Auditoria Interna

Relatório de Auditoria	AUD/JS/05/2019 - 11 de setembro de 2019
Atividade do PAINT	A010 PAINT 2018
Tipo de Serviço	Avaliação
Unidade Auditada	Diretoria de Tecnologia da Informação (DTI/CAPES)
Objeto Auditado	Sistemas de Pagamento de Bolsas e Auxílios da CAPES

1. INTRODUÇÃO

O objetivo geral deste trabalho é apresentar os resultados da atividade de auditoria realizada nos Sistemas de Pagamento de Bolsas e Auxílios da CAPES a cargo da Diretoria de Tecnologia da Informação (DTI).

Essa atividade de auditoria foi prevista no Plano Anual de Auditoria Interna (PAINT) – Exercício de 2018, tendo por objetivo: verificar a confiabilidade e segurança dos pagamentos de bolsas e auxílios realizados pelos sistemas informatizados da CAPES; verificar a análise de riscos envolvidos nas ações de pagamentos via sistemas; verificar a eficácia e eficiência das transações, bem como a efetividade do acompanhamento das bolsas e auxílios.

Escopo:

1. Verificação do andamento das ações propostas no Plano Diretor de Tecnologia da informação e Comunicação (PDTIC 2017-2019) referentes aos sistemas de pagamento de bolsas e auxílios.
2. Verificação das características de qualidade dos sistemas quando da realização de pagamentos.
3. Avaliação dos riscos inerentes ao desenvolvimento, utilização e manutenção dos sistemas e dos controles internos criados pela DTI para mitigação dos riscos.
4. Monitoramento quanto ao atendimento a recomendações emitidas anteriormente pelo controle interno e externo que envolvam os sistemas de pagamento.

O escopo foi definido com base na materialidade (valores repassados pelos sistemas), relevância (o pagamento de bolsas e auxílios depende do bom funcionamento dos sistemas) e criticidade (os riscos envolvidos nas operações realizadas pelos sistemas).

Metodologia: o trabalho de avaliação se deu por meio de análise documental, consolidação das informações prestadas pela DTI em resposta a Solicitações de Auditoria, reuniões com os gestores e comparação de conformidade com normas e boas práticas. Os trabalhos seguiram, ainda, o Manual de Orientações Técnicas da CGU, emitido pela Instrução Normativa nº 08, que orienta a operacionalização do disposto na Instrução Normativa nº 03, de 09 de junho de 2017, e o Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão do Ministério da Economia.

Durante os trabalhos de auditoria, a DTI foi tempestiva na apresentação das informações solicitadas, o que contribuiu para o bom andamento dos trabalhos. No entanto, a redução do quadro de servidores da Auditoria Interna no período retardou a análise das informações e apresentação dos resultados.

2. VISÃO GERAL DO OBJETO

A solução atualmente utilizada para o pagamento de bolsas e auxílios da CAPES compreende os seguintes sistemas:

- SAC – Sistema de Acompanhamento de Concessão
- SGB – Sistema de Gestão de Bolsas
- SCBA – Sistema de Controle de Bolsas e Auxílios
- SAE – Sistema de Gestão de Auxílios à Avaliação Educacional
- Sistema Financeiro

O SAC, SGB e SCBA possibilitam o cadastro, concessão, pagamento, acompanhamento, suspensão e exclusão de bolsas e auxílios. São utilizados pelos técnicos da CAPES, coordenadores das Instituições de Ensino e pelos bolsistas. O SAC e o SGB são sistemas legados e estão em processo de substituição pelo SCBA.

O SAE controla o teto anual de pagamento de Auxílio Educacional. É utilizado pelas secretarias de educação do MEC, CAPES, INEP, pelos favorecidos do Auxílio de Avaliação Educacional (AAE) e pelos indicados para execução de avaliações educacionais.

O Sistema Financeiro realiza as operações orçamentárias e financeiras para a formalização de pagamentos junto ao Sistema Integrado de Administração Financeira do Governo Federal (SIAFI).

Há, também, o Sistema de Conciliação de Pagamento de Bolsas e Auxílios (SCPB), que realiza consultas de beneficiários em todas as bases, consulta de dados na Receita Federal, cadastro de ex-bolsistas como inadimplentes, liberação de bolsistas para pagamento em casos específicos de situações que permitam acúmulos com CNPq e FNDE, dentre outras operações acessórias ao processo de pagamento. Esse sistema não foi incluído no escopo desse trabalho de auditoria, sendo a avaliação direcionada apenas aos sistemas que realizam operações de pagamento propriamente dito.

De acordo com a unidade auditada, os sistemas foram desenvolvidos para resolver problemas como: retrabalho para digitação dos dados de pagamentos no SIAFI, devido à falta de integração; erro na digitação dos dados durante a realização das transações orçamentárias e financeiras, gerando inconsistência entre a informação registrada nos sistemas internos e as cadastradas no SIAFI; recorrentes atrasos nos pagamentos, devido à demora na execução manual das operações; sobrecarga dos servidores e colaboradores para a execução das atividades que envolvem a realização de pagamentos; grande volume de reclamações dos beneficiários por atrasos nos pagamentos; e falta de informação gerencial para tomada de decisão, devido à falta de integração entre os sistemas das áreas gestão de bolsas e a Coordenação Geral de Orçamento e Finanças (CGOF).

Os custos de desenvolvimento, implantação e manutenção dos sistemas, em 2018, totalizaram R$ 20.627.969,00, conforme demonstrado na tabela abaixo:

Ação Orçamentária	Plano Orçamentário	Natureza da Despesa	
2000 - Administração da	0001 - Administração da TIC	44.90.39.92 - Desenvolvimento de Software - Serviços prestados por PJ	13/2014 - Prestação de serviç

Unidade		33.90.40.07 - Manutenção Corretiva/Adaptativa e Sustentação de Software 33.90.40.21 - Serviços técnicos de profissionais de TIC - PJ	30/2014 - Prestação de serviç 41/2016 - Prestação de serviç

Fonte: Memorando 10 (0897445), Planilha (0898547), Despacho CGS 1031422 e Planilha (1042334).

3. RESULTADO DOS EXAMES

No planejamento dos trabalhos, foram elaboradas 07 (sete) Questões de Auditoria para orientar a análise definida no escopo. Com vistas ao levantamento de informações suficientes para responder às questões de auditoria, bem como o entendimento do objeto auditado, das necessidades da gestão da unidade auditada e coleta de evidências para embasamento das conclusões deste relatório, foram encaminhadas 04 (quatro) Solicitações de Auditoria - SA (SEI n° 0797041, 0889285, 0911961 e 0925997).

A seguir é apresentado o resumo dos resultados obtidos através das respostas às Solicitações de Auditoria e das análises e testes realizados pela equipe de auditoria.

3.1. QUESTÃO DE AUDITORIA 1 - As ações previstas no PDTIC 2017-2019, referentes aos sistemas de pagamento de bolsas e auxílios, foram ou estão sendo desenvolvidas?

O Plano Diretor de Tecnologia da Informação e Comunicação da CAPES (PDTIC) em vigor no triênio 2017 a 2019, contempla 05 (cinco) ações que se referem diretamente aos sistemas de pagamento de bolsas e auxílios:

- OB3/N6/AE10 - Aprimorar o sistema único de pagamento de bolsas e auxílios. Unificar os sistemas de pagamentos de bolsas e auxílios, disponibilizando para todas as diretorias competentes, a partir de um profundo entendimento e padronização dos processos.
- OB3/N7/AE11 - Integrar os sistemas de concessão e pagamento da CAPES com os sistemas de repasses de recursos do Governo Federal. Realizar a integração dos sistemas externos de concessão e pagamento em um repositório único da CAPES, a fim de proporcionar a consulta sobre a situação de inadimplência, repasses de recursos, situações de bolsas, dentre outros.
- OB3/N7/AE13 - Integrar os sistemas de pagamento ao SEI. Integrar os sistemas de gestão e concessão de bolsas e auxílios com o SEI com o objetivo de utilizar a numeração de processos NUP da CAPES.
- OB3/N7/AE17 - Integração de sistemas DRI/DAV/DPB/DEB. Complementar a integração dos sistemas de pagamento com as Plataformas Sucupira e Freire.
- OB3/N7/AE39 - Mapear e implantar melhorias no processo de liberação para pagamentos no SCPB. Entender e implementar melhorias no processo de liberação para pagamentos no SCPB, que atualmente envolve diversas diretorias, agilizando o fluxo.

Análise da AUD: De acordo com as informações apresentadas pela DTI no item 1 do Memorando 10 (SEI n° 0897445), todas as ações do PDTIC estão em andamento. Ressalta-se que a DTI adota a boa prática de fazer acompanhamento mensal do plano, em conjunto com representantes de todas as diretorias. A cada reunião de acompanhamento, há deliberações sobre as decisões tomadas no último encontro para atualizar a situação de cada ação e priorizá-las de acordo com as necessidades institucionais.

Apesar de todas as ações estarem em andamento e das reuniões de acompanhamento realizadas, as seguintes iniciativas ainda estão em fase de estudos preliminares: utilização do SIMEC e Convênios para pagamentos do programa PRINT; solução para integração dos sistemas ao SEI; e mapeamento entre as plataformas Freire e Sucupira e definições de gerenciamento negocial e de cotas.

Considerando que restam poucos meses para o término do prazo previsto para a conclusão das ações, depreende-se que há grande probabilidade de que as ações não sejam concluídas. Inclusive, a ação OB3/N7/AE39 já teve o prazo previsto para término expirado.

Resposta: Sim, as ações estão sendo desenvolvidas, mas algumas requerem mais atenção ao prazo de conclusão.

3.2. QUESTÃO DE AUDITORIA 2 - Estão presentes as características de qualidade dos sistemas quando da realização dos pagamentos?

A norma ISO/IEC 25010:2011 define o modelo de qualidade de um *software* e apresenta oito características de qualidade:

1. adequação funcional;
2. eficiência de desempenho;
3. compatibilidade;
4. usabilidade;
5. confiabilidade;
6. segurança;
7. manutenção; e
8. portabilidade

Análise da AUD: A presença de tais características nos sistemas da CAPES foi avaliada levando-se em consideração as circunstâncias em que os diferentes sistemas foram desenvolvidos e as peculiaridades que envolvem o pagamento de bolsas e auxílios.

Em resposta ao item n° 3 da Solicitação de Auditoria n° 1/2019 (SEI 0889285 e 0897445), a DTI informou as ferramentas, rotinas, mecanismos e operações dos sistemas que demonstram a existência das características de qualidade citadas acima nos sistemas objeto dessa auditoria. As informações apresentadas pela DTI foram compiladas no Anexo III.

