Universidade do Estado do Rio de Janeiro
Centro de Ciências Sociais
Faculdade de Administração e Finanças

Kleber Rodger Reis

Controle interno em órgão público: um estudo do Sistema de Pagamento de Pessoal da Marinha do Brasil

Rio de Janeiro
2012

Kleber Rodger Reis

Controle interno em órgão público: um estudo do Sistema de Pagamento de Pessoal da Marinha do Brasil

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Pós-Graduação em Ciências Contábeis, da Universidade do Estado do Rio de Janeiro. Área de concentração: Controle de gestão.

Orientador: Prof. LD. Lino Martins da Silva

Rio de Janeiro

2012

CATALOGAÇÃO NA FONTE
UERJ/REDE SIRIUS/BIBLIOTECA CCS/B

R375 Reis, Kleber Rodger.
Controle interno em órgão público: um estudo do Sistema de pagamento da Marinha do Brasil / Kleber Rodger Reis. − 2012.
155f.

Orientador: Lino Martins da Silva.
Dissertação (Mestrado) − Universidade do Estado do Rio de Janeiro, Faculdade de Administração e Finanças.
Bibliografia: f. 135-145.

1. Pagamento − Administração − Teses. 2. Sistemas de remunerações salariais. 3. Brasil. Marinha. 4. Controle organizacional − Teses. 5. Setor público − Teses. I. Silva, Lino Martins da, 1940- II. Universidade do Estado do Rio de Janeiro. Faculdade de Administração e Finanças. III.Título.

CDU 65.011.56:331.2

_____ 07/02/2012

Assinatura Data

Kleber Rodger Reis

Controle interno em órgão público: um estudo do Sistema de Pagamento de Pessoal da Marinha do Brasil

Dissertação apresentada, como requisito parcial para obtenção do título de Mestre, ao Programa de Pós-Graduação em Ciências Contábeis, da Faculdade de Administração e Finanças da Universidade do Estado do Rio de Janeiro. Área de concentração: Controle de gestão.

Aprovada em 7 de fevereiro de 2012

Banca Examinadora:

_____

Prof. LD. Lino Martins da Silva (Orientador)
Universidade do Estado do Rio de Janeiro

_____

Prof. LD Julio Sergio de Souza Cardozo
Universidade do Estado do Rio de Janeiro

_____

Prof. Dr. (PhD) Paulo Sergio Pagliusi
Information Systems Audit and Control Association

Rio de Janeiro

2012

DEDICATÓRIA

Ao Deus da minha salvação, por tudo.

A meus pais, que me ensinaram o caminho que deveria trilhar.

A minha esposa Yeda e minha filha Danielle, pelo carinho, tranquilidade, harmonia, amor e compreensão que possibilitaram a conclusão deste estudo.

AGRADECIMENTOS

Ao Professor Lino Martins, pela orientação segura e contribuição ao aprendizado dos diversos pontos relativos à contabilidade pública, ao controle e demais assuntos, sem os quais não poderia ter concluído este estudo.

Ao Professor Marcelo Castilho, pela contribuição ao aprendizado dos diversos pontos relativos à Tecnologia da informação.

À Marinha do Brasil, pela confiança em mim depositada e por todo o investimento e capacitação que foram decisivos para meu êxito.

Ao Comandante Quadra, por contribuir com sua larga experiência na área de pagamento de pessoal da Marinha do Brasil.

Ao Comandante Davis, por contribuir com sua experiência e indicar os melhores caminhos para que este estudo fosse bem sucedido.

Ao Comandante Erivelton, por colaborar com sua experiência e indicar materiais e procedimentos para o sucesso deste estudo.

Aos demais chefes navais, que me ajudaram com seus conhecimentos e experiências.

À Coordenação, aos professores e servidores do Mestrado em Ciências Contábeis da Universidade do Estado do Rio de Janeiro, que com seu trabalho muito colaboraram para o bom andamento de todo o curso e para a defesa desta dissertação.

Aos amigos e colegas que torceram, apoiaram e estiveram lado a lado nos diversos passos dessa trajetória.

A todos que, direta ou indiretamente, contribuíram com a dissertação.

Toda leitura é divinamente inspirada e proveitosa para ensinar, para aprender, para corrigir, para instruir em justiça.

2 Timóteo 3:16

RESUMO

REIS, Kleber Rodger. *Controle interno em órgão público:* um estudo do Sistema de Pagamento de Pessoal da Marinha do Brasil. 2012. 155f. Dissertação (Mestrado em Ciências Contábeis) – Faculdade de Administração e Finanças, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2012.

Os administradores da atualidade convivem, por um lado, com o aumento permanente das demanda dos cidadãos por serviços públicos e, por outro lado, com a carência de recursos e a resistência da população à elevação da base tributária. Tal dilema exige que, cada vez mais, os sistemas de controle interno sejam fortalecidos, com o objetivo de disponibilizar informações confiáveis que possibilitem o controle das operações e a melhora do processo de tomada de decisões. Assim, o presente estudo procurou investigar se o sistema de controle interno utilizado pelo Sistema de Pagamento de Pessoal da Marinha do Brasil atende às leis, regulamentos e demais normas vigentes na esfera federal e ao que prevê o referencial teórico e os estudos acadêmicos sobre o assunto. Por meio de um estudo de caso se perseguiu expor os conceitos de controle interno, apresentar processamento da folha de pessoal e analisar o controle interno adotado pelo sistema atual, bem como o processo de atualização do software responsável e seus controles. As fontes utilizadas foram bibliográfica, documental, observação direta e entrevistas semiestruturadas. Foram, também, identificados pontos a explorar e a gerenciar dentro de categorias de requisitos de software, de modo a mitigar os riscos e maximizar as oportunidades do negócio. Os resultados indicam que o processo de modernização, ainda não concluído, está convergindo para uma maior adequação do processamento da folha de pagamento de pessoal às melhores práticas existentes, de modo que seus controles atendam às normas vigentes e ao que prevê a área acadêmica sobre o assunto. A conclusão do presente estudo apontou que o referido sistema de controle interno atende às leis, regulamentos e demais normas vigentes na esfera federal e, parcialmente, ao que prevê o referencial teórico e os estudos acadêmicos sobre o assunto.

Palavras-Chave: Controle Interno. Folha de Pagamento. Tecnologia da Informação.

ABSTRACT

Nowadays administrators have on one hand, the increasing demand for public services and, on the other hand, few resources and public resistance to increasing tax base. This dilemma requires more and more powerful internal control systems in order to provide reliable information to improve operational control and decision making. Thus, this study has investigated if the internal control system used by People Payment System of the Brazilian Navy complies with laws, regulations and other federal rules, and is in agreement with theoretical arguments and academic studies on the subject. Through a case study the concepts of internal control, the activities of People Payment System and its internal control framework were exposed, as well as the respective process of upgraded software in use. The sources used were literature, documentation, direct observation and semi structured interviews. We have also identified points to explore and manage in agreement within requirements of software in order to mitigate risks and maximize business opportunities. These results suggest that the payment software upgrade, not yet concluded, will help to comply with laws and other federal rules and will lead to best practices of internal control. Study conclusion has indicated that the internal control system used by People Payment System of the Brazilian Navy complies with laws, regulations and other federal rules and partially agrees with theoretical arguments and academic studies on the subject.

Keywords: Internal Control. Payment system. Information Technology. Software.

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE ABREVIAÇÕES

ABNT	Associação Brasileira de Normas Técnicas.
ACFE	Association of Certified Fraud Examiners
BDI	Banco de Dados Integrador
CASNAV	Centro de Análise de Sistemas Navais
CF	Constituição da República Federativa do Brasil
CFC	Conselho Federal de Contabilidade
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPF	Cadastro de Pessoas Físicas
DAdM	Diretoria de Administração da Marinha
DATAPREV	Empresa de Tecnologia e Informações da Previdência Social
DBA	Database Administrator
DFM	Diretoria de Finanças da Marinha
DIRF	Declaração de Imposto de Renda Retido na Fonte
DL	Decreto-Lei
FASB	Financial Accounting Standards Board
HTTPS	Hypertext Transfer Protocol Secure
INTOSAI	International Organization of Supreme Audit Institutions
IPSAS	Institute for International Public Sector Accounting Standards
IQ	Informante Qualificado
IQ-MB	Informantes Qualificados da Marinha do Brasil
IQ-EX	Informantes Qualificados Extra-MB
IQ-P	Informante Qualificado Privilegiado
ITGI	Information Technology Governance Institute
LRF	Lei de Responsabilidade Fiscal
MB	Marinha do Brasil
Mod-AD	Módulo de Atualização de Dados do SISPAG2
Mod-CD	Módulo de Captação de Dados do SISPAG2
Mod-CF	Módulo de Cálculo da Folha de Pagamento do SISPAG2
Mod-INLE	Módulo Interface com o Sistema Legado do SISPAG2
MPOG	Ministério do Planejamento, Orçamento e Gestão
MPS	Melhoria do Processo de Software

MPS.BR	Melhoria do Processo de Software Brasileiro
NBC T 16	Normas Brasileiras de Contabilidade Aplicadas ao Setor Público
OC	Organizações Centralizadoras
OMC	Organizações Militares Centralizadas
OP	Órgão Pagador
PAPEM	Pagadoria de Pessoal da Marinha
PASEP	Programa de Formação do Patrimônio do Servidor Público
RAIS	Relação Anual de Informações Sociais
RBEN	Repasse de Beneficiários
PMI	Project Management Institute
RR	Relação de Remuneração
RUP	Rational Unified Process
SCIMB	Sistema de Controle Interno da Marinha do Brasil
SCIPEF	Sistema de Controle Interno do Poder Executivo Federal.
SFC	Secretaria Federal de Controle Interno.
SI	Sistema de Informação
SIAFI	Sistema Integrado de Administração Financeira do Governo Federal
SIAPE	Sistema Integrado de Administração de Recursos Humanos
SIDOR	Sistema Integrado de Dados Orçamentários
SIGPlan	Sistema de Informações Gerenciais e de Planejamento
SIPEM	Sistema de Inativos e Pensionistas da Marinha
SISPAG	Sistema de Pagamento de Pessoal da Marinha do Brasil
SISPAG2	Sistema de Pagamento de Pessoal da Marinha do Brasil em modernização
SISPAG-EX	Sistema de Pagamento de Pessoal da Marinha do Brasil no Exterior
SISRES	Sistema de Responsabilidade
SWOT	Strengths, Weaknesses, Opportunities and Threats
TI	Tecnologia da Informação
TCU	Tribunal de Contas da União.
UG	Unidade Gestora
UO	Unidade Orçamentária

SUMÁRIO

INTRODUÇÃO

Os administradores da atualidade convivem, por um lado, com o aumento permanente das demanda dos cidadãos por serviços públicos e, por outro lado, com a carência de recursos e a resistência da população à elevação da base tributária. Tal dilema exige que, cada vez mais, os sistemas de controle interno sejam fortalecidos com o objetivo de disponibilizar informações confiáveis que possibilitem o controle das operações e a melhora do processo de tomada de decisões.

O fortalecimento do controle interno pode contribuir para uma melhor utilização dos recursos públicos, proporcionando uma prestação de serviços de qualidade para atender às diversas demandas sociais envolvidas. A discussão sobre controle interno não é tão nova, principalmente no Brasil, mas vem passando por profundas mudanças nas últimas décadas e ganhando destaque no plano internacional.

Diversos agentes políticos utilizam declarações recorrentes de apoio ao controle estatal em seus discursos, fazendo de certas expressões, como o "fazer mais com menos" verdadeiros jargões da moda: "É possível gastar com qualidade, fazer mais com menos" (BELCHIOR, 2011, p.1) e "Além disso, torna-se necessário melhorar os mecanismos de controle dos gastos e otimizar o uso dos recursos disponíveis. Devemos aprender a fazer mais com menos" (MERCADANTE, 2011, p.1) são alguns exemplos. Essas e outras declarações demonstram a preocupação do alto escalão da administração pública com medidas que viabilizem a eficiência, eficácia e economicidade do gasto público. Um controle interno bem orientado e organizado pode contribuir para o alcance dessa meta.

Toda instituição se vê obrigada a uma busca constante do aprimoramento da gestão de seus processos internos e das formas de comunicação desses processos com os diferentes interessados. Tendo os processos bem definidos e as responsabilidades atribuídas às diversas áreas, uma organização consegue alcançar seu objetivo final que é a melhoria dos serviços prestados com menores custos e maior rapidez e produtividade.

Os gastos do governo brasileiro têm aumentado significativamente no decorrer da história recente. Esse problema, porém, tem sido contrabalançado com sucessivos recordes de arrecadação. Até mesmo, arrecadações vinculadas a fontes finitas (*royalties* etc.) parecem estar servindo de suporte à expansão dos gastos. Um estudo recente de Werner (2009, p. 314) indica que, em pouco mais de meio século, os gastos governamentais como proporção do PIB saltaram de 19,1% (1949) para 26% (2005) e, em contraponto, a carga tributária, também

proporcional ao PIB, passou de 14,9% (1949) para 38% (2006). Esses dados incluem todos os níveis de governo, excetuando-se as empresas estatais.

Dentro desse cenário, ano após ano, uma maior parcela do orçamento da União, Estados e Municípios tem se destinado a pagamento de pessoal ativo, inativo e pensionista. Em uma visão mais restrita, os orçamentos dos comandos militares têm se destinado em grande parte à manutenção da máquina pública, em especial à folha de pagamento de pessoal militar e civil. Dos recursos previstos no orçamento de 2011 (Lei 12.381, de 9 de fevereiro de 2011) para o Comando da Marinha, R$ 11,33 bilhões (70,83%) correspondem à despesa com pessoal e encargos sociais. Dentro desse contexto, especial atenção deve ser dada pela Marinha do Brasil à administração e controle dos gastos com seu pessoal, por representar, como exposto, mais de dois terços do volume financeiro administrado pela mesma.

Devido ao volume financeiro envolvido no processamento da folha de pagamento de pessoal, os riscos potenciais da ocorrência de práticas inadequadas, desvios e fraudes devem ser vistos e revistos exaustivamente. Também a oportunidade de negócio que se abre dentro desse contexto é enorme, um controle bem sucedido da folha de pagamento pode ser exportado para outros comandos militares e, até mesmo, com algumas adaptações, para o governo federal como um todo. Portanto, os procedimentos de controle do processo de pagamento de pessoal carecem de atualizações constantes, face aos desafios que se apresentam.

Cabe destacar que a referida atividade envolve o provimento de recursos financeiros a um contingente estimado em oitocentas mil pessoas, envolvendo militares (da ativa, da reserva e reformados), pensionistas e dependentes. Desta forma, um fator crítico envolvido é o impacto social que pode ser gerado pela insatisfação dos clientes pelo atraso ou não pagamento das importâncias devidas por falha no processo de pagamento. Este risco deve ser minimizado ou extinto pelos diversos mecanismos de controle existentes em um adequado sistema de processamento de pagamentos, tendo em vista as demandas sociais que podem ser geradas por um fato isolado. O comprometimento de toda a folha por problemas sistêmicos deve ser considerado inaceitável.

Face ao volume de trabalho e aos riscos envolvidos na atividade de administração de recursos humanos da referida Força, um controle interno bem estruturado e presente deve estar organizado, com melhores práticas de controle e domínio sobre interações que ocorrem no referido processo.

Os sistemas informatizados podem contribuir para um incremento de qualidade e segurança das atividades de controle interno, por meio da eliminação de rotinas de controle

desnecessárias ou ambíguas e do refinamento de atividades, relatórios e controles, de modo a haver um incremento da relação custo-benefício dos trabalhos.

Para um melhor atendimento às demandas do processamento da folha de pagamento e maior gerenciamento de todas as atividades envolvidas, o Comando da Marinha iniciou, nos primeiros anos do novo milênio, os debates sobre uma modernização do Sistema de Pagamento de Pessoal da Marinha. Mas, somente em meados de 2008, ocorre o que pode ser considerado como o marco inicial do processo de modernização, com a formação da equipe responsável, a designação do Centro de Análise de Sistemas Navais (CASNAV) para gerência técnica e a definição do projeto de trabalho. O novo sistema recebe o nome de SISPAG2.

Finalmente, o Comando de Força decide pela terceirização e efetiva, em 2009, a contratação de serviços de Tecnologia da informação (TI) para o desenvolvimento e implantação do projeto SISPAG2. Os motivos para a implantação do novo sistema foram promover, entre outros aspectos, maior segurança, eficiência e eficácia, em menos tempo e com maior controle, disponibilizando informações corretas e tempestivas aos verdadeiros agentes responsáveis. Como requisito de integração com outros sistemas, foi deliberado que o pagamento de pessoal deveria utilizar a base de dados de pessoal, a cargo da Diretoria de Pessoal Militar da Marinha, do Comando do Pessoal de Fuzileiros Navais e do Serviço de Inativos e Pensionistas da Marinha.

Dentro desse contexto, a presente pesquisa terá como tema a análise do controle interno utilizado pelo Sistema de Pagamento de Pessoal da Marinha, em fase de modernização, por onde passará a maior parte dos recursos financeiros destinados ao respectivo Comando Militar.

A busca por melhores práticas de controle interno tem motivado profissionais e acadêmicos no intuito de atender às necessidades gerenciais e criar o arcabouço para um adequado controle interno. Foi focado nessa preocupação que surgiu o problema de pesquisa do presente estudo: o sistema de controle interno utilizado pelo Sistema de Pagamento de Pessoal da Marinha do Brasil atende às leis, regulamentos e demais normas vigentes na esfera federal e ao que prevê o referencial teórico e os estudos acadêmicos sobre o assunto?

A discussão desse tema possui relevância, na medida em que pretende contribuir para melhoria do controle interno na Marinha do Brasil e nos demais órgãos governamentais, servindo de base para o desenvolvimento e aperfeiçoamento do planejamento estratégico e das atividades operacionais e gerenciais realizadas em cada uma de suas unidades.

O objetivo geral do estudo é contribuir para o aprimoramento do controle interno dos sistemas de informação governamentais e, mais especificamente, do Sistema de Pagamento de Pessoal da Marinha.

Os objetivos específicos desse estudo serão os seguintes:

- Revisar a literatura sobre controle interno, visando identificar as melhores práticas aplicáveis aos sistemas de informação.
- Analisar o processo de modernização do SISPAG e sua adequação ao que prevê o referencial teórico sobre o assunto.
- Identificar pontos a explorar e a gerenciar no Sistema de Pagamento de Pessoal da Marinha do Brasil.

O debate acadêmico sobre as atividades de controle forma um importante referencial teórico que leva a um delineamento normativo e legal sobre o assunto. Dessa forma, os procedimentos contábeis são discutidos e as normas contábeis e seus respectivos instrumentos legais podem ser instituídos de maneira mais consistente. Esse constante processo de crítica doutrinária objetiva o aperfeiçoamento contínuo dos procedimentos administrativos e um maior grau de confiabilidade das informações produzidas para apoio ao processo decisório.

A importância da abordagem está no fato de poucos estudos na área de Contabilidade terem se dedicado a investigação de sistemas informatizados e suas potencialidades para o desenvolvimento e implantação das melhores práticas contábeis no ambiente organizacional. Os estudos desse tipo ligados à Administração Pública existem em número ainda mais reduzido.

Dessa maneira, a presente pesquisa pretende, ainda, contribuir para o caráter multidisciplinar exigido cada vez mais dos profissionais e acadêmicos ligados às Ciências Contábeis.

Esta dissertação está estruturada em quatro seções. A Introdução traz os objetivos do estudo, justificativa e problema de pesquisa. A primeira seção aborda o referencial teórico utilizado para fundamentar esta pesquisa. A segunda parte apresenta a metodologia utilizada no desenvolvimento do presente estudo. A seção subsequente aborda a análise do sistema em estudo. Finalmente, a última seção apresenta os resultados e conclusões encontrados.

1 REFERENCIAL TEÓRICO

Esta seção aborda os conceitos de controle, controle interno, Administração Pública, informação contábil e tecnologia da informação, bem como apresenta as correlações entre esses importantes pontos dentro do contexto da presente pesquisa.

1.1 Tipos e formas de controle

Em uma atualidade de recursos cada vez mais escassos para a administração pública, o emprego de ferramentas que contribuam para uma maior qualidade do gasto público torna-se um ponto chave para uma organização ser bem sucedida. Um controle interno eficiente e eficaz pode representar um grande diferencial para o sucesso das entidades que despertarem para a importância dessa atividade.

Uma organização privada ou pública deve desenvolver funções básicas que são, também, conhecidas como funções administrativas clássicas. Gil (1998, p. 23) destaca essas funções da seguinte maneira:

- Planejamento: determinação de padrões via sistemas de informações computadorizados, ou seja, informações que traduzem expectativas de comportamentos futuros.
- Execução: caracterização via sistemas de informações computadorizados de medidas, ou seja, informações que representem o registro das operações.
- Controle: acompanhamento via sistemas de informações computadorizados de desvios, ou seja, informações resultantes do cruzamento de medidas com padrões, e obtenção, em termos quantitativos, da intensidade, abaixo ou acima, em que as medidas estiveram em relação aos padrões.

Tompkins (2005, p. 59, p. 263) ensina que as atividades de trabalho das organizações apresentam uma necessidade de controle, o qual deve orientar os processos internos da entidade para consecução de seus objetivos.

Controle, em tema de administração pública, é a faculdade de vigilância, orientação e correção que um Poder, órgão ou autoridade exerce sobre a conduta funcional de outro (MEIRELLES, 2004, p. 639).

No caso especial das entidades públicas, os mecanismos de controle não voltados para uma verdadeira administração pública gerencial têm se demonstrado, por vezes, insatisfatórios.

> Os atuais mecanismos de controle burocráticos e formais são insuficientes para avaliar os resultados alcançados e para tornar efetiva a responsabilidade dos gestores públicos. As burocracias são impessoais, porque o foco é no processo. Assim, não fica claro ao cidadão quem produziu ou deveria ter produzido um resultado. É preciso haver identificação precisa entre os resultados e as pessoas por eles responsáveis, só assim pode existir "accountability". Até mesmo a falta de informação pode ser minimizada se soubermos quais são as metas e quem são os responsáveis (MAWAD, 2001, p. 12).

Para Cruz e Glock (2003, p. 20), o controle se distingue pela averiguação sistemática de registros, de maneira periódica ou permanente, pautada em documento ou outro meio, objetivando a conformidade com o padrão estabelecido, ou com o resultado esperado, ou, ainda, com a legislação e normas em vigor.

Como ensina Meirelles (2004, p. 640), os tipos e formas de controle variam segundo o Poder, órgão ou autoridade que o exercita ou o fundamento, o modo e o momento de sua efetivação e, portanto, conforme o seu fundamento considera-se hierárquico ou finalístico; consoante à localização do órgão que os realiza, pode ser interno ou externo; segundo o momento de sua realização, são considerados prévios ou concomitantes ou, ainda, corretivos; e, finalmente, quanto ao aspecto de controle, podem ser de legalidade ou de mérito.

Em decorrência do exposto, quanto a seu fundamento, um órgão ou autoridade instituída pode exercer o controle de duas formas:

- Controle hierárquico: é o que está relacionado ao aspecto burocrático da Administração Pública, em que um ou mais órgãos se subordinam a um órgão superior.
- Controle finalístico: como ministra Meirelles (2004, p. 641), é o que a norma legal impõe às entidades autônomas, indicando a autoridade controladora, as faculdades a serem exercitadas e as finalidades objetivadas, sendo, por isso mesmo, sempre um controle limitado e externo.

Em outro aspecto, pode-se, também, classificar o controle quanto à localização do órgão que os realiza, conforme abaixo:

- Controle Interno: "[...] é todo aquele realizado pela entidade ou órgão responsável pela atividade controlada, no âmbito da própria Administração" (MEIRELLES, 2004, p. 641).
- Controle Externo: é o que é realizado por entidade diferente da controlada. É realizado pelo Legislativo, Tribunal de Contas da União (TCU), empresas de auditoria independente e órgãos reguladores, entre outros.

De acordo com o momento de sua realização, os controles recebem outras denominações, podendo ser conhecidos como:

- Controle antecedente, prévio, preventivo ou *a priori* – é aquele que antecede a execução das atividades, sendo realizado por meio de leis, normas, manuais, instruções, regimentos, regulamentos, contratos e convênios.
- Controle concomitante ou sucessivo – é o que "[...] é exercido através da vigilância sobre o trabalho administrativo, à medida que ele se processa como emissão de empenhos, arrecadação de receita etc" (SILVA, 2009, p. 22).
- Controle subsequente, corretivo ou *a posteriori* – é o que se efetiva após a conclusão do ato controlado, buscando corrigir eventuais defeitos, declarar sua nulidade ou dar-lhe eficácia (MEIRELLES, 2004, p. 642).

Outra classificação encontrada é quanto ao aspecto de controle:

- Controle de legalidade ou legitimidade, que é o que "[...] objetiva verificar unicamente a conformação do ato ou do procedimento administrativo com as normas legais que o regem" (MEIRELLES, 2004, p. 642); e
- Controle de mérito é o destinado "[...] à comprovação da eficiência, do resultado, da conveniência ou oportunidade do ato controlado" (MEIRELLES, 2004, p. 642).

Cruz e Glock (2003, p. 20) propõem uma classificação, usada especialmente na área pública estatal, semelhante à supracitada: Controles formais (para garantia da observância à legislação e às normas disciplinares) e Controles substantivos (para assegurar a eficiência e eficácia na aplicação de recursos, em termos quantitativos e qualitativos).

Diversos autores (PEIXE, 2006; SÁ, 1998; SILVA, 2009; ALMEIDA, 2010; entre outros) dividem o controle em dois tipos: contábil e administrativo (ou operacional). Nesse contexto, Silva (2009, p. 20) afirma que:

- Controle contábil: engloba o plano de organização e rotinas, métodos e procedimentos relacionados à salvaguarda dos ativos e a fidedignidade dos registros. Peixe (2006, p. 105) complementa que o objetivo do controle contábil é "[...] assegurar a veracidade dos registros das operações no que se refere à legalidade e fidedignidade funcional dos agentes da administração".
- Controle administrativo ou operacional: engloba o plano da organização e rotinas, métodos e procedimentos relacionados à eficiência das operações e ao atendimento das políticas administrativas, estando indiretamente relacionado aos registros. Peixe (2006, p. 105) complementa que o objetivo do controle administrativo é "[...] acompanhar as operações, intervindo na sua realização com a finalidade de

assegurar a continuidade dos programas de trabalho do governo, mormente no que se refere à conveniência e oportunidade da sua efetivação".

Segundo Sá (1998, p.107), um controle depende fundamentalmente da qualidade do pessoal e da excelência técnica do método de trabalho, estando sua eficiência relacionada ao emprego de métodos, meios e pessoal adequado.

Para Peixe (2006, p. 108-110), qualquer mecanismo de controle para ser bem sucedido em seu objetivo requer o atendimento dos seguintes princípios básicos:

1. Definição de autoridade e responsabilidade: todos os indivíduos que compõem a administração pública devem ter seus deveres estabelecidos de forma precisa. A administração pública cumpre isso, em seu contexto, pela definição da autoridade.
2. Segregação de funções: nenhuma pessoa deve ser responsável por uma parcela significativa de qualquer transação, seja para fins operacionais ou contábeis. Esta regra é denominada de oposição de interesses, pois procura fazer com que cada indivíduo ao buscar seus próprios interesses seja conduzido a controlar o ato alheio, fortalecendo o sistema de controle.
3. Estabelecimento de comprovação e provas independentes: quanto ao aspecto de comprovação e provas, é indispensável evidenciar métodos, procedimentos e o fator humano, sendo necessário, ainda, incluir processos de comprovações rotineiras e obter informações de controle independentes para que os atos praticados sejam adequadamente comprovados.

Dependendo do tipo de controle, serão acrescentados outros princípios para um desenvolvimento coerente e adequado da atividade pretendida, mas acredita-se que os princípios expostos nesta parte do estudo deverão ser observados pelos interessados no controle das diversas ações.

1.2 A Administração Pública e o controle

O entendimento do conceito de Administração Pública é de fundamental importância para que se possa prosseguir em seu debate. Ribeiro Filho (1997, p. 13) assim especifica:

> A Administração Pública compreende os meios de que se serve o Estado, entendido como ente soberano, organizado sobre um território para fins de defesa, bem-estar, ordem e progresso social, para efetivar o atendimento das necessidades públicas. Todo o conjunto da estrutura patrimonial de bens, equipamentos, tecnologias e servidores públicos, distribuídos sistematicamente em funções, programas, projetos e atividades, submetidos à lógica da

> captação e aplicação de recursos e organizados sob a égide da legalidade, impessoalidade, moralidade e publicidade dos atos, traduz a macro-entidade denominada de Administração Pública.

A evolução da administração pública brasileira começa no período colonial, passa pela elevação do país à categoria de vice-reino, amadurece no Brasil Império e evolui pelo período republicano até os dias de hoje.

Até o início de 1930, segue-se um modelo de uma Administração Pública Patrimonialista, em que o Estado é uma extensão do poder do soberano e os direitos e deveres são estabelecidos conforme a vontade do indivíduo que ocupa poder, o patrimônio público (*res publica*) se confunde com o patrimônio do soberano (*res principis*). O interesse público é relegado a um segundo plano e predominam, entre outros, o nepotismo, o coronelismo, o empreguismo, a corrupção, a troca de favores e a distribuição de títulos de nobreza a servidores públicos.

Dentro desse contexto, Ribeiro (2002, p. 67) complementa que a Constituição inicial de 1824 remonta às características de apropriação do público pelo privado, da necessidade de intermediários para a população conseguir acesso aos serviços do Estado (coronelismo e populismo) e da tendência de hierarquias de cidadania, sendo que as classes ou estamentos detentores do Poder exercem uma supercidadania, e a população em geral, uma subcidadania.

> [...] são patrimonialistas porque os critérios de sua escolha não são racional-legais, e porque constroem um complexo sistema de agregados e clientes em torno de si, sustentado pelo Estado, confundindo o patrimônio privado com o estatal. (BRESSER-PEREIRA, 2001, p. 7)

No primeiro período do governo de Getúlio Vargas (1930-1945), passa a ser realizada a reforma burocrática da Administração Pública, buscando assegurar, entre outros pontos, a existência da *res publica* distinta da *res principis* e uma estrutura mais voltada ao Capitalismo Industrial. Esse modelo ganha força com um quadro de intensificação do processo de industrialização, levando uma ampla mudança na maneira de administração do erário público. Alguns dos princípios utilizados dentro das estruturas militares passaram a ser ampliados para toda a administração pública. O critério de merecimento para provimento de cargos públicos passa a ser adotado. Persegue-se a estruturação de carreiras, baseadas na hierarquia, no formalismo e no desempenho profissional. Promove-se a valorização do controle pelo Estado, por meio de leis e de regulamentações, como meio de garantia do interesse público. Medidas de combate à corrupção, ao clientelismo e ao nepotismo começam a ser efetivadas, porém esse processo duraria ainda algumas décadas.

Nessa conjuntura, é assinado o decreto 4.536, em 28 de janeiro de 1922, que organizava o Código de Contabilidade da União. O sistema contábil federal era colocado sob a direção da Diretoria Central de Contabilidade da República e sob a fiscalização do Tribunal

de Contas. Apesar de amplamente burocrática, zelando por aspectos de legalidade e formalidade, esse documento é um dos principais alicerces do atual Sistema de Controle Interno do Poder Executivo Federal (SCIPEF).

A divisão da contabilidade pública, como se conhece hoje, em sistema orçamentário, sistema financeiro, sistema patrimonial e sistema de compensação teve um de seus principais pilares na Lei 4.320/64. Esse instrumento legal determinou, também, que a execução orçamentária e financeira dos Entes da Federação fosse controlada pelo Executivo e Legislativo, por meio de controles internos e externos, respectivamente. O art. 75 da Lei 4.320/64 dispõe que o controle da execução orçamentária compreenderá a legalidade dos atos de que resultem a arrecadação da receita ou a realização da despesa, o nascimento ou a extinção de direitos e obrigações; a fidelidade funcional dos agentes da administração responsáveis por bens e valores públicos; o cumprimento do programa de trabalho, expresso em termos monetários e em termos de realização de obras e prestação de serviços.

A Lei 4.320/64, em seu art. 77, coloca que a verificação da legalidade dos atos da execução orçamentária será prévia, concomitante e subsequente. A verificação prévia pode ser realizada, por exemplo, por uma análise prévia de notas de empenho, contratos, convênios ou acordos a serem firmados pela administração pública. A constatação concomitante pode ser realizada *in loco* durante a execução de projetos ou atividades ou por meio de relatórios periódicos. A averiguação subsequente pode ser aquela executada após conclusão de um projeto ou depois do encerramento do exercício financeiro, através da prestação de contas. O art. 78 da Lei 4.320/64 instrui que a tomada ou prestação de contas anual, quando instituída em lei ou por fim de gestão, poderá ocorrer a qualquer tempo.

Apesar de algumas estruturas burocráticas resistirem até o presente, movimentos e tentativas de instauração de um conceito gerencial na Administração Pública são visualizados há mais de meio século.

> A reforma burocrática mal havia iniciado e já em 1938 temos um primeiro sinal da administração pública gerencial, com a criação da primeira autarquia. Surgia então a idéia de que os serviços públicos na "administração indireta" deveriam ser descentralizados e não obedecer a todos os requisitos burocráticos da "administração direta" ou central. (BRESSER-PEREIRA, 2001, p. 12)

Esse novo conceito gerencial toma vulto e produz uma reforma na maneira de administrar a coisa pública. Essa reforma administrativa federal tem como um de seus documentos de maior representatividade o Decreto-Lei (DL) 200, de 25 de fevereiro de 1967, no qual a Administração Pública Federal passa a ser dividida em direta e indireta. A Administração Direta é constituída por serviços integrados na estrutura da Presidência da República e Ministérios. A Administração Indireta compreende as entidades de personalidade

jurídica própria, como autarquias, empresas públicas, sociedades de economia mista e fundações públicas.

Por força do DL 200/67, a ação governamental passa a obedecer a um planejamento, tendo como instrumentos básicos um plano geral de governo, programas de duração plurianual (gerais, setoriais e regionais), um orçamento-programa anual e uma programação financeira de desembolso. Percebe-se, nesse momento, o lançamento das bases do atual processo orçamentário, que é concretizado por meio de três instrumentos, como destacados por Santos (2010, p. 48):

a) Plano Plurianual de Investimentos (PPA): Instituído por lei, estabelece diretrizes, objetivos e metas, possibilitando que o governo ordene suas ações. É elaborado no primeiro ano de mandato de governo para vigência pelos quatro anos seguintes.

b) Lei de Diretrizes Orçamentárias (LDO): Tem a finalidade principal de orientar a elaboração dos orçamentos fiscal, de investimento das empresas estatais e da seguridade social. Busca sintonizar a Lei Orçamentária Anual com as diretrizes, objetivos e metas da administração pública, estabelecidas no PPA.

c) Lei de Orçamento Anual (LOA): Visa a concretizar metas e objetivos propostos no PPA, segundo as diretrizes estabelecidas pela LDO.

O Ministério do Planejamento, Orçamento e Gestão (MPOG, 2011, p. 1) considera o Plano Plurianual (PPA) como "[...] a principal ferramenta de planejamento para o governo organizar sua atuação, buscando obter mais resultados com menos recursos". Portanto, considera-se importante comentar o movimento de reestruturação pelo qual passa esse importante instrumento de planejamento. Esta reestruturação pretende tornar o PPA um verdadeiro espelho para as diretrizes e estratégias nacionais, deixando para o orçamento tratar como viabilizar sua execução. Nesse contexto, o MPOG (2011, p. 1) expõe que, privilegiando o monitoramento e a transparência, o PPA 2012-2015, encaminhado ao Congresso Nacional em 31 de agosto de 2011, prevê 11 Macrodesafios e 65 Programas Temáticos, em contraste com os 217 programas finalísticos previstos anteriormente no PPA 2008-2011. Diversas ações foram incorporadas em um mesmo programa reforçando, juntamente com a criação dos Macrodesafios, o caráter estratégico do PPA.

Os órgãos de direção da Administração Federal devem promover medidas que os liberem de rotinas de execução e de trabalhos de mera formalização de atos administrativos para se concentrarem em atividades de planejamento, supervisão, coordenação e controle, em conformidade com o § 2º do art. 10 do DL 200/67. Esse decreto colocou, ainda, o controle como elemento fundamental para a administração pública, ao definir os princípios

fundamentais das atividades da Administração Federal, que podem ser considerados como referências para as demais esferas públicas:

Planejamento: visa promover o desenvolvimento social e econômico, bem como a segurança nacional, mediante a elaboração de planos e programas que guiarão a execução das atividades governamentais, através de seus instrumentos básicos (plano geral de governo; programas gerais, setoriais e regionais, de duração plurianual; orçamento-programa anual; e programação financeira de desembolso).

> A LRF já fornece um roteiro para realizar uma boa gestão. Contudo, sabemos que fazer planejamento não é muito fácil. O que se exige de alguém que planeja é que tenha um conhecimento profundo da realidade, que consiga diagnosticar corretamente os problemas e encontrar as melhores soluções, que eventualmente já saiba o que não deu certo no passado para não repetir os erros, que tenha conhecimento do que outros entes da Federação já tentaram, de quais são as experiências exitosas e de como se pode inovar na gestão para melhorar (NUNES, 2011, p.16).

Coordenação: é um conjunto de ações orientadas para promover a concentração de esforços e a economia de recursos. Nesse contexto, uma matéria somente poderá ser encaminhada à decisão de uma autoridade superior, após isto ter sido coordenado por pelo menos uma autoridade subordinada, que promoverá consultas e entendimentos com os setores interessados para que surjam subsídios integrados e coerentes com a política geral e setorial de Governo. Todos os níveis da administração devem promover a coordenação, através de chefias individuais atuantes, de reuniões com as chefias subordinadas e da criação e atuação de comissões de coordenação (MEIRELLES, 2004, p. 713).

Descentralização: é a investidura de poder pelo Estado a uma pessoa para que exerça atividade pública ou de utilidade pública e não deve ser confundida com a desconcentração da Administração, que se caracteriza pela distribuição de funções a órgãos da mesma estrutura administrativa, sem quebra de hierarquia (MEIRELLES, 2004, p. 714).

Delegação de Competência: é a transferência de poder decisório a autoridades subordinadas, mediante ato administrativo, com previsão legal, que individualize a autoridade delegante, a delegada e o objeto de delegação. Busca proporcionar maior agilidade e objetividade às decisões ao promover sua aproximação da realidade dos fatos e pessoas a atender. Segundo Meirelles (2004, p. 717), pode ser considerada um ato facultativo e provisório utilizado para atender a requisitos de oportunidade e conveniência da administração pública.

Controle: é um meio de exercício do poder hierárquico, juntamente com o comando, a coordenação e a correção, em que o órgão superior controla seus órgãos subordinados, conferindo a legalidade, regularidade e demais aspectos dos atos de seus subordinados. (MEIRELLES, 2004, p. 717). O DL 200/67 estabelece ainda que:

> Art. 13 O controle das atividades da Administração Federal deverá exercer-se em todos os níveis e em todos os órgãos, compreendendo, particularmente:
> a) o controle, pela chefia competente, da execução dos programas e da observância das normas que governam a atividade específica do órgão controlado;
> b) o controle, pelos órgãos próprios de cada sistema, da observância das normas gerais que regulam o exercício das atividades auxiliares;
> c) o controle da aplicação dos dinheiros públicos e da guarda dos bens da União pelos órgãos próprios do sistema de contabilidade e auditoria.

Os componentes da Administração Federal são obrigados a disponibilizar as informações relativas a créditos orçamentários ao Tribunal de Contas, ou às suas delegações, e devem colaborar com a realização das inspeções de controle externo de órgãos de administração financeira, contabilidade e auditorias, conforme preceitua o art. 75 do DL 200/67. Já o acompanhamento da execução orçamentária será feito pelos órgãos de contabilização, de acordo com o art. 78 do DL 200/67, cabendo à contabilidade sintética ministerial à Inspetoria Geral de Finanças de cada ministério, subordinada tecnicamente à Inspetoria Geral de Finanças do Ministério da Fazenda – órgão central de controle.

Assim, com o DL 200/67, a legislação passa a tratar não somente de aspectos legais, instituindo a conhecida contabilidade gerencial ou controle gerencial na administração pública.

A criação da Secretaria do Tesouro Nacional pelo Decreto nº 92.452, de 10 de março de 1986, para órgão central do Sistema de Administração Financeira Federal e do Sistema de Contabilidade Federal, também se constitui em um ponto importante no amadurecimento da administração pública. A secretaria nasce da união da antiga Secretaria Executiva da Comissão de Programação Financeira e da Secretaria Central de Controle Interno. “Esta estrutura manteve a idéia da dupla subordinação, mas modificou a ênfase que passava de fiscalizadora para a idéia de controle interno e auditoria voltado para aspectos gerenciais e de desempenho” (SILVA, 2000, p. 4).

O art. 1º da Constituição Federal (CF) de 1988 coloca que: “A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito [...]” (BRASIL, 2010, p. 2).

> O Estado entendido como *res publica* corresponde a uma definição parcial de Estado. É, entretanto, importante, porque o Estado democrático moderno nasce quando a *res publica* é claramente distinguida da *res principis*, surgindo então um desafio fundamental para todas as democracias: a defesa da coisa pública contra a corrupção, contra o nepotismo, e contra todas as formas de privatização ou de obtenção de vantagens especiais do Estado (BRESSER-PEREIRA, 1995, p. 87).

De acordo com Carvalho (2008, p. 71), o termo Estado (*stato*) com um sentido de unidade política total foi empregado por Maquiavel em sua obra O Príncipe: “Todos os Estados, todos os domínios que tiveram e têm império sobre os homens são Estados e são ou república ou principados” (MAQUIAVEL, 1513 *apud* CARVALHO, 2008, p. 71).

O entendimento de Estado passa por diversas discussões dentro da Teoria Geral do Direito, mas pode-se dizer que:

> O Estado passa a ter existência a partir do momento em que o povo, consciente de sua nacionalidade, organiza-se politicamente e deve ser estudado como instrumento de organização política da comunidade, que inclui um sistema de funções disciplinadoras e coordenadas para atingir determinados objetivos (SILVA, 2009, p. 1).

O Estado de Direito pode ser entendido como um Estado em que todos os indivíduos, pessoas físicas ou jurídicas, sem exceção, estão obrigados ao cumprimento de leis e costumes normalmente aceitos. O Estado Democrático é aquele em que seu povo participa das decisões diretamente ou por meio de representantes eleitos, em concordância com o que coloca o § único do art. 1º da CF de 1988: "Todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta Constituição" (BRASIL, 2010, p. 2). Kersting (2004, p. 9) entende, ainda, que: "[...] a democracia fundamenta-se na autonomia individual e coletiva e na racionalidade comunicativa. Ela não pode ser imposta por uma força superior".

O art. 37 da CF de 1988 coloca princípios a serem seguidos pelos agentes públicos: "A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência [...]" (BRASIL, 2010, p. 42).

O princípio da legalidade está relacionado ao inciso II do art. 5º da CF de 1988, onde se dispõe que "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei" (BRASIL, 2010, p. 4), devendo a administração pública se sujeitar aos princípios constitucionais e às normas legais estabelecidas. O art. 77 da Lei 4.320/64, ao tratar de controle interno, coloca uma amplitude para a aplicação desse princípio: "A verificação da legalidade dos atos de execução orçamentária será prévia, concomitante e subseqüente".

O princípio da impessoalidade exige que o agente público, no atendimento do interesse público, deve tratar todos de forma igual. Para Meirelles (2004), o princípio da impessoalidade nada mais é que o clássico princípio da finalidade, o qual impõe ao administrador público que só pratique o ato para seu fim legal.

O princípio da moralidade administrativa coloca preceitos éticos para a atuação dos agentes públicos. A esses compete, como ensina Carvalho Filho (2004, p. 15), "[...] não só averiguar os critérios de conveniência, oportunidade e justiça em suas ações, mas também distinguir o que é honesto do que é desonesto".

O princípio da publicidade garante a todos o acesso a informações de atos ou fatos da administração pública, ressalvados alguns casos extremos legalmente previstos. Amplamente ligado ao referido princípio está o inciso XXXIII do art. 5º da CF/88:

> XXXIII − todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;

A eficiência, presente no art. 74 da CF/88, como forma de avaliação de resultados de gestão da Administração Federal e da aplicação de recursos públicos por entidades privadas, foi introduzida, como princípio constitucional, pela Ementa 19/1998. Costódio Filho (1999, p. 214) coloca que esse princípio poderia ser enunciado da seguinte maneira: "[...] a Administração Pública deve atender o cidadão na exata medida da necessidade deste com agilidade, mediante adequada organização interna e ótimo aproveitamento dos recursos disponíveis".

> Além de salvaguardar os bens e recursos públicos, o controle interno, assim entendido, deve avaliar e promover a eficiência operacional, ou seja, garantir que os recursos sejam empregados eficientemente nas operações cotidianas, como forma de se obter a economicidade invocada pelo art. 70 da Constituição Federal. (CRUZ; GLOCK, 2003, p. 24).

O cumprimento das exigências constitucionais e demais disposições deve, a princípio, ser perseguido por um adequado sistema de fiscalização. A CF/88 trata, em seus art. 70 a 75, da fiscalização contábil, financeira, orçamentária, operacional e patrimonial. Nesse sentido, o art. 70 institui que:

> A fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e indireta, quanto à legalidade, legitimidade, economicidade, aplicação das subvenções e renúncia de receitas, será exercida pelo Congresso Nacional, mediante controle externo, e pelo sistema de controle interno de cada Poder (BRASIL, 2010, p. 69).

Como se pode verificar, a CF/88 mantém a figura do controle externo vinculada ao Poder Legislativo, que o exercerá com o auxílio do Tribunal de Contas da União. Essa Constituição ampliou, também, a abrangência do controle interno, que na Lei 4.320/64, na CF/67 e na Emenda Constitucional nº 1 (17/10/1969) era imposto ao Poder Executivo, para que cada Poder possa estabelecer seu controle interno pelo qual será responsável. Essa difusão do poder de controle pelas três esferas governamentais deixou, também, um desafio de coordenação que, no art. 74 da própria CF/88, foi superado ao estabelecer que os três Poderes mantenham de forma integrada seus sistemas de controle interno. A Administração Federal, preocupada com o desempenho dessa tarefa dentro de sua esfera, criou a Comissão de Coordenação de Controle Interno, conforme o art. 23 da Lei 10180/ 2001.

