



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: 41720052 - Salvador-BA  
Fone: 3186-0046. E-mail: [audin@ifbaiano.edu.br](mailto:audin@ifbaiano.edu.br)

**TIPO DE AUDITORIA: ACOMPANHAMENTO DA GESTÃO**  
**UNIDADE AUDITADA: INST.FED. DE EDUC., CIENC.E TEC.BAIANO –**  
**REITORIA**  
**CÓDIGO : 158129**  
**CIDADE : SALVADOR**  
**RELATÓRIO Nº: 09/2013**  
**UCI : AUDIN/IF Baiano**

## **RELATÓRIO DE AUDITORIA**

Prezado Senhor,

Em atendimento ao Plano Anual de Atividades do exercício de 2013, apresentamos os resultados dos exames realizados sob atos e consequentes fatos de gestão, ocorridos nesta Instituição.

### **I. Escopo da Auditoria**

I.I – Execução da ação IV. X – Gestão de Tecnologia da Informação, conforme disposto no PAINT 2013.

I.II - 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 Instituto, a conformidade com as Instruções Normativas da Secretaria de Logística e Tecnologia da Informação e observância das orientações realizadas pelo Órgão Central de Controle Interno e Tribunal de Contas da União.

I.III – Verificação do atendimento às recomendações exaradas no Relatório de Auditoria nº 03/2012, avaliação dos controles internos quanto à vigência de normas de segurança da informação e comunicação, uso seguro das redes sociais, em atendimento à Portaria nº 38 de 11/06/2012 e governança de TI, no que se refere às políticas e controles de TI alinhados aos objetivos da Instituição.

### **III. RESULTADO DOS EXAMES**

#### **III.I Governança e Gestão de TI**

Segundo André Luiz Furtado Pacheco, da Secretaria de Fiscalização de Tecnologia da Informação – Sefti – TCU, “Governança refere-se a todas possibilidades e mecanismos que ajudam as múltiplas partes do negócio a avaliar condições e opções para determinar a direção, o monitoramento, a conformidade, o desempenho e o progresso; alinhando, desta forma, os planos e os objetivos do negócio, visando atingir as metas da organização.” (grifo nosso)

Entende-se que, para que a governança esteja assegurada, é necessário que hajam mecanismos para que manuais ou normas internas sejam aplicados e aderentes aos objetivos institucionais, ou seja, existência de “possibilidades e mecanismos” alinhados à estratégia do negócio. A Gestão de TI são as ações desenvolvidas na utilização desses mecanismos e possibilidades para alcançar um resultado almejado.

##### **III.I.I Capacitação em TI**

Em resposta ao questionário de avaliação dos controles internos e governança de TI encaminhado à Diretoria de Tecnologia da Informação, verificou-se que existe Plano de Capacitação da Área de Tecnologia da Informação, com o objetivo de “direcionar uma proposta de capacitação às Unidades de Tecnologia da Informação e Comunicação (UTIC) e a Diretoria de Gestão e Tecnologia da Informação (DGTI).” De fato, observou-se que existiu um cronograma de execução de cursos “Open Ldap”, “Zimbra”, “Administração de Redes Linux”, Zabbix” e “Invasão de Redes” e diversos servidores dos Campi foram treinados na Reitoria.

#### **Manifestação da Diretoria de Tecnologia da Informação**

“A demanda por capacitação é um processo perene e cíclico. Sendo assim, constará no Planejamento Anual desta Diretoria”

#### **Recomendação**

Identificar as necessidades de treinamento e capacitação na Reitoria e nos Campi, de acordo com as necessidades de cada área da tecnologia da informação e conforme o grau de risco de TI. A capacitação do pessoal de TI, a ser considerada no Planejamento Anual da DGTI, deverá estar condizente com as atividades a serem desenvolvidas nas unidades de TI nos Campi e Reitoria, além de estarem respaldadas com os objetivos estratégicos de TI, constantes do PDTI da Instituição. Havendo limitação de recursos, as prioridades de TI devem ser levantadas e discutidas com os Gestores da Reitoria e Campi.

### **III.1.II Segurança da Informação**

A Política de Segurança da Informação não foi amplamente divulgada a todos os usuários de recursos de TI, sejam eles internos ou externos. Observou-se que não existe norma interna que institui critérios para uso seguro das redes sociais nem servidor responsável nomeado para a função de Agente Responsável, apesar de existir Comitê de Segurança da Informação e Comunicação.