Em relação à adequação funcional e usabilidade, os sistemas de pagamento são adequados às necessidades da CAPES, pois são essenciais para o alcance dos objetivos da instituição, visto que a maior parte de suas atividades consiste em investimentos, na forma de bolsas e auxílios, para a formação de pessoal qualificado no país e no exterior.

Da percepção dos usuários internos dos sistemas, coletadas por meio de pesquisa de satisfação, alguns pontos ainda carecem de melhorias, no tocante à adequação e usabilidade. Os principais pontos apresentados foram referentes a deficiência das informações geradas por meio de relatórios, a determinados sistemas que não são intuitivos, e a falta de integração entre alguns sistemas. A satisfação dos usuários será analisada detalhadamente mais adiante, na questão de auditoria n° 7.

Em relação à eficiência de desempenho, há controles de monitoramento que verificam se as funcionalidades dos sistemas estão sendo executadas dentro do intervalo de tempo esperado e na ordem correta. Não foram encontradas irregularidades nos pagamentos realizados por meio dos sistemas auditados e as impropriedades identificadas ocorreram, principalmente, devido a fatores externos ao funcionamento ou desenvolvimento dos sistemas.

Em relação à compatibilidade, no que se refere às interações internas e externas relacionadas ao pagamento, verificou-se que os sistemas auditados operam de forma integrada com comunicação automatizada. As interações entre esses sistemas são padronizadas por protocolos de comunicação estabelecidos entre as partes, de forma que se tenham formalizados tanto o envio quanto o retorno das operações.

Ainda não há, no entanto, integração dos sistemas auditados com o Sistema Eletrônico de Informações (SEI) nem com o Sistema Integrado de Monitoramento, Execução e Controle (SIMEC). Algumas integrações ainda carecem de aperfeiçoamento, como a integração com o SIPREC, Plataforma Sucupira, Plataforma Freire.

Em relação à confiabilidade e segurança dos sistemas, há controle de verificação/validação dos dados de entrada e saída, controles criptográficos, identificação de vulnerabilidades e aplicação de patches de correção.

A DTI informou que os sistemas possuem processo automatizado de construção de trilhas de auditoria, possuindo rotinas de registro de *log* em tabelas específicas das operações realizadas pelos usuários. Os testes realizados pela equipe de auditoria demonstraram que é possível rastrear informações específicas numa trilha construída automaticamente pelos sistemas.

A CAPES não utiliza, no momento, um modelo de maturidade do processo de construção de *software*, como, por exemplo, o modelo internacional (Capability Maturity Model Integration - CMMI) ou o modelo nacional (Melhoria de Processo de Software Brasileiro - MPS.BR), de forma que não é possível avaliar o nível de maturidade em que a organização se encontra. Apesar disso, com base nas informações prestadas pela DTI, pode-se dizer que a CAPES não mais se encontra no nível inicial de maturidade, tendo avançado bastante na organização, metodologias e gerenciamento da construção de *software*.

Apenas uma fragilidade na segurança dos sistemas foi identificada. Na listagem de usuários internos dos sistemas encaminhada pela DTI (SEI n° 0898545), constam usuários com perfil de acesso a sistemas que não utilizam mais (trocaram de lotação, saíram da CAPES, etc).

Em relação à manutenção e portabilidade, a DTI informou as dificuldades para se realizar manutenção nos sistemas SAE, SAC e SGB por se tratar de sistemas construídos em tecnologia superada, e no sistema Financeiro pela complexidade do negócio. Informou que o SAE será reestruturado em tecnologia mais moderna e que o SAC e SGB serão substituídos pelo SCBA, que já está sendo construído em tecnologia mais moderna. Enquanto as substituições não são concluídas, são realizadas apenas manutenções para a sustentação dos sistemas antigos, evitando-se a realização de manutenções evolutivas.

Resposta: Sim, as oito características de qualidade dos sistemas estão presentes, quando da realização dos pagamentos, carecendo de aperfeiçoamentos em pontos específicos.

3.3. **QUESTÃO DE AUDITORIA 3 - Os riscos envolvidos nas ações de pagamento de bolsas e auxílios por meio de sistemas informatizados foram devidamente identificados, avaliados, tratados e monitorados?**

A área auditada identificou 04 riscos referentes aos sistemas, sendo 02 riscos de natureza tecnológica e 02 riscos de natureza gerencial:

Natureza do risco	Descrição do Risco
Risco de natureza tecnológica	Erro na comunicação entre os sistemas CAPES (SCBA, SAC, SGB, SAE e Financeiro), no momento de envio de lotes de pagamento, podendo gerar pagamentos em duplicidade ou deixando de incluir pagamentos em uma solicitação de liberação de recursos (SLR), registrada no Sistema Financeiro.
	Alto volume e consistência de dados trafegados entre as aplicações.
Riscos de natureza negocial	Pagamentos indevidos a beneficiários por acúmulos de bolsas.
	Pagamentos indevidos de bolsas e auxílios a beneficiários inadimplentes (CADIN, CONTRANSF e CONTAS DIVERSOS RESPONSÁVEIS).

Análise da AUD: A DTI identificou os riscos e informou os controles que foram criados para sua mitigação. O detalhamento dos riscos e respectivos controles encontra-se no Anexo IV. No entanto, não foi apresentada análise de impacto e probabilidade para se definir o nível dos riscos, nem foi aferido o risco residual após implementação dos controles internos. Ou seja, não é realizada gestão de riscos ou a gestão realizada não é formalizada.

Resposta: Os riscos foram identificados, mas não foram avaliados, tratados e monitorados formalmente.

3.4. **QUESTÃO DE AUDITORIA 4 - Existem controles internos consistentes envolvidos no desenvolvimento e na utilização dos sistemas?**

Análise da AUD: Além dos controles internos apresentados no Anexo IV, que foram adotados com o objetivo de mitigar os riscos apresentados na questão anterior, foram identificados outros controles adotados pela DTI referentes a acúmulo de bolsas:

Acúmulos de bolsas CAPES x CAPES

No caso dos sistemas SAC, SGB e SCBA, o procedimento de verificação de acúmulo de bolsas funciona assim: no momento da geração dos lotes de pagamento, para cada intenção de pagamento registrado no lote, o sistema busca por pagamento existentes nos demais sistemas (SGB, SCBA, SAC e a base de bolsistas inadimplentes do SCPB) para o mesmo CPF, mês e ano referência. (SEI n° 0414697 item 4.7).

Acúmulos de bolsas CAPES x CNPq

A primeira providência adotada, em 2015, foi a padronização da nomenclatura referente às modalidades de ensino e de concessão de bolsa dos programas oferecidos pela CAPES em todos os sistemas de pagamento e gestão de bolsas. Tal medida objetivou facilitar o processo automatizado de verificação de pagamentos duplicados, visto a necessidade de identificação inequívoca das modalidades equivalentes de bolsa entre sistemas (Projeto ANGA). Por volta do dia 20 de cada mês a CAPES envia todas as intenções de pagamento registrado no lote e o CNPq retorna à CAPES as suas intenções de pagamento para o mesmo mês. Se existir intenção para o mesmo CPF, mês e ano referência e não contemplar os acúmulos permitidos conforme regulamentos específicos entre os dois órgãos, tal intenção é bloqueada e retirada do fluxo para pagamento (processo automatizado).

Acúmulos de bolsas CAPES x FNDE:

Esse controle será abordado mais adiante, na questão de auditoria 6, que trata do atendimento a recomendações e determinações dos órgãos de controle.

Resposta: Sim, existem controles internos consistentes envolvidos no desenvolvimento e na utilização dos sistemas.

3.5. QUESTÃO DE AUDITORIA 5 - Os controles internos existentes são aptos a mitigar os riscos inerentes às operações dos sistemas?

Análise da AUD: Apesar de não haver, por parte da DTI, uma avaliação do risco residual após a implementação dos controles, os testes de auditoria indicam que os controles adotados para a mitigação dos riscos de natureza tecnológica têm se mostrado aptos, visto que não foram identificados problemas expressivos em relação a pagamentos em duplicidade, não realizados ou, ainda, falhas causadas por inconsistência de dados, no que se refere à operação dos sistemas. Os pagamentos realizados indevidamente ocorreram, predominantemente, devido a falhas pontuais ocorridas nas diretorias responsáveis pela gestão dos programas, que já tomaram providências para resolução dessas falhas.

Já no que se refere aos riscos de natureza negocial, percebem-se os esforços da DTI em promover ações de mitigação a esses riscos, por meio de implementação de regras de validação e restrições para evitar que ocorram pagamentos indevidos. As regras e restrições aos pagamentos são estabelecidas no âmbito das diretorias responsáveis pelo gerenciamento de cada programa da CAPES. Informada das regras, a DTI as implementa nos sistemas.

No entanto, devido à falta de clareza ou até mesmo à ausência de regras por parte das diretorias, bem como dificuldades de troca de informações com o FNDE, os riscos de natureza negocial não têm sido mitigados de forma suficiente, de modo que ainda ocorrem, anualmente, alguns pagamentos indevidos. No próximo item esse assunto será abordado em maiores detalhes.

Resposta: Os controles internos existentes são aptos a mitigar os riscos de natureza tecnológica, mas ainda não são suficientes para mitigar os riscos de natureza negocial.

3.6. QUESTÃO DE AUDITORIA 6 - As recomendações/determinações dos órgãos de Controle foram atendidas?

Nos últimos quatro anos foram expedidas uma recomendação da CGU e uma determinação do TCU acerca de acumulação de bolsas CAPES e FNDE; e uma recomendação da CGU e outra do TCU acerca de benefícios concedidos a inadimplentes.

Sobre acúmulos de bolsas CAPES/FNDE

Recomendação da CGU n° 153896 (auditoria de avaliação da gestão n° 201503635): Providenciar, em interlocução com o FNDE, documento de suporte à DTI, com as regras de negócio acerca das possibilidades ou não de acúmulo de bolsas, fundamentado na legislação vigente. Em seguida, providenciar os procedimentos de tecnologia da informação necessários à complementação dos controles já efetivados.

Determinação do TCU – Item 1.7 do Acórdão nº 1397/2017 – TCU – 1ª Câmara (Processo TC-026.336/2015-4 - Prestação de Contas - Exercício: 2014): implemente procedimentos estruturados de verificação entre os bancos de dados da CAPES e do FNDE, a fim de se evitar a acumulação indevida de bolsas por parte dos bolsistas da CAPES, e informe a este Tribunal sobre as medidas adotadas.

