento;
- a porta não oferece a protecção suficiente em caso de incêndio; e
- a sala de computadores não dispõe de reguladores de humidade.

Por outro lado, ainda não se estabeleceu qualquer contrato com fornecedores para garantir a reposição de equipamentos críticos, no caso da ocorrência de uma contingência significativa, havendo apenas acordos que abrangem a substituição de equipamentos em caso de avaria. Neste momento, as referidas entidades, para procederem à recuperação dos seus sistemas dependem, de forma crítica, dos funcionários de cada Unidade de Sistemas de Informação, podendo a sua indisponibilidade, em caso de calamidade, dificultar a resolução dos problemas.

VI.2.2.3.5. ASSEGURAR A SEGURANÇA DOS SISTEMAS

A avaliação desta actividade aponta para várias fraquezas no que se refere a controlos de acessos, bem como outros controlos essenciais para a segurança lógica dos sistemas e dos dados inerentes ao “processo de atribuição e controlo de pensões”. É importante entender que sem um adequado nível de controlos de acesso é extremamente difícil assegurar a integridade da informação dos sistemas do SSSS.

Os controlos de acesso, no sistema mais crítico para o “processo de atribuição e controlo de pensões”, nomeadamente o sistema *Unisys Clearpath 2200*, são razoáveis, mas muitos dos sistemas abordados em termos desta auditoria, que contribuem com informação para o mesmo processo, não estão adequadamente protegidos. Apresenta-se, na tabela apresentada abaixo, um resumo das principais fraquezas detectadas em cada entidade visitada:

Tabela 10 - Fraquezas de Controlos de Acesso Detectadas

Descrição da Fraqueza de Controlo	Sistema Afetado	CNP	CDSSS		
			Porto	Lisboa	Setúbal
Serviços de TCP-IP Excessivos Activos	Unisys ClearPath	v			
	MVS/ESA			v	
	Windows NT	v	v	v	v
	AS/400				v
Utilizadores Genéricos	IDMS / ADABAS		v		
	Windows NT	v		v	
	AS/400				v
Pobre Qualidade de <i>Passwords</i>	Unisys ClearPath	v			
	Windows NT				v
	AS/400				v



Tribunal de Contas

Descrição da Fraqueza de Controlo	Sistema Afec-tado	CNP	CDSSS		
			Porto	Lisboa	Setúbal
Retirada de Utilizadores Inactivos	Windows NT	v	v	v	v
	AS/400				v
Account Policies Inadequados	Windows NT	v		v	v
Períodos de Expiração de Passwords Inadequados	Unisys ClearPath	v			
	AS/400				v
Configurações de Serviços Inseguros	Windows NT	v	v	v	v
	Windows NT		v		
Permissões e Autorizações Excessivas	AS/400				v
	AS/400				v
Valores de Sistema Inseguros	AS/400				v
Falta de Utilização de Home Directories	Windows NT	v			
Monitorização e Acessos	Windows NT		v		v
	AS/400				v
Mecanismos de Auditoria Inactivos	Windows NT				v
	Windows NT				v
Expiração de Contas Temporárias	Windows NT	v			
Implementação de Software de Segurança	MVS/ESA			v	

O detalhe de cada fraqueza identificada acima encontra-se no **Anexo B – Detalhe dos Resultados da Auditoria**. Dos resultados obtidos, ficou patente que não existe uma abordagem consistente e integrada nas matérias de segurança lógica de sistemas de informação, começando com a falta de políticas e procedimentos de segurança, a falta de gestão das configurações de segurança, bem como da implementação de mecanismos de monitorização que permitam confirmar o cumprimento e funcionamento das medidas de segurança implementadas.

VI.2.2.3.6. IDENTIFICAÇÃO E AFECÇÃO DOS CUSTOS

Nenhuma das entidades visitadas procedeu à definição de níveis de serviço, não sendo, por essa razão, considerado como prioridade o estabelecimento de taxas de débito para imputação do custo de serviço às outras Unidades operacionais. As Unidades de SI são consideradas como centros de custos. No entanto, segundo alega o IIES, “... o processo de afectação total de custos aos projectos encontra-se em fase de análise de requisitos, seguindo-se-lhe, imediatamente, a fase de implementação, estando já seleccionada uma ferramenta para suporte ao processo”.

VI.2.2.3.7. PRESTAÇÃO DE APOIO E FORMAÇÃO AOS UTILIZADORES

O processo de formação de utilizadores não está estruturado nem padronizado. Quando é identificada a necessidade, o responsável de cada Unidade propõe que o utilizador frequente uma



Tribunal de Contas

acção de formação específica. Quando se verifica a introdução de novas soluções aplicacionais, quem, normalmente, fica responsável pela componente de formação e produção de documentação de apoio é o fornecedor contratado, o que limita a contemplação de necessidades específicas de cada entidade do SSSS nas acções de formação. Cada Unidade de SI responde a todas as solicitações de apoio por parte dos utilizadores sem estabelecer prioridades para os pedidos, sendo, ainda assim, prestado um nível de apoio razoável, considerando os recursos disponíveis para esta actividade. A relativa estabilidade dos sistemas tem minimizado o número de solicitações nesta área.

VI.2.2.3.8. APOIAR E ACONSELHAR OS "CLIENTES" DE TI

Na medida em que esta actividade depende de uma função de *Help Desk* formalizada, observou-se que as actividades de apoio aos utilizadores estão pouco estruturadas. Embora cada entidade tenha recursos atribuídos a esta tarefa, o IIES é a entidade responsável pela gestão dos serviços de apoio aos utilizadores, tendo um serviço de *Help Desk*, vocacionado para apoiar aplicações que vai disponibilizando, pretendendo que este serviço de *Help Desk* venha ser alargado a todos os sistemas do SSSS.

VI.2.2.3.9. GESTÃO DA CONFIGURAÇÃO DE SISTEMAS

A configuração presente nos computadores pessoais dos colaboradores do SSSS apresenta um nível de padronização bastante acentuado, não existindo, no entanto, *standards* formais quanto a essas configurações. Dada a inexistência de políticas e procedimentos de utilização de sistemas, formalmente definidos sobre esta matéria, subsiste um vazio de regras quanto à utilização de *software* não autorizado; por outro lado, tendo sido concedido aos utilizadores acesso à Internet, a obtenção e instalação de todo o tipo de *software* ilegal tornou-se uma tarefa mais facilitada. Este risco está a ser colmatado com a implementação de *User Policies* nos clientes de rede com *Windows NT*. Com excepção do CNP, em nenhuma das restantes entidades estão a ser utilizadas ferramentas para efectuar a monitorização e manutenção do *software* instalado nos clientes de rede locais.

Relativamente a este ponto, o IIES informa ter definido um *standard* para a configuração de computadores pessoais e vindo a dotar os diversos serviços com equipamentos com uma configuração protegida, que não permite a instalação de *software*, por parte de utilizadores não autorizados.

VI.2.2.3.10. RESOLUÇÃO E GESTÃO DE PROBLEMAS DE TI



Tribunal de Contas

A gestão dos problemas que vão surgindo é informal. Não tem sido possível realizar análises cuidadas dos incidentes que ocorrem, a fim de poder identificar se estes são reincidentes e poder, assim, apontar soluções similares. As prioridades na resolução de problemas são atribuídas, informalmente, no acto do pedido.



Tribunal de Contas

VI.2.2.3.11. GESTÃO DOS DADOS

Os sistemas de cada uma das entidades do SSSS foram implementados em momentos diferentes. As plataformas que suportam cada um dos sistemas de informação são distintas, o que levou à concepção de diferentes aplicações para servir o mesmo objectivo. Nos vários CDSSS, por exemplo, existe uma panóplia de aplicações, que poderiam ter sido padronizadas. O modelo de dados subjacente a cada uma delas é distinto e não está claramente definido. Actualmente, o IIES está a definir um modelo de dados central, que suportará as novas aplicações do SSSS, não se encontrando ainda concluída a definição das regras para assegurar a sua coerência.

As aplicações existentes foram desenvolvidas sem se observar a implementação de alguns controlos de introdução e alteração de dados, o que poderá resultar em problemas para a integridade e qualidade da informação processada, tendo sido necessário desenvolver, complementarmente, algumas rotinas que possibilitassem a identificação, durante o processamento, da informação de “má qualidade” introduzida nos sistemas.

Não se estabeleceram formalmente regras de classificação e arquivo de dados, existindo, no entanto, alguns procedimentos instituídos para o seu armazenamento. As cópias de segurança efectuadas, devidamente identificadas e catalogadas, são, contudo, com excepção do CNP, guardadas nas próprias instalações de cada serviço, podendo, em caso de acidente, colocar em risco a sua integridade.

As entidades visadas não têm capacidade para gerir informação não estruturada, sendo esta gestão efectuada com recurso ao suporte de papel, o que dificulta as suas consulta e análise.

VI.2.2.3.12. GESTÃO DAS INSTALAÇÕES FÍSICAS

Ainda que existam vários mecanismos para assegurar a segurança física dos sistemas, verificou-se que as salas onde se encontram os sistemas de informação críticos carecem de algumas condições ambientais, designadamente:

- em todas as entidades auditadas, as portas das salas de processamento não oferecem a protecção necessária para fazer face a um incêndio e evitar a propagação rápida das chamas;
- nos CDSSS – Lisboa e Setúbal não estão instalados sistemas automáticos de extinção de incêndio.

As instalações das Unidades de Informática estão localizadas em áreas segregadas, o que permite limitar, mais facilmente, o acesso a essas mesmas instalações, observando-se, inclusivamente, a



Tribunal de Contas

presença de segurança permanente nessas instalações. Verificou-se, por outro lado, que nenhuma das entidades auditadas tinha formalizado um *Disaster Recovery Plan* para os seus sistemas de informação que abrangesse as instalações físicas.

Note-se que, segundo as alegações produzidas, “o IIES tem em curso um projecto para definição dos requisitos a implementar para efeito de recuperação de desastres”.

VI.2.2.3.13. GESTÃO DAS OPERAÇÕES

Nem sempre existe, nas Unidades de Sistemas de Informação dos CDSSS, um manual de operações que defina claramente todos os procedimentos diários a realizar, verificando-se a sua execução de forma informal, decorrente da experiência de cada funcionário. A monitorização e tarefas de suporte efectuadas sobre os sistemas dependem da verificação, *in loco*, dos sistemas ou da resposta a anomalias identificadas pelos utilizadores. Os procedimentos de *backup* são automatizados, de forma a permitir a execução e monitorização dos *backups* efectuados.

VI.2.2.4. PROCESSO DE MONITORIZAÇÃO DOS PROCESSOS DE TI

O Processo de Monitorização dos Processos de TI encontra-se numa fase muito incipiente: nenhuma das actividades que constituem este processo está adequadamente desenvolvida para que o SSSS disponha de processos de monitorização sobre a gestão de TI.

O IIES reconhece, nas suas alegações, a importância deste processo.

VI.2.2.4.1. MONITORIZAÇÃO DOS PROCESSOS DE TI

As entidades integrantes do SSSS carecem de mecanismos de monitorização e avaliação da *performance* dos seus processos de TI, havendo, por outro lado, indefinição quanto aos objectivos que se pretendem atingir e quanto às métricas a utilizar para analisar essa *performance*.

VI.2.2.4.2. AVALIAÇÃO DO CONTROLO INTERNO DE TI

As entidades não dispõem de uma função que avalie o controlo interno dos processos de TI, nem os objectivos que se pretendem atingir com o mesmo. As avaliações realizadas ocorrem sem carácter regular, sendo conduzidas como parte integrante das intervenções dos auditores



Tribunal de Contas

financeiros, com metodologias e valências técnicas que não correspondem às necessidades específicas de cada Unidade de Sistemas de Informação.

VI.2.2.4.3. CERTIFICAÇÃO DE SERVIÇOS E SISTEMAS

Nenhuma das entidades auditadas possui qualquer processo de certificação e avaliação de serviços prestados para a área de sistemas de informação, não estando, neste momento, contemplada qualquer actividade para esse fim.

VI.2.2.4.4. EXECUÇÃO DE AUDITORIAS INDEPENDENTES

Não são realizadas auditorias externas aos processos de TI; o presente trabalho representa a primeira iniciativa neste domínio.

VII. EMOLUMENTOS

São devidos emolumentos, nos termos do n.º 1 do art.º 10º e do art.º 2º do Regime Jurídico dos Emolumentos do Tribunal de Contas, aprovado pelo Decreto-Lei n.º 66/96, de 31 de Maio, a suportar, na proporção do tempo despendido, pelo Instituto da Solidariedade e Segurança Social e pelo Instituto de Informática e Estatística da Segurança Social, no valor total de **€15 516,50**.

Igualmente é devida, nos termos do n.º 3 do art.º 10º do mesmo diploma, conjugado com o n.º 4 do art.º 56º da Lei n.º 98/97, de 26 de Agosto, pelas mesmas entidades e na mesma proporção, a quantia de **€88 885,79**.

Estes encargos distribuem-se como segue:

(Un.: Euros)

Tipo de encargos	Entidade devedora		Totais
	ISSS	IIES	
Emolumentos	11 637,38	3 879,12	15 516,50
Outros encargos	66 664,34	22 221,45	88 885,79
Totais	78 301,72	26 100,57	104 402,29



Tribunal de Contas

VIII. DECISÃO

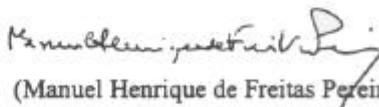
Os Juizes do Tribunal de Contas, em Subsecção da 2.ª Secção, nos termos da alínea a) do n.º 2 do art.º 78.º da Lei n.º 98/97, de 26 de Agosto, deliberam:

- a) Aprovar o presente relatório;
- b) Ordenar que o mesmo seja remetido:
 - Ao Presidente da Assembleia da República, aos Presidentes das Comissões Parlamentares de Execução Orçamental e do Trabalho e dos Assuntos Sociais e aos Líderes de todos os Grupos Parlamentares;
 - Ao Ministro da Segurança Social e do Trabalho;
 - Às entidades ouvidas no âmbito do contraditório;
- c) Determinar a sua remessa ao Ministério Público junto deste Tribunal, em cumprimento do disposto no n.º 4 do art.º 29.º da Lei n.º 98/97;
- d) Após notificação nos termos das alíneas anteriores, colocar o presente relatório e seus anexos A1 a C, E e F à disposição dos órgãos de Comunicação Social, bem como proceder à respectiva divulgação via *Internet*;
- e) Determinar às entidades auditadas que, decorrido o prazo de 180 dias, informem o Tribunal das medidas adoptadas face às recomendações ora formuladas.

Fixar os emolumentos a pagar conforme constante do ponto VII.

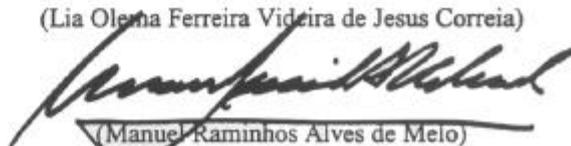
Tribunal de Contas, em 27 de Junho de 2002,

O Conselheiro Relator


(Manuel Henrique de Freitas Pereira)

Os Conselheiros Adjuntos


(Lia Oleina Ferreira Vidreira de Jesus Correia)


(Manuel Raminhos Alves de Melo)



Tribunal de Contas

ÍNDICE DOS ANEXOS

Anexo A1	Súmula de Legislação Relevante
Anexo A2	Glossário de Termos Informáticos
Anexo B	Detalhe dos Resultados da Auditoria
Anexo C	Recomendações Detalhadas
Anexo D	Diferenças Detectadas nos Cálculos Manuais
Anexo E	Levantamento dos Circuitos e da Arquitectura Informática
Anexo F	Alegações Produzidas no Exercício do Contraditório



Tribunal de Contas

Anexo A1 – Súmula de Legislação Relevante

[Decreto-Lei n.º 129/77. DR 78/77 SÉRIE I de 1977-04-02](#)

Ministério dos Assuntos Sociais

Aprova a Lei Orgânica Hospitalar

[Decreto-Lei n.º 124/79. DR 107/79 SÉRIE I-7 de 1979-05-10](#)

Presidência do Conselho de Ministros e Ministérios das Finanças e do Plano e dos Assuntos Sociais

Integra na função pública os trabalhadores dos Serviços Médico-Sociais

[Decreto-Lei n.º 141/79. DR 117/79 SÉRIE I-7 de 1979-05-22](#)

Presidência do Conselho de Ministros e Ministérios das Finanças e do Plano, da Agricultura e Pescas, do Comércio e Turismo e dos Assuntos Sociais

Estabelece disposições quanto à inscrição obrigatória na Caixa Geral de Aposentações do pessoal ao serviço dos organismos de coordenação económica, da Comissão de Viticultura da Região dos Vinhos Verdes, da Federação dos Vinicultores da Região do Douro e da Adega Regional de Colares. **Nota:** Há desconformidade entre o emissor que consta no sumário e o que consta no texto respectivo

[Decreto-Lei n.º 288/79. DR 186/79 SÉRIE I de 1979-08-13](#)

Ministério dos Assuntos Sociais

Define colocação familiar e estabelece os seus objectivos

[Decreto-Lei n.º 301/79. DR 190/79 SÉRIE I de 1979-08-18](#)

Presidência do Conselho de Ministros e Ministérios das Finanças e do Plano e dos Assuntos Sociais

Revoga o artigo 58.º do Estatuto Hospitalar, integrando na Caixa Geral de Aposentações o pessoal das carreiras hospitalares

[Decreto-Lei n.º 247/80. DR 169/80 SÉRIE I-9 de 1980-07-24](#)

Presidência do Conselho de Ministros e Ministérios das Finanças e do Plano e dos Assuntos Sociais

Estabelece normas relativas ao regime de previdência do pessoal da Misericórdia de Lisboa

[Decreto-Lei n.º 250/81. DR 198/81 SÉRIE I de 1981-08-29](#)

Presidência do Conselho de Ministros e Ministérios das Finanças e do Plano e dos Assuntos Sociais

Altera o n.º 2 do artigo 4.º do Decreto-Lei n.º 129/77, de 2 de Abril, aplicando aos trabalhadores dos hospitais o regime previsto no Decreto-Lei n.º 141/79, de 22 de Maio

[Decreto-Lei n.º 37/84. DR 27/84 SÉRIE I de 1984-02-01](#)

Ministérios da Administração Interna, das Finanças e do Plano, do Trabalho e Segurança Social, da Saúde e da Indústria e Energia

Torna obrigatória a inscrição no regime geral da segurança social dos trabalhadores integrados nos quadros da Electricidade de Portugal (EDP), E. P., oriundos das autarquias locais, serviços municipalizados ou federações de municípios

[Decreto-Lei n.º 69/85. DR 64/85 SÉRIE I de 1985-03-18](#)

Ministério do Trabalho e Segurança Social

Altera a redacção do artigo 91.º do Regime Jurídico do Contrato Individual de Trabalho, aprovado pelo Decreto-Lei n.º 49408, de 24 de Novembro de 1969

[Decreto-Lei n.º 169/85. DR 115/85 SÉRIE I de 1985-05-20](#)

Ministério das Finanças e do Plano



Tribunal de Contas

Determina que aos docentes do ensino oficial não superior, ainda que este não se insira na rede pública de ensino dependente do Ministério da Educação, incluindo os docentes dos postos de recepção oficiais do Ciclo Preparatório TV, seja contado, para efeitos de aposentação, o tempo de serviço docente prestado no ensino particular

[Decreto-Lei n.º 321/88. DR 220/88 SÉRIE I de 1988-09-22](#)

Ministério da Educação

Disciplina a inscrição de pessoal docente do ensino não superior, particular e cooperativo, na Caixa Geral de Aposentações e no Montepio dos Servidores do Estado

[Decreto-Lei n.º 59/89. DR 44/89 SÉRIE I de 1989-02-22](#)

Ministério do Emprego e da Segurança Social

Disciplina a intervenção da Segurança Social no reembolso de prestações em processos judiciais

[Decreto-Lei n.º 79-A/89. DR 60/89 SÉRIE I 1º SUPLEMENTO de 1989-03-13](#)

Ministério do Emprego e da Segurança Social

Subsídio de desemprego (revoga o Decreto-Lei n.º 20/85, de 17 de Janeiro, e legislação complementar)

[Decreto-Lei n.º 380/89. DR 248/89 SÉRIE I de 1989-10-27](#)

Ministério do Emprego e da Segurança Social

Permite o pagamento retroactivo de contribuições para a Segurança Social

[Decreto-Lei n.º 141/91. DR 83/91 SÉRIE I-A de 1991-04-10](#)

Ministério do Emprego e da Segurança Social

Estabelece as condições de acumulação das pensões dos regimes contributivos de segurança social entre si, com pensões de outros regimes de protecção social de enquadramento obrigatório e com pensões de regimes não contributivos ou equiparados

[Decreto-Lei n.º 159/92. DR 175/92 SÉRIE I-A de 1992-07-31](#)

Ministério do Emprego e da Segurança Social

Estabelece o regime da pensão unificada

[Decreto-Lei n.º 216/98. DR 162/98 SÉRIE I-A de 1998-07-16](#)

Ministério do Trabalho e da Solidariedade

Estabelece condições mais favoráveis para o acesso a pensões por invalidez por parte de pessoas infectadas pelo HIV

[Decreto-Lei n.º 361/98. DR 267/98 SÉRIE I-A de 1998-11-18](#)

Ministério do Trabalho e da Solidariedade

Regime jurídico da pensão unificada

[Decreto-Lei n.º 9/99. DR 6/99 SÉRIE I-A de 1999-01-08](#)

Ministério do Trabalho e da Solidariedade

Altera o Decreto-Lei n.º 329/93, de 25 de Setembro (regime de protecção na velhice e na invalidez dos beneficiários do regime geral de segurança social)

[Decreto-Lei n.º 95/99. DR 69/99 SÉRIE I-A de 1999-03-23](#)

Ministério da Saúde

Torna extensivo ao pessoal dos antigos hospitais concelhios o regime de pensões vigente para o pessoal dos hospitais centrais e distritais, previsto nos Decretos-Leis n.ºs 129/77, de 2 de Abril, e 301/79, de 18 de Agosto

[Decreto-Lei n.º 119/99. DR 87/99 SÉRIE I-A de 1999-04-14](#)

Ministério do Trabalho e da Solidariedade

Estabelece, no âmbito do regime geral de segurança social dos trabalhadores por conta de outrem, o quadro legal da reparação da eventualidade de desemprego



Tribunal de Contas

[Decreto-Lei n.º 186-B/99. DR 126/99 SÉRIE I-A 1º SUPLEMENTO de 1999-05-31](#)

Ministério do Trabalho e da Solidariedade

Altera o Decreto-Lei n.º 119/99, de 14 de Abril, que estabelece o quadro legal de reparação da eventualidade de desemprego no âmbito do regime geral de segurança social dos trabalhadores por conta de outrem

[Decreto-Lei n.º 199/99. DR 132/99 SÉRIE I-A de 1999-06-08](#)

Ministério do Trabalho e da Solidariedade

Revê as taxas contributivas do regime geral de segurança social dos trabalhadores por conta de outrem

[Decreto-Lei n.º 437/99. DR 253/99 SÉRIE I-A de 1999-10-29](#)

Ministério do Trabalho e da Solidariedade

Altera o Decreto-Lei n.º 329/93, de 25 de Setembro, que estabelece o regime de protecção na velhice e na invalidez dos beneficiários do regime geral de segurança social

[Decreto-Lei n.º 482/99. DR 261/99 SÉRIE I-A de 1999-11-09](#)

Ministério do Trabalho e da Solidariedade

Estabelece regras de antecipação da idade de acesso à pensão por velhice aos profissionais do bailado clássico ou contemporâneo

[Decreto-Lei n.º 483/99. DR 261/99 SÉRIE I-A de 1999-11-09](#)

Ministério do Trabalho e da Solidariedade

Institui um regime de protecção social específico para os trabalhadores do sector portuário

[Decreto Regulamentar n.º 1/94. DR 14/94 SÉRIE I-B de 1994-01-18](#)

Ministério do Emprego e da Segurança Social

Regula o acesso às prestações por morte por parte das pessoas que se encontram na situação de união de facto

[Portaria n.º 193/79. DR 93/79 SÉRIE I de 1979-04-21](#)

Presidência do Conselho de Ministros e Ministérios das Finanças e do Plano, do Trabalho e dos Assuntos Sociais

Actualiza as condições de trabalho dos trabalhadores das instituições de previdência

[Portaria n.º 530/80. DR 191/80 SÉRIE I-1 de 1980-08-20](#)

Conselho da Revolução e Ministério das Finanças e do Plano

Fixa as remunerações a abonar aos professores civis universitários que, em regime de acumulação e por contrato, regerem matérias dos cursos leccionados no Instituto de Altos Estudos Militares

[Portaria n.º 621/89. DR 179/89 SÉRIE I de 1989-08-05](#)

Ministérios da Administração Interna e do Emprego e da Segurança Social

Estabelece os termos e as condições para a concretização do direito dos bombeiros abrangidos pelos regimes contributivos de segurança social à bonificação das pensões de reforma por invalidez, velhice e de sobrevivência



Tribunal de Contas

Anexo A2 – Glossário de Termos Informáticos

Account Policies	Conjunto de regras específicas que permitem gerir os acessos atribuídos aos utilizadores do sistema;
Monitorização	Análise de eventos que possam colocar em causa o ambiente de controlo definido;
Software	Conjunto de programas que servem para o tratamento automático da informação e permitem o «diálogo» entre o homem e o computador;
Hardware	Designação que engloba todos os elementos da aparelhagem e acessórios que fazem parte de um computador (teclado, visor, impressora, etc.);
HTTP (Hypertext Transfer Protocol)	é um conjunto de regras de comunicação de ficheiros (texto, imagens, som, vídeo, e outros ficheiros multimédia) utilizadas na <i>World Wide Web</i> (vulgo Internet);
Passwords	Também designadas por senhas de acesso;
MINPASSLEN	Parâmetro de configuração da extensão mínima das senhas no sistema AS/400;
Serviço Alerter	Mecanismo inerente ao sistema operativo <i>Windows NT</i> , que notifica os utilizadores quando algum evento anormal se verifica no sistema;
Serviço Messenger	Mecanismo inerente ao sistema operativo <i>Windows NT</i> , que permite o envio de mensagens;
Domain Controller	Computador que gere um conjunto de computadores ligados entre si;
Home Directories	Directórios associados à conta de utilizadores;
Serviço de TCP/IP	Conjunto de funcionalidades associadas ao protocolo de comunicação de redes informáticas TCP/IP;
FTP (File Transfer Program)	Um programa utilizado para efectuar transferência de ficheiros entre dois sistemas utilizando o protocolo de comunicação TCP/IP.
Telnet	Um programa inerente ao protocolo de comunicação TCP/IP que permite emular o ecrã de um computador noutra e, assim, realizar transacções remotamente.
Internet Information Server	Computador que serve os serviços de HTTP;
Account Lockout	Mecanismo de bloqueio da conta de utilizador, quando se tenta obter acesso a um sistema informático mais do que x vezes;



Tribunal de Contas

Default Public Authority	Define as autorizações que são dadas a qualquer utilizador, em ambiente AS/400, para assim executar um programa de computador ou editar um ou mais ficheiros;
QCRTAUT	Autorizações de um utilizador de AS/400 para criação de objectos;
Library	Bibliotecas em ambiente AS/400. Equivalente às directorias em MS-DOS ou folders em MS Windows;
Create Authority de SYSVAL	Autorizações de um utilizador para criação de bibliotecas, utilizadores, ficheiros, etc.;
Public Authority de LIBCRTAUT	Autorizações para qualquer utilizador poder criar uma biblioteca;
User Profile	Autorização num sistema AS/400, para este ter acesso aos recursos deste sistema;
Parâmetro QPWDEX-PITV (e todos os outros do mesmo género)	Parâmetros de configuração em ambiente AS/400 que permitem implementar maior qualidade de senhas de acesso ao sistema;
Valor de sistema NOMAX	Configuração do sistema AS/400 que indica que não está definido qualquer valor máximo;
Classe de utilizadores SECOFR	Grupo de utilizadores com permissões para realizar administração do sistema AS/400;
Sign-on ao Sistema	Acto de um utilizador se identificar perante um sistema;
Sign-on do Security Officer	Acto do administrador de segurança do sistema AS/400 se identificar perante o sistema ;
Informações de Sign-on	Indicações de que tentou ou efectuou <i>sign-on</i> ;
Log-off	Acto de um utilizador terminar a utilização do sistema informático;
Programa Attention-Key	Programa executado quando se pressiona a tecla " <i>Attention-Key</i> ";
Limited Capability	Parâmetro de limitação de autorizações do utilizador em ambiente AS/400;
Bibliotecas EFXLIB, EXXLIB (e outras do mesmo género)	Directorias no ambiente AS/400;
Proxy server	Numa entidade que utilize a Internet, um <i>proxy server</i> é o computador que funciona como intermediário entre o computador de um utilizador e a Internet e que permite implementar medidas de controlo de administração e segurança sobre o acesso à Internet;



Tribunal de Contas

Parâmetro de <i>registry</i> <i>RestrictAnonymous</i>	Parâmetro de configuração do sistema <i>Windows NT</i> , que permite proibir o acesso não identificado a esse sistema;
<i>Browsing</i>	Exploração do conteúdo de uma parte específica de um sistema;
Pacotes SMB (<i>Server Message Block</i>)	Funcionalidade de comunicação entre sistemas com sistema operativo <i>MS Windows</i> , que permite regular a transferência bilateral de ficheiros;
<i>Pagefile</i>	Ficheiro temporário criado pelo sistema operativo, para gestão de memória;
<i>Fault Tolerant</i>	Mecanismo ou processo que reforça a resistência a falhas no sistema;
<i>SysKey</i>	Mecanismo de encriptação de senhas em ambiente <i>MS Windows NT</i> ;
<i>Passprop</i>	Mecanismo que permite forçar a melhoria das senhas utilizadas num ambiente <i>Windows NT</i> ;
<i>Resource Kit</i>	Conjunto de programas que permitem efectuar a administração de um sistema <i>MS Windows NT</i> ;
Parâmetro <i>Secureboot</i> no <i>Registry</i>	
Monitorização de <i>Logs</i>	Verificação de informação de um sistema de informático, com o objectivo de detectar anomalias;
<i>Audit Policies</i>	Definições ao nível do sistema <i>Windows NT</i> , que descrevem o detalhe do rasto de auditoria deixado pelo sistema;
Comandos CL (<i>Command Line</i>)	Instruções executadas em ambiente não suportado por menus;
<i>Initial Program</i>	Programa executado quando um utilizador se identifica perante o sistema;
<i>Initial Menu</i>	Menu executado quando um utilizador se identifica perante o sistema;
<i>Current Library</i>	Biblioteca corrente ;
<i>Audit Journal</i>	Registo de eventos de auditoria;
Servidores de Autenticação	Também <i>designations</i> ;
<i>Null sessions</i>	Sessões estabelecidas com um computador remoto sem que seja necessário existir autenticação do utilizador;
<i>Share</i>	Mecanismo que permite estabelecer a partilha de recursos de um sistema entre computadores e utilizadores;
<i>Share IPC\$</i>	Partilha de sistema efectuada por um computador em ambiente <i>MS Windows NT</i> ;



Tribunal de Contas

FAQ – (Frequently Asked Questions)

Perguntas mais frequentes;

Standards

Normas;

Status

Estado;

Backup

Cópia de segurança;

Input

Acto de introdução de informação num sistema;

Output

Acto de emissão de um relatório num sistema;

Design de formulários

Concepção de formulários.



Anexo B – Detalhe dos Resultados da Auditoria

Índice do Anexo

	<u>Pág.</u>
1. AVALIAÇÃO DOS PROCESSOS DE ATRIBUIÇÃO E CONTROLO DE PENSÕES	3
1.1. PROCESSO DE GESTÃO DE REQUERIMENTOS.....	3
1.2. RECEPÇÃO, ORGANIZAÇÃO E REGISTO DO REQUERIMENTO.....	3
1.2.1. Descrição da Actividade.....	3
1.2.2. Situação Actual.....	3
1.2.3. Riscos Significativos Identificados e Seus Impactes.....	7
1.2.4. Avaliação Global da Maturidade da Actividade – Repetitivo	8
1.3. IDENTIFICAÇÃO DO BENEFICIÁRIO	8
1.3.1. Descrição da Actividade.....	8
1.3.2. Situação Actual.....	8
1.3.3. Riscos Significativos Identificados e Seus Impactes.....	9
1.3.4. Avaliação da Maturidade da Actividade – Gerido.....	9
1.4. ENVIO E INTEGRAÇÃO DE INFORMAÇÃO COM O CNP.....	10
1.4.1. Descrição da Actividade.....	10
1.4.2. Situação Actual.....	10
1.4.3. Riscos Significativos Identificados e Seus Impactes.....	11
1.4.4. Avaliação da Maturidade da Actividade – Repetitivo.....	11
2. PROCESSO DE ATRIBUIÇÃO E CÁLCULO DE PENSÕES	12
2.1. A CONFERÊNCIA E DEFERIMENTO DE PROCESSOS.....	12
2.1.1. Descrição da Actividade.....	12
2.1.2. Situação Actual.....	12
2.1.3. Riscos Significativos Identificados e Seus Impactes.....	14
2.1.4. Avaliação da Maturidade da Actividade – Gerido.....	14
2.2. O CÁLCULO DA PENSÃO.....	14
2.2.1. Descrição da Actividade.....	14
2.2.2. Situação Actual.....	15
2.2.3. Resultados dos Testes Efectuados.....	15
2.2.4. Riscos Significativos Identificados e Seus Impactes.....	23
2.2.5. Avaliação Global da Actividade – Repetitivo.....	23
2.3. PROCESSAMENTO E PAGAMENTO DE PENSÕES.....	23
2.4. ALTERAÇÃO PERIÓDICA DAS PENSÕES	23
2.4.1. Descrição da Actividade.....	23
2.4.2. Situação Actual.....	24
2.4.3. Riscos Significativos Identificados e Seus Impactes.....	25
2.4.4. Avaliação de Maturidade da Actividade – Repetitivo	25
2.5. PROCESSAMENTO MENSAL DAS PENSÕES.....	25
2.5.1. Descrição da Actividade.....	25
2.5.2. Situação Actual.....	26
2.5.3. Riscos Significativos Identificados e Seus Impactes.....	26



Tribunal de Contas

2.5.4.	<i>Avaliação da Maturidade da Actividade – Definido</i>	26
2.6.	PAGAMENTO DAS PENSÕES.....	26
2.6.1.	<i>Descrição da Actividade</i>	26
2.6.2.	<i>Situação Actual</i>	27
2.6.3.	<i>Riscos Significativos Identificados e Seus Impactes</i>	28
2.6.4.	<i>Avaliação da Maturidade da Actividade – Definido</i>	29
3.	AVALIAÇÃO DOS PROCESOS DE GESTÃO DE TI	30
3.1.	PLANEAMENTO E ESTRATÉGIA DE SISTEMAS DE INFORMAÇÃO.....	30
3.1.1.	<i>Descrição do Processo</i>	30
3.1.2.	<i>Definição da Estratégia de TI</i>	30
3.1.3.	<i>Definição da Arquitectura de Informação</i>	34
3.1.4.	<i>Definição da Direcção Tecnológica de TI</i>	36
3.1.5.	<i>Definição da Organização de TI e suas Interdependências</i>	38
3.1.6.	<i>Gestão dos Investimentos em TI</i>	40
3.1.7.	<i>Comunicação das Orientações Estratégicas</i>	42
3.1.8.	<i>Gestão dos Recursos Humanos</i>	43
3.1.9.	<i>Cumprimento de Requisitos Externos</i>	46
3.1.10.	<i>Avaliação de Riscos de TI</i>	50
3.1.11.	<i>Gestão dos Projectos em Curso</i>	52
3.1.12.	<i>Gestão da Qualidade</i>	53
3.2.	DESENVOLVIMENTO E IMPLEMENTAÇÃO DE SOLUÇÕES.....	55
3.2.1.	<i>Descrição do Processo</i>	55
3.2.2.	<i>Identificação de Soluções</i>	56
3.2.3.	<i>Aquisição e Implementação de Aplicações</i>	58
3.2.4.	<i>Implementação da Infra-estrutura Tecnológica</i>	59
3.2.5.	<i>Desenvolvimento e Manutenção de Procedimentos de TI</i>	61
3.2.6.	<i>Instalação e Certificação de Sistemas</i>	63
3.2.7.	<i>Gestão da Mudança</i>	65
3.3.	OPERAÇÃO DO AMBIENTE INFORMÁTICO.....	67
3.3.1.	<i>Descrição do Processo</i>	67
3.3.2.	<i>Definição de Níveis de Serviço</i>	67
3.3.3.	<i>Gestão dos Serviços Prestados por Terceiros</i>	69
3.3.4.	<i>Gestão da Performance e da Capacidade</i>	71
3.3.5.	<i>Assegurar a Continuidade de Serviços Prestados</i>	73
3.3.6.	<i>Assegurar a Segurança dos Sistemas</i>	75
3.3.7.	<i>Identificação e Afectação dos custos</i>	91
3.3.8.	<i>Prestação de Apoio e Formação aos Utilizadores</i>	92
3.3.9.	<i>Apoiar e Aconselhar os Utilizadores</i>	94
3.3.10.	<i>Gestão das Configurações</i>	96
3.3.11.	<i>Resolução e Gestão de Problemas de TI</i>	98
3.3.12.	<i>Gestão dos Dados</i>	99
3.3.13.	<i>Gestão das Instalações Físicas</i>	102
3.3.14.	<i>Gestão das Operações</i>	104
3.4.	MONITORIZAÇÃO DOS PROCESSOS DE TI.....	105
3.4.1.	<i>Descrição do Processo</i>	105
3.4.2.	<i>Monitorização dos Processos de TI</i>	106
3.4.3.	<i>Avaliação do Controlo Interno de TI</i>	107
3.4.4.	<i>Certificação de Serviços e Sistemas</i>	108
3.4.5.	<i>Execução de Auditorias Independentes</i>	110



Tribunal de Contas

1. Avaliação dos Processos de Atribuição e Controlo de Pensões

1.1. PROCESSO DE GESTÃO DE REQUERIMENTOS

O processo de Gestão de Requerimentos tem como objectivo principal a recolha e validação de todos os elementos necessários de um requerimento, relativo a uma pensão de invalidez, velhice ou sobrevivência, apresentado em qualquer CDSSS, do ponto vista documental, para subsequente análise pelo CNP.

Este processo tem início com a recepção do requerimento (velhice, invalidez ou sobrevivência) num CDSSS e termina com a transferência do processo para o CNP, após verificação de que todos os elementos necessários foram devidamente apresentados e integrados no processo. Este processo depende de outros anteriores que asseguram, designadamente, o registo da carreira contributiva do beneficiário. O entendimento obtido do processo revelou que este está subdividido, em termos do modelo de processos definido para este projecto, em 3 actividades:

1. Recepção, Organização e Registo do Requerimento;
2. Identificação do Beneficiário;
3. Envio e Integração de Informação ao CNP.

1.2. RECEPÇÃO, ORGANIZAÇÃO E REGISTO DO REQUERIMENTO

1.2.1. DESCRIÇÃO DA ACTIVIDADE

A actividade de Recepção e Registo de Requerimentos tem como objectivo a recepção e conferência dos elementos necessários para que a informação fundamental para a instrução de um processo de pensão seja registada nos sistemas aplicativos pertinentes, assegurando, por outro lado, que os documentos obrigatórios estão presentes junto ao requerimento da pensão, antes do seu envio para o CNP.

1.2.2. SITUAÇÃO ACTUAL

Os procedimentos inerentes a esta actividade estão adequadamente detalhados no *Manual de Procedimentos* elaborado pelo ISSS, tendo suporte no Decreto-Lei n.º 316-A/2000, de 7 de Dezembro, que atribui aos CDSSS a responsabilidade pela execução das medidas necessárias para o reconhecimento de direitos à atribuição e pagamento de prestações, com excepção daquelas que são da competência do CNP. Com base na interpretação desta lei, os CDSSS têm a responsabilidade de preparar o processo de requerimento até ao ponto em que ele esteja suficientemente instruído para que o CNP possa proceder ao reconhecimento do direito à pensão e efectuar o seu cálculo.



Tribunal de Contas

A avaliação desta actividade apontou para os seguintes aspectos que merecem uma maior atenção:

REGISTO DO REQUERIMENTO

A recepção do requerimento resulta na emissão de um recibo manual entregue ao requerente. Os procedimentos actuais requerem que seja efectuado, em livro próprio, um registo manual pela data de entrada do requerimento, criando, assim, um número único, sequencial por dia. Considera-se, no entanto, que é difícil assegurar que não existam omissões na numeração de requerimentos. Dado que a recepção do requerimento e a emissão do recibo não estão informatizadas, é muito laborioso averiguar a situação de cada requerimento, existindo uma grande dificuldade em estabelecer um rasto fiável desde o momento da sua entrega pelo requerente até ao seu eventual deferimento pelo CNP. Neste momento, no caso de um requerimento se extraviar antes do seu registo no sistema (FCR), é muito provável que a situação somente seja detectada quando o requerente reclamar junto do CDSSS ou do CNP.

O sistema actual associa um requerimento directamente ao número de beneficiário, permitindo identificar todos os requerimentos relativos a esse número. Nas pensões de sobrevivência é, de facto, possível existirem vários requerimentos relativos ao mesmo beneficiário. O acesso aos programas de criação de requerimentos no sistema está limitado aos funcionários com as competências devidas.

O requerimento é registado no sistema do CNP, mas a introdução da carreira contributiva do requerente depende da integração destes dados provenientes de outros sistemas distritais. A introdução, em 1994, dos requisitos mínimos da densidade contributiva para futuros descontos criou uma situação transitória em que não existiam dados suficientes nos sistemas informáticos para efectivar o cálculo de pensões de acordo com as regras do Decreto-Lei n.º 329/93, de 25 de Setembro. Esta situação impôs que os dados referentes à carreira contributiva fossem “carregados” pelo CNP e os CDSSS após o registo de um requerimento. Este carregamento não está adequadamente sistematizado de forma a assegurar que todos os elementos necessários para a instrução do processo de uma pensão estejam completos e disponíveis após esta actividade. A existência de informação omissa resulta no envio de processos incompletos para o CNP, o que representa, posteriormente, um trabalho administrativo adicional para esta entidade.

PRIORIDADE DOS REQUERIMENTOS

O processo actual não distingue, em termos da prioridade dada ao seu processamento, requerimentos de cálculo definitivo e de cálculo provável, o que aumenta o número de processos a tratar por todo o sistema, sem dar a devida prioridade aos processos mais urgentes. Embora o ISSS disponibilize aplicações na sua página *Web* para a simulação de cálculo de pensões, o sistema continua a ter uma carga significativa de requerimentos de cálculos de pensões prováveis.



Tribunal de Contas

Note-se que o prazo para atribuição de uma pensão é de três meses nos termos da lei geral (art.º 58.º do Código do Procedimento Administrativo).

No caso da pensão de velhice, os requerimentos podem ser recebidos (data de gravação) até ao máximo de três meses antes da data em que o beneficiário adquire o direito à prestação (artigo 78º do Decreto Lei n.º 329/93, de 25 de Setembro).

EFICIÊNCIA DO PROCESSO

O registo do requerimento nos sistemas acontece após a sua entrega nos CDSSS ou no CNP (no caso dos internacionais). Esta situação implica que, no caso de detecção posterior de omissões ou incoerências de informação entre a contida no pedido de requerimento e a existente nos sistemas do ISSS, seja necessário voltar a contactar o requerente para esclarecer dúvidas.

Considerando que a maior parte da informação sobre o requerente e a sua carreira contributiva inerentes a um requerimento já existe nos sistemas do ISSS, a disponibilidade de informação no sistema permitiria, não só uma pré-verificação dos dados do requerimento, como a redução do trabalho administrativo posterior, resultante da necessidade de contactar o requerente e, obviamente, dos tempos de espera inerentes.

Em sede de contraditório, o ISSS-CNP refere que:

“O sistema de informação não está, por opção, estruturado desse modo.

No formulário de requerimento de pensão, à excepção da identificação, apenas se pedem elementos que não constam do sistema da SSS ou, constando (caixas para onde descontou), são apenas indicativos tendo em vista uma melhor instrução.

O momento da entrega do requerimento pretende-se célere: a recolha dos elementos da carreira contributiva ou ocorreram antes (pelo beneficiário) ou ocorrem depois (pelo sistema).

No momento da entrega do formulário do requerimento, pretende-se que seja verificado se estão preenchidos todos os itens e solicitar o seu preenchimento, caso não estejam (e será um dos maiores contributos para a celeridade do processo).

Aliás, como é sabido, e dado o uso de formulário adequado, fica restringida à falta de assinatura do requerimento o fundamento para se recusar o seu recebimento (Artigo 740 e seguintes do CPA). Por outro lado, dada a relevância da data de entrega do requerimento para a definição do direito do requerente, há que não sobre-carregar esse momento com diligências instrutórias ou confirmativas.”

O alegado suscita o seguinte comentário: a falta de integração de sistemas, bem como a falta de funcionalidades que permitam verificar a informação entregue pelo requerente no acto de apresentação do requerimento, impossibilita a validação do requerimento perante o requerente e acrescenta uma carga administrativa adicional.



Tribunal de Contas

No caso das pensões de invalidez verificou-se que o processo pode ficar pendente, por um período que vai até seis meses, aguardando pelo Certificado de Invalidez. Esta situação resulta do facto da emissão deste certificado só acontecer após a entrada do requerimento de invalidez num CDSSS. Verificou-se também que não existe uma integração automática do parecer do CVIP, sendo este registado nos CDSSS.

INTEGRIDADE DA INFORMAÇÃO

Constatou-se que a interpretação dada a certos campos – v.g. data – varia conforme o tipo de pensão ou, mesmo, consoante o CDSSS que o introduz. A data do requerimento é, em certos casos, a data da aquisição do direito à pensão, sendo, noutros, a data de entrada no CDSSS – coincidente, neste último, com a data da gravação. Esta diferença, embora decorrente da legislação vigente, dificulta, quer a interpretação dos dados inerentes a um processo, quer o processo de conversão da informação no futuro.

Verificou-se, por outro lado, que as aplicações existentes não exigem o preenchimento de alguns campos relevantes para que o registo de um requerimento se possa considerar completo, como, por exemplo:

- a data de requerimento, embora obrigatória, não exige uma data validada (são permitidas datas inexistentes – 31/11/2000 ou 30 /02/2000);
- o preenchimento da data do parecer da junta médica para uma pensão de invalidez não é obrigatório e não é validado pelo sistema.

Estas situações resultam na impossibilidade de criar um rasto efectivo dos acontecimentos pertinentes a um requerimento.

Observou-se que a integridade e a qualidade dos dados relacionados com a carreira contributiva têm tendência para melhorar, dada a introdução, por parte do ISSS, da Declaração Anual de Contribuições. O confronto com os valores apresentados nesta declaração permite que possíveis erros possam ser detectados pelo contribuinte em questão.

De acordo com os testes efectuados, não é possível existir mais que um requerimento do mesmo tipo de pensão, com a mesma data e para o mesmo beneficiário.

O ISSS vem alegar que:

“A data de gravação é automaticamente a data do sistema.

A data do requerimento é meramente indicativa, apenas para indicadores de gestão. A data efectiva de início da pensão é determinada, aquando do reconhecimento do direito, de acordo com a legislação em vigor, não sendo necessariamente coincidente com a data aposta ou registada para o requerimento.”



Tribunal de Contas

O alegado suscita o seguinte comentário: a data de gravação é automática, mas, na maioria dos casos, pode não representar a data de apresentação dos requerimento. Assim, qualquer avaliação de desempenho deste processo está sempre sujeita a problemas de interpretação.

MONITORIZAÇÃO DA ACTIVIDADE

A falta de informatização no início desta actividade contribui para a falta de indicadores de gestão que permitam avaliar a qualidade e fiabilidade da gestão de requerimentos. Ainda assim, os responsáveis pelos vários CDSSS efectuem, de facto, esforços para produzirem estatísticas sobre a gestão dos requerimentos processados. Existe uma lista de requerimentos pendentes que é produzida anualmente pelo CNP para tentar dar resposta a esta questão; no entanto, esta listagem apenas consegue identificar situações anómalas no caso do requerimento ser registado no sistema. O controlo mais efectivo nestas situações é a reclamação do requerente, quando não tem comunicação do CDSSS, dentro de um prazo razoável, sobre o seu processo. Considera-se que esta actividade carece de uma maior e mais atempada informação sobre o estado do requerimento, de forma a permitir uma gestão mais eficaz dos processos em curso.

Nas suas alegações, afirma o ISSS:

“Desde que o requerimento se encontre gravado no Ficheiro Central de Requerentes (FCR), se existem anomalias, serão detectadas através do tratamento de listagens que (de forma pró-activa) são solicitadas periodicamente à unidade de Informática do ISSS CNP.”

No entanto, de acordo com a evidência recolhida no decurso da auditoria, a listagem é apenas requisitada anualmente, periodicidade que poderá não ser suficiente para uma detecção atempada de eventuais anomalias.

1.2.3. RISCOS SIGNIFICATIVOS IDENTIFICADOS E SEUS IMPACTES

Os riscos mais significativos desta actividade estão relacionados com o facto de a mesma não estar direccionada para a identificação de incoerências e deficiências nos requerimentos aceites, contribuindo, assim, para o surgimento dos seguintes riscos:

- ineficiência do processamento de requerimentos que antecede as actividades seguintes;
- falta de definição de prioridades para os requerimentos recebidos e processados;
- criação de um rasto inadequado sobre um requerimento que entre no sistema; e
- criação de registos informáticos incompletos nas aplicações sobre os requerimentos a tratar.



Tribunal de Contas

A integridade deste processo depende significativamente do esforço das pessoas que o suportam. A falta de alguns controlos chave poderá aumentar a possibilidade de erros humanos na gestão dos requerimentos. A melhoria de controlos nesta actividade implicaria aumentar o nível de informatização da mesma, o que contribuiria para uma melhoria significativa na monitorização desta actividade, bem como para a detecção atempada de problemas e atrasos no processamento de requerimentos.

1.2.4. AVALIAÇÃO GLOBAL DA MATURIDADE DA ACTIVIDADE – REPETITIVO

- Existem práticas definidas e documentadas num Manual de Procedimentos e uma transmissão verbal das práticas inerentes à actividade; considera-se, no entanto, que o processo não está suficientemente informatizado para assegurar a integridade e fiabilidade da informação, sendo a sua monitorização reactiva (actua depois da identificação dos problemas);
- Houve, todavia, um esforço de envolver e definir os vários elementos conhecedores das práticas existentes para a definição do Manual de Procedimentos e sistematização das práticas inerentes à actividade.

1.3. IDENTIFICAÇÃO DO BENEFICIÁRIO

1.3.1. DESCRIÇÃO DA ACTIVIDADE

A actividade de Identificação de Beneficiários visa a validação dos elementos identificativos do requerente, bem como a atribuição de número de beneficiário único nacional, caso existam duplicações ou outros problemas a ele associados.

1.3.2. SITUAÇÃO ACTUAL

O CNP criou uma Base de Dados Nacional de Beneficiários e Utentes com os registos de todos os beneficiários que participam no SSSS.

Esta base de dados tem, ao longo dos anos, integrado os beneficiários registados nos CDSSS e nas várias caixas de previdência que, entretanto, foram assimiladas pelo SSSS. Este histórico de integração de informação de várias fontes introduziu algumas carências na qualidade dos dados existentes nesta base de dados. Esta situação levou a que, quer os CDSSS, quer o CNP tenham efectuado um esforço adicional para assegurar a correcta identificação do beneficiário. A análise desta actividade e a inspecção manual efectuada aos processos, revelaram que, em todos os casos, havia provas documentais suficientes para comprovar a identificação do beneficiário de modo a ser correctamente efectuada a validação da identificação do requerente. As alterações dos



Tribunal de Contas

registos de identificação de beneficiários têm sido, nos últimos anos, adequadamente controladas pelo CNP.

Os testes efectuados não apontaram para a existência de registos duplicados com base no número de beneficiário. No entanto, é verosímil a existência de um beneficiário com mais de um número registado na base de dados. Neste momento os responsáveis da Unidade de SI do CNP não têm capacidade para detectar estas situações, mas adoptaram procedimentos para efectuar a sua correcção, sendo esta suportada pela apresentação de documentos por parte do requerente e efectuada somente pelo CNP. A correcção de um número de beneficiário, implica, normalmente, a correcção da carreira contributiva associada a esse número.

“Apenas poderá existir mais que um número de beneficiário para a mesma pessoa, no caso das inscrições antigas, anteriores à integração das Caixas Sindicais de Previdência e à introdução do conceito de “número nacional”.

...

Depois da introdução do conceito de “número nacional” de beneficiário, é assegurado que para a mesma “chave de identificação” (mesmo nome, data de nascimento e naturalidade) apenas é atribuído e apenas existe um único número de beneficiário.” (alegações do ISSS).

1.3.3. RISCOS SIGNIFICATIVOS IDENTIFICADOS E SEUS IMPACTES

Os riscos nesta actividade estão associados à integridade da informação existente na BDNBU. Apesar de existir o risco de anomalias na informação existente na BDNBU, verifica-se uma tendência para a sua redução, através da identificação e correcção de anteriores erros. Esta actividade está razoavelmente bem controlada, ainda que tenham ocorrido vários problemas no passado.

1.3.4. AVALIAÇÃO DA MATURIDADE DA ACTIVIDADE – GERIDO

- Existe um claro entendimento da importância desta actividade e uma clara definição das responsabilidades atribuídas para a sua execução;
- Esta actividade está adequadamente informatizada, embora a tecnologia utilizada tenha algumas carências;
- Existe uma grande preocupação em assegurar uma correcta identificação do beneficiário, sendo este aspecto confirmado pelos testes efectuados;
- Esta actividade tem sido sujeita a melhorias constantes no passado, afigurando-se positiva a introdução, a curto prazo, da nova aplicação de identificação.



Tribunal de Contas

1.4. ENVIO E INTEGRAÇÃO DE INFORMAÇÃO COM O CNP

1.4.1. DESCRIÇÃO DA ACTIVIDADE

Esta actividade visa a introdução da informação sobre os processos de pensão, validados pelos CDSSS, nos sistemas do CNP, para que este efectue o eventual deferimento e cálculo da pensão. Contempla o controlo, por parte dos vários centros distritais, do envio de dados e dos processos físicos de requerimentos para o CNP.

Em sede de contraditório o ISSS-CNP esclarece:

“Contudo existe também um registo informático, quando o requerimento é enviado pelo CDSSS ao CNP e um outro registo de entrada neste organismo.”

1.4.2. SITUAÇÃO ACTUAL

O envio de processos para o CNP é feito através de um procedimento manual, suportado por um protocolo, que garante a comunicação entre as entidades envolvidas. O registo do requerimento é efectuado num sistema partilhado pelos CDSSS e pelo CNP. Os valores mensais de salários/contribuições e o cálculo da densidade contributiva, registados nas bases de dados de carreira contributiva dos centros distritais, são enviados em suporte electrónico, quando possível. No caso dos dados dos centros distritais com plataformas ICL, a integração destes dados está ainda em fase de teste.

Durante o ano de 2000 e até Novembro de 2001, sempre que esta informação estava incompleta nos sistemas do CNP, relativamente aos anos relevantes para o cálculo de pensões, a mesma era introduzida pelos funcionários do CNP directamente nos ficheiros de cálculo, com base nas listagens enviadas pelos centros distritais. Actualmente, os centros distritais (com excepção dos CDSSS com plataforma ICL) enviam ao CNP os dados relativos à carreira contributiva até 2000, os quais foram integrados na BNDBU. A consistência entre os dados posteriormente integrados e os dados utilizados para o cálculo ainda não foi confirmada.

Foram feitos esforços para avaliar a consistência da integração da informação recebida dos centros distritais com a registada na BNDBU, no entanto, adveniente dos atrasos na entrega dos dados, não foi possível dispor, atempadamente, de toda a informação necessária para a efectivação dos testes à integridade dos dados na BNDBU. Mesmo onde este procedimento de integração automática era possível, foi observado que o mesmo só é efectuado anualmente, resultando num desfazamento mínimo de um ano entre a carreira contributiva registada nos sistemas distritais e a constante dos sistemas do CNP. Este facto dá origem a que os últimos anos da carreira



Tribunal de Contas

contributiva tenham sempre que ser “carregados” para efeitos do cálculo. No caso do processo ser enviado para o CNP, não existe qualquer procedimento que valide, de forma independente, que o processo está completo, isto é, se contém todos os dados e elementos necessários para o seu eventual deferimento pelo CNP.

Quando o requerimento é transferido entre Centros Distritais (no caso de o processo não ter dado entrada no centro distrital da área residencial do requerente) para completar o seu processamento, a transferência efectua-se mediante ofício entre as entidades envolvidas, muito embora não tenha sido possível averiguar se este procedimento acontece sempre.

Em Outubro de 2001 constatou-se, nos vários centros distritais, que os dados relacionados com a carreira contributiva estavam na seguinte situação:

- CDSSS Setúbal – todos os dados até 2000 estavam integrados nos sistemas do CNP;
- CDSSS Norte – os dados até 1994 estavam integrados, mas os dados relativos aos restantes anos até 2000 só foram enviados em Dezembro de 2001, não estando ainda integrados;
- CDSSS Lisboa – estavam integrados todos os dados até 1999, sendo os respeitantes a 2000 integrados em Dezembro 2001.

No caso do CDSSS Norte havia inconsistências entre as duas bases de dados que suportavam o registo da carreira contributiva, devido a problemas com a sua sincronização.

1.4.3. RISCOS SIGNIFICATIVOS IDENTIFICADOS E SEUS IMPACTES

A integração da carreira contributiva encontra-se razoavelmente controlada, mas a forma como é efectuada não contribui para uma maior eficiência do processo. Em Dezembro de 2001, os CDSSS tiveram que fazer um esforço significativo para recuperar as carreiras contributivas em atraso até à data da conversão dos seus sistemas para o EURO, continuando, ainda assim, a haver atrasos no envio desta informação por parte de alguns centros distritais. Esta realidade cria situações em que:

- o deferimento do processo sofre atrasos devido à falta de informação necessária; e
- implica um acréscimo de carga administrativa necessária para o deferimento de um processo.

1.4.4. AVALIAÇÃO DA MATURIDADE DA ACTIVIDADE – REPETITIVO

- Existe uma consciência adequada da importância desta actividade e um razoável nível de comunicação para resolver os problemas a ela inerentes;



Tribunal de Contas

- A actividade está padronizada por plataforma, mas a resolução de problemas é intuitiva;
- Face à diversidade de plataformas informáticas existentes nos centros distritais, há um reconhecimento da necessidade de existirem mecanismos de integração uniformes;
- Há uma monitorização limitada e reactiva da actividade, mas o fenómeno da conversão dos sistemas para EURO obrigou a que esta fosse objecto de uma mais apertada monitorização.

2. Processo de Atribuição e Cálculo de Pensões

O Processo de Atribuição e Cálculo de Pensões tem como objectivo a verificação do direito à pensão, o seu deferimento/indeferimento e o cálculo da pensão atribuída. Este processo inicia-se com a recepção, pelo CNP, do requerimento vindo dos CDSSS e termina com a realização do cálculo da pensão ou com o eventual indeferimento e arquivamento do requerimento, estando subdividido em duas actividades, fundamentais:

1. Conferência e Deferimento/Indeferimento dos Processos; e
2. Cálculo da Pensão.

2.1. A CONFERÊNCIA E DEFERIMENTO DE PROCESSOS

2.1.1. DESCRIÇÃO DA ACTIVIDADE

Esta actividade visa a conferência dos requerimentos e processos recebidos dos CDSSS e a solicitação dos documentos em falta, bem como a atribuição do direito à pensão resultante do respectivo deferimento, respeitados que sejam todos os requisitos legais.

2.1.2. SITUAÇÃO ACTUAL

O Manual de Procedimentos de Pensões, elaborado ao abrigo do despacho n.º 47-I/SESSRL/99, de 20 de Agosto, estabelece que o CNP deve proceder à verificação e conferência dos documentos subjacentes a um processo de requerimento, bem como à validação de que o pensionista requerente não é já um pensionista existente. Como anteriormente referido, esta actividade tem sofrido alguns atrasos no CNP devido às inúmeras ocorrências de processos incompletos. De referir que, relativamente a esta matéria, não foi constatada a existência de estatísticas, por parte do CNP ou dos centros distritais, que reflectissem a situação atrás descrita, sendo difícil, sem este tipo de dados, avaliar os impactes e apontar as causas inerentes a este problema.



Tribunal de Contas

Esta actividade, tal como definida, requer a existência de uma segregação de funções clara entre o organizador, o conferente e o responsável pelo deferimento do processo (normalmente o Chefe de Secção ou Chefe de Divisão). Assim, nos procedimentos internos do CNP, o deferimento de um requerimento só pode ser efectuado pelo Chefe de Secção/Divisão visto que, por delegação de competências, são eles os únicos possuidores das necessárias competências para o efeito.

Os testes efectuados sobre a amostra dos processos “manuais”, deferidos em 2000, apontaram para uma percentagem significativa de situações onde esta segregação de funções não teria sido respeitada, em virtude de os despachos de deferimento terem sido, aparentemente, exarados por pessoas sem competência para o efeito.

A este propósito, vem o ISSS alegar:

“(...) a decisão final sobre um pedido de pensão apenas pode ser tomada por quem tenha competências delegadas para o efeito.

Assim, não pode, de modo algum, confirmar-se que haja pedidos de pensão com deferimento efectuado por conferente ou por assistente administrativo especialista.

Esse “despacho” ou consta directamente do suporte de informação elaborado para cada processo ou consta duma relação elaborada para o efeito e cuja existência o relato constata.”

No entanto, no decurso dos trabalhos de campo da auditoria, em entrevista com responsáveis com competência delegada para o deferimento, estes, confrontados com as situações detectadas, referiram que, não sendo o procedimento usual, essa eventualidade poderia ter ocorrido face à falta ocasional de recursos humanos disponíveis para dar resposta a um volume crescente de processos a tratar. Não foi, na altura, feita referência ao facto de os processos em causa poderem ter sido deferidos por relação.

Em 9% dos casos não se encontraram evidências do despacho proferido pela pessoa competente para o efeito, tratando-se, na maior parte destes casos, de pensões “unificadas”, portanto pensões com parcelas atribuídas pela Caixa Geral de Aposentações (CGA). Note-se que, nos casos em que a CGA é o último regime do beneficiário, e apesar de o deferimento ser por ela efectuado, considera-se ser sempre necessário o parecer conclusivo e vinculativo do CNP sobre a decisão a tomar, relativo à atribuição e pagamento da prestação. Por outro lado, os testes efectuados identificaram que, em 26% dos processos, não existe evidência de que os mesmos tenham sido conferidos pelo chefe da unidade, sendo, segundo os responsáveis do CNP, consequência da falta de recursos humanos especializados para dar resposta a um volume crescente de processos tratados.

O ISSS, no exercício do direito de contraditório, vem esclarecer que:

“Mesmo nos casos de participação à CGA, em que o despacho não é da competência do CNP, utilizam-se suportes de informação, criados para esse fim, que prevêem o visto e anuência do Chefe de Equipa e do Director de Núcleo;

No entanto, quando é devida participação ao abrigo de vários regimes ou diplomas ou há lugar a uma participação e à concessão de uma pensão autónoma pode



Tribunal de Contas

acontecer que todos os direitos sejam analisados e deferidos numa só informação, pelo respectivo chefe de secção, muito embora, por necessidades informáticas, possa haver vários suportes de cálculo diferentes, assinados apenas pelos organizadores e pelos conferentes.”

