MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA BAIANO
AUDITORIA INTERNA
Rua do Rouxinol,115 - Bairro do Imbuí - CEP: 41.720-052 - Salvador-BA
Fone: 3186-0046. E-mail: audin@ifbaiano.edu.br

TIPO DE AUDITORIA : OPERACIONAL
UNIDADE AUDITADA : INST. FED. DE EDUC., CIENC. E TEC. BAIANO
CÓDIGO : 158129
RELATÓRIO Nº : 10/2014
UCI : AUDIN/IF Baiano

RELATÓRIO FINAL DE AUDITORIA

Prezado Senhor,

Em atendimento ao Plano Anual de Atividades de Auditoria Interna – PAINT do exercício de 2014, apresentamos o resultado preliminar dos exames realizados sob atos e consequentes fatos de gestão do Campus Guanambi, Santa Inês e da Reitoria, em atendimento à ação IV.IX – Avaliação de Gestão da Tecnologia da Informação.

I. Introdução

Em conformidade ao PAINT 2014, os itens verificados foram avaliação acerca da existência de planejamento de TI, perfil dos recursos humanos envolvidos, procedimentos para salvaguarda da informação, capacidade para o desenvolvimento e produção de sistemas e procedimentos para contratação e gestão de bens e serviços de TI.

Para qualquer contratação na área de Tecnologia da Informação – TI deverá ser observado o que está posto na Instrução Normativa nº 02, de 16 de março de 2010, emanada pela Secretaria de Logística e Tecnologia da Informação – SLTI, a qual dispõe sobre as especificações padrões de bens de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática – SISP, do Poder Executivo Federal.

Todas as contratações de TI deverão ser precedidas de planejamento, elaborado em harmonia com o Plano Diretor de Tecnologia da Informação (PDTI), que, por sua vez, deverá estar alinhado com o planejamento estratégico do Instituto Federal Baiano.

II. Escopo da Auditoria

1) Os trabalhos de auditoria foram realizados mediante a verificação do cumprimento do PDTI – Plano Diretor de Tecnologia da Informação em função do PDI – Plano de Desenvolvimento Institucional e as práticas de TI do IF Baiano, em conformidade com as Instruções Normativas da Secretaria de Logística e Tecnologia da Informação e da observância às orientações realizadas pelo

Órgão Central de Controle Interno e Tribunal de Contas da União - TCU.

2) Verificação do atendimento à legislação vigente: Lei nº 8.666/93 e nº 10.520/02 e demais alterações; Decretos nº 5.450/05 e nº 7.892/13 para aquisição de bens permanentes, observância à Portaria do IF Baiano nº 1.275 de 13/08/2013 e à governança de TI no que se refere às políticas e controles de TI alinhados aos objetivos da Instituição.

3) A metodologia para avaliação da governança de TI no que se refere às políticas e controles de TI alinhados aos objetivos da Instituição restringiu-se a verificação da consistência das respostas ao questionário de governança de TI 2014 do TCU, também sendo utilizados tópicos do COBIT 2014 e norma ISO 17.799.

III. Resultado dos Exames

III.I Constatações

III.I.I Planejamento das atividades de tecnologia da informação

O Plano Diretor de Tecnologia da Informação – PDTI é um instrumento de planejamento, diagnóstico, gestão dos recursos e processos de Tecnologia da Informação que visa a atender às necessidades tecnológicas e de informação do instituto para um determinado período. Possibilita eliminar o desperdício, garantir o controle, aplicar recursos no que é mais relevante com o objetivo de melhorar o gasto público; sendo uma importante ferramenta de apoio à tomada de decisão para o gestor, habilitando-o a agir de forma proativa.

A elaboração e a atualização regular do PDTI pelos órgãos federais é uma orientação estabelecida no âmbito do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP, que agrega as atividades de planejamento, coordenação, organização, operação, controle e supervisão dos recursos de TI dos órgãos e entidades da administração pública federal.

Até o presente momento o PDTI vigente no IF Baiano é o que foi produzido no ano de 2010 para vigência até o ano de 2013, sua elaboração e a definição das atividades que o compõem foram fundamentadas em diagnósticos do estágio dos processos de trabalho e das tecnologias empregadas no instituto, à época.