Histórico das providências adotadas pela DTI/CAPES (Fonte: Docs. SEI º 0414697, 0640359, 0774047, 0843124, 0870731):

2015: a CAPES passou a enviar ao FNDE, nos primeiros dias do mês, um arquivo consolidado com i) todos os pagamentos de mensalidade de bolsa realizados no mês anterior e ii) todas as intenções de pagamento do mês corrente. Esse procedimento acontecia de forma manual (por meio de envio de e-mail).

2016: Com o objetivo de automatizar a troca de dados, a CAPES disponibilizou o serviço de Webservices/CAPES ao FNDE em junho/2016. Com o mesmo objetivo, solicitou a disponibilização do Webservices/FNDE, cujo atendimento se deu em agosto/2016. Entretanto, após várias tentativas de acesso e análise a CAPES concluiu que esses Webservices não atendiam aos requisitos solicitados. Em outubro/2016, a CAPES comunicou a não conformidade com as necessidades e reforçou ao FNDE a solicitação detalhando a demanda.

2017: Em fevereiro/2017 o FNDE disponibilizou o serviço solicitado. Desde setembro/2017, após homologação e carga das informações extraídas do Webservices/FNDE, a carga de dados é executada automaticamente, da seguinte forma: semanalmente, os dados de pagamentos do FNDE são capturados e armazenados no banco de dados da CAPES; ao executar as rotinas de geração de folha de pagamento de bolsas, os sistemas acionam o Webservice de validação de duplicidade; para cada bolsista elegível a receber pagamentos pela CAPES, o serviço de validação de duplicidade realiza a comparação entre CPF, ano/mês de referência, modalidade de bolsas (função no FNDE); caso seja encontrada equivalência, o serviço retorna indicação de duplicidade; de posse do retorno de duplicidade, cabe aos sistemas de gestão e pagamento de bolsas bloquearem, ou não, a solicitação de pagamento.

2018: Em janeiro/2018 a Diretoria de Educação Básica - DEB reportou que o sistema SAC-País suspendeu 925 bolsistas do programa Pibid. Essa suspensão ocorreu por meio do serviço da validação de duplicidade junto ao FNDE, que identificou registros de pagamentos em meses equivalentes, entre os dois órgãos. Esse fato evidenciou efetividade na avaliação de duplicidades e a necessidade de criação de regras de acúmulo de modalidades de bolsas entre a CAPES e FNDE.

Em 18/08/2018, foi realizada uma reunião técnica na DTI com representantes da área que realiza gestão de bolsas do FNDE (Sr. Luiz Sinelson) e da área de TI daquele órgão. Na reunião foi repassado o procedimento realizado na CAPES para verificação de acúmulos e questionada a execução de procedimento similar no FNDE. Os representantes informaram que os procedimentos estavam sendo implementados nos sistemas automatizados do órgão.

No ano de 2018 foram registrados, ainda, 507 pagamentos em duplicidade, porque a geração das SLRs ocorreram antes da importação dos dados de pagamento do FNDE. Alguns desses pagamentos em duplicidade foram liberados pelos gestores da DPB (6 pagamentos) e DEB (3 pagamentos). Dois desses são do programa Memórias (iniciação científica)/CAPES com Bolsa Permanência (aluno indígena)/FNDE; quatro do programa PROEX (mestrado)/CAPES com PSA (aluno PET)/FNDE; e três do programa Residência (residente)/CAPES com PSA (aluno PET)/FNDE.

As regras estabelecidas, até o momento, que permitem acúmulos, se referem aos programas PIBID e Residência Pedagógica da CAPES, com o programa Bolsa Permanência (BP) do FNDE. Essas regras estão formalizadas no art. 38, Portaria Capes n° 96/2013 e art. 4 Resolução FNDE n° 13/2013. Diante disso, a DTI/CAPES realizou a implementação dessa regra nas rotinas de identificação de duplicidades

Após dupla checagem na aplicação das regras de verificação de duplicidade (pela primeira vez nos sistemas de pagamento, no momento da geração da folha de pagamento; e por último, no sistema Financeiro, no momento da geração da SLR) constatou-se a eficiência nos bloqueios das intenções de pagamento que

seriam consideradas duplicidade. A maioria dos pagamentos em duplicidade constatados pela CGU foi realizada pelo FNDE, a posteriori aos pagamentos realizados pela CAPES.

A implantação de rotina automatizada de verificação de acúmulos entre CAPES e FNDE ainda não pode ser completamente implementada em função da ausência de definição clara sobre quais modalidades de bolsa são passíveis de acúmulo e quais não são. Os requisitos das funcionalidades a serem desenvolvidas e implementadas nos sistemas informatizados dependem da definição das regras de negócios informadas conjuntamente pelas áreas finalísticas da CAPES e do FNDE.

Da falta de definição dessas regras decorrem dois problemas: I) o FNDE se restringe à verificação de pagamentos em duplicidade somente entre os programas regidos pela lei nº 11.273/2006 (desconsiderando os demais programas de pagamento de bolsas e suas respectivas legislações); II) diferença na cronologia de pagamentos entre o FNDE e a CAPES. O FNDE realiza a maior parte de seus pagamentos no mês subsequente. A CAPES, ao contrário, realiza seus pagamentos dentro do próprio mês corrente. Esse fato torna praticamente inviável a verificação de acúmulos indevidos no mês corrente, diferentemente do modelo similar adotado com o CNPq.

Uma forma de mitigar impactos causados pela diferença de cronologia seria a comparação entre o período total de vigência da bolsa de estudos, possibilitando análise prévia de intenções de pagamentos que serão ofertadas pelos órgãos. Entretanto, os dados disponibilizados pelo FNDE não apresentam informações sobre intenções de pagamentos, fato que limita a avaliação aos benefícios concedidos em meses anteriores. Com isso, as questões de cronologia de pagamentos não poderão ser tratadas pela CAPES. Essas questões somente poderão ser tratadas pelo FNDE através das informações relacionadas a intenções de pagamentos disponibilizadas pela CAPES via Webservice, fechando assim o ciclo de avaliações.

Diante disso, a DTI entende que a intervenção da Diretoria Executiva da CAPES junto ao FNDE (ou até mesmo junto ao MEC, se for o caso) se faz necessária para que sejam definidas, de forma clara e objetiva, as regras de vedação de acúmulo de bolsas entre a CAPES e o FNDE a serem implementadas nos sistemas, objetivando o cruzamento de informações e depuração de dados, de modo que ocorrências ou restrições de pagamentos nos sistemas informatizados não aconteçam de forma indevida. Estas regras devem ser definidas, com a participação de representantes da CAPES e do FNDE, considerando os diversos tipos de programas de fomento e modalidades de bolsa de ambos os órgãos. É imprescindível que, assim como acontece com o CNPq, tais regras constem em regulamentos e portarias conjuntas entre os órgãos, ou em instrumentos similares.

Análise da AUD: são evidentes os esforços despendidos pela DTI/CAPES no intuito de atender à recomendação e evitar os pagamentos em duplicidade com o FNDE. A opinião desta Auditoria Interna está em harmonia com a opinião da DTI no sentido de que é necessário que regras sejam definidas pelas duas Fundações e constem em portaria conjunta. Nessa perspectiva, e visto que a situação não foi completamente solucionada nas instâncias de TI das Fundações, recomenda-se que o teor deste tópico do relatório seja encaminhado, por instância superior da CAPES, ao FNDE, provocando essa instituição a juntar-se à CAPES na busca conjunta de uma solução para definição das regras de acúmulo.

Resposta: A recomendação da CGU e a determinação do TCU foram atendidas no que cabia à DTI/CAPES. Resta a definição, por parte das diretorias da CAPES e do FNDE, das regras de acúmulos permitidos.

Sobre benefícios concedidos a inadimplentes

Recomendação da CGU nº 175764 (auditoria de acompanhamento da Gestão n° 201604639): Avaliar os sistemas utilizados para a concessão, acompanhamento da execução e prestação de contas dos auxílios do AUXPE e implementar solução para a integração de informações, seja com um sistema único ou com a integração de todos os sistemas utilizados na unidade; atrelando a disponibilização de recursos financeiros ao cadastro dos projetos nos referidos sistemas e mediante verificação de eventual inadimplência dos beneficiários, tanto no âmbito das bolsas e auxílios concedidos pela Capes, inclusive AUXPE, quanto pelo registro de inadimplência no CADIN e SIAFI.

Recomendação do TCU – Item 9.5 do Acórdão 2057/2016 2ª Câmara (TC 010.609/2014-8 – Tomada de Contas Especial): avalie a conveniência e a oportunidade de prever, em seus editais, a impossibilidade de que alunos de ensino médio, graduação, pós-graduação, recém-doutores e pesquisadores sejam beneficiados com bolsas de estudo e/ou auxílios caso estejam inscritos no Cadastro Informativo de Créditos não Quitados de Órgãos e Entidades Federais - CADIN e na conta Diversos Responsáveis, do Sistema Integrado de Administração Financeira – SIAFI, com vistas a impedir que pessoas físicas, em débito para com órgãos e entidades federais, recebam recursos públicos.

Histórico das providências adotadas pela DTI/CAPES (Fonte: Docs. SEI nº 0216458, 0274534, 0312977, 0918872):

Setembro/2016: A DTI apresentou uma proposta de solução para a realização automática de consultas ao CADIN e SIAFI, com vistas a impedir pagamentos indevidos a inadimplentes. A proposta consiste num fluxo de procedimentos técnicos que abarcam: I) a extração de dados de todos os bolsistas, pesquisadores, consultores ativos e candidatos a bolsas ou auxílios; II) comparação desses dados com os cadastros de inadimplência no CADIN e SIAFI; e III) validação de bloqueio tanto da concessão quanto da realização de pagamentos de benefícios.

Outubro/2016: Os mecanismos de bloqueio foram aplicados, mas somente aos pagamentos de AUXPE. Verificou-se que, caso o mecanismo de bloqueio tivesse entrado em funcionamento, cerca de 2.927 beneficiários teriam seus benefícios retidos por estarem inscritos no CADIN ou na conta Diversos Responsáveis do SIAFI (Despacho CGS – SEI n° 0312977).

Novembro/2016: A presidência decidiu por não aplicar os mecanismos de bloqueio aos demais benefícios, nem incluir bolsistas no CADIN até que todas as questões estejam devidamente esclarecidas. Para isso, a CAPES instituiria uma comissão interna para analisar e propor alternativas para a solução desse assunto, bem como faria gestões junto ao TCU no sentido de esclarecer que, em sua avaliação, a questão deve ser melhor discutida, especialmente no que se refere a bolsas, por ser doação e recurso para subsistência do beneficiário

Análise da AUD: O bloqueio, de acordo com a proposta apresentada pela DTI, poderia ocorrer em dois momentos diferentes: no momento da concessão do benefício ou no momento do pagamento do benefício.