À data da conclusão dos trabalhos de campo, os dados da carreira contributiva para o ano 2000 ainda não tinham sido disponibilizados pelos centros distritais e não iriam sê-lo em tempo útil, impossibilitando que fossem cruzados com os utilizados no cálculo dos processos deferidos. Ainda assim, considera-se que eventuais erros nesta actividade serão detectados pelo pensionista quando confrontado com a comunicação que lhe é enviada pelo CNP.

2.1.3. RISCOS SIGNIFICATIVOS IDENTIFICADOS E SEUS IMPACTES

O risco mais significativo e que requer uma maior atenção é o relativo à execução de determinadas funções por funcionários do CNP sem competência para tal. Por outro lado, a ausência da segregação de funções não oferece níveis de confiança adequados para que possíveis erros sejam atempadamente detectados e corrigidos.

2.1.4. AVALIAÇÃO DA MATURIDADE DA ACTIVIDADE – GERIDO

- O deferimento de uma pensão está estabelecido por lei, bem como todos os requisitos documentais inerentes;
- Existe um entendimento adequado das formalidades legais subjacentes e a definição de responsabilidades para esta actividade por parte do CNP;
- Existe um envolvimento por parte dos serviços jurídicos e da secção internacional para resolver eventuais problemas;
- O cumprimento das delegações de competências necessita de alguma melhoria para assegurar uma adequada segregação de funções.

2.2. O CÁLCULO DA PENSÃO

2.2.1. DESCRIÇÃO DA ACTIVIDADE

Esta actividade visa o cálculo da pensão, provisória ou definitiva, de sobrevivência, invalidez ou velhice, com base na carreira contributiva do beneficiário e de acordo com a legislação aplicável.

O cálculo é efectuado, na maioria dos casos, imediatamente após do deferimento do processo, com base nos elementos de informação disponíveis. No caso da omissão de informação pertinente,



Tribunal de Contas

é efectuado um cálculo provisório dando origem a uma pensão provisória, ainda que esta represente somente o valor da pensão mínima.

2.2.2. SITUAÇÃO ACTUAL

O cálculo da pensão é efectuado directamente no sistema do CNP após a integração da informação necessária para a execução deste programa. O resultado do cálculo é registado no sistema e um verbete resumo do cálculo é impresso e uma cópia enviada ao beneficiário. Nos casos em que o beneficiário era já titular de uma pensão de velhice ou invalidez, a pensão de sobrevivência devida traduz-se na mera repartição do valor da pensão existente, considerando-se este um tratamento aceitável, uma vez que os dados base utilizados para as três pensões são os mesmos.

A maioria dos cálculos é efectuada automaticamente, com base na informação registada nos sistemas do CNP, existindo, ainda assim, um volume significativo de cálculos “manuais” que, em grande parte dos casos, diz respeito a pensões que não se enquadram dentro do Regime Geral “puro”. Esta situação dá indicações de que o sistema do CNP não consegue dar resposta a muitas situações onde o conjunto de legislação a considerar no cálculo da pensão se desvia significativamente do referido Regime.

Segundo o ISSS:

“Deve assinalar-se que, quando entra em vigor nova legislação, é normal não haver de imediato programa de cálculo testado e disponível para dar execução às novas normas legais. Foi, designadamente, o caso do DL-119/99, de 14 de Abril, que veio introduzir uma nova modalidade de pensão antecipada (...)”

2.2.3. RESULTADOS DOS TESTES EFECTUADOS

Após a identificação das primeiras diferenças de cálculo, com recurso a reuniões com os responsáveis do CNP, concluiu-se que, por um lado, devido à existência, entre os dados de cálculo das pensões por sobrevivência, de dados que apenas servem de base aos cálculos de Subsídios de Morte (que não fazem parte do âmbito global deste trabalho) e, por outro, devido à existência de processos calculados manualmente, os dados que foram entregues pelo CNP não se apresentavam correctos para efeito de recálculo daquelas pensões. Em resultado, foram pedidos novos ficheiros de cálculo, os quais foram disponibilizados em finais de Dezembro de 2001.



Tribunal de Contas

Em meados de Janeiro de 2002 foi necessário requerer novos ficheiros de cálculo de pensões de sobrevivência, visto que os então recebidos careciam de elementos relativos ao agregado familiar do falecido (“produtor” da pensão). Estes novos ficheiros foram recebidos em finais de Janeiro do corrente ano. Estes factores, apesar de imprevisíveis, aliados à complexidade que está na base de todo este processo de cálculo e validação de pensões (mesmo que seja apenas considerado o Regime Geral) constituíram um elemento constrangedor, originando, por um lado, alguns atrasos no desenvolvimento do trabalho e obrigando, por outro, a assumir pressupostos que, de outra forma, não seriam necessários.

Na execução do trabalho identificaram-se, ainda, algumas limitações ao longo do processo de recálculo de pensões que afectaram a abordagem dos testes efectuados e que se consideram importantes para a interpretação dos resultados. Estas limitações incluem:

➤ Processos “Manuais”

Após a análise do universo dos processos deferidos em 2000 (cerca de 135.000), identificaram-se 2.571 em que as pensões atribuídas foram objecto, por parte do CNP, de um cálculo manual, ou seja, o apuramento do valor da pensão a atribuir foi calculado com recurso a ferramentas não informáticas, por inexistência de programas de uso corrente no CNP que contemplem os regimes específicos ou as especificidades determinadas por lei.

Assim, foi necessário expurgar os processos “manuais” do universo previamente definido e a estes foi dado um tratamento alternativo. Esta triagem de processos “manuais” foi efectuada a partir de ficheiros informáticos disponibilizados pelo CNP, tendo como base o cruzamento entre os registos constantes do ficheiro de pensionistas, onde estão, portanto, inscritas as pensões efectivamente atribuídas, e os que constavam do ficheiro de cálculo. Assim, todos os registos constantes do ficheiro de pensionistas que não estivessem considerados no ficheiro de cálculo seriam, necessariamente, processos com cálculos manuais.

Este tratamento decorre do facto de se tratarem de eventualidades para as quais não foram desenvolvidos programas específicos, o que obrigou a um trabalho casuístico, quer da análise da legislação específica aplicável a cada um deles, quer, em última instância, do apuramento do valor da pensão a atribuir.

Alega o ISSS que:

“...não há cálculos manuais ou efectuados com recurso a ferramentas não informáticas. Haverá, sim, inclusão manual de pensões, após cálculo informático do montante provável e aplicação das especialidades adequadas ao resultado obtido. Aliás, cada vez mais a complexidade do cálculo duma pensão impedirá que se possa calcular uma pensão com uma simples máquina de calcular.”

No entanto, muitos dos processos analisados não incluíam qualquer documento comprovativo de cálculo informático, mas apenas fitas de máquina de calcular.



➤ Diferenças Temporais nos Dados

O trabalho desenvolvido prendeu-se com a forma como as parcelas das pensões se encontram registadas no ficheiro de Pensionistas. O facto de o ficheiro de Pensionistas (que possui o suporte informático para os processamentos de pensões do ano) apagar o registo de pensão anterior, quando existe um novo cálculo da pensão em causa, dando origem a um novo processamento, impossibilita qualquer trabalho de recálculo directo, bem como de auditoria (dado que o rasto de auditoria nesta situação é simplesmente inexistente). Como exemplo, é impossível validar, de forma automática, uma pensão de um beneficiário que possua uma pensão de invalidez, no início do ano de 2000, passando para pensão de velhice a meio do mesmo ano, pois o registo anterior é substituído por este último.

Dado que a extracção dos dados analisados foi efectuada somente em Novembro 2001, os mesmos continham já todos os cálculos processados e todas as alterações efectuadas durante o ano de 2001. Para compensar este efeito, foi imperativo ajustar o cálculo, procedendo às alterações necessárias, para ir ao encontro dos cálculos do CNP. Assim, foi também necessário considerar todas as alterações do ano 2001 de modo a poder-se chegar aos resultados dos cálculos de pensões existentes nos ficheiros recebidos do CNP.

Nas suas alegações, o ISSS afirma:

“Quando se procede a uma revisão de pensão, devida a novos elementos para cálculo ou a uma actualização de pensão resultado da aplicação de legislação, os novos dados substituem os existentes no ficheiro base de pensionistas.

No entanto, o ficheiro de cálculo de pensões, possui todo o histórico dos diferentes cálculos efectuados para o beneficiário.

As actualizações de pensões produzem listagens com os elementos antes da actualização e os posteriores, para todas as pensões actualizadas.

Estas listagens produziram, até ao ano 2000, micro-fichas que podem ser consultadas quando necessário.”

Ora, o que se verificou foi que não existe um rasto completo que permita recriar o histórico dos valores no ficheiro de Pensionistas utilizados para o cálculo, mas somente o resultado de cálculos anteriormente efectuados, registado no ficheiro de pensões. Ainda assim, é possível recorrer a listagens de cálculos efectuados no passado em suporte de papel, mas, para os efeitos da auditoria, tal seria impraticável, face ao volume de processos analisados.

➤ Carreiras Contributivas



Tribunal de Contas

À data da execução dos testes detectou-se que as carreiras contributivas ainda tinham atrasos significativos no seu carregamento e envio para o CNP. O facto de esses mesmos dados não se encontrarem suficientemente actualizados, aliado à circunstância da entrega dos dados relacionados com a carreira contributiva ter sido efectuada numa fase já avançada do trabalho, impossibilitou que se testassem informaticamente os seguintes aspectos:

- o cumprimento dos prazos de garantia;
- a selecção dos 10 melhores anos de salário utilizados para o cálculo;
- a densidade contributiva dos mesmos; e
- a integração correcta dos dados recebidos dos sistemas dos vários CDSSS.

Os testes necessários para salvaguardar o correcto tratamento destes aspectos do cálculo foram efectuados de forma manual e por amostragem. Pela razão anteriormente referida, assumiram-se como correctos, nos cálculos efectuados automaticamente, os dados relativos aos salários (originais e revalorizados) e prazos de garantia dos pensionistas que tiveram pensões de velhice do Regime Geral deferidas durante o ano de 2000.

➤ **Pensão de Invalidez**

A atribuição da pensão de invalidez é efectuada com base num parecer da junta médica, a partir do qual o pensionista tem direito a uma pensão. Visto que a data de junta médica não é um campo obrigatório no sistema do CNP, não foi possível testar, de forma informática, a correcta atribuição desta pensão.

A avaliação efectuada desta actividade apontou para os seguintes aspectos que merecem uma maior atenção:

- a análise dos programas de cálculo revelou que os valores de pensão calculados e registados no ficheiro de pensionistas são gravados por cima dos registos existentes, eliminando o rasto das pensões pagas anteriormente. Dado que o processamento escreve por cima do registo anterior no ficheiro de pensionistas, não foi possível validar directamente a pensão calculada anteriormente. Apesar disso, reconhece-se que é possível, ao CNP, estabelecer o valor provavelmente pago;
- os programas utilizados para esta actividade não registam os salários omissos da carreira contributiva que são introduzidos no sistema no acto do cálculo. A futura integração dos salários omissos poderá criar algumas inconsistências, caso os registos das carreiras contributivas recebidos dos centros distritais não coincidam com os valores introduzidos manualmente no cálculo;



Tribunal de Contas

- embora se tenha conseguido simular e comparar a quase totalidade das pensões calculadas informaticamente, encontraram-se algumas situações em que foi necessário o esclarecimento por parte dos responsáveis do CNP. Estas situações resultam da complexidade e variedade de requisitos legais que são inerentes ao cálculo. Os testes efectuados indicam que o cálculo efectuado pelo sistema funciona correctamente. Considera-se, contudo, que não existe documentação suficientemente detalhada para:
 - discriminar todas as especificidades inerentes ao cálculo; e
 - permitir guardar um rasto adequado das alterações efectuadas.

Considera-se que, se estas especificidades não forem adequadamente documentadas e sistematizadas, poderão originar, no futuro, algumas dificuldades quanto à eficiente transmissão destes conhecimentos sobre os sistemas.

➤ Diferenças de Cálculo de Pensões

A tipificação das diferenças identificadas no recálculo informático das pensões resumem-se na tabela abaixo:

Tipificação das Diferenças Identificadas no Recálculo Informático

Resultado do Recálculo das Pensões	Parcela 01 Pensão Estatutária		Parcela 02 Actualizações	Parcela 11 Complemento Social	Parcela 22 Complemento o Dependência 1º Grau	Parcela 42 Complemento Dependência 2º Grau
	Beneficiário o Não Pensionista	Beneficiário o Pensionista (*)				
Total de Processos	109.135	25.734	38.750	67.211	1.266	472
Dos quais:						
Cálculos sem Diferenças	85,60%	49,93%	50,47%	71,70%	91,5%	93,2%
Cálculos com Diferenças:						
Suspensos	1,30%	7,01%	1,95%	4,09%	8,5%	6,6%
Pensões Especiais	9,09%	2,25%	28,72%	15,97%		
Fora do Regime Geral "puro":						
Contribuições no Estrangeiro	1,25%	8,97%	13,15%	6,78%		0,2%
Contribuições para a CGA	0,02%	0,20%		0,01%		
Processos "Manuais"	2,70%			0,40%		
Cálculos com Diferenças Não Conciliadas	0,05%	31,64%	5,72%	1,06%	0,0%	0,0%
TOTAIS	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%

(*) Pensões de sobrevivência cujo beneficiário era já pensionista à data de falecimento

De acordo com os resultados obtidos no recálculo automático das pensões, pertencentes ao Regime Geral "puro", as diferenças detectadas não são materialmente relevantes.

As diferenças não reconciliadas mais significativas estão relacionadas com pensões de sobrevivência, nos casos em que o falecido ("produtor" da pensão) era já pensionista à data do falecimento. Nestes casos, a pensão é calculada pela mera repartição da pensão existente do



Tribunal de Contas

“produtor”, que podia ou não ser do Regime Geral, ponderada pelos sobreviventes. Nestes casos, não existem dados suficientes nos ficheiros informáticos recebidos para suportar o cálculo das mesmas, sendo apenas efectuado o recálculo dos coeficientes e consequentes valores de pensão, atribuídos aos sobreviventes.

Embora o CNP pretenda examinar exaustivamente e explicar todas as diferenças detectadas, as limitações de tempo para a execução desta auditoria não permitiram o esclarecimento de todas as diferenças encontradas. Nos testes efectuados, as “diferenças” identificadas resultam de pequenas desconformidades no tratamento de arredondamentos. Refira-se, no entanto, que a maioria destas diferenças de arredondamento favorece o pensionista.

Na análise das outras diferenças encontradas observou-se a existência de situações onde os dados existentes sobre a carreira contributiva, nos sistemas e nos ficheiros recebidos, eram insuficientes para suportar o valor da pensão deferida. A identificação de diferenças nestes casos pode ter a sua origem nas pensões com referência a países estrangeiros ou a pensões cujo beneficiário apresentou contribuições para a CGA. Estes casos foram identificados por:

- código de país, no caso das pensões cujos beneficiários fizeram contribuições no estrangeiro;
- código de parcela específico (87), no caso das pensões cujos beneficiários efectuaram descontos para a CGA; e
- código de suspensão, no caso de pensões suspensas, por motivos vários, à data da extracção dos dados.

Nestes casos, as diferenças detectadas entre os recálculos efectuados e os valores processados pelo CNP foram identificadas, mas não foi possível assegurar que essas diferenças eram provenientes somente destes factores.

O ISSS vem esclarecer que:

“Dado que o recálculo das pensões de sobrevivência, de beneficiários falecidos na situação de pensionistas, foi efectuado com base nos salários introduzidos para cálculo do Subsídio por Morte em vez da utilização da pensão do produtor, cujo montante se encontra devidamente actualizado, os resultados tiveram que ser obviamente diferentes, e daí a indicação de 31,64% de diferenças não conciliadas apontadas no relato para a sobrevivência.

Quanto às diferenças encontradas para a parcela 02, devem-se ao facto de as pensões fornecidas terem também anos de início diferentes de 2000, sendo os valores fornecidos resultado de mais que uma actualização de pensões e o seu recálculo não ter sido efectuado aplicando as regras das várias portarias de forma autónoma, correspondente à evolução da pensão real do beneficiário.

As diferenças no Complemento Social, dado tratar-se de um diferencial, são o resultado das incorrecções referidas anteriormente.”



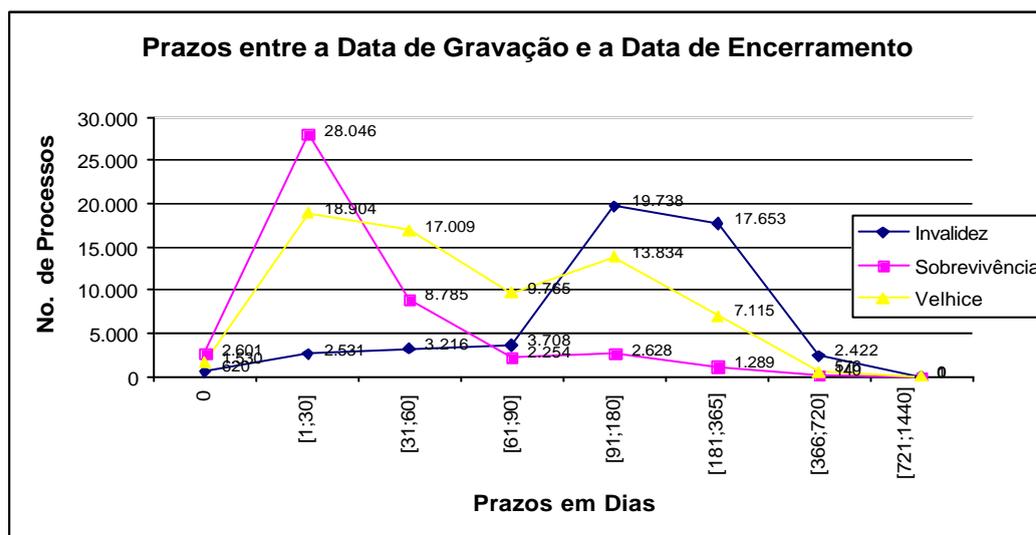
Tribunal de Contas

Quanto aos processos manuais, os erros detectados nos cálculos de pensões tinham por base, fundamentalmente: os designados “erros por simpatia”; deficiente aplicação de factores definidos em tabelas práticas; ou deficiente contagem da carreira contributiva, não derivando, na esmagadora maioria, de um incorrecto entendimento do processo e da legislação. Nos 394 processos analisados detectaram-se 14 erros de cálculo, o que corresponde a cerca de 3,5% da amostra analisada. A tipificação destas ocorrências consta no **Anexo D – Diferenças Detectadas nos Cálculos Manuais**.

➤ Eficiência da Actividade

Como parte da análise desta actividade avaliou-se os prazos médios de deferimento dos processos, observando-se a seguinte situação:

Prazos entre a Data de Gravação e a Data de Encerramento



A avaliação efectuada à eficiência deste processo demonstrou que os prazos de deferimento das pensões estão directamente relacionados com a natureza do requerimento. O gráfico acima confirma que o ISSS demora, em média, cerca de 30 dias para deferir um requerimento para atribuição de uma pensão de sobrevivência. Este prazo poderá ser justificado por, no caso de requerimentos de sobrevivência, a maior parte da informação necessária já existir nos sistemas do CNP, associada à pensão de velhice paga ao beneficiário antes de este falecer. Um requerimento para uma pensão de invalidez demora, em média, mais de 90 dias até ser deferido. Este prazo está directamente relacionado com o período de espera pela Certidão de Invalidez, emitida pelo CVIP. O prazo necessário ao deferimento de uma pensão de velhice pode estender-se de um mês a um ano. Considera-se que as causas prováveis para esta extensão do prazo estejam relacionadas com o envio, por parte dos CDSSS, de quantidade significativa de processos incompletos, em termos



Tribunal de Contas

de carreira contributiva, e com a existência de variados pensionistas com rendimentos no estrangeiro, implicando a obtenção de comprovativos junto de entidades externas.



Tribunal de Contas

2.2.4. RISCOS SIGNIFICATIVOS IDENTIFICADOS E SEUS IMPACTES

Considera-se que os riscos mais significativos desta actividade estão relacionados com a complexidade do cálculo e a probabilidade da ocorrência de erros quando este não é efectuado pelo sistema. Esta complexidade resulta directamente da legislação inerente ao mesmo.

2.2.5. AVALIAÇÃO GLOBAL DA ACTIVIDADE – REPETITIVO

- A avaliação desta actividade indica que a mesma é bem interpretada sob o ponto vista legal, havendo, no entanto, margem para a melhoria no entendimento do funcionamento dos programas de cálculo;
- Os erros mais frequentes, detectados nos processos, não resultam de uma deficiente interpretação da lei;
- Existem orientações documentadas e práticas definidas para a execução automática desta actividade;
- O cálculo encontra-se razoavelmente bem informatizado para as pensões do Regime Geral “puro”, mas ainda requer uma informatização significativa para os regimes especiais;
- Existe uma monitorização adequada do cálculo, baseada numa verificação manual posterior do cálculo efectuado pelo sistema, para os desvios de montante relevante, quando comparados com os processamentos anteriores.

2.3. PROCESSAMENTO E PAGAMENTO DE PENSÕES

Este processo inicia-se com o processamento mensal das pensões deferidas, calculadas e registadas no ficheiro de pensões e termina com a reconciliação dos pagamentos efectuados aos beneficiários e a emissão de estatísticas sobre as prestações. Está subdividido em três actividades:

- alteração periódica das pensões;
- processamento mensal das pensões; e
- pagamento das pensões.

2.4. ALTERAÇÃO PERIÓDICA DAS PENSÕES

2.4.1. DESCRIÇÃO DA ACTIVIDADE

Esta actividade tem como objectivo efectuar a alteração e actualização das pensões, resultantes de alterações na legislação, de novas informações que entram no cálculo e de novas categorias de pensão. A sua existência resulta do facto de o volume de alterações ser significativo e requerer



Tribunal de Contas

recursos importantes para assegurar que as pensões pagas estão correctas, face à informação disponibilizada pelo pensionista e de acordo com a legislação em vigor.

2.4.2. SITUAÇÃO ACTUAL

As alterações periódicas às pensões pagas podem ser divididas em duas grandes categorias:

➤ **Alterações introduzidas por legislação**

Estas podem resultar das seguintes situações:

- actualização anual ou específica das pensões,
- introdução de novos regimes ou categorias de pensão, e
- alteração das regras de aplicação de um regime existente.

As actualizações anuais ou pontuais dos valores das pensões são suportadas por programas que as executam de forma quase automática.

A introdução de novos regimes de pensão e a alteração das regras de aplicação de um regime existente podem resultar em novos programas de cálculos da pensão. Dado que a filosofia dos programas desenvolvidos não oferece muita flexibilidade em termos da sua parametrização, qualquer alteração desta natureza pode exigir um esforço significativo de programação para dar efeito a uma alteração legislativa no cálculo de uma pensão.

Por outro lado, os atrasos na comunicação de alterações legislativas, os prazos estabelecidos para a implementação das alterações daí resultantes e a natureza dos seus impactes sobre os programas existentes, dificultam, por vezes, o processo, resultando num maior risco da não detecção atempada de problemas ou erros de cálculo. Verificou-se, ainda, que a maioria das alterações são testadas e validadas pela Unidade Informática do CNP sem recurso aos elementos das outras Unidades. Salienta-se, no entanto, que não foram encontrados indícios de que tenha havido problemas na execução desta actividade no passado, resultado, em grande medida, do significativo esforço efectuado pelo CNP nesta área.

➤ **Alterações aos dados inerentes ao processo**

A alteração dos dados inerentes a uma pensão implica, por um lado, o seu recálculo e, por outro, o cálculo dos valores atrasados inerentes às referidas alterações. O pagamento dos valores em atraso resulta, muitas vezes, de situações onde o direito à pensão foi reconhecido mas, em consequência de informação omissa, não foi possível determinar, num primeiro momento, o valor real da pensão à qual o beneficiário tinha direito, sendo a diferença posteriormente reposta. Este



Tribunal de Contas

procedimento, protegendo o pensionista ao conceder-lhe uma pensão assim que lhe é reconhecido o direito à mesma, é resultado, em muitos casos, de atrasos administrativos a que este é alheio.

Em face do atrás descrito, diligenciou-se no sentido de efectuar testes à actualização dos cálculos das pensões. Constatou-se, porém, a existência de um obstáculo à sua realização, dada a impossibilidade de estabelecer, no final de 2000, a data efectiva da última actualização do cálculo das pensões; isto, porque o programa de cálculo substitui os valores anteriormente registados no ficheiro de pensionistas cada vez que um cálculo/recálculo é realizado. O sistema actual regista a existência de uma alteração efectuada a uma pensão mas não regista o detalhe suficiente para estabelecer o seu conteúdo. Ainda assim, os testes efectuados não indicaram quaisquer situações onde as alterações às pensões tivessem resultado em erros nas pensões pagas.

2.4.3. RISCOS SIGNIFICATIVOS IDENTIFICADOS E SEUS IMPACTES

Os riscos mais significativos inerentes a esta actividade resultam de uma possível situação onde não seja possível implementar as alterações legislativas em tempo útil, devido a atrasos na comunicação da mesma ou à existência, por alguma razão imprevisível, de incapacidade momentânea para disponibilizar o esforço necessário para efectivar as alterações legislativas.

2.4.4. AVALIAÇÃO DE MATURIDADE DA ACTIVIDADE – REPETITIVO

- Os responsáveis pelo CNP reconhecem a importância desta actividade, mas nem sempre lhes é dado um conhecimento prévio, total e atempado das alterações legislativas a efectuar, o que impossibilita a promoção da sua eficiência;
- O prazo apertado com que esta actividade é efectuada ainda não permitiu a sua padronização;
- Esta actividade implica o constante desenvolvimento de novos programas e não a parametrização do cálculo a efectuar, não permitindo, desta forma, melhorar a sua eficiência.

2.5. PROCESSAMENTO MENSAL DAS PENSÕES

2.5.1. DESCRIÇÃO DA ACTIVIDADE

O objectivo desta actividade é efectuar o processamento mensal das pensões relativas ao mês seguinte e a emissão de relatórios de controlo sobre os pagamentos a efectuar. Esta actividade inicia-se com a execução do processamento mensal de pensões e outros subsídios a pagar e termina com a preparação de bandas magnéticas com os registos dos pagamentos a efectuar.



Tribunal de Contas

2.5.2. SITUAÇÃO ACTUAL

O processamento mensal é efectuado com base no ficheiro de pensionistas, actualizado na actividade anterior. Este processamento efectua um resumo das pensões a pagar, emitindo os vários mapas estatísticos e financeiros necessários para preparação dos planos financeiros mensais, preparando, também, os ficheiros de pensionistas gravados em bandas magnéticas, com o registo das pensões a pagar, que são enviadas para os CTT e para os bancos para a efectivação dos pagamentos. O CNP emite um mapa com as variações das pensões relativamente ao mês homólogo do ano anterior, sendo estas comparadas e analisadas; no entanto, somente os valores globais das pensões pagas mensalmente estão sujeitos a análise, o que torna difícil a identificação de eventuais erros.

2.5.3. RISCOS SIGNIFICATIVOS IDENTIFICADOS E SEUS IMPACTES

O risco mais significativo deste processo está associado à possibilidade de existirem erros, no processamento do “batch” de cálculo das pensões a pagar, não detectados ou corrigidos atempadamente.

2.5.4. AVALIAÇÃO DA MATURIDADE DA ACTIVIDADE – DEFINIDO

- O CNP tem um conhecimento detalhado desta actividade e tem em funcionamento práticas razoavelmente bem definidas;
- Esta actividade está razoavelmente bem informatizada em termos da produção de informação estatística, mas o nível de informatização ainda não permite uma integração eficiente com as áreas financeiras;
- Este processo é monitorizado, considerando-se, ainda assim, que o controlo desta actividade pode ser melhorado com mais informação sobre o funcionamento dos seus controlos.

2.6. PAGAMENTO DAS PENSÕES

2.6.1. DESCRIÇÃO DA ACTIVIDADE

Esta actividade tem como objectivo a efectiva execução dos pagamentos de pensões aos beneficiários, através dos vários meios de pagamento utilizados pelo SSSS, o seu registo contabilístico e a reconciliação dos pagamentos e devoluções. Inicia-se com a preparação dos Planos Financeiros que servem de base para as transferências, do IGFSS para o CNP, das



Tribunal de Contas

dotações necessárias para a efectivação dos pagamentos de pensões, terminando com a reconciliação dos pagamentos efectuados pelos CTT e pelos bancos e respectivo registo das devoluções enviadas por estas entidades.

2.6.2. SITUAÇÃO ACTUAL¹

Os Planos Financeiros são preparados com base nos mapas de processamento, sendo enviados para o IGFSS para que as dotações de fundos necessárias sejam transferidas para as contas do CNP. Estes Planos não são automaticamente preparados pelo sistema informático, mas sim transcritos de vários mapas para uma folha de cálculo. As bandas com os registos electrónicos das pensões a pagar e as respectivas instruções de pagamento são enviadas para os Bancos e para os CTT, sendo os pagamentos efectuados e as devoluções recebidas reconciliados pelos Serviços Financeiros, com base na informação recebida destas entidades.

Os CTT enviam, neste momento, uma banda de retorno com a situação dos vales, permitindo a reconciliação dos vales devolvidos. Esta banda é integrada no sistema do CNP, de forma a permitir manter um registo dos vales enviados e devolvidos. No caso dos bancos, este procedimento não sucede. Este intercâmbio de informação entre o CNP e os bancos centralizadores de pagamentos é fundamental para assegurar o rasto dos pagamentos efectuados e para se poder apurar responsabilidades no caso de eventuais pagamentos indevidos.

Historicamente, a maioria dos pagamentos de pensões tem sido efectuado através de vales de correio, mas esta tendência irá, provavelmente, ser invertida, havendo, por parte do ISSS, um esforço substancial na promoção dos pagamentos por transferência bancária directa, não só por se tratar de uma forma mais expedita e segura de efectuar os pagamentos, como por razões de natureza financeira, já que o pagamento por vales de correio é mais dispendioso.

O CNP não tem, neste momento, capacidade de confirmar, de forma sistemática, que os pagamentos de pensões efectuados pelos bancos são de facto recebidos pelos beneficiários. Este aspecto é muito importante para assegurar que o CNP não está a pagar pensões indevidas a beneficiários já falecidos e para assegurar que não foi debitado duas vezes o mesmo pagamento.

No caso de beneficiários falecidos, o CNP recebe, do Ministério da Justiça, uma banda com registos de falecimentos, mas não tem capacidade de efectuar o cruzamento dessa informação com base num Número de Bilhete de Identidade ou um Número de Contribuinte, o que não facilita a sua identificação, resultando esta situação na incapacidade de, atempadamente, controlar os pagamentos efectuados indevidamente aos mesmos.

¹ Esta matéria foi, em parte, analisada com o recurso a uma ferramenta informática especialmente vocacionada para esta temática: o *DIGITAL ANALYSER*.



Tribunal de Contas

Os pagamentos efectuados pelos bancos, bem como as devoluções recebidas são reconciliados contabilisticamente. Na análise das reconciliações bancárias constatou-se que os registos contabilísticos são efectuados somente no fim do mês, criando uma situação onde a posição contabilística correcta dos bancos centralizadores só é possível estabelecer, também, no fim do mês. Dado que, por um lado, não existe a possibilidade de integrar os ficheiros de extracto de conta bancária e, por outro, subsiste uma grande dificuldade para identificar pensões individuais devolvidas, sucede:

- uma carga administrativa adicional significativa com a imputação desta informação;
- um desfasamento de dois meses, em média, na reconciliação das contas bancárias; e
- uma lista de pendentes significativa em cada mês.

A este respeito, diz o ISSS:

“Atendendo a que, nas devoluções enviadas pela banca, são discriminados os pensionistas e o valor das respectivas pensões, é possível efectuar, juntamente com o extracto bancário, a reconciliação bancária, uma vez que os créditos registados no extracto estão devidamente identificados, permitindo assim actualizar, sistematicamente, a posição bancária e proceder à contabilização no mês respectivo. A lista de pendentes referida, assim como o desfasamento de dois meses, em média, em valores por reconciliar só poderá existir nos casos de reposições de pensões e relativamente a valores que estejam por identificar.”

O alegado suscita o seguinte comentário: o detalhe da informação apresentada nos extractos de contas bancárias não é suficiente para identificar o pensionista subjacente a uma devolução, o que dificulta o processo de reconciliação. Assim, na maioria dos casos, é necessário recorrer aos bancos para obter informação adicional para efectuar a identificação correcta do pensionista.

2.6.3. RISCOS SIGNIFICATIVOS IDENTIFICADOS E SEUS IMPACTES

Os riscos significativos desta actividade encontram-se relacionados com a possibilidade de existirem pagamentos indevidos de pensões, em resultado de:

- alterações de ficheiros de pagamento que são enviados para as instituições bancárias através das bandas magnéticas;
- pagamentos indevidos de pensão de velhice/invalidez, perante a informação extemporânea dos falecimentos ocorridos; e
- os valores relativos a pensões não pagas (por ex., erros no NIB), poderem não ser devolvidos ao CNP ou serem creditadas em contas erradas.



Tribunal de Contas

2.6.4. *AVALIAÇÃO DA MATURIDADE DA ACTIVIDADE – DEFINIDO*

- Existe um claro entendimento da actividade, com práticas bem definidas e padronizadas, embora não suficientemente suportadas por sistemas de informação integrados;
- Existem mecanismos de monitorização reactivos, que apresentam uma grande dependência da reconciliação financeira dos pagamentos efectuados e devoluções recebidas.



Tribunal de Contas

3. Avaliação dos Processos de Gestão de TI

3.1. PLANEAMENTO E ESTRATÉGIA DE SISTEMAS DE INFORMAÇÃO

3.1.1. DESCRIÇÃO DO PROCESSO

O processo de Planeamento e Estratégia de Sistemas de Informação cobre a definição da estratégia tática e operacional dos sistemas e tecnologias de informação, preocupando-se com a identificação da melhor estratégia, através da qual as tecnologias e sistemas de informação podem contribuir para o alcance dos objectivos da Organização.

A realização da visão estratégica de tecnologias e sistemas de informação necessita de planeamento, comunicação e gestão em termos das suas várias perspectivas organizacionais, nomeadamente tecnologias, pessoas e processos.

Este processo está, segundo o modelo CobIT, subdividido em 11 actividades:

1. Definição da Estratégia de TI;
2. Definição de uma Arquitectura de Informação;
3. Definição da Direcção Tecnológica de TI;
4. Definição da Organização de TI e outras Interdependências;
5. Gestão dos Investimentos em TI;
6. Comunicação das Orientações Estratégicas;
7. Gestão dos Recursos Humanos;
8. Cumprimento de Requisitos Externos;
9. Avaliação de Riscos associados aos Processos de TI;
10. Gestão dos Projectos em Curso; e
11. Gestão da Qualidade.

3.1.2. DEFINIÇÃO DA ESTRATÉGIA DE TI

3.1.2.1 Descrição da Actividade

Esta actividade visa estabelecer um plano estratégico para as tecnologias e sistemas de informação, criando um equilíbrio entre as necessidades do SSSS e as oportunidades oferecidas pelas tecnologias de sistemas de informação, para que as actividades de cada unidade de Sistemas de Informação estejam adequadamente alinhadas com as estratégias definidas, capitalizando as vantagens providenciadas pelas capacidades de TI.



Tribunal de Contas

3.1.2.2 Situação Actual

A informática do SSSS demonstra uma longa tradição de descentralização, facto que criou um panorama significativo de plataformas e aplicações diferentes, para dar resposta a uma necessidade nacional de processamento de dados relacionados com o controlo e pagamento de prestações. A descentralização de sistemas permitiu a informatização dos centros regionais e distritais do SSSS mas, devido a factores como as limitações de ligações de telecomunicações, teve a desvantagem de não permitir obter as economias de escala que resultariam de um sistema nacional centralizado. A diversidade de sistemas trouxe também outros problemas, como a falta de integração de informação nos vários centros distritais e a inconsistência de informação nos vários sistemas informáticos do SSSS.

O Instituto de Informática e Estatística da Solidariedade (IIES), criado pelo DL n.º 115/98, de 4 de Maio, e que sucede à estrutura de projecto *ONI – Organismo Nacional de Informática*, tem como principal missão e objectivo a unificação das várias dezenas de sistemas informáticos, de modo a que a visão do cidadão e da empresa seja única e completa à escala nacional. O alcance deste objectivo permitirá a prestação de serviços com iguais padrões de qualidade em todo o território nacional.

O propósito do IIES é *“garantir, tanto para a operação actual da Segurança Social como para a sua reforma estrutural em curso, um sistema de informação que permita melhorar a colecta, controlar a dívida, combater a fraude, pagar atempadamente as prestações, sem que haja períodos de interrupção de rendimentos para os cidadãos, manter de forma única e coerente os históricos de direitos e deveres, em resumo prestar um serviço de qualidade, condizente com uma sociedade moderna e solidária e em que os recursos sociais sejam utilizados com a maior justiça e equidade e em que o reconhecimento de direitos e deveres seja universal e homogéneo a nível nacional”*².

O IIES tem, desde 1998, tem partilhado a responsabilidade pela definição da estratégia de sistemas de informação para o SSSS com as outras entidades do ISSSS e tem efectuado esforços para assegurar a sua execução. Esta estratégia visa, entre outros aspectos, os seguintes:

- a informatização do ciclo de vida de um cidadão no SSSS, desde o seu registo no sistema, até ser, eventualmente, beneficiário de uma pensão;
- o desenvolvimento de um sistema de identificação e qualificação nacional que suporte os vários regimes de protecção social actuais e futuros;
- a migração dos sistemas regionais para sistemas de âmbito nacional para melhorar a consistência e eficiência de informação;
- a padronização de plataformas tecnológicas para melhorar a integração dos sistemas nacionais, bem como a eficiência da sua manutenção e a capacidade de responder a alterações legislativas.

² Fonte: IIES.



Tribunal de Contas

A estratégia traçada ao longo dos anos tem tido os mesmos objectivos, mas os percursos seguidos têm variado consoante as mudanças organizacionais no ISSS. Estes factores originaram uma situação em que, embora a estratégia seja conhecida, esta não esteja totalmente formalizada e actualizada.

3.1.2.3 Riscos Significativos Identificados e Seus Impactes

Na avaliação deste processo, identificámos três riscos com níveis de impactes diferentes, nomeadamente:

➤ A Estratégia do Legislador *versus* a Estratégia de Sistemas de Informação

A estratégia de sistemas de informação de qualquer Organização depende directamente da estratégia de “negócio”. Assim, aquela deve estar sempre alinhada com as estratégias e os objectivos estabelecidos pela estratégia de “negócio”. A estratégia de sistemas de informação, definida pelo IIES, depende directamente dos objectivos estabelecidos pela legislação em vigor, podendo sofrer alterações periódicas consoante as orientações políticas que afectem, directa ou indirectamente, a estratégia de “negócio” do SSSS. Este fenómeno obriga a que a execução da estratégia de sistemas de informação esteja sempre atrasada face às necessidades estabelecidas pelo Estado. A redução do desfasamento temporal entre as necessidades estabelecidas pelo Estado e a implementação de sistemas que dão resposta a essas necessidades é, muitas vezes, um factor crítico para o alcance atempado dos objectivos estabelecidos. Assim, considera-se que a efectiva implementação da estratégia de sistemas de informação contribuiria fortemente para uma significativa melhoria do SSSS, designadamente nos seguintes aspectos:

- qualidade de serviços prestados ao público;
- maior eficácia do sistema;
- melhor planeamento financeiro dos recursos;
- redução dos custos de administração do sistema;
- maior confiança na informação produzida pelos sistemas de informação.

O IIES e o CNP têm acompanhado a evolução da legislação e têm avaliado os impactes da mesma na sua estratégia e nos seus sistemas de informação. No entanto, afigura-se que este acompanhamento é, por vezes, posterior à publicação das alterações legislativas. Considera-se que existe, por isso, o risco de os impactes sobre os sistemas de informação do SSSS, relativos às alterações à legislação, não serem devida e atempadamente considerados antes da sua promulgação.



➤ **Actualização da Estratégia de Sistemas de Informação**

O SSSS encontra-se numa fase de tomada de decisões estratégicas sobre investimentos de longo prazo em tecnologias de informação. É fundamental que, para tal, haja uma clara definição da estratégia de sistemas de informação a médio prazo, para assegurar que os investimentos efectuados em projectos anuais de sistemas de informação sejam os mais adequados e estejam de acordo com os objectivos a médio/longo prazo definidos para o SSSS. A linha geral destas estratégias não tem mudado significativamente desde 1998, mas as políticas para a sua execução têm sido ajustadas por cada Conselho Directivo do IIES. Constatou-se que o plano existente, datado de 1998, poderá requerer uma actualização para reflectir as novas decisões entretanto tomadas, considerando-se, por outro lado, fundamental a existência de uma clara definição dos prazos e das prioridades da estratégia de sistemas de informação e a sua actualização periódica, sem a qual é difícil avaliar, de modo independente, em que medida estas estão a ser alcançadas e se os recursos e os prazos necessários para atingir os objectivos estabelecidos são adequados.

Em sede de contraditório, o IIES informa que “...só após a constituição formal do Conselho Consultivo é possível clarificar e definir, com rigor, a estratégia dos sistema de informação a médio e curto prazo com a consequente apresentação de prazos e prioridades, de forma a poder-se assegurar um correcto plano de investimento nesta área, bem como uma monitorização do processo que permita avaliar o cumprimento dos prazos, objectivos e resultados.

Não obstante constrangimento resultante da não existência do órgão, o IIES tem vindo a efectuar os indispensáveis levantamentos que servirão de base a todo este processo”.

➤ **Horizonte Temporal da Estratégia de Sistemas de Informação**

A transformação e a informatização de qualquer sistema com a dimensão e complexidade do SSSS exigem um horizonte temporal alargado. Para assegurar a qualidade e integridade desta transição é necessário assegurar que:

- os requisitos dos processos existentes sejam adequadamente considerados no desenvolvimento dos novos sistemas; e
- a interpretação das especificidades dos dados históricos garanta uma transição correcta para os novos sistemas.

O SSSS enfrenta, neste momento, um desafio significativo relativamente à idade média dos seus quadros, começando a curto prazo, muitos deles, a entrar na idade de reforma. Esta situação é tanto mais relevante quanto a estratégia definida, e hoje existente, possa não ter ponderado a resolução atempada deste problema.



Tribunal de Contas

3.1.2.4 Avaliação Global – Repetitivo

- A necessidade de planeamento estratégico é reconhecida e compreendida pelo Conselho Directivo do IIES;
- As decisões estratégicas são definidas projecto a projecto mas, possivelmente, sem a consistência oferecida por uma estratégia global actualizada de SI/TI;
- Os riscos e os benefícios das decisões estratégicas importantes são reconhecidos mas a sua definição poderá ainda ser intuitiva.

3.1.3. DEFINIÇÃO DA ARQUITECTURA DE INFORMAÇÃO

3.1.3.1 Descrição da Actividade

A definição de uma arquitectura de informação consiste em aplicar a melhor forma de organização dos seus sistemas através da criação e manutenção de um modelo de informação, assegurando que as aplicações e o modelo de dados estão otimizados para a sua utilização eficiente. Esta actividade considera o desenvolvimento de uma arquitectura de informação que suporte as necessidades da Organização, bem como as normas a aplicar no seu desenvolvimento e manutenção.

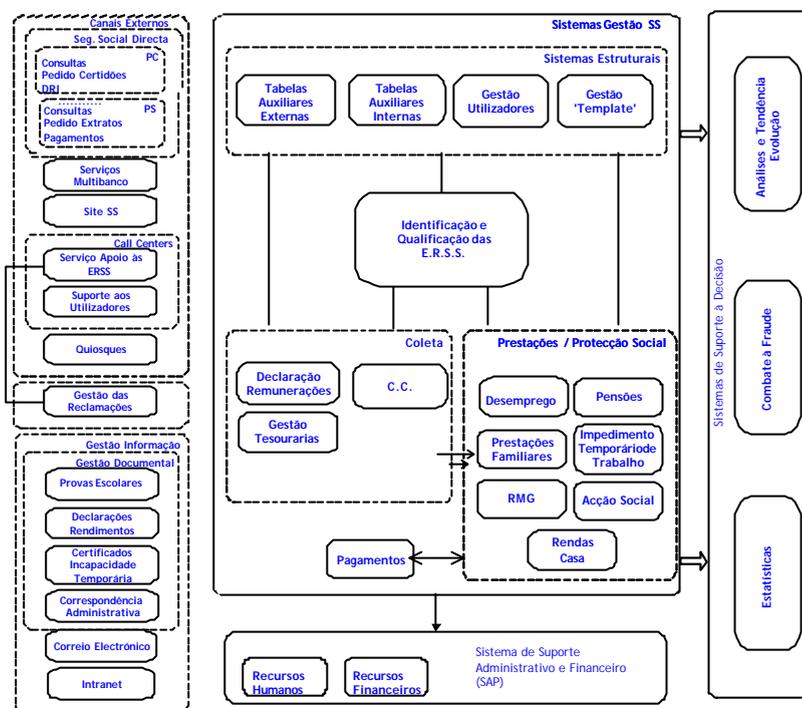
3.1.3.2 Situação Actual

Na avaliação desta actividade identificaram-se duas realidades, complementares mas distintas: por um lado, a realidade do IIES, que representará o futuro dos sistemas da SSSS; por outro, a existência, a nível nacional, de uma multiplicidade heterogénea de sistemas de informação.

A realidade existente abrange uma variedade de sistemas, com modelos de dados diferentes de acordo com a plataforma tecnológica implementada nos vários centros distritais e no CNP. Esta realidade é representativa de ilhas de informação com pouca ou nenhuma interligação entre os vários sistemas e com interpretações diferentes da informação gerida.



Arquitectura Global do Sistema Informação



Fonte: IIES

Afigura-se existir, por parte dos responsáveis do IIES, a consciência de que a arquitectura de informação do SSSS, actualmente existente, requer uma significativa reformulação no sentido de, no futuro, assegurar, designadamente:

- resposta às necessidades de informação cada vez mais exigentes;
- melhor qualidade dos serviços de sistemas prestados ao público português;
- melhor qualidade da informação sobre o SSSS; e
- disponibilização de sistemas de suporte à decisão transversal aos sistemas operacionais do SSSS.

Dado que muitas das aplicações inerentes a este modelo ainda não foram desenvolvidas ou estão, actualmente, em desenvolvimento, os modelos de dados subjacentes a esta arquitectura ainda não se encontram finalizados e a classificação de informação, em termos de categorias de segurança, ainda não foi totalmente definida.

A arquitectura de informação proposta pelo IIES pretende centralizar a informação do SSSS onde possível, alargando a sua disponibilização a todas entidades através de uma rede informática nacional. De sublinhar, relativamente a esta matéria, uma acrescida preocupação por parte dos responsáveis do IIES no sentido de se assegurar a integridade da informação a transitar para os novos sistemas.



Tribunal de Contas

3.1.3.3 Riscos Identificados e Seus Impactes

Os aspectos de classificação de informação são normalmente considerados durante o desenvolvimento do modelo de dados. Esta classificação é importante para relacionar as políticas e procedimentos de segurança ainda por desenvolver. Sem uma classificação adequada da informação do SSSS será difícil assegurar que a informação mais crítica/sensível esteja devidamente protegida ou que investimentos excessivos de segurança não sejam efectuados sobre informação não possuidora daquela qualificação para o SSSS.

3.1.3.4 Avaliação Global – Definido

- Existe um claro entendimento da importância de uma arquitectura de informação definida;
- A responsabilidade pela sua definição é conhecida e está atribuída;
- A definição do modelo de dados é pró activa e focada na resposta das futuras necessidades;
- O desenvolvimento e o cumprimento da arquitectura de informação estão adequadamente suportados por métodos e ferramentas informáticas;
- A arquitectura de informação começa a responder às necessidades, no entanto, são ainda necessários desenvolvimentos significativos para que o IIES consiga dar uma resposta efectiva às principais necessidades do SSSS.

3.1.4. DEFINIÇÃO DA DIRECÇÃO TECNOLÓGICA DE TI

3.1.4.1 Descrição da Actividade

A definição de uma direcção tecnológica de informação visa a obtenção de benefícios e vantagens competitivas das tecnologias de TI para cumprimento das estratégias definidas por uma Organização, contemplando, entre outras:

- a garantia de que a arquitectura tecnológica existente responde às necessidades actuais da Organização e que a estratégia de aquisição e migração de tecnologias de sistemas está de acordo com as necessidades definidas nas estratégias de sistemas de informação;
- a monitorização das tendências e evoluções nos mercados e produtos de TI, para que as mesmas sejam adequadamente consideradas na definição da arquitectura tecnológica de TI;
- a definição de normas tecnológicas que sejam implementadas através do plano de migração de tecnologias de sistemas de informação, assegurando o maior nível de padronização possível.



Tribunal de Contas

3.1.4.2 Situação Actual

Até recentemente, as entidades do SSSS tinham alguma liberdade para escolherem as plataformas que pretendiam implementar, implicando que a direcção tecnológica não fosse definida de forma consistente, o que resultou nas seguintes consequências:

- um investimento significativo em tecnologias e recursos humanos sem o benefício de economias de escala, dada a diversidade de plataformas;
- ineficiências na modificação e manutenção de sistemas, pelo mesmo motivo; e
- incompatibilidades entre plataformas, dificultando a integração da informação e criando um esforço administrativo adicional.

Entretanto, o IIES tem vindo a ganhar uma influência cada vez maior nesta actividade, começando a ter uma intervenção mais directa na negociação e compra de novos sistemas e soluções tecnológicas e na integração dos mesmos, sendo esta intervenção particularmente evidente na recente implementação das redes informáticas que visam a interligação dos vários sistemas do SSSS.

3.1.4.3 Riscos Significativos Identificados e Seus Impactes

O principal risco desta actividade está directamente associado à ineficiência resultante da falta de uma clara definição de uma direcção tecnológica, o que implica custos adicionais decorrentes da necessidade de investimentos em tecnologias, recursos humanos e manutenção de sistemas, inerentes a uma arquitectura tecnológica heterogénea.

3.1.4.4 Avaliação Global da Actividade – Repetitivo

- Existe um reconhecimento da necessidade de planeamento da infra-estrutura tecnológica do SSSS, mas o plano para a sua concretização está contemplado a alto nível;
- Não existe uma definição formal da arquitectura tecnológica a ser adoptada e seguida pelo SSSS, mas subsiste um esforço, por parte do IIES, para padronizar as suas plataformas tecnológicas;
- Historicamente, tem havido uma abordagem reactiva, mediante as necessidades de infra-estruturas informáticas, no entanto, parece haver, actualmente, um esforço para a inversão desta tendência, na medida em que se esboçou uma estratégia de sistemas de informação, aparentemente mais integrada.



Tribunal de Contas

3.1.5. DEFINIÇÃO DA ORGANIZAÇÃO DE TI E SUAS INTERDEPENDÊNCIAS

3.1.5.1 Descrição da Actividade

A definição da Organização de TI e suas interdependências visam a criação de um organismo adequadamente dimensionado em termos de número de efectivos e de competências, com funções e responsabilidades definidas e comunicadas, que facilite o alcance da estratégia informática e o controlo efectivo dos processos de gestão dos sistemas de informação.

3.1.5.2 Situação Actual

A organização dos serviços de TI está a ser realizada por cada uma das entidades do SSSS, existindo, em cada CDSSS e no CNP, um serviço ou unidade responsável pelos serviços de sistemas de informação que suportam as suas plataformas tecnológicas. O IIES, como entidade coordenadora, assume responsabilidade pelas infra-estruturas de redes e pelas infra-estruturas que suportam as novas plataformas.

O SSSS tem uma longa tradição na utilização de sistemas de informação e, em várias áreas, foi pioneiro na informatização dos serviços do Estado; no entanto, estes avanços tecnológicos não têm sido devidamente sustentados com o desenvolvimento contínuo dos recursos humanos afectos a esta área, criando uma situação de grande carência de conhecimentos em várias áreas relacionadas com as tecnologias de informação mais recentes.

O crescimento explosivo, nos anos 90, das tecnologias de sistemas de informação reduziu progressivamente a capacidade do SSSS para atrair e reter funcionários com um nível de conhecimentos informáticos adequados para sustentar a sua modernização. A constituição do IIES e a subcontratação de serviços de desenvolvimento e implementação de serviços têm colmatado alguns problemas nesta matéria, mas o problema continua a ser importante para as outras entidades que integram o SSSS. Dadas as especificidades dos sistemas desenvolvidos, o SSSS continua dependente de funcionários que detêm o conhecimento histórico dos sistemas e dos seus dados, sendo que o risco que advém desta dependência é substancialmente acrescido se tivermos em conta a idade média destes técnicos. Constatou-se, por outro lado, que não existe um plano de desenvolvimento de recursos humanos que prepare os recursos existentes para responder às necessidades dos futuros sistemas do SSSS.

Esta realidade tem criado situações em que não existem recursos humanos suficientes para dar resposta às necessidades de controlo de qualidade de sistemas e informação, bem como para providenciar uma adequada segregação de funções nos serviços de sistemas de informação das várias entidades, tendo-se verificado situações em que:



Tribunal de Contas

- os serviços de sistemas de informação são os “donos” efectivos dos sistemas, dado que nem sempre existe uma clara definição e separação de responsabilidades entre os utilizadores dos sistemas e os serviços informáticos;
- não existe uma segregação de funções entre a gestão de desenvolvimentos, a gestão de dados e a segurança dos sistemas;
- nas matérias de segurança de sistemas de informação nem sempre existe uma clara definição de políticas e responsabilidades.

Embora não haja uma definição única das políticas e procedimentos de sistemas de informação para o SSSS, existe alguma documentação dos procedimentos de gestão e segurança de sistemas de informação. Considera-se, por outro lado, que existe uma definição mínima de responsabilidades nos recursos humanos, nas várias entidades visitadas, mas, em certas áreas (como, por exemplo, a gestão de redes), persiste alguma incerteza das responsabilidades partilhadas entre o IIES, os vários CDSSS e o próprio CNP.

Há uma consciência da necessidade de reformular a estrutura organizacional de TI no ISSS, reconhecendo-se que a estrutura existente está demasiadamente fragmentada, adveniente de abordagens de gestão que variam de entidade para entidade.

Nas suas alegações, o IIES acrescenta: “O IIES é responsável pela totalidade da chamada “Rede Nacional de Dados da Segurança Social”, faz a sua monitorização de forma centralizada, detectando qualquer anomalia que se verifique na comunicação em qualquer ponto da rede, desde os “routers” locais até aos “nós” centrais. Actualmente, está a ser implementada uma ferramenta adicional que permitirá a monitorização das redes locais incluindo estações e impressoras padrão.

Quando considerada útil, a informação de monitorização pode e é disponibilizada ao ISSS e ao IGFSS”.

3.1.5.3 Riscos Significativos Identificados e Seus Impactes

O risco mais significativo nesta actividade está directamente relacionado com a necessidade de dimensionar e dotar o SSSS com o nível e quantidade de recursos humanos na área de sistemas de informação para dar resposta à informatização em curso. A renovação e a requalificação dos recursos humanos existentes representam um desafio significativo, que terá um impacte directo na estratégia de sistemas de informação prevista e nos benefícios que o SSSS obterá dos seus investimentos nesta área.

3.1.5.4 Avaliação Global da Actividade – Repetitivo

- Existe uma consciência da necessidade de reformular a estrutura organizacional dos Serviços/Unidades de Sistemas de Informação no SSSS;



Tribunal de Contas

- As funções e responsabilidades inerentes à estrutura existente estão definidas mas nem sempre formalizadas;
- A organização dos recursos humanos de TI poderá estar desajustada, face às competências necessárias para suportar efectivamente as infra-estruturas de sistemas de informação actuais e futuras do IIES;
- A estrutura actual e a sua dimensão têm uma capacidade limitada, mas tem conseguido responder e actuar efectivamente perante situações de crise.

3.1.6. GESTÃO DOS INVESTIMENTOS EM TI³

3.1.6.1 Descrição da Actividade

A actividade de gestão de investimentos em tecnologias de informação visa a identificação, controlo e monitorização da aplicação de verbas em orçamentos operacionais e em projectos periódicos aprovados pela Organização, considerando também a monitorização e justificação de custos e benefícios associados aos mesmos. Os factores que contribuem para o sucesso deste processo incluem:

- a identificação e correcta classificação de todos os custos com TI;
- um inventário efectivo de investimentos em TI que permita uma medição correcta dos seus custos e a salvaguarda de activos informáticos;
- a existência de um plano de investimentos definido que permita avaliar os projectos em curso e os ciclos de vida das tecnologias adquiridas;
- o processo de decisão de investimentos em TI definido e que considera:
 - impactes a curto e médio prazo;
 - a justificação de custos e benefícios para o SSSS;
 - a sua contribuição para a estratégia do SSSS;
 - o alinhamento com a direcção e arquitectura tecnológica; e
 - os impactes sobre as outras áreas do SSSS;
- o alinhamento dos Orçamentos de TI com a estratégia de TI e com os planos do SSSS;
- a aprovação de despesas devida e claramente delegada; e
- uma definição clara para a gestão e monitorização dos benefícios a serem realizados.

³ Esta vertente foi analisada, exclusivamente, na perspectiva e segundo os desígnios e necessidades do modelo CobIT, pelo que não foram adoptados procedimentos no sentido da verificação da legalidade, regularidade e correcção financeira dos contratos analisados para esse efeito.



Tribunal de Contas

3.1.6.2 Situação Actual

A maioria dos grandes investimentos recentemente efectuados em TI implicou a subcontratação de serviços externos, estruturados em projectos específicos. Existem procedimentos de controlo orçamental para controlar desvios entre as despesas reais e as orçamentadas nos projectos em curso. A definição de orçamentos para projectos é feita caso a caso, com fundamento em propostas e orçamentos de fornecedores e prestadores de serviços que servem de base para a justificação do custo dos projectos, sendo a justificação dos benefícios, na maioria dos casos, qualitativa, dado que a sua medição é difícil e complexa.

3.1.6.3 Riscos Significativos Identificados e Seus Impactes

Normalmente, a maioria dos riscos associados a esta área está relacionada com a falta de controlo orçamental das despesas operacionais e com a inexistência, para o sistema, de retorno do investimento efectuado em projectos de TI. No caso dos projectos analisados, todos eles relativos ao projecto EURO – plataformas *IBM S/390*, *IBM AS/400*, *ICL Series 39* e *UNISYS XR6* – considera-se que os riscos desta actividade estão devidamente controlados, parecendo que:

- existe um controlo orçamental adequado sobre as despesas relacionadas com os projectos; e
- os projectos de TI são aprovados e avaliados, de forma qualitativa, pelo Conselho Directivo do IIES.

3.1.6.4 Avaliação Global da Actividade – Definido

- O processo de selecção de investimentos e a definição dos seus orçamentos são razoavelmente sólidos;
- O processo de investimentos em TI está definido e adequadamente documentado;
- Os projectos em curso estão alinhados com a estratégia de TI e com os planos estratégicos do SSSS;
- A aprovação formal de investimentos seleccionados e dos seus orçamentos é efectuada;
- O equilíbrio entre investimentos em recursos humanos, sistemas e aplicações não é formalmente definido para otimizar os benefícios obtidos dos investimentos em tecnologias de informação.



Tribunal de Contas

3.1.7. COMUNICAÇÃO DAS ORIENTAÇÕES ESTRATÉGICAS

3.1.7.1 Descrição da Actividade

A comunicação das orientações dos órgãos directivos é fundamental para assegurar que a utilização das tecnologias de sistemas de informação está de acordo com os objectivos e intenções da Organização. Esta comunicação é efectuada através de políticas e normas estabelecidas para traduzir opções estratégicas em regras práticas de utilização, administração e segurança. Estas políticas e normas são comunicadas à comunidade de utilizadores e aos elementos responsáveis pela administração e segurança dos sistemas de informação, sendo os factores mais importantes que concorrem para o seu sucesso os seguintes:

- a existência de políticas bem definidas e articuladas para a Organização;
- a possibilidade e capacidade da Organização para assegurar o cumprimento das políticas consideradas durante o seu desenvolvimento;
- a existência de um processo que assegura e mede a conformidade com as políticas estabelecidas; e
- o apoio dos órgãos directivos da Organização às políticas de controlo estabelecidas é levado ao conhecimento do universo de utilizadores.

3.1.7.2 Situação Actual

A responsabilidade pela definição de políticas de segurança tem sido partilhada entre o IIES e os vários CDSSS, tendo-se constatado, ainda assim, a inexistência de políticas consistentes e homogéneas nas várias entidades que compõem o SSSS, o que resulta em planos de segurança que variam de local para local.

As políticas de administração de sistemas encontradas já contemplam alguns procedimentos de *backup* e protecção de dados, mas existem ainda várias áreas em que estas políticas necessitam de ser definidas e implementadas; por outro lado, existe pouca informação concreta sobre a implementação das políticas estabelecidas para as várias plataformas do SSSS e poucos mecanismos de monitorização para assegurar a conformidade com as políticas existentes.

Têm-se efectuado, no âmbito do SSSS, alguns esforços para formalizar as políticas de segurança de sistemas de informação, estando a reavaliar-se, face à sua realidade tecnológica, não só as políticas, como os próprios procedimentos actualmente existentes. Enquanto decorria este trabalho, o IIES tinha em curso um projecto de segurança visando suprimir as carências existentes nesta área, aguardando-se, a curto prazo, a sua aceitação formal por parte dos utilizadores.



Tribunal de Contas

3.1.7.3 Riscos Significativos Identificados e Seus Impactes

A definição de políticas e procedimentos para a utilização e administração dos sistemas de informação do SSSS é fundamental para assegurar que os objectivos, filosofia de segurança e controlo dos seus sistemas são comunicados a todos os funcionários que com ele operam. A inexistência de uma política de segurança formalmente definida aumenta o risco de os utilizadores do sistema e dos seus dados não estarem conscientes da sua importância para o bom funcionamento do sistema e das suas responsabilidades individuais quanto à confidencialidade, à integridade e à disponibilidade desta informação. Acresce, ainda, que, sem uma política de segurança formalmente definida e comunicada, existe o risco dos utilizadores não poderem ser responsabilizados por falhas na segurança da informação⁴.

3.1.7.4 Avaliação Global da Actividade – Repetitivo

- O ISSS reconhece a necessidade da existência de requisitos de segurança e de controlo interno efectivo na área de sistemas de informação;
- As práticas encontradas nas várias entidades do ISSS são informais ou não documentadas de uma forma consistente;
- O IIES tem comunicado a necessidade de serem definidas políticas, procedimentos e normas de controlo, associadas aos seus sistemas de informação;
- As políticas desenvolvidas têm respondido a necessidades pontuais, sendo premente a definição de uma estrutura completa de políticas para o ISSS;
- A formação dos utilizadores ainda não contempla o cumprimento das políticas e procedimentos de segurança do ISSS.