> Ao contrário do que ocorria no passado, quando a ênfase do controle interno residia, exclusivamente, nas questões ligadas ao cumprimento dos aspectos legais do gasto público, os

> novos dispositivos trazem positivas inovações no campo do controle substantivo (GIACOMONI, 2010, p. 344).

Em 4 de maio de 2000, a Lei Complementar nº 101 ou Lei de Responsabilidade Fiscal (LRF) é sancionada para estabelecer normas de finanças públicas voltadas para a responsabilidade na gestão fiscal, aplicáveis à União, Estados, Municípios e Distrito Federal. O § 4º do art. 9º da LRF representou um avanço para o controle da execução orçamentária ao definir uma avaliação quadrimestral de resultados em relação às metas fiscais, em audiência pública, privilegiando uma maior transparência da gestão governamental. A preocupação com as verificações prévia, concomitante e subsequente (definidas na Lei 4.320/64) aparece, também, na LRF. Giacomoni (2010, p. 344) ensina que a Lei de Responsabilidade Fiscal inovou ao estabelecer competências do órgão responsável pelo controle interno, se destacando a necessidade de o responsável firmar, juntamente com a autoridade financeira e outras estabelecidas em ato próprio de cada Poder, o Relatório de Gestão Fiscal organizado por cada Poder e por órgãos dotados de autonomia, como o Ministério Público e o Tribunal de Contas.

A Lei Complementar nº 131, de 27 de maio de 2009, acrescenta dispositivos à LC 101/00 para um fornecimento, em tempo, real, de informações detalhadas sobre a execução orçamentária e financeira da União, Estados, Distrito Federal e Municípios. Para Quintana, Machado, Quaresma e Mendes (2011, p. 141) um aspecto introduzido pela LC 131/2009 "[...] envolve a adoção de sistema integrado de administração financeira e controle que atenda um padrão mínimo de qualidade estabelecido pelo Poder Executivo da União". Em síntese, a LC 131/2009 trata do estabelecimento de mecanismos que incentivem e possibilitem a participação popular nas discussões e no acompanhamento da execução orçamentária e financeira.

Na busca por atender todos os requisitos legais e normativos, o Governo Federal organizou o Sistema de Controle Interno do Poder Executivo Federal (SCIPEF), composto pela Secretaria de Controle Interno e por órgãos setoriais (art. 22 da 10.180/2001), que tem suas finalidades definidas no art. 2º do Decreto nº 3.591/2000 (em conformidade com as finalidades definidas no art. 74 da CF/88), como segue:

> I - avaliar o cumprimento das metas previstas no Plano Plurianual, a execução dos programas de governo e dos orçamentos da União;
> II - comprovar a legalidade e avaliar os resultados, quanto à eficácia e à eficiência da gestão orçamentária, financeira e patrimonial nos órgãos e nas entidades da Administração Pública Federal, bem como da aplicação de recursos públicos por entidades de direito privado;
> III - exercer o controle das operações de crédito, avais e garantias, bem como dos direitos e haveres da União;
> IV - apoiar o controle externo no exercício de sua missão institucional.

A Marinha do Brasil, seguindo a orientação dos órgãos centrais da administração, mantém estruturado o Sistema de Controle Interno da Marinha do Brasil que busca, de acordo

com norma estabelecida (MB, 2010), atender as demandas do SCIPEF e do Tribunal de Contas da União (TCU). O Sistema de Controle Interno da Marinha do Brasil (SCIMB) exerce, entre outras atribuições, as atividades de planejamento orçamentário, de programação e execução financeira, orçamentária e patrimonial e de controle interno e o controle da execução físico-financeira do Plano de Ação. O SCIMB é integrado, entre outras unidades, pela Diretoria de Finanças da Marinha que é a responsável pelas atividades de Programação Financeira e Contabilidade, possuindo como sua subordinada a Pagadoria de Pessoal da Marinha que, por sua vez, tem como responsabilidade efetuar o cálculo da folha de pagamento, efetivar os pagamentos e descontos devidos e prestar as competentes informações contábeis, fiscais e financeiras relativas ao Sistema de Pagamento de Pessoal da Marinha.

Ao longo das últimas décadas, os governos têm intensificado movimentos para viabilização de uma Administração Pública Gerencial, com um foco mais voltado para o interesse público, baseado em um processo decisório descentralizado, dando ênfase ao controle. Sucessivas declarações de políticos, ao assumirem cargos públicos, têm trazido o "[...] fazer mais, com menos [...]" como meta, o que demonstra um maior comprometimento com o princípio da eficiência. A importância de tal princípio pode ser destacada da seguinte forma: "[...] o uso ordenado e eficiente de recursos públicos constitui um dos pré-requisitos essenciais para a adequada gestão das finanças públicas e para a eficácia das decisões das autoridades responsáveis" (INTOSAI, 2009, p. I-9, tradução nossa). Assim, todos os que lidam com recursos públicos devem atentar para esse aspecto.

> Em síntese, depreende-se dos mandamentos legais que o controle das contas públicas vai além da simples verificação de obediência às normas vigentes, mas inclui ainda o aspecto relacionado à eficiência, eficácia e economicidade dos atos públicos (QUINTANA; MACHADO; QUARESMA; MENDES, 2011, p. 144).

Dentro desse contexto, torna-se essencial um entendimento dos conceitos de economicidade, efetividade, eficiência e eficácia. Segundo Cruz (1997, p. 57), a economicidade se refere a produzir mais com o uso dos mesmos recursos e mantendo ou melhorando o nível de qualidade, a efetividade consiste na verificação da existência de determinado objeto ou processo, já a eficiência consiste em executar bem algo específico, enquanto a eficácia é entendida como o fazer a coisa certa diante do objetivo planejado.

Como ensina Ribeiro (2002, p. 70), o Controle Público ou Controle do Estado evolui no mesmo sentido da transformação do próprio objeto controlado: No Estado Absolutista, o Controle Público só fazia sentido se fosse feito em nome *Del Rey*; no liberalismo dos primórdios do Estado Democrático de Direito, o Controle Estatal pouco ultrapassava o

controle judiciário, nada mais natural que no *welfare-state* fossem desenvolvidos mecanismos de respostas mais profundos e sofisticados.

1.3 Visões do controle interno

Um controle interno bem sucedido depende do ambiente organizacional e das características desse ambiente (país, setor, entidade etc.), como cultura e estrutura legal, como fatores que vão influenciar e impor aspectos específicos às referidas atividades. Em virtude dessas características, optou-se por apresentar o controle interno em visões específicas.

1.3.1 A visão do controle interno no Brasil

Em um primeiro momento, destaca-se a colaboração do estudo de Quintana, Machado, Quaresma e Mendes (2011, p. 141): "O controle interno pode ser entendido como todas as ações e medidas adotadas numa entidade, destinadas a prevenir e salvaguardar o patrimônio daquela, bem como acompanhar os processos e rotinas ali existentes".

Franco e Marra (2001, p. 267) entendem que o controle interno é um conjunto de instrumentos que permitem "[...] prever, observar, dirigir ou governar os acontecimentos [...]" que ocorrem na organização. Almeida (2010, p. 42) propõe a seguinte definição: "O controle interno representa em uma organização o conjunto de procedimentos, métodos ou rotinas com o objetivo de proteger os ativos, produzir dados contábeis confiáveis e ajudar a administração na condução ordenada dos negócios da empresa". Destaca-se que os dois primeiros se referem a controles contábeis, enquanto o último a controles administrativos.

Cook (1979, p. 131-132) coloca que o controle interno é utilizado para:

> [...] 1) para proteger seu ativo, 2) aumentar a exatidão e a fidedignidade dos dados e relatórios contábeis e de outros dados operacionais, 3) promover e avaliar a eficácia operacional de todos os aspectos das atividades da empresa e 4) comunicar as diretrizes administrativas e estimular e avaliar a observância das mesmas.

Peter e Machado (2003, p. 24) propõem uma definição mais voltada para o contexto governamental:

> Constituem Controles Internos o conjunto de atividades, planos, métodos e procedimentos interligados utilizado com vistas a assegurar que os objetivos dos órgãos e entidades da Administração Pública sejam alcançados, de forma confiável e concreta, evidenciando eventuais desvios ao longo da gestão, até a consecução dos objetivos fixados pelo Poder Público.

Nesse contexto, torna-se importante, também, a compreensão de quem é afetado ou sujeito a ações do controle interno. Nesse sentido, pode-se registrar que:

> Genericamente, estão sujeitos à atuação do Sistema de Controle Interno, quaisquer pessoas físicas ou jurídicas, públicas ou privadas que utilizem, arrecadem, guardem, gerenciem ou administrem dinheiros, bens e valores públicos ou pelos quais a União, Estado ou Município respondam, ou que, em nome destes entes, assumam obrigações de natureza pecuniária (AZEVEDO; M. LIMA; A. LIMA, 2004, p. 189).

A Secretaria de Controle Interno do Senado Federal considera como um dos princípios do controle interno a aderência às diretrizes e normas legais, colocando como fundamental o estabelecimento de sistemas organizacionais para determinar e assegurar a observância das diretrizes, planos, normas, leis, regulamentos e procedimentos administrativos internos (SENADO FEDERAL, 2011). O controle interno pode ser entendido por um somatório de estrutura e mecanismos institucionais. Cruz e Glock (2003, p. 81) assim descrevem:

> [...] o controle interno é exercido pela conjugação de estrutura organizacional com os mecanismos de controle estabelecidos pela Administração, incluindo as normas internas que definem responsabilidades pelas tarefas, rotinas de trabalho e procedimentos para revisão, aprovação e registro das operações, envolvendo aspectos contábeis e administrativos.

Além do cumprimento às normas e leis estabelecidas, os envolvidos com controle interno devem atender, também, a preceitos éticos. O estabelecimento de um Código de Ética, preferencialmente por escrito, dentro da instituição pode fornecer uma preciosa orientação.

> O emprego da ética é fundamental no exercício de qualquer profissão, em especial nas que envolvem outros profissionais, líderes políticos e grupos de interesse, como é o caso de quem atua nas atividades relacionadas com o Sistema de Controle Interno (Cruz; Glock, 2003, p. 67).

Peixe (2006, p. 103-104) registra que um sistema de controle interno deve atender alguns aspectos básicos:

- Abrangência: definir a área controlada e se os registros, informações e ajustes contábeis devem envolver todos os atos e fatos administrativos.
- Exatidão: identificar se a execução do trabalho, a avaliação dos elementos patrimoniais e as informações estão corretas.
- Legalidade – examinar se as práticas obedecem às prescrições legais.
- Disseminação das informações – identificar quem é responsável por prestar as informações e a pessoa que deve recebê-las, analisá-las e adotar as medidas cabíveis.
- Oportunidade – verificar se as atividades de controle são realizadas de forma tempestiva; fundamentalmente, um sistema de controle se interliga a um sistema

> de informações, sendo o emprego de processamento eletrônico de dados uma opção para promover alta eficiência.

Sarens e Christopher (2010, p. 292) destacam que o estabelecimento de um sistema de gestão de risco para identificar, avaliar, monitorar e gerenciar o risco, bem como para informar os interessados de alteração material no perfil de risco da organização, pode contribuir para identificar e capitalizar oportunidades para criar valor.

A Norma Brasileira de Contabilidade T 16.8 do CFC, aprovada pela Resolução nº 1.135/08 do CFC, determina que o controle interno deva fornecer suporte ao sistema de informação contábil para que seja possível minimizar riscos e oferecer efetividade às informações contábeis, contribuindo para o alcance dos objetivos da entidade pública. Nesse contexto, o CFC instituiu que o controle interno precisa ser exercido em todos os níveis da entidade pública, compreendendo o conjunto de recursos, métodos, procedimentos e processos adotados pela entidade pública, com a finalidade de:

(a) salvaguardar ativos e garantir a veracidade dos componentes patrimoniais;

(b) oferecer conformidade ao registro contábil em relação ao ato correspondente;

(c) propiciar informação oportuna e adequada;

(d) estimular adesão às normas e às diretrizes estabelecidas;

(e) cooperar para a eficiência operacional da entidade; e

(f) contribuir para a prevenção de práticas ineficientes e antieconômicas, erros, fraudes, malversação, abusos, desvios e outras inadequações.

No âmbito da administração pública, Cruz e Glock (2003, p. 80-81) lembram que o responsável pela coordenação do controle interno deve buscar uma constante atualização sobre aspectos técnicos que abarcam o assunto e, principalmente, sobre a legislação aplicável, a fim de ter plenas condições de desempenhar as demais atividades de apoio, dentre as quais, destacam-se:

a) coordenar ações de controle interno e centralizar o relacionamento com o controle externo;

b) assessorar a Administração em assuntos de controle interno e externo e de legalidade dos atos de gestão;

c) interpretar e normatizar aspectos técnicos relacionados com a legislação concernente às finanças públicas;

d) aprovar normas internas sobre rotinas e procedimentos de controle;

e) participar do processo de planejamento e acompanhar a elaboração do PPA, da LDO e do Orçamento Anual;

f) manifestar-se, quando solicitado pela Administração, acerca de regularidade e legalidade de atos, contratos e outras peças;

g) propor melhoria ou implantação de sistemas informatizados para aperfeiçoar os controles internos, melhorar rotinas e aumentar a fidedignidade das informações;

h) acompanhar sindicâncias internas e Tomadas de Contas Especiais;

i) reportar ao Tribunal de Contas irregularidades ou ilegalidades apuradas, para as quais a Administração não adotou medidas, visando à apuração de responsabilidades e ao ressarcimento de danos ao erário;

j) coordenar a preparação e o encaminhamento das prestações de contas anuais, das respostas às diligências e das peças recursais ao Tribunal de Contas;

k) manter registro e acompanhamento de processos no Tribunal de Contas que envolvam a administração da organização;

l) coordenar as respostas às solicitações de documentos e de informações pelos órgãos competentes; e

m) acompanhar auditorias *in loco* realizadas por órgãos de fiscalização.

Pode-se verificar que muitas são as responsabilidades que envolvem o setor de controle interno dentro de uma instituição pública. Portanto, o funcionário designado para exercer a mencionada função deve ter qualificação apropriada e desenvolver habilidades que atendam às expectativas inerentes à função.

Nesse sentido, Cardozo (1994, p. 35-36), Almeida (2010, p. 43-49) e Peter e Machado (2003, p. 25-26) ensinam sobre princípios do controle interno, dentre os quais se destacam os seguintes:

a) Responsabilidade: as atribuições de funcionários ou setores internos da entidade necessitam estar definidas e limitadas, de preferência por escrito, por meio da adoção de manuais internos da organização. Dessa forma, busca-se assegurar que as atividades de controle sejam executadas, de modo a identificar erros ou irregularidades e apurar responsabilidades por omissões.

b) Delegação de poderes e determinação de responsabilidades: a delegação de competência, prevista em lei, representa uma ferramenta de descentralização administrativa, com vistas a garantir maior agilidade e objetividade às decisões. O ato de delegação necessita indicar precisamente o objeto da delegação, a autoridade delegante, que concedeu poder ou responsabilidade no referido ato, e a autoridade delegada, pessoa que recebeu o referido poder ou responsabilidade. Para dar validade à delegação deve existir, também, na organização um

organograma e um regimento ou estatuto que definam adequadamente como deve ocorrer a referida delegação de autoridade e as responsabilidades dos envolvidos;

c) Rotinas internas: todas as rotinas internas devem estar estabelecidas de forma clara e objetiva em um regimento, regulamento ou manual da organização, emitido por autoridade competente. Essas rotinas compreendem, entre outras, o preenchimento de formulários internos e externos, cumprimento de atividades internas de controle (assinaturas, carimbos etc.), processos internos dos setores da entidade.

d) Acesso aos ativos: a organização necessita limitar o acesso de funcionários aos ativos e estabelecer controles físicos sobre esses. O acesso aos ativos representa manuseio de numerário recebido antes de depositado em conta corrente bancária, emissão de cheque sozinho (única assinatura) etc.

e) Segregação de funções: as funções de autorização (ou aprovação), execução, controle e contabilização devem ser exercidas por diferentes pessoas.

f) Confronto de ativos com os registros: os ativos devem ser periodicamente confrontados com os registros da contabilidade. A finalidade é detectar desfalque de bens ou até mesmo registro contábil inadequado.

g) Controles das transações: os fatos contábeis, financeiros e operacionais devem ser efetuados por atos legítimos, dentro da finalidade institucional e autorizados por quem é de direito;

h) Amarrações do sistema: o sistema de controle interno precisa ser estruturado de modo que sejam registradas somente transações autorizadas, por seus valores corretos e no período de competência. Esse fato exige conferência independente do registro, dos cálculos (imposto de renda, férias, 13º salário etc.) e de sua classificação contábil. As rotinas internas de controle devem ser estabelecidas para que uma área controle a outra.

i) Auditoria interna: a auditoria interna deve verificar se as normas internas são seguidas e avaliar a necessidade de novas normas internas ou da atualização das já existentes.

j) Relação entre custos e benefícios: o custo do controle interno não deve exceder aos benefícios que dele se espera obter. Os controles mais onerosos devem ser estabelecidos para transações de valores relevantes, enquanto que os controles mais modestos (de menor custo) devem ser implantados para as demais transações.

k) Qualificação adequada, treinamento e rodízio de funcionários: a política organizacional precisa promover a seleção e treinamento de pessoal de forma criteriosa e sistematizada, atentando, também, para um rodízio de funções e para uma obrigatoriedade do gozo de férias regularmente, entre outros pontos.

l) Aderência às leis, diretrizes e normas: na organização devem ser instituídos sistemas para determinar e garantir a observância de diretrizes, planos, normas, leis, regulamentos e procedimentos administrativos internos.

m) Registros automáticos: a utilização de processos mecanizados, além de poder contribuir com a redução de erros e de usos indevidos das informações, aumenta a eficiência do sistema de controles, permitindo a realização simultânea de vários registros.

Como percebido, muitas das atividades a serem desenvolvidas pelo controle interno envolvem um controle preventivo, que pode ser considerado o tipo de controle mais importante para garantia dos interesses organizacionais. Cruz e Glock (2003, p. 24) corroboram com essa visão: "O processo de controle interno deve, preferencialmente, ter caráter preventivo, ser exercido permanentemente e estar voltado para correção de eventuais desvios em relação aos parâmetros estabelecidos, como instrumento auxiliar de gestão".

A Resolução nº 986 do CFC, de 21 de novembro de 2003, faz uma distinção entre os importantes termos fraude e erro. Assim, a fraude se constitui em um ato intencional de omissão ou manipulação de transações e operações, adulteração de registros, informações, documentos, relatórios e demonstrações contábeis, tanto em termos físicos quanto monetários. Por outro lado, o erro representa um ato não intencional de omissão, desatenção, desconhecimento ou interpretação equivocada de fatos na elaboração de registros, informações e demonstrações contábeis, bem como de transações e operações da entidade, tanto em termos físicos quanto monetários.

Dentro desse contexto, a CGMRJ (2004, p. 9) define risco como "[...] potencial de perda para uma organização devido a erro, fraude, ineficiência, falta de aderência aos requisitos estatutários ou ações que tragam descrédito à organização e que possam afetar negativamente o alcance de seus objetivos". Ou seja, a avaliação de riscos terá como objetivo ser pró-ativa e preventiva, visando reduzir seu potencial de perda.

No combate a fraudes e usos indevidos das informações contábeis, o fortalecimento do controle interno se apresenta como uma importante ferramenta. Em estudo promovido junto a organizações públicas e privadas do *Gulf Cooperation Council*, a empresa de auditoria Deloitte (2011, p. 8) apresentou que 35% dos executivos apontaram pelo menos um caso de fraude em suas empresas no ano de 2010 e 56% dos executivos considerou que o fortalecimento dos processos internos e controles como a principal maneira para detecção de fraudes. Um estudo da KPMG (2009, p. 6) destaca, também, que controles internos inadequados foram citados por 64% dos entrevistados como a principal contribuição para ocorrência de fraudes nas organizações brasileiras. Outro estudo (KPMG, 2011, p. 10),

envolvendo 69 países, destaca que as fraquezas do controle interno contribuíram para que 74% das fraudes ocorressem.

Segundo a *Association of Certified Fraud Examiners* (ACFE, 2010), as fraudes duram uma média de 18 meses antes serem detectadas e a perda média com elas é de US$ 160.000, sendo que cerca de um quarto superam um milhão de dólares. As vítimas mais comuns foram bancos, financeiras, fábricas e setores da administração pública. Os controles bem organizados levam, segundo o referido trabalho, a perdas significativamente menores e a redução do tempo de detecção de esquemas fraudulentos. Os dados da pesquisa mostraram que a maioria das fraudes foi detectada por relatos de funcionários e que as organizações que dispunham de treinamentos com esse foco para funcionários e gestores tiveram menores perdas.

Parodi (2005, p. 209) comenta que, no Brasil, existem poucos e fragmentados dados estatísticos sobre a situação de fraudes internas e expõe que os números principais se constituem de perdas entre 7% a 10% do faturamento global das organizações, sendo 34,3% de um a dez mil reais, 44,8 % de 10 mil e 100 mil reais e 20,9% acima de 100 mil reais. Entre as causas apontadas, estão os controles fracos ou ineficientes e a ausência de acompanhamento sobre os controles.

Diversas são as metodologias existentes que buscam o fortalecimento do controle interno. Algumas dessas propostas são, de acordo com Deloitte (2003, p. 14), as seguintes:

> 1. COSO – Estrutura Integrada de Controles Internos: Desenvolvida pelo Committee of Sponsoring Organizations of the Treadway Commission e patrocinada pela AICPA, FEI e IIA, entre outros, o COSO é a estrutura dominante nos Estados Unidos. As diretrizes foram publicadas em 1991, com revisões antecipadas e atualizações posteriores. Acreditamos que esta será a estrutura escolhida pela grande maioria das companhias de capital aberto sediada nos EUA.
> 2. CoCo – Modelo de Controles: Desenvolvido pelo Criteria of Control Committee of Canadian Institute of Chartered Accountants, o CoCo concentra-se nos valores comportamentais como a base fundamental para os controles internos de uma companhia, e não na estrutura e nos procedimentos de controle.
> 3. Turnbull Report – Controles Internos: Diretrizes para Diretores sobre o Código Combinado: Desenvolvido pelo Committee on Corporate Governance of the Institute of Chartered Accountants in England & Wales, em parceria com a London Stock Exchange, o guia foi publicado em 1999. O Turnbull exige que as companhias identifiquem, avaliem e administrem seus riscos significativos e avaliem a eficácia do sistema de controles internos relacionado.
> 4. ACC – Australian Criteria of. Control: Emitido em 1998 pelo Institute of Internal Auditors – Austrália, o ACC enfatiza a competência da administração e dos funcionários para desenvolver e operar a estrutura de controles internos. Trata-se de um controle independente, que inclui atributos como atitudes, comportamentos e competência, e é promovido como o enfoque mais compensador em termos de custo para os controles internos.
> 5. King Report – Expedido pelo King Committee on Corporate Governance em 1994, promove padrões gerais para governança corporativa na África do Sul. O King Report ultrapassa os aspectos financeiros e reguladores usuais da governança corporativa, direcionando questões sociais, éticas e ambientais.

O presente estudo está focado na metodologia apresentada pelo COSO, por ser a adotada pelo Tribunal de Contas da União, ao qual estão subordinadas todas as unidades de controle interno da Administração Pública Federal.

1.3.2 O controle interno na visão do COSO

Em 1985, nos Estados Unidos, surgiu a *National Commission on Fraudulent Financial Reporting* (Comissão Nacional sobre Fraudes em Relatórios Financeiros), tendo o controle interno como um de seus objetivos de estudo (COSO, 2012). Algum tempo depois, a comissão dá origem ao *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), que é uma entidade sem fins lucrativos que propõe métodos para elaboração de relatórios financeiros que incluem aspectos como efetividade dos controles internos e governança corporativa. Desde sua criação, o COSO tem ganhado destaque em discussões sobre processos mais adequados de controle interno. Algumas alterações na forma de controle dos gastos públicos brasileiros estão amplamente alinhadas aos pronunciamentos desse comitê.

O COSO (1992) colocou que o controle interno é amplamente definido como um processo, efetuado pelo conselho de administração, pela administração e por outras pessoas de uma entidade, destinado a fornecer uma garantia razoável quanto à consecução dos objetivos nas seguintes categorias:

1. Eficácia e eficiência das operações.
2. Confiabilidade dos relatórios financeiros.
3. Conformidade com as leis e regulamentos aplicáveis.

A primeira categoria se relaciona aos objetivos básicos de uma entidade, como a salvaguarda do patrimônio. A segunda se refere à preparação de demonstrações financeiras fidedignas. A terceira trata do cumprimento de requisitos legais e normativos aos quais está subordinada a entidade.

Para o COSO (1992), o controle interno era composto por cinco componentes inter-relacionados: Ambiente de controle; Avaliação de riscos; Atividades de controle; Informação e comunicação; e Monitoramento. Em um relatório mais recente, *Enterprise Risk Management — Integrated Framework* (Quadro de Referência Integrado para Gerenciamento de Riscos Corporativos), que é também conhecido como “COSO II”, o COSO (2004, p. 7,

tradução nossa) coloca que "o controle interno é parte integrante do gerenciamento de riscos corporativos". Esta nova proposta, portanto, não tem a intenção de substituir a anterior, mas de integrá-la à nova abordagem.

> Gerenciamento de riscos corporativos é um processo, efetuado por um conselho de diretores, gerentes e outras pessoas da entidade, aplicado na definição da estratégia e por toda a empresa, desenhado para identificar eventos potenciais que possam afetar a entidade, e gerir o risco para estar dentro de seu apetite pelo risco, para proporcionar uma segurança razoável quanto à consecução dos objetivos da entidade. (COSO, 2004, p. 2, tradução nossa)

Dentro desta nova abordagem, mais três elementos foram acrescentados para um adequado gerenciamento de riscos corporativos, alterando a composição original para oito: Ambiente Interno, Definição de Objetivo, Identificação de Eventos, Avaliação de Riscos, Respostas aos Riscos, Atividades de Controle, Informação e Comunicação, Monitoramento.

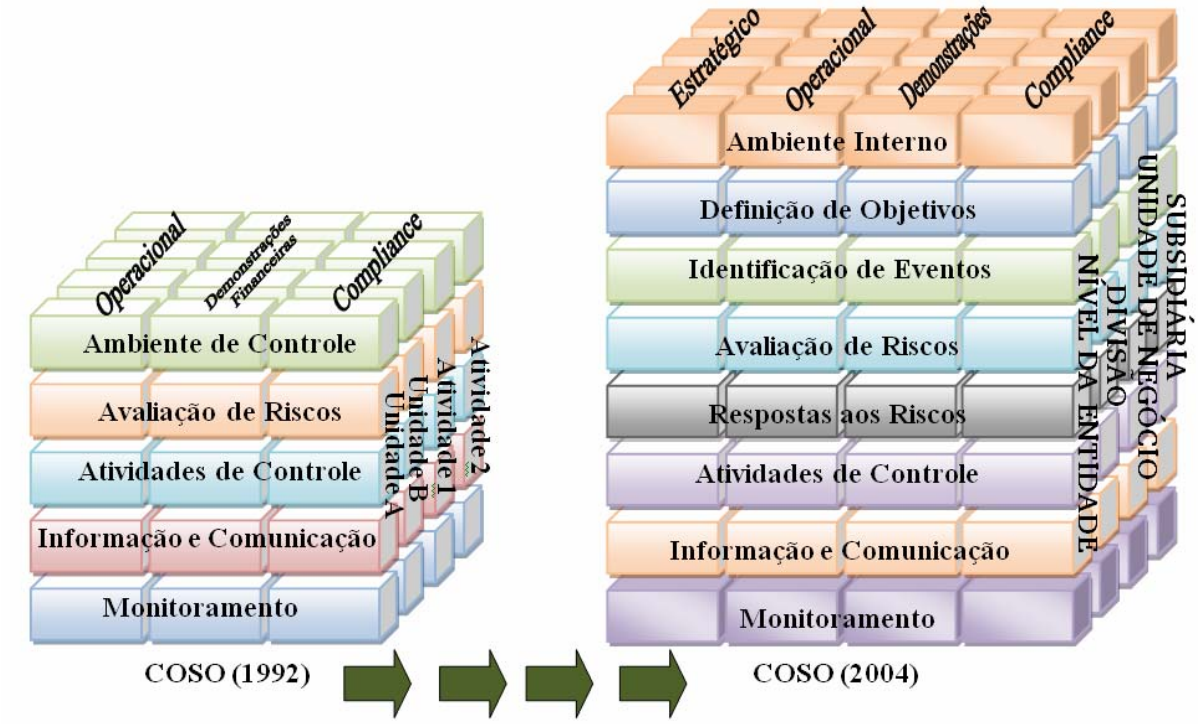

Figura 1: Abordagens do controle interno para o COSO.
Fonte: Adaptado de COSO (2004, p. 5) e COSO (2008, p. 1).

Como se pode perceber na figura 1, além da ampliação do número de componentes para oito foi incluída, também, a perspectiva estratégica. Ou seja, cada vez mais as organizações estão encarando a implantação de controles internos adequados à realidade da empresa como uma necessidade estratégica para assegurar, entre outros fatores, a própria continuidade das atividades da organização. Os componentes propostos pelo COSO (1992, 2004) são discriminados no quadro que segue:

Controle Interno	
Componente	**Descrição**
Ambiente Interno	Componente que prevalece na organização, influenciando a consciência de controle de seu pessoal. Serve de base para todos os outros componentes do controle interno, fornecendo a disciplina e a estrutura necessárias, definindo como os riscos são identificados e tratados pelo pessoal da organização. Integram o ambiente interno: integridade, valores éticos e competências pessoais; filosofia de gestão e estilo de funcionamento; política de gestão de riscos; atribuição de autoridade e responsabilidade; organização e desenvolvimento de pessoal; e atenção e orientação do conselho de administração.
Definição de Objetivo	Processo necessário para que o gerenciamento identifique eventos que possam afetar o alcance do que estiver definido como objetivo. O conjunto de objetivos escolhidos deve estar alinhado e dar suporte a missão da organização.
Identificação de Eventos	Constitui em identificar eventos internos e externos que afetem a realização dos objetivos da entidade, devendo distinguir entre riscos e oportunidades. Uma vez que as condições econômicas, tecnológicas, regulamentares e operacionais estão em constante evolução, é necessário estabelecer mecanismos para identificar oportunidades e riscos específicos associados à mudança. As oportunidades são canalizadas de volta aos processos de elaboração de estratégias de gestão e de definição de objetivos.
Avaliação de Riscos	Componente que promove uma análise de riscos relevantes, considerando sua probabilidade e seu impacto, para a consecução dos objetivos da entidade, servindo de base para determinar como devem ser gerenciados.
Respostas aos Riscos	Ações utilizadas para alinhar os riscos à tolerância e apetite da entidade pelo mesmo. Esse alinhamento pode ser feito ao se evitar, aceitar, reduzir ou partilhar os riscos envolvidos.
Atividades de Controle	Políticas e procedimentos que ajudam a garantir que as diretrizes da administração serão atendidas. Elas ajudam a garantir que ações necessárias sejam tomadas para prevenir riscos à concretização dos objetivos da entidade. As atividades de controle ocorrem em todos os níveis e funções, envolvendo a organização como um todo. Elas incluem diversas atividades como aprovações, autorizações, verificações, reconciliações, revisões de desempenho operacional, segurança de ativos e segregação de funções.
Informação e Comunicação	Informações relevantes devem ser identificadas, capturadas e comunicadas de forma confiável e em um prazo que permitam o cumprimento das responsabilidades individuais. Os sistemas de informação produzem relatórios, contendo informações operacionais, financeiras e de conformidade, que possibilitam a execução e o controle do negócio. Eles trabalham dados gerados internamente e informações sobre eventos externos para subsidiar a tomada de decisões e os relatórios externos. A comunicação eficaz também deve ocorrer em um sentido mais amplo, de cima para baixo, de baixo para cima e entre todos os pares da organização. Todo o pessoal deve receber uma mensagem clara da alta administração de que as responsabilidades pelo controle devem ser levadas a sério. Cada um precisa entender seu papel no sistema de controle interno e a forma como sua atividade se relaciona com as demais. Todos devem ter como comunicar informações significativas à alta administração e precisam ter uma efetiva comunicação com as partes externas, como clientes, fornecedores, reguladores e acionistas.
Monitoramento	Processo que avalia a qualidade e desempenho ao longo do tempo. A totalidade da gestão de riscos corporativos deve ser monitorada para que sejam efetuadas as modificações necessárias. Isso é realizado através de atividades de monitoramento contínuo, de avaliações pontuais, ou de uma combinação desses. O monitoramento contínuo ocorre no curso das operações, através de uma gestão regular, de atividades de fiscalização, e da influência das ações das pessoas no desempenho umas das outras. O alcance e a frequência das avaliações pontuais dependerão essencialmente de uma avaliação de riscos e da eficácia de procedimentos de monitoramento contínuo. As deficiências identificadas no controle interno devem ser comunicadas a alta diretoria e conselho de administração.

Quadro 1: Componentes do controle interno.
Fonte: Elaborado pelo autor com dados de COSO (1992, 2004).

Os diversos componentes necessários ao gerenciamento de riscos estão amplamente integrados para oferecer uma rápida resposta a qualquer mudança. Esse controle interno deve ser interligado às atividades operacionais da entidade, tendo sua eficácia maximizada quando construído dentro da infraestrutura da entidade, sendo parte integrante da própria essência da entidade. Os controles asseguram uma adequada qualidade e potencializam as iniciativas,

evitando custos desnecessários e permitindo uma pronta resposta às mudanças. O gerenciamento de riscos corporativos, por sua vez, não é estritamente um processo serial, onde um componente afete apenas o próximo, é um processo iterativo multidirecional em que normalmente um componente influencia o outro (COSO, 1992, 2004).

Esse processo permeia continuamente toda a entidade, envolvendo os diversos níveis de uma organização, sendo capaz de fornecer uma garantia razoável de que não existem riscos inaceitáveis dentro das estratégias traçadas pela organização.

1.3.3 O controle interno na visão da INTOSAI

As diretrizes da *International Organization of Supreme Audit Institutions* (INTOSAI) abordam aspectos do controle interno, tendo como marco referencial a posição do COSO relativa ao assunto. Em sua abordagem, voltada principalmente para entidades públicas, merecem destaque as diretrizes que se reportam a valores éticos e fornecem mais informações sobre princípios gerais de controle relacionados ao processamento da informação.

Em 2004, a INTOSAI publicou um importante documento, *Guidelines for Internal Control Standards for the Public Sector* no qual aborda importantes pontos de controle interno para uma compreensão mais ampla do assunto dentro das organizações públicas de diversos níveis e esferas governamentais.

A expectativa geral é que os servidores públicos devam servir aos interesses públicos com zelo e gerir os recursos públicos apropriadamente. Os cidadãos devem receber tratamento imparcial, baseado na legalidade e justiça. Portanto, a ética pública é um pré-requisito e um suporte para a confiança pública e a pedra fundamental para uma boa governança (INTOSAI, 2004, p. 3).

> O controle interno em organizações do setor público deve ser entendido dentro do contexto das características específicas dessas organizações, ou seja, seu enfoque para alcançar os objetivos sociais ou políticos; a utilização dos recursos públicos; a importância do ciclo orçamentário; a complexidade de seu desempenho (que demanda um equilíbrio entre valores tradicionais como legalidade, moralidade e transparência e modernos valores gerenciais, como eficiência e eficácia) e o amplo escopo decorrente de sua *accountability* pública (INTOSAI, 2004, p. 4-5, tradução nossa).

Para o INTOSAI (2004, p. 6), o controle interno é um processo integrado efetuado pela direção e pelos funcionários, desenhado para enfrentar riscos e assegurar uma razoável segurança de que, no cumprimento da missão da entidade, os seguintes objetivos gerais serão alcançados:

• execução ordenada, ética, econômica, eficiente e eficaz das operações;

• cumprimento das obrigações de *accountability*;

• cumprimento das leis e regulamentos aplicáveis;

• salvaguarda de recursos contra prejuízos por desperdício, abuso, má administração, erros, fraudes e irregularidades.

O controle interno é considerado um processo integrado porque necessita estar interligado às atividades da entidade e ser concebido dentro de sua estrutura organizacional, tornando-se parte da essência da organização, ao invés de estar superposto às atividades. Não deve ser visto como uma atividade adicional da entidade ou como uma simples obrigação normativa ou uma decisão isolada imposta pela direção da organização.

A direção e os funcionários, de todos os níveis, precisam estar envolvidos nesse processo, para enfrentar os riscos e assegurar uma razoável segurança do alcance da missão institucional e de seus objetivos. Embora a responsabilidade sobre o sistema de controle interno seja da direção, todos na organização devem se envolver para minimizar a exposição aos riscos. As pessoas devem conhecer seus papéis, suas responsabilidades e seus limites de autoridade. O controle interno, também, é afetado pela natureza humana das pessoas que integram o sistema e, desse modo, problemas familiares, finanças pessoais e habilidades individuais e profissionais podem atuar positiva ou negativamente na consecução dos objetivos.

Um sistema de controle interno por mais bem planejado e executado que esteja pode apenas trazer uma garantia razoável de que os objetivos planejados serão alcançados. Isto se deve à existência de riscos não identificados e riscos fora do controle da entidade. O conluio entre pessoas encarregadas pelos controles, por exemplo, pode ser incluído como fora do controle da entidade. A segurança razoável, também, está diretamente relacionada ao custo do controle interno, que não deve exceder os benefícios gerados ou esperados.

O controle interno se propõe a alcançar um conjunto de objetivos gerais, que são viabilizados através de numerosos objetivos específicos, funções, rotinas, processos, operações, ações e atividades.

Para a INTOSAI (2004, p. 6-11), os objetivos gerais são quatro:

- Execução ordenada, ética, econômica, eficiente e eficaz das operações: as operações devem ser executadas de maneira ordenada, ou seja, bem organizadas e estruturadas metodicamente. A ética se refere a princípios morais. A importância da conduta ética e da prevenção e detecção da fraude e da corrupção no setor público têm sido cada vez mais enfatizadas nas últimas décadas. Os servidores

públicos devem gerir adequadamente os recursos públicos. Os cidadãos devem receber tratamento imparcial, baseado na legalidade e na justiça. Por tal motivo, a ética pública é um pré-requisito, oferecendo suporte para a confiança pública e para uma boa governança. Crepaldi (2000, p. 203) complementa que a implantação de um código de ética é fundamental para o estabelecimento de uma política eficaz contra irregularidades. Tratamento econômico significa aplicar uma correta quantidade de recursos, na qualidade adequada, entregue no lugar acertado e no momento preciso, ao mais baixo custo. A eficiência diz respeito à relação entre os recursos aplicados e os resultados gerados. A eficácia se refere ao alcance dos objetivos ou ao nível no qual os resultados de uma atividade atende ao objetivo ou aos impactos pretendidos por aquela atividade.

- Cumprimento das obrigações de *accountability*: *accountability* é o processo através do qual as organizações públicas e seus integrantes tornam-se responsáveis por suas decisões e ações, incluindo a salvaguarda de recursos públicos, a imparcialidade e todos os aspectos de seu desempenho. O processo será alcançado mediante o desenvolvimento, manutenção e disponibilização de informações financeiras e não financeiras fidedignas e relevantes. "Na administração pública, é, certamente, onde mais deve estar presente a filosofia de *accountability* (dever de prestar contas), pois, quando a sociedade elege seus representantes, espera que os mesmos ajam em seu nome, de forma correta, e que prestem contas de seus atos" (SLOMSKI, 2003, p. 367). A informação não financeira pode estar relacionada com a economia, eficiência e eficácia das políticas e operações (informação sobre o desempenho operacional), e com o controle interno e sua eficácia.
- Cumprimento das leis e regulamentos aplicáveis: As organizações estão sujeitas ao cumprimento de uma diversidade de leis e regulamentos que disciplinam a captação e a aplicação dos recursos públicos, bem como sua forma de operação.
- Salvaguarda de recursos contra prejuízo por desperdício, abuso, má administração, erros, fraudes e irregularidades: os recursos públicos visam ao interesse coletivo e a contabilização do orçamento com base na execução financeira, prática muito comum no setor público, não oferece segurança suficiente com relação à aquisição, utilização e disponibilização dos recursos. Como resultado, as organizações públicas nem sempre têm registros adequados de seus ativos, o que as torna mais vulneráveis. Por isso, devem-se adotar controles internos desde a captação até a disponibilização dos recursos da entidade.

A disponibilização de informação, documentação e registros contábeis são a chave para a transparência das operações governamentais. Contudo, a salvaguarda de recursos e arquivos tem se tornado cada vez mais importante desde a chegada dos sistemas informatizados. Informações relevantes armazenadas em meios magnéticos podem ser destruídas ou copiadas, distribuídas ou mal utilizadas, caso não haja um cuidado necessário com a sua proteção (INTOSAI, 2004, p. 11).

O controle interno é um processo integrado e dinâmico que se adapta continuamente às mudanças encaradas pela organização. Desta forma, um modelo considerado ideal dentro da conjuntura atual da entidade poderá ser considerado deficiente dentro de uma realidade futura. A cada dia, novas leis e regulamentos são aprovados e novos conceitos incorporados ao arcabouço da construção de um novo sistema de controle interno.

1.3.4 Limitações dos sistemas de controle interno

Um sistema de controle interno, por melhor que seja, pode fornecer apenas uma razoável segurança de que os objetivos traçados na etapa de planejamento serão atingidos. COSO (1992), Crepaldi (2000), INTOSAI (2004) e Weygandt, Kimmel e Kieso (2011), entre outros, defendem a ideia de que controle interno é incapaz de garantir a realização dos objetivos de uma entidade de maneira absoluta. A Resolução nº 1.203 do CFC (2009, p. 23) traz que:

> Contudo, o controle interno, independentemente da qualidade da sua estrutura e operação, pode reduzir, mas não eliminar, os riscos de distorção relevante nas demonstrações contábeis, por causa das limitações inerentes ao controle interno. Essas limitações incluem, por exemplo, a possibilidade de erros ou equívocos humanos, ou de controles contornados por conluio ou burla inapropriada da administração.

A primeira razão dessa limitação é que os custos de controle não devem superar seus benefícios esperados. Esses benefícios estão relacionados à redução de prejuízos esperados para um cenário de efetivação de um ou mais riscos potenciais.

A segunda razão dessa limitação é que os sistemas de controle são afetados pela natureza humana. Assim, *stress*, fadiga, pressões, endividamentos pessoais, problemas de saúde, cobranças familiares, entre outros, podem conduzir os responsáveis pelo controle a erros de julgamento e a falhas diversas, intencionais ou não. Um estudo da KPMG (2011, p. 9) indicou que a ganância e pressões do trabalho (desemprego e política de distribuição de bônus) foram os principais motivos que levaram as pessoas a cometerem fraudes.

Crepaldi (2000, p. 238), ao colocar que podem acontecer falhas de controle, resultantes de desentendimentos de instruções, erros de juízo, descuidos ou outros fatores humanos, exemplifica consequências de algumas ações:

- Os processos de controle relativos à execução e ao registro das operações ou cuja eficácia dependa da segregação de funções podem ser burlados mediante conivência; e

- Os métodos de controle atinentes à execução e ao registro das operações podem mostrar-se impotentes quanto a erros ou irregularidades efetuados pela administração na preparação das demonstrações financeiras, dos orçamentos e fluxos de caixa.

Weygandt, Kimmel e Kieso (2011, p. 308) instruem que o tamanho do negócio, também, pode impor limitações ao controle interno. Desta forma, por exemplo, uma pequena organização pode encontrar dificuldades para promover uma adequada segregação de funções.

Nenhum controle interno é capaz de assegurar plenamente que tudo está como deveria estar, existindo sempre um ou mais riscos envolvidos. Deve ser considerado, também, que o melhor dos controles internos do século passado certamente não o será hoje em dia, ou seja, o controle interno deve acompanhar as mudanças e se manter atualizado.

1.4 A informação contábil

Segundo a IPSAS 22 do *Institute for International Public Sector Accounting Standards* (IPSAS, 2006, p. 692), os objetivos das demonstrações financeiras são fornecer informações úteis para a tomada de decisão e demonstrar a responsabilidade da entidade para com os recursos que lhe foram confiados e que ela controla.

A informação contábil, especialmente a que integra as demonstrações contábeis, necessita se revestir de certos atributos ou características para atender adequadamente a seus usuários. Esta matéria é discutida por diversas entidades e autores, a *Financial Accounting Standards Board* (FASB, 1980), por exemplo, trata do tema em seu documento *Statement of Financial Accounting Concepts No. 2*.

O COSO (2008, p. 28) propõe o conceito de informação adequada, advertindo que seu entendimento é amplo e implica que a informação deva ser útil dentro do contexto ao qual se destina. Três elementos operam juntos para tornar uma informação adequada: relevância, confiabilidade e oportunidade.

Figura 2: Elementos de uma informação adequada.
Fonte: Adaptado de COSO (2008, p. 28).

Nesse contexto, deve-se ter em mente que a busca pela informação adequada é preciosa para o processo decisório dentro das diferentes organizações, mas que, algumas vezes, os tomadores de decisão serão forçados a definir ações sem terem as necessárias quantidades e qualidades das informações a seu dispor.

A Resolução nº 1.374/11 do CFC instrui que a informação contábil financeira para ser útil precisa ter duas características qualitativas fundamentais, ou seja, ser relevante e representar com fidedignidade o que se propõe a representar, conforme descrito abaixo:

- Relevância - a informação relevante é aquela que pode ser capaz de fazer diferença em uma decisão mesmo que alguns usuários decidam não a levar em consideração ou caso já tenham tomado ciência de sua existência por outras fontes. Essa informação é capaz de fazer diferença no processo decisório se tiver valor preditivo, valor confirmatório ou ambos. O valor preditivo está ligado à utilização da informação como dado de entrada em processos empregados pelos usuários para predizer futuros resultados. O valor confirmatório está em servir como *feedback* que confirmará ou alterará as avaliações prévias. O valor preditivo e o valor confirmatório estão correlacionados e uma mesma informação pode confirmar previsões anteriores e servir de base para planejamentos subsequentes.

Um aspecto de relevância particular da entidade é a materialidade que se refere à natureza e magnitude dos componentes no contexto do relatório contábil e financeiro. A informação material é aquela cuja omissão ou divulgação distorcida (*misstating*) pode influenciar a tomada de decisões pelos usuários.