Quanto ao bloqueio no momento da concessão, discussões foram levantadas pelos gestores dos programas, pois alguns alegavam que, no momento da candidatura, o candidato ao benefício encontrava-se inadimplente, mas, na maioria dos casos, com processo de regularização em andamento. No geral, há um lapso de meses entre a candidatura até o pagamento do benefício. Tempo suficiente para o candidato regularizar a situação que deu causa à inadimplência. Se a situação não fosse regularizada até o momento do pagamento, outro candidato seria escolhido no lugar do inadimplente. Caso o bloqueio ocorresse já no momento da concessão, esses candidatos seriam de imediato impedidos de concorrer ao benefício.

Por outro lado, alguns gestores entendiam que se deveria sim realizar o bloqueio no momento da concessão, até mesmo como medida de construção de cultura de adimplência. Dessa forma, os beneficiários teriam mais cuidado para não ficar inadimplente com a CAPES ou qualquer outro órgão da Administração Pública.

Não havendo definição a respeito, a regra de bloqueio a beneficiários inadimplentes foi aplicada apenas ao AUXPE, sendo que o sistema encaminha automaticamente a recusa da proposta devido à inadimplência.

Ambas opções são válidas administrativamente - bloquear no momento da concessão ou apenas no momento do pagamento. A decisão, porém, precisa ser institucional, não sendo aconselhável aplicar regras diferentes para cada programa. É uma questão a ser levada para discussão da Diretoria Executiva da CAPES para definição da regra mais conveniente.

Em relação ao bloqueio no momento do pagamento, é relevante a preocupação da presidência da CAPES em discutir o assunto antes de aplicar o bloqueio a benefícios que já estão em andamento. Não foi identificado documento de instituição da comissão interna referida pela presidência nem registros referentes a discussão sobre o assunto. Essa auditoria interna entende que, decidida a regra para o bloqueio de novos benefícios, conforme discorrido no parágrafo anterior, e aplicada aos sistemas informatizados, as recomendações já estariam atendidas.

Cabe ressaltar que a regra deve ser definida, não apenas para os beneficiários já inscritos no CADIN ou no SIAFI, mas também para os beneficiários registrados como inadimplentes nos sistemas internos da CAPES. Por exemplo pode-se citar os egressos da DRI e da DPB que estão sendo diligenciados a prestar contas e

seus CPFs ainda não constam nos cadastros externos já citados.

Resposta: As recomendações foram atendidas no âmbito dos sistemas de pagamento, mas apenas para o AUXPE. As medidas de bloqueio estão prontas para implementação para os outros benefícios, faltando apenas a definição, por parte dos gestores, das regras para o bloqueio.

3.7. QUESTÃO DE AUDITORIA 7 - Os sistemas atendem às necessidades dos usuários?

A finalidade dos sistemas é atingir as reais necessidades dos usuários. Conforme Dias (1993, p. 163)[1], "não existe uma medida objetiva e direta para medir a eficácia de um sistema de informação. Em geral, ela é avaliada pela capacidade de o sistema desenvolvido apoiar os objetivos da empresa, segundo a percepção dos usuários do sistema".

No entanto, nem sempre as necessidades explicitadas pelo usuário refletem suas reais necessidades. Isso ocorre porque: (1) frequentemente, o usuário não está consciente de suas necessidades reais; (2) as necessidades podem mudar após terem sido explicitadas; (3) usuários diferentes podem ter ambientes operacionais diferentes e (4) é quase impossível consultar todos os tipos de usuários.

A AUD questionou, por meio da SA n° 1/2019 (0889285), se os usuários estariam satisfeitos em relação aos sistemas de pagamento de bolsas e auxílios da CAPES. Em resposta, a DTI informou: "entende-se que sim, uma vez que são atendidas as necessidades das Diretorias que utilizam os sistemas, em conformidade com o PDTIC vigente. Entretanto, não há registro de pesquisa de satisfação com relação a esse tipo de avaliação" (Memorando 10, Item 3/15/a - SEI n° 0897445).

Em março/2019, a equipe de auditoria realizou, por meio de questionário simples, uma pesquisa de satisfação com todas as diretorias e gabinete da presidência em relação aos referidos sistemas (Processo SEI n° 23038.005010/2019-28).

Análise da AUD: No geral, verificou-se que os sistemas atendem às necessidades primordiais das diretorias, mas carecem de melhorias no que se refere ao apoio à tomada de decisão por meio de relatórios gerenciais mais completos e confiáveis, à usabilidade e à integração com outros sistemas.

Foram reportados pelas diretorias as seguintes insatisfações:

SAE: Não gera relatórios confiáveis devido a falhas e falta de possibilidade de excluir evento; sistema lento; não atende às expectativas; o processo de pagamento é moroso e nada transparente, quando comparado à realização dos procedimentos via SEI; não se comunica (ou se comunica pouco) com os demais sistemas da CAPES; poderia ser melhor empregado como ferramenta de pagamento e de gestão (histórico de tramitação, histórico de pagamento, retorno de erros, consultas de pagamentos por filtros, relatórios gerenciais, etc); não possui perfil de consulta de beneficiários, o que dificulta o acesso a informações sobre pagamentos; arquitetura defasada e com diversas falhas na solicitação do pagamento, na transparência das ações, nas consultas, entre outros; os pagamentos dos consultores não são realizados de forma correta; apresenta falhas na solicitação de pagamento de consultores e retorno com erro do financeiro; não é dinâmico e didático; não atende às expectativas, pois sua utilização é morosa e o resultado final, em muitos casos, não é eficiente e eficaz; não atende às necessidades de controle da informação, pois não proporciona que essa consulta e verificação seja realizada no sistema; falta integração com os demais sistemas da CAPES, sobretudo com a Plataforma Sucupira e com o SEI; é de extrema importância que seja integrado com o banco de dados corporativo, o sistema financeiro e o SAP, de modo que as ações se tornem gerenciáveis e transparentes.

SAC: divergências de informações entre os relatórios e o demonstrativo apresentado em tela (erros na contagem de parcelas) que estão sendo resolvidas pela DTI aos poucos.

SCBA: está em constante processo de melhoria; há melhoria na articulação e comunicação para atendimento às demandas negociais; atende às necessidades de pagamento, mas não possui arquitetura de monitoramento das ações; é utilizado como base para tomada de decisões; é transparente aos beneficiários, uma vez que disponibiliza informações financeiras, orçamentárias, processuais e documentos de seus respectivos processos; há diversas oportunidades de melhoria a exemplo de permitir a consulta de informações de pagamentos com filtragem das informações; é de fácil utilização, tanto para a área técnica da CAPES quanto para os beneficiários – estes recebem um manual de utilização; atende às expectativas parcialmente, uma vez que melhorias e novas funcionalidades são solicitadas mensalmente; há algumas falhas importantes ainda não sanadas, a exemplo de pagamento de forma diferente da forma parametrizada; divergências de informações entre os relatórios e o demonstrativo apresentado em tela (erros na contagem de parcelas) que estão sendo resolvidas pela DTI aos poucos.

SGB: Não é intuitivo e não emite relatórios confiáveis, dificultando a gestão.

Financeiro: preocupação quanto ao nível de controle das informações por pare das áreas técnicas. O pagamento das bolsas é feito em nível de agregação que não permite conferência e verificações por parte da CGOF, a menos que esta consulte cada um dos demais sistemas. Sugestão: que o sistema apresente um relatório das etapas pelas quais as informações foram tratadas e os atestes das áreas técnicas em cada uma dessas etapas, previamente à assinatura do diretor.

Em relação a esse assunto, a DTI realizou, entre 20 de maio e 05 de junho de 2019, pesquisa de satisfação aos usuários, via formulário online encaminhado por e-mail, do qual constavam perguntas a respeito do grau de satisfação com o serviço prestado, a qualidade dos sistemas, se eles atendem às necessidades da CAPES, bem como solicitava sugestões de melhoria. Do universo de 756 usuários, 110 responderam ao questionário. Os resultados ainda não foram divulgados, mas a DTI informou, via *intranet*, que os dados estão sendo trabalhados qualitativamente e serão debatidos e divulgados para obter propostas e transformações que caminhem ao encontro das necessidades dos usuários.

Além disso, a DTI vem implementando Métodos Ágeis para o desenvolvimento das soluções de TIC da CAPES. Tais métodos têm por objetivo aproximar a TI das áreas de negócio, obtendo-se mais agilidade e aprendizado, além de proporcionar um clima mais cooperativo. Nesse sentido, já foram promovidas pela DTI três capacitações de servidores da CAPES como *Product Owner-PO,* tendo o último ocorrido em junho de 2019. Os *POs* são representantes escolhidos pelas diretorias que definirão todas as funcionalidades desejadas para as soluções, descrevendo-as e priorizando-as para a equipe da DTI.

Resposta: Sim, os sistemas atendem às necessidades primordiais das diretorias, no geral, mas carecem de melhorias no que se refere ao apoio à tomada de decisão por meio de relatórios gerenciais mais completos e confiáveis, à usabilidade e à integração com outros sistemas.

4. CONCLUSÃO

As cinco ações do PDTIC referentes aos sistemas de pagamento de bolsas e auxílios da CAPES estão em andamento, sendo que três serão replanejadas para o próximo PDTIC.

Os sistemas de pagamento apresentam as oito características de qualidade de *software* definidas pela norma ISO/IEC 25010:2011, quando da realização de pagamentos, carecendo de aperfeiçoamentos em pontos específicos.

Os riscos foram identificados, mas não foram avaliados, tratados e monitorados formalmente. Existem controles internos consistentes envolvidos no desenvolvimento e na utilização dos sistemas que são aptos a mitigar os riscos de natureza tecnológica, mas ainda não são suficientes para mitigar os riscos de natureza negocial.

As recomendações da CGU e do TCU foram atendidas no âmbito dos sistemas de pagamento. Para o completo atendimento, resta pendente a definição, por parte das unidades gestoras dos programas, definição de regras sobre acúmulos permitidos entre a CAPES e o FNDE e sobre medidas de bloqueio de pagamento a beneficiários inadimplentes.

No geral, verificou-se que os sistemas atendem às necessidades primordiais das diretorias, mas carecem de melhorias no que se refere ao apoio à tomada de decisão por meio de relatórios gerenciais mais completos e confiáveis, à usabilidade e à integração com outros sistemas.

Dos resultados encontrados, foram elaborados 06 achados de auditoria (Anexo I), que representam a base para as conclusões aqui expostas, bem como para as recomendações propostas no Anexo II.