Para este ano está previsto a reavaliação do PDTI pela Diretoria de Gestão de Tecnologia da Informação – DGTI, cuja ação se dará da seguinte forma: formação de grupo de trabalho com membros da DGTI para revisão e posterior submissão ao CGTI – Comitê Gestor de Tecnologia da Informação, o prazo previsto para conclusão dos trabalhos se dará no mês de outubro/2014, conforme explicitado em seu Plano de Ação Anual 2014.

III.I.II Manifestação da unidade auditada

"2. Em relação ao Plano Diretor de Tecnologia da Informação (PDTI), esclarecemos que sua vigência foi prorrogada por 01 (um) ano através da Resolução Nº 01/20141, em 19/03/2014, pelo Presidente do Comitê Gestor de Tecnologia da Informação (CGTI) *ad referendum* deste comitê, que chancelou a prorrogação durante a 5ª Reunião Ordinária do CGTI, ocorrida no período de 22 a 24/10/2014. Nessa reunião também foram discutidas propostas de alterações no documento que deverão ser efetuadas após a publicação do Plano de Desenvolvimento Institucional (PDI), prevista para o mês do corrente ano, tendo em vista o alinhamento estratégico do PDTI com o PDI."

III.I.III Recomendações

Elaborar novo Plano Diretor de TI alinhado ao Planejamento Estratégico do IF Baiano e de acordo com o "**Guia de Elaboração do PDTI do SISP**", da SLTI. Estabelecer metodologia de acompanhamento da implantação da política de TI do IF Baiano nos Campi, de forma a garantir sua efetividade. Diagnosticar e dar tratamento aos riscos de TI, contemplando essa estratégia no PDTI. Articular a estratégia de TI com a alta administração, levando em conta a gestão de riscos e dos

ativos de TI, segurança da informação, estrutura de pessoal e desenvolvimento de sistemas.

III.II Os procedimentos para salvaguarda da informação

O nível de maturidade do gerenciamento do processo de "Garantir a segurança dos sistemas" que satisfaça ao requisito do negócio para a TI de "manter a integridade da infraestrutura de informação e de processamento e minimizar o impacto de vulnerabilidades e incidentes de segurança" foi avaliado no âmbito da Diretoria de TI no IF Baiano.

Com relação à gestão corporativa da segurança da informação, apesar de a unidade possuir gestor de segurança da informação formalmente designado, a Instituição dispõe, ainda incipiente, de política de controle de acesso à informação e aos recursos e serviços de TI formalmente instituída como norma de cumprimento obrigatório nem dispõe de política de cópias de segurança (backup), apesar de existir sistema de backup em várias camadas, com replicação de dados por hora, backups em disco diários e em fita semanais.

Verificou-se a falta de ações para formalização de processo de gestão de vulnerabilidades técnicas de TI e a inexistência de processo de detecção e tratamento dessas vulnerabilidades, no entanto, são utilizadas ferramentas de monitoramento de comportamento (zabbix) e ferramentas de monitoramento de alterações em arquivos de configuração nos servidores. A central de processamento de dados não possui no-breaks compatíveis com a estrutura dos equipamentos, apesar de já terem sido adquiridos no-breaks adequados, porém, não instalados.

Por meio da Portaria nº 113, de 31/01/2014, foi instituído Grupo de Trabalho de Segurança da Informação, contudo, ainda não houve produção de documentos que lastreassem ações realizadas quanto à gestão dos riscos de TI. Dentre as ações preventivas propostas, destaca-se as manutenções periódicas para minimizar possíveis cenários de mau funcionamento.

III.II.I Segurança do ambiente lógico – segurança em redes

São utilizados mecanismos de proteção como: firewall, VPN e Certificado SSL para HTTPS. Esses meios são considerados adequados para a segurança do ambiente lógico.

III.II.II Manifestação da unidade auditada

"3. Em relação aos procedimentos para a salvaguarda das informações e gestão de ativos de TI, informamos que esta Diretoria está provendo, dentro de suas possibilidades, capacitação para seus servidores e solicitando reforço de recursos humanos para prover adequação às práticas consolidadas, a exemplo da norma ISO 17.799. A perspectiva repassada pela alta gestão da Instituição para a DGTI é a de que no ano de 2015 haverá maior incentivo à capacitação assim como um incremento de mão de obra através da admissão de novos servidores para integrar a equipe desta diretoria."