3.1.8. GESTÃO DOS RECURSOS HUMANOS

3.1.8.1 Descrição da Actividade

A gestão de recursos humanos através do recrutamento e retenção de funcionários capazes e motivados é fundamental para assegurar a boa prestação de serviços informáticos e a maximização dos benefícios obtidos dos sistemas e tecnologias de informação, concorrendo para o seu sucesso, designadamente, os seguintes factores:

- a definição de um Plano de Recursos Humanos para a retenção dos funcionários chave das áreas de sistemas de informação da Organização;

⁴ A Lei da Criminalidade Informática (Decreto Lei n.º 109/91, de 17 de Agosto) estabelece uma responsabilidade penal das pessoas colectivas ou equiparadas pelos crimes nela previstos, quando cometidos em seu nome e no interesse colectivo pelos seus órgãos ou representantes, extinguindo-se essa responsabilidade nos casos em que o agente tiver actuado contra as ordens ou instruções expressas por quem de direito.



Tribunal de Contas

- o alinhamento entre as estratégias de Sistemas de Informação e o Plano de Recursos Humanos da Organização;
- a existência de meios adequados atribuídos ao desenvolvimento e formação dos recursos humanos para dar resposta às necessidades da Organização;
- a existência de planos de defesa da continuidade de funções que se considerem pontos de dependência e que minimizem a falta de conhecimentos em áreas críticas para a Organização;
- um processo de rotação de tarefas entre os elementos da área de sistemas de informação que permita o desenvolvimento de carreiras e a redundância de conhecimentos;
- a definição de políticas específicas para a gestão de admissão e saída de funcionários para os Serviços e Unidades de Sistemas de Informação.

3.1.8.2 Situação Actual

A responsabilidade pela gestão dos recursos humanos necessários para suportar sistemas e tecnologias de informação está partilhada entre as várias entidades que integram o ISSS.

O recrutamento e promoção dos funcionários pertencentes aos vários serviços de sistemas de informação seguem os procedimentos adoptados pelo ISSS, com a excepção do IIES, que apresenta uma maior flexibilidade na contratação dos seus recursos humanos. Afigura-se não existir uma definição formal, pelo ISSS, das competências para suportar os sistemas de informação existentes e futuros, sendo, neste sentido, difícil de avaliar e identificar as necessidades de recrutamento ou de formação interna, o que resulta na necessidade de subcontratação de serviços e, assim, numa baixa utilização dos recursos existentes. Existem, pontualmente, necessidades específicas de formação, normalmente associadas à introdução de novos sistemas ou de alterações significativas aos existentes para as quais são disponibilizadas verbas. Por outro lado, consequência da introdução desses novos sistemas e tecnologias, tem surgido a necessidade de desenvolver competências nas áreas de gestão de redes e administração de sistemas e bases de dados, o que implica o aumento do nível de literacia informática necessária a um bom desempenho por parte dos utilizadores do ISSS.

A introdução dos novos sistemas previstos na estratégia de sistemas de informação avançada pelo IIES resultará numa situação em que as competências existentes nos serviços de sistemas de informação das várias entidades pertencentes ao SSSS estarão desajustadas face às necessidades das novas tecnologias introduzidas, implicando a necessidade de que a estratégia traçada seja complementada com um Plano de Recursos Humanos que actualize os conhecimentos e competências existentes para poderem ser enquadrados na futura organização de sistemas de informação. Neste momento, muitos destes detalhes ainda estão por definir. Constatou-se, também, que não existe uma política clara sobre a rotação de tarefas e funções para assegurar a polivalência dos informáticos do ISSS.



Tribunal de Contas

Existem alguns procedimentos que asseguram a disponibilidade de elementos críticos para o funcionamento dos sistemas mais importantes; ainda assim, o SSSS está vulnerável aos impactes provocados pela eventual saída de funcionários chave dos vários serviços informáticos.

Sobre este tema, veio o IIES informar que:

“Qualquer plano para desenvolvimento destes recursos humanos tem de ser visto de uma forma individualizada, atentas, principalmente, a continuidade de exploração dos actuais sistemas durante a fase de transição, a faixa etária, a motivação dos mesmos para as novas tecnologias e a apetência dos interessados para integrar as diversas áreas de actuação.

Perante esta constatação o IIES tomou a iniciativa reunir com os interessados, de forma a que os mesmos sejam ouvidos e apresentem sugestões com vista à elaboração dum plano estratégico de recursos humanos da área informática. Em termos de preparação básica destes recursos, o IIES tem mesmo previsto, no seu plano de actividades para 2002, acções de formação vocacionadas para sistemas abertos”.

Por último, o ISSS carece de políticas específicas relacionadas com os procedimentos de segurança relativos à admissão de novos funcionários ou à rescisão de contratos, nomeadamente no que diz respeito às exigências da Lei da Privacidade de Dados, que impõem uma responsabilidade de sigilo profissional sobre o tratamento de dados por parte dos informáticos.

3.1.8.3 Riscos Significativos Identificados e Seus Impactes

Os benefícios a obter da informatização do SSSS estão directamente relacionados com as eficiências inerentes aos processos informatizados, designadamente os benefícios financeiros que resultam, muitas vezes, directamente da redução efectiva dos recursos humanos envolvidos num processo. No entanto, a inflexibilidade dos acordos laborais da administração pública para reduzir os seus efectivos é um factor importante a considerar na avaliação das eficiências e benefícios a obter dos investimentos efectuados. Assim, esta mudança implica que os recursos humanos eventualmente “libertados” tenham que ser requalificados e alocados a outras actividades de maior valor e importância para o ISSS. Depreende-se, então, que, neste contexto, o eventual retorno dos investimentos em tecnologias de informação está directamente relacionado com a capacidade do SSSS em:

- efectuar e gerir as mudanças necessárias para reduzir os custos com recursos humanos;
- efectuar uma requalificação e obter um melhor aproveitamento dos recursos humanos existentes;
- desenvolver os recursos humanos disponíveis para efectuar um melhor aproveitamento das tecnologias de informação.



Tribunal de Contas

Por tudo o que atrás ficou dito, considera-se que a gestão das mudanças inerentes aos recursos humanos é um factor decisivo para obter um retorno adequado sobre os investimentos de TI efectuados.

3.1.8.4 Avaliação Global da Actividade – Inicial

- É reconhecida a necessidade de gerir os recursos humanos na área de sistemas de informação, mas ainda não se formalizou um plano para esse efeito;
- Existe uma abordagem de aquisição de competências necessárias para dar resposta às necessidades específicas dos projectos em curso;
- Existe uma consciência, cada vez maior, de que a complexidade e a rapidez das alterações tecnológicas criam a necessidade da formação de novas competências que respondam adequadamente às futuras realidades.

3.1.9. CUMPRIMENTO DE REQUISITOS EXTERNOS

3.1.9.1 Descrição da Actividade

A actividade de Cumprimento de Requisitos Externos assegura o cumprimento de responsabilidades legais e contratuais relacionados com a gestão dos processos de tecnologias de informação. Existem, em Portugal, várias leis, algumas transpostas de normas comunitárias, que têm um impacte directo sobre a área de sistemas de informação, nomeadamente:

- Lei das Facturas Electrónicas – Decreto-Lei n.º 375/99, de 18 de Setembro;
- Lei dos Certificados Digitais – Decreto-Lei n.º 290-D/99, de 2 de Agosto;
- Lei da Privacidade de Dados – Decreto-Lei n.º 67/98, de 26 de Outubro;
- Regras Fundamentais no processo de Transição para o Euro – Decreto-Lei n.º 138/98, de 16 de Maio;
- Lei da Protecção de *Software* – Decreto-Lei n.º 252/94, de 20 de Outubro;
- Lei da Criminalidade Informática – Decreto-Lei n.º 109/91, de 17 de Agosto.

Para o bom desempenho desta actividade contribuem, designadamente, os seguintes factores:

- a definição das medidas necessárias para assegurar o cumprimento de requisitos externos;
- o estabelecimento dos custos de cumprimento;
- a garantia de que as políticas e os procedimentos necessários para assegurar o cumprimento de requisitos externos estão documentados e comunicados;
- a existência de uma função que monitoriza o cumprimento dos requisitos externos estabelecidos; e



Tribunal de Contas

- a existência de auditorias internas que validem o seu necessário cumprimento.

Observa-se, no SSSS, um fenómeno que tem impactes directos sobre esta actividade: as alterações legislativas e o surgimento de novas leis relativas ao mesmo. Esta situação afecta directamente a concepção, implementação e manutenção dos sistemas enquadrados no âmbito desta auditoria, nomeadamente os respeitantes à Identificação e Qualificação geridos, actualmente, pelo CNP (futuramente pelo IIES), bem como os sistemas de Cálculo das Prestações de Pensões.

3.1.9.2 Situação Actual

Acrescendo à, já de si, complexa teia legal que envolve o universo em causa, as alterações legislativas ou o surgimento de nova legislação subjacente ao SSSS podem ter impactes profundos nos sistemas informáticos existentes, implicando a necessidade de efectuar desenvolvimentos aos seus programas para dar resposta às modificações ou novidades introduzidas. O CNP dispõe de uma Unidade Jurídica que interpreta os requisitos estabelecidos pela legislação de modo a que se efectuem, correctamente, os desenvolvimentos ou alterações aos programas que forem afectados; no entanto, essas alterações legislativas exigem, por vezes, o registo ou processamento de elementos de informação que podem, ou não, existir nos actuais modelos de dados. Reconhece-se, assim, que o sucesso desta actividade é fundamental, não só para a atribuição e controlo de pensões, mas para todo o SSSS.

Neste momento, o cumprimento funcional das aplicações com as Leis da Segurança Social constitui a preocupação principal dos serviços de sistemas de informação, considerando-se, assim, importante alertar para a existência de outra legislação relacionada com sistemas de informação que também terá relevância para o SSSS: as Leis de Protecção de Dados, Protecção de *Software* e Criminalidade Informática. No caso da Lei de Protecção de Dados, o n.º 1 do art.º 14.º indica que o responsável pelo tratamento deve pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito. Estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger. Como o ISSS, através do CNP, processa dados pessoais referentes aos pensionistas do país, as bases de dados do CNP requerem o seu registo perante a Comissão Nacional para a Protecção de Dados. O registo das bases de dados do CNP foi já efectuado junto daquela Comissão.

As medidas especiais de segurança estabelecidas no art.º 15.º da mesma lei são aplicáveis se uma entidade processa dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo dados genéticos. Com base nos dados existentes nos sistemas do CNP, considera-se que esta entidade tem responsabilidades acrescidas nos termos



Tribunal de Contas

desta lei, dado que os seus sistemas de informação guardam e processam informação relacionada com o estado de saúde dos beneficiários.

A **Lei da Protecção de Dados** – Decreto-Lei n.º 67/98, de 26 de Outubro – estabelece que os responsáveis pelo tratamento de dados pessoais devem tomar as medidas adequadas para:

- impedir o acesso de pessoas não autorizadas às instalações utilizadas para o tratamento desses dados (controlo da entrada nas instalações);
- impedir que suportes de dados possam ser lidos, copiados, alterados ou retirados por pessoa não autorizada (controlo dos suportes de dados);
- impedir a introdução não autorizada, bem como a tomada de conhecimento, a alteração ou a eliminação não autorizadas de dados pessoais inseridos (controlo da inserção);
- impedir que sistemas de tratamento automatizado de dados possam ser utilizados por pessoas não autorizadas através de instalações de transmissão de dados (controlo da utilização);
- garantir que as pessoas autorizadas só possam ter acesso aos dados abrangidos pela autorização (controlo de acesso);
- garantir a verificação das entidades a quem possam ser transmitidos os dados pessoais através das instalações de transmissão de dados (controlo da transmissão);
- garantir que possa verificar-se *a posteriori*, em prazo adequado à natureza do tratamento, a fixar na regulamentação aplicável a cada sector, quais os dados pessoais introduzidos, quando e por quem (controlo da introdução);
- impedir que, na transmissão de dados pessoais, bem como no transporte do seu suporte, os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada (controlo do transporte).

Face a estas exigências, considera-se que existem alguns aspectos dos sistemas informáticos de controlo e pagamento de pensões que podem pôr em risco o cumprimento destes requisitos, nomeadamente:

- o sistema de autenticação do CNP efectua a validação do acesso aos dados de um requerimento com base na transacção executada. Verificou-se que muitas das transacções de consulta aos dados não requerem uma autenticação do utilizador, podendo pôr em causa a confidencialidade da informação de um beneficiário. Reconhece-se, ainda assim, que o acesso a esta informação requer a entrada num terminal com o devido emulador instalado.
- A transmissão de dados não é *encriptada* entre o sistema do CNP e os clientes de rede nem no seu transporte em bandas. Existem, também, troços da rede do ISSS que utilizam ligações via satélite. Dada a dimensão da rede, há sempre o risco de que o tráfego nas redes do ISSS possa ser escutado a partir de qualquer ponto de acesso à rede nas varias instalações do ISSS, comprometendo, assim, a confidencialidade dos dados por si geridos.



Tribunal de Contas

A **Lei de Protecção de Software** impõe obrigações, como o cumprimento de direitos de autor e licenças de utilização associada com *software* adquirido no âmbito do SSSS, estando, assim, todo o *software* instalado sujeito a esta lei. Foram adoptados alguns procedimentos quanto à obrigatoriedade de se utilizar apenas *software* licenciado, no entanto, a instalação, por utilizadores individuais, de *software* obtido através da Internet poderá não ser sujeito ao mesmo controlo e não existem, neste momento, políticas de utilização de sistemas de informação que considerem estas situações.

A **Lei da Criminalidade Informática** poderá afectar o SSSS, dado que, no seu art.º 3.º, se atribui uma responsabilidade penal às pessoas colectivas que integram o SSSS se um crime informático for cometido em seu nome e no interesse colectivo pelos seus órgãos ou representantes. Esta responsabilidade é excluída quando o agente tiver actuado contra ordens ou instruções expressas de quem de direito. A divulgação e emissão de políticas e procedimentos de segurança formalizadas e reconhecidas pelos funcionários do SSSS permitiriam a exclusão desta responsabilidade.

As **Leis de Certificados e Assinaturas Digitais**, embora não directamente aplicáveis à realidade actual do SSSS, poderão afectar, num futuro próximo, as suas actividades, designadamente os pagamentos electrónicos efectuados pelos contribuintes, bem como as suas transacções diárias.

Nas alegações produzidas, o IIES informa, quanto à protecção dos dados detidos pelo SSSS, que *“...encetou diligências no sentido de providenciar a legalização dos mesmos, a nível da segurança social, em detrimento da abordagem por instituição”*.

Em relação à segurança na transmissão dos dados, informa que *“...os acessos de serviços do ISSS aos sistemas do CNP processam-se exclusivamente através da Rede Nacional da Segurança Social (RNSS), a qual é uma rede privativa utilizando circuitos alugados a Operadores Públicos de Comunicações. Nesta medida, existe de facto o risco potencial de o tráfego na RNSS poder ser escutado, tal como existe em todas as redes sobre infra-estruturas de operadores públicos, pelo que estão a ser desenvolvidos projectos que visam melhorar a segurança da Rede, nomeadamente através da inclusão de mecanismos de encriptação e outros. No entanto, os acessos à RNSS encontram-se já protegidos por vários sistemas de segurança e validação de acessos que são auditáveis e auditados. Tanto quanto é do nosso conhecimento, não existe utilização de ligações por satélite na RNSS.”*



Tribunal de Contas

3.1.9.3 Riscos Significativos Identificados e Seus Impactes

Os riscos nesta área partem da falta de conhecimento ou aviso em relação às leis aplicáveis à área de sistemas de informação.

No caso da Lei da Protecção de Dados Pessoais, existem outros controlos ou outros processos que seguem e que reduzem os riscos associados à confidencialidade de dados pessoais. No caso da Lei da Criminalidade Informática e da Lei de Protecção de *Software*, não existem políticas de segurança específicas que minimizem os riscos associados ao não cumprimento destas leis. Na maioria dos casos, as penalidades não são significativas, mas a imagem pública do SSSS pode ser negativamente afectada.

3.1.9.4 Avaliação Global da Actividade – Definido

- Os vários serviços de sistemas de informação do SSSS estão conscientes dos impactes que a legislação tem sobre os sistemas de informação existentes;
- O processo de avaliação desses impactes e o cumprimento das obrigações e responsabilidades no CNP estão adequadamente suportados por procedimentos que asseguram o seu cumprimento;
- Existe alguma monitorização desta actividade e, em certas situações, o cumprimento dos requisitos legais inerentes continua a depender de uma significativa intervenção humana.

3.1.10. AVALIAÇÃO DE RISCOS DE TI

3.1.10.1 Descrição da Actividade

A actividade de avaliação de riscos de TI actua como suporte às decisões do ISSS, sendo um importante instrumento para o alcance dos objectivos delineados na área de sistemas de informação. Este apoio visa, assim, dar resposta à complexidade crescente das decisões relacionadas com tecnologias de informação bem como a identificação e análise de riscos e factores críticos que poderão afectar as decisões tomadas, contemplando, ainda, a identificação de medidas efectivas, dentro de um rácio razoável de custo/benefício, que minimizem os riscos identificados. Os factores determinantes para o sucesso desta actividade incluem:

- a existência de uma política que defina a tolerância ou limites de risco aceites pela Organização;
- a avaliação de riscos, efectuada considerando as ameaças, riscos e valor dos bens informáticos afectados;



Tribunal de Contas

- as responsabilidades relacionadas com a avaliação e gestão de riscos formalmente definidas e atribuídas; e
- a validação por entidades terceiras, aumentando o nível de objectividade associada à gestão e avaliação de riscos.

3.1.10.2 Situação Actual

Esta actividade existe no ISSS mas de forma limitada, não fazendo parte da metodologia de gestão global de sistemas de informação adoptada pelos serviços de sistemas de informação que integram o SSSS. Ainda assim, verificou-se que a análise de risco é efectuada formalmente, pelo IIES, ao nível de projectos de grande envergadura. Por outro lado, constatou-se que, relativamente aos projectos de preparação dos sistemas para o EURO, houve uma preocupação de incluir uma componente formal de avaliação de riscos, tendo esta sido discutida com os vários intervenientes no projecto e os riscos, identificados pró activamente, monitorizados para assegurar o sucesso.

Como referido, a avaliação de risco como uma prática global que abrange todos os sistemas e tecnologias do ISSS ainda não é comum. A falta de políticas e procedimentos de segurança baseada numa avaliação de riscos de sistemas de informação não foi, ainda, definida. Considera-se, assim, que uma avaliação de riscos dos sistemas do ISSS, complementada por políticas e procedimentos de segurança, é importante no sentido da optimização dos investimentos realizados em mecanismos de controlo e segurança nas áreas de maior risco para o ISSS. A conformidade com as políticas e procedimentos ainda por estabelecer deve ser suportada com auditorias realizadas para este efeito.

3.1.10.3 Riscos Significativos Identificados e Seus Impactes

Os responsáveis pelo IIES estão conscientes da necessidade de gerir e minimizar os riscos na área de sistemas de informação. Uma avaliação global dos riscos é fundamental para que os mais significativos sejam devidamente identificados e geridos por parte do SSSS. Sem uma avaliação de risco global, o SSSS poderá não estar a proteger devidamente os seus “activos” de informação, devendo estas avaliações ser suportadas por auditorias informáticas para assegurar que os controlos necessários estão implementados e continuam efectivos.

3.1.10.4 Avaliação Global da Actividade – Repetitivo

- Os responsáveis do ISSS estão conscientes da necessidade de avaliação de riscos de sistemas de informação;
- Existe uma abordagem de alto nível na avaliação de riscos para projectos em curso, mas a prática não é consistente em todo o ISSS;



Tribunal de Contas

- Não existe uma metodologia estruturada e formalizada para a avaliação global de riscos de sistemas de informação;
- Os riscos específicos de TI, nomeadamente de segurança, disponibilidade e integridade de sistemas são considerados pontualmente em termos de cada projecto e em função dos conhecimentos sobre a tecnologia envolvida;
- As avaliações de risco são realizadas no decorrer de projectos sem que, contudo, sejam identificadas como uma componente individual e específica do projecto.

3.1.11. GESTÃO DOS PROJECTOS EM CURSO

3.1.11.1 Descrição da Actividade

Esta actividade visa a gestão de projectos, de acordo com a sua prioridade em termos da estratégia de sistemas de informação e dos planos operacionais estabelecidos, contemplando a aplicação de conceitos importantes de gestão de projectos para assegurar o seu cumprimento dentro dos prazos e orçamentos estabelecidos. Os factores que contribuem para o sucesso desta actividade incluem:

- a existência de gestores de projectos com experiência;
- o apoio e importância dada pela Organização para a execução efectiva dos projectos em curso;
- o envolvimento dos elementos da área de sistemas de informação na definição, implementação e gestão dos projectos em curso;
- a existência de uma metodologia de avaliação de riscos que é aplicada a cada projecto;
- a garantia de que todos os projectos têm um plano que discrimina, de forma clara, as suas fases, actividades e tarefas e incluem estimativas razoáveis dos tempos de execução e as competências necessárias para a sua concretização;
- a existência de uma transferência efectiva de conhecimentos da equipa de implementação para os elementos dos Serviços/Unidades de Sistemas de Informação em termos de um processo estruturado; e
- a existência de uma metodologia de desenvolvimento de sistemas definida e implementada pela organização.

3.1.11.2 Situação Actual

Constatou-se, aquando da avaliação desta actividade, que existem duas realidades distintas: a do CNP e a do IIES. O CNP gere e executa todos os seus projectos de sistemas de informação, internamente definidos, e as suas prioridades e calendário. Por seu lado, a maioria dos projectos de grande envergadura (como foi o caso da transição para o EURO), geridos pelo IIES no último ano, foram objecto de subcontratação a entidades externas, dada a dimensão e complexidade dos trabalhos a efectuar, tendo a sua priorização sido estabelecida pelo seu Conselho Directivo e,



Tribunal de Contas

com excepção do CNP, o acompanhamento partilhado entre esta entidade, os CDSSS que representavam cada plataforma e a entidade subcontratada.

A subcontratação destes projectos foi sujeita à definição de um plano de implementação pelas entidades subcontratadas, com prazos adequadamente definidos, tendo a metodologia de gestão dos projectos variado conforme a entidade externa envolvida. Considera-se que, nos projectos analisados, houve uma metodologia de gestão razoavelmente definida, sendo, na maioria dos casos, os riscos financeiros inerentes, em parte, transferidos para os prestadores de serviços e, por outro lado, contemplada a gestão de riscos associados aos atrasos dos projectos ou incumprimento de expectativas. Neste sentido, o ISSS demonstrou uma grande preocupação com a gestão dos projectos em curso na área de sistemas de informação, implementando as medidas necessárias para assegurar o cumprimento dos prazos estabelecidos. A conformidade atempada dos sistemas do SSSS com o EURO demonstrou o esforço investido nesta actividade.

3.1.11.3 Riscos Significativos Identificados e Seus Impactes

As transferências de conhecimentos dos sistemas implementados e alterações podem apresentar um risco significativo para o SSSS, dado que, em várias situações, o ISSS poderá não ter a capacidade interna necessária para acompanhar os projectos de implementação em curso, de modo a conseguir assegurar a transferência efectiva dos conhecimentos necessários sobre os sistemas implementados.

3.1.11.4 Avaliação Global da Actividade – Repetitivo

- Os responsáveis pelo CNP e pelo IIES estão conscientes e têm comunicado a sua preocupação relativamente à necessidade de gestão dos projectos em curso;
- O ISSS está continuamente a desenvolver a sua capacidade de gestão de projectos, embora muita desta capacidade esteja, também, a ser desenvolvida no IIES;
- A organização dos projectos, bem como as responsabilidades de cada elemento no projecto, está formalizada;
- Os projectos formalizados têm orçamentos, calendários e metas de desempenho definidos;
- Os procedimentos de gestão da qualidade do projecto variam de projecto para projecto, mas, em certos casos, continuam a ser informais;
- A aplicação destas orientações está dependente de um gestor de projectos.

3.1.12. GESTÃO DA QUALIDADE

3.1.12.1 Descrição da Actividade



Tribunal de Contas

A gestão da qualidade contempla o planeamento, implementação e manutenção de normas de qualidade para cada fase de desenvolvimento, através do estabelecimento de responsabilidades explícitas e entregas definidas, que assegurem a qualidade de sistemas desenvolvidos ou implementados e satisfaçam os requisitos previamente estabelecidos. Para o sucesso desta actividade contribuem os seguintes factores:

- um processo de desenvolvimento ou implementação adequadamente definido que permita efectuar avaliações da qualidade do processo seguido;
- a existência de procedimentos de qualidade com responsabilidades claramente definidas e atribuídas para o seu cumprimento;
- a existência de um processo de aprendizagem e melhoria contínua com base em métricas estabelecidas;
- a existência de uma cultura de qualidade promovida pelos órgãos directivos da organização;
- a existência de critérios de qualidade, para cada projecto, previamente estabelecidos; e
- a existência de formação para os elementos da área de sistemas de informação ou para os utilizadores responsáveis pelos testes de novos sistemas ou funcionalidades.

3.1.12.2 Situação Actual

Não está formalmente estabelecido um processo de qualidade para os serviços de sistemas de informação prestados mas, dada a dimensão dos serviços/unidades de sistemas de informação nos vários CDSSS, não seria viável ter esta função operacional. A gestão da qualidade de projectos varia de projecto para projecto, embora se tenha constatado, nos projectos analisados, a existência de procedimentos mínimos de teste com o objectivo de assegurar a qualidade das funcionalidades implementadas. Constatou-se, na avaliação dos projectos, que a sua gestão não tinha como objectivo a retenção de evidências que demonstrassem a execução dos procedimentos de testes efectuados ou dos procedimentos de controlo de qualidade executados.

Na avaliação desta actividade não foi possível identificar a definição formal dos requisitos mínimos de qualidade nem as métricas consistentes para demonstrar o seu funcionamento, tendo-se, no entanto, encontrado evidência de que estes foram efectuados. Constatou-se que existem abordagens distintas relativamente ao envolvimento de utilizadores no processo de gestão da qualidade dos projectos implementados. No caso do CNP, as responsabilidades de gestão de qualidade estão concentradas na Unidade Informática, enquanto que em outros projectos analisados existe alguma intervenção de utilizadores chave nos processos de gestão de qualidade dos sistemas desenvolvidos ou alterados. Em certos casos, a falta do envolvimento dos utilizadores finais não permite a segregação efectiva de funções para garantir que as alterações efectuadas respeitam os mínimos de qualidade estabelecidos.



Tribunal de Contas

3.1.12.3 Riscos Significativos Identificados e Seus Impactes

A introdução de sistemas e aplicações cuja qualidade de desenvolvimento ou implementação não esteja adequadamente validada, acarreta vários riscos em termos da estabilidade dos sistemas e da integridade da informação por eles processada. Considera-se que o ISSS não tem recursos adequados para assegurar a qualidade dos seus sistemas de uma forma sistemática ou para assegurar uma correcta segregação de funções na gestão de desenvolvimentos.

3.1.12.4 Avaliação Global da Actividade – Repetitivo

- É reconhecida a necessidade de definir os requisitos de qualidade associados a qualquer desenvolvimento ou alteração de sistemas, embora não se siga uma metodologia específica e consistente na aquisição e implementação de soluções;
- Os requisitos de qualidade associados às soluções seleccionadas são identificados de forma informal;
- A qualidade de cada projecto depende da experiência do seu gestor e da natureza e extensão dos procedimentos de teste adoptados para o projecto.

3.2. DESENVOLVIMENTO E IMPLEMENTAÇÃO DE SOLUÇÕES

3.2.1. DESCRIÇÃO DO PROCESSO

Para realizar e alcançar os objectivos da estratégia informática de qualquer Organização é necessário identificar, desenvolver ou adquirir, e implementar ou integrar soluções informáticas nos processos das mesmas entidades. Este processo considera, para além do desenvolvimento de novos sistemas, a manutenção dos existentes no sentido de assegurar a sua continuidade e relevância.

Este processo está subdividido, segundo o modelo CobIT, nas seguintes actividades:

1. Identificação de Soluções;
2. Aquisição e Manutenção de Aplicações;
3. Aquisição e Manutenção da Arquitectura Tecnológica;
4. Desenvolvimento e Manutenção de Procedimentos de TI;
5. Instalação e Certificação de Sistemas; e
6. Gestão da Mudança.



Tribunal de Contas

3.2.2. IDENTIFICAÇÃO DE SOLUÇÕES

3.2.2.1 Descrição da Actividade

Esta actividade pretende identificar, através de uma metodologia ou análise objectiva, a solução ou soluções mais adequadas para dar resposta aos requisitos e necessidades de informação e funcionalidades estabelecidas pela Organização. Os factores que contribuem para o seu sucesso incluem:

- um bom conhecimento das soluções disponíveis no mercado local ou internacional;
- critérios estabelecidos para a identificação de projectos que devem ser desenvolvidos internamente, subcontratados ou adquiridos;
- existência de uma metodologia estabelecida, conhecida e implementada para a aquisição ou implementação de sistemas;
- existência de um processo transparente e eficiente para o planeamento e aprovação de soluções;
- a identificação dos utilizadores chave do sistema pretendido para suportar o processo de selecção, análise e recomendação de novas soluções;
- a existência de uma clara definição das responsabilidades do fornecedor;
- a utilização, por regra, de tecnologias comprovadas, sendo consideradas novas tecnologias somente quando necessárias e justificadas por uma necessidade específica da Organização;
- existência de um entendimento do custo total de aquisição de uma solução; e
- consideração atempada das questões de segurança e controlo neste processo.

3.2.2.2 Situação Actual

Esta actividade cabe dentro das responsabilidades do IIES, dado que esta entidade é responsável pela implementação da nova arquitectura de sistemas prevista para o SSSS. Dadas as necessidades especiais do ISSS em termos das funcionalidades inerentes às novas aplicações, o IIES tem apostado no desenvolvimento de soluções “personalizadas” para dar resposta às necessidades do SSSS para os sistemas de identificação e qualificação de beneficiários e contribuintes. No caso dos sistemas administrativos e financeiros, o IGFSS teve um papel importante na identificação e selecção de uma nova aplicação que teria de dar resposta às necessidades do novo POCISSSS e ser compatível com o EURO.

Nestes casos, quando é necessário recorrer à contratação externa de serviços para o desenvolvimento de sistemas, o IIES inicia um processo de consulta aos fornecedores identificados, de acordo com os critérios de avaliação de requisitos estabelecidos pela Administração Publica para a contratação de serviços. Os contratos de prestação de serviços ou aquisição de soluções são a base para o controlo dos custos inerentes a cada projecto.

Existe um processo de acompanhamento do fornecimento do serviço pelo IIES ou, no caso de uma aplicação dos CDSSS, pelos utilizadores chave, no momento em que este vai sendo prestado.



Tribunal de Contas

Na maioria de casos, a definição formal dos requisitos de controlo de qualidade é da responsabilidade do prestador de serviços. Devido à plataforma tecnológica existente, no caso do CNP, esta actividade está direccionada para o desenvolvimento de programas para dar resposta às novas funcionalidades pretendidas, sendo a definição das necessidades estabelecida com os responsáveis das várias unidades.

3.2.2.3 Riscos Significativos Identificados e Seus Impactes

No contexto do ISSS, esta actividade está sujeita aos seguintes riscos:

- as necessidades dos utilizadores podem não ser adequadamente definidas, documentadas, ou compreendidas pela equipa responsável pelo desenvolvimento de novas soluções informáticas para o SSSS;
- durante as etapas iniciais do processo de desenvolvimento de novas soluções para os sistemas de informação podem não ser estabelecidos os requisitos de controlo e segurança que deverão ser incorporados na solução pretendida, o que pode dar origem à entrega de um produto final que não corresponde às expectativas ou necessidades estabelecidas;
- caso o ISSS pretenda que se implemente ou desenvolva uma nova solução de sistemas de informação, poderão não ser suficientemente investigadas as soluções alternativas disponíveis no mercado, podendo traduzir-se esta situação na escolha de um serviço ou solução que não corresponda exactamente ao pretendido;
- a viabilidade do projecto e os recursos exigidos podem ser inadequadamente analisados no início do projecto de desenvolvimento; e
- durante o projecto de desenvolvimento podem não ser adequadamente definidos os critérios de aceitação/rejeição por parte dos utilizadores. Esta definição é imprescindível para definir a métrica sob a qual a qualidade dos desenvolvimentos é avaliada.

3.2.2.4 Avaliação Global da Actividade – Repetitivo

- Não existe uma metodologia formal de aquisição e implementação de soluções, mas os requisitos tendem a ser definidos de forma semelhante por todo o SSSS;
- As soluções são identificadas seguindo um processo informal baseado na experiência e conhecimentos adquiridos pelo Núcleo de Sistemas de Informação;
- O sucesso de cada projecto depende da experiência adquirida individualmente por cada gestor de projecto e a qualidade da documentação de suporte da decisão varia.



Tribunal de Contas

3.2.3. AQUISIÇÃO E IMPLEMENTAÇÃO DE APLICAÇÕES

3.2.3.1 Descrição da Actividade

Esta actividade pretende disponibilizar soluções aplicacionais para suportar os processos de “negócio”, através da definição e implementação faseada de aplicações que respondem às necessidades funcionais e operacionais da cada entidade. Os factores que contribuem para o sucesso desta actividade são, designadamente:

- as melhores práticas de aquisição e desenvolvimento serem adequadamente definidas, conhecidas e aceites;
- a existência de uma separação efectiva entre as actividades de desenvolvimento e de teste;
- a existência de um número adequado de ferramentas de suporte ao processo de desenvolvimento que contribuam para a eficiência da selecção de soluções;
- os requisitos chave de qualquer projecto serem priorizados em função do tempo e custo disponível para o projecto, sem prejuízo da sua qualidade;
- o grau e forma de documentação do projecto serem previamente acordados para o projecto e devidamente respeitados durante o mesmo; e
- a conformidade do projecto com a arquitectura de informação estabelecida para a entidade ser validada.

3.2.3.2 Situação Actual

Nenhuma das entidades auditadas utiliza uma metodologia formal e *standard* adoptada pelo ISSS na execução do trabalho de desenvolvimento de sistemas através das várias fases que perfazem o ciclo de vida de desenvolvimento de sistemas⁵. Verificou-se, ainda assim, que a metodologia do prestador de serviços de desenvolvimento foi, na maioria dos casos, adoptada, considerando-se aceitável esta abordagem, desde que o ISSS assegure que a metodologia apresentada respeita os requisitos mínimos de controlo e qualidade para um projecto de desenvolvimento; neste momento, a avaliação desses requisitos para o processo de desenvolvimento de sistemas é ainda intuitivo, dado que a definição destes mínimos requer uma adequada formalização.

Durante o processo de conversão dos sistemas e dados para o Euro foram adoptados alguns dos pressupostos desta metodologia; contudo, uma vez terminado, a sua aplicação continua a não ser sistemática.

⁵ *System Development Life Cycle – SDLC.*



3.2.3.3 Riscos Significativos Identificados e Seus Impactes

Os riscos associados a esta actividade poder-se-ão resumir como segue:

- a falta de uma metodologia formal de desenvolvimento de sistemas pode resultar na possibilidade dos programas não estarem devidamente autorizados, testados e aprovados antes de serem implementados no ambiente de produção;
- a inexistência de procedimentos formais dificulta a centralização de solicitações, a definição de prioridades, o acompanhamento do ponto de situação, a aprovação formal por parte do utilizador após a realização de testes adequados e a autorização para implementação em produção;
- o facto de se documentar os desenvolvimentos efectuados no próprio código fonte das aplicações, torna difícil, do ponto de vista da gestão, assegurar a fácil e rápida compreensão do trabalho efectuado. Além disso, torna estas entidades altamente dependentes dos funcionários das Unidades de Sistemas de Informação.

3.2.3.4 Avaliação Global da actividade – Repetitivo

- Existem processos para gerir a aquisição e a implementação de aplicações, mas estes dependem da experiência dentro de cada Serviço/Unidade de Sistemas de Informação, sem haver lugar à formalização da metodologia seguida;
- A taxa de sucesso das aplicações implementadas depende, em grande parte, das valências individuais dos gestores de projectos e da experiência dos colaboradores.

3.2.4. IMPLEMENTAÇÃO DA INFRA-ESTRUTURA TECNOLÓGICA

3.2.4.1 Descrição da Actividade

Esta actividade visa a implementação, teste e aceitação de *hardware*, redes, sistemas operativos e outros requisitos de infra-estrutura tecnológica necessários para um ambiente de sistemas de TI. Esta actividade contempla as seguintes tarefas:

- o planeamento e a implementação de alterações à infra-estrutura tecnológica;
- a configuração e a instalação dos sistemas operativos fornecidos;
- a configuração de todos os componentes da infra-estrutura tecnológica;
- a execução dos testes apropriados antes da implementação de novos componentes de tecnologia;



Tribunal de Contas

- a revisão da implementação após a sua conclusão e o *follow-up* de itens pendentes;
- a manutenção de um inventário de *hardware*, diagramas de redes e outra documentação, relativa à infra-estrutura tecnológica;
- a gestão da implementação da infra-estrutura tecnológica;
- o assegurar que os requisitos de continuação de “negócio” são adequadamente considerados; e
- a comunicação e planeamento de alterações para limitar o impacte sobre a entidade.

Os factores que contribuem para o sucesso desta actividade incluem:

- uma metodologia definida de selecção, aquisição, manutenção, implementação e substituição de infra-estrutura tecnológica apoiada pela Direcção e IIES;
- a existência e conhecimento de uma estratégia tecnológica, adequadamente articulada, em que os requisitos da arquitectura tecnológica estão definidos e aprovados pelo IIES;
- a existência de um conhecimento detalhado das infra-estruturas tecnológicas existentes;
- a existência de uma integração efectiva e eficiente entre as várias plataformas tecnológicas;
- o processo de selecção considerar os requisitos de capacidade e desempenho necessários e a utilização de componentes reutilizáveis;
- as relações com fornecedores chave serem adequadamente desenvolvidas; e
- a existência de políticas definidas para minimizar as dependências de fornecedores ou prestadores de serviços únicos ou individuais.

3.2.4.2 Situação Actual

Existe um processo de administração das infra-estruturas que tem, até agora, sido realizado de forma descentralizada, o que resultou, relativamente aos investimentos efectuados nesta área, numa não padronização dos sistemas. Neste momento, o IIES encontra-se a definir uma arquitectura tecnológica para o SSSS que passa pela centralização e padronização de plataformas tecnológicas.

Com a excepção do IIES, nenhuma das entidades auditadas utiliza ferramentas na gestão da sua rede local e dos seus clientes de rede, de uma forma que lhe permita efectuar uma manutenção pró activa e mais eficiente do seu parque de tecnologias de informação; assim sendo, na maioria dos casos, esta manutenção é efectuada de forma reactiva. Por outro lado, ainda não foi estabelecido um Plano de Manutenção para o seu parque de Tecnologias de Informação, sendo corrente o recurso a *outsourcing* para a implementação e manutenção de várias componentes da sua infra-estrutura tecnológica, como forma de responder a problemas e reagir a necessidades de alteração; acresce, ainda, que este procedimento nem sempre resulta na transferência de conhecimentos para os funcionários que serão, futuramente, responsáveis pela administração dos sistemas e tecnologias implementadas.



Tribunal de Contas

As considerações de continuidade das novas tecnologias implementadas começam a ser consideradas de uma forma integrada e concertada com a participação do IIES.

3.2.4.3 Riscos Significativos Identificados e Seus Impactes

Os riscos associados a este processo poder-se-ão resumir como segue:

- a existência de mais que uma plataforma a ser suportada no SSSS exigir que se disponha de mais recursos e competências internas para os gerir;
- a dependência de entidades externas para o suporte de componentes críticos dos sistemas do SSSS poder resultar numa capacidade de resposta reduzida perante situações urgentes; e
- a baixa utilização de ferramentas de gestão não permitir uma eficiente disponibilidade dos elementos das Unidades de Sistemas de Informação de cada uma das entidades.

3.2.4.4 Avaliação Global da Actividade – Princiante

- Não tem existido, até agora, uma abordagem consistente na aquisição e manutenção das infra-estruturas de tecnologias de sistemas de informação;
- A descentralização das decisões criou um conjunto de plataformas distintas com requisitos de manutenção e monitorização diferentes;
- A definição de uma arquitectura tecnológica para o SSSS, que passa pela centralização e padronização de plataformas tecnológicas, permitirá a homogeneização dos procedimentos relacionados com a implementação de novas tecnologias em todo o ISSS.

3.2.5. *DESENVOLVIMENTO E MANUTENÇÃO DE PROCEDIMENTOS DE TI*

3.2.5.1 Descrição da Actividade

Esta actividade pretende assegurar a utilização adequada de soluções aplicacionais e tecnológicas, contemplando, para tal, o desenvolvimento de manuais de procedimentos para os utilizadores e operadores de TI, normas de serviço e material de formação. Como parte do processo de desenvolvimento e manutenção de sistemas, os factores que contribuem para o sucesso desta actividade incluem:

- a existência de acordos de níveis de serviço que assegurem a qualidade da documentação relacionada com os sistemas de informação;
- a infra-estrutura e a entidade promoverem a partilha de documentação, procedimentos técnicos e material de formação;



Tribunal de Contas

- a existência de planos de formação da Unidade de Sistemas de Informação sobre os procedimentos estabelecidos;
- a manutenção dos modelos de processos de cada uma das entidades que integram o SSSS, sendo os procedimentos administrativos e operacionais actualizados com recurso a ferramentas automatizadas;
- o processo de desenvolvimento utilizar os procedimentos estabelecidos de forma padronizada; e
- os procedimentos serem desenvolvidos, distribuídos e actualizados de uma forma automática.

3.2.5.2 Situação Actual

Qualquer uma das entidades auditadas reconhece a necessidade da existência de documentação para esta área, havendo mesmo, relativamente às Pensões, um Manual de Procedimentos, divulgado e de utilização corrente junto dos utilizadores, que oferece algum detalhe sobre as principais transacções inerentes a esses processos. A documentação relativa às operações de sistemas de informação é produzida ocasionalmente e de forma dispersa pelas várias Unidades operacionais, afigurando-se, assim, inconsistente. Por outro lado, muitos dos procedimentos e documentação de suporte actuais estão desactualizados, consequência da falta de tempo para realizar as devidas correcções, sendo a sua manutenção efectuada esporadicamente, conforme as necessidades e disponibilidade de cada momento.

3.2.5.3 Riscos Significativos Identificados e Seus Impactes

Os riscos associados a este processo podem-se resumir como segue:

- não adopção das melhores práticas nos procedimentos e controlo sobre o desenvolvimento, manutenção e operação dos SI;
- procedimentos e controlos estabelecidos que não reflectam os requisitos de controlo estabelecidos pela entidade;
- desconhecimento ou falta de formação dos utilizadores sobre as melhores práticas nos procedimentos de utilização e dos requisitos de controlo.

3.2.5.4 Avaliação Global da actividade – Princiante

- Todas as entidades auditadas reconhecem que é necessário um processo que defina e gira os procedimentos de gestão dos seus sistemas de informação;
- Este procedimento é dificultado pela existência de plataformas tecnológicas e aplicações distintas nos vários organismos que integram o SSSS;



Tribunal de Contas

- A documentação produzida é dispersa e incompleta;
- Não existe, nas várias plataformas, qualquer integração de procedimentos, encontrando-se, muitos deles, desactualizados.

3.2.6. INSTALAÇÃO E CERTIFICAÇÃO DE SISTEMAS

3.2.6.1 Descrição da Actividade

Esta actividade pretende confirmar e verificar que as soluções adoptadas e os sistemas implementados estão devidamente testados, verificados e aceites pelos seus utilizadores como prontos para desempenhar as funcionalidades pretendidas, contemplando, normalmente:

- a conversão de dados para as soluções informáticas implementadas;
- a realização de acções de formação dos futuros utilizadores;
- a realização de testes de conformidade com os requisitos estabelecidos;
- a obtenção de uma certificação independente dos sistemas instalados; e
- a implementação de revisões posteriores à instalação para correcção de possíveis problemas detectados.

Para o bom desempenho desta actividade contribuem os seguintes factores:

- uma metodologia de aquisição e implementação estabelecida e aplicada de uma forma consistente;
- a disponibilidade de recursos e de tempo para a execução de testes num ambiente próprio e independente;
- a disponibilidade de dados de teste que sejam representativos dos dados reais, quer em quantidade, quer em qualidade;
- a existência de procedimentos de teste que validem a capacidade dos sistemas para comportar o volume de processamento actual ou futuramente exigido; e
- a definição clara dos requisitos funcionais e operacionais para novas aplicações ou para novas funcionalidades.

3.2.6.2 Situação Actual

A instalação de novos sistemas tem vindo a ser executada por entidades externas contratadas para o desenvolvimento ou personalização de uma solução informática, sendo a conversão de dados para os novos sistemas e a formação dos futuros utilizadores, usualmente, subcontratada à mesma entidade que desenvolve a nova solução, estando os utilizadores chave, geralmente, envolvidos na certificação das funcionalidades pretendidas. O teste dos aspectos de segurança da nova aplicação nem sempre é considerado como parte desta actividade.



Tribunal de Contas

Verificou-se que, normalmente, não são obtidas aprovações formais dos utilizadores antes do transporte de alterações do ambiente de teste para o ambiente de produção. As abordagens e extensão de testes efectuados variam, já que não é utilizada qualquer metodologia de testes estruturada.

É reconhecida a necessidade de verificar e confirmar se a solução implementada serve os objectivos, necessidades funcionais e padrões de qualidade pretendidos.

A este respeito o IIES, em sede de contraditório, vem esclarecer:

“O IIES tem definida e implementada uma metodologia de gestão de projecto que contempla a certificação de sistemas.”

Apesar de o IIES ter definida uma metodologia de gestão de projectos que contempla a certificação de sistemas, essa metodologia não é consistentemente aplicada por todas as entidades do ISSS.

3.2.6.3 Riscos Significativos Identificados e Seus Impactes

Os riscos associados ao processo existente poder-se-ão resumir como segue:

- erros associados a novas funcionalidades ou novas aplicações poderem não ser identificados e resolvidos antes da sua introdução no ambiente produtivo;
- testes insuficientes para assegurar a qualidade dos sistemas, aceites e aprovados pelos utilizadores; e
- falta de familiarização dos utilizadores com as funcionalidades recém implementadas.

3.2.6.4 Avaliação Global da actividade – Repetitivo

- Existe um reconhecimento da necessidade de verificar e confirmar a integridade das soluções ou das novas funcionalidades implementadas;
- Existe alguma consistência na execução de testes para certificar novos sistemas ou funcionalidades, mas não há nenhuma metodologia formal específica para esta actividade;
- As equipas de desenvolvimento estabelecem, normalmente, a abordagem de testes;
- Existe um processo de aprovação que nem sempre é formalizado de acordo com critérios estabelecidos.



3.2.7. GESTÃO DA MUDANÇA

3.2.7.1 Descrição da Actividade

Esta actividade pretende minimizar a probabilidade de ocorrência de falhas ou interrupções na disponibilidade dos sistemas, alterações não autorizadas e erros, contemplando:

- a identificação das mudanças ocorridas;
- a categorização, definição de prioridades e procedimentos de emergência;
- a avaliação dos riscos e impactes das alterações ou mudanças;
- o processo de autorização para ocorrer a mudança;
- a gestão de novas aplicações e versões; e
- a distribuição e actualização de *software* implementado.

Para o sucesso desta actividade concorrem os seguintes factores:

- a existência de políticas definidas e conhecidas para assegurar a actualização sistemática e atempada de novas versões e actualizações de programas e sistemas;
- a existência de ferramentas para suportar a implementação de novas aplicações ou actualizações das actuais aplicações;
- a existência de procedimentos de testes às novas actualizações antes da sua implementação;
- o impacte sobre a *performance* e capacidade dos sistemas e as interdependências das actualizações a serem efectuadas ser considerado antes da sua implementação;
- a existência de documentação actualizada sobre as aplicações instaladas e suas configurações;
- a existência de uma segregação entre as funções de produção e desenvolvimento; e
- a existência de um processo que valide o sucesso das alterações efectuadas.

3.2.7.2 Situação Actual

Existem duas realidades distintas nesta actividade: a do IIES – responsável pela gestão de mudança dos projectos de grande envergadura – e a dos CDSSS – que efectuam alterações aos sistemas existentes.

Há um reconhecimento por parte de todas as entidades auditadas de que as mudanças devem ser geridas e controladas, mas nem sempre é seguido um processo estruturado que parta de uma metodologia formal e *standard* na execução de trabalho de desenvolvimento de sistemas, através das várias fases do ciclo de vida de desenvolvimento de sistemas. Nos projectos de conversão



Tribunal de Contas

para o EURO, constatou-se que houve a definição e categorização de prioridades e uma gestão e controlo de versões das aplicações alteradas. Mesmo assim, nem sempre foi possível assegurar a segregação dos ambientes de desenvolvimento e produção durante este processo.

A documentação sobre o processo de mudança é limitada ou não existe. As alterações são efectuadas de uma forma que reduz a possibilidade de interrupções nos sistemas de informação, mas poderão ocorrer erros aliados a interrupções no ambiente produtivo, devido a uma gestão inadequada do processo de mudança em certas plataformas. Nos CDSSS de Porto e Setúbal, verificou-se que os desenvolvimentos e testes de novas aplicações ou novas funcionalidades são efectuados directamente no ambiente de produção.

3.2.7.3 Riscos Significativos Identificados e Seus Impactes

Os riscos associados a este processo poder-se-ão resumir como segue:

- falta de detecção atempada de alterações disruptivas efectuadas nos sistemas informáticos;
- e
- alterações não autorizadas, erradas ou fraudulentas efectuadas nos sistemas operacionais.

3.2.7.4 Avaliação Global da actividade – Repetitivo

- Existe um processo de gestão de mudanças em vigor, seguindo a maioria das mudanças a mesma abordagem;
- A consistência da documentação das configurações é variável;
- Existe algum planeamento e consideração dos riscos antes da implementação de qualquer mudança que possa afectar a continuidade e estabilidade dos sistemas de informação.



Tribunal de Contas

3.3. OPERAÇÃO DO AMBIENTE INFORMÁTICO

3.3.1. DESCRIÇÃO DO PROCESSO

Este processo abrange a prestação de serviços necessários para suportar as várias componentes de um ambiente de sistemas. Os serviços prestados variam entre a segurança e a continuidade de sistemas, aspectos de formação dos utilizadores, até ao próprio processamento de dados pelos vários sistemas informáticos. Para assegurar a qualidade dos serviços prestados, os processos de suporte têm que ser geridos e controlados.

Este processo está subdividido nas seguintes actividades, em termos do modelo CobIT:

1. Definição dos Níveis de Serviço;
2. Gestão dos Serviços Prestados por Terceiros;
3. Gestão da *Performance* e da Capacidade;
4. Assegurar a Continuidade dos Serviços Prestados;
5. Assegurar a Segurança dos Sistemas;
6. Identificação e Afectação dos Custos;
7. Prestação de Apoio e Formação aos Utilizadores;
8. Apoiar e Aconselhar os Clientes;
9. Gestão da Configuração;
10. Resolução e Gestão de Problemas de TI;
11. Gestão dos Dados;
12. Gestão das Instalações Físicas; e
13. Gestão das Operações.

3.3.2. DEFINIÇÃO DE NÍVEIS DE SERVIÇO

3.3.2.1 Descrição da Actividade

Esta actividade pretende estabelecer um entendimento comum sobre os níveis de serviço de TI esperados pelas várias Unidades dentro das entidades que compõem o SSSS, observando os seguintes requisitos:

- o estabelecimento de acordos formais entre a Unidade de SI e as outras Unidades da Organização;
- a definição de responsabilidades e prioridades entre as partes envolvidas no acordo;
- a definição de tempos de resposta e níveis de qualidade necessários;
- a definição de um custo de prestação desses serviços;
- o estabelecimento de garantias de integridade; e



Tribunal de Contas

- o estabelecimento de acordos que permitam a continuidade do serviço.

Os factores que contribuem para o sucesso desta actividade são, nomeadamente:

- o estabelecimento, nos termos do contrato, de níveis de serviço, de forma perceptível para os utilizadores;
- a realização de análises quando existem problemas ao nível da prestação dos serviços de sistemas de informação;
- a implementação de ferramentas e recursos humanos com valências suficientes para um nível adequado de monitorização sobre os serviços prestados;
- a dependência dos processos de “negócio” críticos sobre os sistemas de informação estar definida e coberta pelos contratos de níveis de serviço;
- as actividades e responsabilidades pela gestão dos sistemas de informação estarem expressas nos contratos de níveis de serviço;
- os responsáveis pela gestão dos sistemas de informação conseguirem identificar e explicar as variações de custos ocorridas durante a prestação de serviços; e
- existir um sistema para monitorizar a actividade de cada um dos intervenientes no processo de prestação de serviços.

A definição de níveis de serviço – *Service Level Agreements (SLA)* – pode resumir-se como um mecanismo de gestão que pode ser utilizado para gerir as expectativas dos utilizadores e os níveis de serviço a serem prestados por cada Unidade de Sistemas de Informação. A utilização de um SLA permite formalizar as expectativas dos utilizadores, definindo objectivamente os serviços e a estrutura de suporte que as Unidades de SI terão que fornecer aos seus clientes internos. Os SLA estabelecem claramente, relativamente às entidades integrantes do SSSS, as necessidades de apoio aos seus utilizadores, permitindo identificar os recursos necessários para tal e os custos associados à prestação desses serviços às várias Unidades de cada estrutura organizativa.

3.3.2.2 Situação Actual

O SSSS encontra-se, actualmente, a definir a sua estratégia de Sistemas de Informação, sendo esta essencial para definir as prioridades de cada Unidade de SI. Neste momento, não existe uma definição formal dos níveis de serviço esperados de cada Unidade de SI e não está pensada a sua definição. A definição de um SLA necessitaria da determinação de medidas de avaliação de desempenho da prestação de serviços de cada Unidade de SI, não existindo, actualmente, os mecanismos necessários para os efectuar.



Tribunal de Contas

3.3.2.3 Riscos Significativos Identificados e Seus Impactes

A definição de níveis de serviço estabelece, objectivamente, as expectativas dos utilizadores e as responsabilidades de cada Unidade de SI. Dada a inexistência destes mecanismos, não há, em cada entidade integrante do SSSS, uma noção completa da qualidade dos serviços prestados pelas Unidades de SI às restantes Unidades.

3.3.2.4 Avaliação Global da Actividade – Não Existente

- As entidades de que compõem o SSSS ainda não implementaram um processo que defina os níveis de serviço dos sistemas de informação exigidos pelos seus utilizadores.

3.3.3. GESTÃO DOS SERVIÇOS PRESTADOS POR TERCEIROS

3.3.3.1 Descrição da Actividade

Esta actividade pretende assegurar que os serviços prestados por terceiros são claramente definidos de acordo com os requisitos pretendidos e continuamente respeitados, para alcançar os objectivos e necessidades de cada entidade, sendo fundamental para a gestão de acordos com entidades terceiras, através da sua monitorização e actualização.

Normalmente, esta actividade contempla:

- o estabelecimento e monitorização de acordos com fornecedores de serviços;
- o estabelecimento de acordos que permitam a continuidade de serviços em termos dos requisitos estabelecidos por cada entidade;
- a definição de requisitos regulamentares e/ou legais que devam ser respeitados; e
- a monitorização do cumprimento das políticas internas de cada entidade pelos prestadores de serviços.

O sucesso desta actividade é determinado, designadamente, pelos seguintes factores:

- a existência de requisitos e métricas de avaliação do serviço prestado claramente definidos;
- a definição, por parte de quem presta serviço, de mecanismos para o reporte do desempenho do serviço prestado;
- cada entidade deter o controlo, responsabilidade e gestão dos serviços externos contratados;
- os fornecedores externos de serviços subcontratados disporem de mecanismos que assegurem a qualidade dos serviços prestados;



Tribunal de Contas

- os requisitos operacionais e de desempenho estarem suficientemente definidos e serem do conhecimento de todas as partes envolvidas;
- os contratos estabelecidos serem legalmente válidos, sendo sujeitos a uma revisão legal;
- a aplicação dos termos definidos no contrato de prestação de serviços assentar em recompensas e penalidades previamente definidas;
- a existência de alguém, em cada uma das entidades, para gerir a relação com os fornecedores ou prestadores dos serviços;
- estar definido um pedido de proposta *standard*, com um critério de avaliação previamente definido e acordado;
- a existência de um processo que contemple a definição a classificação dos problemas ocorridos durante a prestação do serviço, de acordo com sua importância e o tipo de resposta exigível; e
- a existência de procedimentos estabelecidos para a variação das condições e requisitos dos serviços prestados.

3.3.3.2 Situação Actual

O IIES é responsável pela gestão das relações com prestadores de serviços de TI, delegando essa responsabilidade, quando é necessário recorrer à contratação de serviços, nos directores dos Sistemas de Informação dos CDSSS que iniciam a consulta a vários fornecedores. Os critérios de avaliação são identificados para cada projecto nos casos da contratação de serviços e das variações das condições contratuais. Existe um acompanhamento concomitante do fornecimento do serviço, não se podendo, contudo, considerar que este seja estruturado, uma vez que a sua sequência é intuitiva. Quanto aos aspectos legais dos contratos estabelecidos, existe um processo especialmente vocacionado para os assegurar.

3.3.3.3 Riscos Significativos Identificados e Seus Impactes

Em termos das circunstâncias identificadas, as entidades componentes do SSSS ficam expostas aos seguintes riscos:

- os prestadores de serviços não estarem vinculados às políticas de SI estabelecidas para o SSSS;
- os serviços prestados por terceiros poderem ser inadequados, conduzindo a uma baixa *performance* em relação ao que seriam os níveis mínimos aceitáveis, ou a aumentos de custos não programados no orçamento; e
- a monitorização dos serviços prestados poder ser inadequada, podendo originar deficiências na sua qualidade.



Tribunal de Contas

3.3.3.4 Avaliação Global – Definido

- As relações com prestadores de serviços estão reguladas por contratos formais;
- Existem procedimentos bem documentados que regulam a contratação de serviços de terceiros;
- A natureza dos serviços a prestar está detalhada nos contratos que estabelecem requisitos operacionais, legais e de controlo;
- A responsabilidade pela gestão destes contratos está atribuída e os riscos associados aos contratos estabelecidos são avaliados;
- O processo de monitorização dos serviços providenciados por terceiros e de entrega do serviço propriamente dito é efectuado, na maior parte dos casos, através do reporte efectuado pelos prestadores de serviços;
- Existem, na maioria dos casos, reuniões para estabelecer o *status* dos projectos em curso;
- A prestação de serviços por entidades externas está sempre sujeita a um contrato ou proposta previamente estabelecidos ou negociada;
- Não existem cláusulas contratuais padronizadas que se apliquem a todos os projectos.

3.3.4. GESTÃO DA PERFORMANCE E DA CAPACIDADE

3.3.4.1 Descrição da Actividade

Esta actividade pretende assegurar que existe capacidade de sistemas disponível para suportar as actividades de cada entidade do SSSS e que a sua utilização está optimizada para dar resposta às necessidades de *performance* exigidas e para assegurar a continuidade dos sistemas e dos serviços prestados, contemplando, ainda:

- a definição de requisitos mínimos de disponibilidade e *performance* para os sistemas críticos;
- a monitorização contínua dos sistemas e o acompanhamento dos problemas identificados;
- o dimensionamento adequado dos sistemas para suportar as aplicações instaladas; e
- a gestão do equilíbrio de cargas de trabalho atribuídas aos vários sistemas ou componentes de rede.

Os factores que contribuem para o sucesso desta actividade incluem:

- as implicações e requisitos de capacidade de sistemas das aplicações críticas serem adequadamente identificados e entendidos na concepção de novos sistemas;
- os requisitos de desempenho de sistemas serem identificados e avaliados em todos os seus projectos de desenvolvimento ou manutenção;
- os aspectos de capacidade e desempenho serem, devida e atempadamente, considerados no processo de aquisição ou na metodologia de desenvolvimento adoptada;



Tribunal de Contas

- a infra-estrutura tecnológica ser periodicamente revista para permitir a aquisição de tecnologias cujo rácio custos/desempenho seja o mais adequado para cada entidade; e
- existirem ferramentas ou mecanismos que permitam analisar a capacidade actual e projectar o consumo da capacidade disponível.

3.3.4.2 Situação Actual

A responsabilidade pela monitorização do desempenho e gestão de capacidade dos sistemas de informação é partilhada entre o IIES e os CDSSS. Actualmente, cada uma das entidades analisadas tem alguns procedimentos informais de monitorização de espaço em disco e processamento dos seus servidores. A monitorização do desempenho de rede é pontual, mas existem procedimentos de monitorização constante dos tempos de resposta da rede ou da sua capacidade, nos CDSSS. Dada a importância crítica do seu sistema, o CNP tem procedimentos que asseguram a monitorização constante dos seus sistemas principais. A monitorização efectuada sobre os outros é reactiva, visto que só consegue identificar problemas no momento em que acontecem ou posteriormente ao seu acontecimento. A implementação de quotas de espaço nos servidores serve, de certo modo, como um mecanismo de monitorização, já que os utilizadores são obrigados a contactar os administradores de sistema para obterem mais espaço em disco.

Não existem, actualmente, mecanismos ou procedimentos que permitam detectar e resolver, imediatamente, problemas de falta de capacidade de processamento dos sistemas de informação.

Não se pode considerar que exista um planeamento de capacidade dos sistemas, considerando-se, apenas, a implementação de *upgrades* ou novas soluções, quando não existem alternativas susceptíveis de serem aplicadas ou se verifique, de facto, largos períodos de indisponibilidade dos sistemas.

3.3.4.3 Riscos Significativos Identificados e Seus Impactes

Nestas circunstâncias, cada uma das entidades analisadas no SSSS fica exposta aos seguintes riscos:

- a capacidade de monitorização da *performance* dos sistemas ser inadequada, o que pode conduzir a uma baixa rentabilidade dos sistemas em causa e a interrupções dos serviços prestados; e
- o desempenho dos sistemas e a sua disponibilidade poderem ser inadequados, face aos níveis de serviço prestado por cada Unidade de Sistemas de Informação destas entidades.



3.3.4.4 Avaliação Global – Repetitivo

- Os responsáveis pelas entidades analisadas estão conscientes do impacto que a falta de gestão de *performance* e capacidade de sistemas de informação pode ter sobre o “negócio”;
- Para os sistemas críticos existe alguma monitorização periódica informal efectuada pelos funcionários dos Serviços/Unidades de Informação;
- Existem algumas ferramentas de análise de *performance* e capacidade, mas a consistência da monitorização está dependente dos elementos do Núcleo de Sistemas de Informação;
- Não existe uma avaliação global da capacidade de *performance* ou a consideração de picos de processamento;
- É provável a ocorrência de problemas de disponibilidade, à medida que as entidades que integram o SSSS aumentam a utilização dos seus sistemas de informação.

3.3.5. ASSEGURAR A CONTINUIDADE DE SERVIÇOS PRESTADOS

3.3.5.1 Descrição da Actividade

Esta actividade pretende assegurar a disponibilidade dos serviços de TI e minimizar os impactos de uma falha na disponibilidade dos seus sistemas, contemplando os seguintes aspectos:

- a identificação dos sistemas críticos de cada uma das entidades analisadas e a definição de procedimentos que assegurem a sua disponibilidade;
- a definição de planos formalizados de intervenção para determinadas situações de risco e desastre;
- a implementação de procedimentos alternativos para fazer face às eventuais contingências;
- a implementação de procedimentos de *backup* e recuperação de dados;
- o desenvolvimento de diversas acções de formação e testes sistemáticos dos sistemas;
- o controlo contínuo sobre os recursos de telecomunicações para assegurar que estes se encontram disponíveis; e
- a observação da integridade das bases de dados que suportam algumas das aplicações críticas em utilização nas entidades do SSSS visadas.