Uma versão preliminar deste relatório foi encaminhada à área auditada em 15/07/2019. Em 05/08/2019, foi realizada reunião entre a equipe de auditoria e representantes da área auditada em que os achados foram discutidos com vistas a estabelecer, conjuntamente, medidas julgadas adequadas para mitigar as causas dos achados em questão.

Cumpre observar que o objetivo do presente relatório é o de assessorar os gestores para uma melhor segurança processual e alcance de objetivos estratégicos operacionais, auxiliando, orientando e avaliando a administração no desenvolvimento de suas atribuições. Conforme preceitua o Instituto dos Auditores Internos (*The Institute of Internal Auditors - IIA)*:

> "A Auditoria Interna é uma atividade independente e objetiva que presta serviços de avaliação e de consultoria e tem como objetivo adicionar valor e melhorar as operações de uma organização, auxiliando-a em alcançar seus objetivos, com uma abordagem sistemática e disciplinada apara avaliação e melhoria da eficácia dos processos de gerenciamento de riscos, de controle e de governança corporativa."

É o relatório.

ANEXO I - ACHADOS DE AUDITORIA

ACHADO N° 1 – PROBABILIDADE DE NÃO CONCLUSÃO DAS AÇÕES DO PDTIC NO PRAZO ESTABELECIDO (REFERÊNCIA: QUESTÃO DE AUDITORIA 1)

Das cinco ações do PDTIC analisadas nessa auditoria, três apresentam iminência de não conclusão no prazo estabelecido por possuírem iniciativas complexas ainda em fase de estudos preliminares e uma já teve o prazo previsto para término expirado.

Critério: Ações AE11, AE13 e AE17 do PDTIC 2017-2019 (integração com os sistemas de repasses de recursos do Governo Federal, com o SEI e com as plataformas Freire e Sucupira).

Condição: Apesar de todas as ações estarem em andamento e da realização de reuniões de acompanhamento, as seguintes iniciativas ainda estão em fase de estudos preliminares: utilização do SIMEC e Convênios para pagamentos do programa PRINT; solução para integração dos sistemas ao SEI; e mapeamento entre as plataformas Freire e Sucupira e definições de gerenciamento negocial e de cotas.

Considerando que restam poucos meses para o término do prazo previsto para a conclusão das ações, depreende-se que há grande probabilidade de que as ações não sejam concluídas. Inclusive, a ação OB3/N7/AE39 já teve o prazo previsto para término expirado.

Causa: uma causa possível é que não haja definição das necessidades estratégicas da CAPES antes da elaboração do PDTIC, nem uma análise de riscos para priorizar as ações necessárias para mitigar os riscos mais altos. Assim, cada diretoria demanda suas necessidades (que mudam muito por falta de planejamento) e, ao longo da execução do plano as prioridades vão sendo ordenadas.

Efeito: quantidade de ações constantes do PDTIC além da capacidade da DTI em desenvolvê-las; priorização equivocada das ações; maior tempo gasto em discussões para o entendimento das demandas; constantes alterações e conclusão fora do prazo previsto.

Conclusão: as ações do PDTIC estão sendo desenvolvidas, mas algumas requerem mais atenção ao prazo de conclusão.

Proposta de recomendação: recomenda-se que, caso a DTI constate que não será possível concluir essas ações de no prazo previsto, apresente, em antecipação, proposta de replanejamento para que essa necessidade não se estenda por mais tempo. Recomenda-se, também, que na elaboração do próximo PDTIC, sejam consideradas as prioridades das necessidades da instituição, baseadas nos objetivos estratégicos, em análise de riscos e na capacidade operacional da DTI para que seja possível executar a quantidade de ações propostas dentro do período estabelecido.

Comentário dos gestores: "as ações que não forem concluídas no âmbito do PDTIC 2017-2019 serão replanejadas para o próximo PDTIC, que já está em fase de elaboração. Também está sendo realizado estudo de capacidade para execução das ações do próximo PDTIC."

Análise da AUD: as medidas propostas pela DTI serão suficientes para atender à recomendação da auditoria. A equipe de auditoria irá monitorar a elaboração do PDTIC 2020-2023 e o estudo de capacidade para a execução das ações.

Recomendação final:

À DTI: considerar, na elaboração do PDTIC 2020-2023 as necessidades prioritárias da instituição, baseadas nos objetivos estratégicos, em análise de riscos e na capacidade operacional da DTI para que seja possível executar a quantidade de ações propostas dentro do período estabelecido. Prazo para atendimento: dezembro/2019.

ACHADO N° 2 – FRAGILIDADE NA SEGURANÇA DOS SISTEMAS DE PAGAMENTO - USUÁRIOS COM PERFIL DE ACESSO A SISTEMAS QUE NÃO UTILIZAM MAIS (REFERÊNCIA: QUESTÃO DE AUDITORIA 2).

Critério: ISO/IEC 25010:2011, segurança do software. Espera-se que haja controles internos estabelecidos com procedimentos de monitoramento da movimentação dos usuários e bloqueio dos perfis de acesso aos sistemas quando não fizer mais parte das atribuições do servidor a utilização de determinado sistema.

Portaria nº 137, de 20 de setembro de 2012 - Política de Segurança da Informação e Comunicações (PoSIC).

Condição: na listagem de usuários internos dos sistemas encaminhada pela DTI (SEI n° 0898545), constam vários usuários com perfil de acesso aos sistemas que não os utilizam mais (trocaram de lotação, saíram da CAPES, etc).

Causa: falta de procedimento de segurança para bloqueio de senhas; falta de informação por parte das diretorias das alterações de competência dos usuários e consequente necessidade de alteração ou exclusão de perfis.

Efeito: exposição ao risco de um usuário utilizar seu antigo perfil em benefício próprio ou de outrem com a possibilidade de sua ação passar despercebida pela gestão, pelos bloqueios dos sistemas e pelos controles internos e externos.

Conclusão: as oito características de qualidade dos sistemas estão presentes, quando da realização dos pagamentos, carecendo de aperfeiçoamentos em relação à segurança no que se refere ao controle do perfis de usuários.

Proposta de recomendação: recomenda-se que a DTI estabeleça procedimentos de segurança a serem executados periodicamente para verificação e atualização ou exclusão dos perfis de acesso aos sistemas por servidores e colaboradores, em parceria com as diretorias e com a Coordenação-geral de Gestão de Pessoas.

Comentário dos gestores: "essa fragilidade vai além dos sistemas de pagamento, abrangendo controles referentes a acessos a todos os sistemas de informação, ao wi-fi, às dependências físicas, etc. Uma medida que poderia dar início à mitigação dessa fragilidade seria a elaboração de normativo(s) que regulamente(m) as diretrizes instituídas pela Política de Segurança da Informação e Comunicações (PoSIC), publicada em 2012."

Análise da AUD: de fato, a fragilidade apontada vai além dos sistemas de pagamento. A AUD está de acordo com a sugestão da DTI em mitigá-la de forma mais abrangente por meio do cumprimento da PoSIC.

Recomendação final:

Ao Comitê Gestor de Tecnologia da Informação: prover os instrumentos necessários para o cumprimento das diretrizes estabelecidas pela Política de Segurança da Informação e Comunicações (PoSIC), conforme competência prevista no artigo 16 da Portaria nº 137, de 20 de setembro de 2012 (https://www.capes.gov.br/images/stories/download/legislacao/Portaria-66-16mai12-PoSIC.pdf). Prazo para atendimento: março/2020.

À DTI: elaborar e apresentar plano para manter atualizados os controles de acesso aos sistemas de informação, conforme responsabilidade prevista no artigo 21 da PoSIC, especialmente no que se refere aos sistemas que realizam operações de pagamento de bolsas e auxílio. Prazo para atendimento: dezembro/2019.

ACHADO N° 3 – AUSÊNCIA DE ANÁLISE DE IMPACTO, PROBABILIDADE E RISCO RESIDUAL NA GESTÃO DE RISCOS (REFERÊNCIA: QUESTÃO DE AUDITORIA 3)

Critério: Instrução Normativa Conjunta MP/CGU nº 01, de 10/05/2016 e Portaria GAB nº 37, de 20 de fevereiro de 2018.

Condição: A DTI identificou os riscos, classificando-os em natureza tecnológica e gerencial. Também informou os controles que foram criados para sua mitigação. No entanto, não foi apresentada análise de impacto e probabilidade para se definir o nível dos riscos, nem foi aferido o risco residual após implementação dos controles internos.

Causa: não é realizada gestão de riscos ou a gestão realizada não é formalizada.

Efeito: controles internos criados sem priorização em relação aos riscos mais altos; desconhecimento da efetividade dos controles para a mitigação dos riscos.

Conclusão: Os riscos foram identificados, mas não foram avaliados, tratados e monitorados formalmente.

Proposta de recomendação: recomenda-se que a DTI realize gestão de riscos, conforme instruções nos normativos vigentes, de forma a identificar, avaliar, tratar e monitorar os riscos referentes aos sistemas de pagamento da CAPES.

Comentário dos gestores: "a DTI faz uma espécie de gestão de riscos quando do início de um novo projeto, bem como no planejamento de contratações. Porém, não é realizada Gestão de Riscos, efetivamente, para as atividades da DTI como um todo, nem especificamente em relação aos sistemas de pagamento."

Análise da AUD: a gestão de riscos deve abranger todas as atividades da diretoria, não limitando-se aos projetos e contratações. Todas as unidades da CAPES ainda estão em fase de aprendizado e implementação da gestão de riscos de suas atividades. Gestão de riscos é um tema que está em alta e que será sistematicamente cobrado pelos órgãos de controle nos próximos anos. A AUD se dispoe a orientar a DTI no planejamento da gestão de riscos, no que se refere aos normativos vigentes sobre o tema.

Recomendação final:

À DTI: realizar gestão de riscos e controles internos em seus processos, conforme instruções nos normativos vigentes, de forma a identificar, avaliar, tratar e monitorar os riscos relativos às atividades da DTI, inclusive as atividades referentes aos sistemas de pagamento da CAPES. A gestão de riscos e controles internos deve estar alinhada à estratégia da Capes. Prazo para atendimento: junho/2020.

ACHADO N° 4 – INSUFICIÊNCIA DE MITIGAÇÃO DOS RISCOS DE NATUREZA NEGOCIAL (REFERÊNCIA: QUESTÃO DE AUDITORIA 5).

Os riscos negociais identificados pela DTI referem-se a pagamentos indevidos por acúmulo de bolsas e a beneficiários inadimplentes. Tais não têm sido mitigados de forma suficiente, visto que ocorrem, ainda que a cada ano em quantidade cada vez menor, alguns pagamentos indevidos.

Critério: Implementação de regras e restrições aos pagamentos.