- Representação fidedigna- a informação fidedigna é aquela que representa o que se propõe representar. Essa representação para ser totalmente fidedigna precisa ser completa, neutra e livre de erro. Será completa se a totalidade das informações necessárias for disponibilizada para que o usuário compreenda o fenômeno sendo retratado, incluindo todas as descrições e explicações necessárias. Será neutra se não contiver viés na seleção ou na apresentação da informação contábil financeira. Estar livre de erros significa que não há erros ou omissões na realidade retratada e que o processo empregado para gerar a informação foi selecionado e conduzido sem erros.

Além das características qualitativas fundamentais da informação, quanto mais comparável, verificável, tempestiva e compreensível é essa representação da realidade, maior a sua utilidade. Esses aspectos da informação são chamados, conforme a Resolução nº 1.374/11 do CFC, de características qualitativas de melhoria, conforme detalhado abaixo:

- Comparabilidade- a informação gerada por uma entidade deve ser comparável com informação semelhante sobre outras organizações e com informação similar da mesma entidade gerada em outro período ou data.
- Verificabilidade- significa que diferentes observadores, cônscios e independentes, podem chegar a um consenso (acordo não necessariamente completo) quanto à representação de uma realidade particular ser fidedigna. A verificação pode ser direta (observação direta, como pela contagem de caixa) ou indireta, pela checagem dos dados de entrada do modelo, fórmula ou outra técnica e recálculo dos dados obtidos por meio da aplicação da mesma metodologia.
- Tempestividade- informação deve estar disponível para tomadores de decisão a tempo de poder influenciá-los em suas decisões. COSO (2008) complementa, ainda, que uma informação tempestiva é aquela produzida e usada em um período de tempo que torne possível prevenir ou detectar deficiências de controle antes que elas se tornem materiais para uma organização.
- Compreensibilidade- a informação deve ser caracterizada, classificada e apresentada com clareza para ser compreensível ao usuário. As informações devem ser apresentadas de maneira a maximizar sua compreensão sem, no entanto, tornar os relatórios incompletos ou potencialmente distorcidos (*misleading*).

De maneira geral, as características qualitativas de melhoria devem ser maximizadas o quanto possível, apesar de não terem o poder de tornar uma informação útil, se considerada irrelevante ou sem uma representação fidedigna. Deve-se ter em mente, também, que o aumento da utilidade da informação envolve custos que, a princípio, precisam ser superados pelos benefícios gerados (ou esperados) pelo incremento dessa utilidade.

Portanto, as informações contábeis para serem úteis aos usuários e contribuírem para o cumprimento dos objetivos da entidade devem ser geradas à sombra de qualidades específicas. O controle interno, em atendimento a Resolução nº 1.135/08 do CFC, deve propiciar informações oportunas e adequadas que mitiguem o risco de práticas ineficientes e antieconômicas, erros, fraudes, malversação, abusos, desvios e outras inadequações.

1.4.1 Sistema de informações contábeis

Parece urgente a necessidade de que todos os responsáveis pelo controle interno das diferentes entidades públicas e privadas, ao apurarem erros ou fraudes, promovam ações para que os fatos ocorridos não voltem a ocorrer. Isso vai muito além do que se tem presenciado − um número crescente de agentes punidos, exonerados e muitas vezes presos. Um sistema bem organizado de informações fidedignas pode ser um primeiro passo para o sucesso dessa pretensão. Nesse contexto, Schelling (*apud* KLITGAARD, 1994, p. 12), coloca que:

> Uma organização, comercial ou não, é um sistema de informações, regras de decisão e incentivos; seu desempenho é diferente dos desempenhos individuais das pessoas que a compõem. Uma organização pode ser negligente sem que nenhum de seus integrantes o seja. Esperar que uma organização reflita as qualidades dos indivíduos que trabalham para ela ou imputar aos indivíduos as qualidades que vemos na organização é cometer o que os lógicos denominam "falácia de composição". A falácia não é um erro, claro, mas pode ser traiçoeira.

Muitos dos problemas identificados em organizações tanto públicas como privadas se deve ao fato de os diversos envolvidos em um processo não disporem de todas as informações necessárias. Essa ameaça conhecida, também, como problema de assimetria de informações entre os diversos agentes é estudada mais detalhadamente pela Teoria de Agência. Por não representar o foco desse estudo, destaca-se apenas que dados escassos e imprecisos são um convite a agentes oportunistas. Dessa forma, deve haver mecanismos para assegurar que a informação não seja de domínio exclusivo de uma única pessoa ou grupo. Como proposto por Klitgaard (1994, p. 221), os dirigentes devem ter em mente que medidas podem tomar para rastrear uma informação, analisá-la e utilizá-la para aumentar as chances de um agente

envolvido ser descoberto, responsabilizado e punido. As organizações devem implantar sistemas de informações e controle sólidos que possam identificar padrões e procedimentos incomuns, incompatíveis ou suspeitos, produzindo relatórios próprios para que os dirigentes possam tomar as atitudes cabíveis.

O entendimento do que pode ser considerado um sistema parece importante nesse momento. Audy, Andrade e Cidral (2005, p. 109) advertem que a palavra sistema "[...] tem ampla utilização e genericamente designa todo o conjunto de elementos que interagem entre si, cumprindo determinados objetivos ou tarefas e situam-se em um contexto ambiental". Esse conjunto de elementos se dispõe de maneira bem particular, conforme Padoveze (2000, p. 26) descreve abaixo:

> [...] sistema é um conjunto de elementos interdependentes, ou um todo organizado, ou partes que interagem formando um todo unitário e complexo. [...] Fundamentalmente, o funcionamento de um sistema configura-se com um processamento de recursos (entrada do sistema) obtendo-se, com esse processamento, as saídas ou produtos do sistema (entradas, processamento, saídas).

O sistema, em se tratando de processamento de dados, assume um caráter particular e pode ser definido como:

> Sistema é um conjunto de programas e rotinas de computação que operando de forma conjunta, realizam uma determinada tarefa no todo ou em parte, dependendo da sua abrangência e complexidade, tendo como objetivo um resultado prático (SILVA, 1998, p. 5).

Um conceito que pode ser considerado relevante é o de ambiente de sistema. "Pode-se definir ambiente de sistema como sendo um conjunto de elementos que interfere direta ou indiretamente no seu funcionamento, estando normalmente fora dele" (SILVA, 1998, p. 9). No ambiente contábil, por exemplo, um sistema de informações encerra um caráter mais particular. O item 10 da Norma Brasileira de Contabilidade T 16.2 coloca que:

> O sistema contábil representa a estrutura de informações sobre identificação, mensuração, avaliação, registro, controle e evidenciação dos atos e dos fatos da gestão do patrimônio público, com o objetivo de orientar e suprir o processo de decisão, a prestação de contas e a instrumentalização do controle social.

Outro importante aspecto dentro da abordagem sobre sistemas é a distinção entre sistema fechado e sistema aberto. Um sistema fechado é um sistema em que, por princípio, as interações ocorrem isoladas do ambiente externo, podem ser observados em situações bem específicas e são muito utilizados em estudos feitos nas ciências exatas, como a física e a química. Já os sistemas abertos são aqueles em que há a interação do sistema com o ambiente externo ao mesmo, sendo matéria de estudo de áreas como a contabilidade, a administração e a economia. "A entidade pública é um sistema aberto que comunga no cenário a impactação de energias com os sistemas político, social, econômico, ecológico etc., recebendo e oferecendo oportunidades e ameaças" (SLOMSKI, 2003, p. 402).

Para identificar e distinguir adequadamente ameaças e oportunidades, é necessário um sistema de informações confiável, de modo a minimizar os riscos e maximizar o aproveitamento de oportunidades. “Sistemas de informações compreendem um conjunto de recursos humanos, materiais, tecnológicos e financeiros, combinados segundo uma seqüência lógica para transformar dados em informações” (GIL, 1998, p. 37). Para uma distinção adequada entre riscos e oportunidades, Davis (2006, p. 67) descreve que é necessário que sejam feitas reavaliações regularmente para identificação de novos fatores que possam alterar o impacto esperado e afetar o negócio da organização. Turban et al (2010, p. 59) definem sistema de informação (SI) como “[...] um sistema que coleta, processa, armazena, analisa e dissemina dados e informações para um propósito específico”.

Uma condição prévia para uma informação confiável e relevante sobre transações e eventos é seu registro imediato dentro da classificação adequada. A informação relevante representa uma comunicação tempestiva a pessoas específicas, ou seja, é aquela que é identificada, armazenada e comunicada com forma e prazo que permitam que os funcionários realizem atividades inerentes ao controle interno e demais responsabilidades (INTOSAI, 2004, p. 36). Por esse motivo, o sistema de controle interno deve ser precisamente documentado.

Crepaldi (2000, p. 234) coloca que os sistemas de informação variam de organização para organização por diversos aspectos (tamanho, área de atuação e outros), mas, apesar disso, certas características devem estar presentes em um bom sistema de informações:

- ✓ A informação deve estar suficientemente detalhada para identificar operações desalinhadas ou prováveis problemas;
- ✓ As informações relevantes devem integrar os relatórios disponibilizados aos usuários;
- ✓ As informações de maior importância devem aparecer destacadas;
- ✓ Os usuários das informações devem possuir competência e tempo para entender o real significado do que está diante de seus olhos e providenciar as medidas necessárias. Ou seja, “[...] o controle não existe mediante o simples fornecimento de informação e, sim, com o uso que a administração faz desta” (CREPALDI, 2000, p. 234).

Para Silva (2012, p. 1), é necessário que o sistema de informações de cada organização pública seja examinado e analisado para que sejam cumpridos os seguintes níveis:

a) A informação como uma área de governança permanente da Entidade;

b) A informação como estimuladora dos processos automatizados;

> c) A informação como estimuladora de procedimentos permanente de gestão de riscos e de segurança; e
> d) A informação como um ativo tangível gerador de benefícios econômicos ou potenciais futuros.

Ao abordarem os controles na era da informação, Moscove, Simkin e Bagranoff (2002, p. 223) colocam que os dois objetivos principais para o controle do ambiente de processamento de dados das organizações são garantir que: "[...] (1) o desenvolvimento ou alteração de programas de computador são autorizados, testados e aprovados antes de serem usados e (2) o acesso a arquivos de dados seja restrito a usuários e programas autorizados".

Para Silva (2003, p. 804-805), é necessário compreender que as características de um sistema informatizado diferem, em parte, principalmente devido ao fato de que "[...] burlar as [atividades de controle] embutidas na tecnologia é consideravelmente mais difícil para os atores organizacionais que sofrem o controle do que burlar as burocráticas".

O novo contexto econômico e tecnológico e a busca por melhoria contínua, pelo cumprimento dos objetivos e pelo comprometimento da alta administração exigem dos gestores que têm uma visão multidisciplinar a iniciativa de uma correta implantação, execução e monitoramento dos controles internos, que permita dispor de informações contábeis seguras e fidedignas, assegurando a tomada de decisão com redução de riscos, alocação adequada de recursos, preservação do patrimônio e garantia da confiança e transparência das transações (SILVA, GUIMARÃES, PEREIRA, 2004, p. 16).

1.4.2 Os registros contábeis na Administração Pública Federal

Na administração pública, o sistema de registros contábeis representa uma extensa teia de informações sobre a *res publica*. Silva (2009, p. 73) coloca que, ao implantar novas tecnologias na contabilidade, pode-se observar que não há diferença entre um sistema não informatizado e um sistema informatizado, pois as rotinas e fluxos das operações são os mesmos, sendo as principais características de um sistema, que utilize uma moderna tecnologia da informação, a maior velocidade e flexibilidade no reconhecimento de necessidades e na transformação de dados em informações.

Informatizado ou não, uma das mais importantes necessidades de um sistema contábil é dispor de critérios para um adequado registro de atos e fatos. Nesse sentido, o item 3 da

Norma Brasileira de Contabilidade T 16.5, assim, institui: “A entidade do setor público deve manter procedimentos uniformes de registros contábeis, por meio de processo manual, mecanizado ou eletrônico, em rigorosa ordem cronológica, como suporte às informações”.

Para promover esse registro único de atos e fatos, a Administração Pública Federal optou por realizar a maior parte da escrituração contábil através de sistemas informatizados. Nascimento e Cherman (2007, p. 245-246) discorrem que a contabilização federal é realizada em nível de Unidade Orçamentária (UO) até a conclusão da descentralização orçamentária e, a partir de então, ocorre em nível de Unidade Gestora (UG), estando a atividade financeira do governo federal dividida em seis fases:

1. Planejamento: compete à Secretaria de Planejamento e Investimentos Estratégicos do Ministério do Planejamento, Orçamento e Gestão (MPOG) e é realizado no Sistema de Informações Gerenciais e de Planejamento (SIGPlan).
2. Elaboração do Orçamento: compete à Secretaria de Orçamento Federal do MPOG e é realizado pelo Sistema Integrado de Dados Orçamentários (SIDOR).
3. Aprovação do Orçamento: a cargo do Poder Legislativo, que aprovará a proposta do Executivo, possuindo esta fase apenas caráter legal e de ajustes no Orçamento apresentado, para chegar à sua versão final.
4. Execução Orçamentária e da Programação Financeira: fase realizada no âmbito do Sistema Integrado de Administração Financeira do Governo Federal (SIAFI), em que se inicia o trabalho das UO e, acompanhando a execução orçamentária, é realizada a execução da programação financeira fixada por decreto do Poder Executivo. Esta fase está relacionada à previsão de desembolsos em consonância com o Orçamento aprovado.
5. Execução Financeira (ingressos e dispêndios) e Patrimonial (bens, direitos e obrigações): realizada no domínio do SIAFI pelas UG, que executam o orçamento designado às Unidades Orçamentárias, os estágios da receita (arrecadação e recolhimento) e da despesa (empenho, liquidação e pagamento), bem como a obtenção de bens permanentes, celebração de convênios, transferência de ativos etc. Esta fase está relacionada à efetiva arrecadação e à efetiva saída de caixa do Governo, por intermédio de seus Órgãos e Unidades Gestoras.
6. Controle e Avaliação: têm inicio com a divulgação de demonstrativos do SIAFI e sua análise pelos gestores e por auditores internos da Secretaria Federal de Controle Interno (SFC) da Controladoria Geral da União, ligada à Presidência da República. Depois de todas as fases, o orçamento do exercício e sua execução são

avaliados, já no âmbito do MPOG, e reinicia-se o processo, com as devidas adequações, para um novo exercício.

Portanto, observa-se um processo contínuo em que a avaliação do exercício anterior alimentou o planejamento para o presente exercício e esse, após percorrer todas as fases, servirá de subsídio para o planejamento do próximo exercício. Esse complexo processo, por sua vez, somente é possível de ser realizado de maneira adequada por meio dos robustos processos informatizados envolvidos em sua consecução.

Nesse contexto, o processamento da folha de pessoal dos diversos órgãos públicos é apenas um dos componentes ligados à fase de execução da despesa, mas que devido a sua envergadura financeira, merece cuidadoso tratamento e exige um adequado processo informatizado para sua consecução.

1.5 A tecnologia da informação

Ao iniciar esta subseção, destaca-se a reflexão feita há alguns anos por um estudante e que se acredita válida ainda hoje:

> O investimento tecnológico é vital para o nosso Estado, que passou anos sem a devida renovação de seus equipamentos, uma vez que sua obsolescência implica maior gasto com custos de manutenção, queda na qualidade e no tempo para a informação, aumento do número de horas para manutenção ou confecção de rotinas, etc (COSTA, 1998, p. 605).

A gestão de TI busca assegurar que as informações prestadas a diversos usuários estejam de acordo com as necessidades do negócio. Esse alinhamento pode ocorrer de forma a convergir aos planos de negócio ou mediante ajustes para um maior aproveitamento de oportunidades.

> O conceito de tecnologia da informação deve ser compreendido como sendo muito mais amplo do que apenas considerá-la como processamento de dados, engenharia de software, informática ou o conjunto de hardware e software, devendo ser considerados aspectos humanos, administrativos e da organização (BORGES; PARISI; GIL, 2005, p. 2).

De acordo com o *Information Technology Governance Institute* (ITGI, 2011), a TI é essencial para gerenciar transações, informações e conhecimentos necessários para iniciar e sustentar as atividades econômicas e sociais, que dependem cada vez mais da colaboração das entidades para serem bem sucedidas, sendo a TI, em muitas organizações, fundamental para apoiar, sustentar e fazer crescer o negócio.

A TI deve assegurar um suporte de informação adequado, dinâmico, confiável e eficaz, promovendo aos interessados a obtenção das informações disponíveis, de maneira

mais fácil e resguardando aspectos de sigilo e restrições administrativas ou previstas em disposições legais. Deve, também, estimular o desenvolvimento, a padronização, a integração, a normatização dos serviços de produção, bem como a disseminação de informações de forma desconcentrada e descentralizada. Uma adequada área de TI promove a proteção a informações críticas e contribui para que sejam alcançados os objetivos institucionais.

As capacidades de sistemas computadorizados são diversificadas e mudam de acordo com o objetivo para o qual foi projetado. Algumas dessas capacidades, destacadas por Turban et al (2010, p. 25), são: cálculos em alta velocidade e em grande volume; comunicação rápida, exata, confiável e barata dentro de uma organização e entre diferentes entidades, a qualquer hora e em qualquer lugar; armazenamento de grandes volumes de informações em pequenos espaços; acesso rápido e barato a informações disponibilizadas em todo o mundo e a qualquer hora; aumento de efetividade e eficiência de pessoas que trabalham em grupo; modo incisivo de apresentação de informações que desafiam a mente humana; facilitação do trabalho em ambientes de risco; automatização de processos semiautomáticos e manuais; interpretação de grandes quantidades de dados; facilitação do comércio global; automação ou facilitação do processo de tomada de decisões; conexões sem fio, suportando aplicações únicas em qualquer lugar; e menor custo.

O ambiente de tecnologia da informação permite, segundo Padoveze (2005, p. 48), a adoção do conceito de que os processos organizacionais devem ter primazia em relação às estruturas hierárquicas, ou seja, os novos conceitos aplicados aos sistemas de informação caracterizam-se por uma gestão horizontal (processos) em vez de por uma gestão vertical (departamentos).

A princípio, como ensina o próprio Padoveze (2005, p. 49), os processos devem estar ligados à estrutura hierárquica da organização por meio de *workflow*, adicionando as responsabilidades de cada setor ou pessoa, bem como suas autoridades e faixas ou elementos de autorização, ao banco de dados disponibilizado na rede a todos os usuários autorizados com terminal de computador. Para o mencionado autor, *workflow* é um conceito que congrega procedimentos, métodos, tarefas e responsabilidades hierárquicas, internados computacionalmente, tendo substituído os conceitos antigos de Organização e Métodos e Normas e Procedimentos.

Deve ser perseguida a contínua melhoria dos processos de TI, visando minimizar efeitos indesejáveis como insatisfação do cliente, alcance de resultado abaixo do esperado, desperdício de recursos, descontinuidade de projetos, visão negativa da área de TI, suporte ineficaz ao cumprimento da missão da organização, entre outros.

> Os procedimentos de avaliação dos controles internos definidos até recentemente despendiam pouca ênfase aos riscos em ambiente de informática. O fato é que, na definição dos procedimentos destinados a avaliar os controles internos, ainda não existia total clareza acerca da exposição da empresa a essa modalidade de risco (VIEIRA, 2007, p. 184).

Pode-se dizer que a tecnologia da informação deve estar alinhada à estratégia do negócio, ter uma arquitetura apropriada às demandas presentes e futuras (se conhecidas), mitigando riscos e garantindo a continuidade dos processos e do próprio negócio.

Os controles de tecnologia da informação se relacionam com cada um dos componentes de um sistema de controle interno, se envolvendo com Ambiente Interno, Definição de Objetivo, Identificação de Eventos, Avaliação de Riscos, Respostas aos Riscos, Controle de Atividades, Informação e Comunicação, e Monitoramento.

Sistemas informatizados envolvem procedimentos de controle bem particulares que não devem ser vistos como tema autônomo, mas como parte integrante dos procedimentos de controle da entidade.

> [...] definimos um sistema de informação (SI) como um sistema que coleta, processa, armazena, analisa e dissemina dados e informações para um propósito específico. A composição dos sistemas de informação normalmente é a mesma: Cada um contém hardware, software, dados, procedimentos e pessoas (TURBAN *et al*, 2010, p. 59).

Esses SI devem ter controles suficientes, em quantidade e qualidade, para promover uma segurança adequada do ambiente informatizado. Cruz e Glock (2003, p. 87) descrevem que a segurança informática deve assegurar a "[...] garantia da impossibilidade de acesso não autorizado ao conteúdo das bases de dados e dos programas, assim como da continuidade do processamento de dados em situações decorrentes de riscos".

Por esse motivo, os controles relacionados à tecnologia da informação (TI) são divididos, segundo a INTOSAI (2004, p. 32-34) em dois grandes grupos, o de controles gerais e o de controles de aplicativos, como seguem:

- Controles gerais: constituem o conjunto de estrutura, políticas e procedimentos aplicado aos sistemas de informação da entidade e que ajudam a assegurar seu adequado funcionamento. Eles criam o ambiente em que operam os sistemas aplicativos e de controle. Ele, por sua vez, está subdividido em seis categorias, conforme abaixo:

(1) programa institucional de planejamento e gerenciamento de segurança: oferece uma sistemática de trabalho e um ciclo ininterrupto de gerenciamento de risco, desenvolvimento de políticas de segurança, atribuição de responsabilidades e monitoramento da adequação dos controles institucionais computadorizados;

(2) controles de acesso: limitam ou detectam o acesso aos recursos computadorizados (dados, programas, equipamentos e instalações), protegendo os mesmos contra mudanças não

autorizadas, perda e exposição não desejada. Nesses controles estão incluídos controles físicos e lógicos;

(3) controles de desenvolvimento, manutenção e mudança de softwares aplicativos: previnem tanto a utilização de programas não autorizados quanto modificações nos programas existentes;

(4) controles de sistema de software: limitam e monitoram o acesso a poderosos programas e a arquivos sensíveis, que controlem o hardware dos computadores e as aplicações de segurança apoiados pelo sistema;

(5) segregação de funções: representa políticas, procedimentos e estrutura organizacional que devem prevenir que uma pessoa controle todos os pontos importantes das operações informatizadas e possa executar ações não autorizadas ou obter acesso não autorizado a ativos ou registros;

(6) continuidade do serviço: ajuda a assegurar que, quando ocorrem eventos inesperados, as operações críticas não sofram interrupção ou possam ser prontamente retomadas e a informação crítica e sensível permaneça protegida.

- Controles de aplicativos: constituem o conjunto de estrutura, políticas e procedimentos diretamente relacionados às aplicações de computadores. Sua missão é prevenir, detectar e corrigir erros e irregularidades enquanto a informação flui pelos sistemas de informação. Podem ser dispostos em três fases do ciclo do processo:

• entradas: os dados devem ser autorizados, convertidos a uma forma automatizada e introduzidos na aplicação de maneira precisa, completa e tempestiva;

• processamento: os dados devem ser processados apropriadamente pelo computador e os arquivos devem ser atualizados corretamente; e

• saídas: os arquivos e relatórios gerados pelo aplicativo devem refletir fidedignamente as transações ou eventos que realmente ocorreram e os resultados de seu processamento, e os relatórios produzidos devem ser controlados e distribuídos aos usuários autorizados.

Os controles de aplicativos podem ser classificados segundo os objetivos de controle, incluindo se as transações e a informação são autorizadas, completas, precisas, válidas e tempestivas. Os controles de autorização relacionam-se à validade das transações e buscam certificar que as transações representam eventos que ocorreram efetivamente em um determinado período. Os controles de integralidade são relacionados ao registro e enquadramento adequado de todas as transações válidas. Os controles de precisão se reportam ao registro fidedigno das transações e à exatidão dos dados. Os controles sobre a integridade do processamento e dos registros de dados, quando deficientes, podem anular cada um dos

controles anteriormente mencionados e comportar transações não autorizadas, além de colaborar para existência de dados imprecisos e incompletos (INTOSAI, 2004, p. 34).

Os controles de aplicativos abarcam procedimentos de controle programados, tais como emissões automáticas e acompanhamento manual das informações fornecidas pelo computador, tais como análises de relatórios que indiquem itens rejeitados ou não usuais (INTOSAI, 2004, p. 35).

Os controles gerais e de aplicação são amplamente correlacionados, sendo necessários para promover um processamento adequado e completo da informação (INTOSAI, 2004, p. 35). Os controles relacionados à TI requerem constante atualização para permanecerem eficazes em relação ao objeto controlado.

Gil (1998, p. 38) ensina que o controle interno em sistemas informatizados envolve um ou mais dos seguintes parâmetros:

a) Fidelidade das informações em relação ao dado: deve ser validada e avaliada que as informações (produto final) estão corretas em relação aos dados (matéria-prima) utilizados no sistema computadorizado, assegurando, dessa forma, que não houve perdas ou acréscimos durante o processamento dos dados.

b) Segurança física: relacionada às condições operacionais dos funcionários (saúde, ergonomia etc.) e dos materiais (instalações, *hardware* etc.) que apoiam os sistemas de informação computadorizados.

c) Segurança lógica: busca assegurar um correto rumo dos processos e resultados relacionados com a TI.

d) Confiabilidade: abrange as garantias com relação à quebra de sigilo do sistema computadorizado, seu processo e informações. É a captação, por pessoa ou entidade não autorizada, dos recursos tecnológicos componentes do ambiente computacional.

e) Segurança ambiental: valida condições de operacionalidade dos recursos humanos, materiais e tecnológicos da infraestrutura de computação.

f) Obediência à legislação em vigor: é o atendimento à legislação federal, estadual e municipal.

g) Eficiência: diz respeito à relação benefício/custo, buscando uma combinação ótima de recursos humanos, materiais e tecnológicos ligados a sistemas computadorizados.

h) Eficácia: avalia se a informação foi gerada conforme os objetivos que determinam sua utilidade.

i) Obediência às políticas da alta administração: verifica se o sistema computadorizado atende às normas, diretrizes e políticas emitidas pela administração de topo da organização.

A Instrução Normativa nº 01 da Secretaria Federal de Controle Interno (SFC), de 6 de abril de 2001, estabelece que os sistemas eletrônicos de processamento de dados e suas informações de entrada e de saída devem ser constantemente controlados para se assegurar: a) a segurança física do ambiente e das instalações do centro de processamento de dados; b) a segurança lógica e a confidencialidade nos sistemas desenvolvidos em computadores de diversos portes; c) a eficácia dos serviços prestados pelo setor de informática; d) a eficiência no emprego dos computadores disponíveis na organização.

Polloni (2000, p. 31) ensina que um sistema informatizado eficaz deve atender a alguns pontos fundamentais: gerar informações realmente necessárias, confiáveis, tempestivas e com custo condizente, atendendo a requisitos operacionais e gerenciais; assegurar a concretização dos objetivos, de maneira direta, simples e eficiente; integrar-se à estrutura organizacional e auxiliar a coordenação entre departamentos, divisões, diretorias, e outros por ele interligados; possuir procedimentos internos e externos ao processamento estabelecidos de maneira racional, integrada, rápida e com o menor custo possível; contar com dispositivos de controle interno que garantam a confiabilidade das informações geradas e uma adequada proteção aos dados controlados pelo sistema; e, por fim, ser simples, seguro e rápido em sua operação.

Ao trabalhar com sistemas informatizados, a organização necessita de um controle interno diferenciado, em virtude dos riscos que esta nova forma de trabalho impõe. Dunn (1991, p. 147) discorre que, se os programas foram escritos corretamente e houve uma correta entrada de dados, é quase impossível ocorrer um erro, sem interferência externa, mas se, no entanto, o programa contém erros ou o tratamento de dados está sendo manipulado de alguma forma, então, há uma incapacidade da máquina para questionar a lógica de suas instruções que pode levar a erros sistemáticos que se repetem cada vez que o programa é executado.

Ribeiro (2002, p. 60) destaca que a tecnologia da informação trouxe várias possibilidades de aumento de *accountability* para as atividades do Estado, o que torna possível a divulgação quase que imediata de todos os atos e ações dos diversos governos, quase de forma *online*.

A INTOSAI (2009, p. I-19) coloca que avaliação de sistemas de processamento eletrônico de dados envolve aspectos, tais como: o planejamento de requisitos; o uso econômico de equipamentos de processamento de dados; o uso de pessoal com especialização adequada, de preferência de dentro da administração da organização auditada; a prevenção de uso indevido; e a utilidade das informações produzidas.

Dentro desse contexto, está enquadrado o SISPAG que deve gerenciar todo o processo, as transações, as informações e os conhecimentos requeridos pelos diversos usuários, mitigando riscos, e garantindo o sucesso do processamento da folha de pagamento de pessoal militar da Marinha.

1.5.1 Conceitos relacionados à TI

Um dos primeiros conceitos que se acredita serem necessários para o entendimento dos processos que envolvem TI é o conceito de dado. Audy, Andrade e Cidral (2005, p. 93) discorrem que um dado representa um fato bruto (matrícula de um professor, nome de um empregado, código de um item etc.) ou suas representações (formas, sons, imagens etc.) que podem ou não ser úteis ou pertinentes para um determinado processo.

O conceito de informação também pode ser considerado útil nesse contexto. Além dos debates feitos anteriormente nesse estudo, Audy, Andrade e Cidral (2005, p. 93) descreveram que a informação é um conjunto de dados concatenados, que sofreram um processo de transformação, cuja forma e conteúdo estão adequados para uso específico.

O uso específico da informação remete ao conceito de acesso à informação. Um sistema de informações, principalmente o automatizado, deve possuir, de acordo com Santos, Resende, Neto e Padua (2010, p. 14), mecanismos que permitam a existência de diversos usuários trabalhando em um mesmo sistema, com diferentes níveis de acesso. Esse acesso pode ser remoto, podendo um usuário no outro extremo do Globo acessar as informações disponíveis com uma velocidade semelhante a um usuário na sala ao lado. Essas características estão relacionadas às seguintes necessidades: (i) controle de permissões por função, configurável por usuário e grupo, dentro de um sistema, (ii) acesso remoto e (iii) funcionamento em multiplataformas. (SANTOS; RESENDE; NETO; PADUA, 2010, p. 14).

Um dos recursos mais utilizados nos ambientes informatizados é o banco de dados que é, segundo Silva (2001, p. 3), "[...] um conjunto de informações manipuláveis de mesma natureza inseridos em um mesmo local, obedecendo a um padrão de armazenamento". O banco de dados é muito utilizado devido às potencialidades que oferece, dentre as quais L. C. Silva (2001, p. 5) identificou as seguintes:

- Um banco de dados é compacto, eliminando o volume de arquivos em papel.
- Os dados são recuperados e modificados muito rapidamente.

- O banco de dados proporciona ao usuário um controle centralizado de seus dados operacionais, contrastando nitidamente com ambientes não automatizados em que os dados operacionais são muito dispersos, dificultando o controle sistemático.
- Os dados podem ser compartilhados por diversos usuários, formando um fluxo corrente de disponibilidade de informações certas e atualizadas.
- Acessos permitidos com restrições de segurança.
- Padrões bem definidos, combatendo a ausência e a baixa qualidade das informações disponíveis no banco de dados.

Pode-se perceber que a organização de um banco de dados de forma adequada deve favorecer uma manutenção adequada de dados históricos das atividades operacionalizadas no sistema, contribuindo para o processo de *accountability* da respectiva entidade.

Uma dificuldade presente na maior parte das aplicações existentes no mercado está relacionada, segundo Haberkorn (2009, p. 118), à manutenção dos campos dos vários arquivos e tabelas que compõem o sistema. Para se incluir um simples campo em uma tabela do sistema, podem ser necessárias alterações de diversos programas que façam uso dessa tabela. Para resolver esse problema, foi criado o chamado Dicionário de Dados, que contém todos os campos (e suas propriedades) utilizados pelos diversos programas do sistema. Dessa forma, o usuário para alterar, incluir ou excluir um determinado campo, trabalhará apenas no Dicionário de Dados e automaticamente o campo estará disponível em todos os relatórios, consultas, cadastros e outras disponibilidades do sistema.

As ameaças a um sistema informatizado, principalmente aos de grande porte, estão presentes desde seu projeto de *software*. Várias são as metodologias empregadas para seu desenvolvimento, visando reduzir falhas e conduzir adequadamente o processo, mas, como alerta Humphrey (2005, p. 25), o principal diferencial para um projeto ser bem sucedido é seu planejamento. Um projeto raramente é bem sucedido sem um adequado planejamento e, também, poucas vezes um projeto bem planejado acaba em fracasso (HUMPHREY, 2005, p. 25).

Gherbi, Charpentier e Couture (2011, p. 10) expõem que a segurança dos sistemas de informação continua a ser uma questão extremamente crítica, apesar dos progressos dos últimos 10 anos nas áreas de qualidade de software e confiabilidade do sistema. Para os autores citados, a fim de facilitar o gerenciamento do sistema, reduzir os erros de configuração, e alcançar a portabilidade, a maioria dos sistemas usados hoje em dia executam software substancialmente similar e, como consequência, esses sistemas compartilham

vulnerabilidades que facilitam a propagação de *malware (malicious software)* e permitem a exploração em larga escala dessas vulnerabilidades comuns. Sá (1998, p. 128) já nos alertava sobre esse aspecto ao colocar que: "É enganoso imaginar que os controles de uma empresa são bons porque são Computadorizados".

Atores internos e externos à organização estarão aptos a se aproveitarem de oportunidades que possam aparecer em virtude de vulnerabilidades identificadas em sistemas computadorizados das entidades. Algumas das ações de agentes internos são os acessos a dados não autorizados. Alguns exemplos podem ser vistos no Quadro 2.

Categoria	Características	Detecção	Mitigação
Acesso não autorizado.	Série de tentativas fracassadas de *logon*. Várias tentativas fracassadas seguidas por *logon* bem-sucedido.	Entrar em contas de funcionários ou clientes que deixaram a organização, mas cujas contas continuam ativas.	Criar ou reforçar procedimento para excluir contas de usuários imediatamente quando alguém mudar de função ou deixar a organização. Procurar anomalias como mais de uma pessoa tentando fazer *logon* usando as mesmas credenciais.
Acesso autorizado, de forma não adequada.	Alto nível de "*trolling*", ou seja, usos aparentemente não relacionados de aplicações e acessos aos dados.	Atividades atípicas dentro de aplicações e bancos de dados. Numerosas e repetidas tentativas de acesso a dados por usuário não autorizado.	Restringir o acesso do usuário a aplicações e dados, com base na necessidade de conhecer. Modificar os direitos de acesso, tão logo ocorra uma mudança de função.
Acesso autorizado, fora dos parâmetros normais.	Número excessivo de leituras, inserções e extrações de dados, incompatível com a função do usuário.	Monitorar o uso de aplicações críticas e acesso aos dados. Se uma pessoa deixar a organização, procurar retrospectivamente por comportamento incomum.	Proativa – Estar consciente e pronto para responder a significativas mudanças no ambiente de negócios, nas responsabilidades de usuário etc. Responsabilização – Observar os eventos e usuários envolvidos após os acontecimentos.
Acesso autorizado, dentro de parâmetros normais.	Nenhum desvio óbvio das atividades normais	Aspectos comportamentais, como a insatisfação com a organização, trabalho, mudanças recentes etc.	Incluir um processo de *feedback* sobre funcionários, atitudes no trabalho e outros atributos que possam influenciar.
Acesso não autorizado, fora dos parâmetros normais.	Número excessivo de tentativas de *logon* ou tentativas de acesso a dados ou funcionalidades não autorizadas. Número excessivo de leituras, inserções, extrações de dados etc.	Deve ser detectado antes que o acesso seja concedido, mas se não, então outras discrepâncias de comportamento devem ser consideradas. Número de tentativas de *logon*, número e tipo de acessos a dados sugerem um comportamento anômalo.	Combinar processos para identificar acessos não autorizados e comportamentos anômalos em sistemas e redes.
Acesso não autorizado, dentro de parâmetros normais.	Nenhum desvio óbvio das atividades normais	Outros aspectos fora do sistema, tais como horários incomuns de atividade.	Estabelecer um monitoramento de fatores suspeitos, tais como hora do dia, dia da semana, a frequência de tentativas de acesso etc.

Quadro 2: Detecção e mitigação de acesso não autorizado.
Fonte: Adaptado de Axelrod (2011, p. 22).

A capacidade dos sistemas computadorizados de acessar quase instantaneamente diversos bancos de dados distribuídos pelo planeta traz, também, o problema de exposição de seu banco de dados, em maior ou menor grau, a usuários de diversas regiões e nacionalidades. Em decorrência disso, qualquer sistema de informação conectado a uma rede está exposto, a princípio, a problemas de invasão de privacidade.

Audy, Andrade e Cidral (2005, p. 198-199) destacam alguns tipos de problemas de privacidade, conforme segue:

■ O *hacking,* que pode ser considerado a mais popular forma de invasão de privacidade em ambientes de sistemas de informação. Representa um acesso a um sistema de informação para conseguir dados sem autorização. Algumas vezes, os *hackers* além de se apoderam de forma indevida de dados, também, intencionalmente danificam o sistema. Em certos círculos, distingue-se entre *hackers* e *crackers*. O primeiro termo designaria peritos da área de TI que se especializam em atividades afetas à segurança de sistemas de informação. O termo *crackers* seria empregado para hackers com más intenções e que empregam seus conhecimentos para causar danos em sistemas e extrair informações de forma ilícita.

■ O *jamming* representa um bloqueio de acesso a um sistema de informação por meio do emprego de determinadas rotinas de software. Em acessos via Internet, os serviços disponibilizados pelo sistema atacado são interrompidos, podendo levar a danos que ultrapassam o âmbito do prestador de serviço e alcançam a várias pessoas e organizações.

■ O *sniffing* significa uma interceptação de informações que trafegam por determinada rede por meio do emprego de determinadas rotinas de software. As informações capturadas estão disponíveis a diversos usos não autorizados.

■ O *spoofing* constitui conseguir informações passando-se por outro. Na Internet, uma das formas usadas é a criação de sites falsos que levam os usuários a fornecer dados que poderão ter uso indevido.

■ O *spamming* representa uma prática de enviar e-mails não autorizados para uma pessoa ou organização. O *spam* pode ser utilizado para divulgação de produtos, serviços ou outras informações. Essa prática pode consumir recursos e causar transtornos para as pessoas e organizações vitimadas.

■ O vírus de computador é um *software* que ataca sistemas para causar danos a dados e *softwares* ou para reduzir seu desempenho de processamento. Os vírus têm causado prejuízos e demandado investimentos de recursos em sua prevenção. Políticas de segurança e aquisição de softwares antivírus têm ajudado nesse combate.

Outras formas, ou variantes das formas apresentadas acima, podem vir a ameaçar o ambiente institucional. POLLONI (2000, p. 217) expõe que a solução para os problemas de privacidade em sistemas de computadores está na criptografia. Deve-se relembrar, entretanto, que não existem sistemas que sejam, ainda que criptografados, absolutamente seguros. O estabelecimento de controles internos, em especial os controles prévios, pode contribuir para minimizar possíveis perdas, mas devido à rapidez com que as ameaças avançam em números e tecnologia empregada, esse se constitui um dos ambientes de controle mais desafiadores para os profissionais da área.

1.5.2 Modelos, normas, padrões, metodologias e melhores práticas de TI

Diversos são os modelos, normas, padrões, metodologias e melhores práticas existentes na área de TI. Alguns desses são destacados abaixo.

> O que impressiona, no entanto, é a profusão de normas, padrões, metodologias e melhores práticas que começaram a surgir. Hoje, temos várias, com características pouco diferentes. Quase sempre desenvolvidas por institutos americanos e europeus, estas normas, padrões e metodologias têm um objetivo: o desenvolvimento de *software* deve ser feito com a qualidade adequada, de forma profissional e regulamentada. Em outras palavras, colocar ordem na casa. (HABERKORN, 2009, p. 126, grifo do autor).

A Gestão da Qualidade Total (*Total Quality Management*) é um modelo orientado para criação de uma consciência da qualidade em processos organizacionais, internos ou externos, com o envolvimento de todos os integrantes da entidade. Esse modelo definiu, segundo Haberkorn (2009, p. 127), as normas relativas aos atributos que devem ser avaliados para se estabelecer a qualidade do *software*, partindo dos seguintes pontos básicos:

■ Facilidade de uso: a navegação deve ser feita por usuário sem muito treinamento. O programa deve manter conformidade com as demandas do usuário, estar de acordo com requisitos preestabelecidos e conter muitos *helps* (ajudas), claros e de fácil entendimento.

■ Segurança da informação: o acesso ao sistema deve ser restrito e efetuado por senhas. O programa deve, ainda, ser de difícil invasão.

■ Flexibilidade: o sistema deve se adequar facilmente às necessidades específicas do usuário.

■ Portabilidade: o sistema deve rodar em ambientes como Windows ou Linux; em máquinas Macintosh, Intel etc.; ou ainda, no *palm*, no *pocket* PC etc.

■ Estabilidade: pode ser considerado o mais importante ponto de avaliação. Um sistema estável é aquele que funciona sem travar, sem fechamentos repentinos, sem perda de arquivos ou dados, ou seja, sem erro de *software*.

■ Performance: está relacionado ao desempenho do sistema. Para se avaliar esse ponto, o sistema deve ser analisado dentro de *hardware* equivalente, ou seja, para se comparar performances, todos os sistemas devem estar em uma mesma plataforma de *hardware*.

Capability Maturity Model Integration (CMMI, 2010, p. 7) é um modelo que propõe boas práticas dos processos que envolvem o desenvolvimento, modernização ou manutenção de softwares, representando uma evolução do *Capability Maturity Model* (CMM) que é um modelo, também, focado na melhoria contínua dos processos organizacionais, que teve início a mais de meio século. O CMMI *framework* promove uma estrutura que dispõe de elementos essenciais para trilhar um caminho de melhoria constante, avançando por níveis de capacidade e maturidade de processos, de forma a obter uma maior qualidade e eficácia, gerando modelos de processos, técnicas de treinamento e formatos de relatórios apropriados a cada um dos diversos clientes envolvidos no processo (CMMI, 2010, p. 8). Os níveis de capacidade aplicáveis a uma organização dizem respeito à melhoria de processos individualmente, enquanto os cinco níveis de maturidade estão relacionados à melhoria de múltiplos processos (CMMI, 2010, p. 25-32). O quadro 3 traz uma comparação entre os referidos níveis:

COMPARAÇÃO ENTRE NÍVEL DE CAPACIDADE E DE MATURIDADE		
Nível	**Níveis de Capacidade**	**Níveis de Maturidade**
Nível 0	Incompleto	
Nível 1	Executado	Inicial
Nível 2	Gerenciado	Gerenciado
Nível 3	Definido	Definido
Nível 4		Gerenciado Quantitativamente
Nível 5		Otimizado

Quadro 3: Comparação entre nível de capacidade e de maturidade do CMMI.
Fonte: Adaptado de CMMI (2010, p. 25).

O modelo MPS (Melhoria do Processo de Software) ou MPS.BR (Melhoria do Processo de Software Brasileiro) é um modelo nacional desenvolvido pela Associação para Promoção da Excelência do Software Brasileiro (SOFTEX), vinculada ao Ministério da Ciência, Tecnologia e Inovação, que se baseia em conceitos de maturidade e capacidade de processo para a avaliação e melhoria da qualidade e produtividade de produtos de software e serviços correlatos, em consonância com a Norma Internacional ISO/IEC 12207:2008 e o modelo CMMI, entre outros (SOFTEX, 2011, p. 7).

O *Control Objectives for Information and Related Tecnology* (COBIT), Objetivos de Controle para Informações e Tecnologias relacionadas, é descrito, segundo a ISACA (2010, p. 5), como um conjunto internacionalmente aceito de ferramentas organizadas em um modelo que serve de referência para que os responsáveis de uma instituição possam fazer uso para assegurar que a TI esteja ajudando a atingir suas metas e objetivos. Ele garante que a TI está trabalhando da forma mais eficaz possível para minimizar os riscos relacionados e maximizar os benefícios do investimento em tecnologia, estreitando a lacuna entre o negócio e a TI. As orientações do COBIT, conforme a ISACA (2010, p. 5) descreve, melhoram a eficiência e a eficácia, ajudam na compreensão das demandas de TI, propõem práticas para suprir as necessidades organizacionais da forma mais eficiente possível, certificam o alinhamento entre o negócio e a tecnologia empregada e, ainda, auxiliam no entendimento e gerenciamento dos investimentos em TI em todo o seu ciclo de vida. Para Luciano e Testa (2011, p. 246), o objetivo do COBIT é promover boas práticas através de um *framework* de domínios e processos e apresentar uma estrutura lógica gerenciável.

O *Project Management Institute* (PMI, 2007, p. 1) busca alcançar um gerenciamento de projetos eficaz que possa converter estratégias organizacionais em resultados positivos para os negócios, zelando por premissas como estabelecer prazos, definir tarefas, identificar itens de caminho crítico, especificar e adquirir materiais, acompanhar custos e o valor agregado.

O *Rational Unified Process* (RUP) é, segundo a IBM Rational (2001, p. 1), um processo de engenharia de *software* que oferece uma abordagem disciplinada para atribuição de tarefas e responsabilidades dentro do desenvolvimento de uma nova ferramenta. Por passar por constantes atualizações, tenta oferecer as melhores práticas aplicáveis. Esse processo aumenta a produtividade da equipe, ao definir diretrizes, modelos, ferramentas e uma base única de conhecimento para as atividades de desenvolvimento. Assim, o gerente de projeto, o analista de requisitos, o analista de sistemas, o programador e os demais envolvidos no projeto permanecem integrados por uma linguagem comum. Destacam-se algumas das melhores práticas empregadas:

MELHORES PRÁTICAS NO DESENVOLVIMENTO DE *SOFTWARE*	
Prática	**Descrição**
Desenvolvimento Iterativo	Devido à complexidade envolvida, é necessária uma abordagem iterativa que permita uma maior compreensão do problema através de sucessivos refinamentos, alcançando uma solução efetiva sobre múltiplas iterações. O tratamento dos itens de maior risco em todas as fases do ciclo de vida reduz significativamente o perfil do risco. Essa abordagem iterativa ajuda você a atacar riscos através de executáveis que permitem o envolvimento do usuário final e contínuo *feedback*.
Gerenciamento de	Deve haver uma clara descrição de como extrair, organizar e documentar as funcionalidades e

Requisitos	restrições; acompanhar e documentar compromissos e decisões; e capturar e comunicar requisitos de negócios. Esse processo busca conduzir a um sistema que realmente atenda às expectativas do usuário final.
Arquitetura baseada em componentes	O processo deve inicialmente se concentrar no desenvolvimento de uma arquitetura consistente, flexível e intuitiva, o que levará a uma maior economia de recursos durante o desenvolvimento do sistema. Componentes não são simplesmente módulos, são subsistemas (ou subprocessos) que cumprem uma clara função específica.
Modelagem Visual	O processo deve mostrar visualmente a estrutura das arquiteturas e componentes. Isso permite, entre outras vantagens, verificar como se encaixam os elementos do sistema, mantendo uma coerência entre o projeto e sua implantação e promovendo uma comunicação inequívoca.
Verificação da Qualidade	A qualidade deve ser revista com respeito aos requisitos baseados em confiabilidade, funcionalidade, aplicação e desempenho do sistema. A avaliação da qualidade deve ser construída dentro do processo, envolver todas as atividades e participantes, e não estar como uma atividade a parte, realizada por um grupo específico.
Controle de Alterações	O processo deve descrever como controlar, acompanhar e monitorar alterações para permitir um desenvolvimento iterativo de sucesso. Ele deve, também, estabelecer espaços de trabalho seguros para cada desenvolvedor (para que um não interfira no trabalho de outro) e controlar as mudanças de todos os artefatos de software (por exemplo, modelos, código, documentos etc.).

