Universidade Federal de São Carlos
Unidade de Auditoria Interna
Rodovia Washington Luis, Km 235
Caixa Postal 676 - CEP: 13.565-905 – São Carlos-SP – Brasil
Fone: (016)3351-9782 - Fax (016)3361-2081
E-mail: auditoria@ufscar.br

AUDITORIA INTERNA
UFSCar

TIPO DE AUDITORIA : Acompanhamento da Gestão Integrada
ÁREA AUDITADA : Gestão de Tecnologia de Informação (TI)
RELATÓRIO Nº : **201404**

RELATÓRIO FINAL DE AUDITORIA INTERNA

Magnífico Reitor,

Em cumprimento ao Plano de Trabalho nº 05/2014 - AudIn, apresentamos os resultados dos exames realizados no Acompanhamento da Gestão Integrada" ocorridos no período de 02/01/2014 a 31/08/2014, contemplando:
- *A ação 8.1 do PAINT 2014, na área de Gestão de TI – Tecnologia de Informação.*

I - ESCOPO DO TRABALHO

1. Os trabalhos foram realizados junto à SIn - Secretaria Geral de Informática no período de 01/08/2014 a 29/08/2014.
Foram observadas as normas de auditoria aplicáveis ao serviço público federal objetivando o acompanhamento preventivo dos atos e fatos de gestão ocorridos no período de abrangência do trabalho.
Registramos que não houve quaisquer restrições de informações ao nosso trabalho.

2. Metodologia

Os trabalhos de auditoria consistiram no acompanhamento e Identificação dos riscos na área de TI da Universidade, prevendo a possibilidade de algo acontecer e impactar nos objetivos da integração da gestão em segurança de software e hardware. Buscou-se conformidade com as Instruções Normativas da SLTI - Secretaria de Logística e Tecnologia da Informação, ISO 27001 (Gestão de Segurança da Informação), Request for Comments (RFC) 2196 e especificações técnicas dos componentes da e-PING (Padrões de Interoperabilidade de Governo Eletrônico-2010) e às disposições contidas no Decreto nº 5.707/2006, art. 5º, 2º, c/c Portaria MP nº 208/2006, art. 2º, I e art. 4º.
Inicialmente, foi elaborado um QACI – Questionário de Avaliação de Controles Internos (check-list) contemplando o escopo de verificar o estágio da implantação do PDTI, governança, política de segurança da informação e gestão em TI, ambiente de hardware e software, segurança nos ambientes dos servidores de PED (data center), existência de plano de contingência de riscos, manuais de procedimentos das áreas funcionais entre outros.

Informamos que no próximo tópico deste relatório (Item II - Resultados dos Exames) foram reportadas todas as respostas aos itens contemplados no QACI e respondidas pelos auditados e separadas em tópicos para uma análise mais sucinta das informações e dados apresentados pelo gestor e foram selecionados alguns itens para verificação das informações considerando o tempo de auditoria e a nossa capacidade operacional.

II - RESULTADOS DOS EXAMES
3 ASSUNTO - Acompanhamento da Gestão Integrada – TI

3.1 INFORMAÇÃO – CONTROLES INTERNOS

A) Política de Gestão da Segurança da Informação (PSI)

- Em relação à institucionalização e/ou formalização de uma Política de Segurança da Informação (PSI) na SIn está sendo formalmente implementada por exigência do Plano Diretor de Tecnologia da Informação (PDTI);
- Quanto ao acesso às informações e a rede internet - são adotados padrões mínimos da ISO 27001 (Gestão de Segurança da Informação) com o objetivo precípuo de mitigar e gerir adequadamente os riscos na área de TI;
- Quanto à divulgação da política de segurança de informação, a SIn divulga procedimentos e normas de TI à comunidade em sua página, acessada pelo endereço: www.sin.ufscar.br. Disponibiliza também, tutoriais para configuração e solicitação de serviços (http://helpdesk.ufscar.br/otrs/customer.pl);
- Existe uma política de restrições de segurança ao uso da Internet que engloba o monitoramento de acesso e navegação em sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados, inclusive downloads e uploads de arquivos, filmes, softwares P2P e de IM, o foco das ações de segurança de TI é limitado ao uso da Internet. Entretanto, é uma política incipiente que limita-se a uma forma de controle limitada a "logs";
- Sobre a PSI (política de segurança da informação) na utilização de redes sem fio "Wireless", a SIn iniciou um trabalho de identificação de usuários desde o início de 2014 e atualmente, grande parte das redes wireless já estão sendo identificadas;
- A Secretaria de Informática implantou, também, uma solução em software livre para identificação e autenticação dos usuários das redes sem fios, onde inclusive - parte das redes wireless já contam com mecanismos de autenticação. Esse processo de autenticação prevê o registro de Logs de acesso à rede WIFI, seja o usuário: aluno, docente, estagiário, técnico administrativo. O IP (Internet Protocol) tem sido usado como principal mecanismo de endereçamento e identificação;
- Em relação à segurança dos dados e informações armazenados nos "data center" em cada campi ou ambiente operacional onde se encontram os servidores de arquivos, banco de dados e documentos ou equipamentos de comunicação, está em processo a implantação de "sala cofre" que foi iniciada em 2014 no campus de São Carlos. E que - a partir da experiência dessa implantação e o aporte de novos recursos - deverão ser atendidos os demais campi de Sorocaba, Araras e Lagoa do Sino. Ressalte-se, no entanto que quase todos os sistemas críticos, bancos de dados e outros recursos de TI acessados pelos usuários estão concentrados no "Data Center" de São

