UNIVERSIDADE FEDERAL DE PERNAMBUCO
GABINETE DO REITOR/AUDITORIA INTERNA

NATUREZA DA AUDITORIA	**:**	**ACOMPANHAMENTO**
CÓDIGO DA UNIDADE	**:**	**154728 / 153101 / 153409**
UNIDADE GESTORA	**:**	**PROCIT / NTI / PROGEST**
RELATÓRIO FINAL	**:**	**006/2017**

GESTÃO DE TECNOLOGIA DA INFORMAÇÃO

1. INTRODUÇÃO

Em conformidade com o item 15 do Plano Anual de Auditoria Interna/2017, a Auditoria Interna apresenta neste Relatório o resultado dos exames realizados pelos Auditores Internos da UFPE.

O presente Relatório Final trata de Auditoria de Acompanhamento, realizada com o objetivo de analisar a Gestão de Tecnologia da Informação, verificando a sua regularidade, o cumprimento dos normativos e o controle interno. Os trabalhos foram realizados em estrita observância à Cartilha de Procedimentos de Auditoria da Controladoria Geral da União, bem como ao seguinte conjunto de legislações e boas práticas:

- Instrução Normativa nº 04/2010 DO SLTI/MPOG e alterações.
- Lei nº 10520/2002.
- Decreto nº 7.579, de 11 de outubro de 2011.
- Decreto nº 3.505, de 13 de junho de 2000.
- NBR ISO /IEC 17799:2005.
- NBR ISO/IEC 20000 – SERVIÇOS DE TI.
- NBR ISO/IEC 27000 – SEGURANÇA DA INFORMAÇÃO.
- NBR ISO/IEC 27001:2006 (ABNT, 2006).
- NBR ISO/IEC 27002:2005 (ABNT, 2005).
- NBR ISO/IEC 27005:2008 (ABNT, 2008).
- Cartilha de Procedimentos de Auditoria da Controladoria Geral da União.

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

- Manual de Auditoria de Sistemas do TCU.
- Manual de Boas Práticas em Segurança da Informação do TCU – 2012.
- Norma complementar nº 03, do DSIC/GSI/PR.
- Norma complementar nº 02/N01/DSIC/GSI/PR.
- Norma complementar nº 04/N01/DSIC/GSI/PR.
- Norma complementar nº 06/N01/DSIC/GSI/PR.
- Regimento Interno da Auditoria Interna da UFPE.
- Instrução Normativa nº 1 de 13 de junho de 2008.
- Acórdão nº 2.094/2004 - TCU/Plenário.
- Acórdão nº 1.603/2008 - TCU/Plenário.
- Acórdão nº 562/2006 - TCU/Plenário.
- Acórdão nº 1.521/2003 - TCU/Plenário.
- Acórdão nº 1.598/2006 - TCU/Plenário.
- Acórdão nº 758/2011 - TCU/Plenário.
- Acórdão nº 1.233/2012 - TCU/Plenário.
- Acórdão nº 265/2010-TCU/Plenário.
- Acórdão nº 1.558/2003-TCU/Plenário.

2. ESCOPO

Os trabalhos foram realizados dentro das normas e técnicas de auditoria utilizadas no Serviço Público Federal, em quantidade, profundidade e extensão julgadas necessárias nas circunstâncias, pautando-se nos aspectos da legalidade, legitimidade, eficiência e economicidade.

A auditoria realizada buscou avaliar o Planejamento Estratégico de Tecnologia da Informação da Instituição, os processos de aquisição de bens e serviços de tecnologia da informação e a Política de Segurança da Informação, verificando a sua regularidade, o cumprimento dos normativos e o controle interno.

Neste sentido, avaliamos o Plano Diretor de Tecnologia da Informação (PDTI), no intuito de verificar a sua adequação aos requisitos estabelecidos pelo SISP e sua conformidade com o Plano de Desenvolvimento Institucional (PDI) e com o Plano Estratégico Institucional (PEI).

Analisamos a Política de Segurança da Informação da UFPE e normas relacionadas, bem como as práticas adotadas em relação ao Sistema de Backup, proteção antivírus e restrição de acesso às informações.

Por fim, no intuito de analisar a conformidade nos processos de aquisição de bens e serviços, foram tomados como referência, para composição da base de cálculo do trabalho, a relação dos bens de Tecnologia da Informação, adquiridos pela Progest e pelo Núcleo de Tecnologia da Informação (NTI) no exercício de 2016, bem como dos serviços de TI com contratos vigentes até 2016. Constatou-se um valor total de R$ 6.114.549,62 (seis milhões, cento e quatorze mil, quinhentos e quarenta e nove reais e sessenta e dois centavos). Desse universo foram

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

auditados R$ 2.713.880,84 (dois milhões, setecentos e treze mil, oitocentos e oitenta reais e oitenta e quatro centavos), equivalente a cerca de 44,38% do total.

3. METODOLOGIA

Para a coleta, tratamento e análise dos dados necessários à avaliação prevista no escopo da auditoria foram utilizados os seguintes procedimentos metodológicos:

3.1. A seleção da amostra foi realizada com base na relação dos bens de TI adquiridos pela Progest e pelo Núcleo de Tecnologia da Informação (NTI) no exercício de 2016 bem como os serviços de TI com contratos vigentes até 2016. A AUDINT, utilizando o critério de materialidade e criticidade, selecionou os casos de maior valor.

3.2. Utilizando a metodologia descrita no item 3.1, foram selecionados **02** processos de contratação de serviços de TI que totalizam R$ R$ 2.713.880,84 (dois milhões, setecentos e treze mil, oitocentos e oitenta reais e oitenta e quatro centavos), os quais foram:

Nº LICITAÇÃO	PROCESSO	FORNECEDOR	VALOR	PRAZO DE VIGÊNCIA
66/2012	23076.024847/2015-96	TECNOSET INFORMÁTICA PRODUTOS E SERVIÇOS LTDA	R$ 976.657,09	04/06/2017
258/2013	23076.046320/2013-51	SIG SOFTWARE & CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO	R$ 1.737.223,75	04/02/2018

3.3. Com o fito de obter documentos e informações para subsidiar os exames, foram expedidas as Solicitações de Auditoria:

Nº da S.A.	Responsável	Documentos Solicitados	Objetivo da Solicitação
11/2017 de 01/07/2017	Coordenação de Governança de Tecnologia da Informação / Assessoria da Pró-Reitoria de Comunicação, Informação e Tecnologia da Informação e	• Plano Diretor de Tecnologia da Informação – PDTI 2017-2018; • Situação atual de execução do PDTI 2015-2016; • Documentação que defina de quem é a responsabilidade de elaboração e aprovação do PDTI (ex.: Regimento Interno, Portarias, etc); • Documentação do processo de elaboração do PDTI 2015-2016 e PDTI 2017-2018 (ex.: Atas de reunião, documentos de homologação etc.); • Documento que formaliza a criação de um comitê diretivo de TI. • Documentação que comprove a atuação do Comitê Diretivo de TI (ex.: atas de reunião, ofícios, memorandos, portarias).	Analisar o Planejamento Estratégico de Tecnologia da Informação.

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

		• Lista das ações de TI executadas em 2016 e em 2017 • Processo de Gerenciamento de Riscos relacionado ao PDTI	
12/2017 de 01/07/2017	Diretoria de Licitações e Contratos - DLC	• A relação dos processos licitatórios para aquisição de bens e serviços de TI, contendo as seguintes informações: número do processo licitatório, objeto, empresa contratada, e valor contratado.	Analisar a regularidade da aquisição de Bens e Contratação de Serviços de Tecnologia da Informação
13/2017 de 01/07/2017	Coordenação de Tecnologia da Informação	• Política de Segurança da Informação e Comunicações (POSIC) e demais normas que contenham diretrizes e procedimentos relacionados à segurança da informação e comunicações, e suas atualizações; • Portaria ou documento similar de aprovação da POSIC, ou expresse o apoio/aprovação do dirigente máximo à POSIC; • Documento que formaliza a criação de um comitê de Segurança da Informação; • Portaria de nomeação do Gestor de Segurança da Informação e Comunicações; • Relatório de Testes de verificação do funcionamento do grupo de servidores, gerador e no-break	Analisar a Política de Segurança da Informação e Comunicações (POSIC)

3.4. Em complemento, foram realizadas visitas *in loco* em setores administrativos da Reitoria e do Campus Universitário, no intuito de verificar a efetividade da proteção anti-vírus nos computadores da UFPE. Realizamos testes de observância também no Centro de Informática no intuito de verificar o controle de acesso ao Data Center.

3.5. Solicitamos por e-mail ao Núcleo de Tecnologia da Informação esclarecimentos quanto a forma de armazenamento e arquivamento das cópias de segurança, a adequação dos servidores backup as necessidades institucionais e controle de acesso ao Data Center.