III.II.III Recomendações

Mapear os riscos de TI e implantar modelo de gerenciamento de riscos de no âmbito do Instituto. Considerar, na elaboração do PDTI, as orientações do "Guia de Elaboração do PDTI do SISP" quanto ao planejamento para o gerenciamento de riscos, de acordo com o planejamento estratégico da Instituição.

III.III Gestão de ativos físicos de TI

Em item respondido ao questionário do TCU referente a processo de gestão ativos, a Instituição não formalizou processo de gestão de ativos como norma de cumprimento obrigatório. No caso de existência de ações de gestão de ativos de TI, controle de acesso às instalações de processamento de dados e segurança das instalações quanto a ameaça de fogo, poeira, fumaça, vibração, vazamento de água, explosão, manifestações civis ou desastres naturais foi constatada ausência de qualquer dispositivo que previna tais eventos.

Foi identificada fragilidade no acesso ao "*datacenter*", onde são concentrados os equipamentos de processamento e armazenamento de dados, no sentido da inexistência de controle de acesso. Nesse ponto, é importante observar cuidados com a segurança física, com o intuito de prevenir o acesso físico não autorizado. Além disso, no espaço físico do *datacenter* poderia existir sistema inteligente de detecção de fumaça e extinção de incêndio com gás inerte, para não afetar os equipamentos. O acesso pode ser controlado por cartões eletrônicos e/ou biometria, monitorização permanente e acesso por porta eclusa.

III.III.I Manifestação do Gestor

"*O controle de acesso às instalações de processamento de dados é feito de forma precária, pois a porta do datacenter possui fechadura simples, não temos dispositivos contra ameaças de fogo, poeira, fumaça, vibração, vazamento de água, explosão, manifestações civis ou desastres naturais. O acompanhamento de treinamento da equipe é feito através de sistemas e planilhas*".

III.III.II Recomendação

Em atendimento a norma ISO 17.799 recomenda-se que seja elaborado um projeto de áreas de segurança que contemple escritórios fechados ou com várias salas dentro de um perímetro seguro que considere as ameaças de fogo, poeira, fumaça, vibração, vazamento de água, explosão, manifestações civis ou desastres naturais. Equipamentos instalados em áreas comuns exigem medidas de proteção específicas contra acesso não autorizado, dano ou furto. A norma sugere mecanismos de bloqueio (por exemplo, *time-out*) e treinamento específico para os prestadores de serviços de limpeza e manutenção, nos casos em que não haja expediente nas Unidades.

Sugere-se atualizar norma interna de segurança da informação e promover a aderência aos critérios de segurança do ambiente físico dos ativos de TI, em especial as instalações de processamento de dados.

III.IV Desenvolvimento de sistemas

A IN SLTI nº4/2010 conceitua Solução de Tecnologia da Informação como "conjunto de bens e serviços de Tecnologia da Informação e automação que se integram para o alcance dos resultados pretendidos com a contratação" e Área Requisitante da Solução como "unidade do órgão ou entidade que demande a contratação de uma Solução de Tecnologia da Informação". Segundo o Acórdão 1.480/2007-TCU-Plenário,

> *"Para se chegar aos benefícios, é importante que o órgão ou entidade defina todos os elementos a serem produzidos, além dos produtos e serviços propriamente ditos, de modo que esses produtos e serviços passem a ser encarados como parte de algo maior, que neste texto será denominado "solução de TI".*

Nessa linha, há a possibilidade de se desenvolver um sistema internamente, pela própria equipe de TI do Órgão ou contratar o desenvolvimento do sistema no mercado. Para isso, faz-se necessária a realização de estudos de viabilidade técnica e econômica para seleção de projetos. A tomada de decisão para a melhor escolha deverá contemplar os objetivos da Instituição estabelecidos no planejamento estratégico de TI em alinhamento com o planejamento estratégico da Entidade. Para isso, os processos de trabalho devem estar claramente definidos e alinhados.