Condição: percebem-se os esforços da DTI em promover ações de mitigação a esses riscos, por meio de implementação de regras de validação e restrições para evitar que ocorram pagamentos indevidos. No entanto, os riscos de natureza negocial não têm sido mitigados de forma suficiente, de forma que ainda ocorrem, anualmente, alguns pagamentos indevidos.

Causa: falta de clareza ou ausência de regras por parte das diretorias; dificuldades de troca de informações com o FNDE.

Efeito: ocorrência de pagamentos indevidos; questionamentos dos órgãos de controle.

Conclusão: Os controles internos existentes são aptos a mitigar os riscos de natureza tecnológica, mas ainda não são suficientes para mitigar os riscos de natureza negocial.

Proposta de recomendação, comentário dos gestores e recomendação final: mesmos do achado n° 5.

ACHADO N° 5 – NÃO APLICAÇÃO DE MECANISMOS DE BLOQUEIO DE PAGAMENTOS EM DUPLICIDADE E A BENEFICIÁRIOS INADIMPLENTES (REFERÊNCIA: QUESTÃO DE AUDITORIA 6).

Critério: Recomendação da CGU n° 153896 (auditoria de avaliação da gestão n° 201503635); Determinação do TCU – Item 1.7 do Acórdão nº 1397/2017 – TCU – 1ª Câmara (Processo TC-026.336/2015-4 - Prestação de Contas - Exercício: 2014); Recomendação da CGU nº 175764 (auditoria de acompanhamento da Gestão n° 201604639) e Recomendação do TCU – Item 9.5 do Acórdão 2057/2016 2ª Câmara (TC 010.609/2014-8 – Tomada de Contas Especial).

Condição: Os sistemas já possuem, construídas e prontas para implementação, rotinas automatizadas de verificação de acúmulos e bloqueio de pagamentos. Mas esses mecanismos foram implementados apenas para o AUXPE, não foram implementados para os outros programas.

Causa: ausência de definição clara sobre quais modalidades de bolsa são passíveis de acúmulo e quais não são; o FNDE se restringe à verificação de pagamentos em duplicidade somente entre os programas regidos pela lei nº 11.273/2006 (desconsiderando os demais programas de pagamento de bolsas e suas respectivas legislações); diferença na cronologia de pagamentos entre o FNDE e a CAPES; falta de definição, por parte dos gestores, das regras para o bloqueio de pagamento a inadimplentes.

Efeito: pagamento de benefícios em duplicidade com o FNDE; concessão e pagamento de benefícios a inadimplentes.

Conclusão: As recomendações da CGU e do TCU foram atendidas no âmbito dos sistemas de pagamento, mas apenas para o AUXPE. As medidas de bloqueio estão prontas para implementação para os outros benefícios, faltando apenas a definição, por parte dos gestores, das regras para os acúmulos permitidos e para o bloqueio de pagamento a inadimplentes.

Proposta de recomendação: recomenda-se que o teor deste tópico do relatório seja encaminhado, por instância superior da CAPES, ao FNDE, provocando essa instituição a juntar-se à CAPES na busca conjunta de uma solução para definição das regras de acúmulo. Recomenda-se também, que seja levado para discussão da Diretoria Executiva da CAPES, a necessidade de definição de regra, a nível institucional, mais conveniente sobre bloqueio de pagamento a inadimplentes. Se no momento da concessão ou apenas no momento do pagamento. Cabe ressaltar que a regra deve ser definida não apenas para os beneficiários já inscritos no CADIN ou no SIAFI, mas também para os beneficiários registrados como inadimplentes nos sistemas internos da CAPES. Por exemplo pode-se citar os egressos da DRI e da DPB que estão sendo diligenciados a prestar contas e seus CPFs ainda não constam nos cadastros externos já citados.

Comentário dos gestores: a DTI concorda com o entendimento da AUD de que o assunto necessita ser levado à Alta Administração da CAPES para definição de regras e padronização destas para todas as diretorias, no que se refere a pagamento de benefícios a inadimplentes e pagamentos em duplicidade com o FNDE, bem como contatar o FNDE para definição de tais regras em conjunto com a CAPES.

Recomendação final:

À presidência da CAPES: encaminhar ao FNDE o teor dos achados nº 4 e 5, bem como o desdobramento das questões de auditoria nº 5 e 6, convidando aquela instituição a juntar-se à CAPES na busca conjunta de uma solução para definição das regras de acúmulo de benefícios. Prazo para atendimento: 30 (trinta) dias a contar do recebimento deste relatório final.

À Diretoria Executiva: definir regra mais conveniente, a nível institucional, sobre bloqueio de pagamento a inadimplentes (se no momento da concessão ou apenas no momento do pagamento). Cabe ressaltar que a regra deve ser definida não apenas para os beneficiários já inscritos no CADIN ou no SIAFI, mas também para os beneficiários registrados como inadimplentes nos sistemas internos da CAPES. Por exemplo pode-se citar os egressos da DRI e da DPB que estão sendo diligenciados a prestar contas e seus CPFs ainda não constam nos cadastros externos já citados. Prazo para atendimento: novembro/2019.

ACHADO N° 6 – RELATÓRIOS GERENCIAIS INSATISFATÓRIOS PARA A TOMADA DE DECISÕES E CONTROLE DE INFORMAÇÕES (REFERÊNCIA: QUESTÃO DE AUDITORIA 7).

Os usuários dos sistemas reportaram insatisfações em relação aos relatórios extraídos dos sistemas de pagamento alegando que carecem de melhorias no que se refere ao apoio à tomada de decisão por meio de relatórios gerenciais mais completos e confiáveis.

Critério: relatórios gerenciais completos, com filtros que permitam a extração de informações de apoio à tomada de decisões, bem como ao controle interno e externo.

Condição: Além das insatisfações reportadas pelos usuários, a equipe de auditoria também encontrou dificuldades em gerar relatórios gerenciais, em filtrar informações e em cruzar as informações extraídas desses relatórios. Para obter as informações necessárias para a tomada de decisão, é necessário que o usuário acesse cada sistema envolvido, extraia os relatórios que necessita e tente consolidá-los manualmente.

Causa: sistemas internos e externos complexos e com tecnologia antiga; falta de clarezacdos usuários sobre suas necessidades de gestão; falta de integração entre os sistemas; o SCBA tem sido aos poucos construído com as necessidades de integração solicitadas pelas diretorias, mas, durante a fase de transição, algumas integrações ainda não foram implementadas; integrações com sistemas externos à CAPES dependem de funcionalidades e permissões pré-existentes que, às vezes, limitam a adequação dos sistemas internos àqueles.

Efeito: a falta de integração ou a integração parcial dos sistemas gera, por vezes, a necessidade de inserir as mesmas informações em sistemas diferentes, o que demanda mais tempo e força de trabalho; ocorrência de informações inseridas de forma diferente nos sistemas, dificultando o cruzamento e gerenciamento dos dados entre eles e prejudicando a extração de relatórios gerenciais; controle social também dificultado, bem como o controle realizado pelos órgãos de controle interno e externo; verificou-se que, em atividades de controle realizadas pela CGU nos últimos anos, a CAPES despendeu bastante tempo explicando quase que uma a uma das supostas impropriedades encontradas por aquele órgão de controle nos cruzamentos de dados realizados.

Conclusão: no geral, os sistemas atendem às necessidades primordiais das diretorias, mas carecem de melhorias no que se refere ao apoio à tomada de decisão por meio de relatórios gerenciais mais completos, confiáveis e de fácil extração.

Proposta de recomendação: recomenda-se que a DTI aperfeiçoe os modelos de relatórios dos sistemas de pagamento de acordo com as necessidade apresentadas pelos usuários ou avalie a possibilidade de desenvolver solução para produção de relatórios completos, de fácil extração e filtragem das informações, sem que seja necessário consultar vários sistemas. Sugere-se uma ferramenta de fácil utilização como, por exemplo, os painéis criados pelo governo federal (painel de compras, de obras, de viagens, etc.).

Comentário dos gestores: "há uma disparidade, entre as diretorias, de conceitos e termos utilizados nos programas da CAPES. Acredita-se que essa disparidade será progressivamente resolvida com a unificação dos sistemas. Quanto aos modelos de relatórios dos sistemas, não é viável construir, aumentar ou aperfeiçoá-los dentro dos sistemas, pois estes ficariam muito "pesados" e lentos. A DTI já tem em sua estrutura o Núcleo de Disseminação da Informação (NDI), que atende as diretorias nas consultas de dados, de acordo com as especificidades de cada uma. As consultas são realizadas em diversos painéis já existentes, (GeoCAPES, ADD...) e bancos de dados. A sugestão é de que cada diretoria designe um servidor, ou núcleo, que seja responsável por fazer essas consultas, de forma que seja estabelecido um padrão de dados e definidos modelos de como solicitar e extrair as informações. O NDI continuaria à disposição das diretorias, porém, não receberia demandas de diversos servidores, com visões e conceitos diferentes dentro da mesma diretoria. "

Análise da AUD: A equipe está de acordo com as sugestões da DTI e sugere avaliar a possibilidade de se unificar os painéis existentes num só e viabilizar a consulta ao público externo à CAPES.

Recomendação final:

À DTI:

- Avaliar e se manifestar sobre a possibilidade de unificar os painéis existentes num só e viabilizar a consulta, de forma intuitiva, não somente ao público interno da CAPES, mas também ao público externo. Prazo para atendimento: 30 (trinta) dias a contar do recebimento deste relatório final.

- Divulgar orientações a todas as unidades da CAPES sobre a importância e necessidade de padronização de conceitos, termos e nomenclaturas utilizados nos programas de fomento da CAPES para a extração mais eficiente e confiável de dados e informações. Incentivar a participação ativa de todas as diretorias no desenvolvimento da ação do PDTIC que trata do assunto (caso houver). Prazo para atendimento: 30 (trinta) dias a contar do recebimento deste relatório final.

- Solicitar a todas as diretorias e presidência, via SEI, a indicação de servidores responsáveis por fazer as consultas de informações junto ao NDI em nome da diretoria. De posse dos nomes indicados, realizar encontros entre o(s) técnicos do NDI e o(s) representante(s) das diretorias para definirem modelos para solicitar e para extrair as informações. Prazo para atendimento: 60 (sessenta) dias a contar do recebimento deste relatório final.

À DPB, DRI, DEB e DED:

Instituir grupo de trabalho composto por representante(s) da DPB, DRI, DEB e DED para propor, no prazo de 60 (sessenta) dias, uma padronização do vocabulário utilizado nos programas de fomento da CAPES, no que se refere a bolsas e auxílios (naquilo que é comum entre essas diretorias) com vistas a possibilitar o processo de unificação dos sistemas pela DTI, bem como melhorar a forma que as diretorias solicitam e extraem informações dos sistemas da CAPES. Prazo para atendimento: 30 (trinta) dias a contar do recebimento deste relatório final.