3.6. O roteiro para análise da documentação foi elencado com base na legislação correlata.

4. OBJETIVOS GERAIS E ESPECÍFICOS

O objetivo dessa ação de auditoria consistiu em avaliar a legalidade, legitimidade e economicidade dos processos de aquisições de bens e serviços de tecnologia da informação; verificar as principais políticas de segurança da informação e comunicação e sua difusão junto à Instituição bem como avaliar o Plano Diretor de Tecnologia da Informação (PDTI) e sua conformidade com o Plano de Desenvolvimento Institucional (PDI) e com o Plano Estratégico

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

Institucional (PEI). Os procedimentos aplicados visaram responder as seguintes questões de auditoria:

1. Na UFPE há um Comitê de Tecnologia da Informação e um Comitê de Segurança da Informação? Se sim, são atuantes?
2. Há um Plano Diretor para área de Tecnologia da Informação (PDTI) em vigor?
3. O Plano Diretor de Tecnologia da Informação (PDTI) abrange o conjunto mínimo de itens definidos no modelo de referência do Guia de Elaboração de PDTI do Sistema de Administração de Recursos de Tecnologia da Informação do Poder Executivo Federal (SISP)?
4. O PDTI está alinhado com os objetivos do negócio do órgão definidos no Plano Estratégico Institucional (PEI) e com as metas propostas do Plano de Desenvolvimento Institucional (PDI)?
5. O PDTI está sendo efetivo para direcionar as ações de TI? As contratações de TI estão alinhadas com o PDTI ou documento similar?
6. As metas propostas no PDTI estão sendo alcançadas?
7. As contratações de Soluções de TI estão em conformidade com a IN04 2010 da SLTI? São baseadas nas necessidades reais do órgão/entidade? As soluções de TI contratadas correspondem as mais viáveis economicamente?
8. Os processos licitatórios relacionados à contratação de Soluções de TI foram baseados em critérios objetivos, sem comprometimento do caráter competitivo do certame, e realizados conforme a IN04 2010 da SLTI?
9. Existe uma Política de Segurança da Informação e Comunicações (POSIC) e demais normas que contenham diretrizes e procedimentos relacionados à segurança da informação e comunicações, e suas atualizações formalizadas? A Política de Segurança da Informação e Comunicações (POSIC) é amplamente divulgada?
10. Os computadores servidores e estações de trabalho estão protegidos contra os meios mais comuns de contágio de vírus? Há indícios recentes de problemas decorrentes da proliferação de vírus de computador? Há algum treinamento ou projeto para conscientização de usuários para saberem como combater ou lidar em caso de ocorrência de vírus?
11. Os servidores backup atendem a necessidade da Universidade? O armazenamento e arquivamento das cópias de segurança são realizados em locais e espaços diferentes dos servidores e equipamentos que foram copiados? Sistemas críticos e banco de dados estão concentrados no Data Center? Existe uma política e rotina de procedimentos de controle de acesso ao Data Center?
12. A UFPE possui uma política de manutenção e revogação de acessos ao sistema SIG?
13. Existe um Plano de Tratamento de Riscos de Segurança da Informação e Comunicações – GRSIC?
14. Existe um Programa de Gestão de Continuidade do Negócio?
15. A UFPE possui um Plano de Treinamento em Segurança da Informação?

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

5. RESULTADO DOS EXAMES

AREA 01: CONTROLES DA GESTÃO

SUBÁREA 04: CONTROLES INTERNOS

ASSUNTO: GESTÃO DE TECNOLOGIA DA INFORMAÇÃO

O planejamento estratégico em tecnologia da informação envolve o mapeamento das necessidades institucionais e a identificação das possíveis oportunidades para implementar soluções conforme as diretrizes existentes, alinhando os objetivos de negócio com a tecnologia, possibilitando assim, uma melhor aplicação dos recursos, com mais economicidade e efetividade. Considerando que os riscos de segurança da informação estão relacionados de maneira significativa com processos e recursos de TI, uma estratégia bem elaborada fornece ao gestor o suporte necessário para melhorar seu controle sobre os dados institucionais e torna-se fundamental para que as informações institucionais se mantenham seguras por meio de políticas que promovam a atualização constante dos métodos de segurança da informação.

Nesse sentido, foram realizadas análises de auditoria das quais resultaram as informações e as constatações apresentadas neste Relatório Preliminar.

5.1 INFORMAÇÕES

Sobre o tema, as ações de auditoria permitiram a identificação das seguintes informações abaixo descritas, as quais são consideradas boas práticas realizadas pela unidade auditada ou corresponde a problemas identificados no decorrer da auditoria para os quais já foram tomadas providências no sentido de solucioná-los.

1. INFORMAÇÃO – COMITÊ GESTOR DE COMUNICAÇÃO, INFORMAÇÃO E TECNOLOGIA DA INFORMAÇÃO ATUANTE E COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (CSIC)

UNIDADE AUDITADA: 154728 – PRÓ-REITORIA DE COMUNICAÇÃO, INFORMAÇÃO E TECNOLOGIA DA INFORMAÇÃO

Verificamos por meio de diligências que a UFPE possui um Comitê Gestor de Comunicação, Informação e Tecnologia da Informação (PROCIT) atuante, criado por meio da Portaria nº 07, de 25 de Julho de 2014, responsável pela aprovação do Plano Diretor de Tecnologia da Informação (PDTIC), conforme recomendação do Tribunal de Contas da União - Acórdão nº 1.603/2008-Plenário,

> Promovam ações com o objetivo de disseminar a importância do planejamento estratégico, procedendo ações voltadas à implantação e/ou aperfeiçoamento de planejamento estratégico institucional, planejamento estratégico de TI e comitê diretivo de TI.

Observou-se que, embora não esteja formalizada no Regimento Interno, a responsabilidade pela elaboração, monitoramento e revisão do Planejamento Estratégico de Tecnologia da Informação compete à Coordenação de Governança de TI, da Diretoria de Tecnologias. De acordo com informações concedidas pelo Pró-reitor, essa atribuição será inserida no

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

Regimento Interno da PROCIT até o final de 2017.

Certificou-se também que foi criado um Comitê de Segurança da Informação e Comunicações (CSIC) por meio da Portaria Normativa Nº 9 de 19 de setembro de 2014, alterado pela Portaria Normativa nº 7 de 19 de maio de 2015 e nomeado um Gestor da segurança da Informação, por meio da portaria nº 5527 de 13 de novembro de 2014, em atenção às determinações do TCU nos Acórdãos 380/2011 Plenário e 2938/2010 Plenário, a saber:

> **Acórdão 380/2011 Plenário**
> (...) monitore o funcionamento do comitê gestor de segurança e tecnologia da informação – CSTI de maneira a que este exerça suas atribuições;
> **Acórdão 2938/2010 Plenário**
> em atenção ao artigo 13 da Resolução/CNJ nº 90/2009, institua Comitê de Segurança da Informação e Comunicações, observando as práticas contidas na NBR ISO/IEC 27002, item 6.1.2 – Coordenação de segurança da informação; 9.2.6 – em atenção ao princípio constitucional da eficiência, nomeie Gestor de Segurança da Informação, observando as práticas na NBR ISO/ IEC 27002, item 6.1.3 – Atribuição de responsabilidade para segurança da informação (item 3.14).

Dessa forma, tais ações realizadas pela PROCIT são consideradas boas práticas na Governança de Tecnologia da Informação.

2. INFORMAÇÃO – ALINHAMENTO DO PDTI COM OS OBJETIVOS INSTITUCIONAIS DO ÓRGÃO DEFINIDOS NO PEI E NO PDI

UNIDADE AUDITADA: 154728 – PRÓ-REITORIA DE COMUNICAÇÃO, INFORMAÇÃO E TECNOLOGIA DA INFORMAÇÃO

Ao analisar o alinhamento do PDTI ao Plano estratégico Institucional (PEI) verificamos que cada objetivo descrito no PDTI faz referência explícita aos objetivos institucionais do órgão, descritos no PEI. Verificamos também que as metas propostas no PDTI estão alinhadas as propostas do Plano de Desenvolvimento Institucional, conforme preconiza o TCU no Acórdão nº 1.603/2008-Plenário: "Adotem providências com vistas a garantir que as propostas orçamentárias para a área de TI sejam elaboradas com base nas atividades que efetivamente pretendam realizar e alinhadas aos objetivos do negócio".

3. INFORMAÇÃO – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (POSIC) APROVADA

UNIDADE AUDITADA: 154728 – PRÓ-REITORIA DE COMUNICAÇÃO, INFORMAÇÃO E TECNOLOGIA DA INFORMAÇÃO

Verificamos que a Política de Segurança da Informação e Comunicações (POSIC) da UFPE e outras normas de segurança da informação ainda não foram aprovadas pelo Conselho de Administração da UFPE e consequentemente ainda não estão publicadas. Embora tenha sido aprovada pelo Comitê de Segurança da Informação e Comunicações (CSIC) em 03/10/2016, a mesma encontra-se em processo de análise no Gabinete do Reitor.

Solicitamos esclarecimentos que justifiquem a morosidade na aprovação da POSIC uma vez

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

que se trata de instrumento necessário e fundamental para garantir a efetiva proteção dos dados, informações e conhecimentos gerados e a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações, conforme ABNT NBR ISSO/IEC 17799:2005. O TCU em seus acórdãos 1233/2012 Plenário e 758/2011 Plenário estabelece que:

> **Acórdão 758/2011 Plenário**
> 9.2.6. – em atenção à Instrução Normativa GSI/PR 1/2008, art. 5º, VII, implante Política de Segurança da Informação e Comunicações, com observância das práticas da Norma Complementar 03/IN01/DSIC/GSIPR.
> **Acórdão 1233/2012 Plenário**
> 9.15.12. estabeleça a obrigatoriedade de que os entes sob sua jurisdição implementem os seguintes controles gerais de TI relativos à segurança da informação (subitem II.8): 9.15.12.4. estabelecimento de política de segurança da informação, à semelhança das orientações contidas na NBR ISO/IEC 27.002, item 5.1 – Política de segurança da informação.

CAUSA

Aguardo da análise da PoSIC pelo Reitor e pelos Pró-Reitores e dificuldade de agendamento de uma reunião exclusiva do Conselho de Administração para tratar da aprovação da PoSIC.

MANIFESTAÇÃO DA ENTIDADE AUDITADA

A Política de Segurança da Informação e Comunicações (PoSIC) foi aprovada pelo Comitê de Segurança da Informação e Comunicações (CSIC) em 03/10/2016. Em julho/2017 foi apresentada para o Reitor e Pró-Reitores.

A experiência aprendida com outras instituições demonstra que para o sucesso da implantação de qualquer política faz-se necessário o apoio e envolvimento da alta administração. Assim, optou-se por, primeiramente, apresentar a PoSIC para o Reitor e Pró-Reitores antes de encaminhá-la para o Conselho de Administração.