Carlos, o que justifica ser o primeiro campus a receber a sala cofre. Esse "Data Center" do Campus São Carlos possui no-breaks, gerador de energia (área externa) e estabilizadores de modo a garantir a estabilidade e integridade das bases de dados. Há manutenção periódica ou verificações preventivas nos equipamentos de "no-break" e/ou no gerador de energia através de contratos ou por demandas por chamadas avulsas;
- Nos casos de desligamento de servidores efetivos que tenham acesso a algum ambiente operacional de TI estratégico (data Center, por exemplo) – verificamos que há rotina/procedimento onde toda chave, cartão magnético ou crachá são recolhidos, embora seja um procedimento não formalizado, é aplicado para impedir acessos desse usuário após o seu desligamento; inclusive – também são recolhidos os cartões de acessos das portarias do prédio. Além disso, as senhas de acesso aos "Data Center" são trocadas no caso de saída/desligamento de servidor efetivo da equipe da SIn e não são permitidas reutilizações das mesmas;
- As "senhas" de acessos ao "Data Center" são definidas baseando-se nas recomendações do RFC 2196 e através de um algoritmo próprio da SIn. O acesso físico ao local é controlado por biometria e cartões de acesso;
- São utilizadas fechaduras eletrônicas nas portas de acesso ao "data Center" e o acesso às informações contidas nos servidores de aplicação é realizado por Analistas e Técnicos por meio de login e senha, gerados por algoritmo;
- O "WebMail UFSCar" segue os padrões de atualização e especificações técnicas dos componentes da e-PING (Padrões de Interoperabilidade de Governo Eletrônico-2010) em relação à segurança contemplando: HTTPS, TLS com IMAP, S/MIMEv3, SPF que trata da forma de troca de correio eletrônico seguro utilizando redes inseguras;
- No entendimento da SIn o procedimento de inventário de ativos deve ser realizado pelo Departamento de Patrimônio;
- Há um PDTI em fase de "aprovação", mas que contempla o constante desenvolvimento institucional na área de TI a cada triênio. Esse PDTI é a base para o desenvolvimento na área de TI (disponível no link: www.pdti.ufscar.br**);**

B) Política de Gestão da Infraestrutura de Software e Hardware

Existem as seguintes práticas em nível de gestão de infraestrutura de hardware e software:
- A Resolução sobre Normas e Procedimentos para Uso de Recursos de TI contempla um plano inicial a ser implantado. Para a autenticação da rede cabeada será necessário a troca de Ativos das redes (por ex. switchs) para modelos que possuam a tecnologia com suporte à identificação (Por ex. switch 802.1X). Essa troca demanda recursos financeiros e humanos. (Doc - Normas e Procedimentos para Uso de Recursos de TI – Site da SIn).
- Todas as baixas/doações de equipamentos de hardware onde há gravação de dados/informações só são realizadas após a certificação de eliminação de todos os arquivos com informações classificadas como de uso restrito;
- Com vistas a evitar danos à infraestrutura de hardware, existem na SIn extintores de incêndio do tipo apropriado para combater o fogo em equipamentos eletrônicos classe C (equipamentos elétricos) de forma que