ANEXO II - RECOMENDAÇÕES

À DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO – DTI:

RECOMENDAÇÃO 1 - Considerar, na elaboração do PDTIC 2020-2023 as necessidades prioritárias da instituição, baseadas nos objetivos estratégicos, em análise de riscos e na capacidade operacional da DTI para que seja possível executar a quantidade de ações propostas dentro do período estabelecido. Prazo para atendimento: dezembro/2019. (Referência: achado n° 1).

RECOMENDAÇÃO 2 - Elaborar e apresentar plano para manter atualizados os controles de acesso aos sistemas de informação, conforme responsabilidade prevista no artigo 21 da PoSIC, especialmente no que se refere aos sistemas que realizam operações de pagamento de bolsas e auxílio. Prazo para atendimento: dezembro/2019. (Referência: achado nº 2).

RECOMENDAÇÃO 3 - Realizar gestão de riscos e controles internos em seus processos, conforme instruções nos normativos vigentes, de forma a identificar, avaliar, tratar e monitorar os riscos relativos às atividades da DTI, inclusive as atividades referentes aos sistemas de pagamento da CAPES. A gestão de riscos e controles internos deve estar alinhada à estratégia da Capes. Prazo para atendimento: junho/2020. (Referência: achado nº 3).

RECOMENDAÇÃO 4 - Avaliar e se manifestar sobre a possibilidade de unificar os painéis existentes num só e viabilizar a consulta, de forma intuitiva, não somente ao público interno da CAPES, mas também ao público externo. Prazo para atendimento: 30 (trinta) dias a contar do recebimento deste relatório final. (Referência: achado nº 6).

RECOMENDAÇÃO 5 - Divulgar orientações a todas as unidades da CAPES sobre a importância e necessidade de padronização de conceitos, termos e nomenclaturas utilizados nos programas de fomento da CAPES para a extração mais eficiente e confiável de dados e informações. Incentivar a participação ativa de todas as diretorias no desenvolvimento da ação do PDTIC que trata do assunto (caso houver). Prazo para atendimento: 30 (trinta) dias a contar do recebimento deste relatório final. (Referência: achado nº 6).

RECOMENDAÇÃO 6 -Solicitar a todas as diretorias e presidência, via SEI, a indicação de servidores responsáveis por fazer as consultas de informações junto ao Núcleo de Disseminação de Informações (NDI) em nome da diretoria. De posse dos nomes indicados, realizar encontros entre o(s) técnicos do NDI e o(s) representante(s) das diretorias para definirem modelos para solicitar e para extrair as informações. Prazo para atendimento: 60 (sessenta) dias a contar do recebimento deste relatório final. (Referência: achado nº 6).

AO COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO:

RECOMENDAÇÃO 7 - prover os instrumentos necessários para o cumprimento das diretrizes estabelecidas pela Política de Segurança da Informação e Comunicações (PoSIC), conforme competência prevista no artigo 16 da Portaria nº 137, de 20 de setembro de 2012 (https://www.capes.gov.br/images/stories/download/legislacao/Portaria-66-16mai12-PoSIC.pdf). Prazo para atendimento: março/2020. (Referência: achado nº 2).

À PRESIDÊNCIA DA CAPES:

RECOMENDAÇÃO 8 - encaminhar ao FNDE o teor dos achados nº 4 e 5, bem como o desdobramento das questões de auditoria nº 5 e 6, convidando aquela instituição a juntar-se à CAPES na busca conjunta de uma solução para definição das regras de acúmulo de benefícios. Prazo para atendimento: 30 (trinta) dias a contar do recebimento deste relatório final. (Referência: achados nº 4 e 5).

À DIRETORIA EXECUTIVA:

RECOMENDAÇÃO 9 - definir a regra mais conveniente, a nível institucional, sobre bloqueio de pagamento a inadimplentes (se no momento da concessão ou apenas no momento do pagamento). Cabe ressaltar que a regra deve ser definida não apenas para os beneficiários já inscritos no CADIN ou no SIAFI, mas também para os beneficiários registrados como inadimplentes nos sistemas internos da CAPES. Por exemplo pode-se citar os egressos da DRI e da DPB que estão sendo diligenciados a prestar contas e seus CPFs ainda não constam nos cadastros externos já citados. Prazo para atendimento: novembro/2019. (Referência: achados nº 4 e 5).

À DPB, DRI, DEB E DED:

RECOMENDAÇÃO 10 - Instituir grupo de trabalho composto por representante(s) da DPB, DRI, DEB e DED para propor, no prazo de 60 (sessenta) dias, uma padronização do vocabulário utilizado nos programas de fomento da CAPES, no que se refere a bolsas e auxílios (naquilo que é comum entre essas diretorias) com vistas a possibilitar o processo de unificação dos sistemas pela DTI, bem como melhorar a forma que as diretorias solicitam e extraem informações dos sistemas da CAPES. Prazo para atendimento: 30 (trinta) dias a contar do recebimento deste relatório final. (Referência: achado nº 6).

ANEXO III – CARACTERÍSTICAS DE QUALIDADE DOS SISTEMAS

A - Segurança dos sistemas

Pergunta da Auditoria	SGB	SAC	SCBA	SAE	FINANCEIRO
Quais são os requisitos de segurança?	Login no sistema utiliza o as tecnologias *Lightweight Directory Access Protocol* (LDAP) e Single Sign-On (SSO); utiliza o Sistema de Segurança e de Administração de Usuários da CAPES (Segurança/SAdmin) para autorização de acesso; utiliza o protocolo *Hyper Text Transfer Protocol Secure* (HTTPS); há necessidade de *token* com assinatura digital ICP Brasil para ordenação de pagamentos e ativação de vinculação; o histórico de operações realizadas pelos usuários (log) é registrado no sistema.	Login no sistema utiliza LDAP e protocolo HTTPS; utiliza o Segurança/SAdmin para autorização; há necessidade de *token* para ordenação de pagamentos; o *log* de operações é registrado no sistema.			Login no sistema utiliza LDAP e protocolo HTTPS; utiliza o Segurança/SAdmin para autorização; há necessidade de *token* para ordenação de pagamentos; o *log* de operações é registrado no sistema; o acesso ao sistema é restrito à Intranet da CAPES.
Há controle de verificação/validação dos dados de entrada e saída (caracteres inválidos, informações incompletas, incoerentes ou não autorizadas, limites, faixa de valores, duplicação, etc.)?	Há validação com relação a informações incompletas, incoerentes ou não autorizadas, limites, faixa de valores, caracteres inválidos, duplicação. Validação de duplicidade de pagamento de bolsas com CNPq e FNDE. O SCBA verifica e restringe o pagamento para beneficiário inscrito no CADIN e nas contas Diversos Responsáveis e Impedidos Judicialmente no SIAFI.				Validação de CPF dos beneficiários através da avaliação do dígito verificador módulo 11 e consulta na Receita Federal via serviço INFOCONV fornecido pelo MEC. Validação de inconsistência ou incompletude das informações nos processos de integração com os sistemas solicitantes de lotes de pagamentos de beneficiários através da checagem da quantidade total de beneficiários e de valores a serem pagos por lotes enviados. Validação de duplicidade de pagamento de bolsas e realizados junto aos sistemas internos e externos (FNDE e CNPq). Essa validação é realizada no momento do recebimento de uma lote de pagamentos enviado ao sistema Financeiro. Beneficiários identificados nas regras de duplicidades são retirados da solicitação de pagamento e retornados ao sistema de origem com a identificação de duplicidade ou impossibilidade de pagamento por acúmulo indevido de bolsas com FNDE ou CNPq.

Pergunta da Auditoria	SGB	SAC	SCBA	SAE	FINANCEIRO
Há controles de monitoramento (que verificam se os sistemas estão rodando dentro do intervalo de tempo esperado, se estão sendo executados na ordem correta e se têm a execução interrompida diante de uma falha no sistema)?	A CAPES faz uso de sistema de monitoria de ativos de rede e de aplicação Zabbix. Através desse sistema, são realizadas consultas periódicas a procura de inconsistências nos processos de comunicação e de disponibilidade dos serviços e sistemas envolvidos no processo de pagamento.				
Há controles criptográficos (que garantem a integridade, autenticidade e confidencialidade da informação)?	Utilização de mecanismos de criptografia de dados simétrica e assimétrica presentes nas tecnologias SSO, LDAP, no protocolo HTTPS e nos *tokens* de acesso ICP Brasil.				Utilização de mecanismos de criptografia simétrica e assimétrica presentes nas tecnologias SSO, LDAP, no protocolo HTTPS e nos *tokens* de acesso ICP Brasil. Utilização de Certificação Digital de Equipamento A1 ICP Brasil para garantir a integridade, autencidade e confidencialidade nos processos de comunicação com o SIAFI. Utilização do Protocolo de comunicação *Secure File Transfer Protocol* (SFTP) para garantir a integridade, autencidade e confidencialidade nos processos de comunicação com o Banco do Brasil e BBAméricas.
Há inventário completo e atualizado dos ativos de informação (ex: fabricante, versão, usuários internos, etc):	Há o Catálogo de Sistemas Informatizados da CAPES disponível no endereço http://gestao.capes.gov.br/, onde as todos os sistemas e aplicações desenvolvidas no âmbito da instituição estão cadastradas. No Catálogo, são mantidas informações sobre situação dos sistemas (Em projeto, Em Produção, em Desativação e Desativado), linguagens de programação, tecnologias, URLs de acesso, bases de dados utilizadas, dentre outras, de forma que a Coordenação-Geral de Sistemas possa realizar adequadamente as atividades de desenvolvimento e manutenção dos sistemas de informação do órgão. Em relação ao controle de versões e armazenamento dos códigos-fonte dos sistemas, a CGS utiliza a ferramenta Subversion, também conhecida como SVN. Para realização dos testes dos sistemas, são utilizadas as ferramentas JUnit, Mantis, Testlink e Selenium. Para automação dos processos de liberação de *releases*, são utilizadas as ferramentas Jenkins, Sonar e Nexus. Para publicação dos sistemas, são utilizados os servidores Apache HTTPD, Módulo PHP, Apache Tomcat, Red Hat JBoss. Os sistemas operacionais utilizados nas máquinas servidoras são Linux Ubuntu, Linux CentOS, Linux Red Hat e Microsoft Windows Server. Cabe ressaltar que as orientações tecnológicas e arquiteturais estão relatadas na Metodologia de Desenvolvimento de Sistemas da CAPES, disponível no endereço http://intranet.capes.gov.br/index.php/dti/procedimentos-e-normas/mds-capes.				
É realizada a identificação de vulnerabilidades que os ativos possuem e são aplicados patches de correção ou monitoramento constante da vulnerabilidade?	A identificação de vulnerabilidades e aplicação de *patches* é feita de acordo com a liberação dos mesmos por parte dos fabricantes e comunidades que mantém as tecnologias, ferramentas e servidores utilizados pela CAPES. Eventuais vulnerabilidades identificadas nos sistemas desenvolvidos pela CGS são imediatamente corrigidas por meio dos contratos citados, estabelecendo-se o grau de criticidade alto para os chamados a serem atendidos.				
Há processo automatizado de construção de trilhas de auditoria:	Os sistemas possuem rotinas de registro de *log* em tabelas específicas para as operações realizadas pelos usuários. Como exemplo, podemos afirmar todas as funcionalidades relacionadas às principais transações de ordenação de pagamentos nos sistemas possuem tabelas respectivas com o histórico das transações.				
Qual o nível de rastreabilidade dos sistemas? É possível consultar os dados de forma fácil e confiável?	Conforme mencionado no item anterior, os sistemas possuem registro de *log* em tabelas específicas para as operações realizadas pelos usuários. Sobre se é possível consultar os dados de forma fácil e confiável, os sistemas fornecem diversos relatórios para consulta, de acordo com as necessidades identificadas junto às Diretorias que fazem uso de tais sistemas.				