A importância e densidade da PoSIC requer que a mesma seja objeto único da reunião do Conselho de Administração o que atrasou sua inclusão na pauta.

*A PoSIC foi aprovada pelo Conselho de Administração da UFPE em **18/08/2017**.*

No tocante aos encaminhamentos, a Coordenação de Segurança da Informação:

a) *Iniciará o processo de formação da Equipe de Tratamento de Incidentes de Segurança da Informação. Para tanto será realizada, com a presença do Pró-Reitor, reunião com o NTI e o CIn, para formar a equipe de tratamento de incidentes de segurança da informação - ETISI.*
b) *Elaboração do Plano de Implantação da PoSIC com o apoio da ETISI.*
c) *Elaboração do Plano de Divulgação da PoSIC com o apoio da ETISI.*
d) *Será planejado um workshop com as universidades: UFC, UFRN e UFPB coordenado pela UFPE com o objetivo de colaboração no que tange ao cumprimento das recomendações e determinações quanto a Segurança da Informação.*

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

ANÁLISE DA AUDITORIA INTERNA

Com base no pronunciamento do Comitê de Segurança da Informações e Comunicações verificamos que no decorrer desta ação de Auditoria a PoSIC foi aprovada pelo Conselho de Administração da UFPE. A etapa subsequente é a elaboração dos planos de implantação e de divulgação da PoSIC com o apoio da ETISI. Dessa forma a AUDINT acata os esclarecimentos da Pró-Reitoria de Comunicação, Informação e Tecnologia da Informação – PROCIT, considerando, assim, esta constatação atendida.

4. INFORMAÇÃO – CÓPIAS DE SEGURANÇA E RESTRIÇÃO DE ACESSO AO DATA CENTER

UNIDADE AUDITADA: 153101 – NUCLEO DE TECNOLOGIA DA INFORMAÇÃO

Verificamos que a Universidade realiza o armazenamento e arquivamento das cópias de segurança em locais distintos dos servidores e equipamentos que foram copiados conforme recomendação do TCU no Acórdão 71/2007 Plenário:

> Formalize política de geração de cópias de segurança para o [Sistema], de acordo com o previsto no item 10.5.1 da NBR ISO/IEC 17799:2005; 9.2.16. Armazene as mídias contendo cópias de segurança do [Sistema] em local diverso da operação do sistema, de acordo com a diretriz "d" do item 10.5.1 da NBR ISO/IEC 17799:2005.

Atualmente, a efetivação do Backup ocorre segundo uma política de janela de tempo para cada banco de dados que é armazenado nas unidades de fita através de um robô automatizado de backup.

Averiguamos com base nas informações concedidas pela Diretoria do Núcleo de Tecnologia da Informação que o backup dos dados da UFPE é realizado diariamente de forma parcial, não atendendo as necessidades institucionais, uma vez que a Universidade não possui capacidade nesta tecnologia para salvaguardar tudo. Entretanto, de acordo com o Diretor do NTI, a Universidade adquiriu recentemente uma nova unidade de backup, por meio do empenho nº 800031/2017, com tecnologia atualizada, com mais capacidade e velocidade para atender a demanda atual.

Quanto ao acesso ao Data Center, verificamos que o ambiente é dividido em dois. A anti-sala é acessada por meio de uma chave, retida na portaria do núcleo de tecnologia com acesso ao grupo de redes, suporte e manutenção elétrica e refrigeração. Na outra parte que corresponde ao Centro de Dados ou DataCenter, o controle de acesso de pessoas é realizado por meio da verificação biométrica da face, seguindo a determinação prevista no acórdão 1832/2006 Plenário do Tribunal de Contas de União:

> Estabeleça procedimento para controlar fisicamente o acesso de pessoas aos documentos; estabeleça procedimento para controlar fisicamente e registrar o acesso de pessoas aos documentos que contenham informações estratégicas e/ou privilegiadas, que possam beneficiar terceiros; adote procedimento especial para o registro e a tramitação de todos os documentos, que contenham, de algum modo, informações estratégicas e/ou privilegiadas.

O identificador biométrico facial foi adquirido por meio do Empenho nº 800017/2016.

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

Constatamos assim, boas práticas relacionadas à Segurança da Informação implementadas.

5. INFORMAÇÃO – OBJETIVIDADE NO PROCESSO LICITATÓRIO RESPEITANDO O CARÁTER COMPETITIVO DO CERTAME

UNIDADE AUDITADA: 153409 – PRÓ-REITORIA DE GESTÃO ADMINISTRATIVA - PROGEST

Ao analisar os processos 23076.024847/2015-96 e 23076.046320/2013-51 verificamos que o objeto da contratação foi descrito de forma sucinta, precisa, suficiente e clara, de modo a evitar descrições genéricas, que dificultam o parcelamento do objeto, ou demasiadamente específicas, que possam acarretar o direcionamento do processo licitatório (IN04 2010, arts. 11, IV e 17, I; Decreto nº 3.555/2000, art. 8º, I). Além disso, constatamos que o objeto contém apenas uma solução de TI atendendo ao que reza a IN04/2014 da SLTI/MP, em seu art. 5°, inciso I.

> Art. 5º Não poderão ser objeto de contratação:
> I - mais de uma Solução de Tecnologia da Informação em um único contrato;
> II - gestão de processos de Tecnologia da Informação, incluindo gestão de segurança da informação.

Dessa forma, podemos concluir que os processos licitatórios selecionados relacionados à contratação de Soluções de TI foram baseados em critérios objetivos, sem comprometimento do caráter competitivo do certame, e realizados conforme a IN04/2014 da SLTI/MP.

6. INFORMAÇÃO – ATENDIMENTO AOS REQUISITOS PARA AQUISIÇÃO DE SOLUÇÃO DE TI ORIENTADOS PELA IN 04/2010

UNIDADE AUDITADA: 153409 – PRÓ-REITORIA DE GESTÃO ADMINISTRATIVA - PROGEST

Ao analisar o processo nº 23076.061573/2013-54, verificamos a ausência da análise de riscos e de alguns pontos que contemplam o Estudo Técnico Preliminar da Contratação, conforme determina o art. 9º da IN 04/2010 da SLTI/MP.

> Art. 9º A fase de Planejamento da Contratação consiste nas seguintes etapas:
> I - Instituição da Equipe de Planejamento da Contratação;
> II - Estudo Técnico Preliminar da Contratação;
> III - Análise de Riscos;
> IV - Termo de Referência ou Projeto Básico.
> § 1º Os documentos resultantes das etapas elencadas nos incisos II e III deste artigo poderão ser consolidados em um único documento, a critério da Equipe de Planejamento da Contratação.
> § 2º Exceto no caso em que o órgão ou entidade seja partícipe da licitação, quando são dispensáveis as etapas III e IV do caput deste artigo, é obrigatória a execução de todas as etapas da fase de Planejamento da Contratação, independentemente do tipo de contratação, inclusive nos casos de: (Redação dada pela Instrução Normativa N° 2, de 12 de janeiro de 2015)
> I - inexigibilidade;
> II - dispensa de licitação ou licitação dispensada;
> III - criação e **adesão à Ata de Registro de Preços**; e
> IV - contratações com uso de verbas de organismos internacionais, como Banco Mundial, Banco Internacional para Reconstrução e Desenvolvimento, e outros.

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

Segue abaixo os dados do processo supramencionado:

Nº 23076.061573/2013-54
Objeto: Contratação de empresa especializada para fornecimento de solução de Impressão Departamental com solução de digitalização para integração com os sistemas coorporativos da UFPE autenticados por *smartcard,* de caráter local (TCI/IP).
Fornecedor: Tecnoset Informática Produtos e Serviços Ltda
Contrato: 01/2014
Pregão: 66/2012 – JFPE

Averiguamos que foram contemplados corretamente no processo: o termo de referência com a justificativa do projeto de contratação de serviço de impressão, a descrição sucinta, precisa, suficiente e clara da solução de TI indicando os bens e os serviços que compõem e a identificação dos benefícios a serem alcançados com a solução escolhida em termos de eficácia, eficiência, efetividade e economicidade conforme preconiza a IN 04/2010.

Entretanto, constatamos que a unidade auditada não apresentou a análise de viabilidade da contratação com a definição e especificação das necessidades de negócio e tecnológica, a avaliação das diferentes soluções disponíveis que atendam aos requisitos, o alinhamento com as necessidades do negócio e a avaliação das necessidades de adequação para viabilizar a execução contratual conforme determina o art. 12 IN 04/2010.

Constatamos também que não houve a oficialização da demanda pela Solução de TI por meio do Documento de Oficialização de Demanda (DOD), da área requisitante para o Núcleo de Tecnologia de Informação como reza o art. 11º da IN04/2010 da SLTI/MP.

> Art. 11. A fase de Planejamento da Contratação terá início com o recebimento pela Área de Tecnologia da Informação do Documento de Oficialização da Demanda - DOD, a cargo da Área Requisitante da Solução, para instituição da Equipe de Planejamento da Contratação, que conterá no mínimo:
> I - necessidade da contratação, considerando os objetivos estratégicos e as necessidades corporativas da instituição, bem como o seu alinhamento ao PDTI;
> II - explicitação da motivação e demonstrativo de resultados a serem alcançados com a contratação da Solução de Tecnologia da Informação;
> III - indicação da fonte dos recursos para a contratação;
> IV - indicação do Integrante Requisitante para composição da Equipe de Planejamento da Contratação.

CAUSA

Não observância à Instrução Normativa nº 04/2010 SLTI/MP.