Quadro 4: Melhores práticas no desenvolvimento de software.
Fonte: Elaborado pelo autor com dados da IBM Rational (2001, p. 2).

Para conseguir a consecução de seus objetivos, o RUP é dividido em quatro fases (concepção, elaboração, construção e transição) com propósitos específicos. O processo, também, define claramente quatro elementos de modelagem: trabalhadores (quem está fazendo), atividades (como), artefatos (o que) e o fluxo de trabalho ou *workflow* (quando).

As normas ISO/IEC, também, possuem importante papel na definição de procedimentos e especificações para produtos e, em especial, para produtos ligados à área de informática. Dentro desse universo, destaca-se a ISO/IEC 12207:2008 que estabelece, segundo a ISO (2008, p. 1), um *framework* comum para os processos de ciclo de vida do *software*, com terminologia bem definida, que serve de referência para a indústria e especificando processos, atividades e tarefas que devem ser aplicadas durante a aquisição, serviço, fornecimento, desenvolvimento, operação, manutenção e eliminação dos respectivos produtos. A definição do contexto aplicável e os procedimentos para definir, controlar e melhorar os processos durante todo o ciclo de vida do *software*, também, estão incluídos nesse documento.

Como observado, diversos processos e abordagens podem ser seguidos para o desenvolvimento de um software. O importante é que se escolha um conjunto das melhores práticas existentes que esteja mais adequado ao tamanho do projeto e à realidade da organização.

1.6 O Sistema de Pagamento de Pessoal da Marinha

As crescentes demandas sociais conduzem a um processo de pressão sobre o Legislativo, o que, a princípio, conduz à reformulação de diversas normas legais existentes. Também, o constante progresso tecnológico conduz a novas ameaças e oportunidades. Esta realidade exige novas ferramentas e processos que assegurem a execução das atividades de pagamento com agilidade e confiabilidade. Os aspectos de tempestividade, flexibilidade e fidedignidade exigidos para os sistemas de pagamento favorecem sobremaneira a utilização de ferramentas automatizadas.

Desse modo, uma firme estrutura administrativa é imperativa para assegurar uma plena compreensão dos processos vinculados à atividade de pagamento e para uma identificação mais precisa das necessidades de aprimoramento. Um sistema automatizado de informações contribui com flexibilidade e agilidade para uma resposta apropriada às ameaças e oportunidades que venham a se apresentar.

No Governo Federal, o Decreto nº 2.028, de 11 de outubro de 1996, dispõe que órgãos do Sistema de Controle Interno devem adotar procedimentos destinados a garantir que os pagamentos de pessoal ativo e inativo, assim como de pensionistas, sejam operacionalizados de modo a permitir a emissão de ordem bancária contra o Tesouro Nacional.

Segundo Almeida (1997, p. 1), mesmo em entidades em que a folha de pagamento e seus apensos são trabalhados por sistemas computadorizados, existe a obrigação de se avaliar a qualidade das informações e programas usados no processo, além de confirmar se os mecanismos de controle interno existentes são suficientes e se são efetivamente empregados pelo setor responsável.

As especificidades de direitos e deveres estabelecidos, entre outros, no Estatuto dos Militares (Lei 6.880, de 9 dezembro de 1980) e no Decreto nº 4.307, de 18 de julho de 2002, demandam sistemas de pagamento específicos que possam atender às diversas exigências estabelecidas.

Nesse contexto, a Marinha do Brasil (MB), desde a década de sessenta, vem utilizando o Sistema de Pagamento de Pessoal (SISPAG) para processar as informações atinentes à folha de pagamento de pessoal. Esse sistema foi concebido inicialmente para a automatização do pagamento de inativos e pensionistas, mas, após algum tempo, foi estendido para o processamento do pagamento de pessoal da ativa.

A estrutura administrativa do SISPAG é composta de órgãos e processos que executam um conjunto de tarefas para consecução das finalidades previstas para o sistema de pagamento, conforme pode ser visualizado na figura 3 abaixo:

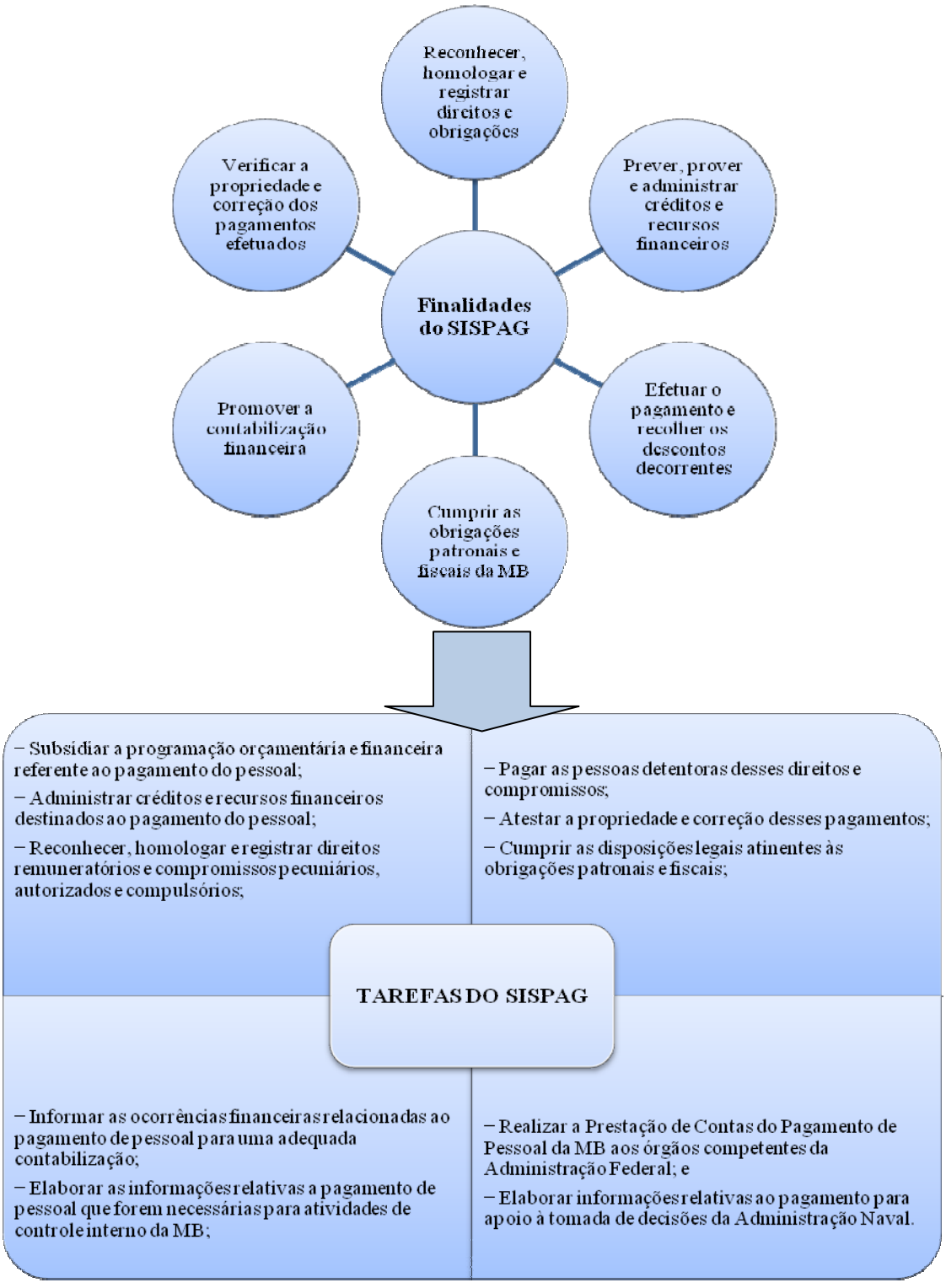

Figura 3: Tarefas e finalidades do Sistema de Pagamento da Marinha do Brasil (SISPAG).
Fonte: Elaborado pelo autor com dados da MB (2007).

As tarefas do SISPAG se concretizam, ainda, de acordo com rotinas anuais, mensais e extraordinárias, assim descritas pela norma (MB, 2007):

a) Anuais: subsidiar a programação orçamentária e financeira do exercício seguinte; prestar contas do exercício corrente; e gerar informações fiscais dirigidas aos indivíduos remunerados pelo SISPAG e aos Órgãos da Administração Federal;

b) Mensais: reconhecer, homologar e registrar direitos e compromissos financeiros das pessoas; calcular e executar pagamentos, descontos e obrigações patronais e fiscais com previsão legal; conferir a propriedade e a correção dos pagamentos efetuados; promover o registro contábil desses pagamentos; e administrar recursos financeiros destinados ao pagamento do pessoal; e

c) Extraordinárias: Executar os procedimentos previstos para as rotinas mensais, em virtude de necessidades específicas e circunstâncias de pagamento de caráter urgente.

O documento interno (MB, 2007) estabelece que as atividades de pagamento de pessoal possam ser Homologatórias, Administrativas Gerenciais ou Administrativas Operacionais, conforme especificado a seguir:

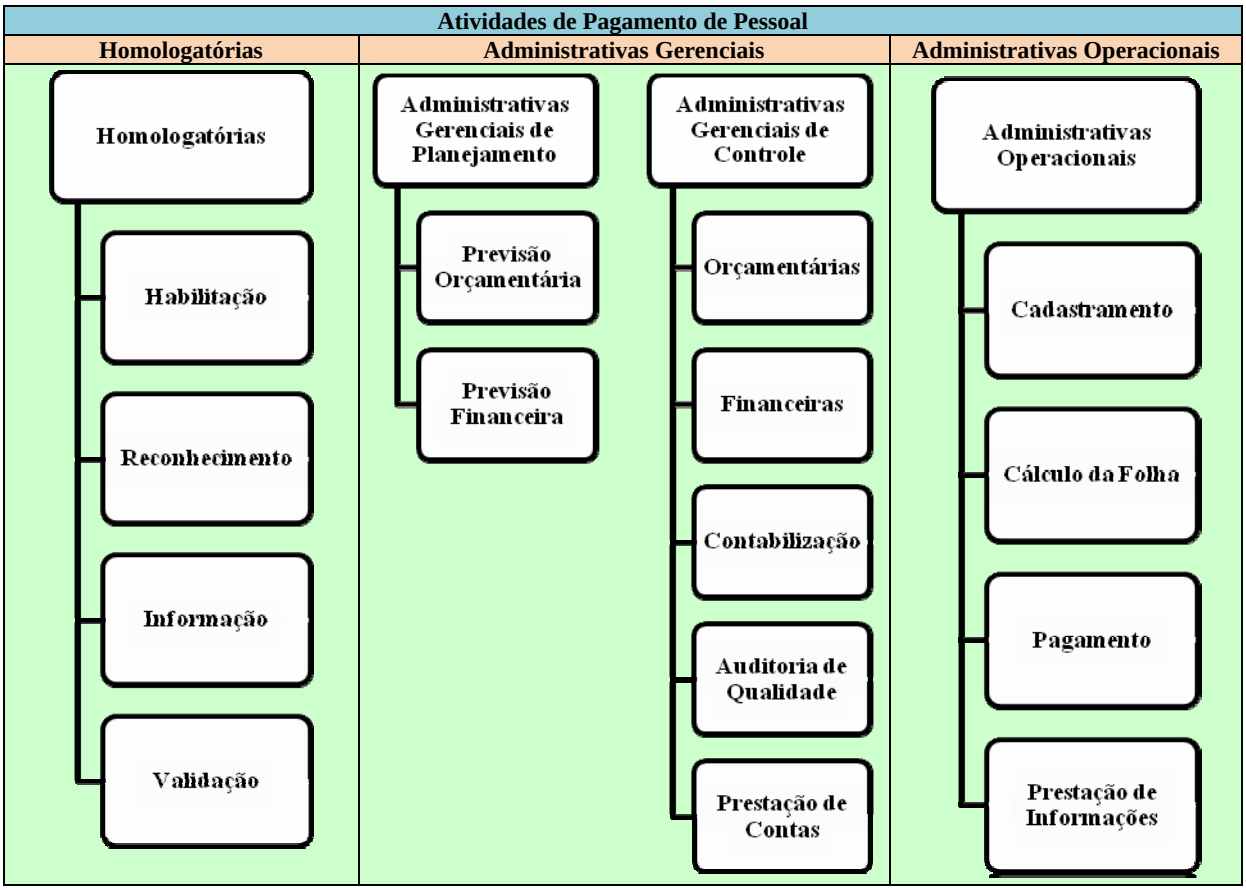

Figura 4: Atividades de Pagamento de Pessoal.
Fonte: Elaborado pelo autor com dados da MB (2007).

- Homologatórias: Atividades atinentes ao reconhecimento de direitos e deveres remuneratórios, relacionados diretamente à função de administração de pessoal, e traduzem-se pela informação de criação ou expansão de direito ou obrigação de uma pessoa por meio de parcela de remuneração ou desconto, tendo em vista o atendimento, pela pessoa, das condições legalmente impostas. Elas envolvem os seguintes processos:

- Habilitação- Processo de estabelecimento e normatização de fatos e atos, que originem direitos ou deveres remuneratórios, e de critérios para sua concessão ao indivíduo com relação e vínculo de remuneração com a MB;
- Reconhecimento- Processo de análise e identificação de indivíduos associadas a direitos e deveres remuneratórios, mediante aplicação das normas e critérios estabelecidos no processo de habilitação;
- Informação- Processo que deixa ciente o Órgão Pagador (OP) do início, alteração ou cessação de direito e dever que gere efeito financeiro, conotado a um indivíduo com relação e vínculo de remuneração com a MB; e
- Validação- Processo que atesta a propriedade e correção de efeitos decorrentes das informações prestadas ao OP.

- Administrativas Gerenciais: Atividades de caráter gerencial que têm por base o reconhecimento e informação dos direitos e deveres remuneratórios fixados no prévio desempenho das atividades homologatórias e o exercício da atividade administrativa operacional de execução. Estão assim distribuídas:

a) Atividades administrativas gerenciais de planejamento:

I) Previsão orçamentária: Processo de julgamento que conduz à organização de um documento com a necessidade de recursos orçamentários, expressa em células de crédito, naturezas de despesa, prazos e períodos, bem como fontes de recursos, quando for o caso, para atender ao pagamento de pessoal; e

II) Previsão financeira: Processo de julgamento que conduz à organização de um documento com as necessidades de recursos financeiros, conotados a prazos e períodos de tempo, bem como fontes de recursos para pagamento de pessoal.

b) Atividades administrativas gerenciais de controle:

I) Controle orçamentário: Processo de provisionamento, acompanhamento e controle dos recursos orçamentários destinados ao pagamento de pessoal;

II) Controle financeiro: Processo de recebimento, acompanhamento e controle dos recursos financeiros destinados ao pagamento de pessoal;

III) Contabilização: Registro de fatos contábeis relacionados ao pagamento de pessoal, abrangendo a apropriação e o controle de pagamentos, descontos e adiantamentos executados, conforme o Plano de Contas da Administração Federal;

IV) Auditoria de qualidade do sistema: Processo com que se verifica a satisfação do usuário final, a correção e tempestividade dos processos do sistema, a utilidade das informações gerenciais produzidas pelo sistema, o cumprimento das normas operacionais e de segurança (lógica e física) por parte dos órgãos envolvidos com o sistema, a manutenção das aplicações do sistema e a consistência e confiabilidade dos dados utilizados pelos processos do sistema, bem como suas etapas, visando à racionalização dos mesmos; e

V) Prestação de contas: Processo de geração e expedição de informações, endereçadas aos Órgãos do Sistema de Controle Interno da Marinha do Brasil (SCIMB) e da Administração Federal, que demonstram a legitimidade e legalidade da aplicação dos recursos.

- Administrativas Operacionais (de Execução): Atividades de caráter operacional que envolvem reconhecimento, informação e validação de direitos e deveres remuneratórios fixados no prévio desempenho das atividades homologatórias de habilitação. Estão assim distribuídas:

a) Cadastramento: Processo em que Informantes Qualificados - IQ (MB, Extra-MB ou Privilegiado) e Organizações Centralizadoras (OC) fornecem informações pessoais, funcionais e financeiras para atualização de cadastros do sistema e cálculo da folha de pagamento;

b) Cálculo da folha de pagamento: Processo em que o OP operacionaliza:

I) informações geradas pelo exercício das atividades homologatórias e das expedidas pelas Entidades Consignatárias habilitadas à troca de informações com o SISPAG;

II) cálculo das remunerações e das obrigações fiscais e patronais da MB; e

III) emissão e expedição de documentação destinada a executar, formalizar e comprovar os pagamentos efetuados;

c) Pagamento: Processo em que o OP efetua o pagamento, normalmente com crédito em contas correntes dos indivíduos com relação e vínculo de remuneração com a MB e naquelas de pessoas, físicas ou jurídicas, credoras dos descontos efetuados; e

d) Prestação de informações:

I) Elaboração de informações fiscais: Processo em que o OP prepara informações em atendimento às obrigações fiscais legalmente previstas, para posterior expedição às pessoas remuneradas pelo SISPAG e aos órgãos competentes da Administração Federal;

II) Averbações individuais: Processo em que o OP procede ao registro dos históricos de pagamentos e descontos efetuados, decorrentes de fatos geradores de nível individual;

III) Apoio à tomada de decisões da Administração Naval: Processo em que o OP produz e presta informações sobre pagamento do pessoal como subsídio à tomada de decisões da Administração Naval; e

IV) Apoio ao SCIMB: Processo em que o OP produz e presta informações sobre pagamento do pessoal aos órgãos de controle interno da Marinha.

1.6.1 Órgãos ligados à folha de pagamento de pessoal

As atividades de pagamento de pessoal demandam um esforço razoável das diversas unidades envolvidas para assegurar uma adequada e tempestiva prestação dos serviços. A estrutura do pagamento de pessoal da MB compreende os seguintes órgãos e atribuições:

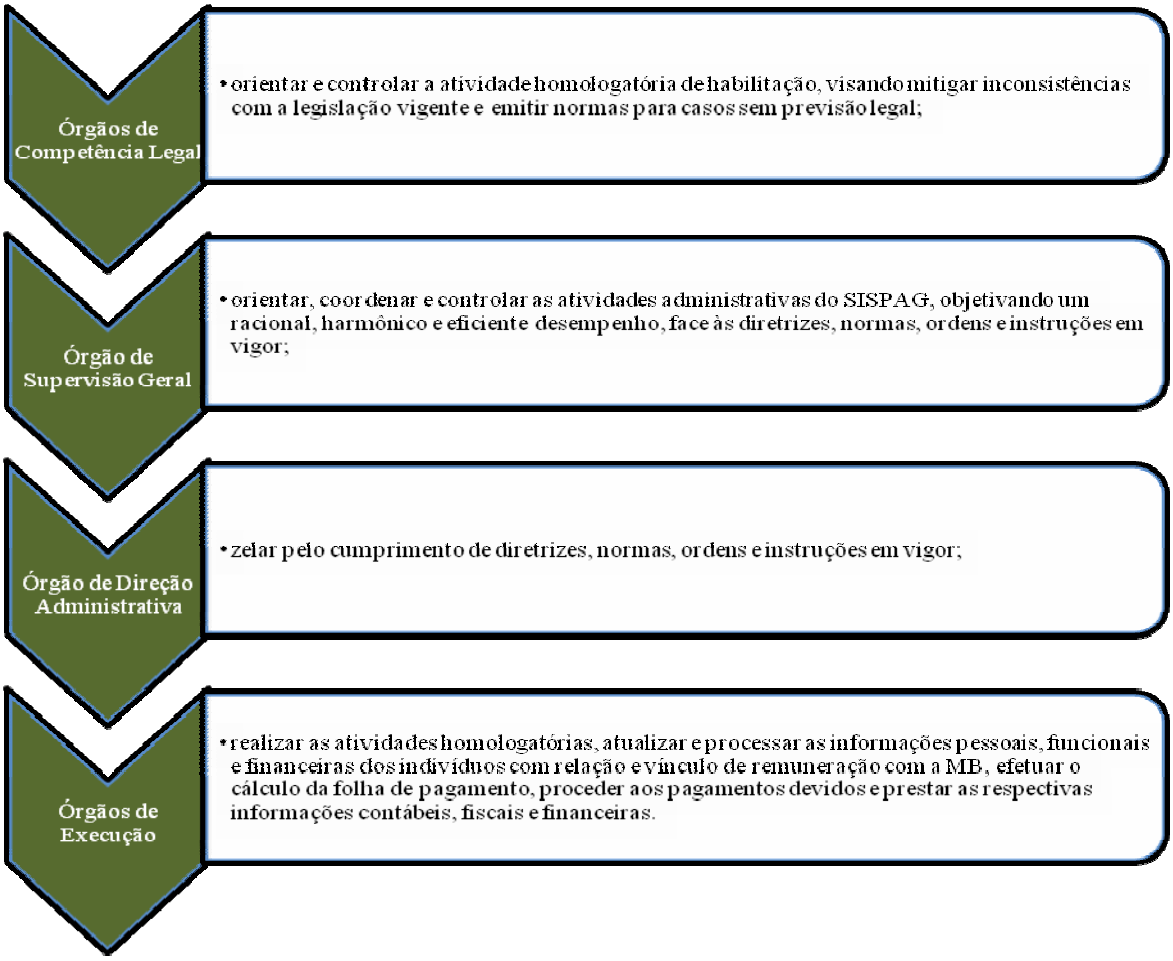

Figura 5: Estrutura de Pagamento de Pessoal da MB.
Fonte: Elaborado pelo autor com dados da MB (2007).

Os Órgãos de Execução são subdivididos pela MB (2007) em diversos tipos, assim definidos:

❖ Informantes Qualificados da MB (IQ-MB)- organizações militares autorizadas a comandar, com exclusividade, informação sob sua jurisdição, com amplitude para alcançar qualquer pessoa remunerada pelo SISPAG, sendo de sua competência o exercício de atividades homologatórias;

❖ Informantes Qualificados Extra-MB (IQ-EX)- organizações que são conhecidas, também, como Entidades Consignatárias, estando autorizadas, pelo OP, mediante convênio, a comandar, com exclusividade, informação sob sua jurisdição, com amplitude para alcançar qualquer pessoa remunerada pelo SISPAG;

❖ Informante Qualificado Privilegiado (IQ-P)- aquele que comanda qualquer informação, mesmo as sob a jurisdição dos IQ-MB ou IQ-EX, com amplitude para alcançar qualquer pessoa remunerada pelo SISPAG, sendo representado pela própria PAPEM;

❖ Organizações Centralizadoras (OC)- organizações militares responsáveis por comandar informações, que não sejam de responsabilidade dos IQ-MB ou IQ-EX, com amplitude para alcançar pessoas de sua lotação ou de organizações militares apoiadas;

❖ Organizações Militares Centralizadas (OMC)- aquelas apoiadas por uma OC nos processos atinentes ao pagamento de pessoal; e

❖ Órgão Pagador (OP)- aquele que efetua o cálculo da folha de pagamento, efetivando os pagamentos e descontos cabíveis e apresentando as informações contábeis, fiscais e financeiras relativas ao SISPAG.

Entre os diversos órgãos ligados à folha de pagamento, o Órgão Pagador (OP) pode ser considerado o principal responsável pela operacionalização do sistema de pagamento. A Pagadoria de Pessoal da Marinha (PAPEM) responde na MB pelas funções de OP.

A PAPEM foi ativada, de acordo com seu site na Internet (PAPEM, 1997, p. 1), em 1997 e possui como lema “Ordem, Prontidão e regularidade!”. Dentro de seu lema, ordem está no sentido de boa administração e determinação, a prontidão se encontra associada à presteza e rapidez e, finalmente, a regularidade diz respeito à harmonia e pontualidade. Existe ainda bem especificada uma diretriz de comportamento: “Todas as ações dos militares e servidores civis da PAPEM devem buscar a melhoria de sua eficiência, eficácia, ordem, prontidão e regularidade, sempre almejando a máxima excelência nos serviços prestados às OM” (PAPEM, 1997, p. 1). O referido órgão possui, de acordo com a PAPEM (2010, p. 10), os seguintes objetivos permanentes:

a) Valorização e Capacitação do Capital Humano- manter os funcionários qualificados, comprometidos com a Missão, dispostos ao aprendizado contínuo e empenhados na realização de tarefas, atendendo as demandas psicossociais da tripulação;

b) Aperfeiçoamento e inovação dos processos – aprimorar os processos executados, estimulando iniciativas inovadoras para a melhoria no atendimento das necessidades de pessoas e organizações que interagem com a PAPEM;

c) Preservar a disciplina, a hierarquia, os valores morais e éticos e as tradições da MB – A disciplina pode ser entendida como o acatamento integral das leis, regulamentos e normas, e a obediência às funções que se deve desempenhar, se constituindo em pedra angular para o desenvolvimento regular das atividades. A hierarquia militar pode ser descrita como a ordenação da autoridade, em níveis diferentes, dentro da estrutura das Forças Armadas. Os valores morais e éticos são essenciais para a compreensão da organização e devem servir de parâmetros para orientação das escolhas e ações individuais. As tradições navais e os usos e costumes marinheiros permeiam as mentes, fortalecendo e incentivando os homens do mar;

d) Defender os interesses da MB nos ambientes em que atua – Interagir com órgãos e setores extra-MB relacionados com a área de atuação da PAPEM e cujas decisões possam vir a impactar os interesses da Marinha; e

e) Excelência de Gestão – Desenvolver um ambiente de excelência de gestão e tornar-se referência, no âmbito das Forças Armadas, na área de Pagamento de Pessoal.

A execução das atividades de folha de pagamento desempenhadas pela PAPEM eram realizadas pela Diretoria de Finanças da Marinha (DFM), que com essa remodelagem passou a exercer, como órgão superior, somente as ações de controle interno (prévio, concomitante e subsequente) sobre o sistema de pagamento de pessoal. Entre as competências do OP, destacam-se as seguintes:

I) administrar recursos destinados ao pagamento de pessoal;

II) processar informações enviadas, calcular as remunerações (pagamentos e descontos) e as obrigações patronais da MB e gerar documentos destinados a executar, formalizar e comprovar os pagamentos;

III) realizar pagamentos por meio de créditos bancários, referentes às remunerações e descontos efetuados;

IV) registrar fatos ligados ao pagamento do pessoal;

V) organizar e encaminhar informações legalmente previstas;

VI) organizar e encaminhar informações para apoio ao controle interno da MB;

VII) organizar e encaminhar informações aos órgãos competentes da Administração Federal, que comprovem a utilização de recursos financeiros, no exercício;

VIII) organizar e encaminhar informações para tomada de decisão da Administração Naval;

IX) cadastrar IQ, especificando a jurisdição de informações a eles atribuídas pelo Órgão de Supervisão Geral;

X) habilitar Entidades Consignatárias;

XI) definir as responsabilidades das Entidades Consignatárias habilitadas;

XII) organizar e encaminhar subsídios para programação orçamentária e financeira; e

XIII) desenvolver, homologar, implantar e manter os sistemas de informação que apoiam o SISPAG.

Para realizar a complexa tarefa de operacionalizar a folha de pagamento, a PAPEM se encontra estruturada em departamentos e assessorias, conforme consta de seu regimento interno, aprovado pela Portaria nº9/PAPEM, de setembro de 2008, como esclarecido nos parágrafos abaixo:

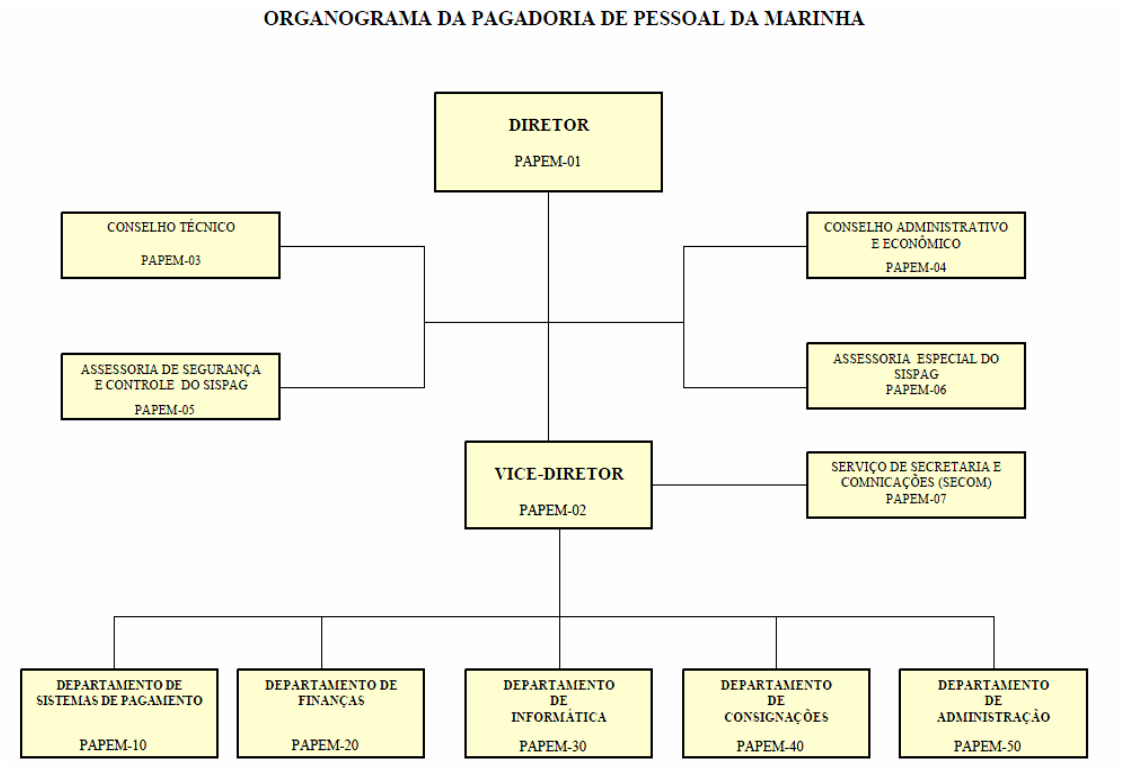

Figura 6: Organograma da Pagadoria de Pessoal da Marinha
Fonte: Anexo A de PAPEM (2008).

O Diretor deve conduzir os serviços e atividades da PAPEM, exercer as funções de Ordenador de Despesa da PAPEM e do Órgão Pagador do PAPEM-SISTEMA e desempenhar

as atribuições legais e normativas para Diretor de Organização Militar e para Diretor de Repartição ou cargo correspondente no Serviço Público da União.

O Vice-Diretor deve auxiliar o Diretor e substituí-lo em seus impedimentos, orientar, coordenar e controlar os serviços e atividades afetos aos Departamentos, coordenar e controlar a administração do pessoal, promovendo a distribuição e realocação de recursos humanos aos departamentos, e exercer as demais atribuições previstas regulamentos e normas em vigor.

O Conselho Técnico assessora o Diretor em assuntos de natureza técnico-administrativa e estuda assuntos técnicos inerentes às atribuições do PAPEM-SISTEMA que lhe sejam apresentados por quaisquer dos seus membros.

O Conselho Administrativo-Econômico assessora o Diretor em assuntos administrativos da organização.

A Assessoria de Segurança e Controle do SISPAG possui, entre outras, as seguintes incumbências:

a) aprimorar o controle interno sobre a atividade de pagamento de pessoal, enfatizando o procedimento de crítica sobre as alterações mensais de pagamento;

b) elaborar séries históricas e projeções de comportamento das despesas relativas às parcelas de pagamento;

c) estabelecer indicadores detalhados que definam comportamentos esperados e que apontem desvios em relação aos citados comportamentos;

d) identificar, registrar e atualizar, detalhadamente, as regras de negócio que condicionam a atividade de pagamento de pessoal;

e) avaliar, comparativamente, as Organizações Centralizadoras (OC), no que tange a comportamentos esperados de parcelas de pagamento; e

f) elaborar estatísticas que permitam estabelecer pontos de controle sobre o desempenho do SISPAG e de seus agentes.

A Assessoria Especial do SISPAG assessora o Diretor em assuntos relacionados ao SISPAG, bem como aqueles atinentes à sua modernização.

O Serviço de Secretaria e Comunicações administra o arquivo geral, o protocolo e as atividades relativas à correspondência oficial e serviços de comunicações da PAPEM.

Ao Departamento de Sistemas de Pagamento compete, especificamente com relação ao SISPAG:

a) administrar o pagamento de pessoal da Marinha, no país e no exterior;

b) administrar o cadastro de pessoal no PIS/PASEP;

c) administrar as atividades operacionais no SISPAG;

d) exercer o controle de qualidade das parcelas e cadastros do pagamento;

e) fazer cumprir as obrigações patronais da Marinha;

f) administrar repasses de benefícios facultativos e compulsórios recolhidos pelo SISPAG;

g) administrar atividades de bloqueios e reversões, referentes ao pagamento de pessoal militar;

h) normatizar e realizar estudos relativos a pagamento de pessoal;

i) supervisionar o recebimento e executar a transferência de dados para o SISPAG;

j) promover, no âmbito interno e externo, treinamento ao pessoal que realiza atividades de pagamento de pessoal; e

k) prestar assessoria jurídica às atividades relacionadas com pagamento de pessoal.

O Departamento de Finanças possui, entre outras, as seguintes atribuições:

a) administrar os créditos de Pagamento de Pessoal;

b) administrar os registros contábeis e financeiros atinentes ao PAPEM-SISTEMA;

c) administrar os recursos financeiros alocados ao PAPEM-SISTEMA;

d) administrar os recursos financeiros especiais alocados à PAPEM;

e) administrar as atividades de bloqueios, reversões e efetuar o controle do rol de devedores atinentes ao pagamento de pessoal; e

f) exercer as atribuições delegadas pelo Diretor.

O Departamento de Informática tem sob sua responsabilidade o gerenciamento de recursos de microinformática, a gerência sobre os dados de sistemas de informação relacionados ao SISPAG e a administração de atividades de concepção, desenvolvimento, implementação e manutenção de sistemas de informação conotados ao SISPAG.

O Departamento de Consignações é responsável por administrar as atividades oriundas das entidades consignatárias, que alimentam o SISPAG.

Ao Departamento de Administração cabe administrar bens patrimoniais, recursos orçamentários e financeiros destinados ao funcionamento da PAPEM, conduzir as atividades de segurança e manutenção das instalações, gerir as atividades de pessoal e treinamento, administrar as atividades de obtenção, promover o apoio operacional aos Departamentos e propor a distribuição, pelos Departamentos, do pessoal militar subalterno e dos servidores civis.

1.6.2 Operacionalização da folha de pagamento de pessoal

O processamento da folha de pagamento de pessoal da MB é efetuado por meio do Sistema de Pagamento de Pessoal da MB (SISPAG), que trabalha as informações exigidas para o pagamento das pessoas com relação de remuneração (RR) com o referido Comando Militar. Uma pessoa pode ter uma ou várias RR e receber valores em moeda nacional, em dólares americanos ou em euros.

Primeiramente, será explicada a operacionalização da folha de pagamento em moeda nacional, de maneira que seja possível a compreensão do que ocorre nas diversas organizações envolvidas. Em um segundo momento, será detalhado cada um dos subprocessos envolvidos em todo o processamento da folha. Desta forma, se espera dar maior entendimento sobre o complexo processo operacional do pagamento de pessoal.

A operacionalização da folha de pagamento em moeda do País é realizada no SISPAG por organizações militares distribuídas pelo território nacional. O início do processo ocorre quando uma das cerca de 150 Organizações Centralizadoras (OC) ou um dos Informantes-Qualificados (IQ), em número próximo a 80, efetua a inserção de parcelas de maneira remota pelo acesso à intranet da MB. Os IQ Extra-MB, por indisporem desse acesso, encaminham suas parcelas pela interface *batch*. As demais OC e IQ em situações de indisponibilidade da intranet também farão uso da modalidade lote. A interface ou modalidade lote é o encaminhamento de um conjunto de parcelas por meio diferente da interface *online* do SISPAG, utilizando, por exemplo, uma mídia magnética.

O conceito de parcela, também conhecida por alteração de pagamento, é uma representação de direito ou obrigação financeira, legalmente fundamentado e normatizado internamente, que uma pessoa detém para fins de remuneração com a MB. Ou seja, cada direito ou obrigação é operacionalizado no SISPAG por meio de uma ou mais parcelas. Por conseguinte, a remuneração devida a uma pessoa é composta por uma ou mais parcelas. Cada uma dessas parcelas passa mensalmente por uma Rotina de Cálculo, que considera diversos parâmetros (como posto ou graduação, por exemplo) para apurar os corretos valores devidos.

Mensalmente, em data e hora especificadas em calendário próprio divulgado aos interessados, o Órgão Pagador (OP) promove o fechamento das alterações de pagamento. A partir desse momento, as organizações que iniciaram o processo, OC e IQ, não podem promover alterações, inclusões ou retiradas no processo de pagamento. As OC e IQ, no entanto, podem promover os bloqueios de pagamento, impedindo o efeito financeiro para as

pessoas envolvidas em situações específicas, como falecimento etc. A figura abaixo traz um exemplo de calendário do quarto trimestre de um ano financeiro.

Evento	Responsável	Out	Nov	Dez
Data limite para entrega das alterações UPLOAD-OC	PAPEM	05/Out	04/Nov	30/Nov
Distribuição do processo de pagamento				
OC de Área Fora do Grande Rio, remessa por malote.	PAPEM	19/Out	22/Nov	09/Dez
OC de Área do Grande Rio: recebimento na PAPEM	OC	20/Out	23/Nov	12/Dez
Encerramento do bloqueio de pagamento				
Mensagem Solicitando bloqueio e bloqueio online: efetuado pelas OC, até às 11:30h.	OC	26/Out	25/Nov	16/Dez
DIA DO PAGAMENTO DA MARINHA - Pessoal no País; Pensão Alimentícia e Aluguel de Casa	Bancos Conveniados	03/Nov	02/Dez	03/Jan/12

Figura 7: Calendário de pagamento do quarto trimestre do ano de 2011.
Fonte: Adaptado de PAPEM (2011).

De posse desses dados, o OP integra à folha de pagamento as parcelas de sua responsabilidade e efetua um processo de depuração (ou crítica) sobre a totalidade da folha. Nesse processo de depuração algumas parcelas são corrigidas, com posterior aprovação, enquanto outras são recusadas e retornam à organização de origem para serem reprocessadas para o mês seguinte. As parcelas aprovadas passam à fase de cálculo, em que são apuradas, também, as obrigações patronais devidas que integrarão a folha de pagamento da MB. Finalmente, após aprovação do Ordenador de Despesas do OP, a folha de pagamento está liberada para ter efeito financeiro e sua respectiva contabilização.

Durante a fase de depuração, as parcelas são analisadas quanto ao atendimento de diversos parâmetros, entre eles, a verificação de valores individuais maiores que tetos predefinidos e a identificação de informação incompleta ou incorreta de parcelas ou dados bancários.

O trabalho do OP continua até o crédito em conta corrente de todo pessoal que tem relação e vínculo de remuneração com a MB e o recolhimento dos devidos tributos, repasses de consignações, de aluguéis residenciais, de benefício-família e de pensão alimentícia, entre outros. Para finalizar o processo, o OP faz a atualização de dados do Repositório Histórico que possibilita a geração de informações e relatórios necessários.

Finalmente, acabado o processamento em moeda nacional, as informações de pagamento em dólares americanos e euros são incluídas no processo, bloqueios de pagamento

são operacionalizados, os dados históricos são atualizados e são gerados os demais relatórios necessários.

O Pagamento de Pessoal da MB é intergrado por subprocessos, em número de 18 (dezoito), como segue:

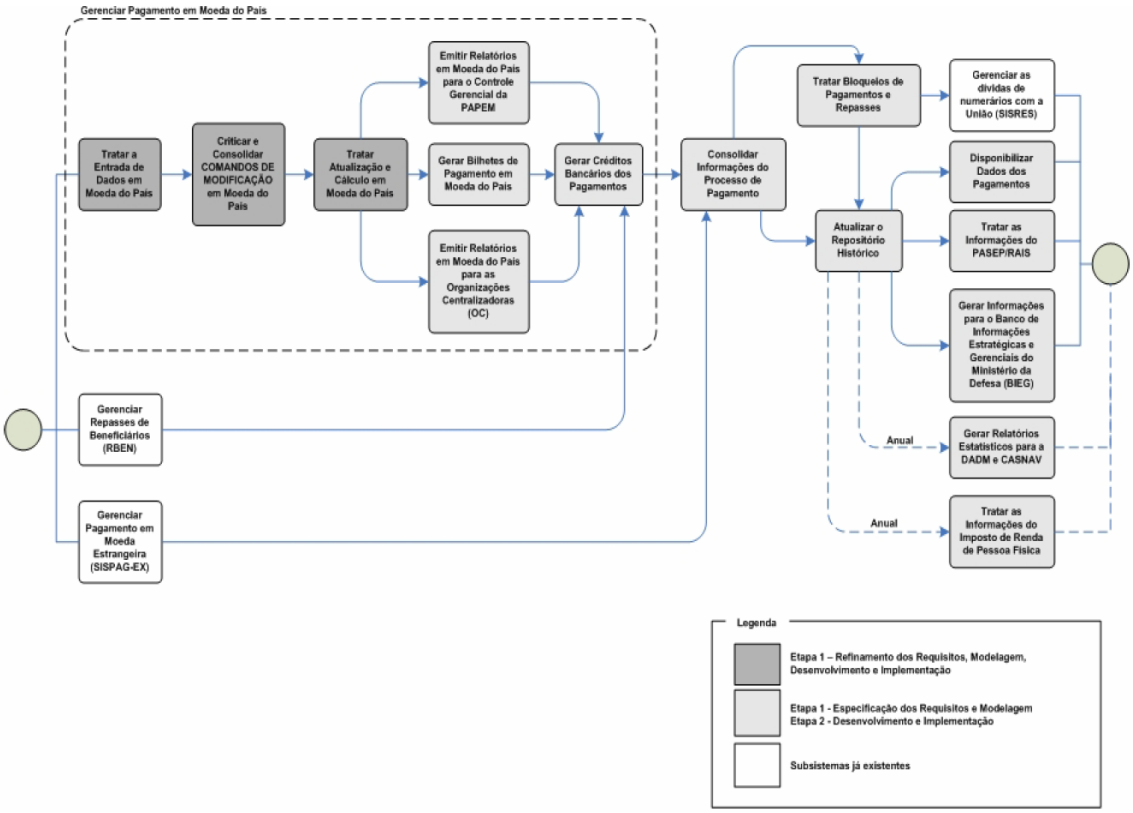

Figura 8: Processo de Pagamento de Pessoal da MB.
Fonte: Adendo A ao Anexo A de DFM (2009).

A partir da exposição do fluxo do processo de pagamento de pessoal, será abordado abaixo cada um dos subprocessos relacionados, conforme especificado em DFM (2009):

a) "Tratar a Entrada de Dados em Moeda do País": Nesse componente, as Organizações Centralizadoras (OC) e os Informantes Qualificados (IQ) comandam alterações de informações pessoais, funcionais e financeiras, relativas aos militares reformados, em reserva remunerada ou em serviço ativo no país e aos pensionistas militares e demais pessoas vinculadas à MB que aufiram remuneração em moeda nacional.

b) "Criticar e Consolidar Comandos de Modificação em Moeda do País": Esse subprocesso recebe os comandos gerados pelas OC, IQ e Sistemas Legados, os consolida e critica, organizando-os em lotes. Esse formato das informações em lotes permite a liberação gradual das informações para o cálculo da folha de pagamento.

c) “Tratar Atualização e Cálculo em Moeda do País”: Atualiza as informações e simultaneamente realiza o cálculo da remuneração das pessoas inscritas no sistema. Ressalta-se que o SISPAG emprega o conceito de processamento por “Grupo de Pagamento” cujo propósito é oferecer mais eficiência ao processo. À medida que um grupo é calculado, o mesmo está liberado para os subprocessos “Emitir Relatórios e Bilhetes de Pagamento” e “Informar Créditos Bancários dos Pagamentos”.

d) “Gerenciar Pagamento em Moeda Estrangeira (SISPAG-EX)”: Gerencia as remunerações de pessoas que estejam em comissão no exterior, por meio do subsistema SISPAG-EXTERIOR. Esse subsistema efetua as atividades referentes ao pagamento em moeda estrangeira, tais como atualização de informações (pessoais, funcionais e financeiras), gerenciamento de comissões no exterior, obtenção de remunerações bruta e líquida, produção de relatórios (como os de apropriação e de controle gerencial), geração de créditos bancários e emissão de Bilhete de Pagamento.

Os sistemas de pagamento em moeda nacional e em moeda estrangeira possuem algumas interações de controle, tais como: suspensão de parcelas de pagamento em moeda nacional das RR incluídas como em comissão no exterior; geração de parcelas de pagamento em moeda nacional para zerar o líquido da Relação de Remuneração; transporte das parcelas geradas em moeda nacional do subsistema do país para o subsistema do exterior, com a referente conversão de moedas e inversão de efeito financeiro; etc.

e) “Emitir Relatórios em Moeda do País para o Controle Gerencial da PAPEM”: Produz relatórios destinados a diversos setores da PAPEM, para que esses possam realizar a apropriação dos respectivos créditos orçamentários e a execução financeira referente à Folha de Pagamento, analisar a qualidade do processo e, eventualmente, bloquear créditos de pagamento. Esses relatórios serão utilizados, também, para auditorias e controle gerencial.