Os factores que contribuem para o sucesso desta actividade incluem:

- a existência de um sistema que garanta o fornecimento de energia eléctrica em caso de quebra de corrente, sendo este regularmente testado para assegurar a sua fiabilidade;
- a identificação e monitorização contínua dos potenciais riscos das infra-estruturas críticas;
- a continuidade de serviços ser o resultado natural do planeamento antecipado da capacidade, da aquisição de componentes de alta fiabilidade, da existência de um nível de



Tribunal de Contas

redundâncias de infra-estruturas adequado, da existência de planos de contingência testados e da remoção de pontos únicos de falha dos sistemas;

- a acumulação de experiência na resolução de falhas nos sistemas resultar na implementação de acções correctivas e pró activas;
- a realização de testes dos planos de contingência possibilitar a identificação de iniciativas pró activas;
- a realização de análises periódicas da disponibilidade dos sistemas de informação;
- utilização de acordos de níveis de serviços para aumentar a cooperação dos fornecedores, de forma a diminuir os riscos de descontinuidade dos sistemas; e
- especificação e quantificação dos custos da interrupção dos sistemas, para motivar o desenvolvimento de planos e mecanismos de contingência.

3.3.5.2 Situação Actual

Da avaliação efectuada desta actividade, constatou-se que nenhuma das entidades abordadas formalizou um Plano de Contingências para os seus sistemas de informação, tendo, apenas, cada uma das Unidades de Sistemas de Informação, um mínimo de procedimentos informais de segurança física e de salvaguarda de informação.

Os procedimentos de salvaguarda de dados contemplam, em todos os casos verificados, a realização de *backups* diários da informação armazenada nos seus servidores; contudo, não está definido – à excepção do CNP – um procedimento complementar que obrigue a guardar as cópias de segurança efectuadas fora das instalações de processamento.

As instalações físicas onde se encontram os sistemas de informação condicionam o nível de salvaguarda da informação, como acontece, por exemplo, no CDSSS de Setúbal, cuja sala de processamento não oferece a protecção física adequada aos sistemas de informação, nomeadamente, porque:

- existe diverso material combustível na sala de processamento;
- a porta não oferece a protecção suficiente em caso de incêndio; e
- a sala de computadores não dispõe de reguladores de humidade.

As entidades do SSSS que foram alvo desta auditoria não procederam a uma classificação da sua informação em termos de confidencialidade e disponibilidade exigida, procedimentos que constituiriam o primeiro passo para perceber qual a informação crítica e quais as medidas necessárias a tomar para a sua salvaguarda. Por outro lado, ainda não se estabeleceu qualquer contrato com fornecedores para garantir a reposição de equipamentos críticos no caso da ocorrência de uma contingência significativa, havendo apenas acordos que abrangem a substituição de equipamentos em caso de avaria. Neste momento, as referidas entidades, para procederem à recuperação dos seus sistemas dependem, de forma crítica, dos funcionários de cada Unidade de



Tribunal de Contas

Sistemas de Informação, podendo a sua indisponibilidade, em caso de calamidade, dificultar a resolução dos problemas.

3.3.5.3 Riscos Significativos Identificados e Seus Impactes

A interrupção do serviço ou a indisponibilidade dos sistemas pode ter um significativo impacte nas operações de cada entidade, ficando o SSSS exposto aos seguintes riscos:

- a disponibilidade dos sistemas no CNP é fundamental para assegurar o atempado processamento das pensões a pagar aos pensionistas, podendo a sua eventual indisponibilidade ter um impacte operacional e social bastante significativo;
- os dados de registo de remunerações dos CDSSS são a base de cálculo das pensões atribuídas pelo CNP; assim, se os CDSSS não assegurarem a disponibilidade destes dados, poderá ser posta em causa a integridade do cálculo e o seu atempado processamento.

3.3.5.4 Avaliação Global – Repetitivo

- Existe uma percepção, cada vez mais forte, da importância de assegurar a continuidade dos sistemas de informação no seio do SSSS, não existindo, contudo, uma consciência clara das implicações resultantes de uma paragem dos mesmos;
- A responsabilidade de assegurar a continuidade dos seus sistemas está atribuída a cada Unidade de Sistemas de Informação, mas as tarefas e responsabilidades individuais necessárias para a recuperação de sistemas não estão formalmente definidas;
- Em caso de descontinuidade dos sistemas, a reacção não estará preparada nem estruturada e os utilizadores poderão ter que procurar soluções alternativas para dar resposta aos problemas que vão surgindo;
- O sucesso da recuperação dos sistemas afectados dependerá da experiência dos funcionários disponíveis para efectuar o processo;
- Não existe uma avaliação dos níveis de continuidade exigidos para os vários sistemas e do seu impacte sobre as operações de cada uma das entidades do SSSS.

3.3.6. ASSEGURAR A SEGURANÇA DOS SISTEMAS

3.3.6.1 Descrição da Actividade



Tribunal de Contas

Esta actividade pretende assegurar o estabelecimento de um nível de segurança apropriado para proteger a informação das entidades que integram o SSSS através da implementação de controlos que limitem, a utilizadores autorizados, o acesso a programas, dados e sistemas. Este processo normalmente considera:

- a implementação de uma arquitectura de segurança para a entidade visada;
- a implementação de controlos de acesso para responder às necessidades de confidencialidade e integridade da informação das entidades do SSSS;
- a administração de sessões de formação sobre segurança;
- a definição, implementação e manutenção de políticas e procedimentos de segurança de sistemas de informação;
- a monitorização e investigação de anomalias de segurança;
- a manutenção de segurança física efectiva sobre os sistemas de informação; e
- a administração da segurança dos sistemas de informação.

Os factores que contribuem para o sucesso desta actividade incluem:

- a existência de um plano global de segurança que estabeleça políticas e normas claras, identifique a implementação de mecanismos de controlo cujo custo/benefício é aceitável para a entidade e defina processos de monitorização que avaliem o cumprimento das políticas estabelecidas;
- a consciência de que um bom plano de segurança leva tempo a desenvolver;
- o responsável, em cada entidade, pela implementação dos planos de segurança reportar directamente à sua Direcção;
- os colaboradores e a Direcção terem um conhecimento adequado das vulnerabilidades e ameaças dos seus sistemas e reconhecerem a necessidade de estabelecer medidas de segurança;
- a avaliação periódica do cumprimento das políticas de segurança por terceiros;
- a existência de um conjunto de regras definidas para aqueles que desenvolvem, implementam e usam os sistemas, bem como para aqueles que supervisionam a sua segurança;
- uma função de segurança que seja capaz de detectar, registar, analisar, comunicar e actuar em situações de falhas de segurança, minimizando a probabilidade de falhas;
- a existência de um processo centralizado de gestão de utilizadores que forneça os meios para identificar e atribuir autorizações de acesso aos utilizadores de forma consistente e eficaz; e
- a existência de um processo de autenticação dos utilizadores com um custo razoável, de fácil implementação e utilização.

3.3.6.2 Situação Actual



Tribunal de Contas

Existem alguns aspectos relacionados com a gestão da segurança da informação que as entidades auditadas necessitam de rever e que resultam, essencialmente, da não definição formal de políticas e procedimentos de segurança.

Dada a multiplicidade de plataformas tecnológicas presentes nas entidades auditadas, existem, sobre cada uma delas, aspectos específicos a relatar quanto ao processo de gestão de segurança. Relatam-se, seguidamente, as realidades observadas nos organismos alvo deste trabalho, pela seguinte ordem: CNP, CDSSS Lisboa, CDSSS Porto e CDSSS Setúbal.

- **CENTRO NACIONAL DE PENSÕES (CNP)**

- **Serviços de TCP/IP – Unisys ClearPath 2200**

O serviço de *HTTP* está activo no sistema *Unisys*. Quantos mais serviços desnecessários estão instalados num servidor, maior é o número de vulnerabilidades que podem ser exploradas, pondo em causa a integridade e disponibilidade dos mesmos.

- **Qualidade das Passwords – Unisys ClearPath 2200**

O parâmetro *MINPASSLEN* tem o valor de 3, o que significa que o sistema *Unisys ClearPath 2200* requer que cada *password* possa ter, no mínimo, 3 caracteres de comprimento. A não existência de procedimentos que forcem o estabelecimento de *passwords*, com uma composição complexa, aumenta o risco da existência de acessos não autorizados ao sistema *Unisys*, colocando em causa a confidencialidade e integridade deste sistema. Desta forma, com os actuais parâmetros, pode ser possível, num curto espaço de tempo, a descodificação das *passwords*, mediante a utilização de programas específicos para tal.

Alega o ISSS:

“Apesar de cada password ter no mínimo 3 caracteres, seria necessário a entrada no sistema para acesso ao ficheiro onde estão encriptadas.”

Uma *password* com somente 3 caracteres oferece pouca protecção contra tentativas de autenticação indevidas



- **Intervalos de Expiração de Passwords – Unisys ClearPath 2200**

No sistema *Unisys ClearPath 2200* não está implementado nenhum mecanismo que obrigue os utilizadores a, de forma regular, alterar a sua *password*. A ausência deste mecanismo implica o risco de que, caso alguém obtenha acesso indevido ao sistema *Unisys*, possa continuar a tê-lo durante um período de tempo indeterminável. Se a *password* for alterada forçará esses indivíduos, com acesso indevido, a abandonar os sistemas.

- **Servidores de Autenticação – Sistema Windows NT**

O servidor *CNPAUT* possui, instalado, o *Internet Information Server* e o *Proxy Server*. Se os servidores de autenticação forem utilizados para outros fins, pode existir o risco de não existirem recursos disponíveis suficientes para todas as tarefas. Para além disso, quanto mais serviços o servidor tiver, mais vulnerável está a ataques, devido ao maior número de portas abertas e serviços de comunicação activos.

- **Serviços activos – Sistema Windows NT**

Existem, no sistema operativo *Windows NT*, serviços activos que se consideram não ser os mais indicados para o seu funcionamento, nomeadamente os serviços *Messenger* e *Alerter*. Quanto mais serviços estão instalados num servidor, maior é o número de vulnerabilidades que podem ser exploradas, pondo em causa a integridade e disponibilidade dos mesmos. Desta forma, os serviços *Messenger* e *Alerter* poderão revelar, a utilizadores não autorizados, informação atractiva sobre o sistema operativo *Windows NT*.

- **Account Policies – Sistema Windows NT**

Na análise às políticas de segurança do domínio CNP, verificou-se que houve alterações nas *Account Policies* dos *Domain Controllers* daquele domínio. Contudo, considera-se que a *parametrização* escolhida poderá ser optimizada em determinados parâmetros. A definição inadequada de *Account Policies* aumenta o risco de ocorrência de acessos não autorizados aos recursos de um domínio *Windows NT*. As políticas estabelecidas poderão deixar o CNP vulnerável a quebras de segurança nos seus sistemas *Windows NT*. A implementação de procedimentos regulares de mudança de *passwords*, associada a uma composição complexa, contribuiria para minimizar este risco.

- **Perfis de Utilizadores – Sistema Windows NT**

Na análise às datas da última autenticação feita pelos utilizadores no domínio CNP, verificaram-se cerca de 113 perfis de utilizadores que não se autenticavam há mais de 3 meses. A manutenção de utilizadores que não se autenticam há um longo período de tempo poderá provocar a ocorrência de tentativas de acesso, não autorizadas, aos recursos dos sistemas *Windows NT*, através da utilização indevida destes utilizadores, agravado pelo facto de alguns desses utilizadores serem administradores dos respectivos domínios. Estes utilizadores representam normalmente funcionários que já não pertencem aos quadros da Organização ou se encontram ausentes durante um longo período de tempo



- **Expiração de Contas Temporárias – Sistema *Windows NT***

As contas dos utilizadores do domínio CNP nunca expiram e as contas genéricas *CNPT33 (Unisys)* e *PARAREDE* possuem privilégios de administração, não estando configuradas para expirar após um determinado período de tempo. A expiração de contas garante que utilizadores temporários ou pertencentes a empresas terceiras fiquem impossibilitados de aceder a recursos do CNP, depois de expirado o prazo de intervenção dessas entidades, como são os casos dos utilizadores *CNPT33* e *PARAREDE*. Se se mantiverem contas que estejam “adormecidas” ou inactivas poderão ocorrer, mais facilmente, tentativas de acesso não autorizadas aos recursos disponibilizados por estes sistemas.

- **Utilizadores Genéricos – Sistema *Windows NT***

Observou-se a existência de utilizadores genéricos no domínio CNP, dentro do grupo de *Administrators*, nomeadamente: *cnpt38* e *cnpt20*. Verificou-se, ainda, a existência de um número elevado de contas genéricas pertencentes ao grupo *Domain Users* que não se encontram atribuídas a nenhum utilizador específico. A existência de utilizadores genéricos limita a possibilidade de atribuição de responsabilidades por acções impróprias no sistema por quem os utiliza, dado que, nos registos dos ficheiros de *log*, surge sempre o mesmo utilizador, independentemente de quem o estiver a utilizar. Devido a este facto, este tipo de utilizadores genéricos é o principal alvo para obtenção de acessos indevidos ao sistema, agravado pelo facto de os utilizadores em causa possuírem privilégios de administração sobre o domínio CNP.

- ***Home Directories* – Sistema *Windows NT***

Verificou-se que não são utilizadas *home directories* para as contas dos utilizadores no domínio CNP. Quando o administrador de sistemas NT controla quais os directórios que fazem parte das *home directories* dos vários utilizadores, torna-se mais fácil proceder a *backups* ou eliminar especificamente alguns ficheiros. Constitui também uma boa política dar a cada utilizador um directório próprio e, se possível, numa *drive* de rede.

- **CDSSS DE LISBOA**

- **Serviços de *TCP/IP* – Sistema *VSE/ESA***

Verificou-se a existência de vários serviços de rede *TCP/IP* activos que poderão não ser necessários e/ou apresentarem vulnerabilidades de segurança, nomeadamente: *FTP*, *TELNET* e *HTTP*. Cada serviço constitui uma potencial porta de entrada no sistema, pelo que a permanência destes serviços activos conduz ao risco de aproveitamento, por parte de elementos hostis, das vulnerabilidades de segurança que os mesmos apresentem, de forma a acederem, indevidamente, aos sistemas do CDSSS de Lisboa. Caso não estejam correctamente definidas as autoridades sobre os objectos/recursos de informação, existe o risco de alguém, de forma deliberada ou não, pôr em causa a confidencialidade de dados.

- ***Internet Information Server* – Sistema *Windows NT***

O *Internet Information Server* encontra-se instalado no *PDC* (*IP address* 172.22.1.10) do domínio. A instalação do *Internet Information Server* implica a consideração de inúmeros aspectos de segurança. Apesar de disponibilizar vários mecanismos de controlo de acesso, uma instalação



incorrecta do *IIS* poderá colocar em risco a integridade e confidencialidade da informação do CDSSS de Lisboa. São conhecidas várias vulnerabilidades nos serviços do *IIS*.

Por outro lado, verificou-se que o *IIS* se encontra instalado no *Primary Domain Controller*. Isto não é aconselhável, uma vez que é permitido ter acesso a esse servidor através de uma conta *IUSR_(nome da máquina)*, que é uma conta *guest*.

○ Utilizadores Genéricos e Sem Utilização – Sistema *Windows NT*

Observou-se a existência de utilizadores pendentes de desactivação [cujas contas não são utilizadas há mais de 2 (dois) meses], bem como de perfis de utilizadores activos com nomes genéricos.

Os perfis dos utilizadores são a primeira ferramenta de defesa contra acessos não autorizados aos sistemas de informação de qualquer entidade. A qualidade dos controlos de acesso com base em perfis de utilizadores e *passwords* é fundamental para assegurar a segregação de funções nos sistemas de informação.

Se forem mantidos perfis de utilizadores abertos que estejam “adormecidos” ou inactivos poderão ocorrer tentativas de acesso não autorizadas aos recursos dos sistemas informáticos. Estes representam, normalmente, funcionários que já não pertencem aos quadros de pessoal, se encontram durante um longo período de tempo ausentes ou, mesmo, consultores externos.

A existência de perfis de utilizadores activos com nomes genéricos está normalmente associada a grupos de utilizadores que utilizam a mesma conta, aumentando, nestas circunstâncias, o risco de acessos não autorizados.

○ Procedimentos de Retirada de Acessos – Sistema *Windows NT*

Não existem procedimentos formais e regulares para assegurar que os direitos de acesso de funcionários saídos do CDSSS de Lisboa, ou transferidos entre Unidades, sejam prontamente removidos ou alterados.

Embora esta situação não tenha especial impacte na actual comunidade de utilizadores, atendendo à existência de utilizadores partilhados, é um ponto a considerar após a implementação da observação do ponto anterior. A acumulação de direitos de acesso de funcionários saídos do CDSSS de Lisboa, ou transferidos entre Unidades, aumenta o risco de acesso não autorizado a dados.

○ *Account Policies* – Sistema *Windows NT*

As *Account Policies* definidas para o servidor de domínio *Windows NT* providenciam um nível de segurança mais baixo do que seria recomendável. Constatou-se, nomeadamente, que:

- vários utilizadores não são obrigados a alterar a sua *password*;
- não está definido o *Account Lockout*;
- não se mantém qualquer histórico das *passwords*, de modo a impedir a sua eterna utilização.

Sendo o nível de segurança providenciado pela definição inicial insuficiente, estas políticas devem ser ajustadas para, assim, se providenciar um nível de segurança mais adequado, no que respeita à identificação e autenticação dos utilizadores nos domínios NT. A definição de uma *Account Policy*



Tribunal de Contas

inadequada aumenta o risco de ocorrência de acessos não autorizados aos recursos dos domínios NT.

- **Software de Segurança para IBM VSE/ESA**

Durante a análise realizada ao sistema *VSE/ESA* verificou-se que não está a ser utilizado qualquer *software* para gerir os aspectos de controlo de acesso à informação neste sistema; assim, dado que não se utiliza qualquer pacote de segurança (ex. *IBM RACF*, *CA TOP SECRET* ou *CA-ACF2*), não se pode gerir de forma eficiente e abrangente os aspectos relacionados com o acesso aos recursos de informação do CDSSS de Lisboa, existindo, portanto, o risco de se estar a permitir o acesso, de forma não consciente, a esses mesmos recursos.

- **CDSSS DE PORTO**

- **Atribuição de Novos Acessos**

Para a atribuição de novos acessos a utilizadores dos sistemas do CDSSS – Porto, verificou-se que não há procedimentos ou evidência formal de aprovação, de descrição de funções e da sua subsequente instalação no sistema. Sem estes procedimentos atribuídos a novos utilizadores, a Direcção de Sistemas de Informação não pode assegurar a correcta atribuição de funções, que a correcta autorização foi obtida e que a instalação foi correctamente efectuada.

- **Retirada de Acessos**

Não existe um procedimento formalmente instituído que faça com que todos os recursos, ao nível de sistemas, de um determinado utilizador, que deixe de estar a funcionar, sejam retirados. A acumulação de direitos de acesso de funcionários saídos do CDSSS-Porto, ou transferidos entre departamentos, aumenta o risco de indivíduos que já não trabalham para a empresa (quando possuem acesso remoto), ou que tenham sido transferidos de departamento, tenham acesso, não autorizado, a dados, ou cujo acesso seja efectuado ou partilhado por outros funcionários. A ausência de evidência de procedimentos regulares de retirada de *userid*s com acesso bloqueado ao sistema dificulta a gestão e manutenção de uma política de acessos.

- **Fracos Controlos de Acesso – IDMS e ADABAS**

Não existem políticas sobre as contas definidas dos utilizadores que permitam ter um nível de segurança adequado. Nos acessos definidos para a base de dados *ADABAS* não existem utilizadores personalizados, mas sim utilizadores comuns a um grupo de funcionários com senha igualmente comum. A inexistência da possibilidade de definição das políticas aumenta o risco de ocorrência de acessos não autorizados aos recursos. A ausência de evidência de procedimentos regulares de retirada de *userid*s com acesso original que o rasto de auditoria se perca, não sendo possível identificar directamente o utilizador.



- **Utilizadores na Classe de *Administrator***

Observou-se a existência de cerca de 45 pessoas cujo perfil é de administrador. O facto de se permitir que exista um número alargado de contas com perfil de administrador, ou utilizadores que conhecem a senha dessas contas, implica que o risco de alterações não autorizadas seja bastante elevado.

- **Monitorização de Acessos**

Não existem procedimentos formais e regulares de revisão de violações de acessos. Podem ocorrer situações de tentativas de acesso que, no caso de serem bem sucedidas, poderão comprometer a confidencialidade e integridade da informação do CDSSS-Porto.

- **CDSSS DE SETÚBAL**

- ***Default Public Authority* – Sistema *OS/400***

O parâmetro *QCRTAUT* determina a *public authority* para cada objecto novo que seja criado no sistema, verificando-se, para tal, duas condições:

- a *library* do novo objecto possuir um *create authority* de **SYSVAL*; e
- o novo objecto é criado com *public authority* de **LIBCRTAUT*.

Observou-se que o parâmetro está configurado com o valor de sistema **CHANGE*.

Existe o risco de qualquer utilizador do sistema *OS/400* poder modificar ou eliminar novos objectos que são criados no sistema, caso a *public authority* esteja configurada com o valor de **CHANGE*. Desta forma, poderão ocorrer alterações a objectos em bibliotecas consideradas críticas para o CDSSS – Setúbal, o que poderá colocar em causa a disponibilidade e integridade da informação do sistema *OS/400*.

- **Segurança de Objectos Críticos – Sistema *OS/400***

Na análise do sistema *OS/400*, verificou-se que o parâmetro *QALWOBJRST* tem o valor de **ALL*. Existe o risco de que objectos que adoptam a sua própria autoridade ou objectos de sistema possam ser recuperados para o sistema *OS/400*, por um perfil de utilizador que não tenha as devidas permissões para o fazer, modificando a autoridade desses objectos. Nesta situação, objectos críticos ou sensíveis poderão ser acedidos por utilizadores não autorizados.

- **Serviços de *TCP/IP* – Sistema *OS/400***

Existem vários serviços de rede *TCP/IP* activos que poderão não ser necessários e/ou apresentarem vulnerabilidades de segurança, nomeadamente: *FTP*, *SMTP* e *POP3*. Cada serviço constitui uma potencial porta de entrada no servidor, pelo que a permanência destes serviços activos conduz ao risco de aproveitamento, por parte de elementos hostis, de vulnerabilidades de segurança dos mesmos, de forma a entrarem indevidamente no sistema *OS/400*. Desta forma é possível estabelecer sessões de *FTP* para o sistema *OS/400* do CDSSS – Setúbal, bem como para cada um dos sistemas *OS/400* pertencentes a cada CDSSS que possuam aquele tipo de sistema. O serviço de *FTP* permite, nomeadamente, executar remotamente alguns comandos do *OS/400*. Caso



não estejam correctamente definidas as autoridades sobre as bibliotecas e objectos, existe o risco de alguém, de forma deliberada ou não, pôr em causa a confidencialidade de dados.

○ **Qualidade das Passwords – Sistema OS/400**

O *AS/400* possui determinados parâmetros que permitem definir a qualidade das *passwords* a utilizar no sistema; de entre eles, distinguiram-se:

- *QPWDRQDDIF* – Este parâmetro tem o valor de sistema = 0, o que possibilita aos utilizadores do CDSSS – Setúbal, alterar a sua *password* para uma já anteriormente utilizada;
- *QPWDLMTAJC* – Este parâmetro tem o valor de sistema = 0, o que permite que os utilizadores possam definir *passwords* com dígitos (0-9) em posições adjacentes (Ex. Permite *passwords* com números sequenciais ou datas);
- *QPWDLMTREP* – Este parâmetro tem o valor de sistema = 0, possibilitando a repetição de caracteres numa *password* (Ex. Permite *passwords* do tipo ‘AAAAAA’);
- *QPWDMINLEN* – Este parâmetro tem o valor de sistema = 1, permitindo que seja utilizado apenas 1 carácter para definir a *password*; e
- *QPWDRQDDGT* – Este parâmetro tem o valor de sistema = 0, o que não obriga a que todas as *passwords* contenham pelo menos um carácter numérico.

As *passwords* dos utilizadores são a primeira linha de defesa contra acessos não autorizados a qualquer sistema, incluindo os sistemas *OS/400*; desta forma, se a sua qualidade for muito fraca, existe o risco de serem facilmente descobertas ou partilhadas por vários utilizadores, podendo conduzir a que indivíduos não autorizados tenham acesso ao sistema em análise, pondo em causa a sua confidencialidade e integridade. Com os actuais parâmetros é ainda possível, num curto espaço de tempo, a descodificação de *passwords*, através da utilização de programas próprios para tal, que incorporam dicionários de *passwords* óbvias.

○ **Intervalos de Expiração de Passwords – Sistema OS/400**

O sistema *OS/400* não obriga os utilizadores a alterarem regularmente as suas *passwords*, uma vez que o parâmetro *QPWDEXPITV* tem o valor de sistema **NOMAX*. A falta de um mecanismo que obrigue os utilizadores a alterar, periodicamente, a sua *password*, implica o risco de que, caso algum indivíduo obtenha acesso indevido ao sistema *OS/400*, possa continuar a tê-lo durante um período de tempo indeterminável, colocando em causa a confidencialidade daquele sistema. Caso a *password* seja alterada, forçará esses elementos não autorizados a abandonar o sistema.

○ **Número de Sessões Concorrentes – Sistema OS/400**

O parâmetro *QLMTDEVSSN* tem o valor de sistema = 0, permitindo o estabelecimento de um número ilimitado de sessões concorrentes no sistema *OS/400*, isto é, possibilita aos utilizadores a abertura de diferentes sessões em diferentes terminais, caso o parâmetro *QLMTDEVSSN* do seu *user profile* seja **SYSVAL*. O sistema *OS/400*, ao não limitar o número de ligações concorrentes para o mesmo utilizador, aumenta o risco de um elemento não autorizado conseguir estabelecer, pelo menos, uma ligação simultânea, com as credenciais de autenticação de outro utilizador, sem haver a possibilidade de ser detectado, podendo, desta forma, ter acesso a informação



confidencial. Esta situação conduz, também, ao risco de partilha de *passwords* entre utilizadores e de acessos a terminais não autorizados.

- **User Profile de Sistema – Sistema OS/400**

O *user profile* de sistema *QSYSOPR* tem atribuído a *password* igual ao nome do *user profile*, a qual vem atribuída por omissão no sistema *OS/400*. As *passwords default* do sistema *OS/400* vêm descritas na maior parte da documentação relativa a este sistema, tornando-as extremamente conhecidas. Desta forma, existe o risco de que *hackers* ou utilizadores do CDSSS – Setúbal, possam utilizar indevidamente este *user profile*, colocando em causa a integridade, confidencialidade e disponibilidade do sistema *OS/400*.

- **Perfis de Utilizadores – Sistema OS/400**

Na análise às datas da última autenticação feita pelos perfis de utilizadores no sistema *OS/400*, verificou-se que há muitos deles que não se autenticam há mais de 3 meses ou que nunca o chegaram a fazer. Dentro destes perfis estão utilizadores com privilégios elevados no sistema *OS/400*. Adicionalmente, detectou-se, ainda, a existência de vários perfis de utilizadores inactivos (*DISABLE*), incluindo perfis pertencentes à classe de utilizadores **SECOFR*. A manutenção de perfis de utilizadores que não se autenticam há um longo período de tempo poderá provocar a ocorrência de tentativas de acesso, não autorizadas, aos recursos do sistema *OS/400* através da utilização indevida destes perfis, agravado pelo facto de alguns desses perfis de utilizadores pertencerem a classes de utilizadores com elevados privilégios neste sistema. Estes utilizadores representam normalmente funcionários que já não pertencem aos quadros da Organização ou se encontram ausentes durante um longo período de tempo.

- **Perfis de Utilizadores Genéricos – Sistema OS/400**

Observou-se a existência de perfis de utilizadores genéricos, pertencente a classes de utilizadores com privilégios elevados no sistema. A qualidade dos controlos de acesso com base nas contas de utilizadores e *passwords* é fundamental para assegurar um nível de segregação de funções adequado nos sistemas de informação. A existência de perfis de utilizadores abertos com nomes genéricos está normalmente associada a grupos de utilizadores que utilizam a mesma conta, existindo, nestas circunstâncias, uma limitação da possibilidade de atribuição de responsabilidades por acções impróprias no sistema por quem os utiliza, dado que, nos ficheiros de *log*, surge sempre o mesmo utilizador, independentemente de quem o estiver a utilizar. Devido a este facto, os utilizadores genéricos são os principais alvos para obtenção de acessos indevidos ao sistema.

- **Sign-on ao Sistema – Sistema OS/400**

Constatou-se que o número máximo permitido para tentativas falhadas de autenticação no sistema *OS/400* é de 10, visto que o parâmetro *QMAXSIGN* tem o valor de sistema = 10. Um método habitual de ataques de intrusão aos sistemas de informação consiste na tentativa de estabelecimento de ligação aos sistemas, nos quais se inclui o *OS/400*, tentando adivinhar as *passwords* de utilizadores *default* do sistema ou de utilizadores cujo nome seja já conhecido. Estas tentativas podem ser manuais, ou através de ataques de *brute force*, procedendo-se a várias tentativas de ligação ao sistema até que uma seja conseguida, aumentando o risco de um elemento não autorizado ganhar acesso indevido à informação crítica do sistema *OS/400*.

- **Sign-on do Security Officer – Sistema OS/400**



O parâmetro *QLMTSECOFR* tem o valor de sistema = 0, o que significa que todos os perfis de utilizadores com as *special authorities* *ALLOBJ e/ou *SERVICE podem efectuar *sign-on* em qualquer terminal que tenha especificado pelo menos a autoridade pública de *CHANGE. O parâmetro *QLMTSECOFR* permite restringir o *sign-on* de perfis de utilizadores com as *special authorities* *ALLOBJ e/ou *SERVICE a computadores específicos. Caso esta funcionalidade não seja utilizada, não é possível limitar a utilização de perfis de utilizadores poderosos em terminais considerados seguros no CDSSS – Setúbal.

- **Informação de Sign-on – Sistema OS/400**

O parâmetro *QDPSGNINF* possui o valor de sistema = 0, significando que o sistema OS/400 não permite que o utilizador visualize informação relevante sobre o seu *sign-on* ao sistema (ex: data da última autenticação no sistema, número de tentativas de acesso inválidas desde a última entrada bem sucedida, número de dias que faltam para a *password* expirar, etc.). A inexistência da informação sobre o último *sign-on*, implica o risco de que o dono do perfil de utilizador não seja capaz de determinar se alguém obteve acesso ao sistema através das suas credenciais de autenticação (nome de utilizador e *password*), uma vez que só o próprio utilizador consegue validar essa informação.

- **Desactivação de Sessões Inactivas – Sistema OS/400**

O parâmetro *QINACTIV* está configurado com o valor de sistema *NONE, significando que o sistema OS/400 nunca termina a sessão de um utilizador (*log-off*), independentemente do período de tempo de inactividade nessa sessão. Observou-se, ainda, que o valor do parâmetro *QINACTMSGQ* é *ENDJOB. Se os utilizadores não forem desactivados automaticamente do sistema OS/400, existe o risco de que algum elemento que obtenha acesso físico ao terminal do utilizador possa obter acesso a informação sensível ou considerada confidencial para o CDSSS – Setúbal. Estando o parâmetro *QINACTMSGQ* com o valor *ENDJOB implica que a sessão corrente seja imediatamente terminada assim que o seu tempo de inactividade for atingido, podendo resultar em perda de informação importante para o utilizador.

- **Dispositivos Virtuais – Sistema OS/400**

O parâmetro *QAUTOVRT* está configurado com o valor de sistema 32767, valor este muito superior ao recomendado. Este parâmetro determina se é possível a configuração automática de dispositivos virtuais para o estabelecimento de sessões no OS/400 mediante a autenticação, naquele sistema, por *pass-through* ou via *Telnet*. Existe o risco do sistema OS/400 disponibilizar até 32767 dispositivos virtuais, de forma a ser possível configurar, automaticamente, pedidos de acesso por *pass-through* ou via *Telnet*. Um dispositivo que disponibilize acessos exteriores de/para a rede pode ser adicionado virtualmente por qualquer elemento, sem existirem as devidas precauções de segurança.

O número de tentativas de acessos remotos permitidas aumenta à medida que o parâmetro *QAUTOVRT* tem um valor superior a 0. O valor constante neste parâmetro traduz que o número de tentativas de acesso autorizadas por intermédio de dispositivos remotos é igual ao valor deste parâmetro multiplicado pelo valor do parâmetro *QMAXSIGN*.

- **Programa Attention-Key – Sistema OS/400**



O parâmetro de segurança *QATNPGM* tem o valor **ASSIST*, o que significa que cada vez que um utilizador do CDSSS – Setúbal utiliza a *Attention-Key* é chamado o programa *ASSIST – IBM Operational Assistant*. Caso se utilize a *Attention-Key* para chamar o **ASSIST* o utilizador poderá ter acesso à linha de comando. Este facto poderá possibilitar ao utilizador executar outros programas aos quais, possivelmente, não deveria ter acesso, o que poderá colocar em causa a disponibilidade e confidencialidade do sistema *OS/400* do CDSSS – Setúbal.

○ Implementação de *Limited Capability* – Sistema *OS/400*

O parâmetro de segurança *QATNPGM* tem o valor **ASSIST*, tendo sido observado, em diversos perfis de utilizadores, que o parâmetro *Limited Capability* tinha o valor de **NO*. Existe o risco dos utilizadores em causa executarem determinados tipos de comandos *CL* na linha de comando ou de poderem modificar os seguintes parâmetros do seu *user profile*:

- *Initial Program*
- *Initial Menu*
- *Current Library*
- *Attention Program*.

Deste modo, os utilizadores têm a possibilidade de contornar o esquema de segurança implementado e ter acesso a programas e informação que, de outra forma, estaria vedado. O risco torna-se ainda mais alto se existirem bibliotecas de produção que não estejam especificamente protegidas.

○ Autorização de Acesso a Bibliotecas – Sistema *OS/400*

As bibliotecas *EFXLIB* e *EXXLIB* (contendo parametrizações e tabelas) têm autorizações públicas de **CHANGE*. Existe o risco de um utilizador, inadvertida ou deliberadamente, colocar em causa a disponibilidade, confidencialidade e integridade da informação residente nas bibliotecas em questão, uma vez que lhes é permitido alterar, adicionar ou eliminar informação constantes das mesmas.

○ Mecanismos de Auditoria – Sistema *OS/400*

O parâmetro *QAUDCTL* tem o valor de **NONE*. Este parâmetro determina se alguma acção de auditoria é realizada no sistema *OS/400*. Desta forma, verificou-se a inexistência de práticas de monitorização e de auditoria sobre as actividades desenvolvidas no sistema *OS/400* em análise. Este parâmetro funciona, ainda, como o método de activação ou de desactivação do parâmetro *QAUDLVL*. A falta de mecanismos de monitorização e de auditoria no sistema *OS/400*, origina que todas as acções aqui praticadas por utilizadores com privilégios elevados e utilizadores com privilégios normais não sejam analisadas, implicando o risco de que acessos não autorizados ou irregulares ocorram sem serem detectados e investigados.

○ *Audit Journal* – Sistema *OS/400*

O parâmetro *QAUDLVL* tem o valor de **NONE*. Este parâmetro determina o tipo de ocorrências registadas no *Audit Journal*, relacionadas com segurança e outros eventos do sistema *OS/400*. Com o valor de **NONE* configurado, o *Audit Journal* está inactivo, o que leva a que nenhum relatório de auditoria sobre a segurança do sistema *OS/400* seja produzido no CDSSS – Setúbal. A monitorização das actividades dos sistemas é a única via de garantia da aplicação das medidas de segurança implementadas nos sistemas de informação, ao mesmo tempo que possibilita que se



reja, oportunamente, contra tentativas de quebras de segurança nesses sistemas. Sem um mecanismo eficiente e completo de auditoria, existe o risco de que actividades suspeitas, ocorridas no sistema *OS/400*, não sejam detectadas num curto espaço de tempo, podendo pôr em causa a sua integridade e disponibilidade. Sem a monitorização de *logs* de segurança do sistema *OS/400* é, ainda, impossível atribuir responsabilidades por alterações indevidas a objectos ou programas.

- **Servidores de Autenticação – Sistema *Windows NT***

O servidor *STBSERAUT* tem instalado o *Internet Information Server* e o *Proxy Server*. Se os servidores de autenticação forem utilizados para outros fins, pode existir o risco de não existirem recursos disponíveis suficientes para todas as tarefas. Para além disso, quanto mais serviços o servidor tiver, mais vulnerável está a ataques, devido ao maior número de portas abertas e serviços de comunicação activos.

- **Ligações Anónimas – Sistema *Windows NT***

No sistema em análise não existe o parâmetro de *registry*, *RestrictAnonymous*. Devido ao facto dos servidores *Windows NT 4.0* permitirem, por omissão, o estabelecimento de ligações anónimas ao *share IPC\$ (null sessions)*, torna-se possível obter informação relevante, como a lista total de utilizadores do domínio SETUBAL e os *shares* existentes naquele servidor, que poderá ser útil para se proceder a ataques de intrusão aos sistemas *Windows NT* do CDSSS de Setúbal.

- **Serviços Activos – Sistema *Windows NT***

Existem serviços relativos ao sistema operativo *Windows NT*, activos nos sistemas em análise, que não se consideram os mais indicados para o seu funcionamento, nomeadamente os serviços *Messenger* e *Alerter*. Verificou-se, ainda, que estes sistemas estão visíveis para qualquer utilizador que faça *browsing* à rede. Quanto mais serviços estão instalados num servidor, maior é o número de vulnerabilidades que podem ser exploradas, pondo em causa a integridade e disponibilidade dos mesmos. Desta forma, os serviços *Messenger* e *Alerter* poderão revelar informação atractiva sobre o sistema operativo *Windows NT* a utilizadores não autorizados. A existência do serviço de *browsing*, aumenta o risco de um utilizador não autorizado ficar a conhecer todos os sistemas *Windows NT* anunciados na rede.

- **Assinatura de pacotes *SMB* – Sistema *Windows NT***

Nos sistemas em análise, não é feita a assinatura de pacotes *SMB – Server Message Block*, sendo que a utilização desta assinatura reduz o risco da conquista hostil de uma ligação em curso.



- **Remoção do Pagefile – Sistema Windows NT**

Nos sistemas em análise, o *pagefile* não é apagado após o *shutdown* do sistema. A credencial de autenticação *password* pode aparecer em texto legível dentro do *pagefile*, podendo ser utilizada, colocando em causa a segurança dos sistemas *Windows NT*.

- **Subsistemas OS/2 e Posix – Sistema Windows NT**

Observou-se, nos sistemas em análise, que os subsistemas *OS/2* e *Posix* não foram removidos. Estes subsistemas não são necessários para o funcionamento normal do *Windows NT* e o facto de estarem activos reduz o nível de segurança dos sistemas, existindo o risco de serem utilizadas vias de processamento alternativo que podem comprometer a segurança do sistema operativo *Windows NT*.

- **Redundância de Discos – Sistema Windows NT**

Verificou-se que nenhum dos sistemas *Windows NT* analisados possuía um sistema de redundância de discos – *Fault Tolerant*. A inexistência de um sistema de redundância de discos aumenta o risco de, no caso de algum dos discos ficar danificado, se perder, de forma irreversível, informação crítica residente nos servidores *Windows NT*, podendo mesmo pôr em causa a disponibilidade destes sistemas.

- **Qualidade das Passwords – Sistema Windows NT**

Não está implementado nenhum mecanismo que aumente a qualidade das *passwords* dos utilizadores. A qualidade da segurança de qualquer sistema, incluindo domínios *Windows NT*, está directamente relacionada com a qualidade das *passwords* dos seus utilizadores, sendo estas, na maioria dos sistemas do CDSSS – Setúbal, imprescindíveis para a autenticação dos seus utilizadores.

A maioria dos utilizadores do CDSSS – Setúbal utiliza a plataforma *Windows NT* para processar parte da sua informação. Considera-se, assim, que a qualidade das *passwords* observada coloca em causa a confidencialidade da informação existente naquela plataforma.

- **Account Policies – Sistema Windows NT**

Na análise às políticas de segurança do domínio SETUBAL, verificou-se a existência de alterações nas *Account Policies* dos *Domain Controllers* daquele domínio. Contudo, considera-se que a *parametrização* escolhida poderá ser otimizada em determinados parâmetros. A definição inadequada de *Account Policies* aumenta o risco de ocorrência de acessos não autorizados aos recursos de um domínio *Windows NT*. As políticas estabelecidas poderão deixar o CDSSS – Setúbal vulnerável a quebras de segurança nos seus sistemas *Windows NT*, podendo a implementação de procedimentos regulares de mudança de *passwords*, associada à sua composição mais complexa, contribuir para minimizar este risco.



- **Implementação do SysKey – Sistema Windows NT**

Não existe o parâmetro *Secureboot* no *registry*, pelo que o *SysKey* não está activo nestes sistemas. A utilização do esquema de *encriptação* que vem, por omissão, com o *Windows NT* é fraca (40 bits), pelo que é possível obter as *passwords encriptadas* e descodificá-las facilmente.

- **Implementação do Passprop – Sistema Windows NT**

A funcionalidade *Passprop*, que pode ser obtida no *Resource Kit* do *Windows NT 4.0*, não está a ser utilizada. Por omissão, o *Windows NT* não bloqueia a conta de administrador, mesmo após se ter excedido o número máximo possível de tentativas para obter autenticação neste sistema. A funcionalidade *Passprop* permite bloquear a conta de administrador, caso se ultrapasse o número de tentativas mal sucedidas de autenticação remotas, definidas nas *Account Policies* do domínio *NT*; contudo, a conta de administrador poderá ser sempre utilizada para se proceder a autenticação local, no próprio sistema *NT*.

- **Perfis de Administração – Sistema Windows NT**

Na análise aos utilizadores do domínio SETUBAL, verificou-se a existência de 2 perfis de utilizadores com privilégios de administração sobre aquele domínio que se encontram inactivos: o *stboperacao* e o *stbpedrorodrigues*. A manutenção de utilizadores que estejam inactivos poderá provocar a ocorrência de tentativas de acesso, não autorizadas, aos recursos dos sistemas *Windows NT*, através da utilização indevida por parte destes utilizadores, com a agravante de serem eles os administradores do domínio.

- **Home Directories – Sistema Windows NT**

Não são utilizadas *home directories* para as contas dos utilizadores no domínio SETUBAL. Quando o administrador de sistemas *NT* controla quais os directórios que fazem parte das *home directories* dos vários utilizadores, torna-se mais fácil proceder a *backups* ou eliminar, especificamente, alguns ficheiros. Constitui, também, uma boa política dar a cada utilizador um directório próprio, se possível, numa área partilhada de rede.

- **Mensagem de Aviso – Sistema Windows NT**

Os servidores em análise não fazem aparecer um aviso legal, antes do utilizador se autenticar nos respectivos servidores, tornando-se, assim, mais difícil exigir responsabilidades por utilização imprópria dos recursos de rede disponibilizados pelo CDSSS de Setúbal.

- **Divulgação do Último Utilizador – Sistema Windows NT**

O nome do último utilizador a autenticar-se localmente no sistema é sempre visível durante o processo de autenticação. Existe o risco de um utilizador não autorizado obter conhecimento de nomes de outros utilizadores do domínio ou identificar os *standards* utilizados para a sua criação nos sistemas *Windows NT* do domínio SETUBAL.

- **Monitorização de Logs – Sistema Windows NT**



Tribunal de Contas

Não existem procedimentos formais e regulares de análise e revisão de *logs*. A não observação regular dos *logs* dos sistemas Windows NT pode gerar que situações de tentativas de acesso, bem sucedidas ou falhadas, não sejam detectadas num curto espaço de tempo por parte do CDSSS – Setúbal.

- **Audit Policies – Sistema Windows NT**

As Audit Policies têm alguns parâmetros activos, considerando-se, no entanto, ainda não optimizados. Uma *Audit Policy* bem definida reúne detalhe suficiente para permitir uma revisão adequada dos eventos ocorridos no domínio NT, sendo a sua adequada definição fundamental para a recolha de eventos críticos ou anormais. Sem a recolha destes eventos é impossível determinar tentativas de violação do sistema, não existindo, por outro lado, evidência para o estabelecimento de possíveis sanções aos utilizadores que executem actividades não autorizadas.

A avaliação da segurança dos sistemas mais críticos do CNP, nomeadamente o sistema *UNISYS Clear Path*, apresenta um nível de segurança razoável, visto tratar-se de um sistema *proprietário* invulgar, que requer *software* de rede específico para que um utilizador lhe possa aceder. Mesmo assim, considerando as suas particulares especificidades, um utilizador com acesso a um cliente de rede com este *software* instalado poderá executar certas transacções de consulta.

3.3.6.3 Riscos Significativos Identificados e Seus Impactes

Neste contexto, cada uma das entidades componentes do SSSS está exposta a vários riscos de segurança lógica, nomeadamente aos seguintes:

- as ameaças à segurança e as vulnerabilidades inerentes aos sistemas podem não ser identificadas e superadas de forma atempada;
- as configurações actuais dos sistemas não apresentam níveis de segurança adequados para assegurar a integridade da informação; e
- a integridade dos dados ou as transacções efectuadas podem não ser adequadas se a autenticidade do utilizador dos sistemas de informação não for garantida.

3.3.6.4 Avaliação Global – Princiante

- Os responsáveis pelas entidades que integram o SSSS reconhecem a necessidade da existência de segurança ao nível dos sistemas de informação, mas a consciência de segurança varia entre os utilizadores;
- As iniciativas da segurança dos sistemas de informação são reactivas;
- As responsabilidades de monitorização não estão claramente definidas e os recursos internos são insuficientes para garantir acções de monitorização continuada;



Tribunal de Contas

- Dada a coexistência de diversas plataformas, não é possível obter uma especialização de conhecimento em todas as áreas, tornando-se, por este motivo, bastante difícil ter um controlo efectivo sobre todos os aspectos de segurança sobre a informação destas entidades;
- São utilizadas poucas ferramentas ou funcionalidades para a monitorização de eventos de segurança nos vários sistemas.

3.3.7. IDENTIFICAÇÃO E AFECTAÇÃO DOS CUSTOS

3.3.7.1 Descrição da Actividade

Esta actividade pretende assegurar uma afectação correcta de custos dos serviços de TI providenciados às diversas Unidades de cada uma das entidades do SSSS, assegurando, igualmente, a existência de uma correcta apreciação e entendimento dos custos associados à prestação de serviços de TI, de modo a permitir uma adequada definição das prioridades dos serviços solicitados. Este processo contempla, genericamente:

- a identificação e medição dos recursos despendidos (por ex. horas/homem afectas a cada projecto);
- a aplicação das políticas e procedimentos de débito das taxas de serviço; e
- a definição e acordo sobre taxas de serviço entre as Unidades de SI e as outras Unidades de cada entidade que integra o SSSS.

Os factores que contribuem para o sucesso desta actividade incluem, designadamente:

- a partilha do entendimento acerca dos requisitos de alocação de custos pelos utilizadores responsáveis das várias Unidades operacionais de cada entidade;
- a identificação, análise e comunicação, de forma automática e atempada, dos custos directos e indirectos relativos aos serviços prestados;
- a cobrança de custos efectuada tendo por base a utilização, o nível de serviços e os princípios de atribuição de custos geralmente aceites;
- a partilha de informação sobre custos, para analisar a *performance* orçamental e identificar oportunidades de optimização de custos;
- a existência de uma relação directa entre o custo do serviço e o nível de serviço acordado; e
- a utilização dos resultados de alocação de custos e da optimização para verificar e medir o valor da contribuição das Unidades de SI para cada uma das entidades.



3.3.7.2 Situação Actual

Nenhuma das entidades visitadas procedeu à definição de níveis de serviço, não sendo, por essa razão, considerado como prioridade o estabelecimento de taxas de débito para imputação do custo de serviço às outras Unidades operacionais. As Unidades de SI são consideradas como centros de custos.

Segundo alega o IIES, “... o processo de afectação total de custos aos projectos encontra-se em fase de análise de requisitos, seguindo-se-lhe, imediatamente, a fase de implementação, estando já seleccionada uma ferramenta para suporte ao processo”.

3.3.7.3 Riscos Significativos Identificados e Seus Impactes

Sem um claro entendimento dos custos associados à prestação de serviços de TI e a sua atribuição às actividades de cada uma das entidades do SSSS, é difícil assegurar a afectação de recursos limitados às necessidades prioritárias. A afectação de custos aos serviços prestados assegura que os clientes internos validam a sua qualidade e contemplam a sua prioridade.

3.3.7.4 Avaliação Global – Não existente

- Não existe qualquer processo implementado para identificar e afectar custos respeitantes aos serviços de sistemas de informação providenciados pelas Unidades de Sistemas de Informação;
- Nenhuma das entidades auditadas reconhece, por enquanto, a necessidade de espelhar esta situação e não pretende desenvolver qualquer iniciativa a esse respeito.

3.3.8. PRESTAÇÃO DE APOIO E FORMAÇÃO AOS UTILIZADORES

3.3.8.1 Descrição da Actividade

Esta actividade visa a prestação de apoio e formação adequada e atempada aos utilizadores para responder às necessidades das entidades e assegurar a utilização correcta dos recursos de sistemas e tecnologias de informação, considerando, nomeadamente:

- a identificação e a definição das necessidades de formação dos utilizadores de cada entidade;
- o desenvolvimento de acções de formação;



Tribunal de Contas

- a formação de utilizadores nas várias fases do processo de implementação de sistemas de informação;
- a monitorização e resolução de problemas, com o objectivo de identificar necessidades de formação;
- a definição de acções de formação dos utilizadores sobre a utilização dos sistemas de informação existentes em cada entidade do SSSS; e
- a criação e actualização de documentação sobre aplicações e sistemas.

Os factores que contribuem para o êxito desta actividade, resumem-se, genericamente, como segue:

- a existência de um programa de formação centrado nas necessidades individuais e da própria entidade;
- as iniciativas de formação estarem adequadamente suportadas com orçamentos, recursos, instalações e formadores;
- a formação ser definida como uma das componentes fundamentais para o desenvolvimento da carreira dos colaboradores;
- os responsáveis pelas várias Unidades e os seus colaboradores identificarem e documentarem as necessidades de formação;
- a formação necessária ser dada atempadamente;
- os funcionários receberem formação em práticas de segurança dos seus sistemas para assegurar a disponibilidade, a confidencialidade e a integridade dos mesmos;
- as políticas de cada entidade requererem que todos os colaboradores tenham conhecimento das práticas de segurança dos sistemas e da utilização permitida dos recursos de tecnologias de informação; e
- existir a aceitação, por parte da Direcção, de que os custos de formação permitem baixar o total de custos relativos à utilização de tecnologias, melhorando a produtividade da Organização.

3.3.8.2 Situação Actual

O processo de formação de utilizadores não está estruturado e padronizado. Quando é identificada a necessidade, o responsável de cada Unidade propõe que o utilizador frequente uma acção de formação específica. Quando se verifica a introdução de novas soluções aplicacionais, quem, normalmente, fica responsável pela componente de formação e produção de documentação de apoio é o fornecedor contratado, o que limita a contemplação de necessidades específicas de cada entidade do SSSS nas acções de formação. Cada Unidade de SI responde a todas as solicitações de apoio por parte dos utilizadores sem estabelecer prioridades para os pedidos, sendo, ainda assim, prestado um nível de apoio razoável, considerando os recursos disponíveis para esta actividade. A relativa estabilidade dos sistemas tem minimizado o número de solicitações nesta área.



3.3.8.3 Riscos Significativos Identificados e Seus Impactes

Neste contexto, os riscos associados a este processo poderão resumir-se como segue:

- as expectativas de formação dos utilizadores poderem não ser atingidas, conduzindo à desmotivação e à incorrecta utilização dos sistemas implementados;
- a familiaridade dos utilizadores com os sistemas poder ser inadequada, conduzindo a ineficiências ou a utilizações pouco eficazes dos sistemas de informação;
- a falta de uma ferramenta de gestão do *Help Desk* não permitir a tipificação dos problemas que, possivelmente, deveriam ser colmatados com formação adequada.

3.3.8.4 Avaliação Global – Princiante

- Existe evidência de que os responsáveis pelas entidades integrantes do SSSS reconhecem a necessidade de promover uma formação adequada dos seus utilizadores, mas não existem processos padronizados nesse sentido;
- Na falta de um processo de formação estruturado, os colaboradores identificam as suas necessidades de formação;
- As entidades em questão carecem, igualmente, de mecanismos adequados que lhes permitam identificar as necessidades em termos de formação.

3.3.9. APOIAR E ACONSELHAR OS UTILIZADORES

3.3.9.1 Descrição da Actividade

Esta actividade pretende assegurar que os problemas relacionados com a utilização dos SI são resolvidos de forma atempada e eficaz, sendo, para tal, necessária a existência de uma função de *Help Desk* que ofereça uma primeira linha de apoio.

Contribuem para o êxito desta actividade os seguintes factores:

- a utilização e disponibilização de FAQ – *Frequently Asked Questions* – com as suas respostas disponíveis;
- todos os problemas e solicitações dos utilizadores serem registados pelo *Help Desk*.
- os problemas que não podem ser resolvidos atempadamente serem escalados por prioridade;



Tribunal de Contas

- existir monitorização de problemas para garantir que os tempos de resposta são razoáveis face às expectativas dos utilizadores;
- serem identificadas tendências que permitam agir de uma forma pró activa face aos problemas que forem surgindo;
- existir políticas e iniciativas em cada uma das entidades do SSSS que permitam formar os utilizadores nas melhores práticas de utilização das tecnologias de informação; e
- os custos de apoio e suporte aos utilizadores serem imputados às várias Unidades, utilizando ferramentas e políticas simples e claras.

3.3.9.2 Situação Actual

Na medida em que esta actividade depende de uma função de *Help Desk* formalizada, observou-se que as actividades de apoio aos utilizadores estão pouco estruturadas. O IIES é a entidade responsável pela gestão dos serviços de apoio aos utilizadores.

O IIES tem um serviço de *Help Desk*, vocacionado para apoiar aplicações que vai disponibilizando. Pretende-se que este serviço de *Help Desk* venha ser alargado a todos os sistemas do SSSS.

3.3.9.3 Riscos Significativos Identificados e Seus Impactes

Neste contexto, os riscos associados a este processo poder-se-ão resumir como se segue:

- os problemas dos utilizadores e os incidentes poderão não ser resolvidos de forma atempada, resultando em insatisfação com os sistemas e, conseqüentemente, no subaproveitamento dos mesmos;
- a repetição de incidentes pode não ser monitorizada de forma a determinar a existência de padrões de comportamento do utilizador, necessidades de formação ou funcionalidades inadequadas;
- a continuidade da baixa *performance* pode conduzir a aumentos de custos e a perdas de produtividade significativas; e
- os utilizadores poderão recorrer ao desenvolvimento interno de aplicações para dar resposta às suas necessidades.

3.3.9.4 Avaliação Global – Princiante

- Os responsáveis por qualquer das entidades que são parte integrante do SSSS reconhecem que é necessário estabelecer um processo de apoio aos utilizadores,



Tribunal de Contas

suportado por ferramentas de gestão e, possivelmente, por colaboradores adicionais para permitir dar resposta às necessidades dos utilizadores e gerir a resolução de problemas;

- Não existe um processo padronizado e o apoio providenciado é reactivo;
- As Unidades de SI efectuam uma monitorização informal dos problemas indicados pelos utilizadores, mas não identificam tendências concretas;
- Não existe qualquer análise do processo de resolução dos problemas.

3.3.10. GESTÃO DAS CONFIGURAÇÕES

3.3.10.1 Descrição da Actividade

Esta actividade pretende identificar e controlar todos os componentes de TI, sejam eles *hardware*, *software* ou componentes de rede e telecomunicações, impedindo que lhes sejam efectuadas alterações não autorizadas, verificando e monitorizando a sua existência física e criando mecanismos efectivos de gestão de alterações. Este processo, normalmente, contempla:

- a criação de um registo de bens com a sua respectiva localização;
- a gestão de mudanças da configuração de sistemas e a verificação periódica da sua existência;
- a detecção de utilização de *software* não autorizado; e
- a existência de controlos de armazenamento de *software*.

Para o bom funcionamento desta actividade concorrem os seguintes factores:

- estarem definidos os responsáveis pela gestão de configurações e pela manutenção do inventário de sistemas e tecnologias de informação;
- a informação de configurações estar acessível e actualizada;
- existir um ambiente de sistemas de informação estruturado que satisfaça as necessidades de segregação de funções entre os ambientes de desenvolvimento, de teste e produção;
- as configurações propostas pelo fornecedor estarem alinhadas com as configurações presentes na entidade;
- existirem definições de uma configuração base que identifique e padronize os componentes mínimos;
- existirem mecanismos automáticos que permitam detectar a configuração actual;
- existir um processo automático de distribuição e implementação de actualizações ou novas configurações; e
- estarem definidas e observadas as regras específicas que salvaguardem a utilização de *software* não licenciado.



Tribunal de Contas

3.3.10.2 Situação Actual

A configuração presente nos computadores pessoais dos colaboradores do SSSS apresenta um nível de padronização bastante acentuado, não existindo, no entanto, *standards* formais quanto a essas configurações. Dada a inexistência de políticas e procedimentos de sistemas formalmente definidas para esta matéria, subsiste um vazio de regras quanto à utilização de *software* não licenciado; por outro lado, tendo sido concedido aos utilizadores acesso à Internet, a obtenção e instalação do referido *software* tornou-se uma tarefa mais facilitada. Este risco está a ser colmatado com a implementação de *User Policies* nos clientes de rede com *Windows NT*, que permite definir e assegurar uma configuração *standard* dos mesmos. Com excepção do CNP, em nenhuma das restantes entidades estão a ser utilizadas ferramentas para efectuar a monitorização e manutenção do *software* instalado nos clientes de rede locais.

Relativamente a este ponto, o IIES informa:

“O IIES, na prossecução da sua missão, definiu um standard para a configuração de computadores pessoais, aplicado a todas as estações de trabalho da rede da SS, documentado na intranet, tendo vindo a dotar os diversos serviços com equipamentos conformes, denominados de “estação padrão”. Esta configuração está devidamente protegida, não permitindo a instalação de software, por parte de utilizadores não autorizados.”

3.3.10.3 Riscos Significativos Identificados e Seus Impactes

Neste contexto os riscos previsíveis associados a este processo podem ser resumidos como se segue:

- poder ser instalado *software* não licenciado nos computadores pessoais dos colaboradores, o que poderá criar prejuízos para as entidades do SSSS;
- passar a existir configurações múltiplas a correr ao mesmo tempo, dificultando o processo de manutenção e apoio;
- a falta de ferramentas para administrar a instalação remota de *upgrades* aos sistemas tornar bastante ineficientes as actualizações das configurações de sistemas; e
- o *software* poder ser copiado ou instalado nos clientes da rede, criando problemas adicionais para a sua manutenção.

3.3.10.4 Avaliação Global – Princiante

- Os responsáveis pelas entidades auditadas reconhecem a necessidade da existência de um processo estruturado para gerir as configurações do sistema;



Tribunal de Contas

- As tarefas básicas de configuração, assim como a de manutenção de *software* e *hardware*, estão a ser asseguradas por cada Unidade de Sistemas de Informação de forma isolada;
- Não são aplicadas quaisquer práticas padronizadas.

3.3.11. RESOLUÇÃO E GESTÃO DE PROBLEMAS DE TI

3.3.11.1 Descrição da Actividade

Este processo assegura que os problemas e interrupções de sistemas são resolvidos com o mínimo de interrupções para a actividade de cada entidade que integra o SSSS e que as suas causas são identificadas para prevenir a sua ocorrência, observando, genericamente, os seguintes requisitos:

- a definição de procedimentos e responsabilidades para a resolução atempada de problemas de TI (ex.: responsabilidades de intervenção no caso de ocorrerem problemas);
- a análise e registo das intervenções nos sistemas de informação; e
- a avaliação da eficiência da resposta dada às interrupções ocorridas.

Os factores que determinam o êxito desta actividade resumem-se como segue:

- existência de uma integração efectiva da gestão de intervenções sobre os sistemas com a gestão da disponibilidade e das mudanças dos mesmos;
- a configuração do sistema estar acessível e ser possível manter o rasto dos problemas para cada componente crítico dos sistemas de informação;
- ser feita uma análise *a posteriori* da forma como os problemas foram resolvidos;
- existirem procedimentos que registem as interrupções de sistemas, os seus sintomas, o diagnóstico efectuado e que assegurem a disponibilidade dos elementos de suporte necessários;
- os elementos das Unidades de Sistemas de Informação disporem de formação adequada à resolução de problemas; e
- existirem procedimentos que assegurem a participação na investigação e resolução de problemas e nas interrupções de sistemas.

3.3.11.2 Situação Actual

A gestão dos problemas que vão surgindo é informal. Não tem sido possível realizar análises cuidadas dos incidentes que surgem, para poder identificar se estes são reincidentes e poder, assim, apontar soluções similares. As prioridades na resolução de problemas são atribuídas, informalmente, no acto do pedido.



Tribunal de Contas

3.3.11.3 Riscos Significativos Identificados e Seus Impactes

Neste contexto, os riscos associados a este processo poderão resumir-se como segue:

- dado que as Unidades de Sistemas de Informação não efectuam qualquer registo das solicitações a que respondem, torna-se, do ponto de vista de gestão, difícil analisar os tipos de problemas que ocorrem com mais frequência, para lhes identificar as tendências e promover soluções uniformes para a resolução de problemas similares;
- adicionalmente, torna-se mais difícil acompanhar o *status* da resolução dos problemas surgidos;
- sem uma ferramenta de gestão, o processo de priorização é informal, pelo que poder-se-á não estar a ser eficiente nem a responder aos problemas mais críticos; e
- o desenvolvimento de planos de formação dos elementos das Unidades de Sistemas de Informação poder não ser adequado, dado que não existe uma análise qualitativa dos problemas que surgem mais frequentemente.

3.3.11.4 Avaliação Global – Princiante

- Os responsáveis pelas entidades auditadas reconhecem que existe a necessidade de gerir a resolução de problemas e avaliar os incidentes;
- Cada elemento das Unidades de Sistemas de Informação providencia assistência perante os problemas, de acordo com a sua área de responsabilidade e com as suas valências técnicas;
- A informação, por vezes, não é partilhada e as soluções adoptadas variam conforme o CDSSS;
- Nestas circunstâncias, os problemas acumulam-se e a produtividade é afectada enquanto se procuram soluções.

3.3.12. GESTÃO DOS DADOS

3.3.12.1 Descrição da Actividade

Assegurar que os dados estão completos, correctos e válidos durante a sua entrada, actualização e armazenamento, através de uma construção efectiva de controlos aplicativos nos processos operacionais e gerais sobre os processos de TI. Este processo contempla, normalmente:

- o desenho de formulários e regras de bases de dados que validem a informação lançada no sistema;
- a implementação de controlos nos documentos fonte;
- a implementação de controlos de processamento;



Tribunal de Contas

- a implementação de controlos de *output*;
- a identificação da informação em *backups* e o registo das movimentações das mesmas;
- a gestão dos procedimentos de *backup* que permitam uma recuperação dos SI; e
- a existência de controlos de acesso que validem a autenticidade das transacções e dados introduzidos.