MANIFESTAÇÃO DA ENTIDADE AUDITADA

*Trata-se do **Relatório de Auditoria Interna nº 006.2/2017-AUDINT** que analisou a contratação de serviço de solução de Impressão Departamental através do Contrato 01/2014 com a Empresa Tecnoset Informática Produtos e Serviços Ltda. Considerando que:*

1. *Na Constatação 1, o relatório observa que foram contemplados corretamente no*

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

processo o termo de referência com a justificativa do projeto de contratação de serviço de impressão, a descrição da solução de TI, incluindo os benefícios a serem alcançados com a contratação;

2. *A época entendíamos ter atendido os preceitos da contratação pública, e a busca da contratação mais vantajosa para a UFPE, visto que submetemos a contração a parecer jurídico e a autorização da autoridade superior;*

3. *Esta contratação coaduna com o caminho da recomendação nº 62970 da OS 20136798 – CGU, onde buscávamos racionalizar o uso de impressoras na UFPE.*

> *"Realizar estudo com o objetivo de adotar solução para minimizar o quantitativo de impressoras de uso individual na UFPE - fomentando o uso compartilhado dos recursos - e de maximizar a uniformização dos tipos de impressoras remanescentes, o que favorecerá a racionalização e à economicidade - tanto na manutenção corretiva e preventiva de equipamentos quanto nas compras dos respectivos suprimentos de impressão, a exemplo de cartuchos, toner e cilindros - além do melhor controle quanto ao uso adequado desse tipo de suprimento. No estudo avaliar a viabilidade da substituição progressiva de impressoras de uso individual por impressoras de uso coletivo e/ou serviço de reprografia, dentre outras soluções eventualmente identificadas."*

4. *Posteriormente buscando avançar na gestão das compras e contratações de TI adotamos para os processos de TI tanto a análise de viabilidade como o Documento de Oficialização de Demanda (DOD) somados aos demais itens da IN 04/2010 SLTI/MP (Anexo I)*

Comprometemo-nos a continuar observando os itens que compõe a IN 04/2010 SLTI/MP para as contrações de TI, inclusive como prevê o subitem 1.9 do RT 01 – Roteiro para análise de processos de licitação para aquisição de material SRP.

ANÁLISE DA AUDITORIA INTERNA

A AUDINT acata os esclarecimentos da Diretoria de Licitações da PROGEST, uma vez que na análise de outro processo de nº 23076.046320/2013-51, verificamos que todos os requisitos foram atendidos: a demanda pela Solução de TI foi devidamente oficializada por meio do DOD (Documento de Oficialização de Demanda), enviado da Progest (requisitante) para o Núcleo de Tecnologia de Informação e anexada ao processo juntamente com a análise de viabilidade da contratação, o plano de sustentação (recursos necessários à continuidade de negócio durante e após a contratação), estratégia da contratação e a análise de riscos, conforme determina o art. 9º da a IN04/2010 da SLTI/MP. Foram apresentadas as necessidades de negócio que se pretende atender com a contratação, a justificativa da solução escolhida, a identificação das soluções e alternativas disponíveis, o alinhamento com as necessidades do negócio, os benefícios esperados com a contratação e avaliação das necessidades de adequação para execução contratual. Obervamos que nesse processo foi realizada também uma pesquisa dos preços praticados no mercado pelo ramo do objeto da licitação conforme preconiza art. 3º III, da Lei nº 10.520/02, art. 9, § 2 do decreto nº 5.450/05 e art. 15, III e 43 IV da Lei nº 8.666/93, para contratação da solução de TI mais viável economicamente.

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

Dados do Processo

Nº 23076.046320/2013-51
Fornecedor: SIG Software & Consultoria em Tecnologia da Informação Ltda
Objeto: Contratação de empresa especializada em serviços de instalação, manutenção, capacitação, apoio a sustentação e suporte dos sistemas integrados de Gestão SIG (SIPAC/SIGAdmin) na UFPE
Contrato: 11/2014
Pregão: 258/2013 – UFPE
Previsto no Eixo (8) – Informação e Comunicação - Ação (8) NTI01 – Ampliação da Oferta de Funcionalidades e Manutenção do Sistema Integrado de Informações e Gestão Institucional do Plano de Ação PAI2014 da UFPE.

Com base nas evidências, concluímos, portanto, que no Processo: 23076.046320/2013-51, a contratação de Solução de TI analisada foi fundamentada nas necessidades reais da Instituição e esteve em conformidade com as orientações a IN04/2010 da SLTI/MP.

Dessa forma, consideramos esta constatação atendida e enfatizamos a necessidade do cumprimento dos requisitos dispostos na Instrução Normativa nº 04/2010 da SLTI/MP tem todos os processos de aquisições de bens e contratação de serviços de Tecnologia da Informação.

5.2 CONSTATAÇÕES

Das análises documentais resultaram as constatações listadas neste Relatório, como segue:

1. CONSTATAÇÃO – INTEMPESTIVIDADE NA ELABORAÇÃO DO PLANO DIRETOR DE TECNOLOGIA DA INFORMAÇÃO REFERENTE AO BIÊNIO 2017-2018
UNIDADE AUDITADA: 154728 – PRÓ-REITORIA DE COMUNICAÇÃO, INFORMAÇÃO E TECNOLOGIA DA INFORMAÇÃO

Observamos que a UFPE possui um Plano Diretor de Tecnologia da Informação, publicado no site da UFPE, relativo aos exercícios 2015 e 2016.

A Instrução Normativa n° 04/2014 define Plano Diretor de Tecnologia da Informação como um instrumento de diagnóstico, planejamento e gestão dos recursos e processos de Tecnologia da Informação que tem como finalidade atender às necessidades tecnológicas e de informação de um órgão ou entidade para um determinado período.

De acordo com o Sistema de Administração de Recursos de Tecnologia da Informação do Poder Executivo Federal (SISP), o período de vigência mínimo sugerido é de 2 (dois) anos, e um novo ciclo de elaboração e acompanhamento do PDTI deve acontecer a cada ano, de modo a atualizar diretrizes, planos e, principalmente, consolidar a proposta orçamentária de TI para o exercício seguinte.

Desse modo, através da Solicitação de Auditoria nº 11/2017 de 01/07/2017 foi requerida a disponibilização do PDTI 2017-2018. Em resposta a Pró-Reitoria da PROCIT expediu o Memo 117/2017:

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

"O documento em questão encontra-se em fase de elaboração, sob a coordenação da Diretoria de Tecnologias e Processos em articulação com o Núcleo de Tecnologia da Informação (NTI). Até o momento, foram realizados o levantamento dos resultados do PDTI anterior, a definição do referencial estratégico (com exceção dos objetivos estratégicos que estão sendo finalizados) e o levantamento de necessidades já priorizadas pela alta administração. Faltam ser executadas fases essenciais para a finalização do planejamento, entre elas as fases de levantamento de necessidades com a comunidade acadêmica, priorização final das necessidades levantadas e seu alinhamento estratégico, definição do plano de metas e ações e do plano de gerenciamento de riscos e aprovação final do documento."

"Todas as fases definidas para a elaboração do PDTIC 2017-2018 da UFPE foram adaptadas do Guia Siso para Elaboração de PDTIC."

Com base nesse pronunciamento, constatamos que a versão 2017-2018 do PDTI está em processo de elaboração. Considerando que o objetivo do planejamento consiste em apoiar a execução das atividades de TI, salientamos que a fase de planejamento deverá ser realizada com antecedência à fase de execução, caso contrário o mesmo perderá a sua finalidade.

CAUSA

Equipe reduzida de servidores no apoio à alta administração.

MANIFESTAÇÃO DA ENTIDADE AUDITADA

O PDTI é um projeto robusto, composto por 3 macroprocessos (Preparação, Diagnóstico e Planejamento). O processo metodológico de elaboração envolve workshop com a alta administração, análise de documentos, realização de pesquisa com a comunidade acadêmica e com os gestores, workshops com a equipe técnica de TIC para elaboração de planos de ação, dentre outros. É um projeto que envolve dedicação de tempo e um conjunto de competências gerenciais (liderança, articulação, negociação, etc) e técnicas (referencial estratégico, planos de ação, dimensionamento de pessoal, gestão de TIC, segurança de TIC, etc) importantes para a sua consecução.

A Coordenação de Governança de TI da UFPE está ainda em processo de consolidação e enfrenta alguns desafios. Dentre eles, destacamos a equipe reduzida e com perfil operacional que impactou diretamente no diagnóstico encontrado por esta auditoria. Com apenas 1 servidor, a coordenação tem se dedicado desde 2016 a projetos de gestão interna da PROCIT (imprescindíveis para a Pró-Reitoria) e a projetos específicos de Governança de TIC. Dessa forma, além de se dedicar ao PDTI, participa dos projetos: Regimento Interno da Procit; Central de Serviços da PROCIT; Monitoramento dos Projetos da PROCIT; Elaboração do Plano de Governança de TIC; Atendimento aos relatórios de órgãos de controle interno e externo à UFPE no tocante a questões de TIC; Portal de Governança; Implantação e apoio ao sistema de monitoramento do PAI UFPE (Sistema Redmine).

Apesar desses desafios, a Diretoria de Processos e Governança de TIC está empenhada em finalizar o plano, tendo realizado três (3) workshops, e se prepara para a fase de escuta à comunidade acadêmica no tocante à satisfação com os serviços de TIC e às necessidades de TIC

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

específicas a cada unidade administrativa.

No tocante aos encaminhamentos, a Diretoria de Processos e Governança de TIC:

a) Está em processo de ampliação de sua equipe, com a chegada de mais uma servidora, e continua pleiteando novos servidores junto à alta administração.
b) Acordou, junto ao Pró-Reitor da PROCIT e a Diretora do NTI, no último workshop de elaboração do PDTIC, em propor ao Comitê de Informação, Comunicação e Tecnologia da Informação que o plano em elaboração tenha validade para o triênio de 2017-2019, frente às dificuldades enfrentadas para a sua elaboração. Segundo a IN04/2014, as contratações de 2017 alinhadas aos planejamentos estratégicos e táticos (PEI, PDI e PAI) em vigor na UFPE podem ser adquiridas sem restrições.
c) Tem dado continuidade ao cronograma de elaboração do plano para sua finalização.