Fonte: Resposta à Solicitação de Auditoria n° 1/2019 (SEI n° 0897445)

B – Confiabilidade dos sistemas

Pergunta da Auditoria	SGB	SAC	SCBA	SAE	FINANCEIRO

Pergunta da Auditoria	SGB	SAC	SCBA	SAE	FINANCEIRO
Como é medida a confiabilidade dos sistemas (maturidade, tolerância a falhas e recuperabilidade)?	Sobre maturidade, não há medida formalmente estabelecida na instituição, mas é de consenso comum entre as Diretorias que utilizam os sistemas que, em condições normais, os pagamentos de bolsas e auxílios devem ser realizados em até 5 dias úteis após sua ordenação. Sobre tolerância a falhas, são medidos o tempo de disponibilidade dos sistemas em ambiente de produção. Sobre a recuperabilidade, são realizados procedimento de backup das bases de dados e dos códigos-fonte dos sistemas.				

Fonte: Resposta à Solicitação de Auditoria n° 1/2019 (SEI n° 0897445)

C – Eficiência e Eficácia dos sistemas

Pergunta de Auditoria	SGB	SAC	SCBA	SAE	FINANCEIRO
O tempo de resposta e velocidade de execução são satisfatórios?	Entende-se que os sistemas apresentam tempo de resposta e velocidade de execução satisfatória. Atualmente a CAPES paga, através dos sistemas, mais de 250 mil bolsas por mês, sem ocorrência de atrasos ou inconsistências nos pagamentos.				
O sistema faz o que foi proposto de forma satisfatória (funcionalidade)?	Entende-se que sim, de acordo com as necessidades das Diretorias que utilizam os sistemas e em conformidade com o PDTIC vigente.				
O sistema é de fácil operação (usabilidade)?	Entende-se que sim, de acordo com as necessidades das Diretorias que utilizam os sistemas e em conformidade com o PDTIC vigente. A CGS procura atender aos direcionamentos relacionados a usabilidade e acessibilidade de acordo com a e-MAG (vide http://emag.governoeletronico.gov.br/) e Planos/Avaliações de Acessibilidade da CAPES. Além disso, através do atendimento à necessidade N13 - "Intensificar o desenvolvimento de aplicativos móveis e inteligentes para os sistemas da CAPES" do PDTIC, a CGS tem intensificado esforços para liberação de funcionalidades por meio de aplicativos, como o App Bolsista CAPES.				
O sistema é de fácil manutenção/modificação/adaptação (escalabilidade)?	O sistema foi concebido antes 2010 e resultante de iniciativas de equipes de desenvolvimento de sistemas do MEC e FNDE, portanto possui complexidade alta e tecnologias antigas. De forma semelhante ao SAC, evita-se a realização de manutenções evolutivas, mas apenas para sua sustentação. Será futuramente substituído pelo SCBA.	Construído em tecnologia superada e em desativação pela CAPES. Não são realizadas novas implementações no sistema, que será substituído pelo SCBA.	As evoluções são realizadas constantemente através de *sprints*, conforme prevê a MDS 4.0, porém alterações neste sistema corporativo são feitas com extrema cautela dado sua importância. Há dificuldades de vazão do *backlog* de demandas nesta fase de expansão do sistema para as diversas diretorias. Em paralelo, atualmente está em execução o projeto SCBA 3.0 para modernização tecnológica do sistema.	Não é um sistema de fácil manutenção. Está prevista a reestruturação do sistema em tecnologia mais moderna, conforme ação AE18 - "Evolução do Sistema de Avaliação Educacional SAE, com integração ao SEI" do PDTIC vigente.	O sistema não é de fácil manutenção, modificação e adaptação devido à complexidade do negócio. Quanto à escalabilidade, as camadas de banco de dados e aplicação são altamente escaláveis. No entanto, a camada de integração com o SIAFI possui baixa escalabilidade devido à limitação do componente utilizado para a integração, que possui restrições de acesso simultâneo de vários usuários.
O sistema está disponível em estado operacional tempo suficiente (disponibilidade)?	Entende-se que sim, pois as interrupções de acesso a sistema ocorrem normalmente apenas para atualização de versão, que não demoram mais do que alguns minutos durante a semana, ou em situações extraordinárias de manutenção elétrica ou relacionada aos ativos de hardware e Sala Cofre do Edifício Sede da CAPES, que normalmente ocorrem em finais de semana ou período noturno, de forma planejada e com comunicação prévia a todos os usuários.				
Os usuários estão satisfeitos?	Entende-se que sim, uma vez que são atendidas as necessidades das Diretorias que utilizam os sistemas, em conformidade com o PDTIC vigente. Entretanto, não há registro de pesquisa de satisfação com relação a esse tipo de avaliação.				

Fonte: Resposta à Solicitação de Auditoria n° 1/2019 (SEI n° 0897445)

ANEXO IV - RISCOS E CONTROLES INTERNOS

Natureza do risco	Descrição do Risco	Controle Interno
Risco de natureza tecnológica	Erro na comunicação entre os sistemas CAPES (SCBA, SAC, SGB, SAE e Financeiro), no momento de envio de lotes de pagamento, podendo gerar pagamentos em duplicidade ou deixando de incluir pagamentos em uma solicitação de liberação de recursos (SLR), registrada no Sistema Financeiro.	Esse risco foi mitigado com a dupla validação dos dados enviados entre os sistemas. Para isso, o sistema de gestão de bolsa, ao enviar um lote de pagamentos para o Sistema Financeiro, envia também um resumo de todos os dados enviados para que o Sistema Financeiro possa checar a quantidade de beneficiários que estão sendo recebidos e o somatório total do valor a ser pago para o determinado lote de pagamentos;

		Caso sejam identificadas inconsistências, o Sistema Financeiro bloqueia automaticamente o lote de pagamentos, impedindo que sejam realizadas transações necessárias para a efetivação do pagamento; Qualquer erro identificado no processo é disponibilizado para consulta automática dos sistemas envolvidos para que sejam tomadas as devidas providências.
	Alto volume e consistência de dados trafegados entre as aplicações.	A comunicação entre os ativos do sistema utilizam atualmente uma conexão de rede de 1 gigabits por segundo. A comunicação VPN com o FTP do Banco do Brasil pode ocorrer por meio de solução de firewall PFsense, com comunicação de 1 gigabits por segundo. A CAPES faz uso de ferramenta de monitoria de ativos de rede e de aplicação Zabbix. Através dessa ferramenta, são realizadas consultas periódicas a procura inconsistências nos processos de comunicação e de disponibilidade dos ativos de rede e sistemas envolvidos no processo de pagamento.
Riscos de natureza negocial	Pagamentos indevidos a beneficiários por acúmulos de bolsas.	Validação interna: os sistemas da CAPES realizam validação entre si, para eliminar a possibilidade de concessão de bolsas em acúmulo indevidos, conforme estabelecido nas portarias e regulamentos de todos os Programas de Fomento da CAPES, bem como portarias conjuntas com outros órgãos. Esta validação é coordenada pelas diretorias gestoras de cada Programa CAPES, que solicitam à DTI a implementação das regras. Validação externa: mediante a troca de arquivos com o CNPq e consultas automatizadas aos serviços Webservices disponibilizados pelo FNDE, a CAPES mitiga a possibilidade de pagamento de bolsas acumuladas indevidamente, conforme estabelecido nas portarias: PORTARIA CONJUNTA Nº 1, DE 12 DE DEZEMBRO DE 2007; PORTARIA CONJUNTA Nº 2, DE 15 DE JULHO DE 2010; PORTARIA CONJUNTA Nº 2, DE 10 DE ABRIL DE 2013; e PORTARIA CONJUNTA Nº 2, DE 22 DE JULHO DE 2014.
	Pagamentos indevidos de bolsas e auxílios a beneficiários inadimplentes (CADIN, CONTRANSF e CONTAS DIVERSOS RESPONSÁVEIS).	Para os beneficiários inadimplentes registrados no CADIN, foi implementada integração entre o Sistema Financeiro da CAPES e a base de dados do Banco Central, permitindo a realização de consultas diárias e on-line quanto à adimplência de beneficiários. Os sistemas de gestão de bolsas e auxílios fazem uso desses dados através de consultas disponibilizadas pelo Sistema Financeiro da CAPES, para evitar a concessão indevida. Para os beneficiários inadimplentes cadastrados no CONTRANSF e CONTAS DIVERSOS RESPONSÁVEIS, o Sistema Financeiro da CAPES realiza consultas diárias ao SIAFI. De posse do retorno dessas informações, a CAPES tanto pode impedir a concessão de bolsas e auxílios quanto a realização de pagamentos para beneficiários inadimplentes ou impedidos judicialmente. Atualmente, tais restrições são aplicadas somente para os beneficiários de Auxílio Financeiro a Projeto Educacional ou de Pesquisa (AUXPE), mas podem ser expandidas para os demais beneficiários.

Fonte: Resposta à Solicitação de Auditoria n° 8/2018 (SEI n° 0805227)

[1] DIAS, D. DE S. Eficácia de sistemas de informação, participação do usuário e mudança organizacional. In: XVII ENCONTRO ANUAL DA ANPAD (1993: Salvador). **Anais...** Salvador: ANPAD, 1993. v. 2. p. 163-172.