Os factores que contribuem para o sucesso desta actividade podem resumir-se, genericamente, como segue:

- os parâmetros que regem a entrada de informação no sistema estarem claramente definidos e suportados por mecanismos automatizados em vários níveis, incluindo na base de dados e nos ficheiros;
- as responsabilidades pela integridade e guarda da informação estarem definidas e aceites em cada entidade;
- a verificação da qualidade da informação ser efectuada no acto do seu lançamento no sistema;
- a informação incorrecta ficar em suspenso pelos sistemas até ser corrigida;
- serem utilizados métodos de detecção eficazes para assegurar a precisão da informação e *standards* de integridade;
- a transição e a tradução da informação entre as diferentes plataformas, ser feita de forma segura, sem perda de integridade dos dados;
- existir uma dependência decrescente relativamente aos dados introduzidos ou reintroduzidos manualmente; e
- a informação ser arquivada e protegida e estar disponível no caso de ser necessário a sua reposição.

3.3.12.2 Situação Actual

Os sistemas de cada uma das entidades do SSSS foram implementados em momentos diferentes. As plataformas que suportam cada um dos sistemas de informação são distintas, o que levou à concepção de diferentes aplicações para servir o mesmo objectivo. Nos vários CDSSS, por exemplo, existe uma panóplia de aplicações que poderiam ter sido padronizadas. O modelo de dados subjacente a cada uma delas é distinto e não está claramente definido. Actualmente, o IIES está a definir um modelo de dados central que suportará as novas aplicações do SSSS, sendo que as regras definidas para assegurar a sua coerência ainda não se encontram concluídas.

As aplicações existentes foram desenvolvidas sem se observar a implementação de alguns controlos de introdução e alteração de dados, o que poderá resultar em problemas para a integridade e qualidade da informação processada, tendo sido necessário desenvolver, complementarmente, algumas rotinas que possibilitassem a identificação, durante o processamento, da informação de “má qualidade” introduzida nos sistemas.



Tribunal de Contas

Não se estabeleceram formalmente regras de classificação e arquivo de dados, existindo, no entanto, alguns procedimentos instituídos para o seu armazenamento. As cópias de segurança efectuadas, devidamente identificadas e catalogadas, são, contudo, com excepção do CNP, guardadas nas próprias instalações de cada serviço, podendo, em caso de acidente, colocar em risco a sua integridade.

As entidades visadas não têm capacidade para gerir informação não estruturada, sendo esta gestão efectuada com recurso ao suporte de papel, o que dificulta as suas consulta e análise.

3.3.12.3 Riscos Significativos Identificados e Seus Impactes

Neste contexto, os riscos associados a esta actividade podem resumir-se como segue:

- visto que não existe um modelo de dados claramente definido, pode tornar-se difícil estabelecer novos desenvolvimentos das aplicações como forma de dar suporte às necessidades de informação da entidade em questão. Adicionalmente, o grau de dependência relativamente aos colaboradores responsáveis pelo desenvolvimento e manutenção de aplicações é bastante acentuado.
- as aplicações não incluem todos os controlos de *input* necessários, o que poderá pôr em causa a qualidade dos dados do sistema; por outro lado, a necessidade de implementar rotinas adicionais para detectar esse tipo de erros diminui a eficiência do processamento.
- os dados contidos nas cópias de segurança podem ficar comprometidos, caso ocorra um desastre nas instalações onde são guardadas, visto serem as mesmas onde estão os sistemas de informação em produção;
- a não capacidade para gerir a informação não estruturada pode reduzir a eficiência dos serviços e a celeridade da localização dessa informação.

3.3.12.4 Avaliação Global – Princípante

- Os responsáveis pelas entidades auditadas reconhecem a necessidade da informação ser precisa e correcta;
- Já existem algumas iniciativas individuais para prevenir ou detectar erros de introdução, processamento e divulgação;
- Contudo, o processo de identificação e correcção deste tipo de problemas depende da iniciativa e intervenção individual de cada um dos CDSSS.



Tribunal de Contas

3.3.13. GESTÃO DAS INSTALAÇÕES FÍSICAS

3.3.13.1 Descrição da Actividade

Esta actividade pretende providenciar um ambiente físico apropriado que proteja, quer o equipamento de TI, quer as pessoas que com ele trabalham, de acidentes com origem em causas naturais ou por intervenção humana. Esta segurança física é assegurada através da instalação de um ambiente físico adequado, com controlos que são, periodicamente, revistos para assegurar o seu efectivo funcionamento. Esta actividade contempla, ainda, o estabelecimento de um nível mínimo de protecção em relação a ameaças ambientais, como fogo, humidade, calor e radiações electromagnéticas excessivas. Os factores que contribuem para o seu sucesso podem resumir-se como segue:

- estarem definidas estratégias e *standards* que abranjam todas as instalações, cobrindo a segurança do pessoal, selecção de locais, sistemas eléctricos e mecânicos e mecanismos de protecção contra situações de fogo, descargas eléctricas ou inundações;
- as políticas e *standards* aplicáveis às instalações estarem alinhados com os requisitos de disponibilidade dos sistemas de informação e políticas de segurança da informação e integradas com planos de continuidade do “negócio” e gestão de situações de crise;
- as instalações são monitorizadas, recorrendo a sistemas automatizados que produzam históricos, circuitos fechados de televisão, sistemas de detecção de entradas ou serem realizadas inspecções físicas e auditorias;
- existir uma aderência rigorosa aos princípios de manutenção preventivos e rigor na gestão das instalações;
- o acesso físico ser rigorosamente monitorizado e limitado por zonas, sendo obrigatório o uso de identificação e, quando necessário, adoptados procedimentos de excepção;
- existir uma boa relação e troca de informação com os agentes da lei, bombeiros e outras autoridades locais; e
- existirem procedimentos de inspecção e detecção de problemas actualizados, suportados por formação adequada.

3.3.13.2 Situação Actual

Ainda que existam vários mecanismos para assegurar a segurança física dos sistemas, verificou-se que as salas onde se encontram os sistemas de informação críticos carecem de algumas condições ambientais, designadamente:

- Em todas as entidades auditadas as portas das salas de processamento não oferecem a protecção necessária para fazer face a um incêndio e evitar a propagação rápida das chamas;
- Nos CDSSS – Lisboa e Setúbal não estão instalados sistemas automáticos de extinção de incêndio.



Tribunal de Contas

As instalações das Unidades de Informática estão localizadas em áreas segregadas, o que permite limitar, mais facilmente, o acesso a essas mesmas instalações, observando-se, inclusivamente, a presença de segurança permanente nessas instalações.

Verificou-se, por outro lado, que nenhuma das entidades auditadas tinha formalizado um *Disaster Recovery Plan* para os seus sistemas de informação que abrangesse as instalações físicas.

Segundo as alegações produzidas, “o IIES tem em curso um projecto para definição dos requisitos a implementar para efeito de recuperação de desastres”.

3.3.13.3 Riscos Significativos Identificados e Seus Impactes

Assim, os riscos associados a este processo resumem-se como se segue:

- em caso de acidente, as entidades que integram o SSSS podem não dispor de instalações alternativas para recuperar os sistemas de informação;
- em caso de incêndio nas salas de sistemas, cada uma das entidades está dependente de intervenção humana para o extinguir; por outro lado, as instalações actuais podem, nestes casos, não oferecer as condições necessárias para impedir a rápida expansão das chamas.

3.3.13.4 Avaliação Global – Princiante

- Os responsáveis por qualquer uma das entidades auditadas reconhecem a necessidade de ter um ambiente físico que proteja pessoas e sistemas contra desastres naturais e humanos;
- Os procedimentos de gestão das instalações não estão formalmente definidos e cada entidade depende das capacidades e competências dos elementos individuais das Unidades de SI;
- Existem alguns controlos ambientais implementados e monitorizados.



3.3.14. GESTÃO DAS OPERAÇÕES

3.3.14.1 Descrição da Actividade

Esta actividade pretende assegurar que as funções mais importantes de suporte de TI ocorrem regularmente e de uma forma controlada, através do registo das actividades de suporte que são realizadas.

Os factores que contribuem para o êxito desta actividade sintetizam-se como segue:

- as instruções das operações estarem bem definidas, de acordo com os *standards* estabelecidos, com a indicação clara de cada um dos pontos críticos de execução;
- existir um nível elevado de padronização das operações para os diversos sistemas;
- existir uma estreita relação e coordenação com os processos relacionados, incluindo gestão da mudança e resolução de problemas e manutenção da continuidade dos sistemas;
- existir um alto nível de automatização das tarefas operacionais;
- os processos operacionais serem estruturados para trabalhar eficientemente em conjunto com ferramentas automáticas;
- a racionalização e padronização das ferramentas de gestão do sistema serem implementadas;
- o tratamento de *inputs* e *outputs* passar, dentro do possível, a estar à responsabilidade dos utilizadores;
- as mudanças no planeamento do trabalho serem analisadas pormenorizadamente;
- os procedimentos de aceitação de mudanças no planeamento do trabalho serem rigorosos, o que inclui, também, a entrega de documentação justificativa;
- os esquemas de manutenção de prevenção estarem em vigor;
- estarem implementados serviços eficientes de inspecção e detecção de problemas; e
- os contratos de apoio com fornecedores serem adequadamente definidos e cumpridos.

3.3.14.2 Situação Actual

Não existe nas Unidades de Sistemas de Informação um manual de operações que defina claramente todos os procedimentos diários a realizar, verificando-se a sua execução de forma informal, decorrente da experiência de cada funcionário. A monitorização e tarefas de suporte efectuadas sobre os sistemas dependem da verificação, *in loco*, dos sistemas ou da resposta a anomalias identificadas pelos utilizadores. Os procedimentos de *backup* são automatizados de forma a permitir a execução e monitorização dos *backups* efectuados.

O ISSS-CNP, em sede de contraditório, alega:



“Contrariamente ao referido, existe no ISSS-CNP um planeamento diário com as operações a executar.

Dado que o sistema é desligado ao fim de semana, existe ainda um manual de operação com os procedimentos pormenorizados para ligar e desligar o sistema”.

Mantêm-se as observações formuladas para os CDSSS visitados.

3.3.14.3 Riscos Significativos Identificados e Seus Impactes

Resumem-se, seguidamente, os riscos associados a este processo, no contexto atrás descrito:

- visto que a monitorização é realizada de forma limitada, dada a não utilização de ferramentas próprias para o efeito, alguns dos problemas podem não ser detectados e resolvidos atempadamente;
- a não formalização de procedimentos poder implicar a não responsabilização dos elementos das Unidades de SI e a não realização de todas as tarefas determinantes para a manutenção dos Sistemas de Informação.

3.3.14.4 Avaliação Global – Princiante

- Os responsáveis pelas entidades auditadas estão atentos à importância que a gestão de operações tem nas actividades de suporte das tecnologias de informação;
- Existem alguns procedimentos informais estabelecidos, mas as actividades operacionais das Unidades de Sistemas de Informação estão, sobretudo, dependentes do rigor exercido no desempenho destas tarefas;
- A maior parte das operações não estão, formalmente, escalonadas;
- Existe uma grande dependência relativamente às valências de cada um dos colaboradores presentes nas Unidades de Sistemas de Informação.

3.4. MONITORIZAÇÃO DOS PROCESSOS DE TI

3.4.1. DESCRIÇÃO DO PROCESSO

Para assegurar que os processos de Planeamento, Desenvolvimento e Aquisição de Soluções e Operação dos Sistemas de TI estão a funcionar correctamente, é necessário monitorizar o seu desempenho.

Este processo está subdividido, em termos do modelo CobIT, nas seguintes actividades:



Tribunal de Contas

1. Monitorização dos Processos de TI;
2. Avaliação do controlo interno de TI;
3. Certificação de Serviços e Sistemas; e
4. Execução de Auditorias Independentes.

3.4.2. MONITORIZAÇÃO DOS PROCESSOS DE TI

3.4.2.1 Descrição da Actividade

Para assegurar que os processos de Planeamento, Desenvolvimento e Aquisição de Soluções e Operação dos Sistemas de TI estão a funcionar correctamente, são, sobre eles, desenvolvidas actividades de monitorização para verificar se os objectivos de *performance* estipulados estão a ser atingidos. Esta monitorização é efectuada através da definição de indicadores de *performance* relevantes, do reporte sistemático do seu desempenho e da resolução atempada dos desvios identificados, sendo, para que tal aconteça, necessário que se verifiquem os seguintes requisitos:

- a existência de relatórios de desempenho dos processos de TI;
- os processos de TI terem indicadores de desempenho adequadamente definidos;
- as métricas de desempenho de TI assegurarem o seu alinhamento com os objectivos de cada entidade e incluírem critérios operacionais, financeiros, satisfação de clientes internos e desenvolvimento de conhecimentos;
- existir uma base de informação histórica sobre o desempenho dos processos; e
- existirem objectivos, por processo, claramente definidos e comunicados.

Segundo o alegado, *“O IIES não ignora a importância deste processo, apenas não constituiu, até agora, prioridade, face à sua curta existência e às actividades e projectos que, obrigatoriamente, o deveriam preceder.”*

3.4.2.2 Situação Actual

As entidades integrantes do SSSS carecem de mecanismos de monitorização e avaliação da *performance* dos seus processos de TI, havendo, por outro lado, indefinição quanto aos objectivos que se pretendem atingir e quanto às métricas a utilizar para analisar a sua *performance*.



3.4.2.3 Riscos Significativos Identificados e Seus Impactes

Associados a este processo podem ocorrer os seguintes riscos:

- o desempenho dos processos poderá ser ineficiente ou ineficaz;
- a baixa *performance* dos processos poderá não ser, atempadamente, detectada;
- a insatisfação dos clientes (utilizadores) dos Sistemas de Informação relativamente aos níveis de serviço prestado pode não ser, oportunamente, detectada e resolvida; e
- as decisões da Direcção de cada entidade sobre os processos de TI poderão basear-se em informação de gestão inadequada ou inválida.

3.4.2.4 Avaliação Global – Não existente

- Os responsáveis pelas entidades auditadas reconhecem a necessidade de existir recolha e análise da informação sobre a monitorização dos processos de TI, porém, essa monitorização é inexistente;
- Ainda não foi estabelecida como uma prioridade a definição de objectivos para os processos de TI

3.4.3. AVALIAÇÃO DO CONTROLO INTERNO DE TI

3.4.3.1 Descrição da Actividade

Esta actividade pretende assegurar o cumprimento dos objectivos de controlo interno definidos para os processos de TI, através da sua monitorização e avaliação periódica. Os factores determinantes para o sucesso desta actividade resumem-se do seguinte modo:

- uma definição clara dos processos de TI e das suas actividades que deverão ser controladas;
- as responsabilidades pelo controlo interno e auditoria interna estarem claramente definidas;
- existirem competências e recursos suficientes para a monitorização do controlo interno;
- existir uma estrutura que permita o reporte atempado das deficiências de controlo;
- existir um alinhamento entre os riscos identificados e a monitorização do controlo interno dos processos de TI necessária para a sua minimização; e
- existir uma partilha de conhecimentos para ultrapassar ou solucionar questões de controlo interno.



Tribunal de Contas

3.4.3.2 Situação Actual

As entidades não dispõem de uma função que avalie o controlo interno dos processos de TI, nem os objectivos que se pretendem atingir com o mesmo. As avaliações realizadas ocorrem sem carácter regular, sendo conduzidas como parte integrante das intervenções dos auditores financeiros, com metodologias e valências técnicas que não correspondem às necessidades específicas de cada Unidade de Sistemas de Informação.

3.4.3.3 Riscos Significativos Identificados e Seus Impactes

Os riscos associados a este processo resumem-se como segue:

- os controlos internos poder-se-ão revelar inadequados para assegurar a integridade dos processos de TI e esse facto pode permanecer desconhecido;
- os controlos internos poderem não ser eficazes e eficientes, não sendo possível, sem a constatação deste facto, implementar controlos adicionais para mitigar os riscos associados; e
- sem a implementação de mecanismos de avaliação do controlo interno, os erros e excepções não serem comunicados de forma atempada, impossibilitando uma intervenção oportuna.

3.4.3.4 Avaliação Global – Princiante

- A avaliação da adequação do controlo interno de TI depende de iniciativas pontuais;
- Não foram atribuídas formalmente responsabilidades de avaliação do ambiente de controlo interno, porque ainda não estão definidas as bases sobre as quais as avaliações devem ser efectuadas.

3.4.4. CERTIFICAÇÃO DE SERVIÇOS E SISTEMAS

3.4.4.1 Descrição da Actividade

Com esta actividade pretende-se aumentar a confiança nos serviços e sistemas de TI entre as Unidades de Sistemas de Informação e os seus clientes internos, contribuintes, beneficiários, fornecedores e outros prestadores de serviços, através de avaliações independentes e periódicas dos níveis de confiança oferecidos pelos processos de TI.



Tribunal de Contas

Este processo contempla:

- a realização de avaliações independentes dos níveis de eficácia;
- a realização de avaliações independentes dos processos de TI;
- a avaliação independente do cumprimento de compromissos contratuais;
- a análise e *benchmark* de fornecedores de serviços adquiridos;
- a execução destas avaliações por pessoal qualificado; e
- o envolvimento pró activo no processo de auditoria.

3.4.4.2 Situação Actual

Nenhuma das entidades auditadas possui qualquer processo de certificação e avaliação de serviços prestados para a área de sistemas de informação, não estando, neste momento, contemplada qualquer actividade para esse fim.

3.4.4.3 Riscos Significativos Identificados e Seus Impactes

Os riscos associados à ausência deste processo poder-se-ão resumir como segue:

- a identificação de problemas e ineficiências nos processos de TI não ser, atempadamente, efectuada; e
- as entidades externas atribuírem um baixo nível de confiança aos processos de TI das instituições que fazem parte do SSSS.

3.4.4.4 Avaliação Global – Não existente

- As entidades auditadas carecem de uma actividade que avalie e certifique a qualidade dos seus processos de TI;
- É necessário definir várias políticas de segurança e de qualidade de serviços;
- Não se estabeleceram, até ao momento, quaisquer acordos sobre os níveis de serviço esperados, pelo que os processos não são avaliados.



Tribunal de Contas

3.4.5. EXECUÇÃO DE AUDITORIAS INDEPENDENTES

3.4.5.1 Descrição da Actividade

Esta actividade pretende aumentar os níveis de confiança relativamente aos sistemas de informação e beneficiar dos conselhos sobre as melhores práticas a utilizar, através de auditorias efectuadas com uma periodicidade regular. De entre os factores determinantes para o sucesso desta actividade destacam-se:

- a obtenção de credenciais de independência da entidade que efectuará a auditoria;
- o envolvimento pró activo de cada entidade no processo de auditoria;
- a execução das auditorias por pessoal adequadamente qualificado;
- o acompanhamento das observações e recomendações que resultem do processo de auditoria; e
- a avaliação dos impactes das recomendações das auditorias efectuadas em termos de custos, benefícios e riscos assumidos.

3.4.5.2 Situação Actual

Não são realizadas auditorias externas aos processos de TI; o presente trabalho representa a primeira iniciativa neste domínio.

3.4.5.3 Riscos Significativos Identificados e Seus Impactes

A ausência desta actividade pode ter associados os seguintes riscos:

- caso existam fraquezas significativas nos processos de gestão de TI, estas poderão nunca ser identificadas;
- a correcção das eventuais debilidades do sistema pode não ser, atempadamente, efectuada.

3.4.5.4 Avaliação Global – Não existente

- As entidades auditadas não dispõem de uma função de auditoria de sistemas de informação que efectue verificações periódicas independentes.



Índice do Anexo

I.	AVALIAÇÃO DOS PROCESSOS DE ATRIBUIÇÃO E CONTROLO DE PENSÕES	2
I.1.	PROCESSO DE GESTÃO DE REQUERIMENTOS.....	2
I.1.1.	<i>Processo de Gestão de Requerimentos.....</i>	2
I.1.1.1.	Recepção, Organização e Registo do Requerimento.....	3
I.1.1.2.	Identificação do Beneficiário.....	4
I.1.1.3.	Envio e Integração de Informação com o CNP	4
I.1.1.4.	A Conferência e Deferimento de Processos	5
I.1.1.5.	O Cálculo da Pensão	5
I.1.1.6.	Processamento e Pagamento de Pensões	7
II.	AVALIAÇÃO DOS PROCESSOS DE GESTÃO DE TI.....	8
II.1.	PLANEAMENTO E ESTRATÉGIA DE SISTEMAS DE INFORMAÇÃO.....	8
II.1.1.	<i>Definição da Estratégia de TI.....</i>	8
II.1.2.	<i>Definição da Arquitectura de Informação.....</i>	8
II.1.3.	<i>Definição da Direcção Tecnológica de TI</i>	9
II.1.4.	<i>Definição da Organização de TI e suas Interdependências.....</i>	9
II.1.5.	<i>Gestão dos Investimentos de TI.....</i>	9
II.1.6.	<i>Comunicação das Orientações Estratégicas.....</i>	9
II.1.7.	<i>Gestão dos Recursos Humanos</i>	10
II.1.8.	<i>Cumprimento dos Requisitos Externos.....</i>	10
II.1.9.	<i>Avaliação de Riscos associados aos Processos de TI</i>	10
II.1.10.	<i>Gestão dos Projectos em Curso</i>	10
II.1.11.	<i>Gestão da Qualidade.....</i>	10
II.2.	DESENVOLVIMENTO E IMPLEMENTAÇÃO DE SOLUÇÕES.....	11
II.2.1.	<i>Identificação de Soluções.....</i>	11
II.2.2.	<i>Aquisição e Implementação de Aplicações.....</i>	11
II.2.3.	<i>Implementação da Infra-estrutura Tecnológica.....</i>	12
II.2.4.	<i>Desenvolvimento e Manutenção de Procedimentos de TI</i>	12
II.2.5.	<i>Instalação e Certificação de Sistemas</i>	13
II.2.6.	<i>Gestão da Mudança.....</i>	13
II.3.	OPERAÇÃO DO AMBIENTE INFORMÁTICO.....	14
II.3.1.	<i>Definição de Níveis de Serviço.....</i>	14
II.3.2.	<i>Gestão dos Serviços Prestados Por Terceiros.....</i>	15
II.3.3.	<i>Gestão do Desempenho e da Capacidade</i>	15
II.3.4.	<i>Assegurar a Continuidade de Serviços Prestados.....</i>	16
II.3.5.	<i>Assegurar a Segurança dos Sistemas.....</i>	18
II.3.6.	<i>Identificação e Afectação de Custos.....</i>	33
II.3.7.	<i>Prestação de Apoio e Formação aos Utilizadores</i>	33
II.3.8.	<i>Apoiar e Aconselhar os Clientes.....</i>	34
II.3.9.	<i>Gestão das Configurações</i>	34
II.3.10.	<i>Resolução e Gestão de Problemas de TI</i>	35
II.3.11.	<i>Gestão de Dados.....</i>	35
II.3.12.	<i>Gestão das Instalações Físicas.....</i>	36
II.3.13.	<i>Gestão das Operações</i>	37
II.4.	MONITORIZAÇÃO DOS PROCESSOS DE TI	37
II.4.1.	<i>Monitorização dos Processos de TI.....</i>	37
II.4.2.	<i>Avaliação de Controlo Interno de TI.....</i>	37
II.4.3.	<i>Certificação de Serviços e Sistemas.....</i>	37
II.4.4.	<i>Execução de Auditorias Independentes.....</i>	38



Tribunal de Contas

I. AVALIAÇÃO DOS PROCESSOS DE ATRIBUIÇÃO E CONTROLO DE PENSÕES

I.1. Processo de Gestão de Requerimentos

I.1.1. *Processo de Gestão de Requerimentos*

A melhoria do processo de gestão de requerimentos deve começar pela integração da informação que, neste momento, existe nos vários sistemas informáticos. Esta integração seria facilitada se existisse uma maior uniformidade das plataformas tecnológicas utilizadas por estes sistemas. Neste sentido, a melhoria deste processo depende, em parte, da definição de uma estratégia de sistemas de informação que vise a integração dos vários sistemas. Para mais pormenores vide ponto **II.1.1 – Definição da Estratégia de TI**.

Uma maior integração dos sistemas do ISSS permitirá que os elementos de informação inerentes a um requerimento de pensão sejam disponibilizados desde logo, de maneira a permitir a validação no momento em que o requerimento é apresentado no CDSSS e, assim, reduzir, na maioria dos casos, o volume de dados a introduzir. Para alcançar este objectivo, será necessário integrar toda a informação sobre a identificação do beneficiário e a sua carreira contributiva, de modo a que, no acto de registo do requerimento, toda esta informação seja passível de verificação.

Para facilitar este processo, deve ser contemplada a utilização da Internet (com os devidos mecanismos de segurança) – a disponibilização do registo do beneficiário permitirá, não só verificar a informação inerente ao mesmo (como a carreira contributiva e outros dados importantes), como também a preparação e apresentação *online* dos requerimentos de pensão. Também, a apresentação das declarações de contribuições em formato electrónico por parte das empresas vai permitir reduzir os atrasos no registo da carreira contributiva, possibilitando ao contribuinte/beneficiário validar os respectivos registos de contribuições e os seus dados pessoais, de forma quase imediata. A apresentação *online* de um requerimento permitirá que:

- A carreira contributiva do requerente possa ser validada pelo próprio antes da apresentação do requerimento;
- Seja possível a validação automática da informação declarada no requerimento;
- O requerente/beneficiário/utente tenha um meio de actualizar os seus dados pessoais, como a morada e informação de natureza bancária;



Tribunal de Contas

- O volume de informação introduzida pelos elementos dos CDSSS seja significativamente reduzido;
- A recepção do requerimento sirva para confrontar a declaração efectuada pelo conferente com os documentos apresentados;
- O *status* do requerimento seja visível ao requerente, quando acede via Internet, poupando assim tempo e custos de deslocações aos CDSSS; e
- Sejam efectuadas *online* as simulações de pensões prováveis, reduzindo assim o volume de requerimentos manuseados pelos CDSSS e pelo CNP.

Com esta opção, o requerente poderá imprimir uma cópia do seu próprio requerimento para eventual apresentação, juntamente com a documentação comprovativa necessária, no CDSSS, poupando tempo e custos no processo de requerimento de uma pensão. Será ainda necessário disponibilizar outras formas de apresentação dos requerimentos de pensão, embora a maior eficiência e eficácia seja a associada à apresentação de requerimentos *online* que permitirá uma maior capacidade de resposta por parte dos CDSSS relativamente a estes casos.

Recomenda-se também que haja uma diferenciação entre requerimentos de cálculos prováveis de pensão e requerimentos de pensão definitivos. Na medida do possível, o ISSS deve desenvolver os conhecimentos e as competências necessárias para que os cálculos de pensões prováveis sejam feitos nos CDSSS, para, por um lado, dar uma resposta mais imediata ao público, e, por outro, reduzir o volume de requerimentos que têm que ser processados e enviados para o CNP. Esta diferenciação permitirá:

- Dar prioridade ao eventual deferimento de requerimentos de pensão definitivos; e
- Criar mais conhecimentos e competências nos CDSSS no que se refere ao processamento de pensões.

I.1.1.1. RECEPÇÃO, ORGANIZAÇÃO E REGISTO DO REQUERIMENTO

As melhorias principais a considerar neste processo incluem:

- A introdução da funcionalidade de impressão automática do requerimento no acto de apresentação do mesmo, que deve ter carácter obrigatório. Esta impressão – que terá mais que uma via – deve integrar toda a informação necessária para a aceitação do requerimento, bem como servir de recibo de aceitação do requerimento. Uma das vias deste impresso deve ser assinada pelo requerente (como declaração de aceitação da integridade da informação apresentada) e incluída no processo.



Tribunal de Contas

- A atribuição automática da data de sistema ao registo do requerimento, bem como de um número sequencial único ao requerimento, no acto de emissão do recibo. Desta forma será mais fácil estabelecer, com base nos dados inerentes aos requerimentos:
 - a data de entrada de um requerimento, bem como os prazos reais até o seu deferimento;
 - os tempos de resposta reais para o deferimento de um processo; e
 - a totalidade dos processos processados e a omissão de processos.

- A introdução da data de junta médica, no caso de uma pensão de invalidez.

A introdução do parecer da junta médica deve, idealmente, ser efectuada directamente no sistema de requerimentos pela junta médica, para que esta informação possa ser validada no acto de apresentação de um requerimento de invalidez.

A validação de toda a informação no acto de recepção do requerimento permitirá reduzir significativamente comunicações posteriores com o requerente para obter informações omissas ou incorrectas. Este aspecto também poupará ao cidadão o número de deslocações aos CDSSS para tratar de questões processuais.

I.1.1.2. IDENTIFICAÇÃO DO BENEFICIÁRIO

A introdução do número de bilhete de identidade na base de dados nacional de beneficiários e utentes será um passo importante para melhorar a fiabilidade da identificação do beneficiário ou utente e permitirá ao ISSS cruzar a informação, em formato electrónico, que recebe de outras fontes, designadamente com o Ministério de Justiça, no que se refere a informação sobre falecimentos. Esta prática já foi adoptada por outros Ministérios e deve ser considerada pelo ISSS. O número de bilhete de identidade também poderá ser utilizado para a identificação positiva de um beneficiário, caso surjam dúvidas.

I.1.1.3. ENVIO E INTEGRAÇÃO DE INFORMAÇÃO COM O CNP

No que se refere ao envio de informação para o CNP, a integração, automática e regular, dos dados da carreira contributiva simplificaria este processo, dado que o CNP teria menos trabalho associado à introdução de dados sempre que os mesmos são omissos no sistema. Se a maioria do trabalho de validação da informação inerente a um requerimento for feita logo no acto de apresentação, considera-se que cada CDSSS estará numa melhor posição para assegurar que os requerimentos enviados



Tribunal de Contas

para o CNP estão completos e correctos. Contudo, será sempre necessário instituir um procedimento que valide e assegure que todos os processos enviados ao CNP vão completos e correctos, diminuindo assim as situações em que o CNP não consegue deferir, em tempo mais curto, um requerimento por falta de informação. O acto de transferência de um requerimento para o CNP deve registar o funcionário responsável pela verificação, para que eventuais erros possam ser identificados e corrigidos.

I.1.1.4. A CONFERÊNCIA E DEFERIMENTO DE PROCESSOS

O acto de deferimento é essencial para estabelecer o direito a uma pensão. A aprovação e o deferimento devem também ser objecto de registo no sistema, para que deles exista um rasto informático. Para alcançar este objectivo, será importante que o sistema actual registe o utilizador que efectuou a operação, restringindo essa capacidade aos utilizadores que disponham das devidas permissões.

I.1.1.5. O CÁLCULO DA PENSÃO

O cálculo da pensão continua a requerer uma disponibilidade de recursos humanos significativa, largamente devido ao facto de:

- existirem várias situações especiais introduzidas pela legislação que não estão contempladas pelos programas de cálculo de pensões;
- existirem vários requerimentos cuja carreira contributiva não está completa na altura do processamento do cálculo e que requerem a introdução dos salários em falta.

Para ultrapassar os problemas associados à falta de informação no acto de cálculo da pensão, é fundamental que haja controlo deste aspecto em dois momentos, especificamente:

- Na verificação e aceitação do requerimento apresentado pelo requerente no CDSSS; e
- Na reverificação do processo antes do seu envio para o CNP.

O CNP já efectua uma codificação do tipo de pensão consoante o tipo de regime aplicável à pensão. Dado o volume de alterações legislativas, é necessário que o programa de cálculo de pensões seja flexível e permita a parametrização da fórmula do cálculo por código de pensão. Recomenda-se, por isso, que a fórmula de cálculo seja parametrizável consoante esse código, de forma a impedir a alteração do programa de cálculo cada vez que um novo cálculo de pensão tenha que ser introduzido.



Tribunal de Contas

A validação do cálculo, por parte do conferente, deve ser efectuada com um programa *online* que permita essa validação (com mensagens de erros, se esse for o caso) e a impressão do verbete no momento em que o cálculo é efectuado. Este aspecto permitirá reduzir o nível de manuseamento de requerimentos e reduzir o prazo necessário para o deferimento. O programa a ser utilizado deverá também assegurar que todos os dados introduzidos para o cálculo sejam gravados e façam parte do registo do cálculo efectuado no sistema. Em situações onde o cálculo da pensão é efectuado mais que uma vez, todos os cálculos que resultem numa alteração ao valor de pensão a pagar devem ficar registados como parte do histórico do requerimento.

Da análise efectuada aos processos com cálculos manuais e das evidências constatadas resultam as seguintes recomendações:

- Sendo esta realidade detentora de uma acentuada dinâmica e uma vez que destes processos são expurgados diversos documentos importantes quando são enviados para a microfilmagem, recomenda-se que, na medida do possível, se elabore e se anexe aos processos uma folha resumo, não expurgável, onde sejam averbadas todas as ocorrências importantes (incluindo os cálculos efectuados), no sentido de facilitar a leitura e compreensão do seu desenvolvimento;
- Sendo o trabalho efectuado com este tipo de processos bastante complexo e exigente, que acarreta um risco de erro considerável, recomenda-se que sejam efectivamente separadas as funções de quem executa, de quem confere e de quem introduz na base de dados, além da adequada supervisão por parte dos responsáveis das unidades;
- Deverão, na medida do possível, ser desenvolvidas ferramentas informáticas de auxílio ao cálculo de pensões com códigos de situação especial, como é o caso da reforma antecipada (DL n.º 9/99, de 8 de Janeiro) e da articulação da antecipação com o desemprego (DL n.º 119/99, de 14 de Abril), no sentido de diminuir o risco de erro e de tornar mais célere a sua execução;
- Os documentos emitidos pelo CNP constantes dos processos, como sejam, os verbetes resumo das transacções efectuadas e a efectuar e as propostas de deferimento, sendo elementos fundamentais para a instrução dos processos, devem ser rigorosamente trabalhados, cuidando-se o seu devido preenchimento, datação e assinatura dos intervenientes;
- As divergências detectadas no decurso da auditoria e elencadas no **Anexo D** deverão ser, quando tal ainda seja possível em face das disposições legais aplicáveis, prontamente rectificadas.



Tribunal de Contas

I.1.1.6. PROCESSAMENTO E PAGAMENTO DE PENSÕES

No que se refere ao pagamento de pensões considera-se importante que o ISSS efectue esforços adicionais para assegurar que recebe dos vários bancos:

- uma confirmação electrónica dos pagamentos efectuados, bem como um ficheiro com as pensões não creditadas. Este ficheiro deverá indicar, pelo menos, o número do beneficiário ao qual o pagamento não foi efectuado.
- um extracto electrónico por cada conta bancária, que poderá ser utilizado para o carregamento automático de transacções efectuadas no sistema financeiro. Desta forma, poderá ser possível reduzir o volume de itens pendentes nas conciliações bancárias.



Tribunal de Contas

II. AVALIAÇÃO DOS PROCESSOS DE GESTÃO DE TI

II.1. Planeamento e Estratégia de Sistemas de Informação

II.1.1. *Definição da Estratégia de TI*

Considera-se importante que o ISSS avance com a constituição do Conselho Consultivo para que a sua estratégia de sistemas de informação a médio prazo seja validada e acordada entre todas as entidades que integram o SSSS. A elaboração deste plano estratégico deve, designadamente:

- Contemplar um processo que permita a prioritização dos objectivos estratégicos que o Sistema de Solidariedade e Segurança Social pretende alcançar;
- Desafiar e testar todos os pressupostos utilizados na formulação do plano estratégico;
- Ser validado por uma entidade terceira, a fim de aumentar a sua objectividade;
- Definir planos de migração de sistemas, aplicações e tecnologias, com datas e planos detalhados para alcançar os objectivos pretendidos; e
- Ser periodicamente avaliado e actualizado, para assegurar que continua a ser relevante e a responder às necessidades do Sistema de Solidariedade e Segurança Social.

Dada a evolução rápida das tecnologias de sistemas de informação, qualquer estratégia de sistemas de informação com horizontes superiores a 3 anos terá um nível de incerteza significativo.

II.1.2. *Definição da Arquitectura de Informação*

Considera-se que o modelo de dados actualmente contemplado para o Novo Sistema de Informação do SSSS deve considerar a classificação da informação, de forma a dar resposta às exigências cada vez maiores de segurança e confidencialidade e para poder suportar uma política integrada de segurança de informação.



Tribunal de Contas

II.1.3. Definição da Direcção Tecnológica de TI

Como parte da definição da sua estratégia de sistemas de informação, o ISSS deve contemplar e planear a migração dos seus sistemas para plataformas tecnológicas estandardizadas que permitam uma maior integração de informação. Para alcançar este objectivo é importante que todas as entidades do ISSS participem neste processo, para assegurar que novos investimentos em TI sejam efectuados de acordo com a estratégia de SI acordada.

II.1.4. Definição da Organização de TI e suas Interdependências

É importante que o ISSS comece a definir, como parte da sua estratégia de sistemas de informação, um Plano de Recursos Humanos que vise assegurar que a mesma disporá das pessoas e das competências para o alcance dos seus objectivos, no que se refere a sistemas de informação. Este Plano de Recursos Humanos deve, não só identificar as necessidades, em termos de competências técnicas exigidas pelos sistemas actuais, como também traçar o percurso necessário para dar resposta às exigências do Novo Sistema de Informação a ser desenvolvido.

II.1.5. Gestão dos Investimentos de TI

Não existem recomendações a efectuar.

II.1.6. Comunicação das Orientações Estratégicas

Considera-se que este processo pode ser melhorado com o desenvolvimento e comunicação de políticas e procedimentos de segurança de sistemas de informação para o ISSS. Estas políticas devem ser comunicadas a todos os utilizadores e disponibilizadas na Intranet do Instituto. Devem ser suportadas com a definição de:

- Procedimentos de administração de sistemas; e
- Standards de configuração para as tecnologias principais do ISSS que dão efeito às políticas estabelecidas.



Tribunal de Contas

II.1.7. *Gestão dos Recursos Humanos*

O ISSS deve definir, enquadrados num Plano de Recursos Humanos, como referido anteriormente, planos de formação para dar resposta às suas necessidades, bem como a introdução de rotação de tarefas que permita o desenvolvimento de competências redundantes, reduzindo assim a sua dependência de elementos individuais. Esta rotação de tarefas permitirá também assegurar as competências necessárias para dar resposta às exigências de segregação de funções normalmente definidas como parte das políticas e procedimentos de segurança.

II.1.8. *Cumprimento dos Requisitos Externos*

Não existem recomendações a efectuar.

II.1.9. *Avaliação de Riscos associados aos Processos de TI*

O ISSS deve considerar a gestão de riscos de TI como uma parte integrante do processo global de gestão de riscos de “negócio”. Torna-se necessário definir um procedimento que considere e avalie estes riscos, de uma forma formal, na definição e avaliação de projectos de sistemas de informação, bem como na avaliação dos processos de gestão dos sistemas do ISSS. Sugere-se que a adopção e aplicação dos conceitos de *IT Governance* sejam considerados e implementados na área de SI, dada a sua importância para o SSSS.

II.1.10. *Gestão dos Projectos em Curso*

As melhorias na gestão de projectos em curso dependem de uma maior disponibilidade dos recursos, por parte do SSSS, para acompanhar novos projectos em curso, bem como para criar mais competências nos vários CDSSS, no que toca à gestão de projectos.

II.1.11. *Gestão da Qualidade*

A gestão da qualidade de projectos deve ser uma responsabilidade partilhada entre todas as entidades do ISSS envolvidas num projecto. Dado o volume de desenvolvimentos e migrações de sistemas contemplados atinentes ao Novo Sistema de



Tribunal de Contas

de Informação, a função de gestão de qualidade de projectos deve ser estabelecida de forma a assegurar:

- ☑ A correcta definição de requisitos e critérios de aceitação de produtos desenvolvidos;
- ☑ O planeamento e monitorização adequado de projectos em curso;
- ☑ A integridade contínua dos dados afectados por desenvolvimentos efectuados ou pela migração de informação para novos sistemas; e
- ☑ A avaliação da conformidade dos produtos resultantes dos vários projectos através da realização de auditorias a projectos.

II.2. Desenvolvimento e Implementação de Soluções

II.2.1. Identificação de Soluções

Não existem recomendações a efectuar.

II.2.2. Aquisição e Implementação de Aplicações

Para mitigar os riscos associados a esta actividade, dever-se-ão considerar os seguintes aspectos:

- ☑ A formalização de uma metodologia de desenvolvimento de sistemas, apoiada pela definição de procedimentos e requisitos de documentação a produzir neste processo;
- ☑ A definição clara dos standards de qualidade em conjunto com os utilizadores chave dos sistemas de informação;
- ☑ A definição dos requisitos de controlo, aquando da definição dos standards de qualidade para os projectos de desenvolvimento ou aquisição de sistemas;
- ☑ A criação de condições para realização de testes e desenvolvimentos em ambientes segregados do ambiente de produção;



Tribunal de Contas

- ☑ A realização de testes documentados por parte dos utilizadores, que permitirão a qualquer entidade validar a qualidade dos testes efectuados.

Neste sentido recomenda-se que a metodologia de desenvolvimento adoptada pelo IIES seja adoptada e implementada por todas as entidades do SSSS, para assegurar a consistência e a integridade das alterações e desenvolvimentos efectuados.

II.2.3. Implementação da Infra-estrutura Tecnológica

Para mitigar os riscos associados a esta actividade, as entidades auditadas e o IIES devem continuar a efectuar esforços para assegurar os seguintes aspectos:

- ☑ Definição de uma plataforma o mais padronizada possível, para permitir uma gestão eficiente e eficaz dentro das capacidades e competências internas das entidades;
- ☑ A utilização do conceito de ciclo de vida da infra-estrutura integrado com a gestão de capacidade e performance, para permitir identificar os problemas e introduzir as necessárias alterações; e
- ☑ Uma maior utilização de ferramentas de apoio para a manutenção pró-activa do parque informático.

II.2.4. Desenvolvimento e Manutenção de Procedimentos de TI

Em consonância com a recomendação efectuada no ponto **II.1.6 – Comunicação das Orientações Estratégicas**, as políticas e procedimentos de segurança devem contemplar a existência de procedimentos que assegurem a actualização periódica da documentação inerente aos sistemas principais. Este procedimento deve considerar, não só os aspectos funcionais, mas também a actualização das políticas e procedimentos de segurança e manutenção de sistemas inerentes aos sistemas afectados. Este procedimento deve também ser considerado parte integrante do processo de Instalação e Certificação de Sistemas.

Recomenda-se que a distribuição e disponibilização desta documentação e dos procedimentos seja efectuada através de uma Intranet, o que permite uma mais fácil actualização.



Tribunal de Contas

II.2.5. *Instalação e Certificação de Sistemas*

A melhoria deste processo passa por uma maior divulgação e aceitação dos procedimentos de instalação e certificação de sistemas adoptados pelo IIES junto dos vários CDSSS de modo a que estes adoptem os mesmos procedimentos relativos às alterações e novas implementações.

II.2.6. *Gestão da Mudança*

As melhorias essenciais neste processo passam pelo estabelecimento de segregação entre as funções de desenvolvimento e as funções de administração de sistemas nos CDSSS de modo a que haja uma identificação atempada de situações que possam ter um impacto negativo sobre a estabilidade dos sistemas. Para mitigar os riscos associados a esta actividade, dever-se-á considerar os seguintes aspectos:

- Implementação de procedimentos de planeamento, aprovação e iniciação que cubram a identificação e priorização das mudanças e a sua categorização em termos de avaliação de impacto;
- Existência de ambientes de desenvolvimento e produção distintos para as aplicações mais críticas das entidades do ISSS;
- A aceitação por parte dos utilizadores afectados pelas mudanças efectuadas, de forma a assegurar que continuam responsáveis pela integridade da informação; e
- Consideração de um processo independente para verificar o sucesso das mudanças efectuadas do ponto de vista de melhorias conseguidas em termos da:
 - eficiência dos processos afectados;
 - funcionalidade e integridade dos sistemas afectados; e
 - aceitação e integração por parte dos elementos do ISSS nos seus processos de trabalho.



Tribunal de Contas

II.3. Operação do Ambiente Informático

II.3.1. *Definição de Níveis de Serviço*

Considera-se a definição formal de níveis de serviços esperados de cada Unidade de SI do SSSS, como uma componente fundamental para o estabelecimento de uma eficiente estratégia de sistemas de informação.

A definição de níveis de serviços constitui uma ferramenta que permite definir as expectativas das diversas entidades do SSSS, em relação à estrutura e serviços de suporte que cada Unidade de SI deverá disponibilizar.

A criação de níveis de serviços exige que cada Unidade de SI consiga definir, qualificar e quantificar os serviços e os custos das tecnologias de informação que disponibiliza aos utilizadores. Por outro lado, esta ferramenta exige tempo, comunicação e cooperação entre as diversas entidades do SSSS, no sentido de definir quais os serviços considerados e quais os acontecimentos quantificados.

Os factores que o SSSS deverá ter em consideração na implementação de níveis de serviços são, entre outros:

- Identificação das partes envolvidas;
- Comunicação efectiva entre as partes envolvidas;
- Definição das condições dos serviços a serem prestados;
- Estabelecimento de avaliação de desempenho da prestação de serviços de cada Unidade de SI;
- Gestão de processos e de recursos humanos das Unidades de SI;
- Definição do tempo de resposta a solicitações dos diversos Departamentos; e
- Gestão eficiente dos custos e encargos de cada Unidade de SI.



Tribunal de Contas

II.3.2. *Gestão dos Serviços Prestados Por Terceiros*

Recomenda-se que o IIES, no cumprimento da sua função de gestão dos serviços de TI prestados por terceiros, considere o estabelecimento de medidas que visem a protecção das diversas entidades do SSSS, nomeadamente:

- A definição de condições contratuais estandardizadas para todos os serviços contratados;
- A definição prévia das métricas próprias de avaliação dos serviços prestados;
- A implementação de programas globais de qualidade; e
- O estabelecimento de auditorias independentes.

II.3.3. *Gestão do Desempenho e da Capacidade*

Considera-se que tanto o IIES como os CDSSS deverão melhorar as suas actividades de monitorização do desempenho e da capacidade dos sistemas de informação do SSSS. Desta forma, o ISSS deverá incorporar na sua estratégia de sistemas de informação, a actualização do seu planeamento de capacidade para toda a infra-estrutura tecnológica, o qual deverá prever ajustamentos periódicos da capacidade dos sistemas, de forma a prevenir possíveis estrangulamentos ou picos de desempenho.

Por outro lado, deverão ser desenvolvidos e implementados procedimentos formais de monitorização e de manutenção dos sistemas. Estes procedimentos deverão abranger as várias plataformas existentes, devendo incluir como procedimentos obrigatórios, a utilização de ferramentas informáticas pró-activas, que monitorizam e emitem avisos, em caso de ocorrência de anomalias.

No caso dos servidores Windows NT deve-se considerar a definição de alertas administrativos para que os próprios servidores efectuem uma monitorização constante dos seus níveis de processamento e espaço em disco. Os alertas administrativos permitem que os administradores de sistemas sejam automaticamente alertados de eventuais problemas nos servidores.



Tribunal de Contas

II.3.4. *Assegurar a Continuidade de Serviços Prestados*

O ISSS deverá criar, num curto espaço de tempo, um plano formal de contingências para os seus sistemas de informação, que abarque todos os sistemas críticos independente da sua localização ou entidade responsável pela sua gestão. A implementação deste plano permitirá assegurar que os riscos de interrupção dos sistemas de informação se encontram identificados e geridos de forma adequada e eficaz. Numa fase posterior este plano deverá ser integrado num plano de continuidade de “negócio”, que cubra todas as funções críticas do ISSS.

A estratégia de recuperação a estabelecer, deverá incluir um entendimento das “funções do negócio”, dos requisitos da organização e das questões-chave associadas, devendo assegurar a recuperação atempada dos centros de processamento de dados críticos, bem como de serviços de dados, redes e telecomunicações, que sejam afectados por uma interrupção inesperada dos mesmos.

Este plano formal de contingência dos sistemas de informação deverá considerar os seguintes aspectos:

Definição dos Riscos Prováveis

Deverá ser a primeira etapa da elaboração do plano, na qual se definirá o risco associado à confidencialidade, integridade e disponibilidade da informação e do ambiente operacional. Este será o passo chave para determinar qual a informação crítica para o ISSS e quais as medidas necessárias para a sua salvaguarda.

Medidas de Minimização de Desastres

Definição das medidas necessárias para a salvaguarda da informação, para dar resposta aos riscos, de forma a minimizar a probabilidade de ocorrência de possíveis desastres, nomeadamente:

- As políticas formais de *backup* ou de salvaguarda de dados;
- Definição formal do coordenador dos esforços de recuperação e dos elementos responsáveis pela recuperação de sistemas críticos;
- Existência de redundância de sistemas, equipamentos de telecomunicações e outros equipamentos essenciais;
- Definição e monitorização das condições ambientais das infra-estruturas que permitem a identificação de uma eventual contingência; e



Tribunal de Contas

- Os procedimentos de segurança física das instalações técnicas das várias Unidades de SI.

□ **Procedimentos de Recuperação de Sistemas**

Estes procedimentos deverão ser implementados de forma a reduzir os prazos de recuperação necessários, reduzindo assim os efeitos adversos de um possível desastre. Para que estes procedimentos sejam efectivos, será necessário assegurar alguns dos seguintes aspectos:

- Que toda a informação e software necessário para reposição e recuperação de sistemas, seja salvaguardada por *backups*, os quais deverão ser guardados *off-site*;
- A existência de procedimentos detalhados, para que elementos externos à diversas Unidade de SI consigam executar com sucesso os planos de recuperação estabelecidos;
- A existência de redundância de conhecimentos sobre os procedimentos de recuperação dos sistemas;
- A existência de uma infra-estrutura *off-site*, que servirá como site alternativo para reposição da informação e de base ao restabelecimento das funções das várias unidades orgânicas do ISSS; e
- A garantia de substituição imediata para equipamentos críticos.

□ **Programa de Consciencialização**

Todos os colaboradores do ISSS deverão estar conscientes da importância da existência de um plano de contingência bem como as suas responsabilidades na sua execução, através da comunicação de normas formais e pela realização periódica de sessões de formação.

□ **Plano de Manutenção e Testes**

O plano de contingência deverá ser actualizado periodicamente. Esta actualização consistirá numa revisão periódica (ex. semestral) de todas as medidas do plano para dar resposta a alterações na arquitectura tecnológica. Esta revisão deve determinar se as alterações, de natureza estratégica ou técnica, justificam a alteração dos procedimentos do plano.



Tribunal de Contas

Para assegurar a eficácia contínua deste plano deverão ser efectuados testes periódicos aos procedimentos de recuperação, de forma a determinar se os mesmos continuam válidos para dar uma resposta atempada, a uma situação de desastre.

II.3.5. Assegurar a Segurança dos Sistemas

O ISSS deverá definir formalmente uma arquitectura de segurança, a qual irá promover entre todas as suas entidades uma maior sensibilização em relação a questões de segurança dos sistemas de informação, e a responsabilização de cada uma na gestão e manutenção dos sistemas e tecnologias de informação.

A definição das políticas e procedimentos de segurança recomendada em pontos anteriores servirá como primeiro passo para a melhoria desta actividade. É importante que as políticas definidas sejam divulgadas a todos os utilizadores e o seu reconhecimento formal seja efectuado. Será necessário também que um processo de actualização e de monitorização periódico acompanhe a implementação de políticas, para que estas sejam cumpridas e respeitadas. A actualização periódica deve ser considerada mediante mudanças significativas na arquitectura tecnológica actual do ISSS. A monitorização das políticas estabelecidas pode ser efectuada através da implementação de mecanismos de monitorização ou através de auditorias periódicas das políticas estabelecidas.

Para mitigar os riscos identificados nesta actividade, o ISSS deverá considerar a implementação das seguintes medidas:

- **Centro Nacional de Pensões (CNP)**

- Serviços de TCP/IP – Unisys ClearPath 2200

Recomenda-se que apenas os serviços absolutamente necessários deverão estar activos no sistema Unisys. Dentro deste contexto, aconselha-se a remoção do serviço HTTP.

- Qualidade das *Passwords* – Unisys ClearPath 2200

Recomenda-se o estabelecimento de políticas formais de segurança no sistema Unisys ClearPath 2200, que incluam procedimentos formais de gestão de *passwords*, de forma a ser obrigatória a existência das mesmas com uma composição mais complexa. Deste modo, aconselha-se a alteração do parâmetro MINPASSLEN para o valor de 8, de modo a que tenham pelo menos 8 caracteres de comprimento.



Tribunal de Contas

- Intervalos de Expiração de *Passwords* – Unisys ClearPath 2200

Recomenda-se a implementação de procedimentos regulares de mudança de *passwords* no sistema Unisys, de forma a que expirem, pelo menos, de dois em dois meses. Desta forma o parâmetro MAXPASSDAY deverá ter o valor de sistema 60.

- Servidores de Autenticação – Sistema Windows NT

Recomenda-se a remoção do Internet Information Server e do Proxy Server deste servidor e respectivos serviços e contas de utilizadores. Estes serviços deverão ser transferidos para um member-server, uma vez que não existe a necessidade de estarem instalados num Domain Controller.

- Serviços activos – Sistema Windows NT

Recomenda-se que apenas os serviços absolutamente necessários deverão estar activos. Em relação aos serviços Messenger e Alerter, aconselha-se que sejam tornados inactivos, caso não exista uma necessidade efectiva da sua utilização para a administração do domínio CNP.

- *Account Policies* – Sistema Windows NT

Recomenda-se que o CNP defina como requisitos mínimos de segurança as definições seguintes para os servidores Windows NT.

Account Policy	Valor Sugerido
Prazo de expiração da senha	30 dias
Permissão para alteração da senha	7 dias
Extensão mínima da senha	6 caracteres
Proibição de repetição das últimas X senhas	5 senhas
Bloqueio após X tentativas mal sucedidas de <i>log-in</i>	3 tentativas
Desbloqueio da conta após X minutos	30 minutos
Duração do bloqueio	120 minutos
Fecho da sessão após o período de <i>log-in</i>	Desliga
O utilizador necessita de efectuar <i>log-in</i> para alterar a sua senha	<i>log-in</i> obrigatório

- Perfis de Utilizadores – Sistema Windows NT

Recomenda-se que os perfis dos utilizadores sejam revistos periodicamente, de forma a averiguar se são realmente necessários. Se forem identificados utilizadores "adormecidos" ou inactivos, estes deverão ser imediatamente removidos do domínio CNP.



Tribunal de Contas

- Expiração de Contas Temporárias – Sistema Windows NT

Recomenda-se que a funcionalidade de expiração das contas de utilizadores, no domínio CNP, seja utilizada para todas as contas de funcionários do CNP e para as contas de utilização temporária pertencentes a entidades terceiras.

- Utilizadores Genéricos – Sistema Windows NT

Recomenda-se que todos os utilizadores genéricos sejam removidos ou desabilitados do sistema e substituídos por contas de utilizadores individualizadas, por cada um dos utilizadores que delas necessita.

- Home Directories – Sistema Windows NT

Recomenda-se que sejam criadas *home directories* para os vários utilizadores do domínio CNP.

- **CDSSS de Lisboa**

- Serviços de TCP/IP – Sistema VSE/ESA

Recomenda-se que apenas os serviços absolutamente necessários para o correcto funcionamento do sistema e das suas aplicações deverão estar activos. Desta forma, é nosso entendimento que o serviço HTTP deverá ser desactivado deste sistema.

- *Internet Information Server* – Sistema Windows NT

Recomenda-se a remoção do *Internet Information Server* e as respectivas contas de utilizadores. Este serviço deverá ser transferido para um *member-server*, uma vez que não existe a necessidade de estar instalado num *Domain Controller*.

- Utilizadores Genéricos e Sem Utilização – Sistema Windows NT

Recomenda-se que os perfis de utilizadores sejam revistos periodicamente para averiguar se são realmente necessários. Se forem identificados perfis de utilizadores "adormecidos" ou inactivos estes deverão ser imediatamente removidos.



Tribunal de Contas

Todos os utilizadores deveram ter a sua própria conta para se poder estabelecer responsabilidades por alterações efectuadas nos sistemas. A manutenção de perfis de utilizadores pré-definidos deverá ser tida em linha de conta, tornando mais simples a defesa contra acessos não autorizados aos sistemas de informação, aumentando a qualidade dos controlos de acesso e assegurando a segregação de funções;

Como forma preventiva desta situação, devem ser implementados e formalizados procedimentos de remoção de acessos aos funcionários que já não façam parte do Centro Distrital, através de uma articulação entre a Unidade de Sistemas de Informação e a Unidade de Recursos Humanos.

o Procedimentos de Retirada de Acessos – Sistema Windows NT

Recomenda-se que sejam definidos formalmente procedimentos para assegurar que os direitos de acesso sejam corrigidos atempadamente perante qualquer movimento de pessoal. Estes procedimentos devem incluir uma *checklist* a completar sempre que um funcionário deixe de prestar funções no Centro Distrital ou que mude de posto de trabalho.

Adicionalmente, deve ser verificada a lista de utilizadores autorizados no sistema. A Unidade de Sistemas de Informação deve enviar, regularmente, uma lista a cada Unidade do Centro Distrital, com a descrição dos utilizadores e seus direitos de acesso para confirmação. Este procedimento possibilita uma menor dependência, da informação fornecida pela Unidade de Recursos Humanos ou em comunicações informais de todas as transferências e saídas do Centro Distrital.

o *Account Policies* – Sistema Windows NT

Recomenda-se que o CDSSS de Lisboa defina como requisitos mínimos de segurança as definições seguintes para os servidores Windows NT.

<u>Account Policy</u>	<u>Valor Sugerido</u>
Prazo de expiração da senha	30 dias
Permissão para alteração da senha	7 dias
Extensão mínima da senha	6 caracteres
Proibição de repetição das últimas X senhas	5 senhas
Bloqueio após X tentativas mal sucedidas de <i>log-in</i>	3 tentativas
Desbloqueio da conta após X minutos	30 minutos
Duração do bloqueio	120 minutos
Fecho da sessão após o período de <i>log-in</i>	Desliga
O utilizador necessita de efectuar <i>log-in</i> para alterar a sua senha	<i>log-in</i> obrigatório



Tribunal de Contas

- *Software* de Segurança para IBM VSE/ESA

Recomenda-se que seja instalada uma versão de VSE/ESA compatível com a instalação de um package de segurança e controlo, de forma a que a Unidade de Sistemas de Informação possa gerir de forma mais eficiente os seus recursos de informação. Este tipo de software irá permitir, nomeadamente:

- Identificar e verificar os utilizadores de sistema;
- Identificar, classificar e proteger os recursos de sistema;
- Autorizar os utilizadores que necessitam de ter acesso aos recursos protegidos;
- Controlar os mecanismos de acesso a esses recursos;
- Registar e reportar as tentativas de obtenção de acesso não autorizado ao sistema e aos recursos protegidos; e
- Administrar a segurança de forma a respeitar as políticas de segurança definidas.

- **CDSSS do Porto**

- Atribuição de Novos Acessos

Recomenda-se o estabelecimento de procedimentos formais de atribuição de novos acessos aos sistemas do CDSSS do Porto. Só deverão ter acesso a estes sistemas os elementos devidamente autorizados e que deles necessitem para o desempenho das suas funções. Deverá ainda existir um rasto de evidência de todo o processo de criação de novos pedidos de acesso.

- Retirada de Acessos

Recomenda-se a implementação de procedimentos formais que estipulem práticas de comunicação periódica (ex. mensal) por parte da Unidade de Recursos Humanos à Unidade de Sistemas de Informação, no sentido de alertar das saídas de colaboradores do CDSSS do Porto.

- Fracos Controlos de Acesso – IDMS e ADABAS

Aconselhamos que todos os perfis de utilizadores genéricos sejam removidos ou desabilitados do sistema e substituídos por perfis de utilizadores individualizados, por cada um dos utilizadores que deles necessita. Este processo irá aumentar a qualidade dos controlos de acesso, o que conduzirá a



Tribunal de Contas

um adequado nível de segregação de funções. Desta forma, existirá um rasto e uma responsabilização directa dos utilizadores.

- Utilizadores na Classe de Administrator

Considera-se que a utilização da conta Administrator ou contas equivalentes deverá estar limitada apenas aos responsáveis directos pela administração dos sistemas e a uma conta de *backup*. Neste contexto, recomendamos que estas autorizações sejam revistas, de forma a existir uma atribuição de permissões em função das tarefas desempenhadas por cada um dos utilizadores do CDSSS do Porto.

- Monitorização de Acessos

Recomenda-se o estabelecimento de políticas formais, que garantam a existência de procedimentos diários de monitorização das actividades críticas dos sistemas do CDSSS do Porto.

- **CDSSS de Setúbal**

- Default Public Authority – Sistema OS/400

O CDSSS de Setúbal deverá considerar valores mais restritivos para este parâmetro, dado existir o risco de se estar a atribuir capacidades excessivas aos utilizadores do Centro. Desta forma, aconselha-se que o valor deste parâmetro seja alterado para *USE (possibilita a leitura de objectos, mas não a sua alteração) ou *EXCLUDE (previne os utilizadores de acederem aos objectos).

- Segurança de Objectos Críticos – Sistema OS/400

Recomenda-se que o parâmetro QALWOBJRST tenha o valor de *NONE, para as tarefas de administração diária do sistema OS/400 do CDSSS de Setúbal, de forma a existir o máximo controlo em termos de segurança sobre objectos de sistema ou sobre programas que adoptam a sua própria autoridade. Este valor necessitará de ser alterado temporariamente para *ALL, em situações de instalação de novas releases do sistema OS/400 ou de instalação de novos PTF'S (Program Temporary Fixes) e em procedimentos de recuperação de objectos do sistema.



Tribunal de Contas

- Serviços de TCP/IP – Sistema OS/400

Recomenda-se que apenas os serviços absolutamente necessários para o correcto funcionamento do sistema e das suas aplicações deverão estar activos.

- Qualidade das *Passwords* – Sistema OS/400

Recomenda-se o estabelecimento de políticas e normas formais de segurança no sistema OS/400, que incluam procedimentos formais de gestão de *passwords*, de forma às mesmas existirem com uma composição complexa. Estas políticas deverão ser comunicadas formalmente a todos os utilizadores do CDSSS de Setúbal.

Deste modo, aconselha-se a implementação de novos valores nos seguintes parâmetros:

- QPWDRQDDIF = 1, o qual não permite a repetição das últimas 32 *passwords* já anteriormente utilizadas;
- QPWDLMTAJC = 1, o que implica que adjacente a cada dígito terá de existir sempre um caracter alfabético;
- QPWDLMTREP = 1, não permite a utilização de caracteres repetidos na mesma *password*;
- QPWDMINLEN = 5, o que implica que seja 5 o número mínimo de caracteres a definir numa *password*; e
- QPWDRQDDGT = 1, o que obriga à utilização de pelo menos 1 dígito na *password*.

- Intervalos de Expiração de *Passwords* – Sistema OS/400

Recomenda-se a implementação de procedimentos regulares de mudança de *passwords* do sistema OS/400, que forcem a sua mudança pelo menos de dois em dois meses. Desta forma o parâmetro QPWDEXPITV deverá ter o valor de sistema 60. Caso seja atribuído algum valor no user *profile*, no parâmetro referente ao intervalo de expiração da *password*, este valor terá preponderância em relação ao valor de sistema referente ao parâmetro QPWDEXPITV.



Tribunal de Contas

- Número de Sessões Concorrentes – Sistema OS/400

Recomenda-se que o parâmetro QLMTDEVSSN seja alterado para o valor de sistema 1, limitando os utilizadores a um único terminal. Caso existam utilizadores específicos que necessitem de aceder ao sistema em mais que um terminal, esta autorização poderá ser concedida a um nível individual, através da alteração do parâmetro LMTDEVSSN, no respectivo *user profile*, para o valor *NO.