Dentre os relatórios produzidos, destacam-se: Mapa Bancário de RR de Servidores do País, Mapa Bancário de RR de Beneficiários, Planilha Bancária de RR País, Auditoria – Salários Brutos, Auditoria – Salários Líquidos, Auditoria – Duplicidade de Depósito Bancário, Apropriação da Folha de Pagamento, Apropriação das Parcelas de Pagamento, Estatística de Efetivo de Militar Ativo-Inativo-Pensionista, Responsabilidade a Regularizar, Auditoria do Processo Anual, Relatório de Consignantes, Multiplicidade de Conta-Corrente, Demonstrativo Financeiro por Parcela e por Natureza de Despesa, Relatório Gerencial para o Conselho Financeiro e Administrativo da Marinha.

f) “Emitir Relatórios em Moeda do País para as Organizações Centralizadoras (OC)”: Produz relatórios destinados às diversas OC, para que essas possam avaliar a qualidade do

processo e, eventualmente, comandar bloqueios de créditos de pagamento. As OC fazem uso desses relatórios, também, para a realização da Tomada de Contas, comprovação da correção do processo junto à Diretoria de Contas da Marinha e para o controle gerencial.

Dentre os relatórios encaminhados, destacam-se: Relatório Estado das Parcelas, Prestação de Contas, Relação dos Pagamentos Depositados, Relatórios de Diferenças, Demonstrativo Financeiro de Natureza de Despesa e Parcelas, Fichas Financeiras, Resumo Financeiro, Comprovante de Rendimentos (uma vez ao ano), Relatório de Servidores em Acerto de Contas e Relatório de Falecimento.

g) "Gerar Bilhetes de Pagamento em Moeda do País": Esse componente gera os Bilhetes de Pagamento que são remetidos, por serviço postal da MB, às OC que os redistribuem às pessoas de sua lotação e às organizações militares apoiadas pela OC para que todos recebam seus respectivos bilhetes.

Para os militares inativos, militares reformados e beneficiários, os Bilhetes de Pagamento podem ser enviados diretamente à residência, pelo serviço dos Correios, ou para o domicílio bancário. Essa mesma facilidade também é estendida para o Comprovante Anual de Rendimentos.

Esse subprocesso apenas gera o arquivo com as informações dos Bilhetes de Pagamento, sendo que a sua impressão é realizada por organização especializada (atualmente, uma empresa contratada). O arquivo apresenta as informações agrupadas de acordo com o destino (OC de lotação da pessoa, banco e agência de crédito da remuneração da pessoa ou residência da pessoa), dispondo cada grupo de critérios de ordenação específicos.

Para menores custos de impressão, as informações são organizadas de forma a disponibilizar a parte externa e a parte interna de dois Bilhetes de Pagamento, lado a lado, constituindo duas colunas. A ordenação criteriosa é iniciada primeiramente na coluna inteira da esquerda e sua continuação é realizada a partir do início da coluna da direita.

O Bilhete de Pagamento é constituído de duas seções destinadas a mensagens: uma externa e uma interna. A seção externa contém uma mensagem padrão para todos os Bilhetes de Pagamento. Já a seção interna contém mensagens específicas para cada situação funcional (militares da ativa, militares inativos e beneficiários). São permitidas, também, mensagens individualizadas relacionadas a uma ou mais situações funcionais ou matrículas financeiras. Uma rotina gerencia as informações, permitindo atualizações e o armazenamento do histórico das mensagens.

h) "Gerar Créditos Bancários dos Pagamentos": Cria arquivos e relatórios que serão transmitidos ou enviados aos bancos conveniados, bem como a geração de relatórios

sintéticos de controle encaminhados ao Departamento de Finanças da PAPEM, contendo as informações requeridas para os créditos de pagamento.

i) “Gerenciar Repasses de Beneficiários (RBEN)”: Componente que operacionaliza repasses relacionados a descontos efetuados nas remunerações de consignantes dos beneficiários de pensões alimentícias, aluguéis de imóveis e benefícios-família, creditando-os em conta-corrente.

Os descontos envolvem parcelas RR específicas e associadas ao respectivo consignante. Essas parcelas são comandadas por meio de rotinas predeterminadas, que buscam as informações necessárias nos repositórios do sistema RBEN.

j) “Consolidar Informações do Processo de Pagamento”: As informações de repasses de pensões alimentícias e as de remunerações em moeda nacional e estrangeira são armazenadas em um repositório de dados. Esse repositório é temporário e será empregado na atividade de Bloqueios de Pagamento e, posteriormente, na atualização do repositório histórico.

k) “Tratar Bloqueios de Pagamentos e Repasses”: Componente em que as OC e a PAPEM efetuam bloqueios de pagamentos e repasses de pensões alimentícias, ou seja, impossibilita depósitos bancários indevidos (erros na digitação de parcelas, falecimentos, deserções etc.) identificados após os subprocessos “Tratar Atualização e Cálculo em Moeda do País” e “Gerenciar Pagamento em Moeda Estrangeira”.

Os bloqueios podem ser de dois tipos, dependendo, basicamente, da época em que se torne necessário: nos de “tipo 1”, são enviadas comunicações aos bancos para que o depósito em conta-corrente não se concretize, enquanto nos de “tipo 2” são solicitados estornos dos depósitos já realizados. No primeiro caso, como ainda não foi realizada a transferência financeira, os valores envolvidos são deduzidos e não integram a Ordem Bancária comandada no SIAFI. O segundo caso é uma tentativa de reversão de depósito e, caso não logre sucesso, o valor do pagamento será registrado no Sistema de Responsabilidade (SISRES), no qual aguardará regularização.

l) “Atualizar o Repositório Histórico”: subprocesso que atualiza o registro histórico com o armazenamento das informações do último processo de pagamento. Com isso, é possível realizar consultas a dados históricos e o processamento de folhas de pagamento suplementares. No presente momento, estão mantidas armazenadas as informações de processos de pagamento dos últimos 10 exercícios, com previsão de agregação contínua dos exercícios subsequentes.

m) “Disponibilizar Dados dos Pagamentos”: possibilita que as OC e IQ consultem interativamente as informações do Repositório Histórico.

n) “Tratar as Informações do PASEP/RAIS”: o SISPAG dispõe de três módulos para o gerenciamento e geração de informações sociais. O primeiro, também chamado “PASEP”, objetiva cadastrar os militares no Programa de Formação do Patrimônio do Servidor Público (PASEP), através do envio de informações ao BB. O segundo, conhecido como “RAIS”, objetiva manter a Relação Anual de Informações Sociais (RAIS) dos militares para fornecimento anual ao Ministério do Trabalho e Emprego. O último, de modo semelhantemente conhecido como “FOPAG”, é o responsável pelo pagamento de abonos e rendimentos do PASEP aos que se enquadram nas normas específicas.

O PASEP é gerenciado pelo Banco do Brasil e possibilita vantagens como distribuição de rendimentos e abonos aos trabalhadores enquadrados em normas próprias do PASEP. Na condição de empregadora, a MB fornece anualmente ao Ministério do Trabalho e Emprego, por meio da RAIS, informações relacionadas à pessoa empregada durante qualquer período do ano-base.

o) “Tratar as Informações do Imposto de Renda de Pessoa Física”: Anualmente é gerado pelo SISPAG o arquivo de Declaração de Imposto de Renda Retido na Fonte (DIRF), que é encaminhado à Receita Federal no último dia do mês de janeiro. O Sistema também gera Comprovantes de Rendimentos, que são enviados às pessoas juntamente com o bilhete de pagamento do mês de fevereiro.

O Comprovante de Rendimentos é um resumo dos valores auferidos durante o ano fiscal. Já a DIRF é composta por um detalhamento mensal da remuneração da RR. Estarão incluídas na DIRF as pessoas que receberam rendimentos acima do limite divulgado pela Receita Federal e as que tiveram retenção de imposto no ano-base.

p) “Gerenciar as dívidas de numerários com a União (Sistema de Responsabilidade - SISRES)”: As relações de remuneração, que não lograram êxito na tentativa de bloqueio do tipo 2 de seu pagamento, são lançadas no SISRES que é, por sua vez, um sistema autônomo com o objetivo de permitir o gerenciamento das dívidas das pessoas com a União.

q) “Gerar Informações para o Banco de Informações Estratégicas e Gerenciais do Ministério da Defesa (BIEG)”: Mensalmente, a PAPEM encaminha ao Ministério da Defesa um arquivo com informações pessoais e funcionais (obtidas junto à Diretoria de Pessoal Militar da Marinha, Serviço de Inativos e Pensionistas da Marinha e Comando do Pessoal de Fuzileiros Navais) e informações financeiras (extraídas do SISPAG).

r) “Gerar Relatórios Estatísticos para a DAdM e CASNAV”: Anualmente ou por demanda específica, são elaborados relatórios estatísticos para a Diretoria de Administração da Marinha (DAdM) e o Centro de Análise de Sistemas Navais (CASNAV). Para o CASNAV é encaminhado o Relatório Estatístico sobre Salário-Contribuição. Para a DAdM são enviados relatórios que integrarão o Anuário Estatístico da Marinha, ou seja: Evolução Mensal das Despesas com Etapa de Desmuniciados; Evolução Mensal das Despesas com Auxílio-Transporte; Evolução Mensal das Despesas com Ajuda de Custo; Evolução Mensal das Despesas com Indenização de Transporte e Bagagem; e Evolução Mensal das Despesas com Pagamento de Pessoal Militar.

1.6.3 A modernização do Sistema de Pagamento de Pessoal

O avanço tecnológico das últimas décadas levou o processamento eletrônico da folha de pagamento da MB a uma inadiável necessidade de atualização. O sistema em uso, doravante, também, chamado de Sistema Legado, tem origem na década de sessenta e passou por diversas atualizações pontuais ao longo de sua vida útil, mas convive, ainda, com linguagens de computador com mais de 40 anos de existência.

Em virtude disso, foram iniciados, após alguns anos de debates entre os diversos setores envolvidos, serviços de Tecnologia da Informação (TI) para o desenvolvimento das atividades do projeto de modernização do Sistema de Pagamento de Pessoal da Marinha do Brasil, que foi denominado de SISPAG2. Entre outras características específicas, para o sistema em desenvolvimento se buscou um processamento *online*, baseado em tecnologia *Web*, com a utilização de um Banco de Dados único, com acesso de qualquer ponto interligado à intranet e com alguns recursos para acesso pela Internet. O tempo de processamento pretendido é quase que instantâneo, por não precisar de migração de dados. A crítica pretendida deve ser *online*, na entrada dos dados (ao invés de depuração do processo). As ações comandadas no sistema devem ter ação e efeitos imediatos. O sistema ainda terá um serviço de mensageiro, no estilo “Quadro de Avisos”, ou seja, quando alguém comandar uma determinada parcela predeterminada (como, por exemplo, uma ajuda de custo), será gerada uma mensagem para o Ordenador de Despesas e para outros agentes interessados previamente cadastrados no sistema.

De acordo com a norma NBR ISO 10006 da Associação Brasileira de Normas Técnicas (ABNT, 2000), projeto é um processo único de atividades coordenadas e controladas com datas de início e término, empreendido para um objetivo conforme requisitos específicos, contendo limitações de tempo, custo e recursos.

Face ao exposto, em 30 de outubro de 2009 foi assinado um contrato junto a uma empresa de TI para o desenvolvimento do projeto, em conjunto com equipe interna da MB, com prazo de término previsto para 29 de abril de 2013, dos quais os 12 (doze) últimos meses serão dedicados à Garantia e ao Suporte Técnico.

Para um adequado desenvolvimento do projeto e garantia dos interesses da instituição, a Pagadoria de Pessoal da Marinha (PAPEM) organizou uma equipe de TI, com dedicação exclusiva ao acompanhamento e fiscalização do projeto, composta pelos seguintes perfis técnicos: Gerente de Projeto; Analista de Requisitos; Analista de Sistemas; Arquiteto de "Software"; Administrador de Dados; Analista DBA (*Database Administrator)*; Analista de Testes; Programador; e *Web designer*. Essa equipe mantém acompanhamento das atividades em execução, interage com a equipe da empresa desenvolvedora, acompanha o cumprimento do cronograma do projeto e avalia a qualidade dos serviços e artefatos produzidos durante o projeto, promovendo a aceitação do serviço ou artefato ou, ainda, relatando os ajustes necessários.

O desenvolvimento de um sistema de pagamento *online* para a Marinha visa, segundo Quadra (2000, p. 65), melhorar o atendimento aos usuários envolvidos e evitar uma despesa excessiva com a manutenção de sistemas ultrapassados.

A modernização do respectivo sistema foi prevista para ocorrer em duas etapas distintas. Os subsistemas já existentes, "Gerenciar Pagamento em Moeda Estrangeira (SISPAG-EX)"; "Gerenciar Repasses de Beneficiários (RBEN)"; e "Gerenciar as dívidas de numerários com a União (SISRES)", passarão por atualizações e ajustes pela equipe de TI da PAPEM, conforme a demanda, não estando incluídos em nenhuma fase específica.

A etapa 2 inclui o desenvolvimento e implementação de subprocessos pela equipe de TI da PAPEM. Os subprocessos que, no processo em curso (etapa 1) estão passando por Refinamento de Requisitos e Modelagem, mas não pelo Desenvolvimento e Implementação, estarão incluídos na etapa subsequente.

O desenvolvimento de um produto e especialmente de um software deve atender a algumas metas, diretrizes e pontos pré-definidos, também conhecidos como requisitos. Eles podem ser subdivididos, segundo Dias e Menna (2008, p. 12), em dois tipos:

• Requisitos funcionais: são as funções que o software deve possuir para atender às necessidades do usuário.

• Requisitos de qualidade ou não funcionais: São características de *software* que descrevem o seu nível esperado de qualidade.

A atividade de levantamento de requisitos tem importância crucial para o sucesso de todo projeto e, além de ser fundamental ao desenvolvimento das próximas atividades, é condicionante à aceitação do sistema pelo usuário final. O objetivo dessa atividade é coletar as informações necessárias ao projeto de sistemas.

Para a primeira etapa da modernização, foram definidos 70 (setenta) requisitos funcionais a serem atendidos pelo novo sistema, conforme consta do Apêndice A. Foram elaborados, também, 30 (trinta) requisitos não funcionais que foram divididos em categorias de segurança, usabilidade, confiabilidade, desempenho, suportabilidade, design e implementação, conforme detalhado no Apêndice B e resumido no quadro abaixo:

REQUISITOS NÃO FUNCIONAIS			
Categoria	**Requisitos**	**Categoria**	**Requisitos**
Segurança	1. Confidencialidade	Desempenho	15. Tempo de resposta.
	2. Integridade.		16. Conexão com o SGBD.
	3. Controle de Acesso		17. Usuários simultâneos.
	4. Disponibilidade e Autenticação.		18. Tráfego de rede.
	5. Segurança lógica.		19. Consumo de banda de transmissão.
	6. Contingência ("*backup* e *restore*").	Suportabilidade	20. Padrões de modelagem.
	7. Auditoria.		21. Dicionarização.
	8. Gerenciamento da transmissão de arquivos.		22. Manual do aplicativo.
Usabilidade	9. Interface gráfica do usuário.		23. Manutenibilidade.
	10. Exibição de data e hora.		24. Registro e tratamento de exceções.
	11. Fácil uso.	Design	25. Ferramentas de Design.
	12. Ajuda.		26. Metodologia.
	13. Preenchimento automático.	Implementação	27. Plataforma cliente.
Confiabilidade	14. Controle de transações.		28. Arquitetura.
			29. Banco de dados.
			30. Licenças de software.

Quadro 5: Requisitos não funcionais do SISPAG2.
Fonte: Elaborado pelo autor com dados de DFM (2009).

Baseado nesses requisitos e demais especificações, a modernização do Sistema de Pagamento da Marinha foi iniciada. Os serviços previstos para a Etapa 1 do projeto incluem as tarefas abaixo, conforme DFM (2009):

a) Refinamento de requisitos, modelagem, implementação, testes, homologação e implantação de módulos automatizados: Captação de Dados (Mod-CD), Atualização de Dados (Mod-AD), Cálculo da Folha de Pagamento (Mod-CF) e Interface com o Sistema Legado (Mod-INLE), de acordo com as especificações dos requisitos, em alto nível;

b) Especificação de requisitos e modelagem de funcionalidades do sistema de pagamento em produção (Sistema Legado) não implementadas na Etapa 1;

c) Elaboração de base de dados a ser utilizada em todo o SISPAG2 e a migração dos dados, atualmente usados pelo Sistema Legado, para sua utilização pelos módulos automatizados em desenvolvimento;

d) Treinamento de usuários nos módulos automatizados resultantes;

e) Treinamento e transferência de tecnologias utilizadas no desenvolvimento do SISPAG2 para a equipe de TI da PAPEM; e

f) Garantia e Suporte Técnico.

Os serviços e atividades da etapa 1 foram divididos em quatro fases distintas, contemplando os seguintes artefatos e atividades:

a) Fase de Concepção: inclui o desenvolvimento das Regras de Negócio e Planos de Desenvolvimento de *Software*, Plano de Projeto, Plano de Implantação, entre outros;

b) Fase de Elaboração: Modelo de Dados, Entidade-Relacionamento e Dicionário de Dados etc.;

c) Fase de Construção: Migração de Dados para teste e Codificação dos Módulos, entre outros; e

d) Fase de Transição: Relatórios da Etapa 1 do SISPAG2, Manuais de Usuário e do Sistema em português, Treinamentos para usuários e técnicos da PAPEM, Etapa 1 do SISPAG2 operacional etc.

Ao término de cada Fase, a equipe de TI da PAPEM avalia a qualidade dos serviços e artefatos produzidos e emite termo de aceitação ou relatando as necessidades de ajuste dos mesmos. Periodicamente, também, são gerados relatórios internos pela equipe de TI da PAPEM, para dar ciência aos níveis estratégicos da MB.

> A *revisão e aprovação* devem ser elaboradas em todas as passagens das fases, considerando: revisão da(s) fase(s) imediatamente anterior(es); apresentação dos produtos à gestão da organização, ao patrocinador, aos gestores, aos clientes ou usuários; deferimento formal dos envolvidos. (RESENDE, 2005, p. 126, grifo do autor).

A Etapa 1 é integrada por diversos elementos (figura 9), dentre os quais merecem destaque os seguintes componentes principais:

a) Módulos:

- Módulo de Captação de Dados (Mod-CD), composto de um aplicativo principal destinado a coletar comandos on-line e em lote, e de dois aplicativos auxiliares “Portal Upload” usado para coletar dados encaminhados remotamente para o SISPAG e “Digitação

em Situação de Contingência", o qual possibilita a digitação de comandos de atualização de dados de pagamento, em situações de indisponibilidade da interface *on-line* do Mod-CD;

- "Módulo de Atualização de Dados" (Mod-AD);

- "Módulo de Cálculo da Folha Mensal de Pagamento" (Mod-CF); e

- "Módulo Interface com o Sistema Legado" (Mod-INLE).

b) "Repositórios do SISPAG2" para o armazenamento de dados permanentes; e

c) Arquivos temporários para: (i) armazenamento de parcelas comandadas nas interfaces *on-line* e lote, denominado "Dados Coletados"; e (ii) comunicação com o sistema legado.

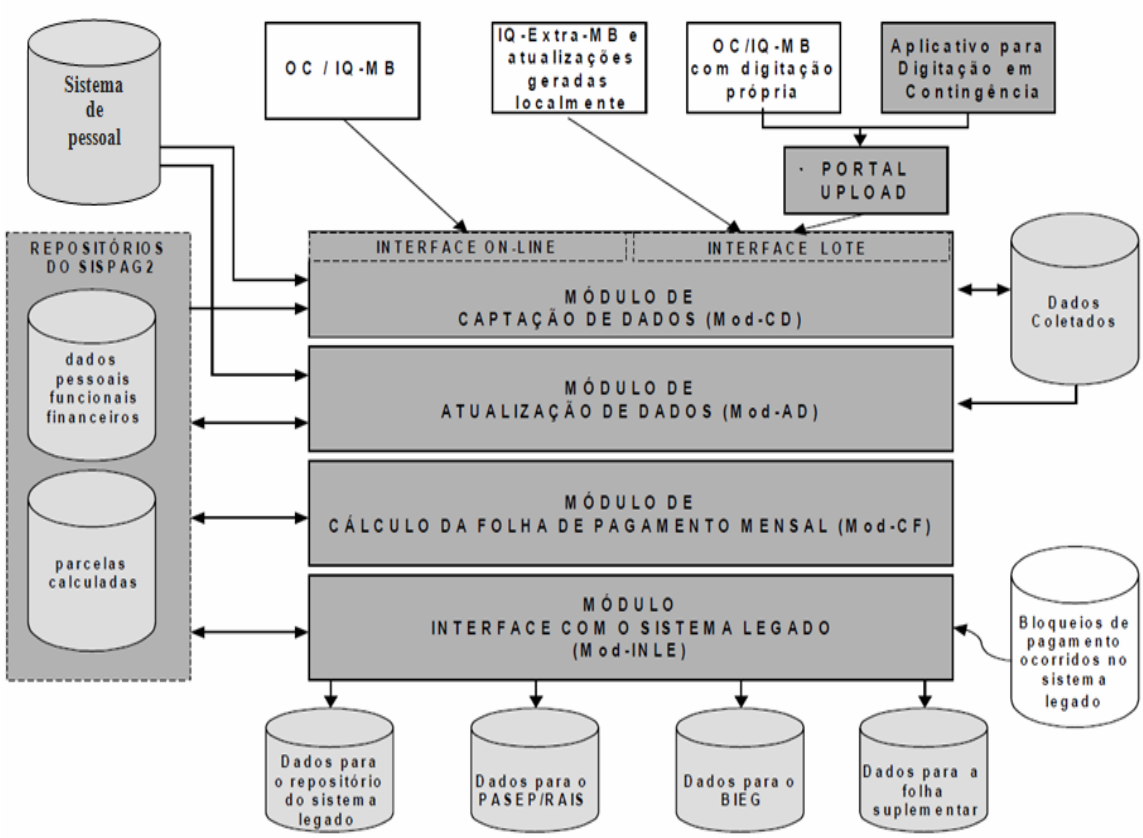

Figura 9: Representação esquemática de Etapa 1.
Fonte: Adaptado do Adendo B do Anexo A de DFM (2009).

Cada um dos Módulos representados possui as seguintes características gerais, conforme DFM (2009):

- Módulo de Captação de Dados (Mod-CD): interage com diversas fontes de alimentação do sistema, se destacando três delas: o sistema de pessoal, para consulta e captura de dados pessoais e de relações de remuneração; os Repositórios do SISPAG2, para consultas; e o arquivo "Dado Coletado", para armazenamento das atualizações de dados de pagamento,

conforme forem sendo captados e criticados. O sistema de pessoal pretendido como base de dados no projeto original da modernização era o Banco de Dados Integrador (BDI) da Diretoria de Pessoal Militar da Marinha que, por problemas técnicos, foi abandonado durante o desenvolvimento do SISPAG2, sendo mantida, até o momento, apenas uma validação de matrícula interna e nome do militar cadastrado no sistema de pagamento junto aos dados do DBI. A integração com a base de dados de pessoal atualmente em curso é com o Sistema de Inativos e Pensionistas da Marinha (SIPEM), de modo a se atualizar todos os dados referentes a esses usuários.

Esse módulo possui duas interfaces principais, que interagem com as OC e IQ e demais setores que produzem dados para o processo de pagamento:

a) Interface *on-line*: é o canal preferencial para se promover as atualizações de pagamento por todas as OC e IQ-MB com acesso à intranet da MB.

b) Interface lote: canal destinado aos OC e IQ sem acesso ou com indisponibilidade de acesso à intranet da MB. As OC e IQ-MB de interface *on-line* indisponível farão uso do "Aplicativo para Digitação em Contingência" para efetuar a atualização de dados financeiros no "Portal Upload". Os OC e IQ-MB que utilizam sistemas próprios para digitação de comandos de atualização de dados de pagamento deverão encaminhar seus dados, também via "Portal Upload".

- Módulo de Atualização de Dados (Mod-AD): responsável pela atualização mensal do repositório de dados do SISPAG2 de acordo com os dados disponibilizados pelo sistema de pessoal e, no fim da captação de dados referente à folha de pagamento de pessoal, usando os dados do arquivo "Dados Coletados". A funcionalidade de simulação, presente nesse módulo, possibilita a identificação e correção de inconsistências antes da atualização final do repositório de dados do SISPAG2.

- Módulo de Cálculo da Folha de Pagamento Mensal (Mod-CF): responsável pelo cálculo mensal do pagamento das RR e pelo respectivo registro no repositório de parcelas calculadas do SISPAG2. A funcionalidade de simulação, presente nesse módulo, possibilita a identificação e correção de inconsistências antes do cálculo final da Folha de Pagamento.

- Módulo Interface com o Sistema Legado (Mod-INLE): componente que estará ativo até a conclusão da Etapa 2 da modernização do sistema, sendo responsável pela geração dos arquivos abaixo, com conteúdo extraído dos repositórios do SISPAG2:

a) Arquivos com periodicidade mensal, compostos, cada um, de dados pessoais, funcionais e financeiros destinados ao: (i) repositório do Sistema Legado; (ii) módulo PASEP

do Sistema Legado; e (iii) módulo Relacionamento com o Ministério da Defesa do Sistema Legado; e

b) Arquivos produzidos por demanda específica, compostos de dados pessoais, funcionais e financeiros e destinados ao módulo de Produção de Folha Suplementar do Sistema Legado.

Depois do processamento dos bloqueios de pagamento, executado no Sistema Legado, o Mod-INLE é, ainda, encarregado de promover a correção do repositório de parcelas calculadas, anulando os registros de pagamento das RR bloqueadas naquela operação.

Além de todas essas interações o Mod-CD terá, também, uma funcionalidade de preparação de Ordens de Serviço, para utilização pelas unidades militares e com capacidade de promover a automação das atividades de geração de comandos e de atualização de dados de pagamento. O Mod-CD, também, terá a seu dispor um aplicativo auxiliar designado "Conversor de Comandos de Pagamento", a ser usado apenas na fase de implantação gradativa da Etapa 1, para tratamento a comandos de pagamento gerados no Sistema Legado e que precisem atingir RR lotadas em OC já implantadas na Etapa 1, ou vice-versa.

A verificação do CPF junto à Receita Federal que, inicialmente, estava prevista para ser viabilizada na etapa 1 do SISPAG, foi abandonada no decorrer do projeto por problemas técnicos. Assim, essa importante chave para integração com outros sistemas de organizações públicas e privadas continuará sem uma eficiente validação. Ressalta-se a importância de viabilização dessa validação como primeiro passo para integração com outros sistemas de interesse.

2 METODOLOGIA

Esta seção aborda o método utilizado para a produção do conhecimento científico, bem como as formas de levantamento dos dados e as ferramentas empregadas para análise e apresentação dos mesmos.

2.1 Organização metodológica

Collis e Hussey (2005, p. 61) alertam que alguns autores usam as palavras metodologia e método alternadamente, sem distinção, e que, no entanto, eles preferem distingui-los como segue: "Metodologia refere-se à maneira global de tratar o processo de pesquisa, da base teórica até a coleta e análise de dados. [...] Métodos, por outro lado, referem-se apenas às várias maneiras de coletar e/ou analisar dados". Portanto, é importante se considerar que as terminologias devam ser entendidas dentro de seu respectivo contexto.

Ao se tratar a metodologia, um entendimento do que pode ser considerado como uma pesquisa parece essencial. "Pode-se definir pesquisa como o processo que tem por finalidade descobrir respostas para os problemas mediante a utilização de procedimentos científicos. A pesquisa constitui o processo de operacionalização do método científico" (GIL, 2000, p. 44).

O estudo científico exige um delineamento do método (ou conjunto de métodos) que será utilizado para resolver determinado problema de pesquisa. Nesse sentido, Kerlinger (1980, p. 1) considera que "A ciência se desenvolveu, em parte, pela necessidade de um método de conhecimento e compreensão mais seguro e digno de confiança do que os métodos relativamente desprovidos de controle geralmente usados".

> O conhecimento científico surge da necessidade de o homem não assumir uma posição meramente positiva, de testemunha dos fenômenos, sem poder de ação ou controle dos mesmos. Cabe ao homem, otimizando o uso da sua racionalidade, propor uma forma sistemática, metódica e crítica da sua função de desenvolver o mundo, compreendê-lo, explicá-lo e dominá-lo. (Köche, 1997, p. 29)

Portanto, para se desenvolver o estudo científico é indispensável o emprego de uma metodologia adequada. Um ponto significante a se esclarecer é a compreensão do que é um método.

> Etimologicamente, método significa *caminho para se chegar a um fim*. Assim, método científico pode ser entendido como "o caminho para se chegar à verdade em ciência" ou como

> "o conjunto de procedimentos que ordenam o pensamento e esclarecem acerca dos meios adequados para se chegar ao conhecimento ["]. (GIL, 2000, p. 31, grifo do original).

O método de estudo da presente pesquisa é o estudo de caso. Yin (2010, p. 32) ensina que: "O estudo de caso é preferido para eventos contemporâneos, mas quando os comportamentos relevantes não podem ser manipulados". Para Collis e Hussey (2005, p.73), um estudo de caso implica uma análise de uma única unidade, como uma organização, um grupo de funcionários, um evento, um processo ou até mesmo um indivíduo.

> O estudo de caso é uma investigação empírica que
> · investiga um fenômeno contemporâneo em profundidade e em seu contexto de vida real, especialmente quando
> · os limites entre o fenômeno e o contexto não são claramente evidentes. (YIN, 2010, p. 39).

A escolha pelo estudo de caso atendeu, entre outras demandas, a uma necessidade de maior flexibilidade para o estudo de processos relacionados a um sistema informatizado, o que não quer dizer que houve falta de rigor metodológico. Como ensina Yin (2010, p. 87): "O ponto é que a flexibilidade necessária não deve diminuir o rigor com que procedimentos de estudo de caso são observados".

A presente pesquisa, por estar direcionada à análise de um único sistema, pode ser dita como um estudo de caso único. Yin (2010, p. 51) exemplifica que: "Os estudos de caso têm sido realizados sobre decisões, programas, processo de implementação e mudança organizacional".

A investigação de um estudo de caso utiliza, segundo Yin (2010, p.40), múltiplas fontes de evidência. Nesse sentido, as fontes de evidências utilizadas foram bibliográfica, documental, observação direta e realização de entrevistas semiestruturadas. As evidências bibliográficas e documentais foram levantadas mediante consultas a livros, revistas, artigos, trabalhos acadêmicos, legislações, normas, manuais, documentos, arquivos magnéticos e Internet. A observação direta foi realizada mediante visitas à organização que detém a estrutura de processamento eletrônico do referido sistema de pagamento de pessoal. As entrevistas foram realizadas com os principais agentes envolvidos no processo estudado.

No roteiro de entrevista, foram incluídas perguntas para serem respondidas de acordo com o grau de concordância ou discordância com cada proposição. Dessa forma, se organizaram os graus propostos em uma escala de Likert. Para Malhotra (2006, p. 266), essa escala de mensuração possui cinco categorias de respostas, variando de "discordo totalmente" a "concordo totalmente" e exige que os entrevistados indiquem um grau de concordância ou discordância com cada uma dos objetos de estímulo.

O roteiro de entrevista foi debatido com profissionais das áreas de controle e de TI que trabalham no apoio a sistemas de controle de outros órgãos públicos para se eliminar pontos

desnecessários e se incluir pontos necessários a uma melhor avaliação do sistema em estudo, antes que as entrevistas fossem realizadas. Ressalta-se que tal procedimento promoveu um refinamento no roteiro, que foi fundamental ao sucesso da presente pesquisa.

Para se alcançar os resultados da pesquisa, buscou-se contato com os profissionais que pudessem responder pelo sistema de pagamento estudado e que detivessem conhecimento das funcionalidades de controle presentes nesse mesmo sistema.

Inicialmente, pretendia-se obter dados junto a mais de dez componentes da equipe de modernização do sistema o que foi abandonado, após a entrevista com o responsável pela gerência do projeto, em virtude do grau de conhecimento exigido pelos questionamentos. Dessa forma, em virtude do nível de conhecimento demandado pelos roteiros de entrevista (Apêndices C e D), foram realizadas entrevistas com o gerente do projeto de modernização do sistema de pagamento da MB e mais cinco pessoas de sua equipe. Os dados coletados foram tabulados e trabalhados no Microsoft Office Excel 2007 para se chegar aos resultados apresentados.

Para se chegar aos resultados da pesquisa, foi feita uma análise e interpretação qualitativa dos dados obtidos. Assim, este estudo também é uma pesquisa qualitativa, que usa uma metodologia de pesquisa "[...] baseada em pequenas amostras que proporciona percepções e compreensão do contexto do problema" (MALHOTRA, 2006, p. 155).

Uma das limitações do estudo pode ser o fato de a modernização do sistema de pagamento de pessoal estudado estar em curso durante toda a fase de elaboração da presente pesquisa. Em virtude de atraso em relação à conclusão do projeto de modernização do referido sistema de informações, até mesmo a abordagem desse estudo teve de ser feita de maneira mais indireta do que o pretendido inicialmente. Dentro desse contexto, muitos testes, análises e avaliações sobre o novo sistema foram impossibilitados e novas formas de abordagem foram definidas para conduzir a um resultado satisfatório. Nesse aspecto, a flexibilidade, característica do estudo de caso, muito contribuiu para o sucesso dessa pesquisa.

Outra limitação do estudo refere-se aos dados terem sido obtidos a partir de uma amostra por conveniência, logo sem o uso de regras estatísticas para seleção. A reduzida quantidade de dados e sua necessidade de entendimento dentro do contexto específico levam ao problema da generalização dos resultados para outras realidades.

A coleta de dados por entrevista também apresenta várias limitações intrínsecas, que precisaram ser superadas ou minimizadas durante sua realização. Dentre essas, destacam-se, conforme Marconi e Lakatos (1990, p. 86), as referentes à disposição do entrevistado em dar

as informações necessárias, a retenção de alguns dados importantes e o pouco controle sobre a situação de coleta de dados.

A presente pesquisa foi organizada em cinco etapas como sugerido por Gil (2000, p. 46). A primeira etapa foi destinada à apresentação do problema de pesquisa e objetivos. Na segunda etapa foi exposto o arcabouço teórico do estudo. Na terceira, foi efetuado um delineamento em que foram definidas as atividades a serem desenvolvidas no processo de pesquisa. Na quarta etapa, procedeu-se à análise e interpretação dos dados. Por fim, para se divulgar os resultados do estudo, foi redigido o relatório definitivo.

3 ANÁLISE DO SISTEMA DE PAGAMENTO DE PESSOAL DA MB

Esta seção apresenta a análise do ambiente organizacional, a análise dos dados obtidos das entrevistas realizadas e a análise geral do Sistema de Pagamento de Pessoal da Marinha do Brasil.

3.1 Análise do ambiente organizacional

Com base no que foi apresentado sobre a literatura e sobre o Sistema de Pagamento da Marinha (em modernização), será efetuada uma análise entre esses dois conjuntos e apresentados os resultados obtidos.

A possibilidade de aumento continuado com as despesas de pessoal da Administração Pública, em decorrência das maiores expectativas de vida da população, impacta diretamente na importância dos controles sobre esses gastos. Dessa maneira, maiores esforços e investimentos devem ser aplicados para atualização dos sistemas de controle existentes. Pode-se dizer que a modernização do Sistema de Pagamento da Marinha do Brasil está em sintonia com essa tendência.

O SISPAG, concebido na década de 1960, foi desenvolvido em um modelo tecnológico que marcou a era de informatização das grandes corporações. Com o passar do tempo, várias funcionalidades foram sendo agregadas ao programa, mas mantendo o padrão tecnológico original, composto basicamente por uma plataforma baseada em computador de grande porte (mainframe) e pelo uso de uma metodologia de engenharia de software utilizada nos primeiros projetos de sistemas. Como resultado dessa estrutura, custos elevados de manutenção de uma tecnologia totalmente ultrapassada pressionavam a administração naval por uma solução que atendesse as necessidades do negócio.

Dentre as diversas carências apontadas pelos usuários no sistema em uso, destacam-se as seguintes: baixa qualidade das informações digitadas, uma vez que o sistema não possui uma crítica na entrada de dados; período relativamente longo (cerca de um mês) entre a digitação e seu efeito financeiro; inexistência de relatórios gerenciais e de controle interno para monitoramento da atividade de digitação; e incapacidade do sistema em relatar as inconsistências que provocaram rejeições de parcelas comandadas.

Para atender essas demandas e operacionalizar uma gestão estratégica do pagamento de pessoal, foi desenvolvido um estudo técnico para considerar as diferentes opções frente à necessidade de modernização, levando a três cenários alternativos ao apresentado nesse estudo. O primeiro, de manutenção do atual sistema, foi considerado oneroso, milhões de reais por ano, e inaceitável, em virtude de grande risco de colapso do sistema em um período de médio ao longo prazo. O segundo cenário, de modernização de forma autônoma, foi, também, considerado inaceitável, em virtude dos riscos decorrentes da grande probabilidade de construção de ambiente tecnológico inadequado e da limitação dos recursos humanos. O terceiro cenário, de contratação de uma consultoria e utilização do pessoal de TI da PAPEM, foi considerado de limitada exequibilidade, em virtude dos riscos de atraso do projeto e de indesejável subordinação à empresa consultora.

A estratégia aplicada na modernização foi uma substituição gradual dos módulos do SISPAG atual, uma vez que a complexidade e a missão crítica do sistema inviabilizam sua especificação, construção e implementação em uma única etapa.

A opção para o desenvolvimento do novo software foi a de se utilizar um padrão aberto para atender ao requisito de portabilidade e facilitar a padronização com outros sistemas corporativos.

Os benefícios pretendidos com a modernização do sistema são muitos e, dentre os quais, destacam-se os seguintes:

- ✓ aumento da qualidade das alterações de pagamento;
- ✓ possibilidade de correção de dados inconsistentes durante a digitação;
- ✓ adoção de medidas de efetivo controle interno;
- ✓ ampliação da data-limite para digitação; e
- ✓ integração com as bases de dados dos sistemas de gestão de pessoal.

Para análise de um sistema informatizado, torna-se importante que se compreenda os diversos aspectos envolvidos, que basicamente podem ser divididos em três grupos: físicos, lógicos e humanos. Nesse sentido, destaca-se um agrupamento desses aspectos, por camadas, feito por Netto e Silveira (2007, p. 379-380), como segue:

- ➢ Camada Física: ambiente em que está instalado fisicamente o hardware, podendo ser o escritório, a fábrica, a residência do usuário etc.
- ➢ Camada Lógica: caracterizada pelo uso de softwares responsáveis pela funcionalidade do hardware, por transações em base de dados organizacionais, criptografia de senhas e mensagens etc.

- Camada Humana: todos os recursos humanos presentes na organização, principalmente os que possuem acesso aos recursos de TI, seja para manutenção ou uso.

Dentro desse contexto, pode-se dizer que existem dois ambientes de controle no SISPAG2. O primeiro, referente ao ambiente web no qual estará inserido. O segundo, o ambiente organizacional em que os usuários efetuam as entradas de dados e se utilizam de relatórios e informações originadas do sistema.

No ambiente Web, relacionado com a camada lógica, entre os vários riscos envolvidos e medidas de gerenciamento aplicadas pelo sistema, se destacam dois: risco de invasão, que pode ser mitigado pela utilização de sistemas de segurança, como por exemplo um firewall, e risco de intercepção de dados, que deve ser mitigado por meio da criptografia dos dados enviados pela fonte.

O ambiente organizacional, relacionado com as camadas física e humana, está estruturado de acordo com princípios e tradições militares, baseados na hierarquia e disciplina. Um código de conduta está formalmente estabelecido e quaisquer desvios disciplinares ou de conduta são apurados, julgados e, quando justificados, punidos à luz dos instrumentos legais, regulamentos e normas vigentes. As divulgações das normas de conduta são feitas, entre outras formas, em páginas da intranet das Diretorias de Pessoal (civil e militar), em treinamentos e em cursos de formação e atualização ministrados. Há, ainda, uma cópia impressa na organização para consulta. A mentalidade de conduta ética é, ainda, reforçada algumas vezes, pela divulgação dentro de cada unidade por meio de um informativo diário de trechos dos referidos instrumentos orientadores.

As faltas e atrasos de pessoal, em virtude das características da atividade militar, não são registrados para fins de descontos em folha. Por isso, os sistemas de controle de ponto não são aplicados, optando-se por outros tipos de controles. Os indivíduos que incorrerem em tais situações estão sujeitos a responder apurações disciplinares ou penais, dependendo da caracterização das ocorrências, conforme leis e regulamentos específicos.

A organização considera, ainda, que a cultura de segurança das informações digitais deva sensibilizar e conscientizar os integrantes da organização para a importância do cumprimento das instruções de segurança digital, assegurando uma maior confiabilidade no trabalho realizado.

O ambiente organizacional do respectivo sistema pode, ainda, ser subdividido em dois microambientes:

- de sistema, em que estão alocados os servidores da área de TI e que cuidam da manutenção, atualização e funcionamento de programas e aplicativos; e

- de usuário, em que estão militares e civis de diversas especialidades existentes na Marinha. Desta forma, existem administradores, contadores, economistas, estatísticos e outros operando direta ou indiretamente o referido sistema. Esse ambiente de ampla diversidade acadêmica impõe um desafio ao sistema: ser de fácil entendimento e operação para um usuário de formação diversificada e com pouca ou nenhuma experiência na manipulação de sistemas informatizados (apesar de alguns operadores terem muitos anos de experiência) e na área de pagamento.

Para a equipe de TI, a capacitação no novo sistema é feita por meio de treinamentos quinzenais com os desenvolvedores, após os quais são feitas avaliações para atestar até que grau os conhecimentos foram adquiridos. Na conclusão de cada atividade, é apresentado um plano de treinamentos e *mentoring* a ser seguido. Não foi possível a verificação de documentos que atestassem a realização de tais orientações.

O manual do sistema se constitui em uma das principais ferramentas para que a equipe de TI da PAPEM possa estar apta às atividades inerentes pelas quais será responsável. Esse deve, ainda, estar concluído e revisado antes da disponibilização do sistema aos usuários finais.

Para as OC e IQ da MB, os treinamentos serão realizados por ocasião da implantação dos módulos da etapa 1 do novo sistema, em turmas para até 20 (vinte) usuários, dependendo da capacidade de cada local de realização. Devem ser aproveitadas essas oportunidades para o aumento da mentalidade de segurança dos usuários, fortalecendo assim o controle interno do processo de pagamento.

O manual do usuário deve definir cada uma das funções, preferencialmente, identificando as telas de trabalho por meio de ilustrações e exemplos de casos de uso. O tutorial do sistema deve estar devidamente explicado em um dos capítulos do referido documento.

Os erros mais comuns no processo de pagamento são disponibilizados na página da intranet da PAPEM para consulta pelos interessados.

A definição de responsabilidades, bem como a segregação de funções, está definida no Regimento interno e especificada mais detalhadamente nas ordens internas da PAPEM.

O Centro de Dados da Diretoria de Finanças da Marinha (DFM) fornece à PAPEM os serviços de hospedagem de servidores, armazenagem de dados, cópias de segurança (backups), solução de contingência, arquivamento e guarda de mídias magnéticas e relatórios

gerados pelo Sistema de Pagamento de Pessoal da Marinha (SISPAG). Por estar localizado em uma ilha, ao nível do mar e a menos de quinhentos metros de um cais, o risco de incidentes naturais virem a afetar o processamento da folha de pagamento parece iminente e está gerenciado através de ferramentas de *restore* e backup dos dados do sistema de pagamento, sendo o conjunto de arquivos para tal procedimento guardado em local diferente do referido centro de dados. Os riscos referentes à segurança lógica do sistema por perda de dados referentes a picos de luz ou quedas de raios estão gerenciados pela instalação e manutenção periódica de equipamentos, como pára-raios, geradores e *no-breaks*.

Um ponto de controle que fortalece principalmente a *accountability* ligada às atividades de pagamento de pessoal é a existência de um Conselho Administrativo-Econômico, integrado pelos principais agentes da organização, que possui, entre outras atribuições, as de verificação das contas de pagamento de pessoal (país e exterior), os registros contábeis dos atos e fatos da gestão orçamentária financeira e patrimonial, inerentes ao sistema de pagamento de pessoal (país e exterior), bem como verificar a produtividade dos diversos setores envolvidos. O conselho, ainda, analisa os Demonstrativos de Pagamento de Pessoal antes de serem encaminhados à Diretoria de Finanças da Marinha, para composição do Processo de Tomadas de Contas Anual. As reuniões dos respectivos membros ocorrem duas vezes ao mês ou quando convocados extraordinariamente pelo presidente. Os responsáveis pelas verificações das contas possuem roteiros de verificação em que estão especificadas algumas trilhas de auditoria para orientar a análise. Acredita-se, no entanto, que o número de trilhas de auditorias possa ser trabalhado e ampliado de forma a se instituir maior controle sobre o processo.

Todos os relatórios gerados, assim como todos os BP impressos por firma terceirizada, após a entrega na PAPEM, são armazenados em armários devidamente fechados, a fim de resguardar as informações.

O acesso à divisão de processamento de dados é permitido somente a pessoal com credenciais de segurança adequadas. Após o expediente, a chave é entregue lacrada por funcionário do respectivo setor ao pessoal de serviço e somente pode ser retirada por pessoa previamente autorizada no início do expediente do próximo dia útil.

Para facilitar a informação e comunicação, a disposição física da equipe da empresa desenvolvedora está ao lado da equipe da PAPEM, o que pode ser considerado um aspecto importante para uma adequada interação entre todos os envolvidos na modernização do sistema, facilitando o desenvolvimento de funcionalidades de acordo com a visão do cliente.

Entre os aspectos de monitoramento, o processo de crítica instantânea dos comandos de pagamento inseridos no SISPAG2 representa uma evolução para o pagamento da MB, uma vez que o Sistema Legado utiliza o conceito de processamento de críticas ou depuração. Nesse ponto, o novo sistema está sendo desenvolvido para um maior controle concomitante das transações, em substituição dos controles subsequentes atualmente utilizados.