ANÁLISE E RECOMENDAÇÃO DA AUDITORIA INTERNA

Com base na manifestação da Pró-reitoria de Comunicação, Informação e Tecnologia da Informação – PROCIT recomendamos a efetivação do Plano Diretor de Tecnologia da Informação da UFPE com validade para o triênio de 2017-2019 conforme proposto, com a realização do acompanhamento anual de modo a atualizar diretrizes, planos e consolidação da proposta orçamentária para o exercício seguinte. Recomendamos também a ampliação da equipe de apoio à alta administração de modo a viabilizar a realização dos objetivos do planejamento tempestivamente.
Este item será objeto de análise quando no acompanhamento das implementações recomendadas, no Plano de Providências Permanente.

2. CONSTATAÇÃO – ATENDIMENTO PARCIAL DO PDTI 2015-2016 DA UFPE AOS REQUISITOS DEFINIDOS PELO SISP NO MODELO DE REFERÊNCIA DO GUIA DE ELABORAÇÃO DO PDTI

UNIDADE AUDITADA: 154728 – PRÓ-REITORIA DE COMUNICAÇÃO, INFORMAÇÃO E TECNOLOGIA DA INFORMAÇÃO

Ao analisar a adequação do Plano Diretor de Tecnologia da Informação (PDTI) relativo ao Biênio 2015-2016 ao modelo de referência do Guia de Elaboração do PDTI do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, constatamos por meio desta auditoria que ele contempla: a descrição da metodologia utilizada para elaboração do plano, as atividades desenvolvidas, o levantamento da situação atual, análise e categorização do SWOT da TI, a elencagem das necessidades, o cronograma de execução dos projetos, os fatores críticos para implantação do PDTI, a descrição dos projetos incluídos nos planos e suas prioridades frente aos objetivos e às metas da instituição bem como a relação dos principais resultados esperados.

Entretanto, verificamos que o PDTI relativo ao Biênio 2015-2016 não apresentou o Plano de Investimentos e Custeio, o Plano de Gestão de Pessoas, a Proposta Orçamentária da TIC bem como o Plano de Gestão de Riscos.

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

Em resposta a Solicitação de Auditoria nº 11/2017 relativa ao Plano de Gestão de Riscos o Pró-reitor da PROCIT informou por meio do Memorando nº 117/2017 que *"o processo de gerenciamento de riscos do PDTI está previsto como parte das etapas de elaboração do PDTI 2017-2018".*

Frisamos que o gerenciamento de riscos envolve o levantamento de informações sobre como os riscos serão identificados, como a análise qualitativa será desenvolvida, como a análise quantitativa será criada, como será realizado o planejamento de resposta aos riscos e como serão monitorados (GOMES, 2008).

Destacamos que esses itens são definidos no Guia de Elaboração do PDTI do Sistema de Administração de Recursos de Tecnologia da Informação (SISP), do Poder Executivo Federal.

O SISP é responsável pelo planejamento, controle e supervisão dos recursos de tecnologia da informação dos órgãos e entidade da administração publica federal direta, autárquica e fundacional, em articulação com os demais sistemas utilizados direta ou indiretamente na gestão da informação pública federal. Nesse contexto, o Ministério do Planejamento atua por meio da Secretaria de Logística e Tecnologia da Informação – SLTI, na normatização, gestão e coordenação das ações do SISP, como órgão central deste sistema. De acordo com a Instrução Normativa n° 2, de 12 de janeiro de 2015 da SLTI/MP,

> Art. 1º As contratações de Soluções de Tecnologia da Informação pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) serão disciplinadas por esta Instrução Normativa (IN).
>
> Art. 3º Em consonância com o art. 4º do Decreto nº 7.579, de 2011, o órgão central do SISP elaborará, em conjunto com os órgãos setoriais e seccionais do SISP, a Estratégia Geral de Tecnologia da Informação e Comunicação - EGTIC para a Administração direta, autárquica e fundacional do Poder Executivo Federal, revisada e publicada anualmente, para servir de subsídio à elaboração dos PDTI pelos órgãos e entidades integrantes do SISP.

Diante do exposto, questionamos quanto à completude das informações necessárias para o PDTI 2017-2018 conforme orientação do SISP.

CAUSA

Situação existente na época da elaboração do planejamento, por se tratar do primeiro planejamento estratégico de TI da Universidade: dedicação parcial da equipe de elaboração, dificuldade para incluir as necessidades das áreas de TI não gerenciáveis pelo NTI, pouco envolvimento da Alta Administração na elaboração do Plano, visão da TI da UFPE indefinida, princípios e diretrizes da UFPE para TI desconhecidos, setor de governança da UFPE em processo de consolidação e falta de maturidade adequada para consolidação dos Planos de Gestão de Pessoas e de Gerenciamento de Riscos.

MANIFESTAÇÃO DA ENTIDADE AUDITADA

É importante entender o atendimento parcial do PDTI 2015-2016 da UFPE às orientações do Guia SISP no escopo do próprio nível de maturidade da própria Universidade no tocante à

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

elaboração de planejamentos estratégicos e táticos.

O primeiro PDTIC surgiu da necessidade crescente de um Planejamento Estratégico de TI - inclusive por questões legais (IN04/2011) - e no contexto em que esforços nesse sentido já estavam sendo realizados pelo Núcleo de Tecnologia da Informação (NTI). Dessa forma, o PDTI 2015-2016 surge a partir de uma revisão, ampliação e adaptação do planejamento estratégico e tático do Núcleo de Tecnologia da Informação (NTI), que teve esta iniciativa autônoma em 2013/2014 em busca da profissionalização da sua gestão.

A necessidade de adaptação da metodologia de elaboração do PDTI e a não inclusão de todos os planos solicitados pelo Guia Sisp deu-se durante o processo de revisão e ampliação do documento, sendo consequência da adaptação da UFPE à esta exigência e a consolidação do setor de governança na UFPE, que hoje está devidamente consolidada na Diretoria de Governança de TIC e Processos da Procit.

A equipe de elaboração do PDTI 2015-2016 relatou, em relatório final encaminhado à Diretoria do NTI, algumas das dificuldades enfrentadas naquele período, que podem auxiliar na compreensão do contexto vivido: a) ausência de planejamento estratégico institucional (PEI e PDI) quando os trabalhos foram iniciados; b) equipe de elaboração com dedicação parcial; c) dificuldade para incluir as necessidades das áreas de TI não gerenciáveis pelo NTI, como Centro de Informática, Departamento de Física; d) pouco envolvimento da Alta Administração na elaboração do Plano; e) a visão da TI da UFPE não estava clara para todos; f) princípios e diretrizes da UFPE para a TI não são conhecidos; entre outros.

O Guia SISP apresenta-se como uma referência e, constatado que os níveis de maturidade das instituições são diferenciados, permite que adaptações sejam realizadas no processo de elaboração do PDTIC. Portanto, frente ao nível de maturidade para a consolidação dos planos de Gestão de Pessoas e de Gerenciamento de Riscos decidiu-se por sua não elaboração, apenas a elaboração do Plano de Ações e Metas. No caso do plano orçamentário de TIC, o do NTI era o único disponível e não representava a UFPE em sua completude e, por isso, decidiu-se pela sua não inclusão.

No tocante aos encaminhamentos, quanto ao PDTIC 2017-2019, a Diretoria de Processos e Governança de TIC:

a) *Prevê a inclusão dos seguintes planos: Plano de Gerenciamento de Riscos, Plano de Gestão de Pessoas e Plano Orçamentário de TIC.*

   i) Os esforços de inclusão do Plano de Gerenciamento de Riscos ocorrem junto ao próprio processo de amadurecimento da Governança Institucional nesta área, que possibilitou capacitação neste sentido.
   ii) O Plano de Gestão de Pessoas deverá ser composto por estudo de necessidade de pessoal para o NTI e Natis das unidades bem como de plano de capacitação.
   iii) O Plano Orçamentário de TIC será elaborado conjuntamente ao NTI para cada Objetivo Estratégico, com base na lista de necessidades de TIC.

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

ANÁLISE E RECOMENDAÇÃO DA AUDITORIA INTERNA

Recomendamos a inclusão do Plano de Gerenciamento de Riscos, do Plano de Gestão de Pessoas e do Plano Orçamentário de TIC no PDTI 2017-2019. Esta constatação será objeto de análise no acompanhamento das implementações recomendadas.

3. CONSTATAÇÃO – ATENDIMENTO PARCIAL ÀS METAS PROPOSTAS NO PDTI 2015-2016 E FALTA DE ALINHAMENTO ENTRE AS SOLUÇÕES ADQUIRIDAS/DESENVOLVIDAS E AS AÇÕES PREVISTAS NO PDTI

UNIDADE AUDITADA: 154728 – PRÓ-REITORIA DE COMUNICAÇÃO, INFORMAÇÃO E TECNOLOGIA DA INFORMAÇÃO

Ao analisar o relatório de resultados PDTI 2015-2016, verificamos que a maioria das ações propostas para o referido biênio não foram totalmente finalizadas. Da totalidade de 151 (cento e cinquenta e uma) metas propostas apenas 9 (nove) foram concluídas, 45 (quarenta e cinco) estão em andamento, enquanto 97 (noventa e sete) ações para atendimento sequer foram iniciadas sendo, portanto replanejadas para o próximo biênio.

A partir da análise da lista de ações de TI executadas em 2016 e 2017 averiguamos também que a solução adquirida/desenvolvida está relacionada apenas com objetivo ao qual atende, não havendo alinhamento com a ação prevista no PDTI 2015-2016 que está sendo realizada.

CAUSA

Generalidade das ações e ausência de revisão e monitoramento do documento.