- *User Profile* de Sistema – Sistema OS/400

Recomenda-se a alteração da *password* referente a este *user profile*, independentemente do mesmo ser utilizado ou não nas actividades de administração do sistema OS/400.

- Perfis de Utilizadores – Sistema OS/400

Recomenda-se que todos os perfis de utilizadores sejam revistos periodicamente, de forma a se averiguar se são efectivamente necessários. Neste contexto, aconselha-se que os perfis de utilizadores que se encontram no estado de DISABLE ou que não se autenticam no sistema há mais de 3 meses sejam avaliados se são realmente necessários. Se forem identificados perfis de utilizadores "adormecidos" ou inactivos deverão estes ser imediatamente removidos do sistema OS/400.

- Perfis de Utilizadores Genéricos – Sistema OS/400

Recomenda-se que todos os perfis de utilizadores genéricos sejam removidos ou desabilitados do sistema e substituídos por perfis de utilizadores individualizados por cada utilizador. Dessa forma, aumenta a qualidade dos controlos de acesso e atinge-se um nível de segregação de funções mais adequado. Aconselha-se, ainda, que o perfil de utilizador PDES01, o qual possui acesso à linha de comando e tem a Special Authority de *ALLJOB, seja removido do sistema, uma vez que o mesmo já não é necessário.

- *Sign-on* ao Sistema – Sistema OS/400

Recomenda-se a alteração do parâmetro QMAXSIGN para o valor de sistema de 3 tentativas de acesso inválidas, antes da execução da acção de *Disable Device* e *Disable User Profile* definida pelo parâmetro QMAXSGNACN.



Tribunal de Contas

- *Sign-on do Security Officer* – Sistema OS/400

Recomenda-se que o valor do parâmetro QLMTSECOFR seja alterado para o valor de 1. Esta modificação irá garantir que os utilizadores com as special authorities *ALLOBJ e/ou *SERVICE apenas possam fazer sign-on em estações de trabalho que foram especificamente atribuídas para o efeito.

- Informação de *Sign-on* – Sistema OS/400

Recomenda-se que o valor do parâmetro QDPSGNINF seja alterado para 1, para que o utilizador disponha de toda informação relativa à autenticação no sistema OS/400. Caso seja atribuído algum valor no user profile, no parâmetro referente à disponibilização de informação sobre o sign-on, este valor terá preponderância em relação ao valor de sistema referente ao parâmetro QDPSGNINF.

- Desactivação de Sessões Inactivas – Sistema OS/400

Recomenda-se a implementação de mecanismos de controlo que forcem a desconexão automática de um utilizador no sistema, após um certo período de inactividade (ex. 60 minutos). Este procedimento deverá ser implementado através do parâmetro QINACTITV = 60.

Aconselha-se, ainda, a alteração do parâmetro QINACTMSGQ para *DSCJOB, o que significa que a sessão apenas é terminada quando o intervalo de tempo de desconexão, especificado pelo parâmetro QDSCJOBTIV for atingido (240 minutos).

- Dispositivos Virtuais – Sistema OS/400

Recomenda-se que seja considerada a alteração do valor do parâmetro QAUTOVRT para 0, de forma a que o sistema OS/400 não permita a configuração automática de novos dispositivos virtuais, usados para o estabelecimento de sessões por pass-through ou por Telnet.

- Programa *Attention-Key* – Sistema OS/400

Recomenda-se que o valor do parâmetro QATNPGM seja alterado para o valor *NONE, o qual forçará o utilizador a regressar ao Menu ou Programa Inicial. Adicionalmente cada perfil de utilizador criado deverá ter o parâmetro ATNPGM com o valor *SYSVAL, com o objectivo de forçar o sistema OS/400 a utilizar a configuração definida para o parâmetro de segurança QATNPGM. Desta forma, o CDSSS de Setúbal



Tribunal de Contas

pode assegurar a consistência deste parâmetro de acesso, limitando o acesso à linha de comando.

- Implementação de *Limited Capability* – Sistema OS/400

Os perfis de utilizador devem ter as *limited capabilities* activas para se limitar os comandos que poderão ser executados, o que significa que o parâmetro *Limited Capability* deverá ter o valor de *YES. Recomenda-se que o CDSSS de Setúbal efectue uma revisão de todos os perfis de utilizadores que tenham actualmente o valor "NO" no parâmetro *Limited Capability* e o ajustem para aqueles que não necessitem deste atributo para realizarem as suas funções diárias. Todos os que mantiverem esta configuração deverão ser objecto de monitorização para se garantir que não se está a permitir acessos indevidos a objectos sensíveis.

- Autorização de Acesso a Bibliotecas – Sistema OS/400

Recomenda-se que as autorizações sobre estas bibliotecas sejam revistas e alteradas para *USE, de forma a que os utilizadores apenas tenham possibilidade de ler a informação e não de alterá-la (caso isso não faça parte das suas funções).

- Mecanismos de Auditoria – Sistema OS/400

Recomenda-se o estabelecimento de políticas formais, que garantam a existência de procedimentos diários de monitorização de actividades críticas do sistema OS/400. Desta forma, aconselha-se que o parâmetro QAUDCTL tenha o valor *AUDLVL, o qual possibilita que sejam elaborados relatórios de funções definidas no valor de sistema QAUDLVL e no parâmetro AUDLVL constante nos perfis de utilizadores. O valor *OBJAUD também pode ser considerado se for definida a monitorização de acessos a objectos específicos.

- *Audit Journal* – Sistema OS/400

Recomenda-se que o mecanismo de registo de eventos de segurança seja activado no parâmetro QUADLVL, de forma a que todas as ocorrências relacionadas com segurança sejam detectadas e investigadas regularmente através dos relatórios produzidos. Activando o *Audit Journal*, leva a que 14 categorias de eventos de segurança produzidos no sistema OS/400, sejam registados no *Audit Journal*, o que permite atingir um nível de segurança que vai de encontro às necessidades de segurança do CDSSS de Setúbal. Aconselha-se que o parâmetro QUADLVL contenha pelo menos os seguintes valores:

- *PGMFAIL – Regista violações da integridade do sistema;



Tribunal de Contas

- *SECURITY – Regista operações relacionadas com segurança;
- *SYSMGT – Regista a utilização de funções de administração do sistema OS/400; e
- *SERVICE – Regista a utilização de ferramentas relacionadas com serviços

Outra das vantagens do *Audit Journal* é o facto de este não poder ser eliminado do sistema OS/400.

- Servidores de Autenticação – Sistema Windows NT

Recomenda-se a remoção do Internet Information Server e do Proxy Server deste servidor e respectivos serviços e contas de utilizadores. Estes serviços deverão ser transferidos para um member-server, uma vez que não existe a necessidade de estarem instalados num Domain Controller.

- Ligações Anónimas – Sistema Windows NT

Recomenda-se a restrição de ligações anónimas a todos servidores Windows NT em geral, e nos *Domain Controllers* em particular, de forma a prevenir a obtenção não autorizada de informação sensível do domínio SETUBAL.

A partir do Service Pack 3 para o Windows NT, existe a possibilidade de restringir ligações anónimas a sistemas NT. Recomenda-se, por isso, que se restrinja este tipo de acesso, criando o parâmetro de registry RestrictAnonymous na seguinte chave:

HIVE: HKEY_LOCAL_MACHINE

KEY: \System\CurrentControlSet\Control\LSA

Este parâmetro deverá ser igual a um (1) para estar activo.

A activação desta chave do registry não bloqueia na totalidade o estabelecimento de null sessions, o que também não é o pretendido em Domain Controllers ou em Member Servers que façam parte de um domínio, uma vez que as ligações Netbios são indispensáveis para o funcionamento normal de um domínio NT. No entanto, esta chave de registry previne que informação sensível e confidencial, como a informação dos utilizadores do domínio ou da máquina ou a respectiva lista de shares, seja obtida pelo estabelecimento deste tipo de ligações.



Tribunal de Contas

- Serviços Activos – Sistema Windows NT

Recomendamos que apenas os serviços absolutamente necessários deverão estar activos. Em relação aos serviços Messenger e Alerter, aconselhamos a torná-los inactivos, caso não exista uma necessidade efectiva da sua utilização para a administração do domínio SETUBAL. Todos os servidores críticos não devem anunciar a sua existência na rede, devendo o serviço de browsing ser desactivado. Para tal, dentro na chave de registry –

HIVE: HKEY_LOCAL_MACHINE

KEY:

`\System \CurrentControlSystem \Service \Lanmanserver \parameters`

– deverá existir o parâmetro Hidden, cujo valor deverá ser igual a um (1). Desta forma, os servidores não aparecerão nas listas de browsing.

- Assinatura de pacotes SMB – Sistema Windows NT

Recomenda-se a utilização da funcionalidade de assinatura de pacotes SMB (SMB signing), a qual providencia uma forma de autenticação colocando assinaturas de segurança digitais em cada pacote SMB, o qual é verificado por clientes e pelo servidor. Desta forma, nos sistemas Windows NT, deverão existir os parâmetros EnableSecuritySignature e RequireSecuritySignature, ambos igual a um (1), dentro da seguinte chave de registry:

HIVE: HKEY_LOCAL_MACHINE

KEY:

`\System \CurrentControlSet \Services \LanManServer \parameters`

Nas máquinas NT Workstation 4.0 deverão existir os mesmos parâmetros iguais a um (1), mas na chave de registry:

HIVE: HKEY_LOCAL_MACHINE

KEY:

`\System \CurrentControlSet \Services \Rdr \parameters`

Esta opção só deve ser utilizada caso os sistemas em utilização sejam apenas NT Servers e NT Workstations.

- Remoção do *Pagefile* – Sistema Windows NT

Recomenda-se que o *pagefile* seja automaticamente apagado durante o *shutdown* dos sistemas, devendo, para isso, existir o parâmetro ClearPageFileAtShutdown, na chave de *registry* –



Tribunal de Contas

HIVE: HKEY_LOCAL_MACHINE

KEY:

\System \CurrentControlSet \Control \SessionManager
\MemoryManagement

– o qual deverá ser igual a um (1). Dessa forma, o *pagefile* será apagado automaticamente durante o shutdown do sistema Windows NT.

- Subsistemas OS/2 e Posix – Sistema Windows NT

Recomenda-se que os subsistemas OS/2 e Posix sejam removidos. Desta forma, deverão ser removidos da seguinte da chave de registry, os parâmetros opcionais referentes a OS/2 e Posix:

HIVE: HKEY_LOCAL_MACHINE

KEY:

\System \CurrentControlSet \Control \SessionManager \Subsystem

- Redundância de Discos – Sistema Windows NT

Recomenda-se a implementação de um sistema de redundância de discos (Raid 5, Mirroring ou Disk Striping com paridade), de forma a aumentar a consistência e disponibilidade dos sistemas Windows NT.

- Qualidade das *Passwords* – Sistema Windows NT

Recomenda-se o estabelecimento de políticas formais, que definam quais os procedimentos de atribuição e administração de *passwords* para utilizadores internos (funcionários do CDSSS de Setúbal), externos (empresas prestadoras de serviços), aplicativos (utilizados pelas aplicações) e para utilizadores normais dos servidores Windows NT.

Dentro deste contexto, Recomenda-se que seja obrigatória a utilização de *passwords* complexas para aceder aos recursos dos sistemas NT. Para tal, deverá existir o parâmetro *Passfilt* na seguinte chave de registry:

HIVE: HKEY_LOCAL_MACHINE

KEY:

\System \CurrentControlSet \Control \Lsa

O *Passfilt*, quando instalado, requer que as *passwords* tenham pelo menos seis caracteres de comprimento, não podendo conter o nome do utilizador ou alguma parte do nome completo inserido no campo Full Name e terão de conter caracteres de, pelo menos, três das seguintes alternativas:



Tribunal de Contas

- Caracteres alfabéticos em letras maiúsculas (A, B, C,...Z);
- Caracteres alfabéticos em letras minúsculas (a, b, c,...z);
- Caracteres numéricos inteiros (0,1,2,...9); e
- Caracteres não alfanuméricos (@, #, !, &, ...).

○ *Account Policies* – Sistema Windows NT

Recomenda-se que o CDSSS de Setúbal defina como requisitos mínimos de segurança as definições seguintes para os servidores Windows NT.

Account Policy	Valor Sugerido
Prazo de expiração da senha	30 dias
Permissão para alteração da senha	7 dias
Extensão mínima da senha	6 caracteres
Proibição de repetição das últimas X senhas	5 senhas
Bloqueio após X tentativas mal sucedidas de <i>log-in</i>	3 tentativas
Desbloqueio da conta após X minutos	30 minutos
Duração do bloqueio	120 minutos
Fecho da sessão após o período de <i>log-in</i>	Desliga
O utilizador necessita de efectuar <i>log-in</i> para alterar a sua senha	<i>log-in</i> obrigatório

○ Implementação do *SysKey* – Sistema Windows NT

Recomenda-se a activação da funcionalidade *SysKey*, para aumentar o nível de segurança dos sistemas ao possibilitar um esquema de encriptação de 128 bits das hashes das *passwords* dos servidores Windows NT mais críticos. O *SysKey* poderá residir localmente no servidor ou numa unidade de *diskette*.

○ Implementação do *Passprop* – Sistema Windows NT

Recomenda-se a utilização desta funcionalidade, de forma a permitir que a conta do utilizador ADMINISTRATOR possa ser desabilitada da rede, caso se ultrapasse o número máximo de tentativas falhadas de autenticação, permitidas pelas *Account Policies*.

○ Perfis de Administração – Sistema Windows NT

Os perfis dos utilizadores são a primeira forma de defesa contra acessos não autorizados aos sistemas Windows NT. A qualidade dos controlos de acesso com base em perfis de utilizadores e *passwords* é fundamental para assegurar a segregação de funções nos sistemas de informação. Desta forma, recomendamos que os perfis dos utilizadores sejam revistos periodicamente, de forma a averiguar se são realmente necessários. Se forem identificados utilizadores "adormecidos" ou inactivos, estes deverão ser imediatamente removidos.



Tribunal de Contas

- *Home Directories* – Sistema Windows NT

Recomendamos que sejam criadas home directories para os vários utilizadores do domínio NT em análise.

- Mensagem de Aviso – Sistema Windows NT

Recomenda-se que seja utilizado um aviso legal em todos os sistemas em análise, cujo objectivo é o de informar os utilizadores que estão a utilizar recursos do CDSSS de Setúbal e que qualquer tipo de acesso ou utilização indevida pode levar a que o infractor seja processado. Para tal deverão ser activados os parâmetros LegalNoticeCaption e LegalNoticeText, na seguinte chave de registry:

HIVE: HKEY_LOCAL_MACHINE

KEY:

\Software

\Microsoft

\Windows NT

\CurrentVersion

\Winlogon

- Divulgação do Último Utilizador – Sistema Windows NT

Recomenda-se a desactivação da opção de mostrar automaticamente o nome do último utilizador a autenticar-se localmente nos servidores Windows NT.

Para tal, o parâmetro DontDisplayLastUserName deverá existir e ser igual a um (1), na seguinte chave de registry:

HIVE: HKEY_LOCAL_MACHINE

KEY:

\Software \Microsoft \WindowsNT \Current Version \Winlogon

- Monitorização de *Logs* – Sistema Windows NT

Recomenda-se que sejam implementados procedimentos formais e regulares de revisão dos relatórios de violação de acessos ou logging, produzidos pelos sistemas NT, bem como definidas as respectivas responsabilidades sobre as acções de follow-up. Estes procedimentos assumem maior importância com o crescimento do CDSSS de Setúbal, e consequentemente com o aumento da complexidade da rede e do número de utilizadores.



Tribunal de Contas

○ *Audit Policies* – Sistema Windows NT

Recomenda-se que os sistemas Windows NT localizados no CDSSS de Setúbal possuam nas *Audit Policies* a configuração dos seguintes parâmetros:

- Logon and Logoff: Success and Failure;
- File and Object Access: Failure (para os ficheiros mais sensíveis);
- Use of User Rights: Failure;
- User and Group Management: Success and Failure;
- Restart, Shutdown and System: Success and Failure;
- Process Tracking: Failure; e
- Security Policy Changes: Success and Failure.

II.3.6. *Identificação e Afecção de Custos*

A afecção de custos por serviços prestados, só faz sentido quando as várias entidades do SSSS tiverem uma clara noção dos níveis de serviços a serem prestados por cada Unidade de SI, bem como quando possuírem adequados mecanismos e recursos para os monitorizar.

II.3.7. *Prestação de Apoio e Formação aos Utilizadores*

Apesar das várias Unidades de SI reconhecerem a necessidade de gerir os seus recursos humanos na área de formação de sistemas de informação, o ISSS deverá desencadear esforços no sentido de estabelecer um processo estruturado que permita definir as necessidades de formação individuais e globais por cada entidade do ISSS.

Após o levantamento das necessidades de formação, e enquadrado no Plano de Recursos Humanos, dever-se-á proceder ao desenvolvimento de um adequado programa de formação que dá resposta às necessidades dos utilizadores, de forma a melhorar o nível de utilização dos sistemas de informação disponíveis. Por outro lado, uma apropriada formação técnica será a garantia de uma correcta e optimizada utilização dos recursos tecnológicos disponibilizados pelas várias Unidades de SI.

Esta actividade deverá ainda assegurar que cada novo projecto de implementação de soluções aplicacionais considera as necessidades de formação dos utilizadores, a qual deverá ser ministrada por utilizadores chave de cada Unidade. É nosso entendimento que o ISSS deverá também tipificar os problemas dos utilizadores originados pela falta de formação. Esta tipificação é normalmente efectuada com as estatísticas providenciadas por uma ferramenta de gestão de *Help Desk* referida no ponto seguinte.



Tribunal de Contas

II.3.8. *Apoiar e Aconselhar os Clientes*

Como forma de melhorar o desempenho deste processo, as várias entidades do ISSS deveriam considerar a função de *Help Desk* como um instrumento de gestão, para que sejam identificados os problemas de maior recorrência ou de maior complexidade. Desta forma, será possível reagir de forma pró-activa aos problemas e necessidades dos utilizadores das várias entidades do ISSS através da instituição de medidas correctivas.

A eficiência da função de *Help Desk* deverá ser avaliada através de uma ferramenta de gestão, a qual permitirá medir dados objectivos, os quais incluem normalmente o volume de solicitações, a disponibilidade, o tempo de resposta, a percentagem de resolução de problemas e outros indicadores de performance e estatística da função de *Help Desk*.

As várias entidades do SSSS deverão também desenvolver acções de formação técnica para os seus utilizadores, para que os problemas de menor complexidade possam ser solucionados autonomamente pelos utilizadores, aliviando assim a carga de solicitações às Unidades de SI.

II.3.9. *Gestão das Configurações*

Considera-se que as várias Unidades de SI do ISSS deverão definir políticas formais que garantam a implementação de standards de configurações a adoptar nos diversos sistemas. As configurações estandardizadas devem ser extendidas para os sistemas principais do ISSS. Assim considera-se necessário a definição de configurações standard para as outras plataformas com AS/400, VSE/ESA, Windows NT Server que suportam as aplicações principais do ISSS. A implementação destas configurações deve ser efectuada de forma a assegurar a uniformidade de configurações de sistemas. Por outro lado, deverá existir um adequado controlo de todas as alterações efectuadas às configurações destes sistemas, as quais deverão ser objecto de uma aprovação formal, por parte dos responsáveis de cada Unidade de SI, no caso de serem alterações significativas às configurações dos sistemas.

Como parte desta definição de configurações de segurança, o ISSS deve assegurar o cumprimento dos acordos de licenciamento de todo o *software* utilizado e prevenir a utilização de *software* não formalmente autorizado.

Estas políticas a definir deverão também englobar procedimentos formais de inventariação periódica de *hardware* e de *software*, para assegurar a actualização sistemática e atempada de novas versões, nas várias plataformas de sistemas



Tribunal de Contas

existentes no ISSS, bem como nos computadores dos seus utilizadores, através de ferramentas remotas de gestão.

II.3.10. Resolução e Gestão de Problemas de TI

Apesar das várias Unidades de SI reconhecerem a necessidade de gerir a resolução de problemas e de avaliar os incidentes, considera-se necessária a utilização de ferramentas informáticas específicas para gerir a resolução de problemas técnicos, originados pelos utilizadores das várias unidades do SSSS. Este tipo de ferramenta normalmente está integrado numa aplicação de HelpDesk que tipicamente regista por solicitação os seguintes aspectos:

- A origem do pedido;
- O sintoma do problema;
- A prioridade de resolução;
- O *status* da resolução do problema;
- As soluções adoptadas;
- Os elementos responsáveis pela resolução; e
- Outros comentários

A análise desta informação é importante para:

- Identificar tendências de problemas ocorridos para que medidas pró-activas sejam implementadas;
- Identificar eventuais necessidades de informação por parte de certos utilizadores;
- Medir o desempenho da resposta do Helpdesk à resolução de problemas.

II.3.11. Gestão de Dados

Como forma de melhorar o desempenho desta actividade, considera-se que o futuro modelo de dados pretendido para o Novo Sistema de Informação do ISSS deve ser detalhado para que os dados omissos nos sistemas existentes possam ser recolhidos até á data em que transitam para o novo sistema. Como parte da definição do futuro modelo de dados considera-se necessário assegurar que:

- os requisitos de validação e integridade referencial do modelo de dados são devidamente considerados;



Tribunal de Contas

- ☑ a informação criada em cada fase do ciclo de vida de um beneficiário ou utente é integrada para poder suportar adequadamente os processos operacionais; e
- ☑ o modelo consegue gerir, armazenar e partilhar a informação não estruturada do ISSS.

As várias entidades do ISSS deverão assegurar a redução ao mínimo possível do tratamento manual dos dados, através da disponibilização de sistemas em que o tratamento dos mesmos é efectuado de forma automática, isto é, com intervenção humana limitada. Para isto, é necessário que os sistemas implementados tenham os necessários controlos de introdução e processamento de dados, de forma a garantir a integridade da informação.

II.3.12. *Gestão das Instalações Físicas*

O ISSS deverá considerar a melhoria dos seguintes aspectos nesta actividade:

- ☑ Restrição do acesso físico às salas técnicas, nos CDSSS de Lisboa e Setúbal, apenas a elementos devidamente autorizados;
- ☑ Todos os bastidores deverão estar permanentemente fechados com protecções adicionais de segurança;
- ☑ Implementação de medidas que visem dotar as salas técnicas de melhores condições ambientais, de forma a proteger a integridade dos vários sistemas;
- ☑ Integração das políticas de segurança física nas políticas de segurança do ISSS;
- ☑ Estabelecimento de contratos ou acordos, para no caso de ser necessário estarem disponíveis instalações alternativas durante um desastre; e
- ☑ Definição de um plano formal de contingência para os seus sistemas de informação, que contemple as instalações físicas dos sistemas de informação.



Tribunal de Contas

II.3.13. *Gestão das Operações*

Recomenda-se que as Unidades de SI do SSSS, procedam à criação de documentação formal de suporte à operação e manutenção dos seus sistemas de informação para as várias plataformas tecnológicas. Estes procedimentos operacionais deverão definir a periodicidade das tarefas a realizar, relacionadas com a operação dos sistemas de informação. Em certos casos será somente necessário actualizar os procedimentos já definidos.

Nesta actividade, deverá também ser contemplada uma definição clara de responsabilidades de monitorização dos sistemas de informação, bem como uma automatização dos procedimentos de monitorização, através da implementação de ferramentas adequadas.

II.4. Monitorização dos Processos de TI

II.4.1. *Monitorização dos Processos de TI*

Recomenda-se que sejam implementados indicadores de gestão e de monitorização para os diferentes processos de TI. As informações estatísticas destes indicadores deveram estar disponíveis para todas as entidades do ISSS, como forma de as encorajar a trabalhar por um objectivo comum de melhoria contínua da sua performance. Com a utilização destes indicadores, o ISSS assegurará que os processos de TI estão alinhados com o seu plano estratégico.

II.4.2. *Avaliação de Controlo Interno de TI*

De forma a mitigar os riscos associados a esta actividade, o SSSS deverá considerar a definição clara de quais os processos de TI que considera prioritários, bem como a implementação de uma metodologia de avaliação de riscos e controlo interno. A avaliação do controlo interno deve ser efectuada periodicamente com base em auditorias independentes.

II.4.3. *Certificação de Serviços e Sistemas*

Não existem recomendações a efectuar.



Tribunal de Contas

II.4.4. Execução de Auditorias Independentes

Recomenda-se que o ISSS deva proceder a auditorias regulares independentes aos seus processos de gestão de sistemas de informação. Considera-se que para alcançar este objectivo, o ISSS deverá:

- proceder à definição de um plano global de auditoria de sistemas, de acordo com o nível de risco associado aos vários processos bem como à prioridade da área ser auditada;
- criar competências internas ou subcontratar serviços para dar resposta às suas necessidades.

As melhorias necessárias identificadas nestas auditorias deverão ser integradas no plano de actividades das Unidades de SI consoante a sua prioridade de implementação.



Anexo D – Diferenças Detectadas nos Cálculos Manuais

N.º do Processo	Tipo de Pensão	Legislação Aplicável	Descrição do Erro
105 722 978	PV	DL n.º 329/93, de 25 de Setembro, conjugado com os DL n.º 119/99, de 14 de Abril e DL n.º 9/99, de 8 de Janeiro	<p>O valor da Pensão atribuída está <u>correcto</u>. No entanto, o cálculo respeitante ao apuramento do <i>complemento social</i> (CS), está deficientemente instruído, como seguidamente se demonstra:</p> <ul style="list-style-type: none">• Valor da <i>Pensão Estatutária</i> (PE): 22.670\$00;• Factor de redução aplicável (FR): 0,875;• Pensão (P): PE x FR = 19.840\$00. <p>Como o valor mínimo, neste caso de <i>pensão antecipada</i>, é o valor da <i>pensão social</i> (PS) – em 1999, 23.600\$00 –, ter-se-ia um CS igual à diferença entre PS e P, ou seja, 23.600\$00 – 19.840\$00 = 3.760\$00, e não o valor resultante da diferença PS e PE, 930\$00, que foi, efectivamente, o valor considerado para o cálculo.</p>
120 053 607	PV	DL n.º 329/93, de 25 de Setembro, conjugado com os DL n.º 119/99, de 14 de Abril e DL n.º 9/99, de 8 de Janeiro	<p>Foi aplicado um Factor de Redução (FR) incorrecto:</p> <ul style="list-style-type: none">• Início da P em 05/06/2000;• 56 anos de idade à data do requerimento;• 35 anos de contribuições aos 55 anos de idade;• FR aplicável: 0,865. <p>Foi aplicado um FR de 0,820.</p>
126 294 283	PV	DL n.º 329/93, de 25 de Setembro, conjugado com os DL n.º 119/99, de 14 de Abril e DL n.º 9/99, de 8 de Janeiro	<p>Foi aplicado um Factor de Redução (FR) incorrecto:</p> <ul style="list-style-type: none">• Início da P em 07/01/2000;• 56 anos à data do requerimento;• 35 anos de contribuições aos 55 anos de idade;• FR aplicável: 0,865. <p>Foi aplicado um FR de 0,910.</p>
105 120 200	PV	DL n.º 329/93, de 25 de Setembro, conjugado com os DL n.º 119/99, de 14 de Abril e DL n.º 9/99, de 8 de Janeiro	<p>Foi aplicado um Factor de Redução (FR) incorrecto:</p> <ul style="list-style-type: none">• Início da P em 25/05/2000;• 59 anos à data do requerimento;• 40 anos de contribuições aos 55 anos de idade;• FR aplicável: 1 <p>Foi aplicado um FR de 0,910.</p>



Tribunal de Contas

N.º do Processo	Tipo de Pensão	Legislação Aplicável	Descrição do Erro
018 663 061	PV	DL n.º 329/93, de 25 de Setembro, conjugado com os DL n.º 119/99, de 14 de Abril e DL n.º 9/99, de 8 de Janeiro	Foi atribuído à Pensão Estatutária (PE) o valor mínimo definido na Portaria n.º 1069/99, de 10 de Dezembro, para 34 anos de carreira contributiva (49.400\$00), com o qual se efectuou o cálculo da pensão, quando, por aplicação do disposto no n.º 5 do art.º 43.º do DL 329/93, de 25 de Setembro, estes valores "não são aplicáveis às pensões antecipadas atribuídas ao abrigo do regime de flexibilização da idade de pensões de velhice (...)", sendo o valor da PE, tão só, o que resulta do produto da taxa global pela remuneração de referência, ou seja, 41.460\$00, neste caso.
018 538 707	PV	DL n.º 329/93, de 25 de Setembro, conjugado com os DL n.º 9/99, de 8 de Janeiro e o DL n.º 195/95, de 28 de Julho	Da aplicação do n.º 1 do art.º 4.º e n.º1 e 2 do art.º 5.º do DL 195/95, de 28 de Julho, afigura-se que o beneficiário tinha direito ao complemento de mineiro. Existe um código na base de dados – "N.º anos de Mineiro" – para fazer face a estas situações, no entanto, por ausência de espaço para a inclusão de outros campos relativos a situações especiais (como no presente caso, o relativo à reforma antecipada), utiliza-se referido campo. Assim, no caso vertente, existindo as duas situações e apenas um código para a sua inclusão na base de dados, acabou por não ser incluído o complemento de mineiro a que o beneficiário tinha direito.
149 049 342	PI	DL n.º 329/93, de 25 de Setembro, conjugado com o DL 141/79, de 22 de Maio	Afigura-se não terem sido incluídos, para a efectivação do cálculo da pensão, todos os registos salariais do beneficiário – período de 1970 a 1978 –, considerando-se apenas os relativos a 1970, 1975, 1976, 1977, 1978.
105 137 423	PI	DL n.º 329/93, de 25 de Setembro	Afigura-se não terem sido incluídos, para a efectivação do cálculo da pensão, todos os registos de salários do beneficiário, descurando-se um mês de contribuições.
149 081 612	PI	DL n.º 329/93, de 25 de Setembro, conjugado com o DL n.º 169/85, de 20 de Maio e DL n.º 361/98, de 18 de Novembro	O beneficiário não tinha 24 meses de contribuições, não tendo sido aplicada, em conformidade, a pensão proporcional correspondente.
105 201 875	PI	DL n.º 329/93, de 25 de Setembro conjugado com o DL n.º 169/85, de 20 de Maio	O beneficiário não tinha 24 meses de contribuições, não tendo sido aplicada, em conformidade, a pensão proporcional correspondente.
073 206 619	PS/SM	DL n.º 322/90, de 18	



Tribunal de Contas

N.º do Processo	Tipo de Pensão	Legislação Aplicável	Descrição do Erro
		de Outubro conjugado com o Decreto Regulamentar n.º 1/94, de 18 de Janeiro	A pensão paga aos descendentes não é actualizada desde Dezembro de 2000. Esta situação ocorre dado que se trata de uma situação especial – <i>agregado familiar incompleto</i> , a companheira aguarda decisão judicial de reconhecimento da equiparação a cônjuge – e nestes casos as actualizações não são efectuadas automaticamente, havendo necessidade de elaboração de listagens com este tipo de ocorrências para, posteriormente, caso a caso, se efectuar a respectiva actualização.
105 100 580	PS	DL n.º 322/90, de 18 de Outubro	Cálculos relativos aos montantes em atraso mal efectuados.
009 242 410	SM	DL n.º 322/90, de 18 de Outubro	Foi atribuído um Subsídio por Morte de 176.100\$00, quando do cálculo resulta 170.100\$00.
029 358 080	SM	DL n.º 322/90, de 18 de Outubro	Foi atribuído um Subsídio por Morte de 382.280\$00, quando do cálculo resulta 382.800\$00.



ÍNDICE DO ANEXO

	<u>Pág.</u>
1. ARQUITECTURA DA BASE DE DADOS E RESPECTIVAS APLICAÇÕES INFORMÁTICAS.....	2
1.1. ESTRUTURA DE DADOS.....	2
1.2. APLICAÇÕES INFORMÁTICAS (SISTEMA ACTUAL).....	7
1.3. NOVO PROJECTO DE PENSÕES.....	11
2. TRAMITAÇÕES PROCESSUAIS OPERADAS NOS CDSSS REFERENTES ÀS PENSÕES.....	12
2.1. PENSÃO DE INVALIDEZ.....	13
2.1.1. <i>A requerimento do beneficiário.....</i>	<i>13</i>
2.1.2. <i>Promoção oficiosa – a partir de 365 até 1095 dias de doença subsidiada.....</i>	<i>19</i>
2.1.3. <i>Promoção oficiosa – 1095 dias de doença subsidiada.....</i>	<i>23</i>
2.2. PENSÃO DE VELHICE.....	27
2.2.1. <i>Simples.....</i>	<i>27</i>
2.2.2. <i>Articulação com o Desemprego.....</i>	<i>32</i>
3. TRAMITAÇÕES PROCESSUAIS EFECTUADAS NO CNP RELATIVAS A PENSÕES.....	36
3.1. OPERAÇÕES COMUNS NA TRAMITAÇÃO DE REQUERIMENTOS DE VELHICE E INVALIDEZ.....	37
3.1.1. <i>Descrição das operações relativas à Pensão de Invalidez.....</i>	<i>38</i>
3.1.2. <i>Descrição das operações relativas à Pensão de Velhice.....</i>	<i>42</i>
3.2. TRAMITAÇÃO DE REQUERIMENTOS DE PENSÃO DE SOBREVIVÊNCIA.....	45
3.2.1. <i>Descrição das operações relativas à Pensão de Sobrevivência.....</i>	<i>46</i>
3.3. TRAMITAÇÕES FINANCEIRAS RELATIVAS AO PAGAMENTO DE PENSÕES.....	50
3.4. TESTES.....	51



Tribunal de Contas

1. ARQUITECTURA DA BASE DE DADOS E RESPECTIVAS APLICAÇÕES INFORMÁTICAS

1.1. Estrutura de Dados

Toda a informação relacionada com os processos de atribuição e controlo de pensões, no domínio das prestações mediatas¹, cuja gestão é cometida ao CNP, nos termos do art.º 23.º do Decreto-Lei n.º 316-A/2000, de 7 de Dezembro, assenta sobre uma arquitectura Unisys DMS 2200 e está suportada fundamentalmente em duas estruturas de dados:

- ◇ **Banco Nacional de Dados de Beneficiários e Utentes (BNDBU)** que integra o **Ficheiro Central de Requerimentos (FCR)**;
- ◇ **Ficheiro de Pensionistas (FP)**.

São estruturas hierárquicas de rede, em que as relações entre os registos são estabelecidas através de *sets*, sendo um dos registos definido como *owner* (pai) e o outro (ou outros) como *member* (filho); o *owner* de um *set* pode ser também *member* doutro *set*. Os registos *member* que fazem parte dum *set* pertencem todos ao mesmo *owner* e podem ser de tipos diferentes.

Os esquemas seguintes expõem a arquitectura das bases de dados, designadamente, das relativas a:

- ◇ áreas comuns a todas as aplicações;
- ◇ beneficiários e requerentes; e
- ◇ pensionistas.

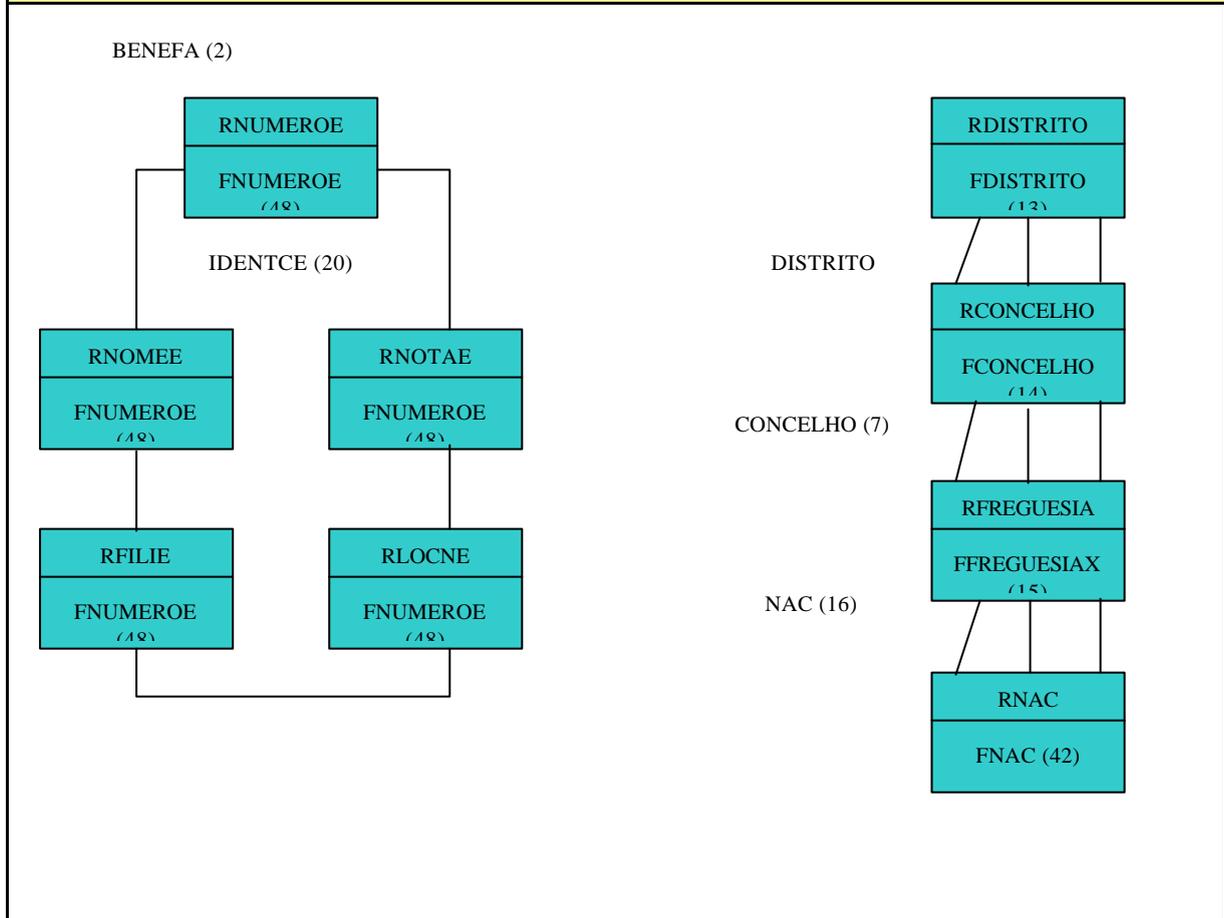
¹ Também usualmente chamadas *benefícios diferidos* por serem temporalmente posteriores ao período de contribuições dos beneficiários.

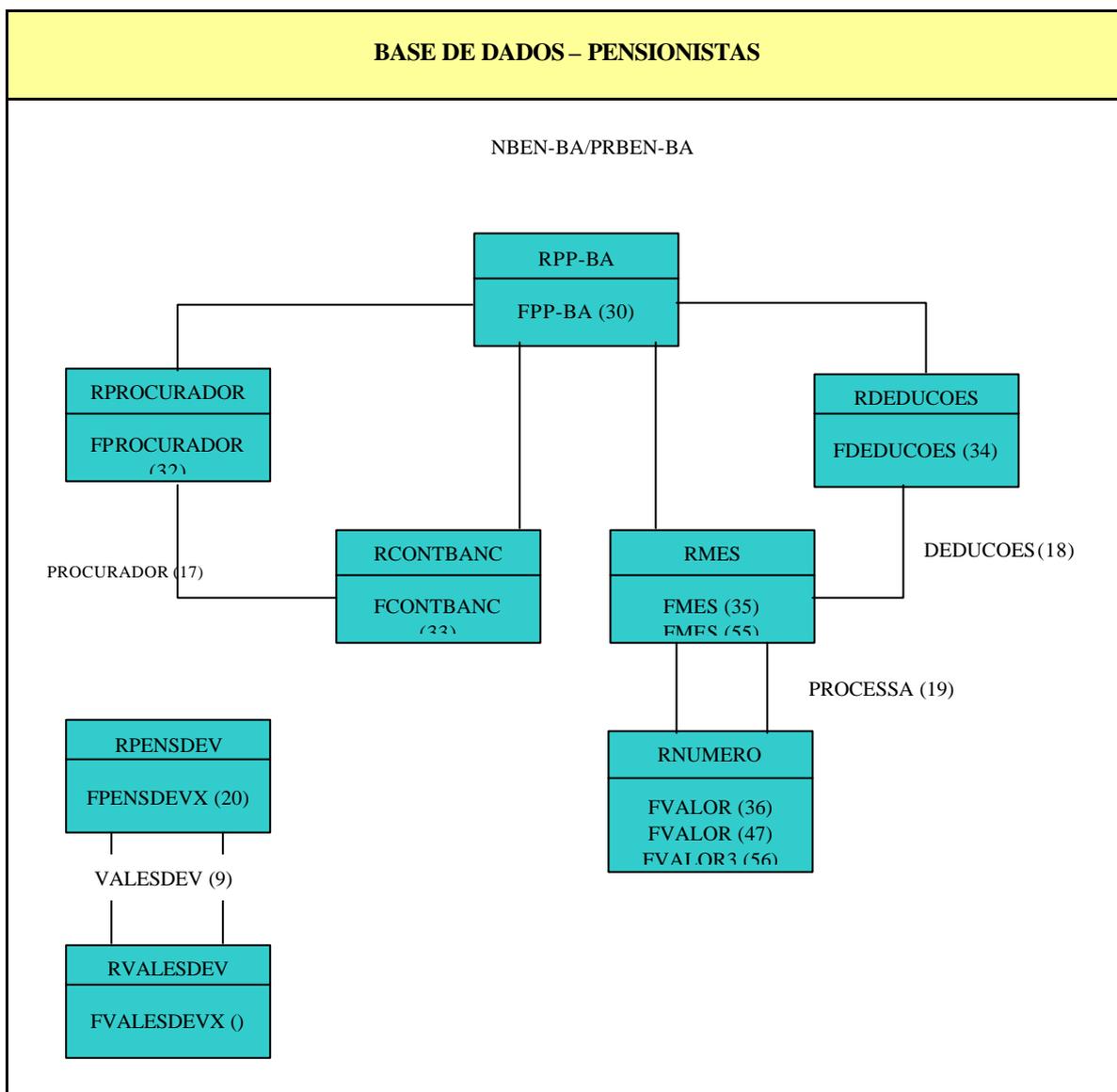


Tribunal de Contas

BASES DE DADOS – ÁREAS COMUNS A TODAS AS APLICAÇÕES

Informação complementar para beneficiários naturais de países da U.E





Além da gestão dos benefícios diferidos, o CNP é ainda responsável por:

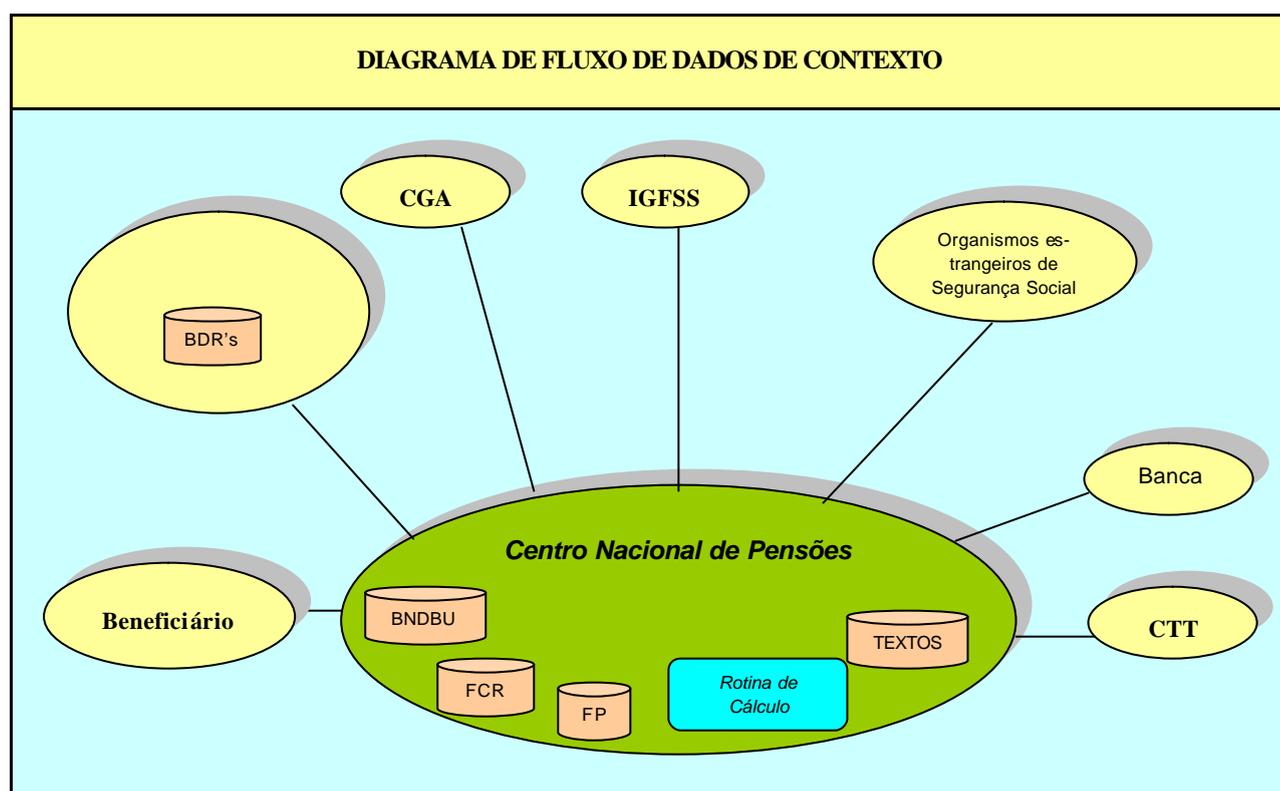
- ◇ assegurar a existência e funcionamento do BNDBU com vista a permitir, designadamente, a identificação nacional e a carreira contributiva dos pensionistas em articulação com as bases de dados regionais, bem como emitir os cartões de beneficiário e de pensionista;
- ◇ gerir a rede de transmissão de dados da sua área de intervenção.

Funcionalmente, o CNP organiza e implementa formas de protecção social relativas aos eventos de invalidez, velhice, morte e outras prestações que com elas se relacionem ou sejam determinadas pelo mesmo facto.



Tribunal de Contas

A fim de proporcionar uma visão mais geral do sistema de informação em causa, o diagrama a seguir representa o contexto do Centro Nacional de Pensões com as entidades externas com as quais interage.



O Banco Nacional de Dados de Beneficiários e Utentes (BNDBU) deve manter:

- ◇ a centralização das identificações dos beneficiários e confirmar o número nacional a atribuir;
- ◇ o registo dos salários anuais por CDSSS/ANO DE REFERÊNCIA/REGIME/CONTRIBUINTE de todos os beneficiários activos;
- ◇ actualizados todos os requerimentos de prestações diferidas.

A recolha e validação dos dados é, nos dois primeiros casos, feita por duas vias distintas: por terminal em tempo real, ou através de ficheiro com o consequente tratamento em *batch*, sendo, no último caso, unicamente em tempo real.

Pré-requisitos de gravação no Ficheiro Central de Requerentes (FCR)

- ◇ A gravação dos requerimentos no Ficheiro Central de Requerentes (FCR) deve ser precedida da confirmação no Banco Nacional de Dados de Beneficiários e Requerentes (BNDBU) da



Tribunal de Contas

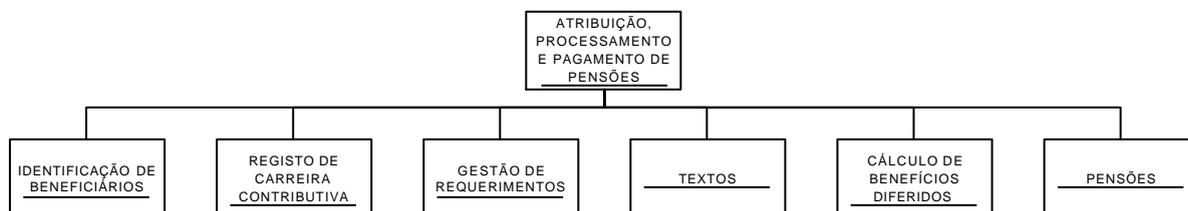
identificação (nome, naturalidade e data de nascimento) e morada do beneficiário, bem como da existência de registo de activo no número da inscrição em que se pretende gravar o requerimento;

- ◇ Estes requerimentos devem ser gravados com o Número Nacional do beneficiário;
- ◇ Caso se verifique divergência entre os elementos constantes do requerimento e do BNDBU, os Serviços Regionais de Segurança Social (CRSS) e as Caixas de Previdência (CP) devem proceder à gravação do requerimento, rectificando, posteriormente, os elementos incorrectos através de transacção adequada;
- ◇ O acesso vai transaccional ao BNDBU, para efeitos de INCLUSÃO/ALTERAÇÃO de elementos de identificação; apenas é permitido após a gravação dos requerimentos, e enquanto os mesmos se encontrarem em instrução nos CDSSS/CXS;
- ◇ A gravação dos requerimentos é efectuada através da transacção REQGR.

1.2. Aplicações Informáticas (Sistema actual)

As aplicações informáticas para atribuição e controle de benefícios são efectuadas em linguagem COBOL, sendo utilizado o DMS para as bases de dados e o TIP para as transacções.

Apresenta-se, de seguida um diagrama de decomposição funcional de 1.º nível com a identificação dos diferentes módulos aplicativos:



- ◇ O módulo **Identificação de Beneficiários**, composto por 22 programas e 12 transacções, integra as seguintes funções:
 - ◆ centralizar as identificações no BNDBU e confirmar o número nacional a atribuir;
 - ◆ disponibilizar a informação existente no BNDBU, através de consulta por terminal.



Tribunal de Contas

Nota: a recolha e validação dos dados é feita por duas vias distintas: por terminal, em tempo real; ou através de ficheiro, com o conseqüente tratamento em *batch*.

◇ O módulo **Registo de Carreira Contributiva**, composto por 10 programas e 2 transacções, integra as seguintes funções:

- ◆ registar no BNDBU os salários anuais por CR/ANO DE REFERÊNCIA/REGIME /CONTRIBUINTE DE TODOS OS BENEFICIÁRIOS ACTIVOS;
- ◆ disponibilizar a informação através de consulta por terminal.

Nota: a recolha e validação dos dados é feita por duas vias distintas: por terminal, em tempo real; ou através de ficheiro, com o conseqüente tratamento em *batch*.

◇ O módulo **Gestão de Requerimentos**, composto por 13 programas e 11 transacções, integra as seguintes funções:

- ◆ manter actualizado o BNDBU no que diz respeito a todos os requerimentos de prestações diferidas;
- ◆ disponibilizar indicadores de gestão e a informação existente através de consulta por terminal.

Nota: a actualização da informação é feita por terminal, em tempo real.

◇ O módulo **Textos**, composto por 2 programas e 4 transacções, integra as seguintes funções:

- ◆ manter actualizado um ficheiro com os ofícios padrão para correspondência com possibilidade de serem parametrizados;

Nota: o envio de um ofício é desencadeado a partir do terminal, incluindo, o operador, os parâmetros necessários.

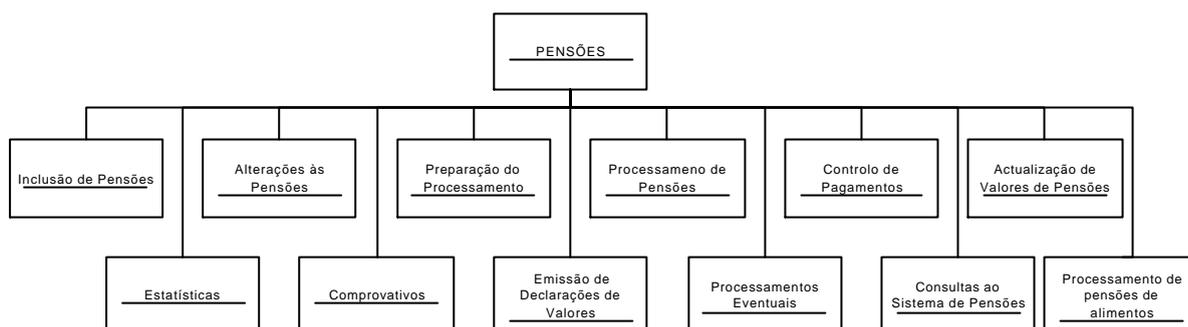
◇ O módulo **Cálculo de Benefícios Diferidos**, composto por 19 programas e 11 transacções, integra as seguintes funções:

- ◆ efectuar os cálculos dos valores das pensões, dos atrasados, das deduções, dos subsídios e complementos do regime contributivo e do regime não contributivo;
- ◆ efectuar os cálculos dos acréscimos às pensões de velhice do regime contributivo;
- ◆ efectuar os cálculos dos pagamentos por uma só vez;



Tribunal de Contas

- ◆ incluir os novos pensionistas na base de dados de pensionistas e efectuar alterações a esta base de dados;
 - ◆ disponibilizar os dados considerados no cálculo, através de consulta por terminal.
- ◇ O módulo "**Pensões**" decompõe-se, ainda, nos seguintes módulos:



- ◇ O módulo **Inclusão/Alteração**, composto por 5 programas e 32 transacções, integra a função:
- ◆ incluir/alterar, via teleprocessamento ou *batch*, todos os dados necessários ao processamento da pensão.
- ◇ O módulo **Processamento**, composto por 31 programas, integra a função:
- ◆ efectuar mensalmente o cálculo do valor a pagar e obter os *outputs* necessários ao pagamento e contabilização.
- ◇ O módulo **Controle de Pagamentos**, composto por 18 programas e 8 transacções, integra a função:
- ◆ identificar os valores que foram efectivamente recebidos.
- ◇ O módulo **Actualização dos Valores das Pensões**, composto por 8 programas, integra a função:
- ◆ proceder à alteração dos valores das pensões decorrente de legislação ou de acordos colectivos de trabalho.
- ◇ O módulo **Estatísticas**, composto por 18 programas, integra a função:



Tribunal de Contas

- ◆ obter estatísticas mensais e anuais relativas a pensionistas e valores processados de acordo com o plano de acção estatística da Segurança Social e para apoio à gestão.
- ◇ O módulo **Comprovativos**, composto por 5 programas e 1 transacção (Prova Escolar) e por 5 programas e 2 transacções (Prova P. Social), integra a função:
 - ◆ proceder à verificação do direito à pensão.
- ◇ O módulo **Emissão de Declaração de Valores**, composto por 6 programas e 1 transacção, integra a função:
 - ◆ proceder ao envio a cada pensionista e ao Ministério das Finanças dos valores pagos no ano anterior e do valor retido para IRS e, no caso dos pensionistas, do valor actual da pensão.
- ◇ O módulo **Processamentos Eventuais**, executado no ano 2000 por 60 programas diferentes, integra a função:
 - ◆ dar resposta a pedidos eventuais de informação sobre o sistema de pensões. O número é variável, dependendo dos pedidos.
- ◇ O módulo **Consultas ao Sistema de Pensões**, composto por 6 transacções, integra a função:
 - ◆ disponibilizar a informação existente no sistema de pensões através de terminal.
- ◇ O módulo **Processamento de Pensões de Alimentos**, composto por 1 programa e 1 transacção, integra a função:
 - ◆ obtenção mensal do documento de pagamento para os destinatários destas pensões, a partir do valor deduzido na pensão dos pensionistas da Segurança Social;
 - ◆ manter actualizado o ficheiro com os nomes e moradas destes destinatários.
- ◇ O módulo **Processamento dos Benefícios por uma só vez**, composto por 1 programa e 1 transacção, integra a função:
 - ◆ obtenção mensal do documento de pagamento de subsídio por morte e reembolso de despesas de funeral.



Tribunal de Contas

1.3. Novo Projecto de Pensões

O módulo **Pensões** está, no presente, a ser objecto de alterações, conforme se constata na Informação n.º 099/MTC/2000, de 09/11/00, e que consubstancia o que se designa por "Novo Projecto de Pensões".

Este novo projecto visa permitir, com a introdução de novas funcionalidades, que o tratamento dos dados seja feito no sentido de possibilitar a consulta por pensionista, e não por pensão (concepção actual), com vista a aglutinar todo o processamento de benefícios diferidos devidos a um único pensionista num determinado período de tempo.

Presentemente, este projecto está na Etapa IV (1.ª fase) – processamentos paralelos com a base de dados real –, tendo-se previsto inicialmente que a fase de passagem à produção se concretizasse em Novembro do corrente ano, conforme o cronograma aprovado, constante da Informação n.º 521 de 30/11/00.

Não obstante, a acta da 48.ª reunião de Gestão do Projecto “Aplicação de Pensões” refere que *“(...) face ao atraso verificado [impossibilidade de aceitação do primeiro paralelo] e à situação actual do desenvolvimento, a Unisys considera esta meta não exequível (...)”*, pelo que o Centro Nacional de Pensões, no sentido de ultrapassar os inconvenientes daí resultantes, designadamente, no que se refere à questão da conformidade do sistema ao "EURO", irá proceder à adaptação dos programas (rotinas de cálculo) do actual sistema em exploração, montando também, no mesmo sentido, o plano de contingência para o período do final do ano.



2. TRAMITAÇÕES PROCESSUAIS OPERADAS NOS CDSSS REFERENTES ÀS PENSÕES

Na sequência das alterações legislativas ao regime de protecção nas eventualidades de invalidez e velhice do regime geral, nomeadamente no que se refere à antecipação da idade de acesso à pensão de velhice de alguns grupos profissionais, foram efectuadas revisões e actualizações do Manual de Procedimentos de Pensões elaborado pela ex- Direcção-Geral dos Regimes de Segurança Social (DGRSS) e pelo Centro Nacional de Pensões (CNP), com a colaboração dos ex-Centros Regionais de Segurança Social (CRSS).

Assim, foi constituído, pelo Despacho n.º 47-I/SESSRL/99, de 20 de Agosto, um Grupo de Trabalho com representantes da DGRSS, CNP, e CRSS do Centro e de LVT, para além da colaboração dos restantes CRSS. Deste trabalho resultou um novo manual de procedimentos de pensões que inclui a informação sobre os circuitos e os procedimentos administrativos, integrando os meios necessários à correcta aplicação de legislação e à harmonização de procedimentos.

Por reflectirem matérias intimamente relacionadas com o trabalho a realizar, posteriormente, no CNP, achou-se pertinente transpor para o presente relato as descrições constantes desse manual, designadamente, das referentes às operações realizadas pelos actuais CDSSS em matéria de tratamento, quer processual, quer informático, das pensões de velhice e invalidez e das particularidades a elas subjacentes².

Para uma melhor compreensão dos circuitos operacionais implementados, apresentam-se, em primeiro lugar, os fluxogramas³ onde se enumeram os processos em curso em cada uma das operações; seguidamente, explicitam-se, em detalhe, as operações subjacentes a cada um desses procedimentos.

² Pensão de Invalidez:

- A requerimento do beneficiário;
- Promoção oficiosa – a partir de 365 até 1095 dias de doença subsidiada;
- Promoção oficiosa – 1095 dias de doença subsidiada.
- Pensão de velhice:
- Simple;
- Articulada com o desemprego.

NOTA: No Manual de Procedimentos mencionado não estão representados os procedimentos relativos à pensão de sobrevivência.

³ Veja-se simbologia no ANEXO I e glossário das transacções informáticas no ANEXO II.



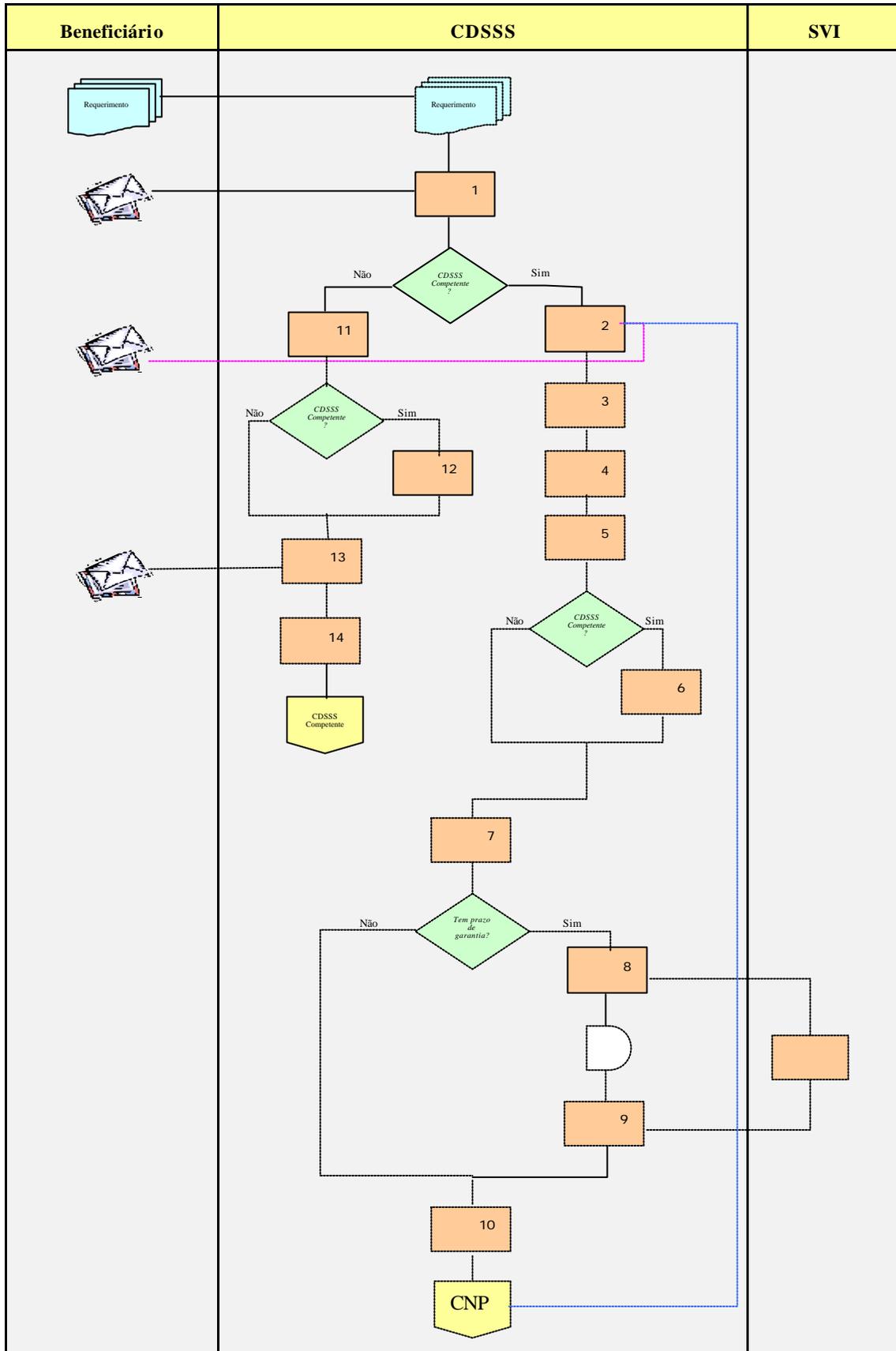
Tribunal de Contas

2.1. Pensão de Invalidez

2.1.1. A requerimento do beneficiário



Tribunal de Contas





Descrição das Operações	Transação Informática
<p>1. REGISTA ENTRADA E PASSA RECIBO</p> <p>Recebe e regista entrada do requerimento de pensão de Invalidez (Mod. CNP 211 587) e demais documentação e passa recibo comprovativo da sua entrega presencial. No caso de envio por via postal, a devolução do recibo verificar-se-á se o requerente tiver remetido sobrescrito endereçado e franquiado.</p> <p>SE <i>o requerimento não for entregue no CDSSS da área da residência procede às operações descritas no processo 11 e seguintes</i></p> <p>2. VERIFICA E CONFERE DOCUMENTOS</p> <p>Verifica e confere elementos identificativos e demais documentos, designadamente:</p> <ul style="list-style-type: none">◇ Fotocópia do Bilhete de Identidade;◇ Fotocópia do Bilhete de Identidade do rogado, no caso de requerimento assinado a rogo;◇ Fotocópia do cartão de contribuinte (n.º de identificação fiscal);◇ Informação médica – Mod. SVI 007/99 – DGRSS;◇ Declaração da actividade exercida – Mod. RP5023 – DGRSS;◇ Questionário⁴;◇ Fotocópia dos documentos comprovativos do serviço militar obrigatório (caderneta militar ou certidão da Direcção de Recrutamento Militar (DRM), no caso daquela prova não ter sido efectuada;◇ Declaração – Mod. CNP 501 590 (para os casos de incapacidade com responsabilidade de terceiros).◇ Constatando haver falta de algum elemento, solicita ao beneficiário a sua entrega/esclarecimento. <p>SE <i>o pedido for de pensão unificada e o beneficiário apresentar o último período contributivo na Caixa Geral de Aposentações, remete, após gravação no FCR, o respectivo requerimento, bem como a documentação que o acompanhar, ao CNP, para desenvolvimento dos procedimentos administrativos adequados.</i></p> <p>3. CONSULTA BNDBU / BDR / FCR / FP</p> <ul style="list-style-type: none">◇ Confirma que o beneficiário ainda não é pensionista;◇ Verifica se existe registo em FCR em como o beneficiário faltou ou não foi considerado com incapacidade permanente, pela CVIP, há menos de um ano;◇ Confirma (mediante fotocópia do BI e requerimento):<ul style="list-style-type: none">■ Nome;	<p>NOM HST PNS NUMP NUMQ NUMR</p>

⁴ Aplicável apenas aos trabalhadores com carreira contributiva nos países da UE. Verificando-se a falta deste questionário, deve o mesmo ser enviado ao beneficiário, com a indicação de devolução directa ao CNP.