No Relatório Mensal de Incidentes de Segurança, fornecido pela Rede Nacional de Ensino e Pesquisa, foram notificados 38 incidentes na Instituição, no período de fevereiro a abril, sendo que em agosto foi detectado um incidente no item “Fraude” do Relatório, correspondente à violação de direitos autorais. Segundo o Diretor de Gestão de TI, as Normas de Segurança da Informação encontram-se em processo de elaboração.

Segundo o Comitê Gestor da Internet no Brasil, os antivírus são programas que procuram detectar e, então, anular ou remover os vírus de computador. Um bom antivírus deve:

- identificar e eliminar a maior quantidade possível de vírus e outros tipos de malware;
- analisar os arquivos que estão sendo obtidos pela Internet;
- verificar continuamente os discos rígidos (HDs), flexíveis (disquetes) e unidades removíveis, como CDs, DVDs e pen drives, de forma transparente ao usuário;
- procurar vírus, cavalos de tróia e outros tipos de malware em arquivos anexados aos e-mails;
- criar, sempre que possível, uma mídia de verificação (disquete ou CD de boot) que possa ser utilizado caso um vírus desative o antivírus que está instalado no computador;
- atualizar as assinaturas de vírus e malwares conhecidos, pela rede, de preferência diariamente.

Existe proteção antivírus na rede interna da Reitoria, com dispositivo de atualização da versão do software. Apesar dos benefícios, o antivírus não pode impedir que uma ameaça explore alguma vulnerabilidade em um computador. Nesse ponto, um firewall pode controlar o acesso de ameaças nas redes de computadores.

A Política de Segurança da Informação não contempla processo de Gestão de Riscos, monitoramento e análise periódica de riscos, apesar da adoção de uma nova solução de firewall e segmentação das redes de computadores que compõem a infraestrutura de conectividade. Segundo o TCU, na publicação “Boas práticas em segurança da informação”, “O monitoramento dos sistemas de informação é feito, normalmente, pelos registros de log, trilhas de auditoria ou outros mecanismos capazes de detectar invasões. Esse monitoramento é essencial à equipe de

segurança de informações, já que é praticamente impossível eliminar por completo todos os riscos de invasão por meio da identificação e autenticação de usuários.”

### **Manifestação da Diretoria de Tecnologia da Informação**

“As normas de Segurança da Informação foram elaboradas. O dito documento foi aprovado pelo Comitê Gestor de TI no dia 18/11/2013 (Anexo I)”.

### **Análise da manifestação do auditado**

Verificou-se que a norma interna de segurança da informação contempla gestão de riscos, nos níveis estratégico e tático, porém, não institui critérios para uso seguro das redes sociais.

### **Recomendação**

Ao Comitê Gestor de TI:

Considerar, na Norma de Segurança da Informação do IF Baiano, critérios de Uso Seguro das Redes Sociais e submeter à aprovação da Alta Administração.

À Diretoria de Gestão Tecnologia da Informação:

Coordenar e supervisionar o desenvolvimento da Política de Segurança da Informação. Propor diretrizes estratégicas de Segurança da Informação e Comunicações (SIC) para a gestão do uso seguro das redes sociais. Fomentar o fortalecimento da cultura de Segurança da entidade, no que diz respeito ao uso seguro das redes sociais.

Aos Diretores Gerais dos Campi e Gestores da Reitoria:

Implementar as ações necessárias para garantir a segurança dos sistemas de informação. Aprovar as diretrizes estratégicas alinhadas à Segurança da Informação e Comunicações, que norteiam o uso seguro das redes sociais no Instituto. Nomear um servidor público, ocupante de cargo efetivo, para a função de Agente Responsável pela gestão do uso seguro de cada perfil institucional nas redes sociais, com o seguinte perfil profissional: capacidade de estabelecer bons relacionamentos interpessoais, de interagir e dialogar com as demais áreas presentes nas redes sociais, proativo e, principalmente, que conheça e entenda o negócio do órgão ou entidade da APF a que esteja vinculado.

### **III.1.III Aquisição de bens e serviços de Tecnologia da Informação**

Segundo a Instrução Normativa SLTI nº 04, de 19/0/2008, art. 3º, “As contratações de que trata esta Instrução Normativa deverão ser precedidas de planejamento, elaborado em harmonia com o Plano Diretor de Tecnologia da Informação - PDTI, alinhado à estratégia do órgão ou entidade.”

Existem procedimentos internos para aquisição de bens e serviços de Tecnologia da Informação, delineados em fluxograma de processos estabelecido pela DGTI

(Diretoria de Gestão de TI). Verificou-se que esses procedimentos têm sido atendidos, embora exista a necessidade de consolidá-los nos Campi. Existe a necessidade de implementação desse processo no âmbito do IF Baiano, envolvendo todos os níveis de gestão do Instituto.