MANIFESTAÇÃO DA ENTIDADE AUDITADA

Destacamos dois aspectos que tiveram impacto nesta constatação e que se complementam: 1. A granularidade alta das ações; 2. A ausência de revisão e monitoramento do documento. As ações definidas para a primeira versão do PDTI da UFPE foram elaboradas em nível de granularidade alto, característica comum de PDTI´s de instituições que ainda não aprimoraram sua capacidade de planejamento institucional. Para exemplificar, tomemos as ações de sistemas: tendo em vista a dificuldade de definição, por parte da Alta Administração, dos sistemas que seriam implantados, decidiu-se por definição de ações com alto nível de granularidade para que esta fosse detalhada à medida que os sistemas fossem definidos pela alta administração. Esse desafio foi superado pela equipe de elaboração do PDTI 2017-2019, que conta com maior clareza e alinhamento com a alta administração no tocante a projetos cruciais, em especial aqueles relativos à área de sistemas, o que diminuirá essa disparidade no momento de elaboração dos planos de ação. Esta clareza é fruto dos esforços de consolidação da PROCIT, que gerou maior alinhamento entre as áreas de negócio e a TIC. Outro aspecto importante diz respeito ao processo de revisão e monitoramento, etapas importantes previstas para ajustes do documento que não foram executadas.

No tocante aos encaminhamentos, a Diretoria de Processos e Governança de TIC:

a) Tem fortalecido a equipe de Governança de TIC da UFPE e tem clareza do papel da PROCIT na avaliação e monitoramento dos planos de ação.

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

b) Já apresenta maior alinhamento com a alta administração sobre alguns focos estratégicos de TIC, o que impacta positivamente em uma definição mais objetiva das metas a serem alcançadas;

c) Prevê processo de revisão e monitoramento das ações do plano do PDTIC.

ANÁLISE E RECOMENDAÇÃO DA AUDITORIA INTERNA

Com base na manifestação da Pró-reitoria de Comunicação, Informação e Tecnologia da Informação – PROCIT verificamos que a gestão tem tomado providências no sentido de melhorar o alinhamento com a alta administração sobre focos estratégicos de TIC para uma definição mais objetiva das metas a serem alcançadas e se comprometeu a realizar o processo de revisão e monitoramento das ações do plano do PDTIC.

Esta constatação será objeto de análise no acompanhamento das implementações recomendadas.

4. CONSTATAÇÃO – REPRESENTANTE DA AUDITORIA INTERNA, MEMBRO DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO.

UNIDADE AUDITADA: 154728 – PRÓ-REITORIA DE COMUNICAÇÃO, INFORMAÇÃO E TECNOLOGIA DA INFORMAÇÃO

Ao analisar a Portaria Normativa nº 09 de 19 de setembro de 2014 constatamos a inclusão de Representante da Auditoria Interna como membro do Comitê de Segurança da Informação, contrariando o disposto no art. 12º, parágrafo único, do Regimento Interno da Auditoria Interna da UFPE, que assim determina:

> Não se deve atribuir à Unidade de Auditoria Interna e aos Auditores Internos atividades de gestão, sobretudo despachos em processos administrativos, participação em comissões, entre outras que possam causar conflito com a atividade típica de auditoria.

A Auditoria Interna tem o papel de assessorar, orientar, acompanhar e avaliar os atos de gestão, no intuito de garantir a regularidade, sendo vedada a participação do Auditor e servidores lotados na Auditoria Interna em quaisquer grupos de trabalho que envolva assuntos de gestão, exceto as pertinentes as atividades de auditoria, para que não comprometa a sua independência.

CAUSA

Entendimento equivocado do gestor em relação as atribuições da Auditoria Interna.

MANIFESTAÇÃO DA ENTIDADE AUDITADA

O CSIC é um órgão consultivo e propositivo da Universidade Federal de Pernambuco, que tem a finalidade de propor, assessorar, desenvolver e implementar políticas e ações de Segurança da Informação e Comunicações, portanto, não se trata de uma comissão ou grupo de trabalho.

A formação do CSIC é abrangente e representada por membros das diversas unidades

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

institucionais. Assim, como a auditoria é uma unidade da UFPE que também é impactada pela Segurança da Informação e Comunicações foi incluída em sua formação.

ANÁLISE E RECOMENDAÇÃO DA AUDITORIA INTERNA

Na atuação da auditoria interna, os auditores não podem assumir responsabilidades extra-auditoria para que não haja enfraquecimento da objetividade, na medida em que seria auditada atividade sobre a qual aqueles profissionais teriam autoridade e responsabilidade (Manual de Auditoria do TSE, 2008). Além disso, cabe ressaltar que de acordo com o item 1.2, TC-010.240/2005-1, Acórdão nº 1.214/2006 – TCU -1ª Câmara, as funções de auditoria interna deverão ser segregadas das demais atividades da Entidade.

Diante do exposto, recomendamos ao Comitê de Segurança da Informação que realize uma segunda alteração da portaria normativa nº 09 de 19 de setembro de 2014, já alterada pela Portaria Normativa nº 07 de 19 de maio de 2015 para que seja efetivada a exclusão do inciso XVI do art. 2º.

Esta constatação será objeto de análise no acompanhamento das implementações recomendadas.

5. CONSTATAÇÃO – AUSÊNCIA DE UMA POLÍTICA DE REVOGAÇÃO DE ACESSO
UNIDADE AUDITADA: 154728 – PRÓ-REITORIA DE COMUNICAÇÃO, INFORMAÇÃO E TECNOLOGIA DA INFORMAÇÃO

Verificamos que a UFPE executa o procedimento de rotina de inclusão de perfis inspirados e alteração de restrição de acesso de acordo com a mudança de Cargo de Direção e Função Gratificada. Entretanto, não identificamos uma Política de revogação de acesso ao Sistema SIG com a definição de procedimentos de rotina para manutenção e exclusão de direitos de acesso ao sistema SIG, de modo a garantir que servidores que não integram mais o quadro funcional da UFPE não permaneçam com cadastros ativos no sistema mantendo privilégios e direitos nos módulos, conforme NBR ISO/IEC 17799:2005, item 8.3.3: "Convém que os direitos de acesso de todos os funcionários, fornecedores e terceiros às informações e aos recursos de processamento da informação sejam retirados após o encerramento de suas atividades, contratos ou acordos, ou ajustado após a mudança destas atividades".

Corroborando com esse posicionamento, o TCU, por meio do Acórdão 782/2004 1ª Câmara, determina que: Adote procedimentos formais de concessão e de validação periódica de senhas de usuários de sistemas informatizados, bem como de cancelamento de acesso de usuários que são desligados da unidade.

CAUSA

Falta de critérios formais que normatizem a retirada de direitos de acesso dos usuários desvinculados da Instituição.

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

MANIFESTAÇÃO DA ENTIDADE AUDITADA

A Diretoria de Processos e Governança de TIC, o Núcleo de Tecnologia da Informação e a Coordenação de Segurança da Informação deram encaminhamento à elaboração da norma de revogação de acesso. Assim que finalizada, a norma deverá ser aprovada pelo Comitê de Segurança da Informação e Comunicações e encaminhada para publicação.
Encaminhamento: Norma em fase de elaboração (em anexo).

ANÁLISE E RECOMENDAÇÃO DA AUDITORIA INTERNA

Diante do exposto e com base nos esclarecimentos apresentados pela PROCIT, verificamos que a gestão está engajada na elaboração de uma Norma de Revogação de Acesso. Neste sentido, recomendamos ao Comitê de Segurança da Informação que finalize e implante a Norma de Revogação de Direitos de Acesso para toda a Instituição, organizada nos termos das orientações contidas NBR ISO/IEC 17799:2005, item 8.3.3 Retirada de direitos de acesso.

Aplicar e manter sempre atualizado os procedimentos de revogação de acessos aos sistemas institucionais dos servidores que não mais integrem a UFPE, especialmente através de um fluxo e uma rotina que envolva a comunicação tempestiva da Diretoria de Gestão de Pessoas à PROCIT/NTI das alterações das situações funcionais dos servidores, para que estas possam executar as alterações e especialmente as revogações de maneira célere. Esta constatação será objeto de análise quando no acompanhamento das implementações recomendadas.

6. CONSTATAÇÃO – AUSÊNCIA DO PLANO DE TRATAMENTO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES – GRSIC

UNIDADE AUDITADA: 154728 – PRÓ-REITORIA DE COMUNICAÇÃO, INFORMAÇÃO E TECNOLOGIA DA INFORMAÇÃO

Constatou-se que a UFPE não dispõe de Plano de Tratamento de Riscos. De acordo com a Norma Complementar nº 04/N01/DSIC/GSI/PR, o processo Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC tem a finalidade de manter os riscos em níveis aceitáveis, sendo composto pelas etapas de definições preliminares, análise/avaliação dos riscos, plano de tratamento dos riscos, aceitação dos riscos, implementação do plano de tratamento dos riscos, monitoração e análise crítica, melhoria do processo de Gestão de Riscos de Segurança da Informação e Comunicações e comunicação do risco.

CAUSA

- Não observância a Norma Complementar nº 04/N01/DSIC/GSI/PR.
- Necessidade da aprovação da Política de Segurança da Informação e Comunicações (PoSIC), para embasar e apoiar tais ações.
- Insuficiência de servidores especializados na área de segurança da informação e comunicações.

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

MANIFESTAÇÃO DA ENTIDADE AUDITADA

Na tentativa de unir esforços para minimizar as dificuldades de implementar a Segurança da Informação na UFPE, recentemente foram realizadas visitas técnicas à UFC, UFRN e UFPB. A intenção é conhecer as forças e fraquezas das referidas instituições e como podemos trabalhar colaborativamente no sentido de evoluir o processo de forma mais rápida e eficaz.