Segundo o Gestor de TI, "além da falta de recursos humanos na DGTI, os demandantes de sistemas na maioria dos casos não assumem a postura de utilizador e gestor do sistema. A falta de vontade dos usuários finais é latente, seja por falta de conhecimento pessoal, habilidade e/ou comunicação. Já os gestores não têm o compromisso de cobrar e acompanhar o andamento das atividades demandadas deixando de lado e tendo a ilusão que ter um sistema é o mesmo que usufruir do sistema".

III.IV.I Constatação
1. Dificuldades da DGTI elaborar e desenvolver sistemas devido a descontinuidade do processo de elaboração desses sistemas.

III.IV.I I Recomendações
Considerando a falta de acompanhamento da elaboração de sistemas pelos usuários finais e dificuldades operacionais para desenvolvê-los, recomenda-se que, para elaboração e desenvolvimento de sistemas no âmbito do IF Baiano, seja formalizada abertura de processo administrativo, contendo a definição clara da solução de TI que se pretende alcançar, estudos de viabilidade e processos de trabalho claramente definidos.

III.V Aquisições de TI
O IF Baiano segue o entendimento do Acórdão 2094/2004-TCU-Plenário, no qual decide que: "todas as aquisições devem ser realizadas em harmonia com o planejamento estratégico da instituição e com seu plano diretor de informática, quando houver, devendo o projeto básico guardar compatibilidade com essas duas peças, situação que deve estar demonstrada nos autos referentes às aquisições."

Seguindo essa orientação e a Instrução Normativa n° 4 de 12 de novembro de 2010 foi elaborada a Portaria nº 1.275, em 13/08/2013, pela DGTI, a qual normatiza os procedimentos para aquisição de bens e serviços de TI no âmbito do IF Baiano, contendo um fluxograma do trâmite a ser seguido pelas áreas solicitantes quanto à solicitação de bens e serviços, para que estejam em consonância com o planejamento estratégico da instituição e seu plano diretor de informática.

Os processos licitatórios para aquisições de TI dos Campus Guanambi e Santa Inês não mostraram conformidade com a Portaria nº 1.275 de 13/08/2013 do IF Baiano, que normatiza os procedimentos para aquisição de bens e serviços de TI no âmbito do Instituto. Anexo à Portaria encontra-se o Documento de Oficialização da Demanda (DOD) de TI - Campus, de acordo com o art. 9°, § 2° da IN n° 4/10, emitida pela SLTI, que estabelece o fluxo a ser seguido nas aquisições de TI.

III.V.I Constatação
1 . Portaria nº 1.275, em 13/08/2013 necessita ser atualizada conforme art. 1º da IN SLTI nº 02/2012 e na IN SLTI nº 04/2014.

III.V.II Manifestação da unidade auditada
"4. Em relação às aquisições de TI, informamos que a DGTI, em diversas oportunidades relembra (divulgando no site da diretoria, e-mail institucional e em reuniões do Colégio de Dirigentes) aos gestores das unidades do IF Baiano a existência da Instrução Normativa MP/SLTI Nº 04 de 12 de novembro de 2010 e da Portaria IF Baiano Nº1.275 de 13 de agosto de 2013. Reforçaremos as ações de divulgação desses documentos no âmbito do IF Baiano."

III.V.III Recomendações
1. Reforçar a necessidade de atendimento à Portaria IF Baiano Nº1.275 de 13 de agosto de 2013 pelos Gestores do IF Baiano, no que se refere à aquisições de TI;
2. Atualizar a norma interna para aquisições, considerando o disposto no inciso II, parágrafo único do art. 1º da IN SLTI nº 02/2012 e na IN SLTI nº 04/2014.

CAMPUS GUANAMBI

Os pontos analisados foram: verificação do atendimento às recomendações exaradas no Relatório de Auditoria nº 26/2014 e avaliação do processo licitatório - Pregão 74/2014, para aquisição de bens

permanentes, em atendimento à Portaria nº 1.275 de 13/08/2013 e governança de TI no que se refere às políticas e controles de TI alinhados aos objetivos da Instituição.