Nos contratos de aquisições de bens e serviços de TI constatou-se a adoção parcial de acordos de níveis de serviço, o que pode prejudicar o atendimento às necessidades dos usuários do serviço.

### **Recomendação 1**

Adotar acordos de níveis de serviço em contratos de TI. Planejar as aquisições de bens e serviços de TI conforme estudo prévio das necessidades da Entidade.

### **Manifestação da Diretoria de Tecnologia da Informação**

“No que tange a Diretoria de Gestão de Tecnologia da Informação (DGTI), as aquisições de bens e serviços são norteadas por acordos de níveis de serviços. Ademais, na última reunião do Comitê Gestor de TI, realizada no dia 18/11/2013 deliberou-se o acompanhamento semestral dos contratos de TI (anexo I).”

### **Recomendação 2**

Sugere-se que o acompanhamento seja contínuo para contratos de serviços de TI, com fiscal do contrato capacitado da área de TI. As necessidades de TI da Entidade devem ser planejadas e o parecer da unidade de TI deve constar nos autos dos processos de compras e serviços de TI. Implementar e acompanhar os procedimentos de aquisição de bens e serviços de Tecnologia da Informação conforme Portaria nº 1275, vigente a partir de 13/08/2013.

## **III.II Atendimento às recomendações elencadas no Relatório de Auditoria nº03/2013**

### **Assunto – Cumprimento do Plano Diretor de Tecnologia da Informação**

#### **Constatação III.IV**

Não atendimento aos itens: Serviços Básicos de Tecnologia da Informação e Comunicação e Padronização dos Endereçamentos e Nomes dos Recursos de Tecnologia da Informação e Comunicação.

### **Recomendação**

Ao Comitê Gestor de Tecnologia da Informação do IF Baiano, promover política de acompanhamento, execução de projetos e diretrizes que envolvam padrões de integração, qualidade e segurança de informações necessárias ao atendimento de serviços básicos de TI no âmbito dos Campi.

À Diretoria de Gestão de Tecnologia da Informação do IF Baiano buscar a uniformização dos serviços básicos de TI, atendendo as diretrizes do CGTI, desenvolvendo ações junto às Coordenações de TI nos Campi.

Aos Diretores Gerais dos Campi do IF Baiano viabilizar, com o assessoramento da DGTI, os serviços básicos de TI e comunicação.

Aos controles internos administrativos da Reitoria promover o devido acompanhamento da implantação das providências, alinhando à estratégia do Plano de Desenvolvimento Institucional do IF Baiano às soluções de Tecnologia da Informação.

### **Providências adotadas**

“Será encaminhado ao Comitê Gestor de Tecnologia da Informação (CGTI) a proposta para criação de uma política de acompanhamento, execução de projetos e diretrizes. No que tange a Diretoria de Gestão de Tecnologia da Informação (DGTI), existe a busca constante em definir/manter a padronização dos recursos tecnológicos deste Instituto”

### **Análise das providências adotadas**

A Diretoria de Gestão de TI reconhece a importância do atendimento aos serviços básicos de TI no cumprimento do Plano Diretor de TI, no entanto, há providências a serem adotadas no aspecto da governança de TI, ou seja, definir métodos e diretrizes alinhados à gestão de TI.

### **Constatação III.V**

Ausência de execução da Política de Segurança da Informação e Comunicação.

### **Recomendação**

Implementar políticas de segurança da informação, conforme item 9 do documento “Política de Segurança da Informação e Comunicação”, no âmbito da Reitoria e dos Campi.

### **Providências adotadas**

“As normas de Segurança da Informação foram elaboradas (Anexo I). O dito documento será encaminhado para análise e aprovação do CGTI no dia 18/11 (Anexo II).”

### **Análise das providências adotadas**

Política de Segurança da Informação pendente de implementação. Reitera-se a recomendação exaradas no Relatório de Auditoria nº 03/2013. A Política de Segurança da Informação carece de apreciação e aprovação pelo Órgão máximo da Instituição.

## **Recomendação**

Sugere-se que o Conselho Superior aprecie a proposta de segurança da informação do Instituto. Uma vez aprovada, o acompanhamento da implementação das ações de segurança da informação deve ser realizado pelos órgãos competentes nos Campi e Reitoria.

## **Constatação III.VI**

Utilização parcial de software livre como padrão de sistema operacional e aplicativos no âmbito do IF Baiano.