A UFC estuda há dois a gestão de riscos e possui equipe exclusiva para tratar a segurança da informação e comunicações. A equipe é formada por cinco servidores entre analistas e técnicos em segurança da informação devidamente capacitados e especializados. Desta forma, percebe-se o grau de complexidade da elaboração e implementação do referido plano.

No que tange a UFPE, antes de qualquer ação relacionada à segurança faz-se necessário a aprovação da Política de Segurança da Informação e Comunicações (PoSIC), visto que é preciso um instrumento que embase e apoie tais ações.

Outro ponto a ressaltar, refere-se a dificuldade que a UFPE enfrentada no momento, no que tange a contratação de servidores especializados para a área de segurança da informação e comunicações. Importa salientar que a UFPE reconhece esta necessidade, afinal, a equipe de segurança conta apenas com dois servidores. Desta forma, torna-se evidente a dificuldade para desenvolver tantas tarefas complexas e simultâneas face a carência de pessoal e relevância de tal plano.

No tocante aos encaminhamentos, a Coordenação de Segurança da Informação:

a) *O Plano de Tratamento de Riscos em Segurança da Informação e Comunicações será elaborado pela ETSI com o apoio da Procit.*
b) *Será realizada reunião com a Controladoria da UFPE - Ana Luiza - que está desenvolvendo o plano de gestão de riscos da UFPE.*
c) *Será solicitada capacitação da RNP quanto a gestão de riscos para os servidores da Procit - Coordenação de Segurança da Informação.*

ANÁLISE E RECOMENDAÇÃO DA AUDITORIA INTERNA

Diante do exposto e com base nos esclarecimentos apresentados pela PROCIT, recomendamos ao Comitê de Segurança da Informação que defina e implante um Plano de Tratamento de Riscos em Segurança da Informação e Comunicações para toda a Instituição com base na Norma Complementar nº 04/N01/DSIC/GSI/PR e promova a capacitação de servidores da PROCIT em gestão de riscos para atuar na elaboração desse planejamento. Esta constatação será objeto de acompanhamento por esta Audint.

7. CONSTATAÇÃO – AUSÊNCIA DO PROGRAMA DE GESTÃO DE CONTINUIDADE DO NEGÓCIO

UNIDADE AUDITADA: 154728 – PRÓ-REITORIA DE COMUNICAÇÃO, INFORMAÇÃO E TECNOLOGIA DA INFORMAÇÃO

Constatou-se que a UFPE não dispõe de um Programa de Gestão de Continuidade do Negócio. De acordo com a Norma Complementar nº 06/IN01/DSIC/GSI/PR, a implantação do processo de Gestão de Continuidade de Negócios busca minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão ou entidade, além

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação, conforme determina o acórdão do TCU nº 1137/2012 Plenário:

> Em atenção à Norma Complementar - IN01/DSIC/GSI/PR 6/2009, implante um Programa de Gestão da Continuidade de Negócios adequado às necessidades do ministério, (...) observando ainda as diretrizes presentes no item 14 da Norma Técnica ABNT NBR ISO/IEC 27002:2005.

CAUSA

- Não observância a Norma Complementar nº 06/IN01/DSIC/GSI/PR.
- Necessidade da aprovação da Política de Segurança da Informação e Comunicações (PoSIC), para embasar e apoiar tais ações.
- Insuficiência de servidores especializados na área de segurança da informação e comunicações.

MANIFESTAÇÃO DA ENTIDADE AUDITADA

Idem a Constatação 8

No tocante aos encaminhamentos, a Coordenação de Segurança da Informação:

a) Será solicitada capacitação da RNP quanto à gestão de segurança da informação para os servidores da Procit - Coordenação de Segurança da Informação.

ANÁLISE E RECOMENDAÇÃO DA AUDITORIA INTERNA

Diante do exposto e com base nos esclarecimentos apresentados pela PROCIT, recomendamos ao Comitê de Segurança da Informação que formalize um Plano de Continuidade do Negócio (PCN) de modo a garantir, em caso de falhas ou desastre natural significativo, a retomada tempestiva do funcionamento do órgão, protegendo os processos críticos, de acordo com o previsto no item 14 da NBR ISO/IEC 17799:2005, e segundo orientações contidas no Cobit 4.1, item DS4.2-Planos de Continuidade de TI. Além disso, recomendamos a capacitação de servidores da PROCIT em Gestão de Segurança da Informação com vistas a fortalecer a equipe de apoio para elaboração desse planejamento.

Salientamos que esta constatação será objeto de acompanhamento por esta Audint.

8. CONSTATAÇÃO – AUSÊNCIA DO PLANO DE TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

UNIDADE AUDITADA: 154728 – PRÓ-REITORIA DE COMUNICAÇÃO, INFORMAÇÃO E TECNOLOGIA DA INFORMAÇÃO

Constatou-se que a UFPE não dispõe de um Plano de Treinamento em Segurança da Informação. De acordo com a Norma Complementar nº 02/N01/DSIC/GSI/PR, o Gestor de Segurança da Informação e Comunicações deverá implementar programas de conscientização e treinamento, sendo necessário: assegurar que todo pessoal que tem responsabilidades atribuídas no plano de metas receba o treinamento adequado para desempenhar suas tarefas; manter registros sobre habilidades, experiências e qualificações do efetivo do órgão ou

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

entidade relativos à segurança da informação e comunicações; assegurar que todo efetivo do órgão ou entidade esteja consciente da relevância e importância da segurança da informação e comunicações em suas atividades e como cada pessoa pode contribuir para o alcance dos objetivos das ações de segurança da informação e comunicações.

CAUSA

- Não observância a Norma Complementar nº 02/N01/DSIC/GSI/PR.
- Necessidade da aprovação da Política de Segurança da Informação e Comunicações (PoSIC), para embasar e apoiar tais ações.
- Insuficiência de servidores especializados para a área de segurança da informação e comunicações.

MANIFESTAÇÃO DA ENTIDADE AUDITADA

Idem a Constatação 8

No tocante aos encaminhamentos, a Coordenação de Segurança da Informação:

a) Com o apoio da Equipe de Tratamento de Incidentes de Segurança da Informação - ETISI,será elaborado Plano de Treinamento em Segurança da Informação considerando as necessidades de capacitação dos referidos membros da ETISI.

No que diz respeito a capacitação da comunidade acadêmica, o plano de treinamento está em fase de elaboração e sua execução será negociada com a Reitoria em busca de soluções às restrições orçamentárias da UFPE.

ANÁLISE E RECOMENDAÇÃO DA AUDITORIA INTERNA

Diante do exposto e com base nos esclarecimentos apresentados pela PROCIT, recomendamos ao Comitê de Segurança da Informação que elabore e implante um Plano de Treinamento em Segurança da Informação com base na Norma Complementar nº 02/N01/DSIC/GSI/PR. Esta constatação será objeto de acompanhamento por esta Audint.

9. CONSTATAÇÃO – UTILIZAÇÃO PARCIAL DE PROTEÇÃO ANTIVÍRUS E QUANTIDADE INSUFICIENTE DE CONTROLADORES DE DOMÍNIO, NO ÂMBITO DA UFPE.

UNIDADE AUDITADA: 153101 – NUCLEO DE TECNOLOGIA DA INFORMAÇÃO

Com o suporte técnico de especialistas da área de TI, examinamos os computadores dos setores selecionados para análise, no intuito de averiguar se os mesmos possuem mecanismos de proteção contra problemas de segurança lógica.

Tendo em vista que as principais ameaças relacionadas à segurança lógica estão ligadas as falhas na rede provocadas por software estranho, fraudes e sabotagens e acessos indevidos, o emprego de recursos tecnológicos nos processos, como por exemplo, utilização de firewalls, antivírus, anti-spam entre outros, torna-se imprescindível.

Constatamos que diante dos custos inerentes à contratação de proteção antivírus e da restrição orçamentária, a maior parte das Unidades Gestoras da Universidade vem utilizando

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

softwares-livres: Avast, Microsoft Security Essentials, Avira. Esses programas antivírus são atualizados frequentemente e estão configurados para monitorar os meios mais comuns de contágio de vírus. Entretanto, constatamos que alguns dos computadores servidores e estações de trabalho não possuem programas antivírus instalados. Quanto à utilização de software livre nos órgãos públicos o TCU fez as seguintes considerações:

> **Acórdão 1598/2006 Plenário**
> Abstenha-se de proceder à aquisição de bens e contratação de serviços de informática sem a prévia análise de sua necessidade, realizando, para esse fim, estudos detalhados, levantamento e planejamento adequados para cada setor, mediante Plano Diretor de Tecnologia de Informação que considere as seguintes diretrizes:
> • proposição de soluções corporativas que contemplem a padronização de equipamentos de suporte e de sistemas, com vistas à minimização de custos de manutenção e ao melhor aproveitamento recursos disponíveis no mercado;
> • minimização da relação custo/benefício no fornecimento de produtos, na utilização de programas e na prestação de serviços;
> • adoção de alternativas para a redução sensível de despesas com o pagamento de licenças de uso de programas de computador, a exemplo da implementação projetos pilotos tendentes à migração para o software livre, baseados no Linux, como vem sendo adotado pelo Governo Federal;
> • redução significativa de custos de licenciamento de programas e de ajustes de serviços a ele vinculados mediante a contratação de empresa para o desenvolvimento de sistemas corporativos, com a obrigatoriedade de disponibilizar os respectivos códigos-fonte à contratante. Com isso, dispensa-se a necessidade de pagar patentes e contratar diretamente as mesmas empresas, fornecedoras exclusivas de sistemas, para atualização, Licitações e Contratos - Orientações e Jurisprudência do TCU manutenção, treinamento e consultoria. Para tanto, é necessário que a empresa estatal disponha, em seu quadro efetivo, de pessoal técnico qualificado que reúna o conhecimento necessário ao desenvolvimento desses programas.
> **Acórdão 1521/2003 Plenário**
> Não obstante a indicação de marca, desde que circunstanciadamente motivada, possa ser aceita em observância ao princípio da padronização, este como aquela não devem ser obstáculo aos estudos e à efetiva implantação e utilização de software livre no âmbito da Administração Pública Federal, vez que essa alternativa poderá trazer vantagens significativas em termos de economia de recursos, segurança e flexibilidade.