Descrição das Operações	Transação Informática
<ul style="list-style-type: none">▪ Data de nascimento;▪ Naturalidade;▪ Morada. <p>◇ Valida n.º nacional de beneficiário.</p> <p>SE o beneficiário não constar ou não estiver activo na BDR, cria registo com número de contribuinte fictício (960 000).</p> <p>4. GRAVA FCR</p> <p>◇ Regista informação adequada, de acordo com as normas de gravação.</p> <p>5. ACTUALIZA CARREIRA CONTRIBUTIVA</p> <p>◇ Insere / actualiza no BNDBU as remunerações dos anos relevantes para o cálculo da pensão e confirma a sua coerência com a BDR, no caso de nesta existirem remunerações relevantes;</p> <p>◇ Actualiza, no BNDBU, período(s) de situações especiais, nomeadamente do serviço militar obrigatório, se for caso disso;</p> <p>◇ Havendo registo de remunerações por equivalência, designadamente por doença, maternidade ou desemprego, procede ao registo dessa informação no FCR de acordo com as normas de gravação.</p> <p>SE não existirem períodos contributivos noutros CDSSS procede às operações descritas no processo 7 e seguintes</p> <p>6. PEDE ACTUALIZAÇÃO DE CARREIRA CONTRIBUTIVA</p> <p>◇ Emite o ofício n.º 200 252 e /ou n.º 200 037, da base de textos, solicitando aos CDSSS a actualização, no BNDBU, de períodos contributivos ou de registo de remunerações.</p> <p>7. VERIFICA EXISTÊNCIA DE PRAZO DE GARANTIA</p> <p>◇ Verifica a existência de prazo de garantia;</p> <p>◇ Tendo o requerente carreira contributiva nos países da UE, procede às operações subsequentes se o mesmo apresentar registo de remunerações em Portugal por período igual ou superior a 12 meses.</p> <p>SE o beneficiário não tiver prazo de garantia procede às operações descritas no processo 10.</p>	<p>REQGR 1IN</p> <p>SALAR (remunerações até 31/12/93) SAL94 (remunerações a partir de 01/01/94) IDA REQSD</p> <p>WTX</p>



Descrição das Operações	Transação Informática
<p>8. ENVIA SVI</p> <ul style="list-style-type: none">◇ Solicita a realização de exame médico ao SVI da área de residência do beneficiário;◇ Se existir registo em FCR em como o beneficiário faltou ou não foi considerado com incapacidade permanente, pela CVIP, há menos de um ano, o pedido de exame médico deve salientar este facto, por forma a que o mesmo só seja efectuado se o médico relator considerar devidamente fundamentado o agravamento do estado do beneficiário. <p>9. RECEBE E ANALISA RESULTADO DO SVI</p> <ul style="list-style-type: none">◇ Recebe e analisa a informação recebida do SVI:<ul style="list-style-type: none">▪ Comunicação da deliberação da CVIP;▪ Comunicação da não realização do exame médico por falta injustificada do requerente;▪ Comunicação da não realização do exame médico por não se ter concluído do especial agravamento do estado de saúde do requerente. <p>10. ACTUALIZA FCR E REMETE AO CNP</p> <ul style="list-style-type: none">◇ Introduce data da deliberação da CVIP;◇ Emite ofício n.º 300 142 da base de textos;◇ Se tiver sido solicitado ao beneficiário o questionário – Mod. CNP 501 458 – remete, também, ao CNP, cópia desse pedido;◇ Tratando-se de beneficiário com carreira contributiva nos países da UE, o processo deve ser acompanhado do relatório do médico relator, dos elementos auxiliares de diagnóstico e dos relatórios de especialidade;◇ Envia processo ao CNP para apreciação do direito à prestação. <p>11. CONSULTA BNDBU / BDR / FCR / FP</p> <ul style="list-style-type: none">◇ Confirma que o beneficiário ainda não é pensionista;◇ Confirma (mediante fotocópia do BI e requerimento):<ul style="list-style-type: none">▪ Nome;▪ Data de nascimento;▪ Naturalidade;▪ Morada.◇ Valida n.º nacional de beneficiário;◇ Se o beneficiário constar da BDR, insere / actualiza no BNDBU os períodos contributivos e/ou remunerações, de acordo com as normas de gravação des-	<p>REQJM WTX</p> <p>NOM HST PNS NUMP NUMQ NUMR</p>

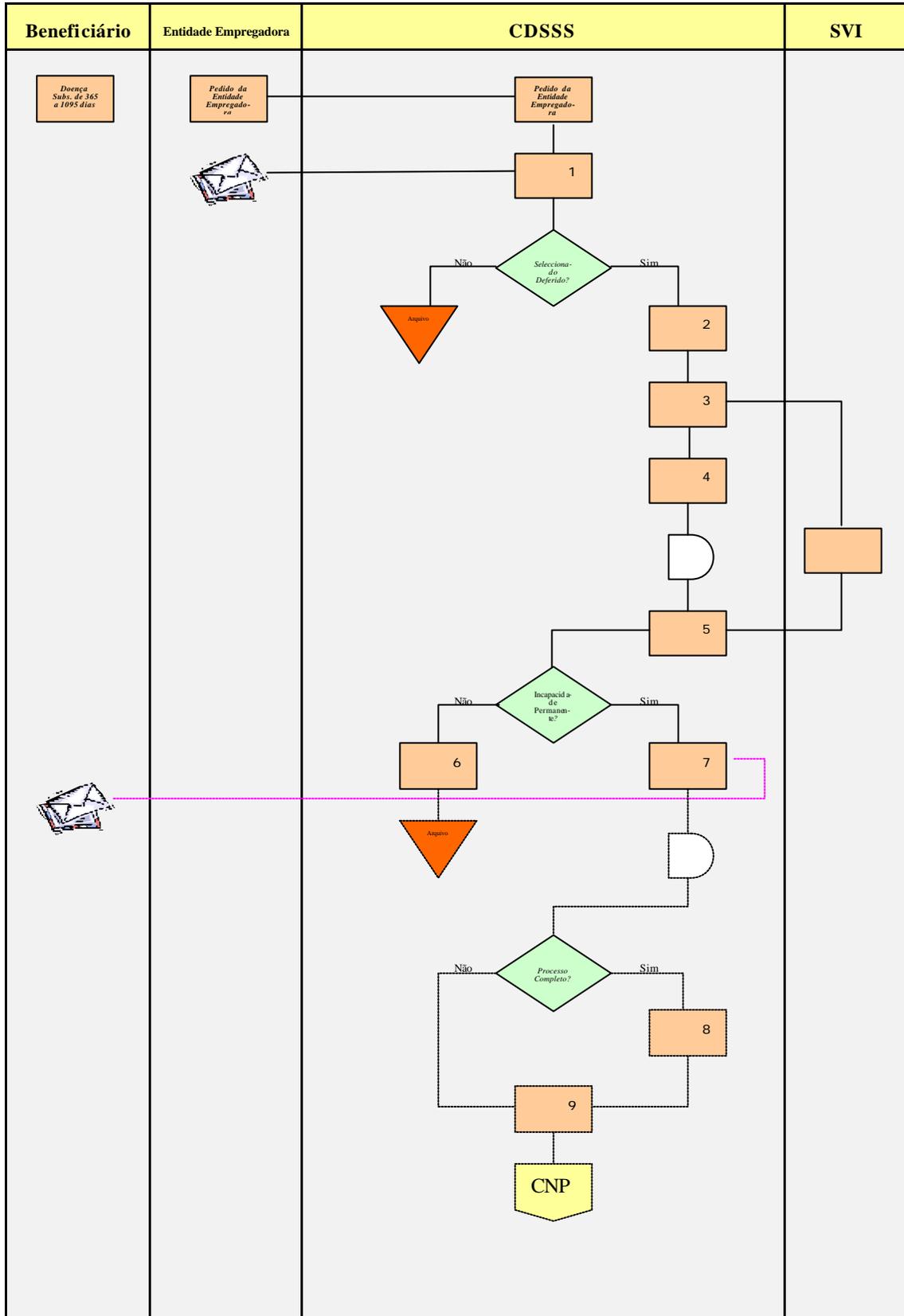


Tribunal de Contas

Descrição das Operações	Transação Informática
<p>descritas no processo 5.</p> <p>SE não puder gravar o requerimento, procede às operações descritas no processo 13 e seguinte</p> <p>12. GRAVA FCR</p> <ul style="list-style-type: none">◇ Regista a informação adequada, de acordo com as normas de gravação. <p>13. INFORMA TRANSFERÊNCIA</p> <ul style="list-style-type: none">◇ Emite ofício informando da transferência do processo:<ul style="list-style-type: none">▪ Ofício n.º 300 143 da base de textos, se o requerimento tiver sido gravado;▪ Ofício manual, em caso contrário. <p>14. ENVIA PARA CENTRO DISTRITAL COMPETENTE</p> <ul style="list-style-type: none">◇ Emite ofício N.º 200 144 da base de textos;◇ Transfere processo.	<p>REQGR 1 IN</p> <p>WTX</p> <p>WTX</p>



2.1.2. Promoção oficiosa – a partir de 365 até 1095 dias de doença subsidiada





Descrição das Operações	Transação Informática
<p>1. SELECCIONA DEFERE/INDEFERE PEDIDO</p> <ul style="list-style-type: none">◇ Selecciona beneficiários tendo em atenção os critérios estabelecidos na Norma IV (caso de promoção oficiosa) do Despacho 94/SESS/90, de 4/12, que reunam, cumulativamente, os seguintes requisitos (art.º 34.º do DL n.º 132/88, de 20/4, na redacção dada pelo DL n.º 287/90, de 19/9 e art.º 42.º do DL n.º 360/97, de 17/12):<ul style="list-style-type: none">▪ Tenham prazo de garantia para a atribuição de pensão de invalidez;▪ Não tenham registo em FCR em como o beneficiário faltou ou não foi considerado com incapacidade permanente, pela CVIP, há menos de um ano (art.º 64.º do DL n.º 360/97, de 17/12).◇ Analisa o pedido da entidade empregadora no sentido de ser verificada a incapacidade permanente do trabalhador, cuja incapacidade temporária, pelo seu carácter prolongado e reiterado, faça supor a existência de situações invalidantes (art.º 35.º do DL n.º 132/88, de 20/4, na redacção dada pelo DL n.º 287/90, de 19/9 e Despacho 94/SESS/90, de 4/12);◇ Informa a entidade empregadora do deferimento ou indeferimento. <p>SE o pedido da entidade empregadora for indeferido comunica-lhe esta informação e arquiva o processo.</p> <p>2. GRAVA FCR</p> <ul style="list-style-type: none">◇ Regista a informação adequada, de acordo com as normas de gravação, com a data de requerimento fictícia (9999 99 99);◇ Emite ofício manual, acompanhado de informação médica – Mod. SVI 007/99-DGRSS, e:<ul style="list-style-type: none">▪ Ofício n.º 900 411 ou ofício n.º 900 242 da base de textos <p>SE o beneficiário não devolver a informação médica, a avaliação da incapacidade é efectuada com os elementos disponíveis</p> <p>3. ENVIA SVI</p> <ul style="list-style-type: none">◇ Solicita a realização de exame médico ao SVI da área da residência do beneficiário. <p>4. ACTUALIZA CARREIRA CONTRIBUTIVA</p>	<p>REQGR 1LB</p> <p>WTX</p> <p>SALAR (remunerações até 31/12/93) SAL94</p>



Descrição das Operações	Transação Informática
<p>◇ Insere / actualiza no BNDBU as remunerações dos anos relevantes para o cálculo da pensão e confirma a sua coerência com a BDR, no caso de nesta existirem remunerações relevantes;</p> <p>◇ Actualiza, no BNDBU, período(s) de situações especiais, nomeadamente do serviço militar obrigatório, se for caso disso;</p> <p>◇ Havendo registo de remunerações por equivalência, designadamente por doença, maternidade ou desemprego, procede ao registo dessa informação no FCR de acordo com as normas de gravação.</p> <p>5. RECEBE E ANALISA RESULTADO DO SVI</p> <p>◇ Recebe e analisa informação recebida do SVI:</p> <ul style="list-style-type: none">▪ Comunicação da deliberação da CVIP;▪ Comunicação da não realização do exame médico por falta injustificada do requerente. <p>SE foi confirmada a incapacidade permanente do beneficiário procede às operações descritas no processo 7 e seguintes.</p> <p>6. ACTUALIZA FCR</p> <p>◇ Introduce data da deliberação da CVIP;</p> <p>◇ Introduce código de encerramento do não reconhecimento da incapacidade permanente;</p> <p>◇ Emite ofício n.º 300 273 da base de textos;</p> <p>SE não foi confirmada a incapacidade permanente do beneficiário, remete, ao serviço que solicitou a verificação da incapacidade e ao serviço processador do subsídio de doença, a informação recebida do SVI</p> <p>7. SOLICITA ELEMENTOS AO BENEFICIÁRIO</p> <p>◇ Envia o requerimento de pensão de invalidez – Mod. CNP211 587 – no qual foi previamente aposta a data de requerimento igual à data da incapacidade fixada pela CVIP, indicando, igualmente, o prazo de 30 dias para a sua devolução (art.º 8.º da Portaria n.º 833/94, de 17/9).</p> <p>SE não se verificar a devolução do requerimento, procede às operações descritas no processo 9</p> <p>8. GRAVA FCR</p>	<p>(remunerações a partir de 01/01/94)</p> <p>IDA</p> <p>REQENC REQJM WTX</p> <p>REQENC (Cod.B) REQENC</p>



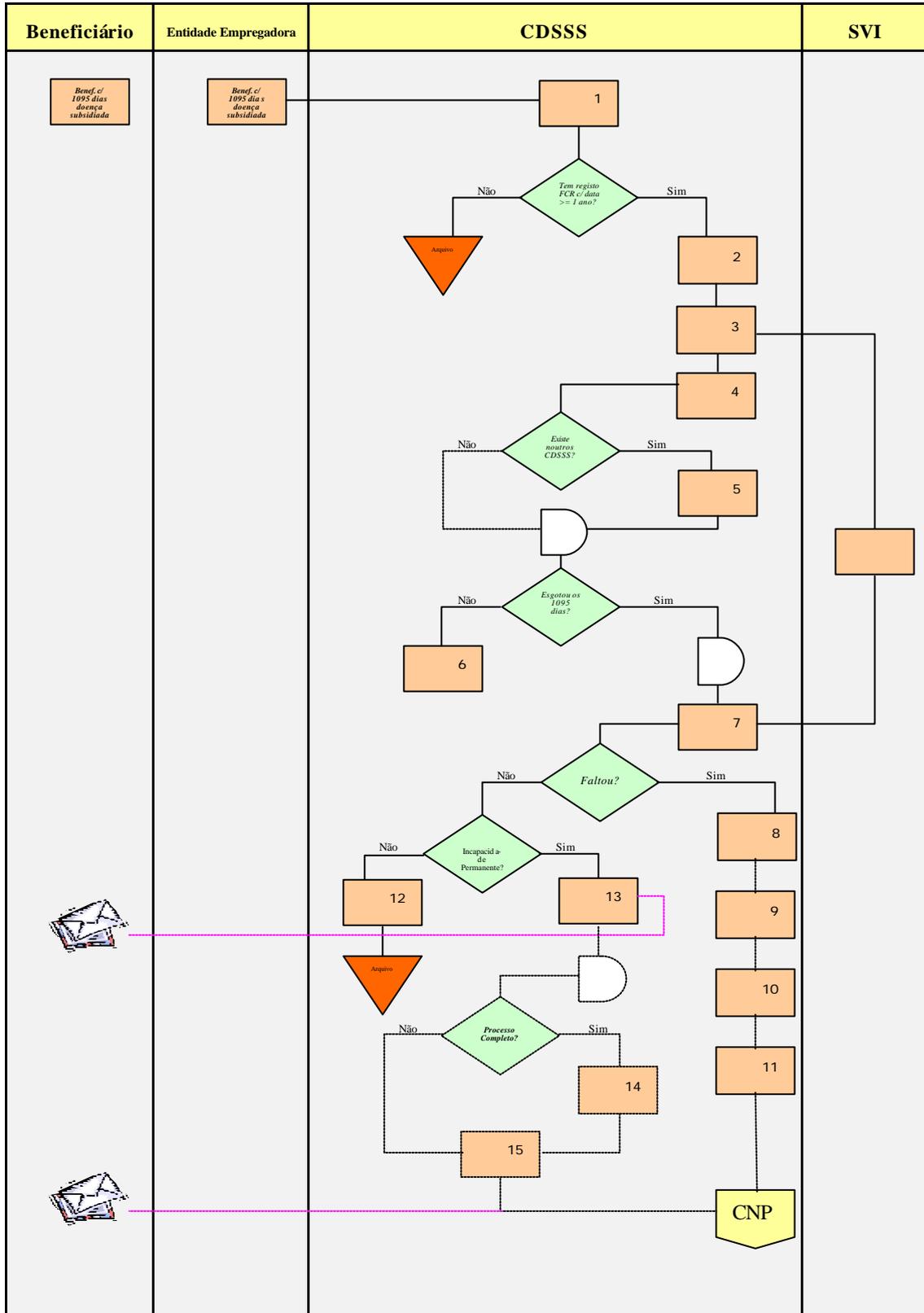
Tribunal de Contas

Descrição das Operações	Transação Informática
<ul style="list-style-type: none">◇ Anula o requerimento/registo 1LB gravado no processo 2;◇ Procede ao registo do requerimento de pensão em FCR de acordo com as normas de gravação. <p>9. ACTUALIZA FCR REMETE AO CNP</p> <ul style="list-style-type: none">◇ Introduce data da deliberação da CVIP;◇ Emite ofício n.º 300 142 da base de textos;◇ Se o beneficiário tiver carreira contributiva nos países da UE envia-lhe o questionário – Mod. CNP 501 458 – com indicação de devolução directa ao CNP;◇ Tratando-se de beneficiário com carreira contributiva nos países da UE, o processo deve ser acompanhado do relatório do médico relator, dos elementos auxiliares de diagnóstico e dos relatórios de especialidade;◇ Se existir carreira contributiva noutra CDSSS emite ofício n.º 200 252 e/ou n.º 200 037 da base de textos, solicitando ao CDSSS a actualização da BNDBU, de períodos contributivos ou de registo de remunerações◇ Envia processo ao CNP para apreciação do direito à prestação.	REQJM WTX



Tribunal de Contas

2.1.3. Promoção oficiosa – 1095 dias de doença subsidiada





Descrição das Operações	Transação Informática
<p>1. CONSULTA FCR</p> <ul style="list-style-type: none">◇ Verifica se existe em FCR em como o beneficiário faltou ou não foi considerado com incapacidade permanente, pela CVIP, há menos de um ano;◇ Se existir registo em FCR, nas condições referidas, o processo de promoção oficiosa de invalidez não é desencadeado;◇ Verifica se existe registo de requerimento de pensão de invalidez. <p>2. GRAVA FCR (data 1096 dias)</p> <ul style="list-style-type: none">◇ Regista a informação adequada, de acordo com as normas de gravação, com data de requerimento igual ao 1096.º dia de doença subsidiada⁵;◇ Emite ofício manual acompanhado de informação médica – Mod. SVI 007/99 –DGRSS. <p>SE o beneficiário não devolver a informação médica, a avaliação da incapacidade é efectuada com os elementos disponíveis.</p> <p>3. ENVIA SVI</p> <ul style="list-style-type: none">◇ Solicita a realização de exame médico ao SVI da área de residência do beneficiário;◇ Se existir registo de requerimento de pensão de invalidez, efectuado por outro CDSSS, solicita ao mesmo que lhe dê conhecimento do resultado da CVIP. <p>4. ACTUALIZA CARREIRA CONTRIBUTIVA</p> <ul style="list-style-type: none">◇ Insere / actualiza no BNDBU as remunerações dos anos relevantes para o cálculo da pensão e confirma a sua coerência com a BDR, no caso de nesta existirem remunerações relevantes;◇ Actualiza, no BNDBU, período(s) de situações especiais, nomeadamente do serviço militar obrigatório, se for caso disso;◇ Havendo registo de remunerações por equivalência, designadamente por doença, maternidade ou desemprego, procede ao registo dessa informação no FCR de acordo com as normas de gravação. <p>SE não existirem períodos contributivos noutros CDSSS procede às operações descritas:</p>	<p>NUMP NUMQ NUMR</p> <p>REQGR 1LB</p> <p>SALAR (remunerações até 31/12/93) SAL94 (remunerações até 31/12/93) IDA</p>

⁵ Nesta situação há lugar à emissão automática de ofício, da base de textos, a informar o beneficiário do pagamento da pensão provisória por limite de doença subsidiada.



Descrição das Operações	Transação Informática
<p>➤ No processo 6 se o beneficiário não tiver esgotado os 1095 dias;</p> <p>➤ No processo 7 e seguintes em caso contrário.</p> <p>5. PEDE ACTUALIZAÇÃO DE CARREIRA CONTRIBUTIVA</p> <p>◇ Emite ofício n.º 200 252 e/ou n.º 200 037 da base de textos, solicitando aos CDSSS a actualização, no BNDBU, de períodos contributivos ou de registo de remunerações</p> <p>6. ACTUALIZA FCR / INFORMA SVI</p> <p>◇ Actualiza FCR por forma a impedir o processamento da pensão provisória e informa SVI para suspender a realização de exame médico.</p> <p>7. RECEBE E ANALISA RESULTADO DO SVI</p> <p>◇ Recebe e analisa informação recebida do SVI:</p> <ul style="list-style-type: none">▪ Comunicação da deliberação da CVIP;▪ Comunicação da não realização do exame médico por falta injustificada do requerente. <p>SE o beneficiário faltou injustificadamente, procede às operações descritas nos processos 8 a 11;</p> <p>SE o beneficiário foi considerado incapaz permanentemente, procede às operações descritas nos processos 13 a 15;</p> <p>SE não foi confirmada a incapacidade permanente do beneficiário, procede às operações descritas no processo 12.</p> <p>8. CALCULA DÉBITO / GRAVA FICHEIRO DE DÉBITOS</p> <p>◇ Calcula débito correspondente aos valores de pensão provisória de invalidez que tenham sido pagos;</p> <p>◇ Insere registo desse valor no Ficheiro de Débitos</p> <p>9. ACTUALIZA FCR/FP E CESSA PAGAMENTO DA PENSÃO PROVISÓRIA</p> <p>◇ Rectifica o código de encerramento para não reconhecimento da incapacidade permanente;</p> <p>◇ Cessa o pagamento da pensão provisória;</p> <p>◇ Introduce data da deliberação da CVIP.</p>	<p>WTX</p> <p>REQENC (Opção anulação)</p> <p>PNS CONCOR LPROG DEDINC</p> <p>REQJM REQENC SUSP</p>



Descrição das Operações	Transação Informática
<p>10. INFORMA BENEFICIÁRIO DA CESSAÇÃO E DÉBITO</p> <ul style="list-style-type: none">◇ Emite ofício n.º 400 254 da base de textos, indicando o montante do débito a repor, relativo às prestações recebidas indevidamente, nos termos do n.º 3, art.º 72.º do DL n.º 329/93, de 25/9. <p>11. REMETE AO CNP</p> <ul style="list-style-type: none">◇ Envia o processo ao CNP, acompanhado dos seguintes documentos:<ul style="list-style-type: none">▪ Declaração do SVI em como o beneficiário faltou à convocatória;▪ Fotocópia da convocatória do SVI ou do aviso de recepção;▪ Declaração com indicação do período de doença subsidiada. <p>12. ACTUALIZA FCR/FP</p> <ul style="list-style-type: none">◇ Introduce / rectifica o código de encerramento para não reconhecimento da incapacidade permanente;◇ Suspende pensão provisória;◇ Emite ofício n.º 400 202 ou n.º 300 236, da base de textos, ao beneficiário;◇ Introduce data da deliberação da CVIP. <p>13. SOLICITA ELEMENTOS AO BENEFICIÁRIO</p> <ul style="list-style-type: none">◇ Envia o requerimento de pensão de invalidez – Mod. CNP211 587 – no qual foi previamente aposta a data de requerimento igual à data da incapacidade fixada pela CVIP, indicando, igualmente, o prazo de 30 dias para a sua devolução (art.º 8.º da Portaria n.º 833/94, de 17/9). <p>SE não se verificar a devolução do requerimento, procede às operações descritas no processo 15</p> <p>14. GRAVA FCR</p> <ul style="list-style-type: none">◇ Anula o requerimento / registo 1LB gravado no processo 2, caso o mesmo não esteja encerrado com DEFERIDO;◇ Procede ao registo do requerimento de pensão em FCR, de acordo com as normas de gravação. <p>15. ACTUALIZA FCR / FP e REMETE AO CNP</p> <ul style="list-style-type: none">◇ Introduce data da deliberação da CVIP;	<p>WTX</p> <p>REQENC REQJM SUSP WTX</p> <p>REQENC REQGR 1IN</p>



Tribunal de Contas

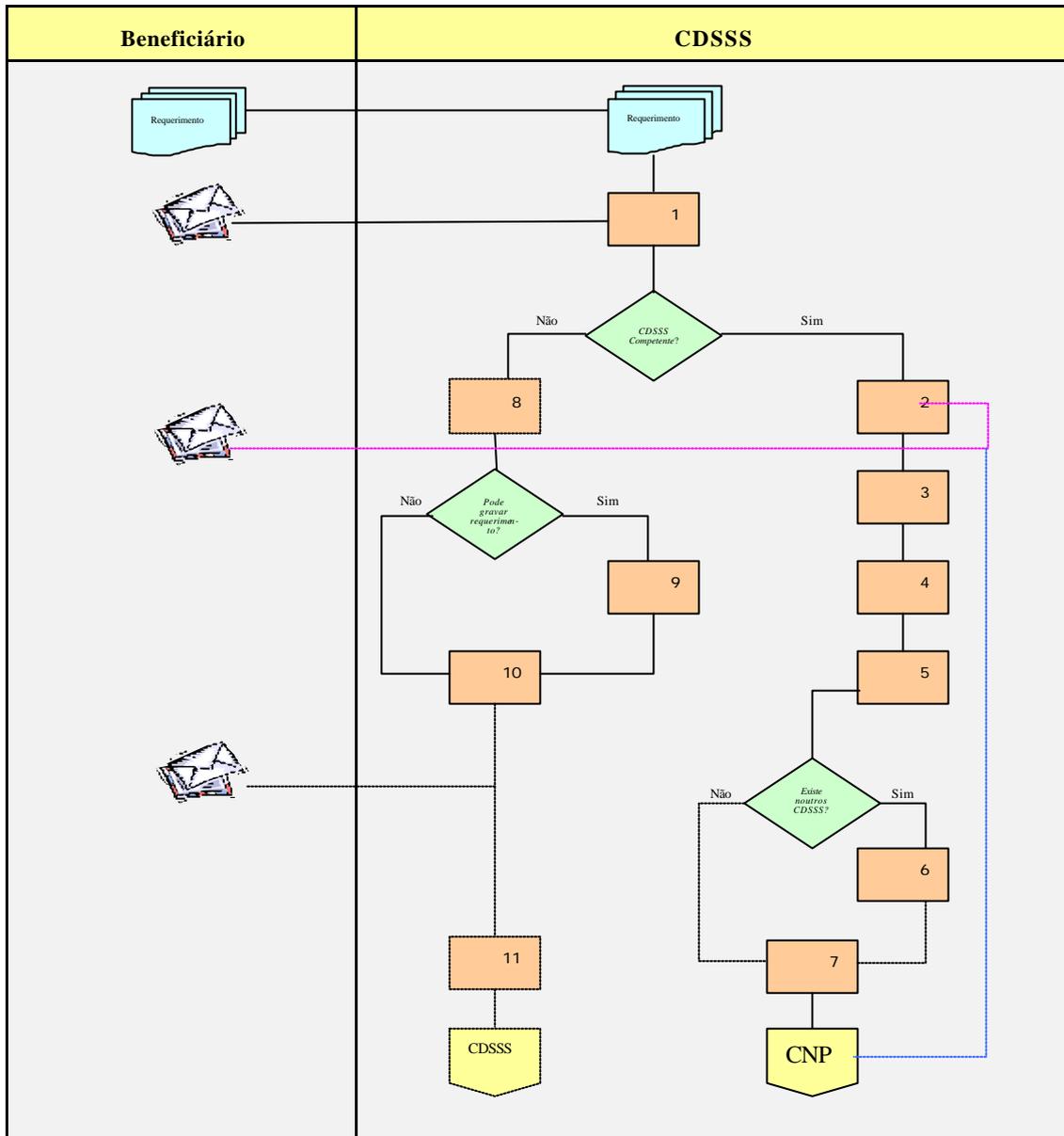
Descrição das Operações	Transação Informática
<ul style="list-style-type: none">◇ Emite ofício n.º 300 142 da base de dados;◇ Se o beneficiário tiver carreira contributiva nos países da UE, envia questionário – Mod. CNP 501 458 – com a indicação de devolução directa ao CNP;◇ Tratando-se de beneficiário com carreira contributiva nos países da UE o processo deve ser acompanhado do relatório do médico relator, dos elementos auxiliares de diagnóstico e dos relatórios de especialidade;◇ Envia processos ao CNP para apreciação do direito à prestação.	REQJM XTX

2.2. Pensão de Velhice

2.2.1. *Simplex*



Tribunal de Contas





Descrição das Operações	Transação Informática
<p>1. REGISTA ENTRADA E PASSA RECIBO</p> <p>Recebe e regista entrada do requerimento de pensão de Velhice (Mod. CNP 211. 587) e demais documentação e passa recibo comprovativo da sua entrega presencial. No caso de envio por via postal, a devolução do recibo verificar-se-á se o requerente tiver remetido sobrescrito endereçado e franquiado.</p> <p>SE <i>o requerimento não for entregue no CDSSS da área da residência procede às operações descritas no processo 8 e seguintes</i></p> <p>2. VERIFICA E CONFERE DOCUMENTOS</p> <p>Verifica e confere elementos identificativos e demais documentos, designadamente:</p> <ul style="list-style-type: none">◇ Fotocópia do Bilhete de Identidade;◇ Fotocópia do Bilhete de Identidade do rogado, no caso de requerimento assinado a rogo;◇ Fotocópia do cartão de contribuinte (n.º de identificação fiscal);◇ Declaração da actividade exercida – Mod. RP5023 – DGRSS;◇ Questionário⁶;◇ Fotocópia dos documentos comprovativos do serviço militar obrigatório (caderneta militar ou certidão da Direcção de Recrutamento Militar (DRM), no caso daquela prova não ter sido efectuada;◇ Outros documentos comprovativos de situações especiais de antecipação da idade de acesso à Pensão de Velhice;◇ Constatando haver falta de algum elemento, solicita ao beneficiário a sua entrega/esclarecimento. <p>SE <i>o pedido for de pensão unificada e o beneficiário apresentar o último período contributivo na Caixa Geral de Aposentações, remete, após gravação na FCR, o respectivo requerimento, bem como a documentação que o acompanhar, ao CNP, para desenvolvimento dos procedimentos administrativos adequados.</i></p> <p>3. CONSULTA BNDBU / BDR / FCR / FP</p> <ul style="list-style-type: none">◇ Confirma que o beneficiário ainda não é pensionista nem requerente de pensão;◇ Confirma (mediante fotocópia do BI e requerimento):<ul style="list-style-type: none">■ Nome;■ Data de nascimento;	<p>NOM HST PNS NUMP NUMO NUMR</p>

⁶ Aplicável apenas aos trabalhadores com carreira contributiva nos países da UE. Verificando-se a falta deste questionário, deve o mesmo ser enviado ao beneficiário, com a indicação de devolução directa ao CNP.



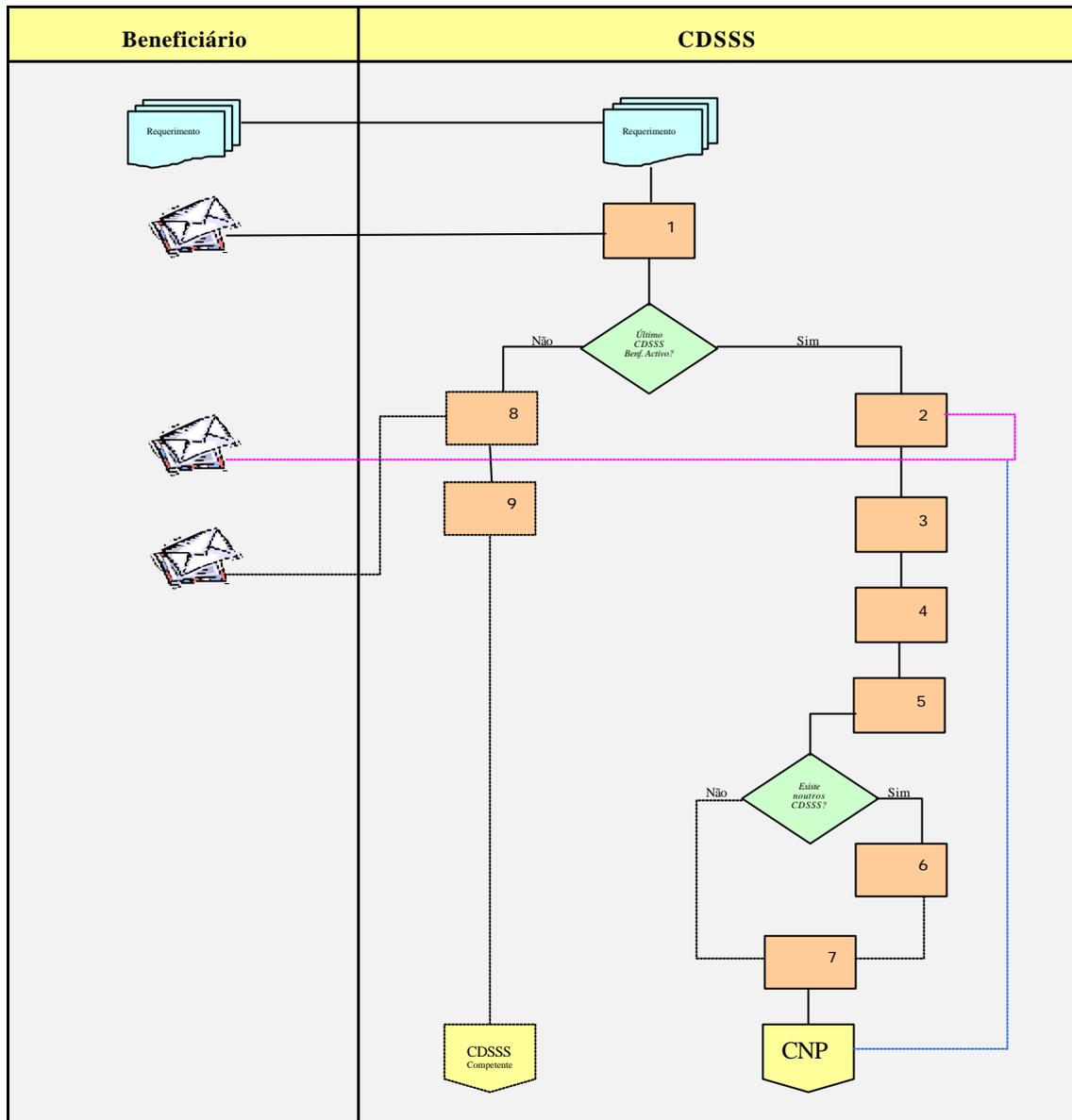
Descrição das Operações	Transação Informática
<ul style="list-style-type: none">▪ Naturalidade;▪ Morada. <p>◇ Valida n.º nacional de beneficiário.</p> <p>SE o beneficiário não constar ou não estiver activo na BDR, cria registo com número de contribuinte fictício (960 000).</p> <p>4. GRAVA FCR</p> <p>◇ Regista informação adequada, de acordo com as normas de gravação.</p> <p>5. ACTUALIZA CARREIRA CONTRIBUTIVA</p> <p>◇ Insere / actualiza no BNDBU as remunerações dos anos relevantes para o cálculo da pensão e confirma a sua coerência com a BDR, no caso de nesta existirem remunerações relevantes;</p> <p>◇ Actualiza, no BNDBU, período(s) de situações especiais, nomeadamente do serviço militar obrigatório, se for caso disso;</p> <p>◇ Havendo registo de remunerações por equivalência, designadamente por doença, maternidade ou desemprego, procede ao registo dessa informação no FCR de acordo com as normas de gravação.</p> <p>SE não existirem períodos contributivos noutros CDSSS procede às operações descritas no processo 7 e seguintes</p> <p>6. PEDE ACTUALIZAÇÃO DE CARREIRA CONTRIBUTIVA</p> <p>◇ Emite o ofício n.º 200 252 e /ou n.º 200 037, da base de textos, solicitando aos CDSSS a actualização, no BNDBU, de períodos contributivos ou de registo de remunerações.</p> <p>7. ACTUALIZA FCR / REMETE CNP</p> <p>◇ Emite ofício n.º 300 142 da base de textos;</p> <p>◇ Se tiver sido solicitado ao beneficiário o questionário – Mod. CNP 501 458 – remete, também, ao CNP, cópia desse pedido;</p> <p>◇ Envia processo ao CNP para apreciação do direito à prestação.</p> <p>NOTA: no caso de não estarem disponíveis elementos que confirmem a existência de prazo de garantia, mas se presume que o mesmo possa ser completado até ao mês de entrada do requerimento, o processo só deve ser remetido ao CNP depois de verificada aquela presunção.</p>	<p>REQGR 1VE</p> <p>SALAR (remunerações até 31/12/93) SAL94 (remunerações a partir de 01/01/94) IDA REQSD</p> <p>WTX</p> <p>WTX</p>



Descrição das Operações	Transação Informática
<p>8. CONSULTA BNDBU/BDR/FCR/FP</p> <ul style="list-style-type: none">◇ Confirma que o beneficiário ainda não é pensionista;◇ Confirma (mediante fotocópia do BI e requerimento):<ul style="list-style-type: none">▪ Nome;▪ Data de nascimento;▪ Naturalidade;▪ Morada.◇ Valida n.º nacional de beneficiário;◇ Se o beneficiário constar da BDR, insere / actualiza no BNDBU os períodos contributivos e/ou remunerações.	NOM HST PNS NUMP NUMO NUMR
<p>SE não puder gravar o requerimento, procede às operações descritas nos processos 10 e 11.</p>	
<p>9. GRAVA FCR</p> <ul style="list-style-type: none">◇ Regista a informação adequada, de acordo com as normas de gravação.	REQGR 1VE
<p>10. INFORMA TRANSFERÊNCIA</p> <ul style="list-style-type: none">◇ Emite ofício informando da transferência do processo:<ul style="list-style-type: none">▪ Ofício n.º 300 143 da base de textos, se o requerimento tiver sido gravado;▪ Ofício manual, em caso contrário.	WTX
<p>11. ENVIA PARA CDSSS COMPETENTE</p> <ul style="list-style-type: none">◇ Emite ofício N.º 200 144 da base de textos;◇ Transfere processo.	WTX



2.2.2. Articulação com o Desemprego





Descrição das Operações	Transação Informática
<p>1. REGISTA ENTRADA E PASSA RECIBO</p> <p>Recebe e regista entrada do requerimento de pensão de Velhice (Mod. CNP 211 587) e demais documentação e passa recibo comprovativo da sua entrega presencial. No caso de envio por via postal, a devolução do recibo verificar-se-á se o requerente tiver remetido sobrescrito endereçado e franquiado.</p> <p>SE o requerimento não for entregue no CDSSS da área da residência – CDSSS competente⁷ – procede às operações descritas no processo 8 e seguinte</p> <p>2. VERIFICA E CONFERE DOCUMENTOS</p> <p>Verifica e confere elementos identificativos e demais documentos, designadamente:</p> <ul style="list-style-type: none">◇ Fotocópia do Bilhete de Identidade;◇ Fotocópia do Bilhete de Identidade do rogado, no caso de requerimento assinado a rogo;◇ Fotocópia do cartão de contribuinte (n.º de identificação fiscal);◇ Declaração da actividade exercida – Mod. RP5023 – DGRSS;◇ Questionário⁸;◇ Fotocópia dos documentos comprovativos do serviço militar obrigatório (caderneta militar ou certidão da Direcção de Recrutamento Militar (DRM), no caso daquela prova não ter sido efectuada;◇ Constatando haver falta de algum elemento, solicita ao beneficiário a sua entrega/esclarecimento. <p>3. CONSULTA BNDBU / BDR / FCR / FP</p> <ul style="list-style-type: none">◇ Confirma que o beneficiário ainda não é pensionista nem requerente de pensão;◇ Confirma (mediante fotocópia do BI e requerimento):<ul style="list-style-type: none">▪ Nome;▪ Data de nascimento;▪ Naturalidade;▪ Morada.◇ Valida n.º nacional de beneficiário. <p>4. GRAVA FCR</p>	<p>NOM HST PNS NUMP NUMQ NUMR</p>

⁷ Nos termos do n.º 3 da Norma 6.ª, da Portaria n.º 833/94, de 17/09, que regulamenta os procedimentos das pensões.

⁸ Aplicável apenas aos trabalhadores com carreira contributiva nos países da UE. Verificando-se a falta deste questionário, deve o mesmo ser enviado ao beneficiário, com a indicação de devolução directa ao CNP.



Descrição das Operações	Transação Informática
<p>◇ Regista informação adequada, de acordo com as normas de gravação.</p>	REQGR 1VE
<p>5. ACTUALIZA CARREIRA CONTRIBUTIVA</p> <p>◇ Insere / actualiza no BNDBU as remunerações dos anos relevantes para o cálculo da pensão e confirma a sua coerência com a BDR, no caso de nesta existirem remunerações relevantes;</p> <p>◇ Actualiza, no BNDBU, período(s) de situações especiais, nomeadamente do serviço militar obrigatório, se for caso disso;</p> <p>◇ Havendo registo de remunerações por equivalência, designadamente por doença, maternidade ou desemprego, procede ao registo dessa informação no FCR de acordo com as normas de gravação.</p> <p>NOTA: informa CNP do último dia com direito ao Subsídio de desemprego ou Social de Desemprego.</p>	SALAR (remunerações até 31/12/93) SAL94 (remunerações a partir de 01/01/94) IDA REQSD
<p>SE não existirem períodos contributivos noutros CDSSS procede às operações descritas no processo 7 e seguintes</p>	
<p>6. PEDE ACTUALIZAÇÃO DE CARREIRA CONTRIBUTIVA</p> <p>◇ Emite o ofício n.º 200 252 e /ou n.º 200 037, da base de textos, solicitando aos CDSSS a actualização, no BNDBU, de períodos contributivos ou de registo de remunerações.</p>	WTX
<p>7. ACTUALIZA FCR / REMETE CNP</p> <p>◇ Emite ofício n.º 300 142 da base de textos;</p> <p>◇ Se tiver sido solicitado ao beneficiário o questionário – Mod. CNP 501 458 – remete, também, ao CNP, cópia desse pedido;</p> <p>◇ Envia processo ao CNP para apreciação do direito à prestação.</p>	WTX
<p>8. INFORMA TRANSFERÊNCIA</p> <p>◇ Emite ofício informando da transferência do processo:</p> <ul style="list-style-type: none">▪ Ofício n.º 300 143 da base de textos, se o requerimento tiver sido gravado;▪ Ofício manual, em caso contrário.	WTX
<p>9. ENVIA PARA CDSSS COMPETENTE</p> <p>◇ Emite ofício N.º 200 144 da base de textos;</p>	WTX



Tribunal de Contas

Descrição das Operações	Transação Informática
◇ Transfere processo.	



3. TRAMITAÇÕES PROCESSUAIS EFECTUADAS NO CNP RELATIVAS A PENSÕES

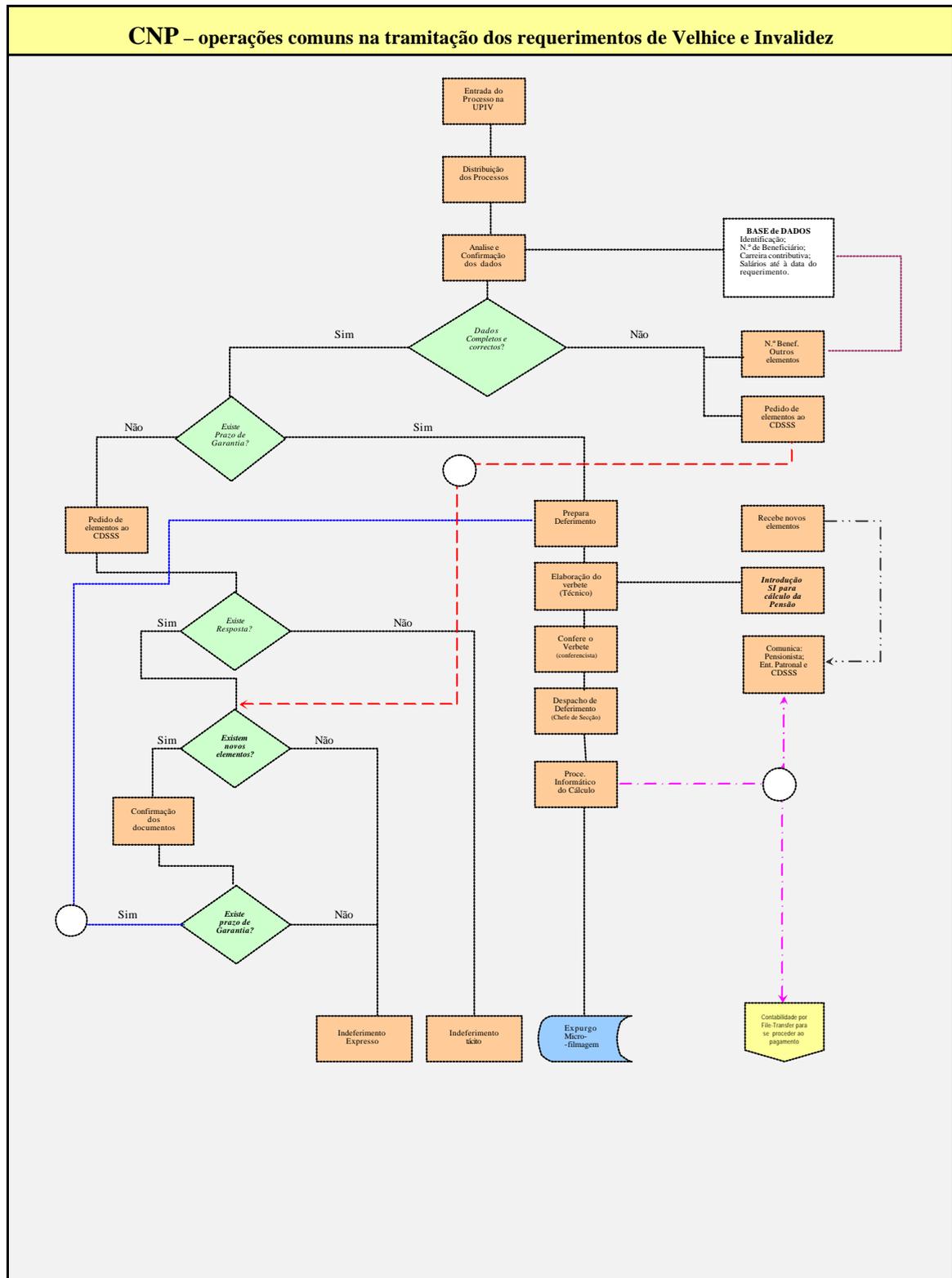
Para se ter uma ideia precisa dos procedimentos subjacentes à instrução dos requerimentos de pensão de velhice, invalidez e sobrevivência, apresentam-se, em primeiro lugar, os fluxogramas onde se expõem as tramitações operadas, subjacentes a cada uma das referidas pensões⁹ e, de seguida, descrevem-se, detalhadamente, os processos (operacionais e informáticos¹⁰), com base nos levantamentos efectuados *in loco* e nos manuais de procedimentos em vigor no CNP:

⁹ No caso da Pensão de Invalidez e Velhice apresentam-se as tramitações efectuadas num único fluxograma, visto os procedimentos fundamentais serem comuns.

¹⁰ Não se encontram exaustivamente descritas as transacções informáticas subjacentes a cada uma das operações. Para uma leitura mais detalhada vejam-se os manuais de procedimentos do CNP relativos às três modalidades de pensões aqui tratadas.



3.1. Operações comuns na tramitação de requerimentos de Velhice e Invalidez





Tribunal de Contas

As operações prévias executadas na tramitação dos requerimentos de velhice e invalidez, ao nível das Unidades Operacionais, atrás descritas, até à sua entrada no CNP são, essencialmente, as seguintes:

- A. O requerimento¹¹ é **apresentado** pelos interessados junto do CDSSS¹² da sua área de residência;
- B. Depois de suficientemente **instruído**, o CDSSS efectua a **gravação** no FCR e **remete o processo** ao CNP acompanhado de protocolo;
- C. O processo é **recepcionado** no serviço de Recepção de Correspondência, que **registra informaticamente** a sua entrada e faz a sua **distribuição**, por n.º de beneficiário ou país de residência, pelos serviços das Unidades Operacionais competentes.

3.1.1. Descrição das operações relativas à Pensão de Invalidez

Descrição das Operações	Transações Informáticas
<p>1. RECEBE E ANALISA OS DOCUMENTOS CONSTANTES DO PROCESSO;</p> <p>2. CONSULTA¹³ A BDNBU – FCR – FP E CONFIRMA OS DADOS NECESSÁRIOS:</p> <ul style="list-style-type: none">◆ Nome, data de nascimento, naturalidade, morada, n.º fiscal de contribuinte;◆ Inscrições registadas, situação de pensionistas, existência (ou não) de processos microfilmados, descodifica o nome de todos os contribuintes existentes.	NOM, HST, FRG, PNS, ALTPNS, LMIC, CNT, NUMP, NUMQ, NUMR, WTX, REQGR

¹¹ Quando for apresentado ao CNP, este deverá remetê-lo ao CDSSS competente.

¹² Entidade responsável pela instrução inicial dos processos, à excepção dos residentes no estrangeiro e dos abrangidos por instrumentos internacionais, cujo requerimento deverá ser apresentado directamente aos serviços do CNP.

¹³ Se o requerimento não está correctamente preenchido, procura regularizá-lo;

Se o requerimento deu entrada directamente no CNP (residente no estrangeiro), efectua a sua gravação no FCR.

¹⁴ Até 31 de Dez. de 1993 – ver art.º 101 n.º 1 do DL n.º 329/93

A partir de 1 de Janeiro de 1994 – ver art.º 15.º e 16.º do citado diploma.



Tribunal de Contas

Descrição das Operações	Transações Informáticas
<p>Se necessário:</p> <p>2.1. Actualiza a BDNBU;</p> <ul style="list-style-type: none">◆ Se o requerente não tem n.º nacional, selecciona-o e preenche data de admissão;◆ Se tem mais de um n.º nacional, solicita desnacionalização ao NTI (através do CNP 221 621). <p>2.2. Actualiza a carreira contributiva, solicitando os dados aos CDSSS (através de ofícios 200 096, 200 156, 200 252).</p>	<p>IDN</p> <p>WTX</p> <p>WTX</p>
<p>3. CONFERE A EXISTÊNCIA DE PRAZO DE GARANTIA¹⁴</p>	
<p>Se não existe prazo de garantia:</p> <p>3.1. Notifica o beneficiário (ofício 300 309)</p> <ul style="list-style-type: none">◆ Se há novos elementos, solicita-se actualização da carreira contributiva;◆ Se não há novos elementos, preenche mod. CNP 211 602, para despacho » indeferimento expresso, emite ofício 300 331 e envia para microfilmagem. <p>3.2. Não existindo resposta » indeferimento tácito e envia para microfilmagem.</p>	<p>WTX</p> <p>REQENC WTX</p>
<p>4. ANALISA A DELIBERAÇÃO DO CVIP E RESPECTIVAS NOTIFICAÇÕES</p>	
<p>4.1. Analisa a deliberação:</p> <ul style="list-style-type: none">◆ Se o requerente faltou ao exame médico sem justificação, arquiva requerimento, preenche mod. CNP 211 602 para despacho, emite ofício e procede às operações para microfilmagem;◆ Se não foi confirmado o agravamento do estado de saúde do requerente; se este foi considerado apto; se foi considerado incapaz por acidente de trabalho, por doença profissional, por acidente de viação (todas estas situações, que constituem ou razão de indeferimento do requerimento ou afectam o valor da pensão a ser processado, obrigam sempre à notifica-	<p>REQENC WTX</p> <p>REQENC WTX</p>



Descrição das Operações	Transações Informáticas
<p>notificação do requerente, da intenção de indeferir o requerimento, ou à solicitação de dados adicionais junto do próprio ou de entidades terceiras, determinando a suspensão do processo).</p> <p>4.2. Analisa notificações</p> <ul style="list-style-type: none">◆ Se não existe resposta no prazo estipulado, é dado indeferimento tácito, encerra com código P e envia para microfilmagem;◆ Se existe resposta fora do prazo, é preenchido o mod. CNP 211 602, para indeferimento expresso, encerra com código I, emite ofício 300 301 e procede às operações para microfilmagem;◆ Se existe resposta sem indicação de médico ou sem relatório médico (residente no estrangeiro), preenche mod. CNP 211 602, para indeferimento expresso, emite ofício 300 331 e procede às operações para microfilmagem;◆ Se dentro do prazo, solicita CPIV de recurso ao CDSSS, emite ofício e aguarda o parecer. <p>4.3. Analisa as deliberações sobre os recursos</p> <ul style="list-style-type: none">◆ Da reavaliação do processo pode resultar:<ul style="list-style-type: none">■ Deferimento, nos termos do ponto 5;■ Arquivamento, procedendo-se ao preenchimento do mod. 211 602, à introdução do código de encerramento e ao envio para a microfilmagem;■ Indeferimento expresso, procedendo-se ao preenchimento do mod. 211 602, à introdução do código de encerramento, à emissão de ofício e ao envio para a microfilmagem. <p>5. DEFERIMENTO DO PROCESSO</p> <p>5.1. Preenche formulário para despacho (CNP 211 559);</p> <p>5.2. Preenche verbete de cálculo (CNP 502 483);</p> <p>5.3. Encerra com o código D.</p> <p>6. PROCEDE AO CÁLCULO E PROCESSAMENTO DA PENSÃO</p> <p>6.1. Cálculo:</p>	<p>REQENC</p> <p>REQENC WTX</p> <p>REQENC WTX</p> <p>REQENC WTX</p> <p>REQENC WTX</p> <p>REQENC WTX</p> <p>REQENC WTX</p> <p>REQENC</p>



Descrição das Operações	Transações Informáticas
<ul style="list-style-type: none">◆ Pensão provisória;◆ Pensão definitiva;◆ Com suspensão de pensão. <p>6.2. São emitidos automaticamente os seguintes ofícios:</p> <ul style="list-style-type: none">◆ Comunicação ao pensionista do deferimento da pensão (definitiva – CNP 108 400; provisória – CNP 108 408);◆ Comunicação ao <u>CDSSS</u> para suspensão de eventuais subsídios de doença ou desemprego – CNP 100 700;◆ Comunicação de retenção de IRS (CNP 103 500 e CNP 103 700);◆ Comunicação à entidade patronal da passagem à situação de pensionista – CNP 102 300. <p>6.3. Recálculo da pensão provisória, sempre que existam novos elementos relevantes:</p> <p>6.3.1. Analisa e trata os novos elementos, preenchendo formulário para despacho e verbete de cálculo (ver ponto 5);</p> <p>6.3.2. Proceda às operações descritas nos pontos 6.1 e 6.2.</p> <p>7. EXPURGO PARA MICROFILMAGEM</p> <p>7.1 Os processos concluídos, com cálculo definitivo, são expurgados e enviados para o serviço competente para se proceder à respectiva microfilmagem.</p>	ELCAL



3.1.2. Descrição das operações relativas à Pensão de Velhice

Descrição das Operações	Transações Informáticas
<p>1. RECEBE E ANALISA OS DOCUMENTOS CONSTANTES DO PROCESSO</p> <p>2. CONSULTA¹⁵ A BDNBU – FCR – FP E CONFIRMA OS DADOS NECESSÁRIOS:</p> <ul style="list-style-type: none">◆ Nome, data de nascimento, naturalidade, morada, n.º fiscal de contribuinte;◆ Inscrições registadas, situação de pensionistas, existência (ou não) de processos microfilmados, descodifica o nome de todos os contribuintes existentes. <p>Se necessário:</p> <p>2.1. Actualiza a BDNBU;</p> <ul style="list-style-type: none">◆ Se o requerente não tem n.º nacional, selecciona-o e preenche data de admissão;◆ Se tem mais de um n.º nacional, solicita desnacionalização ao NTI (através do CNP 221.621). <p>2.2. Actualiza a carreira contributiva, solicitando os dados aos CDSSS (através de ofícios 200 096, 200 156, 200 252).</p> <p>3. VERIFICA A IDADE¹⁶ DO REQUERENTE</p> <p>3.1. Se não tem idade para requerer a pensão, preenche mod. 211 601 e notifica beneficiário através de ofício 300 307;</p>	<p>NOM, HST, FRG, PNS, ALTPNS, LMIC, CNT, NUMP, NUMQ, NUMR, WTX, REQGR</p> <p>IDN</p> <p>WTX</p> <p>WTX</p>

¹⁵ Se o requerimento não está correctamente preenchido, procura regularizá-lo;

Se o requerimento deu entrada directamente no CNP (residente no estrangeiro), efectua a sua gravação no FCR.

¹⁶ Ver art.º 22º e 103.º, do DL n.º 329/93.

¹⁷ Até 31 de Dez. de 1993 – ver art.º 101 n.º 1 do DL n.º 329/93

A partir de 1 de Jan. de 1994 – ver art.º 15.º e 16.º do citado diploma.