No decorrer do processo mensal, o SISPAG2 interage com o sistema de pessoal para consulta e captura de dados pessoais e de RR. Serão apenas consideradas pelo sistema as parcelas direcionadas a pessoas previamente cadastradas no banco de dados de pessoal, com exceção dos dois casos abaixo:

- pagamentos eventuais por motivos diversos, pela "interface on-line": motivados por eventualidades como determinações judiciais são realizados através de inclusão única, dependente de análise e liberação do Gerente das Atividades de Controle Interno.
- pagamentos de auxílio-funeral, pela "interface on-line": efetuados nas situações de falecimento de dependente, militar ou beneficiário, dependendo, também, de análise e liberação do Gerente das Atividades de Controle Interno.

Diversas ferramentas de controle (tabelas, cronogramas, controles orçamentários, quadro de áreas de responsabilidade etc.) foram elaboradas para permitir o acompanhamento adequado do projeto de modernização do sistema.

3.2 Análise das entrevistas

Para se identificar pontos a gerenciar e pontos a explorar, foram realizadas entrevistas com os principais agentes envolvidos no processo de modernização do sistema de processamento da folha de pagamento. Por se tratar de uma modernização em módulos de um sistema já existente, apesar de envolver a recodificação para uma nova linguagem, pode se dizer que o sistema atual é um referencial para que seja possível uma alcançar um controle interno adequado para o sistema modernizado.

Primeiramente, será realizada uma avaliação por categoria e, depois, uma avaliação mais geral.

3.2.1 Categoria segurança

A categoria ligada à segurança pode ser considerada uma das mais importantes em qualquer sistema. A segurança da informação representa a proteção sobre esse ativo cada vez mais importante que é a informação. Netto e Silveira (2007, p. 377) destacam três dos principais requisitos dessa categoria:

- Confidencialidade - "[...] é a garantia de que somente pessoas autorizadas terão acesso a ela, protegendo-a de acordo com o grau de sigilo do se conteúdo" (NETTO E SILVEIRA, 2007, p. 377);
- Integridade - assegura que a informação manipulada conserva todas as propriedades originais estabelecidas pelo proprietário da informação, incluindo, entre essas, o controle de mudanças e a garantia de seu ciclo de vida (nascimento, manutenção e destruição) (DFM, 2009).
- Disponibilidade - assegura que as informações estejam sempre disponíveis para os usuários autorizados.

O controle de acesso ao sistema é um ponto fundamental dentro de uma adequada segurança física ou lógica. Ele se constitui de um conjunto de ferramentas para que somente pessoas autorizadas acessem o sistema. As barreiras físicas se constituem em limitação de trânsito em áreas sensíveis, cadeados (não lógicos), trancas, detectores de metal, paredes, muros etc. A segurança lógica envolve o uso de senhas, certificações digitais etc. Em se tratando de um sistema informatizado, deve-se trabalhar, entre outros, com autenticação (quem pode), autorização (o que pode) e auditoria (como fez). Em um ambiente *online*, como pretendido pelo SISPAG2, torna-se, ainda, importante a utilização de um protocolo com certificação digital do tipo HTTPS − *Hypertext Transfer Protocol Secure* (Nottingham; Hammer-Lahav, 2010). Esse procedimento efetua o tráfego de dados através de uma conexão criptografada e certifica a autenticidade de cada componente da rede, busca assegurar que a informação transmitida na rede não seja visualizada por terceiros, ainda que seja interceptada.

No caso específico do órgão pagador (PAPEM), por ocasião do ingresso de todos os militares e civis (servidores, estagiários, contratados etc.), são previstos treinamentos sobre os serviços de informática prestados, contemplando principalmente o assunto de segurança. O treinamento visa apresentar aos novos usuários a importância e a necessidade de comprometimento dos usuários de recursos computacionais com a efetiva segurança dos ambientes de redes de computadores na MB.

Para avaliar essa importante categoria, questões foram formuladas e geraram o quadro abaixo:

SEGURANÇA ATUAL		
Pergunta	MÉDIA	DESVPAD
P.1.1	5,00000	0,00000
P.1.2	4,00000	0,00000
P.1.3	4,00000	0,70711
P.1.4	3,40000	0,89443
P.1.5	4,00000	0,70711
P.1.6	4,00000	1,41421
P.1.7	2,80000	1,30384
P.1.8	3,00000	1,00000
P.1.9	1,20000	0,44721
P.1.10	3,00000	1,22474
P.1.11	1,80000	1,30384
P.1.12	2,80000	0,83666
P.1.13	2,20000	1,09545
P.1.14	3,00000	0,00000
P.1.15	3,20000	0,83666
Média Geral	3,16000	

SEGURANÇA DO SISPAG2		
Questão	MÉDIA	DESVPAD
Q.1.1	5,00000	0,00000
Q.1.2	4,83333	0,40825
Q.1.3	4,83333	0,40825
Q.1.4	4,33333	1,63299
Q.1.5	4,83333	0,40825
Q.1.6	4,83333	0,40825
Q.1.7	4,16667	0,98319
Q.1.8	4,50000	0,54772
Q.1.9	4,16667	1,60208
Q.1.10	4,16667	0,98319
Q.1.11	4,83333	0,40825
Q.1.12	5,00000	0,00000
Q.1.13	5,00000	0,00000
Q.1.14	4,83333	0,40825
Q.1.15	4,50000	1,22474
Média Geral	4,65556	

Quadro 6: Resultados para categoria segurança.
Fonte: O autor.

Ao início da avaliação, buscou-se verificar se o aspecto de autenticação restringe o acesso ao sistema somente a pessoas autorizadas. A autenticação está amplamente relacionada à responsabilização e, dessa forma, garantir uma perfeita autenticação é garantir que as responsabilidades dentro do sistema possam ser atribuídas de acordo com o que foi estabelecido. Pode-se dizer que uma perfeita autenticação (quem pode) em conjunto com uma adequada autorização (o que pode) são pré-requisitos para a responsabilização dos servidores envolvidos dentro do ambiente computacional. Pela análise (P.1.1 e Q.1.1), o sistema de pagamento, tanto na versão atual quanto após a modernização, não deixa dúvidas quanto a uma perfeita autenticação dos acessos.

Também quanto ao requisito de autenticação, o aplicativo deve permitir a um usuário obter uma única conexão ao sistema, não deixando que ocorra acesso de um mesmo usuário em mais de um terminal ao mesmo tempo. Deverão, ainda, fazer parte dos registros de auditoria, os horários de conexão e desconexão de cada usuário. Para o sistema atual, esse ponto de análise obteve posicionamentos diversos dos respondentes (P.1.6 e Q.1.6), ou seja, alguns apontaram que pode haver a conexão simultânea de um mesmo usuário e outros que

isso não é possível. A modernização, dentro desse contexto, promoverá avanços para os respondentes que consideraram a possibilidade de acesso simultâneo.

Envolvendo, ainda, o requisito de autenticação (somente usuários autorizados tenham acesso às informações), um sistema deve utilizar ferramentas adequadas para autenticação (teclado virtual para *login*, *tokens*, biometria e outras) dentro do que há de mais moderno no mercado. Um recurso muito popular para aumentar a segurança de sistemas é o teclado virtual, no qual o usuário digita sua senha. A principal função de sua utilização é que programas do tipo *key logs* não consigam capturar as senhas. Apesar de existirem métodos para burlar o teclado virtual, como a cópia de sua página em outro servidor e programas que filmam a digitação, por exemplo, considera-se que, em conjunto com outras medidas de segurança, esse recurso contribua para aumentar a autenticação em um sistema.

Ainda envolvendo o aspecto de autenticação, outro recurso que vem se difundindo é a utilização de *tokens* (chave eletrônica) para acesso a sistemas informatizados. Esse processo de certificação digital tem sido difundido no Governo Federal e já é de utilização obrigatória em acessos como ao Portal de Compras do Governo Federal. Pode-se dizer que esse tipo de controle preventivo se constitui em um importante aliado para uma maior autenticação e, consequentemente, maior segurança dos sistemas informatizados contra possíveis fraudes. Uma das maiores vantagens desse método de autenticação é que algumas empresas sobrevivem, quase que exclusivamente, da venda dessas ferramentas, o que torna bem complicado o extravio desses verdadeiros segredos industriais das empresas de segurança digital.

> Prevenção de fraude consiste em tomar medidas para evitar que ocorram fraudes antes do término de uma transação. A prevenção é feita normalmente durante a fase de autenticação de um usuário tradicionalmente utilizando senhas, frases secretas, dispositivos de geração de códigos secretos (tokens), etc. (KOVACH, 2011, p. 24).

Na vanguarda no aspecto de autenticação, os recursos de identificação por características biométricas podem ser utilizados sozinhos ou em conjunto com os citados acima. Alguns dos recursos biométricos mais utilizados são: o reconhecimento de digitais dos dedos ou da palma da mão inteira, o exame da retina ou íris dos olhos e a análise de padrões de voz. Apesar de seus méritos, também, estão sujeitos a diversas técnicas de fraude como, por exemplo, o uso de moldes de silicone com a impressão das digitais requeridas pelo sistema de controle.

A análise dos dados (P.1.9 e Q.1.9) indica claramente que o sistema em uso não utiliza ferramentas adequadas para autenticação (teclado virtual para *login*, *tokens*, biometria e outras) e dentro do que há de mais moderno no mercado. Para o sistema já modernizado, os

dados indicaram que o programa utilizará tais ferramentas. Os resultados são corroborados ao se verificar *in loco* que, para o sistema atual, nada disso é exigido e que o planejamento do SISPAG2 prevê a utilização de teclado virtual e de *tokens* para o acesso. A autenticação por biometria, mesmo no sistema após a modernização, não será utilizada.

Em um segundo momento, foi verificado se os recursos utilizados durante o tráfego dos dados promovem uma adequada segurança contra a interceptação de dados por pessoas não autorizadas. A segurança contra a interceptação busca assegurar que os dados, ainda que cheguem a mãos mal intencionadas, não tenham utilidade, uma vez que desconhecendo o processo de decriptografia, decodificação ou outro semelhante não é possível fazer uso das mensagens recebidas. Nesse ponto, houve um consenso (P.1.2 e Q.1.2) em apontar que o sistema dispõe de uma boa segurança quanto ao tráfego de dados e que a modernização somente agregará à melhoria desse requisito.

O requisito de integridade do sistema busca assegurar que as informações não sofrerão modificações não autorizadas. Dessa forma, a informação inserida deve sofrer ordenação e disposição em diversas telas, sem ter seu conteúdo comprometido, e gerando novas informações confiáveis (como exemplo, quanto inútil seria um sistema contábil em que o campo "total" do balanço não corresponda à soma das parcelas do mesmo). Também, a disposição das informações deve ser padronizada dentro do uso corrente, de forma a não induzir o usuário a um entendimento incorreto. Portanto, procurou-se saber se todas as informações, inclusive as geradas pelo próprio sistema, podem ser consideradas confiáveis e dispostas em formato compatível com o de utilização. Nesse ponto, houve uma concordância (P.1.3 e Q.1.3) em indicar que o sistema disponibiliza informações confiáveis e arranjadas adequadamente e que a modernização somente contribuirá para melhora desse requisito.

O sistema deve manter os registros de tempo de criação, modificação e acesso, além dos atributos de arquivos e demais dados gerados pelo usuário. A figura 10 traz um exemplo de registros para análise de um arquivo de interesse para melhor visualização.

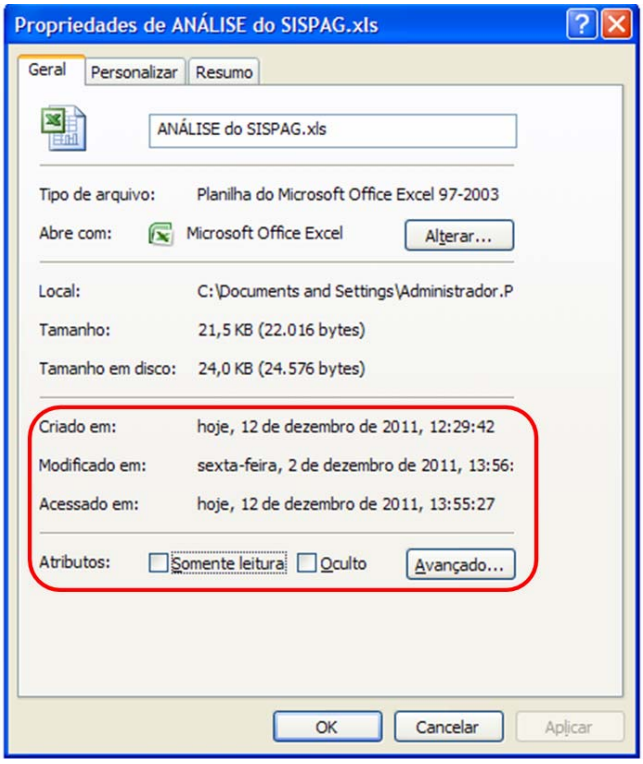

Figura 10: Exemplo de registros para análise de integridade.
Fonte: O autor.

Se os dados, arquivos ou demais componentes do sistema são criados, modificados ou se tem seus atributos alterados, o sistema estará com sua integridade comprometida e deve ser procedida uma apuração detalhada dos fatos e ações que levaram a essa situação.

Ainda dentro do requisito de integridade do sistema, o aplicativo deve garantir que a informação tratada pelo programa mantenha todas as características originais definidas por quem as inseriu no sistema. Nesse ponto, buscou-se saber se uma informação específica pode ser alterada pelo sistema sem a autorização do usuário que a inseriu. Pela análise (P.1.4 e Q.1.4), pode se dizer que o sistema atual tem problemas para manter a forma e o conteúdo dos dados inseridos. Essa dificuldade deverá ser resolvida pela modernização do programa.

O aplicativo deve permitir um efetivo e rigoroso controle de usuários e ter especificada uma política de senhas, mesmo para o caso do acesso *offline*. A política de acesso deve promover um controle rigoroso e atualizações periódicas do perfil do usuário e da permissão de acesso para evitar uso indevido da informação. As exceções possíveis e os privilégios concedidos aos usuários devem ser de conhecimento do responsável pelo controle interno e do administrador da rede.

Esse monitoramento por meio de senhas e perfis de atividade individual é indispensável para identificação de possíveis usos indevidos do sistema de informações. Kovach (2011, p. 75) exemplifica três análises possíveis:

- Frequência de transações de pagamento: o monitoramento desse perfil é feito para identificar um aumento repentino das transações que seja anormal a um usuário legítimo.

- Erros de senha: esse perfil é monitorado para detectar um número excessivo de tentativas de acesso com senha incorreta, o que pode se caracterizar em uma tentativa de invasão.

- Frequência de *login*: esse perfil monitora tentativas de acesso em períodos de tempo incomuns para os usuários legítimos.

Nesse contexto, devem ser desenvolvidas métricas e padrões para que se possam distinguir quais operações devem receber um tratamento particular do sistema e pessoal envolvido, por terem maiores possibilidades ou probabilidades de serem acessos indevidos ao sistema.

O uso de aplicativos e o acesso aos dados (P.1.5 e Q.1.5) dentro do programa em uso, segundo a análise, são controlados e monitorados por meio de senhas individuais atribuídas a pessoas pré-cadastradas e enquadradas em um perfil. A modernização somente contribuirá, segundo os respondentes, para melhora desse requisito.

A disponibilidade de um sistema de informações é um dos fatores críticos de um sistema. A princípio, quanto maior a disponibilidade de um programa, maior será a qualidade desse produto. Acredita-se que um sistema que foi desenvolvido para ser *online* deva ter uma disponibilidade próxima a 100%. A maior parte dos respondentes (P.1.7 e Q.1.7) discorda que o sistema atualmente em uso tenha essa disponibilidade. Quanto às expectativas para o sistema modernizado, um terço dos respondentes permanece neutro (nem concordam nem discordam) quanto a esse requisito.

Outro fator que afeta diretamente a disponibilidade do sistema são os momentos de pico de demanda pelos usuários a que o sistema está submetido. O sistema deve ser testado sob essas situações para que não deixe de atender satisfatoriamente. Em especial, no caso de um sistema de pagamento de pessoal que cumpre um rígido calendário, pode haver momentos de pico em dias próximos ao fechamento da folha de pagamento. Quanto ao sistema atual, a avaliação (P.1.8 e Q.1.8) foi de neutralidade (nem discordo nem concordo), que pode ser entendido como, no mínimo, uma falta de divulgação quanto à existência das respectivas previsões. Para o sistema modernizado, todos responderam que estão previstos momentos de pico para a operação do sistema.

A atualização do banco de dados exige que o usuário utilize uma senha para se conectar e atualizar suas tabelas. Devido aos riscos envolvidos, esse acesso deve ser limitado e controlado de maneira eficaz. O aplicativo precisa, ainda, gerenciar e monitorar a conexão com o banco de dados, se certificando de todas as medidas necessárias para realizá-la e mantê-la de forma automática, gerando e mantendo registro (*logs*) de tudo o que está sendo realizado. Durante a digitação na caixa de senha, devem ser mostrados símbolos (asteriscos, por exemplo) em vez dos números digitados. O registro das senhas de acesso em *logs* e relatórios do sistema devem ter tratamento semelhante, para que pessoas mal intencionadas que tenham acesso aos mesmos não copiem essas senhas para utilização indevida. As respostas obtidas (P.1.10 e Q.1.10) apontam para uma melhora desse aspecto no processo de modernização. Reitera-se, no entanto, que é recomendável que todos os sistemas utilizem senhas criptografadas para conexão ao Banco de Dados, em virtude dos grandes riscos envolvidos.

Os usuários sem conexão devem trabalhar na modalidade lote e encaminhar as alterações de pagamento por meios *offline* como entrega pessoal por mensageiro ou por via postal. Dentro da política de segurança aplicável ao sistema, não deve ser permitido acesso sem conexão à rede da MB como, por exemplo, pela Internet (P.1.11 e Q.1.11). Para o sistema atualmente em uso, a maioria das respostas apontou para o fato de o programa possibilitar acesso sem conexão à rede da MB para funções normalmente feitas pela rede interna. Com a conclusão da modernização, dentro da mesma análise, o sistema deverá impedir tal acesso.

As rotinas e procedimentos para uma rápida e perfeita recuperação de dados em possíveis situações adversas (P.1.12 e Q.1.12), além de especificadas em documentos formais como o manual do aplicativo, devem ser de conhecimento de todo o pessoal responsável para que o tempo despendido na tarefa seja mínimo. Quanto ao sistema atual, a avaliação foi próxima à posição de neutralidade (nem discordo nem concordo), quanto a uma perfeita e rápida recuperação de dados em uma possível situação adversa. Para o sistema modernizado, todos responderam que as medidas previstas cumprirão plenamente o recomendado.

Para o atendimento do requisito de auditoria do sistema (P.1.13 e Q.1.13), a totalidade das atividades processadas, bem como o usuário, a data e a hora das transações devem estar armazenadas em local próprio, a fim de permitir a realização de auditorias subsequentes por pessoal qualificado. Nenhum respondente concordou que o referido armazenamento ocorra no atual sistema. Para o sistema modernizado, todos responderam que as medidas previstas cumprirão totalmente o recomendado.

As atividades de controle ligadas ao requisito de auditoria devem estar baseadas em um criterioso acompanhamento, que envolve a análise de trilhas de auditorias e o estabelecimento de métricas ou padrões para se comparar com o que está sendo realizado no sistema, para apontar as atividades que têm maiores possibilidades ou probabilidades de serem uso indevido do sistema. Nesse aspecto (P.1.14 e Q.1.14), para o sistema atual todas as respostas foram neutras (nem discordo nem concordo), enquanto que foi quase unanime que o sistema modernizado disporá desse rigoroso monitoramento.

Ligado ao requisito de gerenciamento de transmissão de arquivos, o sistema deve permitir ao usuário receber confirmação de recepção para que possa identificar os registros enviados para não haver reenvio indesejado, informar a última data em que esta carga ocorreu e disponibilizar um relatório de erros, contendo os registros rejeitados e o motivo de cada um. Esse ponto pode ser entendido como necessário para economia de recursos, pois, devido à criticidade das operações envolvidas, o profissional que utiliza o sistema necessita estar ciente de quais informações estão sendo corretamente incluídas no processo de pagamento. Dessa forma, poderá haver vários reenvios desnecessários e, ainda, o usuário pode utilizar outras formas (ligações telefônicas para o órgão pagador, mensagens eletrônicas para os responsáveis pelo sistema etc.) para obter um retorno sobre suas atividades. Qualquer dessas redundâncias vai de encontro ao princípio da economicidade dos recursos públicos.

A análise desse ponto (P.1.15 e Q.1.15) leva a considerar que, no sistema atual, o usuário recebe confirmação de recepção de arquivos enviados, porém nem todos os envios são contemplados com esse retorno. De forma geral, segundo os respondentes, o sistema modernizado enviará uma confirmação de recepção, por registro, para não haver reenvio indesejado.

Ainda no requisito de gerenciamento de transmissão de arquivos, é recomendável que, durante a transferência de arquivos, o aplicativo deva indicar em tela o progresso da operação (barra de progresso) para informar ao usuário que a solicitação está sendo operada e dar uma ideia de quanto tempo a mesma levará para estar concluída. Esse tempo estimado de conclusão libera o usuário para arrumar sua mesa, conferir as ordens de serviço pendentes, checar sua agenda do dia e outras tarefas que podem representar uma economia recursos razoável, se considerado todo o processo de pagamento da Força.

Finalmente, como indicado pelos respondentes, o sistema atual deixa bastante a desejar em requisitos da categoria segurança. A modernização, no entanto, pretende corrigir a maioria dessas dificuldades existentes.

3.2.2 Categoria usabilidade

Oliveira, Queiroz-Neto e Maeta (2007, p. 3) ensinam que "[...] a usabilidade significa facilidade de uso, já que de nada adianta ter uma nova tecnologia, mas que de tão complexa seja inútil para o seu público alvo", definindo alguns atributos da usabilidade:

- Facilidade de aprendizado: facilitar uso com a seleção de opções em uma interface amigável. As imagens, símbolos e ícones que fazem parte do dia-a-dia também podem contribuir para facilitar a compreensão da interface;
- Eficiência: evitar a criação de muitos menus e submenus aninhados. As opções mais comuns devem ser apresentadas em primeiro plano;
- Facilidade de memorização: agrupar menus e submenus de forma lógica para os usuários;
- Baixa taxa de erros: permitir a seleção de reduzido número de operações, reduzindo confusões e ambiguidades;
- Satisfação subjetiva: usar moderadamente elementos gráficos, cores berrantes, sons de alerta etc.

Como se pode perceber a usabilidade, além de relacionada à satisfação do cliente e contribuir diretamente com o controle interno na redução de erros do processo, vai, também, ao encontro dos princípios da eficiência e da economicidade (menor dispêndio de recursos, em virtude de facilitar o aprendizado e a memorização). O quadro abaixo resume os resultados obtidos.

USABILIDADE ATUAL		
Perguntas	MÉDIA	DESVPAD
P.2.1	3,80000	0,44721
P.2.2	2,60000	0,54772
P.2.3	2,20000	1,09545
P.2.4	3,20000	0,44721
P.2.5	2,60000	0,89443
P.2.6	1,40000	0,54772
Média Geral	2,63333	

USABILIDADE DO SISPAG2		
Questão	MÉDIA	DESVPAD
Q.2.1	4,66667	0,51640
Q.2.2	4,66667	0,51640
Q.2.3	4,83333	0,40825
Q.2.4	4,83333	0,40825
Q.2.5	4,50000	0,83666
Q.2.6	5,00000	0,00000
Média Geral	4,75000	

Quadro 7: Resultados para categoria usabilidade.
Fonte: O autor.

Um adequado programa de treinamentos pode reduzir significativamente as dúvidas dos usuários, aumentando a produtividade e reduzindo os custos envolvidos no processo.

Essa maior interação entre o usuário e o próprio sistema, também, pode conduzir a sugestões que colaborem com uma maturidade mais precoce de todo o processo sistêmico. A maior parte dos respondentes (P.2.1 e Q.2.1) concorda que, tanto o atual sistema quanto o SISPAG2, têm um programa próprio de treinamentos para que os usuários operem adequadamente.

As interfaces gráficas interativas devem permitir uma boa navegabilidade entre as diversas janelas. Nenhum entrevistado (P.2.2 e Q.2.2) considerou que as interfaces gráficas interativas do sistema em uso permitem boa navegabilidade e facilidade de uso pelos usuários e todos concordaram que as interfaces do sistema em desenvolvimento permitirão essas experiências pelo usuário. Para o SISPAG2 foi definido, ainda, que as interfaces gráficas serão semelhantes ao padrão de telas utilizado atualmente pelo Setor de TI da PAPEM.

O manual do usuário busca, entre outras finalidades, explicar o funcionamento geral do sistema, os conteúdos das diversas telas e os elementos usados para atividades como inserir, alterar, excluir e consultar dados no sistema. Pela análise (P.2.3), pode-se dizer que o manual do usuário do sistema atual não descreve adequadamente as telas, seu conteúdo e seu uso.

O manual do usuário pode ser elaborado durante o desenvolvimento do software, no entanto, sua redação final está amarrada à execução da atividade de teste e ao sucesso na homologação. As respostas (Q.2.3) indicaram que o manual do SISPAG2 descreverá as telas, seu conteúdo e modo de uso.

Um sistema que disponibiliza, nos casos devidos, uma lista de opções para preenchimento, pode ser considerado um sistema mais ágil (dispensa digitação) e sem problemas de erros de digitação, atendendo aos princípios da economicidade e eficiência. Apesar de nenhum respondente (P.2.4 e Q.2.4) discordar da apresentação de tais listas no sistema atualmente em uso, o resultado próximo à neutralidade pode ser entendido como uma identificação de casos de uso (das listas) que ainda não estão atendidos. Para o SISPAG2 os resultados apontam que, nos casos devidos, será oferecida uma lista de opções para preenchimento.

A existência de um bom *menu* de ajuda disponível pode orientar consideravelmente novas funcionalidades e interfaces do sistema ou aquelas de pouca utilização no ciclo mensal de processamento da folha de pagamento. Pode servir, também, para introduzir o sistema a um novo funcionário, enquanto o mesmo aguarda a possibilidade de participação em treinamentos específicos. Essa facilidade vai ao encontro do princípio da economicidade e da eficiência do gasto público, em função do menor tempo para solução de dúvidas e consequente menor gasto envolvido. As respostas sobre esse aspecto (P.2.5 e Q.2.5)

traduzem uma reconhecida carência do atual sistema e a visão de uma possível solução para o SISPAG2.

Para atender ao requisito de interface gráfica do usuário, o programa deve ser operado através de interfaces gráficas interativas de acordo com um padrão preestabelecido. Esse requisito está ligado ao princípio da economicidade, uma vez que o usuário, ao se habituar ao padrão de interfaces de uma tela, estará apto a operar todas as outras com maior rapidez e economia de tempo e recursos. Para o SISPAG2, foi definido o padrão de telas utilizado atualmente pelo Setor de TI da PAPEM, ou seja, a princípio, os usuários já estarão ambientados ao tipo de interfaces a serem utilizados. Todos os respondentes (P.2.6 e Q.2.6) concordam plenamente que as interfaces gráficas serão padronizadas no SISPAG2. Os entrevistados apontaram, também, uma falta de padronização do programa em uso.

Finalmente, como indicado pelos respondentes, o sistema atual deixa bastante a desejar em requisitos da Categoria Usabilidade. Uma das justificativas para parte desse problema é a linguagem ultrapassada que possui o sistema em uso. A recodificação do sistema, no entanto, pretende corrigir a maioria dessas dificuldades.

3.2.3 Categoria desempenho

Nos requisitos ligados à categoria de desempenho, é importante relembrar que uma ampla gama de fatores externos influencia o desempenho de um *software*. Para uma adequada avaliação, devem-se promover testes com rigorosos parâmetros para se chegar a uma adequada mensuração. Para os fins desse estudo, o desempenho mencionado refere-se ao atingido pelo *software*, em uma situação teórica em que se pudesse isolá-lo de outras interferências externas (não mencionadas). Esclarecidos esses aspectos, o quadro abaixo resume os resultados obtidos.

DESEMPENHO ATUAL		
Pergunta	MÉDIA	DESVPAD
P.4.1	3,40000	0,89443
P.4.2	2,00000	1,41421
P.4.3	1,20000	0,44721
Média Geral	2,20000	

DESEMPENHO DO SISPAG2		
Questão	MÉDIA	DESVPAD
Q.4.1	4,16667	0,75277
Q.4.2	4,83333	0,40825
Q.4.3	4,33333	0,51640
Média Geral	4,44444	

Quadro 8: Resultados para categoria desempenho.
Fonte: O autor.

Para atender ao requisito de desempenho, o aplicativo deve buscar eficiência no uso de banda da infraestrutura de conectividade, principalmente para as transações *online*, assim como nas demais que demandem tráfego na rede dados da Marinha, sem, contudo, afetar o desempenho do software, em especial, o de tempo de resposta. Destaca-se da análise das respostas (P.4.1 e Q.4.1) que o tempo de resposta do sistema em uso foi considerado adequado, com uma perspectiva de pequena melhora para o programa recodificado. Uma das causas possíveis dessa adequabilidade do atual sistema pode ser creditada ao esforço continuado que a MB tem empregado na modernização das estruturas que dão suporte a seus sistemas corporativos.

Um sistema de grande porte deve suportar um significativo número de acessos simultâneos, sem degradação de seu desempenho. A definição do número de acessos deve ser feita com certa margem de segurança, para não trazer problemas de readequação a médio e longo prazo. Outro ponto importante a se considerar é que esse número deve ser definido de acordo com os momentos de pico do sistema. No caso do SISPAG2, estão previstos um mínimo de 1.000 (mil) acessos simultâneos (DFM, 2009). Para um sistema de pagamento que trabalha com mais de 200 organizações (DFM, 2009), entre OC e IQ, pode-se dizer que essa proporção prevista de acessos simultâneos é baixa (menos de cinco acessos simultâneos por organização) para os momentos de pico. Como o presente estudo não teve acesso ao total de número de senhas disponibilizadas atualmente e nem a outros documentos que possam ter subsidiado essa previsão, não se pode afirmar que o número chega a ser insuficiente.

Uma vez definido o número de acessos simultâneos esperados, deve-se promover uma averiguação prática (testes de stress) para atestar se a arquitetura desenvolvida pode realmente responder ao número de usuários que poderão acessar ao mesmo tempo, mitigando o risco envolvido de que alguns usuários fiquem sem conexão nas épocas mais críticas do processo de pagamento de pessoal. Da análise dos dados (P.4.2 e Q.4.2), pode-se dizer que o número de acessos simultâneos será aferido por uma ferramenta de teste de stress para o SISPAG2. Para o sistema atual, o conjunto de dados resultantes foi considerado insatisfatório, por apresentar desvio padrão muito alto (DESVPAD>MÉDIA/2) e nada poder indicar precisamente.

Para um sistema que se destina a atender usuários localizados em regiões distantes dos grandes centros urbanos, torna-se imprescindível saber se o usuário conseguirá acessar e utilizar o sistema ou se as dificuldades em trafegar dados permitirão apenas utilizações esporádicas ou, ainda, nenhum acesso. Para tal, esse tráfego de dados deve ser averiguado por uma ferramenta (teste de stress), que pode ser, por exemplo, um software gerador de fluxo de

dados, para atestar que a localidade consegue receber e transmitir dados mesmo nas situações de pico de demanda do sistema. Esse requisito vai ao encontro dos princípios da eficácia e da efetividade. A análise dos dados (P.4.3 e Q.4.3) indica que o acesso remoto de regiões com maiores dificuldades em trafegar dados, não avaliado pelo sistema em uso, será averiguado por teste de stress para o caso do SISPAG2.

Finalmente, como indicado pelos respondentes, o sistema atual deixa bastante a desejar em requisitos da Categoria Desempenho. Uma das justificativas para parte desse problema é a linguagem ultrapassada e as diversas adaptações pelas quais o sistema passou no decorrer de cerca de meio século de uso. Uma reestruturação do Centro de Dados da DFM foi concluída para, entre outras metas, criar a infraestrutura necessária para que a recodificação do sistema de pagamento possa corrigir a maioria dessas dificuldades. Recomenda-se que o sistema seja efetivamente testado quanto a seu desempenho, principalmente em condições extremas, como em picos de demandas.

3.2.4 Categoria suportabilidade

Destaca-se sua importância para uma concreta independência da empresa desenvolvedora do *software*, para fins de sua correta e tempestiva manutenção. Ou seja, além de combater o risco de descontinuidade da empresa desenvolvedora, esses requisitos buscam atender ao princípio da economicidade.

SUPORTABILIDADE ATUAL		
Pergunta	MÉDIA	DESVPAD
P.5.1	2,60000	0,54772
P.5.2	3,20000	1,09545
P.5.3	3,80000	0,44721
Média Geral	3,20000	

SUPORTABILIDADE DO SISPAG2		
Questão	MÉDIA	DESVPAD
Q.5.1	4,50000	0,54772
Q.5.2	4,16667	0,75277
Q.5.3	5,00000	0,00000
Média Geral	4,55556	

Quadro 9: Resultados para categoria suportabilidade.
Fonte: O autor.

No manual do aplicativo devem estar discriminadas as informações indispensáveis para configuração dos servidores, instalação e operação do programa, de forma a possibilitar a sua manutenção por pessoal qualificado da MB. Pelas respostas obtidas (P.5.1 e Q.5.1), o manual do sistema atual não define perfeitamente a configuração dos servidores e a instalação

e operação do aplicativo, o que pode gerar uma dependência do conhecimento pessoal de funcionários especializados no sistema. Essa situação pode ser observada, na prática, pela presença de funcionários na PAPEM com décadas de trabalho dedicadas ao SISPAG, gerando um risco de perda desses especialistas por aposentadoria, demissão ou movimentação para outras organizações. Recomenda-se que para o SISPAG2 essa situação seja evitada. O manual do sistema deve permitir que um funcionário com pouca ou nenhuma experiência com o sistema possa operá-lo adequadamente.

Devido à criticidade do sistema de pagamento de pessoal, é necessário um planejamento adequado para situações específicas, com a definição de um plano de contingência, um plano de backup e uma política de habilitação de usuários. Essas rotinas devem fazer parte do manual do aplicativo para que seja possível uma precisa e tempestiva manutenção do sistema.

O plano de contingência é um planejamento para que processos vitais do sistema (ou negócio) voltem a funcionar o mais rápido possível, mitigando os riscos e prejuízos de uma paralisação prolongada.

A cópia de segurança (*backup*) é a cópia de dados de um ambiente como a Internet ou intranet para outro com maior segurança. O plano de backup define procedimentos de automação dos processos para promover uma maior segurança e rapidez no armazenamento de dados, visando possível necessidade de utilização (*restore*).

A política de habilitação de usuários se destina a cadastrar e habilitar pessoas para acessarem as diversas partes ou módulos do sistema, de modo eficaz e de acordo com as normas e leis vigentes.

O manual do programa em uso, segundo as respostas (P.5.2 e Q.5.2), não define plenamente um plano de contingência, um plano de backup e uma política de criação de usuários, o que deverá ocorrer no manual do SISPAG2.

A capacitação da equipe responsável pelo sistema pode ser considerada um dos mais importantes fatores de sucesso no desenvolvimento, manutenção ou modernização do mesmo. Dessa forma, as necessidades que podem surgir durante o processamento da folha de pagamento podem receber tratamento adequado e com menor tempo de resposta ao cliente. Pela análise (P.5.3), o treinamento da equipe do programa em uso foi considerado, de maneira geral, adequado. Destaque importante foi para a concordância total (Q.5.3) de que a equipe de TI responsável pelo SISPAG2 receberá treinamento adequado para atuar nessa tarefa.

3.2.5 Categorias confiabilidade, implementação e capacitação da equipe

Passando à análise das categorias de confiabilidade, implementação e capacitação da equipe, o quadro abaixo destaca os resultados.

	SISPAG ATUAL			SISPAG2		
CATEGORIA	Questão	MÉDIA	DESVPAD	Questão	MÉDIA	DESVPAD
CONFIABILIDADE	P.3.1	2,00000	1,00000	Q.3.1	4,50000	0,83666
IMPLEMENTAÇÃO	P.6.1	2,80000	1,30384	Q.6.1	3,50000	1,76068
CAPACITAÇÃO DA EQUIPE	P.7.1	2,20000	1,09545	Q.7.1	4,50000	0,83666

Quadro 10: Resultados para as categorias confiabilidade, implementação e capacitação da equipe.
Fonte: O autor.

A categoria confiabilidade está intimamente ligada ao requisito de controle de transações, em que o aplicativo deve controlar as transações de modo a assegurar, em qualquer caso de erro de comunicação ou interno, que o programa permaneça em uma condição consistente. Dessa forma, o requisito de confiabilidade do sistema estará assegurado. Esclarece-se que a confiabilidade aqui citada não deve ser confundida com a confiabilidade das informações geradas pelo sistema, que dependerá, também, de outros requisitos do sistema e de aspectos que extrapolam o ambiente de TI, como, por exemplo, uma correta entrada de dados pelo usuário. Quanto mais falhas o sistema apresenta ao usuário (fechamentos repentinos, reinicialização da estação de trabalho etc.), menos confiável pode ser considerado esse sistema. Pode-se considerar que quanto menos confiável um sistema, menos confiável é a informação gerada pelo mesmo. O sistema em uso tem um problema crítico de corromper algumas das tabelas de dados e provocar perda parcial ou total dos dados presentes nessas tabelas. A análise das respostas (P.3.1 e Q.3.1) indica que o controle de transações no SISPAG2 assegurará a consistência do aplicativo, mesmo em caso de erro.

Devido à criticidade de um sistema dessa complexidade, pode ser compreensível que o banco de dados não seja do tipo software livre. A pessoa jurídica detentora do software é uma garantia adicional para o órgão contra possíveis riscos que podem afetar o banco de dados. A manutenção de uma equipe de TI atualizada e operante para promover garantia semelhante, além de não ser objetivo do negócio, poderia ser muito mais custosa do que terceirizar. Diferente disso, a dependência extrema de um desenvolvedor único representa um risco significativo para a continuidade das atividades envolvidas, pois, caso a empresa detentora do *software* encerre suas atividades, o órgão interessado ficaria sem ter a quem recorrer. Esse

risco deve ser gerenciado para impedir uma possível paralisação das atividades por falta de suporte ao banco de dados. Algumas respostas (P.6.1 e Q.6.1), quando analisadas individualmente indicaram que pode haver dependência do SISPAG2 em relação ao fornecedor do Banco de Dados, o que já ocorre parcialmente com o sistema em uso. Esse aspecto se concretizando necessariamente não compromete a qualidade ou segurança do produto final, mas gera um permanente risco a ser gerenciado.

Pode-se dizer que uma equipe com formação ou qualificação adequada às funções que desempenhou ou desempenha em um projeto ou sistema já operacional pode ajudar em muito no andamento dos trabalhos e afetar indiretamente a qualidade dos serviços prestados e de seus produtos resultantes. Da análise das respostas (P.7.1 e Q.7.1), pode-se dizer que a equipe se considera com formação ou qualificação adequada às funções que desempenhou ou desempenha no SISPAG2.

3.2.6 Categorias noções de controle interno, ciência da missão e atualização das normas

As categorias de noções de controle interno, ciência da missão e atualização das normas são comuns ao sistema atual e ao SISPAG2 e afetam indiretamente os serviços ligados a eles. O quadro abaixo destaca os resultados.

	COMUNS AO SISTEMA ATUAL E AO SISPAG2		
CATEGORIA	Questão	MÉDIA	DESVPAD
NOÇÕES DE CONTROLE INTERNO	Q.8.1	3,33333	1,21106
CIÊNCIA DA MISSÃO	Q.9.1	4,00000	0,63246
ATUALIZAÇÃO DAS NORMAS	Q.10.1	4,16667	0,40825

Quadro 11: Resultados para categoria noções de controle interno, ciência da missão e atualização das normas.
Fonte: O autor.

O grau de conhecimento do Regimento Interno, Ordens Internas, Leis e demais normas que estabeleçam controles internos pelo pessoal envolvido no desenvolvimento ou manutenção de um sistema pode contribuir ou dificultar o estabelecimento ou aprimoramento de adequados controles dentro do referido sistema, afetando indiretamente a qualidade e a segurança do *software*. Nesse aspecto, os resultados (Q.8.1) apontam para um razoável grau de conhecimentos dos referidos instrumentos de controle interno.

O conhecimento do objetivo do negócio, da missão e tarefas atribuídas à organização deve estar na mente dos envolvidos no desenvolvimento e manutenção de um sistema, guiando cada ação para um ponto comum. Ressalta-se que o desconhecimento desses fatores pode levar a uma perda de foco e afetar indiretamente a segurança e qualidade do software. Nesse sentido, o grau de conhecimento da missão e tarefas atribuídas à organização (Q.9.1) de maneira geral foi considerado bom, o que indica que o mesmo ainda pode ser melhorado por meio da inclusão de tópicos sobre o assunto em Planos do dia (informativo interno diário) e em treinamentos ministrados.

Como o ambiente ligado a TI é bastante dinâmico, estando em constante evolução, as ordens internas ligadas à área de informática, também, devem passar por revisões periódicas para que estejam sempre acompanhando a realidade dos fatos. Esse aspecto pode afetar indiretamente a manutenção, segurança e qualidade do software, além de estar ligado a um dos princípios do controle interno (atribuição de responsabilidades) dentro do ambiente de TI. As ordens internas utilizadas pelo pessoal da área de TI (Q.10.1) foram consideradas atualizadas pelos respondentes. Pela análise documental, verificou-se que todas as referidas ordens internas têm menos de seis anos da data de sua assinatura e algumas já estão com data de assinatura de 2011, o que demonstra uma preocupação nesse aspecto.

3.2.7 Categorias segregação de ambientes e design

As categorias de segregação de ambientes e design estão ligadas à área de desenvolvimento de *softwares*, no caso o SISPAG2. O quadro abaixo destaca os resultados.

SEGREGAÇÃO DE AMBIENTES (SISPAG2)		
Questão	MÉDIA	DESVPAD
Q.11.1	4,83333	0,40825

DESIGN DO SISPAG2		
Questão	MÉDIA	DESVPAD
Q.12.1	4,83333	0,40825
Q.12.2	4,83333	0,40825
Q.12.3	4,83333	0,40825
Q.12.4	4,16667	0,98319
Média Geral	4,66667	

Quadro 12: Resultados para as categorias segregação de ambientes e design.
Fonte: O autor.

A separação dos ambientes de produção, desenvolvimento e homologação pode ser considerada uma das características mais importantes para a produção de um *software* com qualidade e segurança. No desenvolvimento do SISPAG2, a separação dos três ambientes está a cargo da PAPEM (ambientes de produção e homologação) e da empresa desenvolvedora (ambiente de desenvolvimento). O ambiente de desenvolvimento está ligado à construção, adequação ou atualização do sistema. O ambiente de homologação está relacionado a diversos testes sobre o que foi desenvolvido. O ambiente de produção pode ser entendido como o ambiente no qual o sistema atuará após sua implantação. Essa separação em ambientes busca contribuir para que o programa chegue à fase de produção com menor risco de apresentação de problemas. A documentação deve ocorrer paralelamente às atividades de cada ambiente até a entrega do produto final. Os registros resultantes de cada atividade devem ser atualizados antes da efetiva implantação do sistema. Dentro dessa abordagem, os resultados (Q.11.1) apontam para a existência de ambientes de produção, desenvolvimento e homologação separados, o que indica um primeiro passo no caminho do sucesso do projeto.

Nas ferramentas de design utilizadas no desenvolvimento de software devem estar todos os artefatos (resultado de certa atividade ou conjunto de atividades) e UML previstos anteriormente na fase de planejamento. Claro que não significa que o planejamento não possa ser alterado, mas, sim, que deve haver um controle da ação planejada eficiente e devidamente documentado.

A *Unified Modeling Language* (UML), Linguagem de Modelagem Unificada, serve para um melhor entendimento das inter-relações entre os diversos componentes, objetos, casos de uso, iterações e outras partes do projeto (OMG, 2005). As informações da UML podem ser representadas graficamente em diagramas específicos para melhor compreensão (OMG, 2005). Como o próprio nome sugere, a UML possibilita que todos os integrantes da equipe de desenvolvimento possam ter uma comunicação uniforme sobre a modelagem do software. Essa padronização de linguagem independe da metodologia de desenvolvimento empregada no projeto (OMG, 2005).

Dessa forma, o que ocorre é que, de posse de uma linguagem única, são iniciadas atividades, que geram artefatos que devem ser documentados e podem servir de base para outros artefatos ou documentações. Durante todo o processo, deve existir um monitoramento para identificar se os resultados estão de acordo com as metas estabelecidas (realizações, tempestividade, custos etc.).

Nas ferramentas de modelagem previstas para o SISPAG2 (Q.12.1) estão, segundo os dados obtidos, todos os artefatos e UML estabelecidos no contrato. Alguns documentos

internos da PAPEM, também, definem uma arquitetura, baseada no emprego dos diagramas relacionados à UML e seguindo um modelo incremental e iterativo, para uma orientação básica à equipe responsável, definindo processos de desenvolvimento e manutenção de software que possam ser adequados e utilizados por diferentes projetos para atender à realidade da área de informática.

O transcorrer do projeto, o contato com usuários e demais fatores podem levar a novas demandas que não estavam previstas no início do projeto. Essas demandas levarão à mudanças no processo de desenvolvimento em curso. Destaca-se que essas modificações referem-se às que o cliente impõe ao desenvolvedor e não as alterações que visam à adequação e viabilidade técnica do projeto, que já devem estar previstas pela organização desenvolvedora dentro de sua análise de riscos do projeto. Os impactos dessas mudanças podem ser grandes ou pequenos, mas sempre haverá algum impacto. Alterações em interfaces, design e processos já aprovados são alguns exemplos que podem afetar significativamente, entre outros fatores, os prazos e orçamentos previstos. Existe, ainda, um risco de a qualidade do produto final ser afetada por essas alterações. Assim, documentações e registros detalhados sobre as mudanças devem ser gerados e arquivados em local seguro. Para o SISPAG2, todos os entrevistados (Q.12.2) concordam que as mudanças ao longo do processo estão sendo registradas e documentadas.