Pregão Eletrônico: 74/2013 **Processo:** 23330.501599/2013-91 **Valor:** R$125.415,00 **Objeto:** Aquisição de 74 (setenta e quatro) notebooks para atender às necessidades do Campus			
DESCRIMINAÇÃO DO OBJETO	**QUANT.**	**EMPRESA VENCEDORA**	**VALOR**
Microcomputador Pessoal Notebook – marca ACER	08	Click Data Soluções Informática Ltda - ME	14.800,00
Microcomputador Pessoal Notebook – marca EVOLUTE	66	RWX Comércio e Representação de Informática Ltda - ME	110.615,00
		TOTAL GERAL =	**125.415,00**

Em consonância com o trabalho de auditoria, todo o processo acima foi apreciado em seus atos e documentos presentes nos autos e constata-se que o mesmo se encontra em aderência ao que preza a Lei nº 10.520/02 e Decreto nº 5.450/2005 (Pregão); Portaria nº 02/2010 SLTI (Compras Sustentáveis); à Lei nº 8.666/93 e suas alterações, bem como a formalização do processo (numeração de páginas, assinaturas em documentos que se fazem pertinentes, etc).

Há apenas uma desconformidade a ser considerada:

Ausência da adoção dos procedimentos da Portaria nº 1.275 de 13/08/2013 do IF Baiano

Encaminhado, em 26/06/2014, Solicitação de Auditoria nº 26/2014 a área responsável questionando a aquisição de notebooks sem a devida aderência à Portaria Interna, a qual normatiza a aquisição de bens e serviços de tecnologia da informação no âmbito do Instituto.

Manifestação da unidade auditada:

"Em resposta a solicitação de auditoria nº 26/2014, gostaria de salientar que não foi solicitado um parecer técnico de Setor de Tecnologia para aquisições ao Pregão nº 74/2013. Por essa razão não foram produzidos os documentos necessários."

Análise da Auditoria Interna:
O Gestor desconhece a existência de norma interna que regulamenta as aquisições de bens e serviços de TI.

Recomendação:
Recomenda-se o atendimento à Portaria nº 1.275 de 13/08/2013 do IF Baiano, que estabelece procedimentos internos de aquisições de bens e serviços de TI aos gestores da Reitoria e dos Campi.

CAMPUS SANTA INÊS

Foram apreciados os seguintes processos:

I) Processo: *23332.000453/2013-11*
Pregão Eletrônico: *34/2013* **Valor:** *R$35.702,88*
Objeto: *Aquisição de equipamentos para atender à demanda dos laboratórios de biologia e química nas aulas práticas do Campus*

II) Processo: *23332.000499/2013-21*
Pregão Eletrônico: *37/2013* **Valor:** *R$102.047,26*
Objeto: *Aquisição de equipamentos de informática e materiais destinados a montagem de laboratório para atender o Projeto Atlas Digital e às aulas de computação de designs gráficos do Campus*

Constatação
Ausência da adoção dos procedimentos da Portaria nº 1.275 de 13/08/2013 do IF Baiano

Um dos requisitos para que uma boa gestão seja assegurada é o atendimento às normas internas existentes, sejam elas: portarias internas, leis vigentes, instruções normativas e guias de boas práticas sejam observadas e aplicadas efetivamente, bem como a elaboração dos processos de aquisições de bens e/ou serviços estejam aderentes aos objetivos institucionais. Na situação descrita não há aderência à normativa interna.

Informamos que tal orientação foi encaminhada ao gabinete dos Campi para conhecimento e providências, em 14/Agosto/2013, através de e-mail conforme pode ser visto abaixo:

-------- Mensagem original --------

Assunto:	Cópia de Portaria
Data:	Wed, 14 Aug 2013 11:54:54 -0300 (BRT)
De:	Gabinete <gabinete@ifbaiano.edu.br>
Para:	Aécio José A P Duart <aecio.duarte@bonfim.ifbaiano.edu.br>, "Alex Batista Dias "<alex.batista@catu.ifbaiano.edu.br>, "Ariomar Rodrigues " <ariomar.rodrigues@lapa.ifbaiano.edu.br>, "AURELUCI ALVES DE AQUINO " <aureluci.aquino@guanambi.ifbaiano.edu.br>, CARLOS ELÍZIO COTRIM<carlos.cotrim@guanambi.ifbaiano.edu.br>, dap@gm.ifbaiano.edu.br, Euro Oliveira de Araújo<euro.araujo@urucuca.ifbaiano.edu.br>, Francisco Harley de Oliveira Mendonça<francisco.mendonca@valenca.ifbaiano.edu.br>,gabinete@bonfim.ifbaiano.edu.br,gabinete@catu.ifbaiano.edu.br,gabinete@gm.ifbaiano.edu.br,gabinete@guanambi.ifbaiano.edu.br,gabinete@itapetinga.ifbaiano.edu.br,gabinete@lapa.ifbaiano.edu.br,gabinete@si.ifbaiano.edu.br,gabinete@teixeira.ifbaiano.edu.br,gabinete@urucuca.ifbaiano.edu.br,gabinete@valenca.ifbaiano.edu.br, "Jose Dionisio "<jose.dionisio@itapetinga.ifbaiano.edu.br>, "Marcelito Trindade Almeida "<marcelito.almeida@teixeira.ifbaiano.edu.br>, NELSON VIEIRA DA SILVA FILHO<nelson.silva@si.ifbaiano.edu.br>, Valdir Jose de Almeida Fonseca<valdir.almeida@gm.ifbaiano.edu.br>, Yone Carneiro de Santana Gonçalves<yone.carneiro@catu.ifbaiano.edu.br>, "DAP "<dap@gm.ifbaiano.edu.br>,dap@catu.ifbaiano.edu.br,dap@bonfim.ifbaiano.edu.br, E-mail do DAP do campus<dap@guanambi.ifbaiano.edu.br>,dap@itapetinga.ifbaiano.edu.br,dap@lapa.ifbaiano.edu.br,dap@si.ifbaiano.edu.br,dap@teixeira.ifbaiano.edu.br,dap@urucuca.ifbaiano.edu.br,dap@valenca.ifbaiano.edu.br
CC:	andre.rezende<andre.rezende@ifbaiano.edu.br>

A Portaria visa também pôr em prática a utilização do Documento de Oficialização da Demanda de Tecnologia de Informação – DOD, tanto para a Reitoria quanto para os Campi, que após concluído seu trâmite deverá ser anexado ao processo de compras.

Em cumprimento aos trabalhos de auditoria os processos acima: **I** e **II** foram apreciados em seus atos e documentos presentes nos autos e seguiram os trâmites essenciais para que ocorressem. Constata-se que os mesmos se encontram em sua totalidade em aderência ao que preza a Lei nº 10.520/02 e Decreto nº 5.450/05 (Pregão Eletrônico); concordância às normas da ABNT NBR – 15448-1 e 15448-2 quanto aos critérios de sustentabilidade ambiental; à Lei nº 8.666/93 e suas alterações, bem como a sua formalização (numeração de páginas, assinaturas em documentos que se fazem pertinentes, etc) está em conformidade à legislação pertinente.

Recomendações
Observar o atendimento à Portaria nº 1.275 de 13/08/2013 do IF Baiano, que normatiza os procedimentos para aquisição de bens e serviços de TI no âmbito do IF Baiano.

IV. Considerações Finais

Diante do exposto, reitera-se a necessidade de realização de planejamento das ações de TI, ou seja, do que se pretende atender com recursos de TI, tendo em vista os riscos, gargalos e oportunidades. Necessário também articular uma estratégia de implementação da política de TI nos Campi junto a alta administração. O delineamento de previsão orçamentária, como norteador para implementação da política de TI, deve ser articulado junto à alta administração e balizador para a elaboração do novo PDTI.

Importante destacar a necessidade de atualizações das normativas internas sobre aquisições de bens e serviços de TI, tendo em vista as contantes atualizações nas normativas que orientam essas contratações no âmbito do Governo Federal. As normas editadas pelo Conselho Superior têm abrangência em todo o Instituto e também devem ser observadas pelos Campi.

Em face do acima exposto, submetemos o presente relatório à consideração superior, instruindo a necessidade de atenção quanto aos pontos onde houve recomendações da Auditoria, de modo a possibilitar oportunidade de manifestação quanto à medidas implementadas e considerações no prazo de até trinta dias úteis a contar do seu recebimento.

Salvador, 17 de novembro de 2014.

Flávia de Paula Dias
Contadora/AUDIN
Siape 1888200

Guilherme Principe de Oliveira Galheigo
Coordenador/AUDIN
Siape 2616370