Descrição das Operações	Transações Informáticas
<p>3.2. Em resposta à notificação:</p> <ul style="list-style-type: none">◆ Se a resposta tiver fundamento, confere prazo de garantia;◆ Se não tiver fundamento, prepara indeferimento expresso, preenchendo mod. 211 602, encerra com o código I, emite ofício 300 331 e procede às operações de microfilmagem;◆ Se não houver resposta no prazo estipulado, implica indeferimento tácito, encerramento com o código T e procede às operações para microfilmagem.	REQENC WTX
<p>4. CONFERE A EXISTÊNCIA DE PRAZO DE GARANTIA¹⁷</p> <p>4.1. Se não existe prazo de garantia, preenche mod. 211 601 para despacho, notifica o beneficiário (ofício 300 308) e aguarda resposta;</p> <p>4.2. Se existe prazo de garantia para invalidez mas não para velhice, preenche mod. 211 601 para despacho, notifica o beneficiário (ofício 300 310) e aguarda resposta.</p> <p>4.3. Resposta dos notificados:</p> <ul style="list-style-type: none">◆ Se há novos elementos, solicita-se actualização da carreira contributiva junto das instituições competentes;◆ Se não há novos elementos, preenche mod. CNP 211 602, para despacho de indeferimento expresso, encerra com o código I, emite ofício 300 331 e envia para microfilmagem.◆ Não existindo resposta ou a resposta não altera a situação, resulta o indeferimento tácito, encerra com o código T e envia para microfilmagem.	REQENC WTX WTX WTX REQENC WTX
<p>5. DEFERIMENTO DO PROCESSO</p> <p>5.1. Preenche formulário para despacho (CNP 211 559);</p> <p>5.2. Preenche verbete de cálculo (CNP 502 483);</p> <p>5.3. Encerra com o código D.</p>	REQENC
<p>6. PROCEDE AO CÁLCULO E PROCESSAMENTO DA PENSÃO</p> <p>6.1. Cálculo:</p>	REQENC

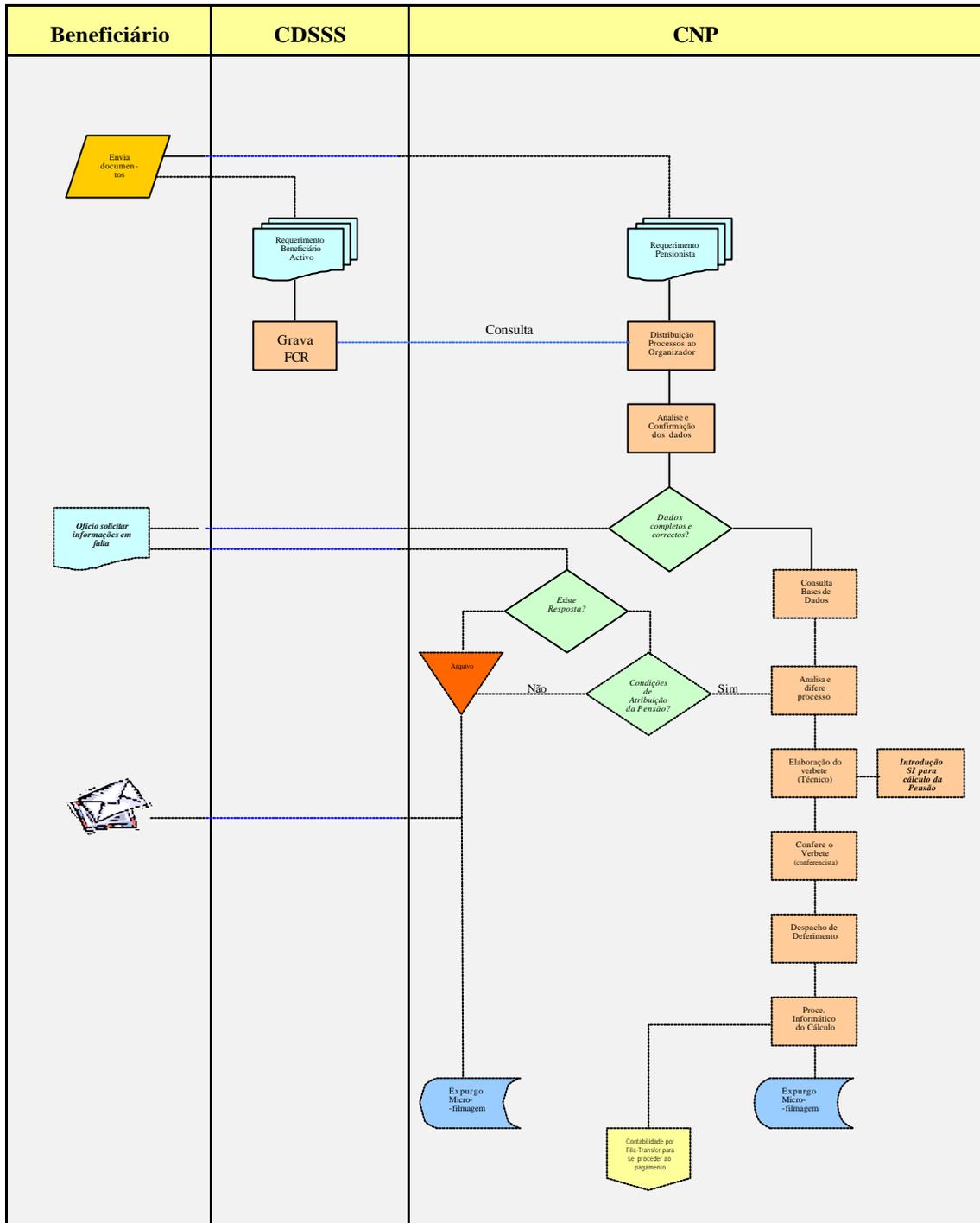


Tribunal de Contas

Descrição das Operações	Transações Informáticas
<ul style="list-style-type: none">▪ Pensão provisória;▪ Pensão definitiva;▪ Com suspensão de pensão. <p>6.2. São emitidos automaticamente os seguintes ofícios:</p> <ul style="list-style-type: none">◆ Comunicação ao pensionista do deferimento da pensão (definitiva – CNP 108 400; provisória – CNP 108 408);◆ Comunicação ao <u>CDSSS</u> para suspensão de eventuais subsídios de doença ou desemprego – CNP 100 700;◆ Comunicação de retenção de IRS (CNP 103 500 e CNP 103 700);◆ Comunicação à entidade patronal da passagem à situação de pensionista – CNP 102 300 <p>6.3. Recálculo da pensão provisória, sempre que existam novos elementos relevantes:</p> <p>6.3.1. Analisa e trata os novos elementos, preenchendo formulário para despacho e verbete de cálculo (ver ponto 5);</p> <p>6.3.2. Procede às operações descritas nos pontos 6.1 e 6.2.</p> <p>7. EXPURGO PARA MICROFILMAGEM</p> <p>7.1 Os processos concluídos, com cálculo definitivo, são expurgados e enviados para o serviço competente para se proceder à respectiva microfilmagem.</p>	ELCAL



3.2. Tramitação de requerimentos de Pensão de Sobrevivência





Tribunal de Contas

As operações prévias relativas a esta pensão diferem das duas anteriores. Neste caso o processo desenvolve-se da seguinte forma:

A. A recepção do requerimento dentro do CNP efectua-se por dois sectores:

- ◆ No Serviço Informativo “Entrega de Documentos” – para entregas feitas pelos próprios (ou seus mandatários) e no caso do beneficiário ter falecido na situação de pensionista.
 - A correspondência é conferida, autenticada e registada.
- ◆ Na Secção de “Expediente I”, por protocolo – para pedidos remetidos pelos CDSSS e no caso do beneficiário ter falecido na situação de activo ou pensionista.
 - É efectuado registo de entrada via terminal.

B. O processo é **distribuído** pelos Serviços de Benefícios Diferidos, conforme tabela existente¹⁸.

3.2.1. Descrição das operações relativas à Pensão de Sobrevivência

Descrição das Operações	Transações Informáticas
<p>1. RECEBE E ANALISA OS DOCUMENTOS CONSTANTES DO PROCESSO;</p> <ul style="list-style-type: none">◆ Elabora a capa do processo (mod. CNP 502 004) e ordena a documentação apensa ao requerimento (mod. CNP 211 020)	
<p>2. VERIFICA A INTEGRALIDADE E EXACTIDÃO DOS DADOS DO REQUERIMENTO E DA DOCUMENTAÇÃO (ver ponto 3)</p> <ul style="list-style-type: none">◆ Se incompletos ou incorrectos, emite ofício (300 001 ou 300 379) e aguarda a resposta (até 90 dias);◆ Se não respondeu, preenche proposta de arquivamento do processo (mod. CNP 211 613), encerra o processo no terminal (código Q), emite ofício a comunicar o arquivo (of. 300 353), expurga documentos apenso ao processo, protocola em triplicado os processos (mod. CNP 112 140) e remete para microfilmagem (ao fim de 3 meses).	WTX WTX REQENC

¹⁸ Área Nacional – os 4 últimos dígitos do n.º de beneficiário;
Área Internacional – por País e os 4 últimos dígitos do n.º de beneficiário.



Descrição das Operações	Transações Informáticas
<p>3. CONSULTA¹⁹ A BDNBU – FCR – FP TENDO EM ATENÇÃO:</p> <ul style="list-style-type: none">◆ Grau de parentesco do(s) requerente(s), causa da morte, regime de pensão, situação do requerente, data do casamento, assinatura do requerente (ou de outrem a rogo, com fotocópia do BI); <p>3.1. Consulta os elementos, na base de dados, respeitantes a:</p> <p>3.1.1. Produtor:</p> <ul style="list-style-type: none">◆ identificação, situação à data do falecimento (activo, pensionista ou requerente) e histórico dos salários – procede à realização das operações que forem necessárias efectuar;◆ imprime os dados e junta as folhas ao processo (FCR); <p>3.1.2. Requerente(s):</p> <ul style="list-style-type: none">◆ Identifica-o no terminal e verifica se o requerimento já se encontra gravado<ul style="list-style-type: none">▪ Se já se encontra, preenche os campos relativos ao código de regime, tipo de benefício a pagar e motivo da concessão, através do registo de activo e 1º desconto;▪ Se não, cria identificação na BDN dos elementos do agregado familiar e procede à sua gravação;◆ Imprime os dados e junta ao processo; <p>4. ANALISA A DOCUMENTAÇÃO RELATIVA:</p> <ul style="list-style-type: none">◆ ao produtor, no que respeita ao extracto de salários e certidão de nascimento;◆ ao requerente: estado civil, descendentes e ascendentes. <p>5. CONFERE A EXISTÊNCIA DE PRAZO DE GARANTIA</p> <p>5.1. Se não existe prazo de garantia, é atribuído o reembolso de contribuições de sobrevivência, correspondente a 2,7% do total das remunerações;</p>	<p>NOM, FRG, HST</p> <p>NOM, PNS, NUMP</p> <p>IDA IDN, IDM, IDA</p> <p>REQGR, RE-QALT</p> <p>REQENC</p>

¹⁹ Se o requerimento não está correctamente preenchido, procura regularizá-lo;

Se o requerimento deu entrada directamente no CNP (residente no estrangeiro), efectua a sua gravação no FCR.



Descrição das Operações	Transações Informáticas
<p>5.2. Se existem falhas no prazo de garantia, emite texto 300 234 e solicita ao CDSSS competente os respectivos salários (WTX 200 155), excepto se constarem no BDNBU e BDR (Lisboa);</p>	
<p>6. DEFERIMENTO DO PROCESSO</p>	
<p>6.1. Se for de atribuir a pensão:</p>	
<p>6.1.1. Preenche proposta de deferimento (CNP 502 617);</p>	
<p>6.1.2. Preenche o verbete de cálculo (CNP 202 431);</p>	
<p>6.1.3. Relaciona os processos por ordem numérica, na relação de processos de benefícios diferidos (mod. CNP 211 422);</p>	
<p>6.1.4. Preenche os campos destinados à data e ao n.º de relação, na proposta de deferimento, e assina a mesma;</p>	
<p>6.1.5. Deferido o processo, encerra com o código D.</p>	
<p>6.2. Se não existirem condições para a atribuição da pensão:</p>	
<p>6.2.1. Preenche proposta de indeferimento e notifica o requerente por ofício;</p>	
<p>6.2.2. Procede ao indeferimento, datando e assinando a proposta;</p>	REQENC
<p>6.2.3. Encerra o processo, com o código I, e procede a expurgo para microfilmagem.</p>	
<p>6.3. De acordo com a resposta à notificação:</p>	
<p>6.3.1. Se existe resposta com fundamento, procede às operações descritas no ponto 8</p>	
<p>6.3.2. Se a resposta não tem fundamento, encerra com o código I, emite ofício 300 354, procede a expurgo para microfilmagem;</p>	
<p>6.3.3. Se não existe resposta, procede ao indeferimento (ofício 300 355), encerra com o código I e procede a expurgo para a microfilmagem</p>	
<p>7. PROCEDE AO CÁLCULO E PROCESSAMENTO DA PENSÃO</p>	
<p>7.1. Introduz os elementos para cálculo e processamento (mod. CNP 202 431), recorrendo às opções existentes</p>	REQENC WTX REQENC
<p>◆ Pensão provisória;</p>	
<p>◆ Pensão definitiva;</p>	WTX REQENC
<p>7.2. Imprime a informação e anexa ao processo;</p>	
	IDN, IDM, IDA – no

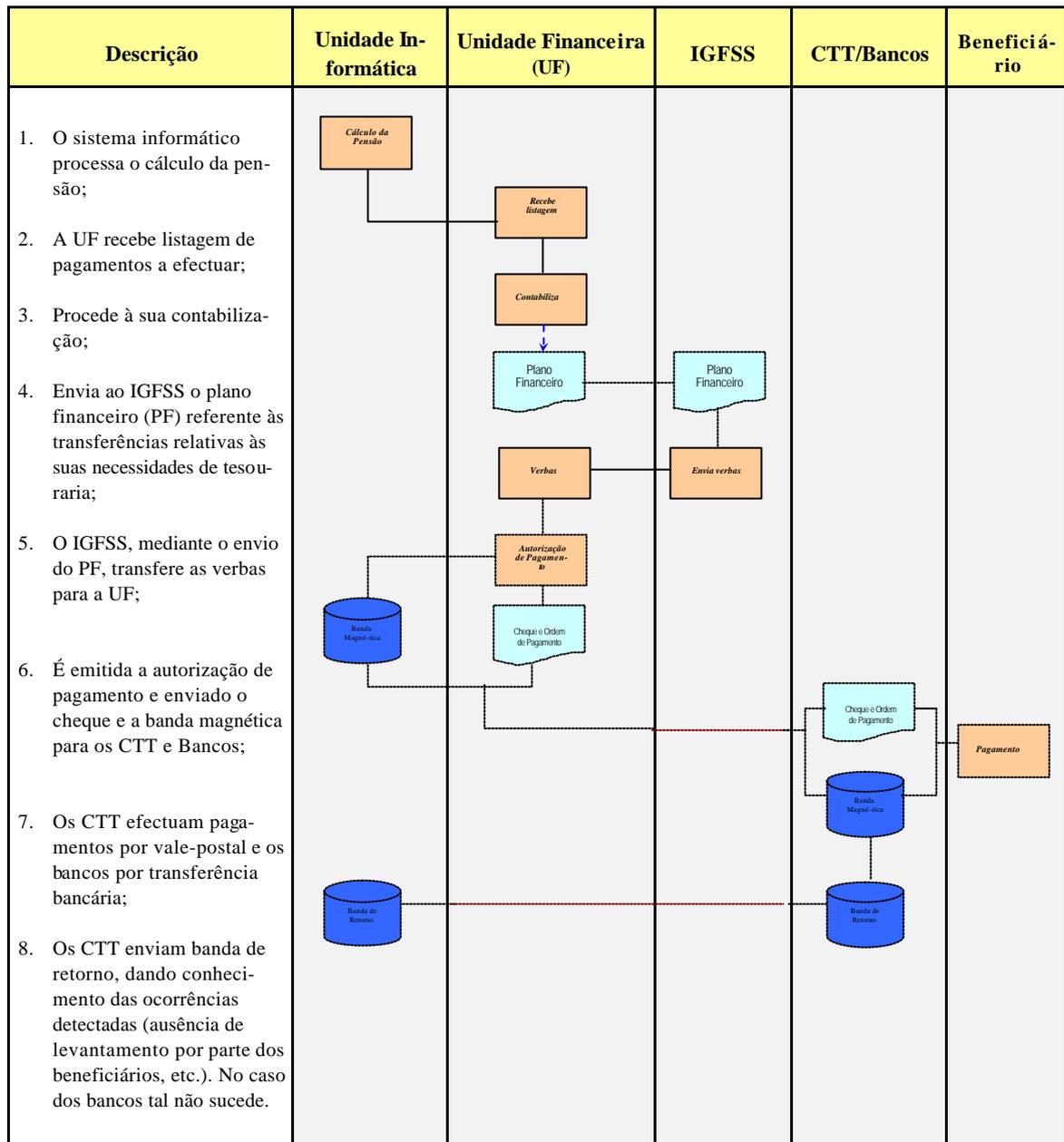


Tribunal de Contas

Descrição das Operações	Transações Informáticas
<p>7.3. Aguarda confirmação, a nível informático, sobre o valor a pagar</p> <p>7.4. É emitido automaticamente o ofício a comunicar ao(s) requerente(s) o deferimento da pensão e respectivo valor.</p> <p>8. RECEPÇÃO DE NOVOS ELEMENTOS:</p> <p>Sempre que existam novos elementos para o cálculo ou para a passagem da pensão provisória para definitiva:</p> <p>8.1. Procede à avaliação da situação e ao respectivo tratamento;</p> <p>8.2. Preenche o mod. CNP 502 617, para despacho, e o verbete de cálculo – revisão (mod. CNP 202 431);</p> <p>8.3. Procede às operações descritas no ponto 7 e a expurgo para microfilmagem.</p> <p>9. EXPURGO PARA MICROFILMAGEM</p> <p>9.1. Os processos concluídos, com cálculo definitivo, são expurgados, protocolados em triplicado (112 140) e enviados para o serviço competente para se proceder à respectiva microfilmagem (ao fim de 3 meses).</p>	<p>BNDBU e</p> <p>ELCAL – no ficheiro de cálculo</p> <p>RSOBP</p>



3.3. Tramitações Financeiras relativas ao pagamento de Pensões





Tribunal de Contas

3.4. Testes

Para averiguar da conformidade dos circuitos de tramitação processual descritos nos pontos 3.1 e 3.2, foram efectuados os testes julgados pertinentes, de que resultou a confirmação dos mesmos. Quanto ao circuito de tramitação financeira, exposto no ponto 3.3, apenas se efectuou o levantamento do mesmo, deixando-se para a segunda fase os respectivos testes.

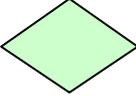


ANEXO I

SIMBOLOGIA UTILIZADA NOS FLUXOGRAMAS



Tribunal de Contas

 Correspondência enviada;	 Entrada/saída de dados;
 Documento (ofício, parecer, informação etc.);	 Conexão exterior/Seguimento;
 Documentação vária;	 Dados armazenados (microfilmagem)
 Banda (disco) Magnética(o)	 Arquivo;
 Registo contabilístico;	 Atraso
 Decisão;	 Conexão



ANEXO II

GLOSSÁRIO DAS TRANSACÇÕES INFORMÁTICAS



GLOSSÁRIO

Transacções que dão acesso à INCLUSÃO/ALTERAÇÃO de dados, relativamente aos requerimentos:

TRANSACÇÕES DE GRAVAÇÃO	P/ Rectificação	REQALT
	P/ Inclusão da data da deliberação da CVIP	REQJM
	P/ Inclusão Doença/ Desemprego	REQSD
	P/ Respostas a Pedidos	REQRES

TRANSACÇÕES DE CONSULTA	P/ Nome	NOMR
	P/ N.º Produtor	NUMP
	P/ N.º Requerente	NUMQ
	P/ Requerimento	NUMR

TRANSACÇÕES DE ENCERRAMENTO	P/ Anulação	REQENC
	P/ Encerramento* * das atribuições do CNP	



TRANSACCÕES INFORMÁTICAS

Transação	Descrição
CONCOR	Identifica, por número de pensionistas, o valor das pensões processadas, qualquer que seja o modo de pagamento e devoluções de valores processados por centralizador ou conta bancária
IDA	Inclui ou rectifica o número de contribuinte, regime e 1.º desconto
DEDINC	Inclui deduções a pensionistas
HST	Identifica, por número de beneficiário, os períodos contributivos e remunerações previamente lançadas no BNDBU
LPROG	Identifica, por número de pensionista, os totais anuais de pensões pagas
NOM	Identifica, por nome, as inscrições do beneficiário no BNDBU
NUMP	Identifica, por número de beneficiário, todos os requerimentos gravados
NUMQ	Identifica, por número de beneficiário, o tipo de requerimento e o eventual encerramento
NUMR	Identifica, por número de beneficiário, o registo do requerimento
PNS	Identifica, por número de beneficiário, a situação do pensionista
REQENC	Regista encerramento do processo
REQENC (cód. B)	Anula registo, que permanece consultável
REQGR	Regista requerimento de benefícios diferidos de requerentes, previamente identificados no BNDBU
REQGR 1IN	Regista requerimento de pensão de invalidez
REQGR 1LB	Regista requerimento de pensão provisória por limite de doença subsidiada
REQGR 1VE	Regista requerimento de pensão de velhice
REQJM	Regista data de deliberação da CVIP (inicial ou de recurso)
SAL94	Identifica remunerações a partir de 01/01/94
SALAR	Identifica remunerações até 31/12/93
SUSP	Suspende pagamento das prestações



Tribunal de Contas

Transação	Descrição
WTX	Emite ofícios da base de textos



Tribunal de Contas

**IIES - Instituto de Informática
e Estatística da Solidariedade**

MINISTÉRIO DA SEGURANÇA SOCIAL E DO TRABALHO



RECEBIDO

Departamento de Auditoria VII

Em 12/06/02

Exm^o Senhor
Director - Geral do Tribunal de Contas
Av.^a. Barbosa du Bocage, 61
1069 - 045 LISBOA

V/Ref.

Proc^o

N/Ref.

1449

Data: 06/06/2002

ASSUNTO: Auditoria aos Sistemas de Atribuição e Controlo de Pensões

Conforme citação feita pelo ofício n^o 4694, de 20/05/2002, apresentam-se os seguintes comentários sobre a parte que respeita ao IIES, relativamente ao Relatório da Auditoria aos Sistemas de Atribuição e Controlo de Pensões:

1. O Instituto de Informática e Estatística da Solidariedade (IIES) foi criado pela Lei Orgânica do Ministério do Trabalho e da Solidariedade (Decreto-Lei n^o 115/98, de 4 de maio), fixando-se-lhe "como principal missão e objectivos a criação, implementação e disponibilização do sistema de informação da segurança social de modo a reflectir a orientação estratégica global de desenvolver sistemas e aplicações nacionais que assegurem a qualidade e acesso á informação de forma coerente e universal, garantindo assim uma melhoria da gestão...".
Os seus estatutos foram aprovados pelo Decreto-Lei n^o 41-A/99, de 9 de Fevereiro;
2. À data da implementação do IIES, existiam, na Segurança Social (SS), bases de dados distritais e no CNP, assentes em plataformas tecnológicas diferentes e desintegradas e aplicações distintas, de âmbito institucional, distrital ou local;
3. Perante o quadro existente e a missão e os objectivos que lhe foram definidos, o IIES iniciou o processo de criação de um novo sistema de informação, assente em bases de dados nacionais e únicas de contribuintes e beneficiários, associadas à implementação de um sistema de identificação e qualificação nacional e único de todas as entidades relevantes para a SS (IDQ) e materializado em aplicações nacionais e universais.

DGTC 12 06 02 14027



IIES - Instituto de Informática e Estatística da Solidariedade

MINISTÉRIO DA SEGURANÇA SOCIAL E DO TRABALHO



Paralelamente e até à entrada em produção das novas aplicações nacionais, torna-se necessário garantir a continuidade das aplicações existentes, assegurando os indispensáveis níveis de manutenção e assistência aos sistemas existentes;

4. A criação de um Novo Sistema de Informação tão complexo e abrangente como este, contemplando um universo de mais de sete milhões de pessoas singulares, mais de quatrocentas mil pessoas colectivas, operado por quase duas dezenas de milhar de funcionários, abrangendo todo o Continente e Regiões Autónomas e servido por um grande sistema de redes de comunicação constitui um processo delicado e de grande envergadura e que tem, natural e inevitavelmente, os seus tempos de execução próprios...;
5. Como se referiu em anteriores comentários remetidos a esse Tribunal, no âmbito da auditoria aos sistemas de atribuição e controlo das prestações de desemprego (ofício nº 877, de 2002/04/11), o IIES já disponibiliza, para o sistema de segurança social, designadamente para o Instituto de Solidariedade e Segurança Social (ISSS) e Instituto de Gestão Financeira da Segurança Social (IGFSS):
 - a) Bases de Dados Nacionais (BD) de Beneficiários e Contribuintes, desde o início de 2002, estando prevista, para o último trimestre do corrente ano, a disponibilização do Sistema de IDQ;
 - b) Uma aplicação nacional de Gestão de Tesourarias (GT), suportada pelas BD referidas na alínea anterior, desde o início do corrente ano;
 - c) A informação recolhida através de um sistema nacional de leitura óptica (CLO) que permite a leitura e o lançamento automático dos dados constantes das folhas de remunerações em suporte de papel, desde o início do corrente mês;
 - d) Sistemas nacionais de recepção das declarações das remunerações via internet (DRI) e via suporte magnético (DRD) e respectivos lançamentos;
 - e) Os sistemas CLO, DRI e DRD permitirão a disponibilização imediata da indispensável informação ao processamento e pagamento atempado das prestações e, simultaneamente, ao apuramento da dívida declarada e, associados à GT e aos outros sistemas de recolha das contribuições recebidas (vias Multibanco, CTT e bancos), permitirá o apuramento das respectivas contas correntes e a implementação de mecanismos de combate à evasão contributiva;
 - f) Uma aplicação nacional do Rendimento Mínimo Garantido (RMG) que permite o controlo de todo o processo da prestação, desde o deferimento do pedido até ao seu efectivo pagamento;



- g) Um Repositório de Dados Nacionais Estatísticos de Desemprego que possibilita a verificação de eventuais irregularidades, nomeadamente a ocorrência de sobreposições;
- h) Ainda quanto à sobreposição da prestação de desemprego com trabalho remunerado, o IIES também dispõe, no âmbito do sistema de datawarehouse, de um mecanismo vocacionado para este controlo, actualmente implementado apenas no Centro Distrital de Solidariedade e Segurança Social de Setúbal, como centro piloto, mas que, a curto prazo, terá aplicabilidade nacional, passando-se a dispor de um importante instrumento de combate à fraude:
6. Foi criada e montada uma rede de comunicações própria da SS, que é adaptada, em cada momento, às necessidades colocadas pelas aplicações, rede essa que suporta o funcionamento e a exploração de todo o sistema de informação;
7. Prevê-se que, até final do corrente ano, seja disponibilizada uma aplicação nacional e única para a prestação de desemprego, que será, inevitavelmente, um instrumento eficaz de controlo e apoio à gestão processual desta prestação;
8. Também até final do corrente e em simultâneo com a entrada em produção da aplicação referida no ponto anterior, será disponibilizado um sistema que efectuará a gestão integral das reposições referentes ao sistema prestacional;
9. Por se reconhecer ser, eventualmente, fastidioso e até, porventura, inoportuno, atento o âmbito específico dos presentes comentários, não se vai aqui referir todo o programa do Novo Sistema de Informação da Segurança Social. Aliás, ele é já do conhecimento desse Tribunal, quer por via de anterior remessa quer por via de explicações fornecidas a auditores, em reuniões realizadas neste Instituto;
10. Sobre questões concretas abordadas ou afirmadas no Relatório, julgo de utilidade referir o seguinte:

10.1 VI.2.2 Processos de Gestão de Sistemas de Informação

Como se sabe, a estratégia de sistemas de informação de qualquer organização está directamente dependente da estratégia de negócio e tem, necessariamente, de estar alinhada com esta. Nesta conformidade, a responsabilidade do Planeamento e Estratégia dos Sistemas de Informação da SS



**IIES - Instituto de Informática
e Estatística da Solidariedade**
MINISTÉRIO DA SEGURANÇA SOCIAL E DO TRABALHO



não poderá ser da exclusiva responsabilidade do IIES, mas sim de uma atitude concertada entre as entidades envolvidas nos processos.

Julgamos que aqui será importante o papel do Conselho Consultivo do IIES - em fase de constituição - , previsto no artigo 12º do DL 41-A/99, de 9/2 e onde têm assento os dirigentes máximos dos serviços e organismos do sistema de solidariedade e segurança social, a quem compete, designadamente, nos termos do artigo 13º do mesmo diploma, pronunciar-se sobre as grandes linhas de orientação estratégicas relativas ao sistema de informação da segurança social.

Segundo o mesmo articulado, deve ainda o mesmo órgão ser ouvido sobre o plano anual de actividades e sobre as decisões de carácter estratégico relacionados com a definição e operação do sistema de informação da segurança social.

Na sua falta e tendo em vista a indispensável articulação e integração, o IIES elaborou o plano de actividades de 2002 com base em reuniões parcelares com os Conselhos Directivos do ISSS e IGFSS, principais instituições que usufruirão do sistema de informação:

10.2 VI.2.2.1 Planeamento e Estratégia de Sistemas e Informação - "Actualização da Estratégia de Sistemas de Informação"

Como já foi referido, só após a constituição formal do Conselho Consultivo é possível clarificar e definir, com rigor, a estratégia dos sistema de informação a médio e curto prazo com a conseqüente apresentação de prazos e prioridades, de forma a poder-se assegurar um correcto plano de investimento nesta área, bem como uma monitorização do processo que permita avaliar o cumprimento dos prazos, objectivos e resultados.

Não obstante constrangimento resultante da não existência do órgão, o IIES tem vindo a efectuar os indispensáveis levantamentos que servirão de base a todo este processo:

10.3 VI.2.2.1.4. Definição da Organização de TI e suas Interdependências

O IIES é responsável pela totalidade da chamada "Rede Nacional de Dados da Segurança Social", faz a sua monitorização de forma centralizada, detectando qualquer anomalia que se verifique na comunicação em qualquer ponto da rede, desde os "routers" locais até aos "nós" centrais. Actualmente, está a ser implementada uma ferramenta adicional que permitirá a monitorização das redes locais incluindo estações e impressoras padrão.



Quando considerada útil, a informação de monitorização pode e é disponibilizada ao ISSS e ao IGFSS;

10.4 VI.2.2.1.7. *Gestão de Recursos Humanos*

Os sistemas actuais, distribuídos por 5 plataformas principais e 23 centros de informática, dependem dos técnicos que, de uma forma geral, estiveram na sua génese e têm vindo a garantir a sua continuidade.

Qualquer plano para desenvolvimento destes recursos humanos tem de ser visto de uma forma individualizada, atentas, principalmente, a continuidade de exploração dos actuais sistemas durante a fase de transição, a faixa etária, a motivação dos mesmos para as novas tecnologias e a apetência dos interessados para integrar as diversas áreas de actuação.

Perante esta constatação o IIES tomou a iniciativa reunir com os interessados, de forma a que os mesmos sejam ouvidos e apresentem sugestões com vista à elaboração dum plano estratégico de recursos humanos da área informática. Em termos de preparação básica destes recursos, o IIES tem mesmo previsto, no seu plano de actividades para 2002, acções de formação vocacionadas para sistemas abertos;

10.5 VI.2.2.1.8 *Cumprimento de Requisitos Externos*

No cumprimento da sua missão, a Segurança Social processa dados que requerem o respectivo registo na Comissão Nacional para a Protecção de Dados. Atendendo a que, de uma forma geral, se trata do mesmo tipo de dados, independentemente do fim a que se destinam e da plataforma que os suporta, o IIES encetou diligências no sentido de providenciar a legalização dos mesmos, a nível da segurança social, em detrimento da abordagem por instituição;

Em relação à segurança na transmissão dos dados, cabe-nos informar que, os acessos de serviços do ISSS aos sistemas do CNP processam-se exclusivamente através da Rede Nacional da Segurança Social (RNSS), a qual é uma rede privativa utilizando circuitos alugados a Operadores Públicos de Comunicações. Nesta medida, existe de facto o risco potencial de o tráfego na RNSS poder ser escutado, tal como existe em todas as redes sobre infraestruturas de operadores públicos, pelo que estão a ser desenvolvidos projectos que visam melhorar a segurança da Rede, nomeadamente através da inclusão de mecanismos de encriptação e outros. No entanto, os acessos à RNSS encontram-se já protegidos por vários sistemas de segurança e validação de acessos que são auditáveis e auditados. Tanto quanto é do nosso conhecimento, não existe utilização de ligações por satélite na RNSS.

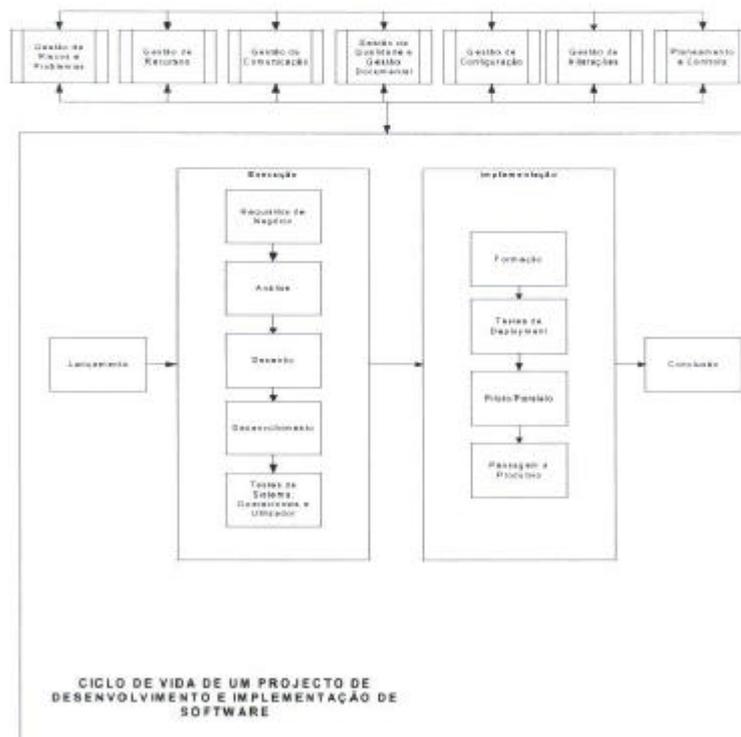


10.6 VI.2.2.2.5 Instalação e Certificação de Sistemas

O IIES tem definida e implementada uma metodologia de gestão de projecto que contempla a certificação de sistemas.

Para melhor clarificar o assunto, junta-se o fluxograma do ciclo de vida de um projecto de desenvolvimento e implementação de software, em uso no IIES, bem como o que, neste contexto, se entende por qualidade.

Fluxograma - Ciclo de Vida do Projecto





**IIES - Instituto de Informática
e Estatística da Solidariedade**

MINISTÉRIO DA SEGURANÇA SOCIAL E DO TRABALHO



Gestão da Qualidade - Tem como objectivo planear e controlar a qualidade do projecto e seus produtos e gerir a documentação associada e produzida durante o projecto. Os benefícios resultantes da aplicação deste processo são os seguintes:

- Identificação dos critérios de aceitação dos produtos e/ou procedimentos aplicáveis;
- Planeamento das acções de controlo aos produtos gerados pelo projecto;
- Avaliação da conformidade dos projectos, através da realização de auditorias;

10.7 VI.2.2.3.6. Identificação e Afectação de Custos

No IIES, o processo de afectação total de custos aos projectos encontra-se em fase de análise de requisitos, seguindo-se-lhe, imediatamente, a fase de implementação, estando já seleccionada uma ferramenta para suporte ao processo;

10.8 VI.2.2.3.8 Apoiar e Aconselhar os "Clientes" de TI

O IIES tem um serviço de Help Desk, numa primeira fase, vocacionado para as aplicações que vai disponibilizando, quer internas ao sistema quer às entidades empregadores. Está, neste momento, a decorrer um processo de implementação de um sistema assente em ferramentas e metodologias adequadas.

Porém, pretende-se que esta infra-estrutura venha a ser alargada a todo o sistema de segurança social;

10.9 VI.2.2.3.9 Gestão da Configuração de Sistemas

O IIES, na prossecução da sua missão, definiu um standard para a configuração de computadores pessoais, aplicado a todas as estações de trabalho da rede de SS, documentado na intranet, tendo vindo a dotar os diversos serviços com equipamentos conformes, denominados de "estação padrão". Esta configuração está devidamente protegida, não permitindo a instalação de software, por parte de utilizadores não autorizados;



**IIES - Instituto de Informática
e Estatística da Solidariedade**

MINISTÉRIO DA SEGURANÇA SOCIAL E DO TRABALHO



10.10 VI.2.2.3.12 Gestão das Instalações Físicas

Sobre este assunto e no que respeita ao Novo Sistema de Informação, o IIES tem em curso um projecto para definição dos requisitos a implementar para efeito de recuperação de desastres, de forma a que a disponibilidade dos sistemas não seja afectada, para além do tempo considerado aceitável;

10.11 VI.2.2.4 Processo de Monitorização dos Processos de TI

O IIES foi constituído em 1998, tendo estado a sua actividade centrada, essencialmente, nos processos de instalação e de criação de infra-estrutura tecnológica necessária à implementação das aplicações do novo sistema. O IIES não ignora a importância deste processo, apenas não constituiu, até agora, prioridade, face à sua curta existência e às actividades e projectos que, obrigatoriamente, o deveriam preceder.

Com os melhores cumprimentos,

O Presidente do Conselho Directivo,

Manuel da Cruz Pires



Tribunal de Contas



SOLIDARIEDADE E SEGURANÇA SOCIAL

RECEBIDO

Departamento de Auditoria VII

Em 14/06/02

Exm.º Senhor
Director-Geral do Tribunal de Contas
A/C do Auditor Coordenador Sr. Dr. António
Manuel Fonseca da Silva
Av. Barbosa do Bocage, 61
1069 – 045 LISBOA

Sua referência

Sua Comunicação

Nossa referência C.D./ISSS
25 792, de 14/06/02

Assunto: Auditoria aos Sistemas de Atribuição e Controlo de Pensões (Proc.º n.º 26/01-AUDIT-DA VII)

Reportando-me ao ofício n.º 4692, de 20 de Maio, e à Mensagem Fax n.º 02/02-DA VII, de 07/06/2002, remeto em anexo a RESPOSTA ao Relato do Processo n.º 26/01-AUDIT relativo à "Auditoria aos Sistemas de Atribuição e Controlo de Pensões".

Com os melhores cumprimentos

O PRESIDENTE DO CONSELHO DIRECTIVO

JOSÉ CARLOS FREIRE
Presidente do Conselho

Anexo: Documento referido

Instituto de Solidariedade e Segurança Social

Conselho Directivo

DGTC 14 06 02 14252

Rua Rosa Araújo, 43 - 1250-194 LISBOA - Telef: 213 102 000 - Fax: 213 102 093



SOLIDARIEDADE E SEGURANÇA SOCIAL

**RESPOSTA
DO
INSTITUTO DE SOLIDARIEDADE E SEGURANÇA SOCIAL
NO PROC. 26/01 – AUDIT, DO TRIBUNAL DE CONTAS**

ASSUNTO: AUDITORIA AOS SISTEMAS DE ATRIBUIÇÃO E CONTROLO DE PENSÕES

A presente resposta segue a estrutura do Apêndice F (Detalhe dos Resultados da Auditoria)

De acordo com a interpretação que se fez do Relatório, da sua análise parecem resultar algumas imprecisões que a seguir se esclarecem:

1.- AVALIAÇÃO DOS PROCESSOS DE ATRIBUIÇÃO E CONTROLO DE PENSÕES

1.2. RECEPÇÃO, ORGANIZAÇÃO E REGISTO DE REQUERIMENTO

A "descrição da actividade" e da "situação actual" deverá ser complementada e entendida de acordo com o que estabelece os artigos 74º, 75º e 76º do DL-329/93, de 25 de Setembro, e que é mantido e desenvolvido pelo Estatuto do ISSS, aprovado pelo DL-316-A/2000, de 7 de Dezembro:



SOLIDARIEDADE E SEGURANÇA SOCIAL

REGISTO DO REQUERIMENTO

A possibilidade de registar o requerimento no ficheiro de requerentes no momento da entrega e a eventual emissão de recibo por via informática, reconhecendo-se como desejável e estando nos horizontes, depende de alguns factores que se esperam vir a ultrapassar, como, por exemplo, a maior disponibilidade de equipamento informático e a melhoria da Base Nacional de Dados de Identificação.

A proximidade dos serviços ao cidadão e a sua comodidade, levaram a optar pela manutenção da descentralização na recepção de requerimentos, com o seu posterior registo informático

De qualquer modo, encara-se como possível a informatização de toda a actividade relativa ao processo administrativo (manual) de pensão, incluindo a integração com aplicações de gestão documental.

Quanto à referência ao "*registo do detalhe da carreira contributiva*" não se compreende a sua associação ao registo do requerimento, nem a referência à introdução da densidade contributiva em 1994:

- Por um lado, a carreira contributiva vai-se registando ao longo da vida activa do beneficiário. O registo do requerimento de pensão é autónomo e independente dos registos existentes da carreira contributiva.
- Por outro, a densidade contributiva introduzida em 1994 apenas passou a ser exigida para os descontos futuros não tendo afectado a carreira contributiva passada.

PRIORIDADE DE REQUERIMENTOS

Constata-se que, por parte dos beneficiários, se verifica uma maior acuidade na preparação da passagem à reforma, nomeadamente na recolha de elementos relativos



SOLIDARIEDADE E SEGURANÇA SOCIAL

à carreira contributiva e no montante provável da pensão e que, em muitos casos, a opção pela reforma está pendente de informação do ISSS-CNP.

Para esse beneficiário, é urgente receber a resposta do sistema (CNP) para poder tomar uma das decisões mais importantes da sua vida: pedir a reforma (deixando a vida activa) ou adiar o pedido (continuando a trabalhar). Daí que os pedidos de montante provável estejam a dar origem a cada vez mais reclamações.

Apesar disso, não há (e entende-se não serem de dar) orientações para secundarizar os pedidos de montante provável de pensão. No entanto, o certo é que, em termos de gestão, é dada de facto prioridade aos pedidos efectivos de pensão em detrimento dos pedidos de montante provável. Basta atentar que existe um quadro mensal de indicadores que acompanha e controla, por unidade, a produção e o tempo médio de atraso na conclusão dos processos (pedidos efectivos de pensão por invalidez, por velhice ou de sobrevivência), que constitui uma pressão permanente sobre a organização e desenvolvimento das tarefas mensais e donde estão excluídos os pedidos de montante provável de pensão.

Atente-se que o tratamento dos "cálculos prováveis" não tem prejudicado o andamento dos restantes processos, uma vez que o ISSS-CNP tem conseguido, desde há vários anos, como é reconhecido no Relatório, taxas de conclusão dos processos de pensão próximas dos 100%.

EFICIÊNCIA DO PROCESSO

O Relato parte do princípio de que a informação constante do requerimento deve ser validada com a existente no sistema.

O sistema de informação não está, por opção, estruturado desse modo.

3

Instituto de Solidariedade e Segurança Social
Conselho Directivo

Rua Rosa Araújo, n.º 43 1250-194 LISBOA - Telef.: 213 102 000 - Fax: 213 102 093



SOLIDARIEDADE E SEGURANÇA SOCIAL

No formulário de requerimento de pensão, à excepção da identificação, apenas se pedem elementos que não constam do sistema da SSS ou, constando (caixas para onde descontou), são apenas indicativos tendo em vista uma melhor instrução.

O momento da entrega do requerimento pretende-se célere: a recolha dos elementos da carreira contributiva ou ocorreram antes (pelo beneficiário) ou ocorrem depois (pelo sistema).

No momento da entrega do formulário do requerimento, pretende-se que seja verificado se estão preenchidos todos os itens e solicitar o seu preenchimento, caso não estejam (e será um dos maiores contributos para a celeridade do processo).

Aliás, como é sabido, e dado o uso de formulário adequado, fica restringida à falta de assinatura do requerimento o fundamento para se recusar o seu recebimento (Artigo 74º e seguintes do CPA). Por outro lado, dada a relevância da data de entrega do requerimento para a definição do direito do requerente, há que não sobrecarregar esse momento com diligências instrutórias ou confirmativas.

Por tudo isto, considera-se que o desenvolvimento da actividade deverá encaminhar-se, cada vez mais, para a existência duma fase preparatória da reforma, prévia ao requerimento (de preferência, *pró-activa*) e não para uma sobrecarga de diligências na altura da apresentação do pedido. Certamente que a integração da carreira salarial numa base de dados nacional virá a possibilitar alguns passos nesse sentido.

INTEGRIDADE DA INFORMAÇÃO

A consulta e análise do *"rasto efectivo dos acontecimentos"* tem sido fundamentalmente necessária para as situações anómalas, sempre excepcionais.

4

Instituto de Solidariedade e Segurança Social
Conselho Directivo

Rua Rosa Araújo, n.º 43 1250-194 LISBOA - Telef.: 213 102 000 - Fax: 213 102 093



SOLIDARIEDADE E SEGURANÇA SOCIAL

A data de gravação é automaticamente a data do sistema.

A data do requerimento é meramente indicativa, apenas para indicadores de gestão. A data efectiva de início da pensão é determinada, aquando do reconhecimento do direito, de acordo com a legislação em vigor, não sendo necessariamente coincidente com a data aposta ou registada para o requerimento.

O mesmo se diga da data da junta médica que não é utilizada automaticamente (no cálculo de pensões) como data de início de pensão.

MONITORIZAÇÃO DA ACTIVIDADE

A detecção de atrasos ou extravios não resulta apenas de reclamação do beneficiário.

Desde que o requerimento se encontre gravado no Ficheiro Central de Requerentes (FCR), se existem anomalias, serão detectadas através do tratamento de listagens que (de forma *pró-activa*) são solicitadas periodicamente à unidade de Informática do ISSS-CNP.

Assim, consideramos que a partir do registo informático do requerimento, é e tem sido possível *“avaliar a qualidade e fiabilidade da gestão de requerimentos”*.

1.3.- IDENTIFICAÇÃO DO BENEFICIÁRIO

É referido que *«é verosímil a existência de um beneficiário com mais de um número registado na base de dados»* e que *“os responsáveis da Unidade de SI do CNP não têm capacidade para detectar estas situações”*.



SOLIDARIEDADE E SEGURANÇA SOCIAL

Apenas poderá existir mais que um número de beneficiário para a mesma pessoa, no caso das inscrições antigas, anteriores à integração das Caixas Sindicais de Previdência e à introdução do conceito de "número nacional". Trata-se duma situação perfeitamente conhecida e sob controlo.

Depois da introdução do conceito de "número nacional" de beneficiário, é assegurado que para a mesma "chave de identificação" (mesmo nome, data de nascimento e naturalidade) apenas é atribuído e apenas existe um único número de beneficiário.

1.4.- ENVIO E INTEGRAÇÃO DE INFORMAÇÃO COM O CNP

É referido que o envio dos processos ao CNP é feito através de um procedimento manual, suportado por um protocolo. Contudo, além disso, há também um registo informático, quando o requerimento é enviado pelo Centro Distrital ao CNP e outro registo de entrada neste organismo.

Quanto à carreira contributiva, desenvolvem-se esforços no sentido da sua integração imediata e actualização na Base Nacional de Beneficiários e Utentes, mas prevê-se a médio prazo a sua integração completa numa Base de Dados Nacional.

2.- PROCESSO DE ATRIBUIÇÃO E CÁLCULO DE PENSÕES

2.1.- A CONFERÊNCIA E DEFERIMENTO DE PROCESSOS

Conforme vem referido, encontram-se claramente definidos no ISSS-CNP os procedimentos internos com vista à tomada de decisão sobre um pedido de pensão. Como é sabido e consciencializado por todos os intervenientes desde sempre, a decisão final sobre um pedido de pensão apenas pode ser tomada por quem tenha competências delegadas para o efeito.

6

Instituto de Solidariedade e Segurança Social
Conselho Directivo

Rua Rosa Araújo, n.º 43 1250-194 LISBOA - Telef.: 213 102 000 - Fax: 213 102 093



SOLIDARIEDADE E SEGURANÇA SOCIAL

Assim, não pode, de modo algum, confirmar-se que haja pedidos de pensão com deferimento efectuado por conferente ou por assistente administrativo especialista.

A referência a 32% dos deferimentos nestas condições mais alicerça a firme convicção de que aquela conclusão será eventualmente devida a uma deficiente interpretação dos elementos constantes dos processos pela equipa de auditoria.

Dos 394 processos analisados pela equipa de auditores foi ainda possível, no curto espaço de tempo para esta resposta, verificar cerca de 235.

De entre estes 235 processos não se encontrou nenhum cujo deferimento tivesse sido feito pelo conferente ou pelo assistente administrativo especialista.

Importa referir que no processo que conduz ao deferimento, intervêm o organizador, o conferente e o chefe de secção ou de equipa e, muitas vezes, ainda o Director de Núcleo e Director de Unidade.

Constitui orientação permanente que haja sempre um despacho formal proferido por funcionários com competência, por delegação de poderes (Chefe de secção/equipa, Chefe de Repartição/Director de Núcleo ou Director de Serviços/Unidade), embora tal possa não resultar claramente da «leitura» imediata do “despacho”.

Esse “despacho” ou consta directamente do suporte de informação elaborado para cada processo ou consta duma relação elaborada para o efeito e cuja existência o relato constata.

Nos casos em que o despacho consta duma relação de processos elaborada para o efeito, verifica-se o seguinte:

7

Instituto de Solidariedade e Segurança Social
Conselho Directivo

Rua Rosa Araújo, n.º 43 1250-194 LISBOA - Telef.: 213 102 000 - Fax: 213 102 093



SOLIDARIEDADE E SEGURANÇA SOCIAL

- A assinatura do funcionário com competência delegada para decidir pedidos de pensão (chefe de secção, repartição ou director de serviços) consta, como se referiu, da relação; Estas relações encontram-se arquivadas em cada secção.
- Do processo consta uma anotação, em regra, assinada pelo conferente, com a indicação do número e data da relação onde consta o deferimento.

Este procedimento foi sancionado há muito através de relatório apresentado por um grupo de trabalho nomeado para estudo das normas conducentes à legalidade formal dos despachos.

Quanto aos 9% de casos em que *"não se encontram evidências do despacho proferido pela pessoa competente"*, refere-se o seguinte:

Mesmo nos casos de comparticipação à CGA, em que o despacho não é da competência do CNP, utilizam-se suportes de informação, criados para esse fim, que prevêem o visto e anuência do Chefe de Equipa e do Director de Núcleo.

No entanto, quando é devida comparticipação ao abrigo de vários regimes ou diplomas ou há lugar a uma comparticipação e à concessão de uma pensão autónoma pode acontecer que todos os direitos sejam analisados e deferidos numa só informação, pelo respectivo chefe de secção, muito embora, por necessidades informáticas, possa haver vários suportes de cálculo diferentes, assinados apenas pelos organizadores e pelos conferentes.

Assim e em conclusão:

- Não se confirma a conclusão de que não há segregação de funções;



SOLIDARIEDADE E SEGURANÇA SOCIAL

- Não se confirma a conclusão de que há deferimentos efectuados por conferentes e assistentes administrativos;
- Não se confirma que haja processos concluídos sem a adequada decisão;
- Os serviços de organização de processos do ISSS-CNP estão à disposição do Tribunal de contas para confirmar, com qualquer amostra e de qualquer ano, o que se acaba de referir.

2.2. O CÁLCULO DE PENSÃO

2.2.1.- DESCRIÇÃO DA ACTIVIDADE

Todos os cálculos, provisórios ou definitivos, são efectuados imediatamente **após** o deferimento do processo e não antes, como é afirmado no Relatório.

2.2.2.- SITUAÇÃO ACTUAL

A informatização do Cálculo de Pensões abrange quase todas as especificidades do Regime Geral e não apenas o Regime Geral «puro», como referido no documento.

Deve assinalar-se que, quando entra em vigor nova legislação, é normal não haver de imediato programa de cálculo testado e disponível para dar execução às novas normas legais. Foi, designadamente, o caso do DL-119/99, de 14 de Abril, que veio introduzir uma nova modalidade de pensão antecipada e que, no ano de 2000 a que se reportou a auditoria, ainda não era objecto de cálculo informático, mas que veio a ser logo em



SOLIDARIEDADE E SEGURANÇA SOCIAL

27/09/2000. Assim, a maior parte dos casos que foram vistos pela auditoria como cálculos "manuais" actualmente já se encontram informatizados.

De entre os "cálculos especiais" não informatizados, têm mais significado os casos de comparticipação à CGA. Estando, no entanto, a ser desenvolvido um novo sistema de cálculo, com nova filosofia, no âmbito do projecto de implementação do DL-35/2002, de 19 de Fevereiro, considera-se possível virem a ser informatizados alguns dos cálculos especiais, principalmente as comparticipações à CGA.

2.2.3. Resultados dos testes efectuados

A Unidade de Informática do CNP forneceu à equipa de auditores do TC vários ficheiros com elementos extraídos da base de dados de identificação (completa), do Ficheiro Central Requerimentos (Regime Geral de Invalidez/Velhice e de Sobrevivência, com data de requerimento do ano 2000), da Base de Dados de Pensionistas (pensões do Regime Geral incluídas no ano 2000) e respectivas deduções e atrasados e os elementos da carreira contributiva existentes nos ficheiros de cálculo.

Aquando da reunião com os auditores do TC, em 16 de Outubro de 2001, não foi claramente entendido qual o tratamento a que iriam ser submetidos estes dados, pois foi referido que se pretendiam efectuar «os processamentos relativos ao ano 2000».

Nas reuniões subsequentes, verificou-se que o TC pretendeu desenvolver uma aplicação de cálculo de pensões e comparar os resultados com os dados fornecidos.

Esta aplicação não foi validada por qualquer elemento do ISSS-CNP, tanto da Unidade de Informática como dos utilizadores, o que levou a que não tenha sido possível



SOLIDARIEDADE E SEGURANÇA SOCIAL

completá-la, em tempo útil, para abranger todas as situações e que fossem solicitados posteriormente dados adicionais necessários ao recálculo das pensões.

Dado que o recálculo das pensões de sobrevivência, de beneficiários falecidos na situação de pensionistas, foi efectuado com base nos salários introduzidos para cálculo do Subsídio por Morte em vez da utilização da pensão do produtor, cujo montante se encontra devidamente actualizado, os resultados tiveram que ser obviamente diferentes, e daí a indicação de 31,64% de diferenças não conciliadas apontadas no relato para a sobrevivência.

Quanto às diferenças encontradas para a parcela 02, devem-se ao facto de as pensões fornecidas terem também anos de início diferentes de 2000, sendo os valores fornecidos resultado de mais que uma actualização de pensões e o seu recálculo não ter sido efectuado aplicando as regras das várias portarias de forma autónoma, correspondente à evolução da pensão real do beneficiário.

As diferenças no Complemento Social, dado tratar-se de um diferencial, são o resultado das incorrecções referidas anteriormente.

De todo o modo, para que não subsistam dúvidas quanto à fiabilidade dos cálculos informáticos efectuados no ISSS-CNP, esclarece-se que todos os programas de cálculo foram devidamente testados antes da entrada em produção e são diariamente testados e controlados, nos seus resultados, pelos utilizadores e pelos próprios beneficiários pensionistas através das suas reclamações quanto ao valor das pensões.

Em conclusão, considera-se que os programas de cálculo informático existentes no ISSS-CNP cumprem rigorosamente o objectivo de calcular as pensões devidas de acordo com os critérios legais aplicáveis.



SOLIDARIEDADE E SEGURANÇA SOCIAL

CÁLCULOS MANUAIS

A referência a cálculos manuais não é correcta: Quando e enquanto não há programa de cálculo adequado para determinada situação, é utilizado o programa informático de cálculo de montante provável. Assim, *não há cálculos manuais ou efectuados com recurso a ferramentas não informáticas*. Haverá, sim, inclusão manual de pensões, após cálculo informático do montante provável e aplicação das especialidades adequadas ao resultado obtido. Aliás, cada vez mais a complexidade do cálculo dum pensão impedirá que se possa calcular uma pensão com uma simples máquina de calcular.

Consequentemente, o sistema do CNP consegue dar resposta à quase totalidade dos cálculos exigidos pela legislação em vigor e, àqueles a que ainda não dá resposta directa, disponibiliza ferramenta adequada e de recurso para o efeito.

DIFERENÇAS TEMPORAIS NOS DADOS

As dificuldades relatadas apenas comprovam a complexidade do sistema face à variedade das situações e dos requisitos legais a ter em conta, a que o sistema informático do CNP sempre tendo dado conta ao longo dos anos.

A Base de Dados de Pensionistas, que possui o suporte informático para os processamentos de pensões, como referido, tem os dados actualizados para os beneficiários activos.

Possui também um histórico de pensões suspensas, qualquer que seja o motivo dessa suspensão, com os valores das pensões à data da suspensão.

Quando se procede a uma revisão de pensão, devida a novos elementos para cálculo, ou a uma actualização de pensão resultado da aplicação de legislação, os novos dados substituem os existentes no ficheiro base de pensionistas.



SOLIDARIEDADE E SEGURANÇA SOCIAL

No entanto, **o ficheiro de cálculo de pensões, possui todo o histórico dos diferentes cálculos efectuados para o beneficiário.**

As actualizações de pensões produzem listagens com os elementos antes da actualização e os posteriores, para todas as pensões actualizadas.

Estas listagens produziram, até ao ano 2000, micro-fichas que podem ser consultadas quando necessário.

A partir de 2001 esta informação está armazenada num sistema COLD que pode ser consultado em vários postos de trabalho da rede do CNP.

Para todos os pensionistas processados em cada mês são gravados registos de todos os valores discriminados de pensão, atrasados e deduções efectuadas, até 60 meses, que podem ser consultados "online" em toda a rede da Segurança Social. Da análise desta informação pode verificar-se quais os valores de pensão em cada mês para todos os pensionistas.

Ao fim de 60 meses, os dados do 61.º mês mais antigo são apagados da base de dados e passados para micro-fichas e actualmente para o sistema COLD.

Não existe portanto qualquer perda de rasto das pensões pagas anteriormente, como referido no relato.

Relativamente ao referido quanto à inexistência de documentação, suficientemente detalhada, para «discriminar todas as especificidades inerentes ao cálculo e permitir guardar um rasto adequado das alterações efectuadas» esclarece-se o seguinte:



SOLIDARIEDADE E SEGURANÇA SOCIAL

Foram fornecidas ao TC as versões actualizadas das análises detalhadas de todos os programas que constituem as rotinas de cálculo e processamento de pensões, bem como as normas de actualização de pensões dos anos 1999 e 2000, para além de outras relacionadas com a identificação de beneficiários e de gestão de requerentes e requerimentos.

Foram também fornecidos os códigos de alguns programas que constituem o cálculo de pensões.

Dada a complexidade da rotina de cálculo, uma vez que inclui todas as actualizações resultantes da legislação publicada desde 1974 até à data actual, bem como das variadíssimas situações especiais contempladas, é provável que a simples leitura destes documentos levante significativas dificuldades.

Concluindo: considera-se que existe *documentação suficientemente detalhada para discriminar todas as especificidades inerentes ao cálculo e permitir guardar um rasto adequado das alterações efectuadas.*

2.6. PAGAMENTO DAS PENSÕES

2.6.2.- SITUAÇÃO ACTUAL

Quanto ao conhecimento oportuno do falecimento dos pensionistas.

Naturalmente que o falecimento dos pensionistas será sempre um facto de conhecimento "à posteriori", pelo que potencial causador de pagamentos indevidos. É um risco inerente ao Sistema.



SOLIDARIEDADE E SEGURANÇA SOCIAL

No entanto, este risco é largamente atenuado porque do falecimento dos pensionistas poderão resultar, na maior parte dos casos, benefícios por morte. Por outro lado, acresce o facto de no desenvolvimento da sua actividade o CNP contacta uma vez por ano e por via postal todos os seus pensionistas (envio da declaração anual), controlando as devoluções de correspondência.

Por estas razões, quando a banda do Ministério da Justiça é cruzada com o a Base de dados de Identificação, já a esmagadora maioria dos pensionistas falecidos estão excluídos.

- ENVIO DE FICHEIROS E PENSÕES DEVOLVIDAS

Conforme é referido, os ficheiros com os registos electrónicos resultantes do processamento são enviados para os Bancos e para os CTT.

Enquanto as bandas enviadas para os CTT são, depois de lidas, reenviadas ao CNP e integradas no sistema informático, permitindo assim um conhecimento imediato sobre os vales que irão ser emitidos (número de vale e data e n.º de emissão), na banca as bandas de retorno não têm tratamento informático.

Após a leitura das bandas por parte das instituições bancárias, estas enviam, em suporte papel, listagens onde constam discriminados, por número de pensionista, os valores que não foram creditados.

Estes dois procedimentos em nada diferem relativamente à segurança dos recebimentos das pensões:

- No pagamento por vale de correio tem-se a certeza que o vale vai ser emitido;
- No pagamento pela banca tem-se a certeza que a conta do pensionista vai ser creditada;



SOLIDARIEDADE E SEGURANÇA SOCIAL

No primeiro caso, ao fim de 60 dias, os CTT enviam um ficheiro com os vales emitidos e não pagos e sempre que há lugar a pagamentos indevidos, a confirmação do devedor poderá ser feita através do pedido de fotocópia do vale.

No caso dos pagamentos por crédito em conta, não há valores não creditados (v.g. por erros do NIB, dado que foi confirmado antes) e, havendo pagamentos indevidos, diligencia-se a sua reposição quer junto da banca (tem havido uma resposta muito positiva por parte de toda a banca para este efeito), quer junto dos herdeiros do pensionista falecido.

- POSIÇÃO E RECONCILIAÇÃO BANCÁRIAS

Atendendo a que, nas devoluções enviadas pela banca, são discriminados os pensionistas e o valor das respectivas pensões, é possível efectuar, juntamente com o extracto bancário, a reconciliação bancária, uma vez que os créditos registados no extracto estão devidamente identificados, permitindo assim actualizar, sistematicamente, a posição bancária e proceder à contabilização no mês respectivo. A lista de pendentes referida, assim como o desfasamento de dois meses, em média, em valores por reconciliar só poderá existir nos casos de reposições de pensões e relativamente a valores que estejam por identificar.

2.6.3 RISCOS SIGNIFICATIVOS IDENTIFICADOS E SEUS IMPACTES

Os ficheiros de pagamento enviados para as instituições bancárias são remetidos, uma vez por mês, através de banda magnética ou por file-transfer, contendo os elementos referentes a novos pensionistas e todas as rectificações introduzidas pelos serviços competentes e que irão ter reflexo no processamento do mês em causa.

Os pagamentos indevidos resultam, essencialmente, de pagamentos efectuados para além da morte do pensionista. Logo que haja conhecimento do óbito, quer por



SOLIDARIEDADE E SEGURANÇA SOCIAL

habilitação aos benefícios por morte, quer através da banda do Ministério da Justiça, é desencadeado um processo de recuperação através do qual o CNP procura reaver todos os valores pagos indevidamente.

No que concerne às pensões não pagas poderem não ser devolvidas pela banca ao CNP, esta questão só poderá ser equacionada se se puser em causa a credibilidade da banca e nos casos de não reclamação por parte dos beneficiários lesados.

De facto, todos os intervenientes no pagamento duma pensão têm de comprovar a entrega do valor da pensão ao pensionista no caso de reclamação ainda que tardia.

3.- AVALIAÇÃO DOS PROCESSOS DE GESTÃO DE TI

3.2.- DESENVOLVIMENTO E IMPLEMENTAÇÃO DE SOLUÇÃO

3.2.7. GESTÃO DA MUDANÇA

3.2.7.2.- SITUAÇÃO ACTUAL

Não compreendemos a referência a que *"No CNP ... verificou-se que os desenvolvimentos e testes de novas aplicações ou novas funcionalidades são efectuados directamente no ambiente de produção"*, dado que no ISSS-CNP existem duas máquinas diferentes: a 2200/500 para desenvolvimento e o ClearPath para produção, não tendo a equipa de desenvolvimento possibilidade de acesso à máquina de produção.

3.3.- OPERAÇÃO DO AMBIENTE INFORMÁTICO



SOLIDARIEDADE E SEGURANÇA SOCIAL

3.3.5. Assegurar a Continuidade dos Serviços Prestados

Contrariamente ao referido, existe um procedimento que obriga a guardar cópias de segurança fora das instalações de processamento na Av. da República, existindo para o efeito um cofre forte na Rua Filipe de Magalhães.

3.3.6. ASSEGURAR A SEGURANÇA DOS SISTEMAS

3.3.6.2.- SITUAÇÃO ACTUAL – CENTRO NACIONAL DE PENSÕES

Qualidade das Passwords

Apesar de cada password ter no mínimo 3 caracteres, seria necessário a entrada no sistema para acesso ao ficheiro onde estão encriptadas. Consideramos esse acesso muito difícil, como é aliás referido no relato na página 89, último parágrafo.

As únicas pessoas detentoras de password são os técnicos de informática da área de sistemas e de bases de dados, num total de 9 pessoas, para além dos operadores-chefe.

É da responsabilidade deste número reduzido de funcionários a gestão das respectivas passwords que são alteradas quando entendem necessário.

3.3.12. GESTÃO DE DADOS

Tal como referido relativamente ao ponto - 3.3.5. Assegurar a Continuidade dos Serviços Prestados, também as cópias de segurança dos dados são guardadas no cofre forte instalado fora das instalações dos serviços, pelo que consideramos salvaguardada a sua integridade em caso de acidente.



SOLIDARIEDADE E SEGURANÇA SOCIAL

3.3.14. GESTÃO DAS OPERAÇÕES

Contrariamente ao referido, existe no ISSS-CNP um planeamento diário com as operações a executar.

Dado que o sistema é desligado ao fim de semana, existe ainda um manual de operação com os procedimentos pormenorizados para ligar e desligar o sistema.

CONCLUSÕES:

- 1.- Consideramos que muitas das observações constantes do Relato constituirão mais um importante contributo para o permanente esforço de melhoria do sistema de informação relativo à gestão das prestações diferidas, pelo que não deixarão de ter concretização nos próximos planos de actividade dos organismos envolvidos;
- 2.- Aliás e como é sabido, o sistema de informação da SSS encontra-se em profunda reformulação, designadamente através da integração de Bases de Dados Nacionais, pelo que muitas das ineficiências conhecidas serão ultrapassadas nessa oportunidade e permitirão uma prestação de serviços ao cidadão de maior qualidade.
- 3.- Esperamos que os esclarecimentos prestados contribuam para a correcção de algumas das conclusões, designadamente as relativas à segregação de funções;

Lisboa, 14/06/2002.