O *Rational Unified Process* (RUP) emprega algumas das melhores práticas aplicáveis ao desenvolvimento de software, proporcionando um aumento na produtividade da equipe, ao definir diretrizes, modelos, ferramentas e uma base única de conhecimento para as atividades de desenvolvimento. Ressalta-se que outras metodologias poderiam ser usadas no processo de desenvolvimento com semelhante sucesso, uma vez que existem diversas metodologias com as melhores práticas aplicáveis. Pode-se dizer que o mais importante é a escolha de uma metodologia e que haja um acompanhamento para assegurar que ela está sendo seguida. Todos os entrevistados concordaram (Q.12.3) que o processo de desenvolvimento do SISPAG2 está seguindo os passos descritos pelo processo unificado da metodologia RUP.

Não somente é necessário haver um cronograma formalmente estabelecido para o projeto como, também, deve haver um eficiente e eficaz acompanhamento para que se possa saber em que parte do desenvolvimento efetivamente se está.

O cronograma deve ser determinado em conjunto com a equipe de TI na fase de planejamento do projeto e, uma vez definido, deve ser cumprido para não impactar outras áreas com estreito interesse no cumprimento dos prazos estipulados.

O cronograma pode ser considerado uma das principais peças para se medir a produtividade de um projeto em execução. O compromisso dos envolvidos no desenvolvimento aumenta, na medida em que vão ficando mais focados e perseguindo as metas estabelecidas no cronograma. Apesar de um atraso no cronograma não significar o fracasso do projeto, sinaliza que alguma coisa está indo mal e necessita de urgente atenção. Nesse sentido, Robic e Sbragia (1996, p. 10) chamam a atenção para o fato de que "[...] o atraso pode ser entendido como um termômetro da situação do projeto, indicando que, se não resolvidos a tempo, podem acabar definindo o fracasso do empreendimento". Da análise das respostas (Q.12.4), pode ser observado que, apesar da maioria concordar que existe um acompanhamento eficiente e eficaz do cronograma de projeto, alguns respondentes indicaram uma posição neutra (nem discordo nem concordo), o que pode se traduzir em áreas do projeto que estão mais deficientes em atender ao andamento planejado. A princípio, todas as áreas devem ser gerenciadas e conduzidas de modo a proporcionar que todo o projeto seja concluído conforme o estabelecido no planejamento. O projeto SISPAG2 está atrasado em cerca de um ano em relação ao cronograma inicial do projeto. Esse atraso pode ser devido, em parte, às alterações nas atividades de desenvolvimento definidas no projeto inicial.

3.2.8 Pontos a gerenciar e a explorar

Após uma análise individual, as perguntas, dentro de suas categorias, foram divididas em dois grupos (ambiente de TI e ambiente externo) de modo que fosse possível promover uma análise SWOT (*Strengths, Weaknesses, Opportunities and Threats*) para identificar, respectivamente os pontos de forças, fraquezas, oportunidades e ameaças ao sistema. Os dados obtidos foram analisados e posicionados em um quadro indicando as categorias que devem ser gerenciadas e as que devem ser exploradas. Como parâmetro para divisão em pontos a explorar ou a gerenciar, foi utilizada a média das médias das diversas categorias como exposto nos quadros abaixo. Para o sistema atual se obteve os resultados do quadro 13.

	SISPAG ATUAL			
CATEGORIA	**MÉDIA**	**DESVPAD**	**MÉDIA-DESVPAD (*)**	**MÉDIA+DESVPAD (**)**
Segurança	3,16000	0,78475	2,37525	**3,94475**
Usabilidade	**2,63333**	0,66329	1,97004	3,29662
Confiabilidade	2,00000	1,00000	**1,00000**	3,00000
Desempenho	2,20000	0,91862	**1,28138**	3,11862
Suportabilidade	3,20000	0,69679	2,50321	**3,89679**
Implementação	2,80000	1,30384	**1,49616**	4,10384
Capacitação da Equipe	2,20000	1,09545	**1,10455**	3,29545
TOTAL	**2,59905**	0,92325	**1,67580**	**3,52230**

Quadro 13: Análise de médias e desvios padrões para o SISPAG em uso.
Fonte: O autor.

Para o SISPAG2 se obteve os resultados representados no quadro 14.

	SISPAG2			
CATEGORIA	**MÉDIA**	**DESVPAD**	**MÉDIA-DESVPAD (*)**	**MÉDIA+DESVPAD (**)**
Segurança	4,65556	0,62823	4,02733	**5,28378**
Usabilidade	4,75000	0,44766	4,30234	**5,19766**
Confiabilidade	4,50000	0,83666	3,66334	**5,33666**
Desempenho	**4,44444**	0,55914	3,88530	5,00358
Suportabilidade	**4,55556**	0,43350	4,12206	4,98905
Implementação	3,50000	1,76068	**1,73932**	5,26068
Capacitação da Equipe	4,50000	0,83666	3,66334	**5,33666**
Noções de Controle Interno	3,33333	1,21106	**2,12227**	4,54439
Ciência da Missão	4,00000	0,63246	**3,36754**	4,63246
Atualização das Normas	**4,16667**	0,40825	3,75842	4,57491
Segregação de Ambientes	4,83333	0,40825	4,42509	**5,24158**
Design	4,66667	0,55198	4,11468	**5,21865**
TOTAL	**4,32546**	0,72621	**3,59925**	**5,05167**

Quadro 14: Análise de médias e desvios padrões para o SISPAG2.
Fonte: O autor.

Cabe ressaltar que, devido ao desvio padrão muito alto da categoria implementação (DESVPAD>MÉDIA/2), essa categoria teve sua análise prejudicada e, por convenção para que a mesma constasse da matriz SWOT, foi considerada prudentemente como a gerenciar.

Face ao exposto, foi elaborada a matriz SWOT para o sistema em uso, conforme quadro abaixo:

	EXPLORAR	GERENCIAR
Ambiente de TI	Segurança** Suportabilidade** Usabilidade	Confiabilidade* Desempenho* Implementação*
Ambiente Externo		Capacitação da Equipe*

Quadro 15: Análise SWOT do SISPAG em uso.
Fonte: O autor.

Da matriz acima, podem ser observadas características de um sistema de sucesso, mas que sofre com sua ultrapassada tecnologia. Dessa forma a segurança, suportabilidade e usabilidade, apesar de requererem melhoramentos, representam, ainda assim, pontos fortes do sistema em uso e podem ser considerados alguns dos motivos de sucesso desse programa com cerca de meio século de idade. As demais categorias devem ser trabalhadas para o novo sistema, podendo ser entendidas como os pontos degradados pelo tempo de uso e pelas adaptações sucessivas para o atendimento a necessidades pontuais dos usuários. Ressalta-se que as categorias do Ambiente Externo que são comuns ao SISPAG2 estão representadas apenas na matriz desse último. Assim, apresenta-se a matriz SWOT do sistema modernizado, conforme segue:

	EXPLORAR	GERENCIAR
Ambiente de TI	Confiabilidade** Segurança** Design** Usabilidade** Suportabilidade Desempenho	Implementação*
Ambiente Externo	Capacitação da Equipe** Segregação de Ambientes**	Noções de Controle Interno* Ciência da Missão* Atualização das Normas

Quadro 16: Análise SWOT do SISPAG2.
Fonte: O autor.

Da análise acima, verifica-se a necessidade de se gerenciar mais efetivamente o ambiente externo do novo sistema. Os pontos a explorar identificados devem ser, após a prontificação do programa, testados para se aferir a realidade desses apontamentos. A figura abaixo traz um comparativo entre o sistema em uso e o que se espera do novo sistema após a modernização.

	EXPLORAR	GERENCIAR
Ambiente de TI	Segurança ⇑ ⇐ Suportabilidade ⇑ ⇐ Usabilidade ⇑	Confiabilidade Desempenho Implementação
Ambiente Externo	⇐	Capacitação da Equipe

Figura 11: Análise SWOT da evolução esperada com a modernização para o SISPAG2.
Fonte: O autor.

Como pode ser percebido o projeto SISPAG2, segundo os dados obtidos, irá resolver algumas dificuldades vivenciadas pelos usuários do sistema em uso. Porém, ressalta-se que, uma vez que o sistema ainda está na fase de construção, algumas modificações devem ocorrer até o fim do projeto.

3.2.9 Análise geral do sistema

Para responder à pergunta de pesquisa − O sistema de controle interno utilizado pelo Sistema de Pagamento de Pessoal da Marinha do Brasil atende às leis, regulamentos e demais normas vigentes na esfera federal e ao que prevê o referencial teórico e os estudos acadêmicos sobre o assunto? – estabeleceram-se para as categorias discutidas alguns pesos que, multiplicados pelas médias, darão um valor por categoria que, somados, indicarão uma nota geral do sistema.

	SISPAG2	SISPAG em uso
CATEGORIA	PERCENTAGEM	PERCENTAGEM
Segurança	55,00%	60,00%
Usabilidade	5,00%	5,00%
Confiabilidade	15,00%	15,00%
Desempenho	5,00%	5,00%
Suportabilidade	5,00%	5,00%
Implementação	5,00%	5,00%
Capacitação da Equipe	1,00%	2,00%
Noções de Controle Interno	1,00%	1,00%
Ciência da Missão	1,00%	1,00%
Atualização das Normas	1,00%	1,00%
Segregação de Ambientes	1,00%	-
Design	5,00%	-
TOTAL	100,00%	100,00%

Quadro 17: Pesos atribuídos a cada categoria.
Fonte: O autor.

A atribuição de pesos foi debatida não somente com o orientador, mas, também, com profissionais ligados à área de TI, para que se pudesse chegar a pesos adequados. A maior porcentagem atribuída à categoria Segurança deve-se ao fato de esta ser um requisito crítico que pode levar a impactos profundos em todo o sistema e afetar ou comprometer, também, outros requisitos. Por exemplo, um sistema deficiente em segurança não pode ser considerado um sistema confiável, uma vez que um indivíduo mal intencionado pode invadir esse sistema

e retirar, acrescentar ou alterar dados. Destacam-se impactos da segurança nas categorias de usabilidade e desempenho da seguinte maneira:

> A necessidade de termos uma estrutura de segurança impacta na performance e facilidade de uso dos sistemas. São senhas e mais senhas, textos criptografados, assinatura digital, *firewalls* (proteção), antivírus, controles cruzados, uso de *tokens* (dispositivo que gera números aleatórios validados pelo sistema para permitir a entrada do usuário) e até sensores biométricos, como o reconhecimento digital pela íris, face ou voz. (Haberkorn, 2009, p. 25, grifo do original).

As demais categorias estão mais ligadas aos aspectos de qualidade do sistema de informação, que estão diretamente ligadas à satisfação dos anseios dos usuários. Dentre elas, destaca-se a atribuição de peso maior à confiabilidade, o que se deve a seu relacionamento com uma das principais razões para o desenvolvimento de um sistema de informações, que é fornecer informações confiáveis aos usuários interessados. Netto e Silveira (2007, p. 377) chamam a atenção para o fato de grande parte dos dados importantes ao negócio estar armazenada em computadores e "[...] por isso as organizações dependem da confiabilidade de seus sistemas baseados em TI; se a confiança nesses dados for destruída, o impacto pode ser comparável à própria destruição do sistema".

Destaca-se, também, que foi debatida a atribuição de um maior peso para a categoria de desempenho, por estar diretamente ligada ao aspecto de tempestividade das informações contábeis, mas devido a outros fatores externos ao programa (banda de transmissão, entre outros exemplos) que afetariam com maior significância o desempenho do sistema, essa diferenciação de pesos foi abandonada.

As categorias de segregação de ambientes, ciência da missão, capacidade da equipe e atualização das normas receberam os menores pesos por serem externas ao sistema e terem somente influência indireta na qualidade do sistema desenvolvido.

Definidos os pesos e respondidos os questionários, pode-se chegar a uma avaliação geral do sistema.

Netto e Silveira (2007, p. 377) definem segurança da informação como "[...] área do conhecimento que visa à proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade a fim de garantir a continuidade do negócio e minimizar os riscos". A segurança do SISPAG baseia-se, segundo a norma aplicada (MB, 2007), nos seguintes princípios e instrumentos:

- Controle de acesso: garantido por funcionalidade que controla e monitora o uso de aplicativos e o acesso aos dados, por meio de senhas individuais utilizadas por pessoas previamente cadastradas, habilitadas e enquadradas em um perfil de usuário;

- Fidedignidade dos dados inseridos: manutenção da forma e do conteúdo dos dados incluídos pelas OC e IQ;

- Funcionalidades de segurança: manutenção da integridade dos dados; e

- Inalterabilidade: garantia de que as informações dos documentos produzidos pelo SISPAG não serão mudadas após o fechamento do processo de pagamento.

Nesse contexto, definidas as porcentagens para cada categoria, utilizaram-se as referidas médias para se chegar a um produto, cujo somatório representa a análise do sistema.

Categoria	Percentagem	MÉDIA do SISPAG em uso	PRODUTO
Segurança	60,00%	3,16000	1,89600
Usabilidade	5,00%	2,63333	0,13167
Confiabilidade	15,00%	2,00000	0,30000
Desempenho	5,00%	2,20000	0,11000
Suportabilidade	5,00%	3,20000	0,16000
Implementação	5,00%	2,80000	0,14000
Capacitação da Equipe	2,00%	2,20000	0,04400
Noções de Controle Interno	1,00%	3,33333	0,03333
Ciência da Missão	1,00%	4,00000	0,04000
Atualização das Normas	1,00%	4,16667	0,04167
TOTAL	100,00%	-	**2,89667**

Quadro 18: Resultados por categoria pra o sistema atual.
Fonte: O autor.

Como exposto acima e considerando que nenhuma ilegalidade ou irregularidade foi encontrada pelo presente estudo, pode-se dizer que o sistema de controle interno utilizado pelo Sistema de Pagamento de Pessoal da Marinha atualmente em uso atende às leis, regulamentos e demais normas vigentes na esfera federal e, parcialmente, ao que prevê o referencial teórico e os estudos acadêmicos sobre o assunto.

Categoria	Percentagem	MÉDIA DO SISPAG2	PRODUTO
Segurança	55,00%	4,65556	2,56056
Usabilidade	5,00%	4,75000	0,23750
Confiabilidade	15,00%	4,50000	0,67500
Desempenho	5,00%	4,44444	0,22222
Suportabilidade	5,00%	4,55556	0,22778
Implementação	5,00%	3,50000	0,17500
Capacitação da Equipe	1,00%	4,50000	0,04500
Noções de Controle Interno	1,00%	3,33333	0,03333
Ciência da Missão	1,00%	4,00000	0,04000
Atualização das Normas	1,00%	4,16667	0,04167
Segregação de Ambientes	1,00%	4,83333	0,04833
Design	5,00%	4,66667	0,23333
TOTAL	100,00%	-	**4,53972**

Quadro 19: Resultados por categoria pra o SISPAG2.
Fonte: O autor.

Como exposto acima e considerando que nenhuma ilegalidade ou irregularidade foi encontrada pela análise do estudo, pode-se dizer que o sistema de controle interno utilizado pelo Sistema de Pagamento de Pessoal da Marinha após a modernização atenderá às leis, regulamentos e demais normas vigentes na esfera federal e, parcialmente, ao que prevê o referencial teórico e os estudos acadêmicos sobre o assunto, de modo mais completo que o sistema atualmente em uso.

4 CONCLUSÃO

Na realização da presente estudo, constatou-se que um controle interno adequado é impossível de ser estabelecido sem o apoio em soluções tecnológicas. O enorme volume de dados a serem trabalhados somente é possível por meio do uso de computadores.

O processamento, a crítica e o fechamento da folha dentro do programa de pagamento de pessoal, bem como todos os controles e rotinas envolvidos no processo, são executados sob a responsabilidade da Pagadoria de Pessoal da Marinha (PAPEM).

A etapa 1 do projeto de desenvolvimento do SISPAG2 se encontrava, quando da conclusão desse estudo, na fase de construção do software, que envolve a codificação dos aplicativos, programação e testes. Com o atraso no projeto, essa fase inicialmente prevista para terminar no final do mês de outubro de 2011 tem nova previsão para o segundo semestre de 2012. Esse atraso inviabilizou diversas análises, como as relativas ao desempenho do sistema, que se pretendia realizar nesse estudo, uma vez que somente poderiam ser realizadas sobre o produto final.

Pode-se dizer que o controle interno do sistema de processamento da folha de pagamento de pessoal está em constante evolução, aprimorando seus mecanismos de controle e adaptando-os às demandas geradas por novas ameaças, tecnologias ou leis, regulamentações e normas de interesse. Os diversos órgãos envolvidos no processamento da folha de pagamento auxiliam a PAPEM nessa difícil tarefa, encaminhando sugestões e reportando falhas identificadas na estrutura sistêmica. Dessa forma, o processo de pagamento evolui no caminho de oferecer informações adequadas (relevantes, confiáveis e oportunas) às necessidades do usuário.

Alguns controles já são utilizados pelo programa de pagamento no processo de depuração (crítica), como o limite para remuneração de servidor dentro do teto constitucional (art. 37 da CF/88), valores máximos para parcelas comandadas com valor, parcelas inconsistentes com a situação do servidor, número de dependentes relativamente alto, tentativa de alteração de situação do servidor por organização diferente daquela em que está lotado, tentativa de inclusão de servidor com matrícula já existente, direcionamento de remuneração para banco não conveniado à MB, limite para o total de descontos dentro da margem consignável do servidor, parametrização de parcelas de pagamento ou desconto, verificação pelo Órgão Pagador de comandos relativos a exercícios anteriores, parcela de

vale-transporte relativamente alta e tentativa de alteração de posto de servidor inativo ou pensionista por organização diferente do Serviço de Inativos e Pensionistas da Marinha.

Outros controles, no entanto, estão em planilhas ou programas desenvolvidos em diversas linguagens espalhados por vários setores envolvidos no processamento da folha de pagamento. Considera-se imperioso que tais controles sejam identificados e analisados para que os mais importantes venham a ser incorporados ao SISPAG2. Tal procedimento, além de ampliar os importantes controles a todos os envolvidos com o sistema de pagamento, vai acabar com a redundância de possíveis controles, favorecendo os princípios da eficiência e da economicidade.

Dentre os controles feitos por fora do sistema, foi possível identificar os seguintes: diferentes pessoas com relação de remuneração (RR) com a mesma conta corrente para depósito; relação de remuneração suspensa ou bloqueada e reativada no mês seguinte (pode indicar fraude); operações de acerto de contas (encerramento de uma RR) repetidas; alteração de conta corrente para RR em acerto de contas; mudança de organização de pessoa com RR em acerto de contas; parcelas em duplicidade; RR em duplicidade; auxílio-transporte sem desconto de parcela do beneficiário; desconto de auxílio transporte sem recebimento da parcela; auxílio fardamento em valor maior que o soldo; adicional natalidade em valor maior que o soldo; recebimento de assistência pré-escolar sem cota-parte e vive-versa; descontos, relacionados à pensão militar e ao Fundo de Saúde da Marinha, não implantados; espaço reservado ao número do Cadastro de Pessoas Físicas (CPF) em branco ou em duplicidade; e pagamento suspenso por mais de três meses.

Importante avanço que está sendo viabilizado na modernização do sistema é a crítica *online* dos dados inseridos, que permitirá uma maior eficiência e economicidade no processamento da folha de pagamento de pessoal, contribuindo para o fortalecimento do controle concomitante das atividades envolvidas. Dessa forma, os dados criticados podem ser revistos e terem efeito financeiro dentro do mesmo processo de pagamento.

Outro aumento no controle concomitante diz respeito aos alertas disponibilizados em quadro de aviso para os agentes responsáveis e demais perfis cadastrados. Dessa forma, o gestor de pagamento e o ordenador de despesas poderão acompanhar concomitantemente os comandos de pagamento de maior interesse.

A linguagem do atual sistema e a que está sendo utilizada na modernização do programa são de conhecimento público e, por isso, estão expostas a todas as vulnerabilidades dos programas desenvolvidos na mesma linguagem. Dessa forma, o programa está sujeito, mesmo que atualizado tempestivamente, a ataques de pessoal especializado nessa linguagem.

Essa fragilidade deve ser minimizada com a atualização periódica da estrutura lógica e física que dá suporte ao sistema de modo a impedir, ou ao menos dificultar, que pessoas mal intencionadas tenha acesso ao sistema. Deve-se ter em mente que a chance de ser apanhado, por si só, já impede que muitos fraudadores potenciais atuem.

A maior parte dos controles identificados visa à preservação da forma e do conteúdo da informação que alimenta o sistema. Dessa forma, estão voltados para padronizar a entrada de dados e para prevenção de erros por parte dos operadores do sistema, e não para prevenção e detecção de fraudes ou mau uso das informações.

Mesmo com o novo sistema operando *online*, algumas organizações, por motivos diversos, continuarão encaminhando suas alterações pela interface *batch*. Nesse aspecto, devem ser desenvolvidos, também, controles mais eficientes para esse tipo de remessa das alterações de pagamento. A criptografia desse tipo de remessa deve impedir, além da visualização por pessoas de fora da Marinha, que as alterações de pagamento enviadas por uma organização sejam interceptadas, abertas e alteradas em outra organização que possua o programa de pagamento instalado.

Essas duas interfaces disponibilizadas pelo sistema após a modernização demandarão um sistema mais robusto de controle, uma vez que ele estará exposto às ameaças oriundas de ambas as interfaces.

Os controles que estarão disponíveis no sistema modernizado e, em particular, os ligados à segurança do *software*, devem ser gradativamente estendidos aos cadastros de pessoal que alimentam o pagamento, pois uma fragilidade desses cadastros de pessoal pode torná-los vítimas preferenciais de pessoas que queiram obter vantagens financeiras ilícitas.

Com a conclusão do projeto do sistema de pagamento, devem ser feitos exaustivos testes para constatação da efetiva integração entre esse e o cadastro de pessoal. A quantidade de militares em ambos os cadastros deve ser igual e verificada mensalmente. Os casos excepcionais devem constar em relatórios específicos, com detalhamentos suficientes para sua perfeita identificação, a serem encaminhados aos responsáveis pelo controle interno das organizações envolvidas, com cópia para a Diretoria de Contas da Marinha.

A modernização do sistema de pagamento da Marinha deverá contribuir, entre outros pontos, com uma melhor qualidade das informações digitadas, em virtude principalmente da crítica na entrada de dados; período mais curto entre a digitação e seu efeito financeiro; disponibilização de relatórios gerenciais e de controle interno para monitoramento da atividade de digitação; e relatórios de inconsistências que provoquem rejeições de parcelas comandadas.

É aconselhável que o sistema de pagamento, para o fortalecimento de seu controle interno, caminhe no sentido de se integrar a sistemas de interesse como o SIAPE, Sistema de Controle de Óbitos da DATAPREV e Declaração do Imposto de Renda de Pessoa Física da Receita Federal. Somente dessa forma, será possível o estabelecimento de trilhas de auditoria para identificar, através do cruzamento de dados entre os diferentes programas, situações irregulares ou potencialmente incoerentes − como, por exemplo, pessoas falecidas que recebem, por um ou mais meses, como em efetivo serviço ou militares reformados por invalidez permanente, que se encontrem trabalhando em organizações públicas ou privadas.

Nesse aspecto, a não integração do sistema de processamento da folha de pagamento ao sistema de pessoal conhecido como Banco de Dados Integrador (BDI) da Diretoria de Pessoal Militar da Marinha pode ser considerado uma das maiores perdas do processo de desenvolvimento do SISPAG2 em relação ao projeto inicialmente planejado. Apesar de continuarem os esforços para viabilização da integração do novo sistema ao Sistema de Inativos e Pensionistas da Marinha (SIPEM), o que representará um avanço considerável em relação ao sistema atualmente em uso, a falta do cadastro do pessoal da ativa manterá o cadastro próprio do SISPAG, o que, a princípio, vai de encontro à segregação de funções, pois permite que quem paga, também, cadastre o recebedor dos proventos.

A validação de matrícula e nome completo com o BDI permitirá que não sejam cadastradas pessoas de fora da MB como servidores da ativa. Esse controle, juntamente com a integração ao SIPEM, impedirá que pessoas sem vínculo de remuneração com a MB possam receber valores, sem se enquadrarem em situações especiais (como, por exemplo, pagamentos por determinações judiciais).

A verificação do CPF junto à Receita Federal, inicialmente prevista, foi abandonada no decorrer do projeto. Essa verificação deve ser perseguida, uma vez que o CPF é um dos principais campos utilizados para integração com sistemas de outras instituições governamentais e privadas.

A existência do Portal de Ordens de Serviço, disponível na página da intranet da Diretoria de Contas da Marinha, tem sido um importante apoio para facilitar a *accountability*, economizando tempo e recursos importantes de todos os envolvidos. Considera-se que a facilidade de confecção de Ordens de Serviço proposta para o SISPAG2, se utilizada como principal meio de inserção de documentos geradores de direitos remuneratórios, possa ajudar não somente o controle subsequente, mas, também, o controle prévio. Ou seja, todas as Ordens de Serviço serão incluídas na rede interna até determinada data, para que possam ser processadas para o pagamento do respectivo período, ficando vedada a inclusão de parcelas

relativas a documentos ainda não incluídos. Nessa sistemática, a pressão sobre a implantação de parcelas passaria da equipe de pagamento para o encarregado de elaborar as Ordens de Serviço. Dessa forma, acabaria com situações como uma Ordem de Serviço com mais de dez páginas, que chega para ser incluída no meio do último dia das alterações de pagamento, aumentando as possibilidades de erros do processo. Assim, diversos riscos relativos à recepção intempestiva de documentos com parcelas para implantação serão mitigados.

Nos treinamentos a serem realizados, tanto para a equipe de TI quanto para os usuários finais, devem ser incluídos pontos voltados para uma maior conscientização de seus participantes para evitar que informações cheguem a pessoas indevidas. Nesses pontos, os treinamentos podem colaborar com o controle na redução das oportunidades para que fraudes possam ocorrer.

Devem ser realizadas, ainda, auditorias internas inopinadas, ou para atender a demandas específicas, por pessoal qualificado da organização. Devem, periodicamente, ser realizadas auditorias externas por pessoal qualificado de fora da organização. Para isso, pode ser solicitada formalmente pela PAPEM ou DFM a atuação de uma equipe de auditoria de sistemas da Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM).

Em conformidade com o que foi exposto pelo presente estudo, considera-se que o mesmo atingiu seu objetivo geral, ou seja, contribuiu efetivamente para o aprimoramento do controle interno dos sistemas de informação governamentais e, mais especificamente, do Sistema de Pagamento de Pessoal da Marinha.

Ao se confrontar os achados com o plano de referência teórico que deu fundamento a esse estudo, considera-se que o sistema de controle interno utilizado pelo sistema de pagamento de pessoal da Marinha do Brasil está parcialmente de acordo com o referencial teórico. Dessa forma, foram cumpridos os dois primeiros objetivos específicos do estudo, pela revisão da literatura sobre controle interno com a identificação de melhores práticas aplicáveis aos sistemas de informação e pela analise da adequação do processo de modernização do SISPAG ao referencial teórico.

A aplicação da análise SWOT permitiu identificar os pontos a explorar e a gerenciar no SISPAG, levando, assim, ao alcance do terceiro objetivo específico proposto.

Nenhuma ilegalidade ou irregularidade foi encontrada pelo presente estudo, mas, quanto ao que se têm como melhores práticas de controle interno, o sistema ainda apresenta pendências.

Em face do exposto e em resposta ao problema de pesquisa, pode-se dizer que o sistema de controle interno utilizado pelo Sistema de Pagamento de Pessoal da Marinha do

Brasil atende às leis, regulamentos e demais normas vigentes na esfera federal e, parcialmente, ao que prevê o referencial teórico e os estudos acadêmicos sobre o assunto.

Os sistemas de controle da administração pública devem despertar para o fato de que o descrédito pode nascer dentro da própria organização, se acomodar com as escassas vitórias no combate aos erros e fraudes identificados, e isto deve ser considerado uma atitude inconsistente com a manutenção da máquina pública e dos interesses da população. Portanto, deve-se continuar na busca incessante do aperfeiçoamento dos processos e rotinas, pois sempre haverá muito a fazer para um atendimento adequado ao cidadão.

No decorrer do estudo, puderam ser identificados alguns pontos que carecem de aprofundamento em estudos posteriores. Nesse contexto, sugere-se como pesquisa uma análise da viabilidade de integração entre diferentes sistemas governamentais, como o SISPAG2 e o Imposto de Renda de Pessoa Física da Receita Federal, para que os mesmos possam cruzar informações e identificar possíveis usos indevidos dos recursos públicos.

REFERÊNCIAS

ACFE. Association of Certified Fraud Examiners. *Report to the nations* on occupational fraud and abuse. Global Fraud Study. 2010. 84p.

ALMEIDA, Marcelo Cavalcanti. *Auditoria:* um curso moderno e completo. 7. ed. São Paulo: Atlas, 2010. 517p.

ALMEIDA, Sergio Henrique da Silva. *Auditoria em Sistema de Pagamento de Pessoal do Ministério da Marinha***:** Um Estudo de Caso. 1997. 83p. Dissertação (Mestrado em Ciências Contábeis) - Faculdade de Administração e Finanças, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 1997.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR 10006***:** Gestão da qualidade: diretrizes para a qualidade no gerenciamento de projetos. Rio de Janeiro, ABNT, dez. 2000.

ASSOCIAÇÃO PARA PROMOÇÃO DA EXCELÊNCIA DO SOFTWARE BRASILEIRO. *MPS.BR - Melhoria de Processo do Software Brasileiro*: Guia Geral. Campinas, SP: SOFTEX, 2011. 57p. Disponível em: <http://www.softex.br/mpsbr/_guias/guias/MPS.BR_Guia_Geral_2011.pdf >. Acesso em: 7 fev. 2012.

AUDY, Jorge Luis Nicolas; ANDRADE, Gilberto Keller de; CIDRAL, Alexandre. *Fundamentos de sistemas de informação*. Porto Alegre: Bookman, 2005. 208p.

AXELROD, C. Warren. Creating Data from Applications for Detecting Stealth Attacks. *Crosstalk* − The Journal of Defense Software Engineering, v. 24, n. 5, p. 19-24, sep. /oct. 2011. Disponível em: < http://www.crosstalkonline.org/storage/issuearchives/2011/201109/ 201109-0-Issue.pdf >. Acesso em: 7 fev. 2012.

AZEVEDO, Maria Thereza Lopes de; LIMA, Manuel Messias Pereira; LIMA, Ana Luiza Pereira. *Introdução à contabilidade pública*. Rio de Janeiro: Freitas Bastos, 2004. 332p.

BELCHIOR, Miriam. Entrevista: Miriam Belchior toma posse no ministério do Planejamento e garante ampliação dos investimentos... /Regina Alvarez e Cristiane Jungblut: depoimento de 03 jan. 2011. *O Globo*, Rio de Janeiro, 03 jan. 2011. Disponível em: <http://oglobo.globo.com/pais/mat/2011/01/03/miriam-belchior-toma-posse-no-ministerio-do-planejamento-garante-ampliacao-dos-investimentos-publicos-923409010.asp >. Acesso em 21 jan. 2012.

BORGES, Tiago Nascimento; PARISI, Cláudio; GIL, Antonio de Loureiro. *O Controller como gestor da Tecnologia da Informação: realidade ou ficção? Revista de Administração Contemporânea*, Curitiba, v. 9, n. 4, [p. 1-17], dez. 2005. Disponível em: <http://www.anpad.org.br/rac/vol_09/dwn/rac-v9-n4-tnb.pdf>. Acesso em: 17 set. 2011.

BRASIL. Constituição (1967). Constituição da República Federativa do Brasil**.** *Diário Oficial [da] República Federativa do Brasil,* Brasília, DF, 24 jan. 1967. Seção 1. Disponível em:

<http://www.planalto.gov.br/ccivil_03/constituicao/Constitui%C3%A7ao67.htm>. Acesso em: 29 dez. 2011.

_____. Constituição (1967). Emenda Constitucional nº 1, de 17 de outubro de 1969. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 18 out. 1969. Seção 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/Constitui%C3%A7ao67.htm>. Acesso em: 24 ago. 2011.

_____. Constituição (1988). *Constituição da República Federativa do Brasil*: promulgada em 5 de outubro de 1988. Atualizada até a Emenda Constitucional n˚ 62 de 9 de dezembro de 2009. 44. ed. São Paulo: Saraiva, 2010. 432p.

_____. Decreto-lei nº 200, de 25 de fevereiro de 1967. Dispõe sôbre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 26 fev. 1967. Seção 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del0200.htm>. Acesso em: 1 set. 2011.

_____. Decreto nº 2.028, de 11 de outubro de 1996. Dispõe sobre os procedimentos relativos à execução financeira da folha de pagamento de pessoal do Governo Federal e dá outras providências. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 14 out. 1996. Seção 1, p. 24. Disponível em: <http://www.in.gov.br/imprensa/visualiza/index.jsp?jornal=1&pagina=24&data=14/10/1996>. Acesso em: 7 fev. 2012.

_____. Decreto nº 3.591, de 6 de setembro de 2000. Dispõe sobre o Sistema de Controle Interno do Poder Executivo Federal e dá outras providências. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 8 set. 2000. Seção 1, p. 193. Disponível em: <http://www.in.gov.br/imprensa/visualiza/index.jsp?jornal=1&pagina=193&data=08/09/2000>. Acesso em: 7 fev. 2012.

_____. Decreto nº 4.307, de 18 de julho de 2002. Regulamenta a Medida Provisória no 2.215-10, de 31 de agosto de 2001, que dispõe sobre a reestruturação da remuneração dos militares das Forças Armadas, altera as Leis nos 3.765, de 4 de maio de 1960, e 6.880, de 9 de dezembro de 1980, e dá outras providências. *Diário Oficial [da] República Federativa do Brasil,Brasília*, DF, 19 jul. 2002. Seção 1, p. 2. Disponível em: <http://www.in.gov.br/imprensa/visualiza/index.jsp?jornal=1&pagina=2&data=19/07/2002>. Acesso em: 7 fev. 2012.

_____. Decreto nº 4.536, de 28 de janeiro de 1922. Organiza o Código de Contabilidade da União. *Diário Oficial [da] República Federativa do Brasil, Brasília*, DF, 29 jan. 1922. Seção 1. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto/historicos/dpl/dpl4536.htm>. Acesso em: 8 ago. 2011.

_____. Decreto nº 92.452, de 10 de março de 1986. Cria, no Ministério da Fazenda, a Secretaria do Tesouro Nacional (STN), extingue a Secretaria Central de Controle Interno (SECIN), e dá outras providências. *Diário Oficial [da] República Federativa do Brasil,Brasília*, DF, 11 mar. 1986. Seção 1. Disponível em: <http://www6.senado.gov.br/legislacao/ListaPublicacoes.action?id=130053>. Acesso em: 8 ago. 2011.

_____. Lei Complementar n.º 101, de 4 de maio de 2000. Estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal e dá outras providências. *Diário Oficial [da] República Federativa do Brasil,* Brasília, DF, 5 maio 2000. Seção 1, p. 82. Disponível em: <http://www.in.gov.br/imprensa/visualiza/index.jsp?jornal=1&pagina=82&data=05/05/2000> . Acesso em: 7 fev. 2012.

_____. Lei Complementar n.º 131, de 27 de maio de 2009. Acrescenta dispositivos à Lei Complementar nº 101, de 4 de maio de 2000, que estabelece normas de finanças públicas voltadas para a responsabilidade na gestão fiscal e dá outras providências, a fim de determinar a disponibilização, em tempo real, de informações pormenorizadas sobre a execução orçamentária e financeira da União, dos Estados, do Distrito Federal e dos Municípios. *Diário Oficial [da] República Federativa do Brasil,* Brasília, DF, 28 maio 2009. Seção 1, p. 2. Disponível em: <http://www.in.gov.br/imprensa/visualiza/index.jsp?jornal=1&pagina=2&data=28/05/2009>. Acesso em: 7 fev. 2012.

_____. Lei nº 6.880, de 9 de dezembro de 1980. Dispõe sobre o Estatuto dos Militares. *Diário Oficial [da] República Federativa do Brasil,* Brasília, DF, 10 dez. 1980. Seção 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L6880.htm>. Acesso em: 26 nov. 2011.

_____. Lei nº 10.180, de 6 de fevereiro de 2001. Organiza e disciplina os Sistemas de Planejamento e de Orçamento Federal, de Administração Financeira Federal, de Contabilidade Federal e de Controle Interno do Poder Executivo Federal, e dá outras providências. *Diário Oficial [da] República Federativa do Brasil,* Brasília, DF, 7 fev. 2001. Seção 1, p. 2. Disponível em: <http://www.in.gov.br/imprensa/visualiza/index.jsp?jornal=1&pagina=2&data=07/02/2001>. Acesso em: 7 fev. 2012.

_____. Lei nº 12.381, de 9 de fevereiro de 2011. Estima a receita e fixa a despesa da União para o exercício financeiro de 2011. *Diário Oficial [da] República Federativa do Brasil,* Brasília, DF, 10 fev. 2011. Seção 1, p. 1. Disponível em: <http://www.in.gov.br/imprensa/visualiza/index.jsp?jornal=1&pagina=1&data=10/02/2011>. Acesso: 7 fev. 2012.

_____. Lei nº 4.320, de 17 de março de 1964. Estatui Normas Gerais de Direito Financeiro para elaboração e controle dos orçamentos e balanços da União, dos Estados, dos Municípios e do Distrito Federal. *Diário Oficial [da] República Federativa do Brasil,* Brasília, DF, 23 mar. 1964. Seção 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L4320.htm>. Acesso em: 5 ago. 2011.

_____. Marinha. Diretoria de Finanças. *Edital de Licitação nº 06/2009*. Rio de Janeiro: DFM, 17 jul. 2009.

_____. _____. Pagadoria de Pessoal da Marinha. *Lema*. Rio de Janeiro: PAPEM, [1997]. Disponível em: <http://www.mar.mil.br/papem/>. Acesso em: 7 fev. 2012.

_____. _____. _____ *Calendário do Quarto Trimestre - País*. Rio de Janeiro: PAPEM, 2011. Disponível em: <http://www.mar.mil.br/papem/>. Acesso em: 29 set. 2011.

_____. _____. _____. *Portaria nº 9/PAPEM, de 3 de setembro de 2008*. Aprova o Regimento Interno da PAPEM. Rio de Janeiro: PAPEM, 2008. 23p.

_____. _____. _____. *Relatório de Gestão do Exercício de 2009*. Rio de Janeiro: PAPEM, 2010.

_____. _____. Secretaria-Geral. *SGM-302 - Normas sobre Pagamento de Pessoal na MB*. 3. rev. Brasília: Marinha do Brasil, 2007.

_____. _____. _____. *SGM-302 - Normas sobre Auditoria, Análise e Apresentação de Contas na Marinha*. 4. rev. Brasília: Marinha do Brasil, 2010.

_____. Ministério da Fazenda. Secretaria Federal de Controle Interno. *Instrução Normativa nº 01/01*. Brasília, DF: Ministério da Fazenda, 2001.

_____. Ministério do Planejamento, Orçamento e Gestão. *PPA 2012-2015 PREVÊ R$ 5,4 TRILHÕES ATÉ 2015*. Brasília: MPOG, 31 ago. 2011. Disponível em: <http://www.planejamento.gov.br/noticia.asp?p=not&cod=7573&cat=47&sec=8>. Acesso em: 29 dez. 2011.

_____. Senado Federal. Secretaria de Controle Interno. *Princípios de Controles Internos*. Brasília: Senado Federal, 2011. Disponível em: <http://www.senado.gov.br/sf/senado/scint/insti/controles_internos_02_principios.asp>. Acesso em: 29 dez. 2011.

BRESSER-PEREIRA, Luiz Carlos. *DO ESTADO PATRIMONIAL AO GERENCIAL*. In PINHEIRO, Wilheim; SACHS (Orgs.). *Brasil*: Um Século de Transformações. São Paulo: Cia. das Letras, 2001: p. 222-259.

_____. Estado, Sociedade Civil e Legitimidade Democrática. *Lua Nova*: Revista de Cultura e Política, São Paulo, n. 36, p. 85-200, 1995. Disponível em: <http://www.scielo.br/pdf/ln/n36/a06n36.pdf >. Acesso em: 07 fev. 2012.

CARDOZO, Julio Sergio de Souza. Controles Internos: Conceitos, Objetos e Princípios. *Revista Brasileira de Contabilidade*. ano 23, n. 87, p. 34-41, jun. 1994.

CARVALHO, Kildare Gonçalves. *Direito constitucional*. 14. ed., rev. atual. e ampl. Belo Horizonte: Del Rey, 2008. 1352p.

CARVALHO FILHO, José dos Santos. *Manual de direito administrativo*, 11. ed., Rio de Janeiro: Lumen Júris, 2004.

CONSELHO FEDERAL DE CONTABILIDADE (Brasil). Resolução CFC nº 986/03. Aprova a Norma Brasileira de Contabilidade TI 01 – Da Auditoria Interna. *Ata CFC nº 850,* Brasília, DF, 21 nov. 2003. Disponível em: <http://www.cfc.org.br/sisweb/sre/detalhes_sre.aspx?Codigo=2003/000986>. Acesso em: 7 fev. 2012.

_____. Resolução CFC nº 1.129/08. Aprova a Norma Brasileira de Contabilidade T 16.2 – Patrimônio e Sistemas Contábeis. Ata CFC nº 919, Brasília, DF, 21 nov. 2008. Disponível em: <http://www.cfc.org.br/sisweb/sre/detalhes_sre.aspx?Codigo=2008/001129>. Acesso em: 7 fev. 2012.

_____. Resolução CFC nº 1.132/08. Aprova a Norma Brasileira de Contabilidade T 16.5 – Registro Contábil. Ata CFC nº 919, Brasília, DF, 21 nov. 2008. Disponível em: <http://www.cfc.org.br/sisweb/sre/detalhes_sre.aspx?Codigo=2008/001132>. Acesso em: 7 fev. 2012.

_____. Resolução CFC nº 1.135/08. Aprova a Norma Brasileira de Contabilidade T 16.8 – Controle Interno. Ata CFC nº 919, Brasília, DF, 21 nov. 2008. Disponível em: <http://www.cfc.org.br/sisweb/sre/detalhes_sre.aspx?Codigo=2008/001135>. Acesso em: 7 fev. 2012.

_____. Resolução CFC nº 1.203/09. Aprova a Norma Brasileira de Contabilidade TA 200 – Objetivos Gerais do Auditor Independente e a Condução da Auditoria em Conformidade com Normas de Auditoria. Ata CFC nº 931, Brasília, DF, 27 nov. 2009. p. 1-25. Disponível em: <http://www.cfc.org.br/sisweb/sre/detalhes_sre.aspx?Codigo=2009/001203>. Acesso em: 7 fev. 2012.

_____. Resolução CFC nº 1.374/11. Dá nova redação à Norma Brasileira de Contabilidade TG Estrutura Conceitual – Estrutura Conceitual para Elaboração e Divulgação de Relatório Contábil-Financeiro. Ata CFC nº 959, Brasília, DF, 8 dez. 2011. Disponível em: <http://www.cfc.org.br/sisweb/sre/detalhes_sre.aspx?Codigo=2011/001374>. Acesso em: 7 fev. 2012.

CONTROLADORIA GERAL DO MUNICÍPIO DO RIO DE JANEIRO. *Planejamento estratégico em auditoria, auditoria baseada em risco*. Rio de Janeiro: Controladoria Geral, 2004. 35p.

CMMI PRODUCT DEVELOPMENT TEAM. *CMMI for Acquisition, Version 1.3*. University Pittsburgh, PA. : Software Engineering Institute Carnegie Mellon, nov. 2010. 423p. Disponível em: <http://repository.cmu.edu/cgi/viewcontent.cgi?article=1277&context=sei>. Acesso em: 20 jan. 2012.

COLLIS, J.; HUSSEY, R.. *Pesquisa em administração*: um guia prático para alunos de graduação e pós-graduação. 2. ed. Porto Alegre: Bookman, 2005. 348p.

COOK, J. W.; WINKLE, G.M. *Auditoria*: filosofia e técnica. São Paulo: Saraiva, 1979.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. *Internal Control - Integrated Framework.* [s.l.: s.n., 1992]. Disponível em: <http://www.coso.org/documents/Internal%20Control-Integrated%20Framework.pdf >. Acesso em: 20 jan. 2012.

_____. *Enterprise Risk Management — Integrated Framework*: Executive Summary. [s.l.: s.n.], set. 2004. Disponível em: <http://www.coso.org/documents/COSO_ERM_Executive Summary.pdf>. Acesso em: 20 jan. 2012.

_____. *Internal Control — Integrated Framework*. Guidance on Monitoring Internal Control Systems. [s.l.: s.n.], jun. 2008. Disponível em: <http://www.coso.org/documents/VolumeII-Guidance.pdf>. Acesso em: 9 jun. 2011.

_____. *About Us*. Disponível em: < http://www.coso.org/aboutus.htm>. Acesso em: 20 jan. 2012.

COSTA, Alan Gonzaga da. SIAFI e as finanças governamentais: uma abordagem holística. 1998. 45 p. In: PRÊMIO TESOURO NACIONA DE MONOGRAFIA, 3., 1998. *Anais Eletrônicos...* Brasília: Ministério da Fazenda, Escola de Administração Fazendária, Diretoria de Cooperação Técnica e Pesquisa, out. 1998. Disponível em: <http://stn.gov.br/Premio_TN/conteudo_mono.html>. Acesso em: 15 out. 2011.

COSTÓDIO FILHO, Ubirajara. A Emenda Constitucional 19/98 e o Princípio da Eficiência na Administração Pública. *Revista de Direito Constitucional e Internacional*: Cadernos de Direito Constitucional e Ciência Política, São Paulo, n. 27, p. 209-217, abr./jul. 1999.

CREPALDI, Silvio Aparecido. *Auditoria contábil*: teoria e prática. São Paulo: Atlas, 2000. 477 p.

CRUZ, Flávio da. *Auditoria governamental*. São Paulo: Atlas, 1997. 256 p.

CRUZ, Flávio; GLOCK, José Osvaldo. *Controle interno nos municípios*: orientação para a implantação e relacionamento com os tribunais de contas. São Paulo: Atlas, 2003. 164p.

DAVIS, Marcelo David. *A importância da gestão de riscos nos sistemas de controle interno da administração pública:* aplicação em uma organização militar prestadora de serviços. 2006. 109 p. Dissertação (Mestrado em Ciências Contábeis)- Faculdade de Administração e Finanças, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2006.