Verificamos também que a PROACAD, a PROPESQ e a Diretoria do CCS possuem controladores de domínio. Dessa forma, os usuários vinculados a essas Unidades Gestoras não possuem permissão para instalar programas, qualquer procedimento relacionado à Tecnologia da Informação é executado pelo profissional de TI responsável.

Entretanto nas demais pró-reitorias: PROAES, PROEXC, PROGEPE, PROPLAN não há esse tipo de controle. O NATI-Reitoria realiza a instalação de softwares livres nos computadores de todos os setores, mas como toda a demanda da Reitoria é centralizada nele e a equipe de especialistas é reduzida, cada usuário tem autonomia para instalar e desinstalar programas bem como realizar as rotinas de verificação do antivírus e somente quando há problemas, os NATIS são acionados. Nos centros acadêmicos a realidade é a mesma. Isto se torna perigoso

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

uma vez que na Universidade não há treinamento ou projeto de conscientização de usuários para saberem como combater ou lidar em caso de ocorrência de vírus. Constatamos inclusive que alguns computadores analisados estavam sem o programa antivírus porque o próprio usuário havia procedido à desinstalação. Particularmente, o acórdão 562/2006 – TCU Plenário determina que:

> Elabore e distribua a todas as centrais manual de procedimentos, instruindo sobre operação e controle dos sistemas monousuários, que contemple pelo menos procedimentos detalhados para realização, guarda e restauração de cópias de segurança; orientação quanto ao uso de senhas por parte dos operadores do sistema; orientação quanto à segurança física dos equipamentos que efetuam o processamento do sistema; **orientação quanto à utilização de software de proteção contra programas maliciosos (vírus**); e elaboração de "plano de contingência" para o sistema, de forma a evitar que, em eventuais falhas no seu funcionamento ou nos equipamentos, as listas de prováveis receptores deixem de ser emitidas.

Constatamos a necessidade de um especialista responsável pelo controle de domínio para cada Pró-Reitoria e grupo de departamentos em cada centro, além de um maior incentivo para implantação e utilização dos softwares livres em toda a universidade.

CAUSA

Falta de critérios formais na política de TIC da UFPE e no PDTIC 2017-2019 para padronização e controle do uso de uma solução antivírus que atenda às necessidades da UFPE.

MANIFESTAÇÃO DA ENTIDADE AUDITADA

O Núcleo de Tecnologia da Informação juntamente com a PROGEST tem nos últimos dez anos adquirido computadores com licença de Sistema Operacional incluída. Já para atender as demandas de aplicativos office, o NTI orienta por meio dos NATI´s a instalação exclusiva de soluções de software livre.

No tocante ao antivírus, o NTI também tem implantado soluções gratuitas. Neste quesito, no entanto, o órgão tem avaliado a inviabilidade de manutenção de solução gratuita por esta não ser gerenciável em um nível corporativo. Nesse sentido, o NTI está atualmente em busca de uma solução, baseada em inteligência artificial, que deve atender às necessidades da UFPE tecnicamente, em relação ao custo/benefício e quanto ao nível gerencial. O NTI tem reunião técnica agendada com fornecedores para o próximo dia 25 de agosto e pretende implantar nos próximos noventa dias um projeto piloto no NTI, devendo posteriormente ser implantado na Reitoria e demais Pró-reitorias para avaliação da solução antes de iniciar uma implantação mais abrangente em toda a UFPE.

No tocante aos encaminhamentos, a PROCIT:

1) *Discutirá a diretriz de uso de software livre explicitada nesta constatação com o NTI e demais órgãos da alta administração, para que esta seja incluída na política de TIC da UFPE e no PDTIC 2017-2019.*
2) *Convocará reunião de alinhamento entre a Diretoria de Governança de TIC e Processos, o NTI e a Coordenação de Segurança da Informação sobre a viabilidade de controladores de domínio descentralizados e quanto à norma de uso de antivírus.*

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

ANÁLISE E RECOMENDAÇÃO DA AUDITORIA INTERNA

Com base na manifestação da Pró-reitoria de Comunicação, Informação e Tecnologia da Informação – PROCIT verificamos que o NTI tem tomado providências no sentido de avaliar a implementação de uma solução, baseada em inteligência artificial, que atenda às necessidades da UFPE tecnicamente, em relação ao custo/benefício e quanto ao nível gerencial uma vez que a manutenção de solução gratuita mostra-se inviável por esta não ser gerenciável em um nível corporativo. Enquanto esse processo não é finalizado a PROCIT se compromete a discutir a diretriz de uso de software livre explicitada nesta constatação com o NTI e demais órgãos da alta administração, para que esta seja incluída na política de TIC da UFPE e no PDTIC 2017-2019 bem como convocar uma reunião de alinhamento entre a Diretoria de Governança de TIC e Processos, o NTI e a Coordenação de Segurança da Informação sobre a viabilidade de controladores de domínio descentralizados e quanto à norma de uso de antivírus.
A AUDINT acata os seus esclarecimentos, reservando tais justificativas como objeto de análise quando no acompanhamento das implementações recomendadas.

6. CONSIDERAÇÕES FINAIS

Concluídos os exames de auditoria e recebidas às justificativas/esclarecimentos das unidades auditadas acerca dos questionamentos apontados, pode-se observar o engajamento da Universidade para o fortalecimento da Governança de Tecnologia de Informação e Segurança da Informação. A UFPE possui um Plano Diretor de Tecnologia da Informação, com objetivos alinhados ao PEI e ao PDI. A Instituição também possui uma política de segurança da Informação aprovada, as cópias de segurança da instituição são realizadas por um sistema de backup com tecnologia atualizada com capacidade e velocidade para atender a demanda atual cujo acesso ao Data Center é controlado por verificação biométrica da face.

Entretanto, identificamos fragilidades nos controle internos ora auditados, especialmente quanto ao monitoramento das ações do plano do PDTIC, à morosidade na atualização do PDTI 2017-2019 bem como a ausência de normas e procedimentos específicos relacionados à Segurança da Informação.

Em face dos exames realizados, somos de opinião que as Unidades Gestoras auditadas deverão adotar medidas corretivas com vistas a elidirem os pontos ressalvados neste Relatório Final, pelo que recomendamos sobretudo:

- Efetivar a finalização e aprovação do Plano Diretor de Tecnologia da Informação da UFPE com validade para o triênio de 2017-2019. Ampliar a equipe de apoio à alta administração de modo a viabilizar a realização dos objetivos do planejamento tempestivamente.
- Proceder a inclusão do Plano de Gerenciamento de Riscos, do Plano de Gestão de Pessoas e do Plano Orçamentário de TIC no PDTI 2017-2019.
- Melhorar o alinhamento com a alta administração sobre focos estratégicos de TIC para uma definição mais objetiva das metas a serem alcançadas. Realizar o processo de revisão e monitoramento das ações do plano do PDTIC.

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com

- Realizar uma segunda alteração da portaria normativa nº 09 de 19 de setembro de 2014, já alterada pela Portaria Normativa nº 07 de 19 de maio de 2015 para que seja efetivada a exclusão DA Participação da Auditoria Interna da UFPE no Comitê de Segurança da Informação.
- Formalizar e implantar um Plano de Continuidade do Negócio (PCN), Norma de Revogação de Direitos de Acesso, um Plano de Tratamento de Riscos em Segurança da Informação e Comunicações, um Plano de Treinamento em Segurança da Informação e promover a capacitação de servidores da PROCIT em gestão de riscos para atuar na elaboração desses planejamentos.
- Avaliar a implementação de uma solução, baseada em inteligência artificial, que atenda às necessidades da UFPE tecnicamente, em relação ao custo/benefício e quanto ao nível gerencial e a viabilidade de controladores de domínio descentralizados. Incluir na política de TIC da UFPE e no PDTIC 2017-2019 uma norma de uso de antivírus.

As recomendações exaradas por esta Unidade de Controle Interno serão objeto de monitoramento, quando na emissão do Relatório de Acompanhamento, com o fito de verificar as suas implementações.

Com efeito, vencidos os trabalhos de análises nas UG's PROCIT, NTI E PROGEST, encaminhamos este Relatório Final ao Gabinete do Reitor para ciência, solicitando o seu envio à Controladoria Geral da União, em obediência à Instrução Normativa CGU – SCI nº 24, de 17 de novembro de 2015.

A AUDINT também encaminhará este Relatório às UG's auditadas para que os procedimentos já adotados nesse trabalho sejam mantidos e aperfeiçoados em toda a Instituição e para que seja realizada a implementação das recomendações emanadas por essa Auditoria Interna. Por oportuno, informamos que, em cumprimento à IN-CGU outrora mencionada, a AUDINT dará conhecimento ao Conselho de Administração sobre o presente Relatório.

Salientamos que o objetivo deste trabalho desenvolvido pela AUDINT foi atender ao seu Plano Anual de Atividades da Auditoria Interna, bem como, buscar a melhoria constante da gestão da UFPE.

Recife, 25 de setembro de 2017.

Jediene Galdino Gonçalves
Auditora interna da UFPE
SIAPE 1959532

Rosana Medeiros Ferreira
Contadora
SIAPE 1924312

Av. Prof. Moraes Rego, 1235, Salas 148 e 149, Prédio da Reitoria, CEP 50670-901, Recife-PE.
Fone: (81) 2126-8196; Fone/Fax: (81) 2126-8181.
E-mail: audint.ufpe@hotmail.com