## **Recomendação**

Realizar estudo de viabilidade envolvendo o levantamento de custos de implantação das tecnologias livre e proprietária definindo detalhadamente os processos associados ao ciclo de vida do software, identificando os custos efetivos que o uso de uma determinada tecnologia irá demandar.

## **Providências adotadas**

“A DGTI formalizará um projeto para execução em 2014, relativo ao estudo de viabilidade envolvendo o levantamento de custos para implantação de soluções livres”

## **Análise das providências adotadas**

Apesar da utilização parcial de software livre em ferramentas de escritório, verificamos a ausência da utilização de sistema operacional baseado no Linux. Existe o interesse, pela Diretoria de Gestão de TI, de ações voltadas para implantação do software livre no IF Baiano em sua totalidade. Recomenda-se a avaliação de viabilidade da implantação de software livre, destacando a redução de custos caso seja implantado em sua totalidade.

## **III.III Desenvolvimento e Produção de Sistemas**

O organograma da Diretoria de Gestão de TI contempla uma Gerência de Sistemas, que tem como competências “Propor soluções de software para o sistema de informação do IFBAIANO, gerenciar o desenvolvimento de sistemas informatizados, propor e disseminar normas e padrões para o desenvolvimento de sistemas informatizados, garantir, em conjunto com a GETEC, a interoperabilidade dos sistemas de informação do IFBAIANO, manter atualizado levantamento de demandas de sistemas no âmbito do IFBAIANO, propor normas e critérios para a disseminação de informações automatizadas, coordenar e supervisionar a contratação e o desenvolvimento de sistemas informatizados para o IFBAIANO.”

Em resposta à Solicitação de Auditoria nº 40/2013, a DGTI informou que são desenvolvidas soluções de TI, como segue abaixo:

Sigla	Sistemas	Acompanhamento
CEN	Sistema de Certificação do ENEM	<a href="http://redmine.ifbaiano.edu.br/projects/certifica-enem">http://redmine.ifbaiano.edu.br/projects/certifica-enem</a>
DIP	Sistema de emissão de diplomas e certificados	<a href="http://redmine.ifbaiano.edu.br/projects/dip">http://redmine.ifbaiano.edu.br/projects/dip</a>
SRA	Sistema de Registro de Ações Institucionais	<a href="http://redmine.ifbaiano.edu.br/projects/sra">http://redmine.ifbaiano.edu.br/projects/sra</a>
ALM	Sistema de Gestão do Almoxarifado	<a href="http://redmine.ifbaiano.edu.br/projects/alm">http://redmine.ifbaiano.edu.br/projects/alm</a>
COT	Sistema de Gestão de Contatos Institucionais	<a href="http://redmine.ifbaiano.edu.br/projects/cot">http://redmine.ifbaiano.edu.br/projects/cot</a>
CON	Sistema de Gestão de Contratos	<a href="http://redmine.ifbaiano.edu.br/projects/con">http://redmine.ifbaiano.edu.br/projects/con</a>
PAT	Sistema de Gestão Patrimonial	<a href="http://redmine.ifbaiano.edu.br/projects/pat">http://redmine.ifbaiano.edu.br/projects/pat</a>
PRT	Sistema de Controle de Protocolo	<a href="http://redmine.ifbaiano.edu.br/projects/prt">http://redmine.ifbaiano.edu.br/projects/prt</a>
VEI	Sistema de Gestão de Veículos	<a href="http://redmine.ifbaiano.edu.br/projects/vei">http://redmine.ifbaiano.edu.br/projects/vei</a>
SCS	Sistema de Gestão do Catálogo de Serviços	<a href="http://redmine.ifbaiano.edu.br/projects/scs">http://redmine.ifbaiano.edu.br/projects/scs</a>
MAN	Administração do Sistema	<a href="http://redmine.ifbaiano.edu.br/projects/mad">http://redmine.ifbaiano.edu.br/projects/mad</a>

Foi verificada a existência de procedimentos formalizados para desenvolvimento das soluções de TI. Existem servidores encarregados de levantar as necessidades de informatização das rotinas administrativas.

### **Considerações finais**

Ante o exposto, submetemos o presente relatório às considerações da unidade auditada e autoridade superior, de modo a possibilitar oportunidade de manifestação quanto a medidas implementadas e considerações, no prazo de até trinta dias úteis, a contar do recebimento.

Salvador, 27 de novembro de 2013.

Guilherme Príncipe de Oliveira Galheigo  
Coordenador/AUDIN