DELOITTE. *GCC fraud survey*: Facing the challenge of fraud. May 2011. 16 p. Disponível em: <http://www.kpmg.com.au/aci/docs/Fraud-Survey-2004.pdf>. Acesso em: 12 set. 2011.

DELOITTE. *Lei Sarbanes-Oxley*. Guia para melhorar a governança corporativa através de eficazes controles internos. Brasil, 2003. 28p. Disponível em: <http://www.deloitte.com/ assets/DcomBrazil/Local%20Assets/Documents/guia_sarbanes_oxley%281%29.pdf>. Acesso em: 7 fev. 2012.

DIAS, Leonardo Cardoso; MENNA, Romulo da Silva. *Teste de desempenho a partir de modelos UML para componentes de software*. 2008. 60 p. Monografia (Graduação em Ciência da Computação)-Faculdade de Informática, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2008. Disponível em: <http://revistaseletronicas.pucrs.br/ojs/index.php/graduacao/article/viewFile /2547/2156>. Acesso em: 7 nov. 2011.

DUNN, John. *Auditing*: theory and practice. Hemel Hempstead: Prentice Hall, 1991. 267 p.

FINANCIAL ACCOUNTING STANDARDS BOARD OF THE FINANCIAL ACCOUNTING FOUNDATION. *Statement of Financial Accounting Concepts No. 2*: Qualitative Characteristics of Accounting Information. Norwalk, Connecticut: FASB, May

1980. Disponível em: <http://www.fasb.org/cs/BlobServer?blobcol=urldata&blobtable=MungoBlobs&blobkey=id&blobwhere=1175820900499&blobheader=application%2Fpdf>. Acesso em: 20 jan. 2012.

FRANCO, H.; MARRA, E. *Auditoria contábil*. 4. ed. São Paulo: Atlas, 2001.

GHERBI, Abdelouahed; CHARPENTIER, Robert; COUTURE, Mario. Software Diversity for Future Systems Security. *Crosstalk*: The Journal of Defense Software Engineering. v. 24, n. 5, p. 10-13, Sep. /Oct. 2011. Disponível em: <http://www.crosstalkonline.org/storage/issue-archives/2011/201109/201109-0-Issue.pdf >. Acesso em: 20 jan. 2012.

GIACOMONI, James. *Orçamento Público*. 15. ed. São Paulo: Atlas, 2010. 369 p.

GIL, A. C. *Técnicas de pesquisa em economia e elaboração de monografias***.** 3. ed. São Paulo: Atlas, 2000. 217p.

GIL, Antonio de Loureiro. *Auditoria de computadores*. 3. ed. São Paulo: Atlas, 1998. 226p.

HABERKORN, Ernesto. *Um bate-papo sobre T. I.*: tudo que você gostaria de saber sobre o ERP e tecnologia da informação, mas ficava encabulado de perguntar. São Paulo: Saraiva, 2009. 184p.

HUMPHREY, Watts S. Why Big Software Projects Fail: The 12 Key Questions. *Crosstalk:* The Journal of Defense Software Engineering, v. 18, n. 3, p. 26-29, mar.2005. Disponível em: <http://www.crosstalkonline.org/storage/issue-archives/2005/200503/200503-0-Issue.pdf >. Acesso em: 20 jan. 2012.

IBM RATIONAL. Rational: the software development company. *Rational Unified Process*: Best Practices for Software Development Teams. Rational. rev. 11/01. 18p. Disponível em: <http://www.ibm.com/developerworks/rational/library/content/03July/1000/1251/1251_bestpractices_TP026B.pdf>. Acesso em: 21 jan. 2012.

INTERNATIONAL ORGANIZATION OF SUPREME AUDIT INSTITUTIONS. *Lima Declaration of Guidelines on Auditing Precepts*. INTOSAI General Secretariat c/o Austrian Court of Audit, Dampfschiffstraße 2, A-1031 Vienna, Austria: INTOSAI, 2009. 20 p. Disponível em: < http://www.intosai.org/uploads/englisch.pdf >. Acesso em: 7 fev. 2012.

_____. *Guidelines for Internal Control Standards for the Public Sector*. Áustria: INTOSAI, 2004. 71 p.

INSTITUTE FOR INTERNATIONAL PUBLIC SECTOR ACCOUNTING STANDARDS. D*isclosure of financial information about the general government sector*. New York, USA: IPSAS, Dec. 2006. Disponível em: <http://www.ipsas.org/PDF_ipsas_standards_ifac/IPSAS22_Disclosure_General_Gov_Sector.pdf >. Acesso em: 7 fev. 2012.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION. *COBIT ® Val IT ™ based on COBIT ® Risk IT based on COBIT ®*:Frameworks and related products that help professionals attain value from information systems. Illinois, USA: ISACA, [2010]. 16p.

Disponível em: <http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT-Products.pdf>. Acesso em: 20 jan. 2012.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO/IEC 12207:2008*: Systems and software engineering: Software life cycle processes. Geneva, Switzerland: ISO, 2008. Disponível em: <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm? csnumber=43447>. Acesso em: 21 jan. 2012.

INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE. *About IT Governance*. Illinois, USA: ITGI, [2011]. Disponível em: <http://www.itgi.org/template_ITGIa166.html?Section=About_IT_Governance1&Template=/ContentManagement/HTMLDisplay.cfm&ContentID=19657>. Acesso em: 29 dez. 2011.

KERLINGER, Fred Nichols. *Metodologia da Pesquisa em Ciências Sociais*: um tratamento conceitual. São Paulo: EPU: EDUSP, 1980. 378 p.

KERSTING, Wolfgang. Hobbes, Kant, a Paz Universal e a Guerra contra o Iraque**.** *Kant e-Prints*, local, v. 3, n. 2, p. 1-13, 2004.

KLITGAARD, Robert E. *A corrupção sob controle*. tradução de Octavio Alves Velho. Rio de Janeiro: Jorge Zahar, 1994. 262 p.

KÖCHE, José C. *Fundamentos de Metodologia Científica*: teoria da ciência e prática de pesquisa. Rio de Janeiro: Vozes, 1997.

KOVACH, Stephan. *Detecção de fraudes em transações financeiras via Internet em tempo real*. 2011. 134p. Tese (Doutorado em Engenharia Elétrica) –Departamento de Engenharia de Computação e Sistemas Digitais, Universidade de São Paulo, São Paulo, 2011.

KPMG. *A Fraude no Brasil*: Relatório da Pesquisa 2009. Advisory. Brasil: KPMG, 2009. 33p. Disponível em: <http://www.kpmg.com.br/publicacoes/forensic/Fraudes_2009_port.pdf>. Acesso em: 24 jan. 2012.

_____. *KPMG Analysis of global patterns of fraud*. Who is the typical fraudster? Canadá: KPMG, 2011. 24p. Disponível em: <http://www.kpmg.com/Ca/en/IssuesAndInsights/ArticlesPublications/Documents/5879_Who%20is%20the%20typical%20fraudster_v4_web.pdf>. Acesso em: 24 jan. 2012.

LUCIANO, Edimara Mezzomo; TESTA, Mauricio Gregianin. Controles de governança de tecnologia da informação para a terceirização de processos de negócio: uma proposta a partir do COBIT. JISTEM. *Revista de Gestão da Tecnologia e Sistemas de Informação*. v. 8, n. 1, p. 237-262, 2011.

MALHOTRA, Naresh K. *Pesquisa de marketing*: uma orientação aplicada. 4. ed. Porto Alegre: Bookman, 2006. 720p.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. *Técnicas de pesquisa*: planejamento e execução de pesquisas, amostragens e técnicas de pesquisa, elaboração e interpretação de dados. São Paulo: Atlas, 1990. 231p.

MAWAD, Ana Paula de Barros. *Sistema de Informação e Cidadania*: Um Desafio na Gestão de Recursos Públicos. Brasília: ESAF, 2001. 59 p. In: PRÊMIO TESOURO NACIONAL, 7., 2001, Brasília.. *Anais Eletrônicos...* Brasília, DF: Tesoouro Nacional, 2001. Disponível em: <http://stn.gov.br/Premio_TN/conteudo_mono.html>. Acesso em: 21 jan. 2012.

MEIRELLES, Hely Lopes. *Direito Administrativo Brasileiro*. 29. ed. São Paulo: Malheiros, 2004. 798 p.

MERCADANTE, Aloizio. Devemos Aprender A Fazer Mais Com Menos. *O Estado de S. Paulo*, São Paulo, 03 jan. 2011. Disponível em: <http://www.estadao.com.br/noticias/nacional,mercadante-devemos-aprender-a-fazer-mais-com-menos,661452,0.htm>. Acesso em: 21 jan. 2012.

MOSCOVE, S. A., SIMKIN, M. G., BAGRANOFF, N. A. *Sistemas de Informações Contábeis*. São Paulo: Atlas, 2002.

NASCIMENTO, Leonardo do; CHERMAN, Bernardo. *Contabilidade Pública*. Rio de Janeiro: Ferreira, 2007. 576p.

NETTO, Abner da Silva; SILVEIRA, Marco Antonio Pinheiro da. Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. *Revista de Gestão da Tecnologia e Sistemas de Informação*. Journal of Information Systems and Technology Management, v. 4, n. 3, p. 375-397, 2007.

NOTTINGHAM, Mark; HAMMER-LAHAV, Eran. RFC 5785. *Defining Well-Known Uniform Resource Identifiers (URIs)*. [s.l.: s.n.], Abr. 2010. Disponível em: <http://www.rfc-editor.org/rfc/pdfrfc/rfc5785.txt.pdf>. Acesso em: 7 fev. 2012.

NUNES, Selene Peres Peres. Entrevista. *Revista do Tribunal de Contas do Estado de Minas Gerais*, Belo Horizonte: ano 29, ed. Especial, p. 15-33, 2011. Disponível em: <http://200.195.70.14/Revista/Content/Upload/Materia/1162.pdf>. Acesso em: 29 dez. 2011.

OLIVEIRA, Lílian Simão; QUEIROZ-NETO, José Pinheiro de; MAETA, Silvio M. A usabilidade em interfaces interativas no desenvolvimento de aplicativos para tv digital. In: CONGRESSO DE PESQUISA E INOVAÇÃO DA REDE NORTE NORDESTE DE EDUCAÇÃO TECNOLÓGICA, 2., 2007, João Pessoa. *Anais Eletrônicos...*João Pessoa: [s.n], 2007. Disponível em: <http://www.redenet.edu.br/publicacoes/arquivos/20080110_150450_INFO-002.pdf>. Acesso em: 21 jan. 2012.

OBJECT MANAGEMENT GROUP. *Introduction to OMG's Unified Modeling Language™ (UML®)*. Updated July 2005 to reflect formal adoption of UML 2.0 Superstructure. Needham, MA, USA: OMG, 2005. Disponível em: < http://www.omg.org/gettingstarted/what_is_uml.htm>. Acesso em: 07 fev. 2012.

PADOVEZE, Clóvis Luís. *Sistemas de informações contábeis*: fundamentos e análise. 2. ed. São Paulo: Atlas, 2000.

_____. *Controladoria avançada*. São Paulo: Pioneira Thomson Learning, 2005. 326p.

PARODI, Lorenzo. *Manual de Fraudes*. Rio de Janeiro: Brasport, 2005. 242p.

PEIXE, Blênio César Severo. *Finanças Públicas*: controladoria governamental. Curitiba: Juruá, 2006. 252p.

PETER, Maria da Glória Arrais; MACHADO, Marcus Vinícius Veras. *Manual de auditoria governamental*. São Paulo: Atlas, 2003. 241p.

PROJECT MANAGEMENT INSTITUTE. *Sobre o PMI*. Brasil: PMI, 2007. Disponível em: <http://www.pmi.org.br>. Acesso em: 21 jan. 2012. 1p.

POLLONI, Enrico Giulio Franco. *Administrando sistemas de informação*. São Paulo: Futura, 2000. 284p.

QUADRA, Léo Fernandes. *A aplicação do balanced scorecard em uma organização militar pagadora*: um estudo de caso. 2000. 76p. Dissertação (Mestrado em Ciências Contábeis) – Faculdade de Administração e Finanças, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2000.

QUINTANA, Alexandre Costa; MACHADO, Daiane Pias; QUARESMA, Jozi Cristiane da Costa; MENDES, Roselaine da Cruz. *Contabilidade pública*: de acordo com as novas normas brasileiras de contabilidade aplicadas ao setor público e a lei de responsabilidade fiscal. São Paulo: Atlas, 2011. 243 p.

REZENDE, Denis Alcides. *Engenharia de software e sistemas de informação*. 3. ed. rev. e ampl. Rio de Janeiro: Brasport, 2005. 344p.

RIBEIRO, Renato Jorge Brown. O Problema Central do Controle da Administração Pública pode ser resumido ao Debate sobre Modelos? *Revista do Tribunal de Contas da União*, Brasília, v.33, n. 93, p. 55-73, jul./set. 2002.

RIBEIRO FILHO, José Francisco. Controle Gerencial para Entidades da Administração Pública. 1997. 76 p. In: PRÊMIO TESOURO NACIONAL DE MONOGRAFIA. 2., 1997. *Anais eletrônicos...* Brasília: Ministério da Fazenda, Escola de Administração Fazendária, Diretoria de Cooperação Técnica e Pesquisa, set. 1997. Disponível em: <http://stn.gov.br/Premio_TN/conteudo_mono.html>. Acesso em: 21 jan. 2012.

ROBIC, André Ricardo; SBRAGIA, Roberto. Sucesso em Projetos de Informatização: Critérios de Avaliação e Fatores Condicionantes. *Caderno de Pesquisas em Administração*, São Paulo, v.1, n.1, p.1-11, jan./jul. 1996.

SÁ, Antônio Lopes de. *Curso de auditoria*. 8. ed. rev. ampl. atual. São Paulo: Atlas, 1998. 533p.

SANTOS, Ismayle Sousa; RESENDE, Rodolfo S. Ferreira de; NETO, Pedro Alcântara Santos; PADUA, Clarindo Isaias P. da Silva e. Requisitos e aspectos técnicos desejados em Ferramentas de testes de software: um estudo a partir do uso do SQFD. *Revista Eletrônica de Sistemas de Informação*, v. 9, n. 2, [p. 1-21], 2010.

SANTOS, Waldir Jorge Ladeira. *Financiamento e investimento da educação nos municípios de Duque de Caxias e de Nova Iguaçu – RJ*: avaliação da eficácia, da efetividade e da transparência das políticas públicas. 2010. 300f. Tese (Doutorado em Políticas Públicas e Formação Humana). Programa de Pós-graduação em Políticas Públicas e Formação Humana. Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2010.

SARENS, Gerrit; CHRISTOPHER, Joe. The association between corporate governance guidelines and risk management and internal control practices. Evidence from a comparative study. *Managerial Auditing Journal*, v. 25, n. 4, p. 288-308, 2010.

SILVA, Lino Martins da**.** *Contabilidade governamental***:** um enfoque administrativo da nova contabilidade pública. 8. ed. São Paulo: Atlas, 2009.

_____. *Análise do Sistema de Controle Interno*: Passado – Presente – Futuro. In: PALESTRA, 2000, Rio de Janeiro. *Anais Eletrônicos...* Rio de Janeiro:TCMRJ, 06 nov. 2000. Disponível em: <http://www.tcm.rj.gov.br/Noticias/147/TCMRJ.pdf>. Acesso em: 21 jan. 2012.

_____. *Tribunais de contas e a informação como ativo*: As armadilhas da LC 131/2009. Blog [Internet. s.n.]: Lino Martins Silva, 22 jan. 2012. Disponível em: <http://linomartins.wordpress.com/>. Acesso em: 25 jan. 2012.

SILVA, Luciano Carlos da. *Banco de Dados para a Web do Planejamento à Implementação*. São Paulo: Érica, 2001. 242p.

SILVA, Nelson Peres da. *Projeto e Desenvolvimento de Sistemas*. 5. ed. São Paulo: Érica, 1998. 145p.

SILVA, R. C. Controle organizacional, cultura e liderança: evolução, transformações e perspectivas. *RAP*, Rio de janeiro, v. 37, n. 4, p. 797-816, jul./ago. 2003.

SILVA, S. M., GUIMARÃES, I. C., PEREIRA, A. C. Controles Internos Contábeis nas Empresas. In: CONGRESSO BRASILEIRO DE CONTABILIDADE, 17., 2004, Santos. *Anais...*Santos: CFC, 2004.

SLOMSKI, Valmor. *Manual de contabilidade pública*: um enfoque na contabilidade municipal, de acordo com a Lei de Responsabilidade Fiscal. 2. ed. São Paulo: Atlas, 2003. 475 p.

TOMPKINS, Jonathan R. *Organization Theory and Public Management*. Boston, MA: Wadsworth Cengage Learning, 2005.

TURBAN, Efraim; LEIDNER, Dorothy; MCLEAN, Ephraim; WETHERBE, James. *Tecnologia da Informação para Gestão*. 6. ed. Porto Alegre: Bookman, 2010. 720p.

VIEIRA, S. A. A auditoria e os sistemas de controles internos no Brasil: antecedentes e evolução. *Revista de Economia Mackenzie*. v. 5, n. 5, p. 175-193, 2007.

YIN, Robert K. *Estudo de caso*: planejamento e métodos. 4. ed. Porto Alegre: Bookman, 2010. 248p.

WERNER, Baer. *A economia brasileira*; tradução de Edite Sciulli. 3. ed. rev. ampl. atual. São Paulo: Nobel, 2009. 541 p.

WEYGANDT, Jerry J.; KIMMEL, Paul D.; KIESO, Donald E. *Financial Accounting, IFRS Edition*. New Jersey: John Wiley & Sons, 2011. 707 p.

APÊNDICE A- Requisitos funcionais do SISPAG2

1. GENÉRICOS REUTILIZÁVEIS
Requisito Funcional
1.1. Incluir automaticamente informações pessoais e funcionais de uma pessoa.
1.2. Incluir informações pessoais e funcionais de uma pessoa.
1.3. Controlar autoria do comando.
1.4. Atribuir automaticamente informações financeiras durante a inclusão de uma RR no SISPAG.
1.5. Incluir informações financeiras de uma RR.
1.6. Realizar críticas nos comandos pessoais e funcionais.
1.7. Realizar críticas nos comandos financeiros.
1.8. Controlar a integridade dos comandos referentes à mesma pessoa.
1.9. Consultar informações gerais, pela interface on-line.
1.10. Permitir a realização de Pré-Cálculo

Fonte: Elaborado pelo autor com dados de DFM (2009).

2. MÓDULO DE CAPTAÇÃO DE DADOS (MOD-CD)	
Categoria	**Requisito Funcional**
Tratamento de Pessoa	2.1. Incluir uma pessoa, pela interface on-line.
	2.2. Excluir uma pessoa, pela interface on-line.
	2.3. Alterar informações pessoais e funcionais de uma Pessoa, pela interface on-line.
Tratamento de Relação de Remuneração (RR)	2.4. Incluir uma relação de remuneração (RR), pela interface on-line.
	2.5. Alterar informações funcionais de uma RR, pela interface on-line.
	2.6. Excluir uma relação de remuneração (RR), pela interface on-line.
	2.7. Terminar uma Relação de Remuneração (RR), pela interface on-line.
	2.8. Comandar a movimentação de RR para outra OM, pela interface on-line.
	2.9. Comandar a suspensão de uma RR, pela interface on-line.
	2.10. Comandar a reativação de uma RR suspensa, pela interface on-line.
	2.11. Comandar a suspensão de RR em bloco, pela interface on-line.
	2.12. Comandar a reativação de RR suspensas em bloco, pela interface on-line.
	2.13. Comandar a condição de "em Acerto de Contas" para uma RR, pela interface on-line.
Captação de Informações Financeiras de Relação de Remuneração (RR)	2.14. Incluir informações financeiras de uma RR.
	2.15. Alterar informações financeiras de uma RR.
	2.16. Excluir informações financeiras de uma RR.
	2.17. Comandar a inclusão de informações financeiras de RR em bloco, pela interface on-line.
	2.18. Comandar a alteração de informações financeiras de RR em bloco, pela interface on-line.
	2.19. Comandar a exclusão de informações financeiras de RR em bloco, pela interface on-line.
	2.20. Comandar a suspensão de uma Parcela RR, pela interface on-line.
	2.21. Comandar a reativação de uma Parcela RR suspensa, pela interface on-line.
Relação de Remuneração (RR) em Situação Especial no País	2.22. Sinalizar uma RR como "em Situação Especial no País", pela interface on-line.
	2.23. Alterar a informação de datas de início/término da "Situação Especial no País" e de "informações de dependentes" de uma RR "em Situação Especial no País", pela interface on-line.
	2.24. Alterar a informação do Documento de Designação da Comissão de uma RR "em Situação Especial no País", pela interface on-line.
	2.25. Excluir a Sinalização de "Situação Especial no País" de uma RR, pela interface on-line.
Acerto de comandos prévios	2.27. Acertar comandos armazenados no arquivo "Dados Coletados", pela interface on-line.
	2.28. Sinalizar, pela interface on-line, que existem comandos de pagamento rejeitados, armazenados no arquivo "Dados Coletados".
	2.29. Criticar automaticamente o arquivo "Dados coletados".
Elaboração de Ordem de Serviço	2.30. Elaborar Ordem de Serviço, pela interface on-line.
Operacionalizações Especiais	2.31. Operacionalizar o pagamento de diferenças financeiras relativas a exercícios

	anteriores, pela interface on-line.
	2.32. Operacionalizar o ressarcimento de adiantamentos imediatos pela interface on-line.
	2.33. Operacionalizar o retorno de pagamentos indevidos pela interface online.
	2.34. Operacionalizar os pagamentos eventuais para militares retirados do SISPAG, pela interface on-line.
	2.35. Operacionalizar Rotina de Cálculo para a Retenção de Remuneração para Depósito em Conta Judicial.
	2.36. Operacionalizar pagamentos eventuais por motivos diversos, pela interface on-line.
	2.37. Operacionalizar pagamentos de Auxílio-Funeral, pela interface on-line.
	2.38. Operacionalizar a verificação do CPF entre o SISPAG e a Receita Federal.
	2.39. Operacionalizar a suspensão de uma Parcela Geral, pela interface on-line.
	2.40. Comandar a reativação de uma Parcela Geral suspensa, pela interface on-line.
	2.41. Atribuir parcelas RR em casos especiais de alteração de dados pessoais e/ou funcionais.
Controle das interfaces	2.42. Definir o cronograma do processo corrente.
Aplicativos Auxiliares	2.43. Aplicativo “Portal Upload”
	2.44. Aplicativo “ED para Contingência”
	2.45. Aplicativo “Conversor dos Comandos de Atualização”

Fonte: Elaborado pelo autor com dados de DFM (2009).

REQUISITOS FUNCIONAIS		
3. Módulo de Atualização de Dados (MOD-AD)	**4. Módulo de Cálculo da Folha Mensal de Pagamento (MOD-CF)**	**5. Módulo Interface com o Sistema Legado (MOD-INLE)**
3.1. Atualizar os dados pessoais e funcionais a partir do sistema de pessoal.	4.1. Calcular a Folha de Pagamento.	5.1. Transferir as informações da Folha de Pagamento para o sistema legado.
3.2. Simular a atualização.	4.2. Calcular o valor pecuniário das parcelas de uma RR.	5.2. Calcular Folha Suplementar.
3.3. Atualizar os dados pessoais e funcionais e financeiros a partir do arquivo “Dados Coletados”.	4.3 Atribuir parcelas RR a partir do tratamento de saldos de uma RR.	5.3. Registrar os bloqueios de pagamento ocorridos no sistema legado.
	4.5 Tratar a margem consignável da RR.	
	4.6 Tratar Margem Consignável de RR em Situação Especial no País.	
	4.7 Realizar simulações de cálculo.	
	4.8 Cancelar a Folha de Pagamento.	
	4.9 Emitir Relatório de Controle Interno da Folha de Pagamento.	

Fonte: Elaborado pelo autor com dados de DFM (2009).

APÊNDICE B - Requisitos não funcionais do SISPAG2

REQUISITOS NÃO FUNCIONAIS	
Requisito	**Atividades**
1. Confidencialidade	O aplicativo deverá garantir que as informações sejam acessíveis apenas para aqueles que estão autorizados a acessá-las e o tráfego de dados na rede deverá ser criptografado. O aplicativo deverá ser multiplataforma ("*Web*"), para evitar problemas com as evoluções dos sistemas operacionais, e utilizar o protocolo (HTTPS) com certificação digital.
2. Integridade.	O aplicativo deverá garantir que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).
3. Controle de Acesso	O aplicativo deverá permitir o controle de usuários e a definição da política de senhas, mesmo para o caso do acesso off-line. O Gerente das Atividades de Controle Interno concederá privilégios aos usuários através do enquadramento dos mesmos em perfis previamente definidos.
4. Disponibilidade e Autenticação.	Para o acesso on-line, o aplicativo deverá assegurar que somente os usuários autorizados tenham acesso às informações. A página "Web" deve ter um "*login*" com teclado virtual e possível através de "*tokens*". O aplicativo não deverá permitir a um mesmo usuário obter mais do que uma conexão simultânea. Deverão fazer parte dos registros de auditoria os horários de conexão e desconexão de cada usuário. O sistema deverá ser preparado para operar 24 (vinte e quatro) horas durante 7 (sete) dias na semana (24x7), com disponibilidade de 99,9 (noventa e nove vírgula nove) %, admitindo um "*downtime*" semanal de 10,1(dez vírgula 1) minutos.
5. Segurança lógica.	O aplicativo deverá garantir a segurança do segmento de rede onde residirão os servidores (Rede segregada por "Firewall" devidamente dimensionado) e estes devem ser auditados quanto aos aspectos de segurança do sistema operacional e aplicações.
6. Contingência ("*backup* e *restore*").	O aplicativo deverá cumprir as melhores práticas que englobam o espelhamento dos dados.
7. Auditoria.	O aplicativo deverá registrar todas as transações realizadas, armazenando a identificação do usuário, a data e a hora (até milissegundos, com base no relógio do sistema), a fim de permitir a realização de auditorias subsequentes. Estes dados deverão ser armazenados pelo aplicativo a fim de compor uma base histórica de pelo menos 5 (cinco) anos. Estas bases deverão ser incluídas nas rotinas de backup do aplicativo. O aplicativo deverá permitir a realização de consultas on-line, através do uso de filtros de seleção: período de data e hora, usuário, transação etc. O administrador do sistema deverá ter a possibilidade de emitir o resultado da consulta em arquivo PDF.
8. Gerenciamento da transmissão de arquivos.	Durante a transmissão de arquivos, o aplicativo deverá apresentar tela que indique o progresso na transmissão dos dados (barra de progresso). Deverá também permitir ao usuário receber confirmação de recepção e marcar os registros enviados para não haver reenvio indesejado, informar a última data em que esta carga ocorreu e relatório de erros, contendo os registros rejeitados e o motivo de cada um.
9. Interface gráfica do usuário.	O aplicativo deverá ser operado através de interfaces gráficas interativas semelhantes ao padrão de telas utilizado atualmente pelo Setor de TI da PAPEM.
10. Exibição de data e hora.	As telas do aplicativo deverão mostrar a data e hora corrente.
11. Fácil uso.	O aplicativo deverá permitir boa navegabilidade entre as diversas janelas.
12. Ajuda.	Todas as janelas do aplicativo deverão possuir um menu ou botão que permita acesso a um texto explicativo de ajuda relativo às ações e ao preenchimento dos campos disponíveis. O Mod-CD deverá possuir um tutorial on-line para apresentar ao usuário as funcionalidades da atividade de captação de dados.
13. Preenchimento automático.	O aplicativo, nos casos devidos, deverá permitir o preenchimento de um campo a partir do apontamento, pelo operador, de um item de uma lista de opções.
14. Controle de transações.	O aplicativo deverá possuir controle de transações que garanta, em qualquer caso de erro – seja de comunicação ou interno – que o aplicativo permaneça em um estado consistente. As transações deverão ser realizadas, nesse sentido, de forma atômica.
15. Tempo de resposta.	O tempo de resposta ou de execução para deverá atender aos seguintes limites: a) 1 (um) segundo: para terminar Relação de Remuneração (RR) ou, ainda, incluir, alterar, excluir, suspender ou reativar uma parcela, ambos pela interface on-line. b) 2 (dois) segundos: para incluir, excluir, alterar informações pessoais e funcionais; incluir, alterar, excluir, movimentar, suspender, reativar uma RR; sinalizar ou excluir sinal de "em Acerto de Contas" ou "em Situação Especial no País", para uma RR; elaborar Ordem de Serviço; operacionalizar pagamentos de Auxílio-Funeral; e calcular o valor pecuniário das parcelas de uma RR − todos pela interface on-line. c) 10 (dez) minutos: comandar a suspensão ou reativação de RR em bloco; comandar a inclusão, alteração ou exclusão de informações financeiras de RR em bloco; e suspensão ou reativação de

	uma Parcela Geral − todos pela interface on-line−. E, ainda, operacionalizar a verificação do CPF entre o SISPAG e a Receita Federal; atualizar os dados pessoais e funcionais a partir do sistema de pessoal; e simular a atualização, d) 1 (uma) hora: atualizar os dados pessoais e funcionais e financeiros a partir do arquivo "Dados Coletados", e transferir as informações da Folha de Pagamento para o sistema legado. e) 2 (duas) horas: calcular a Folha de Pagamento, realizar simulações de cálculo, e cancelar a Folha de Pagamento. f) O tempo das operações de geração dos relatórios não deve ser maior que 1 (um) minuto.
16. Conexão com o SGBD.	O aplicativo deverá gerenciar e monitorar a conexão com o banco de dados, tomando todas as providências necessárias para realizá-la e mantê-la de forma automática, gerando e mantendo registro ("*logs*") de tudo o que for realizado.
17. Usuários simultâneos.	O aplicativo deve permitir o acesso de pelo menos 1000 (um mil) usuários simultâneos, através da rede local.
18. Tráfego de rede.	O aplicativo deverá buscar eficiência no uso de banda da infraestrutura de conectividade nas transações online, assim como nas demais que demandem tráfego na rede dados da Marinha, sem, no entanto, degradar os requisitos de desempenho, em especial o de tempo de resposta.
19. Consumo de banda de transmissão.	Um arquivo gerado, com 200 (duzentas) transações, deverá ser transmitido através de uma conexão discada, a 56 (cinquenta e seis) Kbps, em no máximo 20 (vinte) segundos. Uma tela qualquer do aplicativo, acessada a partir de um cliente baseado em um navegador "Web", não deverá conter demasiados elementos gráficos, nem excessiva quantidade de dados, a fim de poder ser transmitida através de uma conexão discada, a 56 (cinquenta e seis) Kbps, em no máximo 20 (vinte) segundos.
20. Padrões de modelagem.	Os nomes de objetos de banco de dados deverão seguir as Normas e Padrões Técnicos para Denominação de Objetos no Banco de Dados, da Administração de Dados da PAPEM.
21. Dicionarização.	Todos os objetos de banco de dados do aplicativo deverão estar definidos no dicionário de dados e no modelo de dados.
22. Manual do aplicativo.	Deverá ser elaborado um manual do aplicativo, com as informações necessárias para configuração dos servidores, instalação e operação do aplicativo. Deverão constar também nesse manual um plano de contingência, um plano de backup e uma política de criação de usuários.
23. Manutenibilidade.	O aplicativo será estruturado em camadas, de forma que as atualizações e manutenções possam ser efetuadas mais eficientemente, preservando a integridade das outras camadas.
24. Registro e tratamento de exceções.	O aplicativo deve dar tratamento às exceções de processamento, visando facilitar sua manutenção corretiva.
25. Ferramentas de Design.	O aplicativo deverá ser documentado segundo o padrão da UML ("Unified Modelling Language"), contendo diagramas de casos de uso, diagramas de classes, diagramas de sequencia, diagramas de estados e diagramas de atividades.
26. Metodologia.	O processo de desenvolvimento deverá seguir os passos prescritos pelo Processo Unificado.
27. Plataforma cliente.	O aplicativo deverá rodar nos sistemas operacionais Windows (9X/Millenium/NT/2000/XP/Vista), Linux (Conectiva, Debian, Fedora, Kurumin, Red Hat e SUSE) e Freebsd.
28. Arquitetura.	O desenvolvimento do aplicativo deverá ser realizado com total aderência ao padrão estabelecido. Isto implicará na obediência estrita às especificações, ou seja, sem utilização de qualquer recurso proprietário (função, biblioteca etc.), com a utilização somente de produtos que possuam certificado de compatibilidade, e com a certificação da própria aplicação. O aplicativo deverá manter independência em relação à fonte de dados.
29. Banco de dados.	Para o desenvolvimento e produção do aplicativo será utilizado o Banco de Dados Oracle 10g.
30. Licenças de software.	Para o desenvolvimento do aplicativo deverá ser priorizado o emprego de software livre, entendendo-se com isto o uso de produtos "open source" e que, preferivelmente, não possuam custo de aquisição de licenças de uso. Isto sem abrir mão da certificação de compatibilidade, robustez, escalabilidade e desempenho. Sempre que um destes requisitos não puder ser atendido, deverão ser apresentadas soluções alternativas ao software livre para análise e escolha, a critério do gerente do projeto.

Requisitos não funcionais do SISPAG2.
Fonte: Elaborado pelo autor com dados de DFM (2009).

APÊNDICE C - Roteiro de entrevista para o SISPAG2

Roteiro de Entrevista a ser utilizado em Dissertação a ser apresentada à Universidade do Estado do Rio de Janeiro para a obtenção do grau de mestre em Ciências Contábeis

Prezado (a) Servidor (a),
Meu nome é Kleber Rodger Reis, sou Capitão-tenente (IM) e aluno do Programa de Mestrado em Ciências Contábeis da Universidade do Estado do Rio de Janeiro (UERJ). Esta entrevista tem por objetivo coletar dados para elaboração da dissertação a ser apresentada ao Programa de Pós-Graduação em Ciências Contábeis da Faculdade de Administração e Finanças da UERJ para obtenção do grau de Mestre em Ciências Contábeis sob orientação do prof. Ld. Lino Martins da Silva. Assim, participo que as referidas respostas serão utilizadas unicamente para fins acadêmicos.
ROTEIRO DE ENTREVISTA: A entrevista está direcionada a servidores que trabalham, trabalharam ou contribuíram diretamente com o **SISPAG2** (Sistema de Pagamento da Marinha do Brasil, em modernização). A pesquisa trata de como o sistema de controle interno utilizado pelo Sistema de Pagamento de Pessoal da Marinha atende às normas vigentes e ao que prevê a área acadêmica sobre o assunto.
O entrevistado deverá atribuir graus conforme abaixo:
1- Discordo totalmente
2- Discordo
3- Não concordo nem discordo
4- Concordo
5- Concordo plenamente
Cada entrevistado deve responder a todas as perguntas e fazer todos os comentários que achar pertinente após atribuir o referido grau.
Desde já agradeço sua cooperação!

Categoria	Questões	Avaliação
1. SEGURANÇA	Q.1.1- Somente pessoas autorizadas poderão acessar o sistema?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.1.2- Os recursos a serem utilizados na transmissão de dados (criptografia, por exemplo) promoverão uma adequada segurança contra a interceptação de dados por pessoas não autorizadas?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.1.3- O sistema disponibilizará ao usuário informações confiáveis, corretas e dispostas em formato compatível com o de utilização?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.1.4- A forma e o conteúdo dos dados inseridos pelo usuário estarão mantidos?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.1.5- O uso de aplicativos e acesso aos dados será controlado e monitorado por meio de senhas individuais atribuídas a pessoas pré-cadastradas e enquadradas em um perfil?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.1.6- Um usuário poderá se *logar* somente em um terminal ao mesmo tempo?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.1.7- O sistema operará 24x7 (24 horas durante sete dias por semana) com disponibilidade próxima a 100%?	○ ○ ○ ○ ○ 1 2 3 4 5

	Q.1.8- Estão previstos momentos de pico para a operação do sistema?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.1.9- O sistema utilizará ferramentas adequadas para autenticação (teclado virtual para *login*, *tokens,* biometria e outras) e dentro do que há de mais moderno no mercado?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.1.10- A conexão ao Banco de Dados será feita por senhas criptografadas?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.1.11- O sistema impossibilitará acesso sem conexão à rede da MB para funções normalmente feitas pela rede interna (por exemplo, nos casos excepcionais pela Internet)?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.1.12- As medidas previstas permitirão uma rápida e perfeita recuperação de dados em possíveis situações adversas?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.1.13- Para cada transação realizada serão armazenados os dados da transação, a identificação do usuário, a data e a hora para consulta por pessoa autorizada?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.1.14- Está previsto um criterioso acompanhamento para identificar e apontar possíveis usos indevidos de senhas? (Por exemplo, número de transações incomuns, tentativas de acesso a documentos não autorizados etc.).	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.1.15- Em todas as operações com transmissão de arquivos, o usuário receberá confirmação de recepção, por registro enviado, para não haver reenvio indesejado?	○ ○ ○ ○ ○ 1 2 3 4 5
2. USABILIDADE	Q.2.1- Está previsto um programa de treinamentos para que os usuários operem adequadamente o sistema?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.2.2- Todas as interfaces gráficas interativas permitirão boa navegabilidade e facilidade de uso pelos usuários?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.2.3- O manual do usuário descreverá todas as telas, incluindo conteúdo e uso?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.2.4- O aplicativo, nos casos devidos, oferecerá uma lista de opções para preenchimento?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.2.5- Um *menu* de ajuda estará disponível e operativo em todas as janelas?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.2.6- Todas as interfaces gráficas serão padronizadas?	○ ○ ○ ○ ○ 1 2 3 4 5
3. CONFIABILIDADE	Q.3.1- O controle de transações assegurará a consistência do aplicativo, mesmo em caso de erro?	○ ○ ○ ○ ○ 1 2 3 4 5
4. DESEMPENHO	Q.4.1- O tempo de resposta do sistema será adequado (por exemplo, inclusões de parcelas feitas instantaneamente)?	○ ○ ○ ○ ○ 1 2 3 4 5

	Q.4.2- O número de acessos simultâneos suportados atenderá as demandas e será aferido por um teste de *stress*?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.4.3- O acesso remoto de regiões com maiores dificuldades em trafegar dados será averiguado por teste de *stress*?	○ ○ ○ ○ ○ 1 2 3 4 5
5. SUPORTABILIDADE	Q.5.1- O manual do aplicativo definirá perfeitamente a configuração dos servidores e a instalação e operação do aplicativo?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.5.2- O manual do aplicativo definirá um plano de contingência, um plano de backup e uma política de criação de usuários?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.5.3- A equipe de TI responsável pelo sistema receberá treinamento adequado para atuar nessa tarefa?	○ ○ ○ ○ ○ 1 2 3 4 5
6. IMPLEMENTAÇÃO	Q.6.1- O sistema terá independência em relação ao fornecedor de Banco de Dados? (por exemplo, se mudar de Oracle para SQL, o sistema continuará operacional sem grandes modificações).	○ ○ ○ ○ ○ 1 2 3 4 5
7. CAPACITAÇÃO DA EQUIPE	Q.7.1- Possui formação ou qualificação adequada às funções que desempenhou ou desempenha no SISPAG2?	○ ○ ○ ○ ○ 1 2 3 4 5
8. NOÇÕES DE CONTROLE INTERNO	Q.8.1- Qual seu grau de conhecimento do Regimento Interno, Ordens Internas, Leis e demais normas que estabeleçam controles sobre sua atividade?	○ ○ ○ ○ ○ 1 2 3 4 5
9. CIÊNCIA DA MISSÃO	Q.9.1- Qual o seu grau de conhecimento da missão e tarefas atribuídas à organização?	○ ○ ○ ○ ○ 1 2 3 4 5
10. ATUALIZAÇÃO DAS NORMAS	Q.10.1- As ordens internas que você utiliza estão atualizadas?	○ ○ ○ ○ ○ 1 2 3 4 5
11. SEGREGAÇÃO DE AMBIENTES	Q.11.1- Existem ambientes de produção, desenvolvimento e homologação separados?	○ ○ ○ ○ ○ 1 2 3 4 5
12. DESIGN	Q.12.1- Nas ferramentas de modelagem previstas estão todos os artefatos e UML (*Unified Modelling Language*) estabelecidos no contrato?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.12.2- As mudanças ao longo do processo estão sendo registradas e documentadas?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.12.3- O processo de desenvolvimento está seguindo os passos prescritos pelo processo unificado?	○ ○ ○ ○ ○ 1 2 3 4 5
	Q.12.4- Existe um acompanhamento eficiente e eficaz do cronograma de projeto?	○ ○ ○ ○ ○ 1 2 3 4 5

APÊNDICE D- Roteiro de Entrevista para o Sistema em Operação

Roteiro de Entrevista a ser utilizado em Dissertação a ser apresentada à Universidade do Estado do Rio de Janeiro para a obtenção do grau de mestre em Ciências Contábeis.

Prezado (a) Servidor (a),
Meu nome é Kleber Rodger Reis, sou Capitão-tenente (IM) e aluno do Programa de Mestrado em Ciências Contábeis da Universidade do Estado do Rio de Janeiro (UERJ). Esta entrevista tem por objetivo coletar dados para elaboração da dissertação a ser apresentada ao Programa de Pós-Graduação em Ciências Contábeis da Faculdade de Administração e Finanças da UERJ para obtenção do grau de Mestre em Ciências Contábeis, sob orientação do prof. Ld. Lino Martins da Silva. Assim, participo que as referidas respostas serão utilizadas unicamente para fins acadêmicos.
ROTEIRO DE ENTREVISTA: A entrevista está direcionada a servidores que trabalham ou trabalharam recentemente com o **atual SISPAG** (Sistema de Pagamento da Marinha do Brasil). A pesquisa trata de como o sistema de controle interno utilizado pelo Sistema de Pagamento de Pessoal da Marinha atende às normas vigentes e ao que prevê a área acadêmica sobre o assunto.
O entrevistado deverá atribuir graus conforme abaixo:
1- Discordo totalmente
2- Discordo
3- Nem discordo nem concordo
4- Concordo
5- Concordo totalmente
Cada entrevistado deve responder a todas as perguntas e fazer todos os comentários que achar pertinente após atribuir o referido grau.
Desde já agradeço sua cooperação!

Categoria	Pergunta	Avaliação
1. SEGURANÇA	P.1.1- Somente pessoas autorizadas podem acessar o sistema?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.1.2- Os recursos utilizados na transmissão de dados (criptografia, por exemplo) promovem uma adequada segurança contra a interceptação de dados por pessoas não autorizadas?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.1.3- O sistema disponibiliza ao usuário informações confiáveis, corretas e dispostas em formato compatível com o de utilização?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.1.4- A forma e o conteúdo dos dados inseridos pelo usuário são mantidos?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.1.5- O uso de aplicativos e acesso aos dados é controlado e monitorado por meio de senhas individuais atribuídas a pessoas pré-cadastradas e enquadradas em um perfil?	○ ○ ○ ○ ○ 1 2 3 4 5

	P.1.6- Um usuário pode se *logar* somente em um terminal ao mesmo tempo?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.1.7- O sistema opera 24x7 (24 horas durante sete dias por semana) com disponibilidade próxima a 100%?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.1.8- Estão previstos momentos de pico para a operação do sistema?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.1.9- O sistema utiliza ferramentas adequadas para autenticação (teclado virtual para *login*, *tokens*, biometria e outras) e dentro do que há de mais moderno no mercado?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.1.10- A conexão ao Banco de Dados é feita por senhas criptografadas?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.1.11- O sistema impossibilita acesso sem conexão à rede da MB para funções normalmente feitas pela rede interna (por exemplo, nos casos excepcionais pela Internet)?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.1.12- As medidas previstas permitem uma rápida e perfeita recuperação de dados em possíveis situações adversas?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.1.13- Para cada transação realizada são armazenados os dados da transação, a identificação do usuário, a data e a hora para consulta por pessoa autorizada?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.1.14- Há um criterioso acompanhamento para identificar e apontar possíveis usos indevidos de senhas? (Por exemplo, número de transações incomuns, tentativas de acesso a documentos não autorizados etc.).	○ ○ ○ ○ ○ 1 2 3 4 5
	P.1.15- Em todas as operações com transmissão de arquivos, o usuário recebe confirmação de recepção, por registro enviado, para não haver reenvio indesejado?	○ ○ ○ ○ ○ 1 2 3 4 5
2. USABILIDADE	P.2.1- Existe um programa de treinamentos para que os usuários operem adequadamente o sistema?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.2.2-Todas as interfaces gráficas interativas permitem boa navegabilidade e são de fácil uso pelos usuários?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.2.3- O manual do usuário descreve telas incluindo conteúdo e seu uso?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.2.4- O aplicativo, nos casos devidos, oferece uma lista de opções para preenchimento?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.2.5- Um *menu* de ajuda está disponível e operativo em todas as janelas?	○ ○ ○ ○ ○ 1 2 3 4 5

	P.2.6- Todas as interfaces gráficas são padronizadas?	○ ○ ○ ○ ○ 1 2 3 4 5
3. CONFIABILIDADE	P.3.1- O controle de transações assegura a consistência do aplicativo, mesmo em caso de erro?	○ ○ ○ ○ ○ 1 2 3 4 5
4. DESEMPENHO	P.4.1-O tempo de resposta do sistema é adequado (por exemplo, inclusões de parcelas feitas instantaneamente)?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.4.2- O número de acessos simultâneos permitidos foi aprovado por uma ferramenta de teste de *stress*?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.4.3- O acesso remoto de regiões com maiores dificuldades em trafegar dados foi atestado por teste de *stress*?	○ ○ ○ ○ ○ 1 2 3 4 5
5. SUPORTABILIDADE	P.5.1- O manual do aplicativo define perfeitamente a configuração dos servidores e a instalação e operação do aplicativo?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.5.2- O manual do aplicativo define um plano de contingência, um plano de backup e uma política de criação de usuários?	○ ○ ○ ○ ○ 1 2 3 4 5
	P.5.3- A equipe de TI responsável pelo sistema recebeu treinamento adequado para atuar nessa tarefa?	○ ○ ○ ○ ○ 1 2 3 4 5
6. IMPLEMENTAÇÃO	P.6.1- O aplicativo mantém independência em relação ao fornecedor de Banco de Dados (por exemplo, se mudar de Oracle para SQL o sistema continua operacional sem grandes modificações)?	○ ○ ○ ○ ○ 1 2 3 4 5
7. CAPACITAÇÃO DA EQUIPE	P.7.1- Possui formação ou qualificação adequada às funções que desempenhou ou desempenha no atual SISPAG?	○ ○ ○ ○ ○ 1 2 3 4 5