não danifique os mesmos. São 16 extintores assim distribuídos: 2 na sala da operação, 2 no corredor no. 01, 2 no corredor no. 02, 3 no saguão, 2 no corredor no. 03, 3 no corredor no. 04, 1 no depósito no. 01 e 01 no depósito no. 02;
- Quanto às aquisições de softwares ou hardwares (equipamentos de TI) nos vários setores da Universidade, não há norma instituída pela Universidade para que as aquisições de equipamentos de TI sejam discutidas e aprovadas pela Câmara Assessora de Tecnologia da Informação CATI. Assim, os setores da Universidade têm autonomia para adquirir equipamentos de acordo e conforme as suas necessidades;
- Os recursos de TI disponíveis são avaliados de forma "parcial" que é realizada com base no especificado no ano anterior no PDTI;
- Há na SIn uma sistemática de transferência de "know-how" para servidores da unidade/setor referente a produtos e serviços (hardware/software) de TI que são terceirizados, por exemplo: Sistema Integrado de Gestão Acadêmica (SIGA-UFSCar). Entretanto, não para hardware proprietário, pois são realizados contratos de manutenções com as empresas fornecedoras dos mesmos;
- Existe na SIn a política de seguir as boas práticas da Engenharia de Software e Banco de Dados. Por exemplo, o novo ERP e os novos sistemas, como o de Controle de Acesso e Patrimônio, estão sendo construídos com uma arquitetura baseada em padrões de software e o banco de dados normalizado para evitar redundâncias e inconsistências. No seguinte link: http://www.sin.ufscar.br/servicos/sistemas-de-informacao, foi disponibilizado o Manual de Procedimentos para desenvolvimento de sistemas contendo as principais informações sobre as tecnologias utilizadas na área de Engenharia de Software;
- São previstas e efetuadas atualizações das "Contratações de Licenças" de software e hardwares existentes na SIn, algumas são feitas por contratos anuais, embora a maioria das "licenças" sejam contratos vitalícios adquiridos no ato da compra do hardware. Entretanto, essa política adotada de controle e fiscalização dos contratos de Licença de uso de softwares operacionais e aplicativos em uso na UFSCar com o intuito de manter os softwares originais (legais) possui um caráter parcial a nível de software, tanto no âmbito interno da SIn bem como nos laboratórios de Informática controlados por ela;
- A SIn mantém política de monitoramento das atualizações e/ou melhorias no sistemas implantados ou em implantação na Universidade, exemplos: SAGUI (ERP) e SIGA, através da interação com os POs (donos dos produtos) mantém os sistemas atualizados com os novos requisitos funcionais e não funcionais;
- Existe um controle parcial dos softwares, tanto no âmbito interno da SIn bem como nos laboratórios de Informática controlados por ela. Novas medidas estão sendo tomadas para que todos os softwares sejam legalizados na SIn, ou substituídos por software livres;
- Há canais de comunicação divulgados e disponíveis na página da SIn como o "helpdesk" – disponível no link: www.helpdesk.ufscar.br, ferramenta que serve como canal de comunicação entre a SIn e todos os usuários de software/hardware na Universidade. Assim, todas as solicitações dos usuários, as sugestões e as reclamações sobre TI são direcionadas ao setor

responsável, no caso o DeASU (Departamento de Apoio e Suporte ao Usuário) criado com a reestruturação da SIn é o setor responsável por esse serviço.

C) Política de Gestão da Infraestrutura Administrativa (Peopleware)

- Em relação à infraestrutura administrativa, a SIn disponibiliza em seu sítio eletrônico (www.sin.ufscar.br) um organograma com os seus respectivos setores e servidores responsáveis.
- Existe uma previsão de cursos de capacitação/treinamento periódico para o pessoal de TI efetivos na SIn. A capacitação é sob demanda. Anualmente, um levantamento é realizado na SIn e encaminhado à Administração para providenciar sua realização.

3.2 CONSTATAÇÕES

A) Política de Gestão da Infraestrutura de Software e Hardware

3.2.1 CONSTATAÇÃO: Ausência de plano de contingência para amenizar os riscos em TI.

MANIFESTAÇÃO DO AUDITADO: A Resolução sobre Normas e Procedimentos para Uso de Recursos de TI contempla um plano inicial a ser implantado. Para a autenticação da rede cabeada será necessário a troca de Ativos das redes (por ex. switchs) para modelos que possuam a tecnologia com suporte à identificação (Por ex. switch 802.1X). Essa troca demanda em recursos financeiros e humanos. (Doc - Normas e Procedimentos para Uso de Recursos de TI – Site da SIn).

ANÁLISE DA AUDITORIA INTERNA: Verificamos alto risco de segurança da informação, e.g. - vazamentos de informação, uso indevido da infraestrutura de TI por "terceiros" - e de continuidade e/ou interrupções de serviços de TI críticos que comprometam ou inviabilizem as operações normais da Universidade.

3.2.1.1 RECOMENDAÇÃO: Que a SIn intensifique ações que promovam a melhoria da gestão de riscos e de controles internos em conformidade com as Instruções Normativas da SLTI - Secretaria de Logística e Tecnologia da Informação, ISO 27005 (Gestão de Segurança da Informação), Request for Comments (RFC) 2196 e especificações técnicas dos componentes da e-PING (Padrões de Interoperabilidade de Governo Eletrônico-2010).

MANIFESTAÇÃO DO AUDITADO NO RELATÓRIO PRELIMINAR: *"A autenticação dos usuários da rede UFSCarnet foi iniciada em Maio/2014, começando pelas áreas publicas onde os riscos de usos indevidos são maiores.Com recursos próprios ano 2014 (RTN), conseguimos atingir 30% (trinta por cento) de autenticações dos usuários de rede sem fio.*
Para o ano 2015, temos como meta implantar mais 30% (trinta por cento) de autenticações dos usuários na rede sem fio chegando a 60% (sessenta por cento) e também iniciar as autenticações dos usuários da rede cabeada alcançando 30% (trinta por cento) no ano de 2015.A implantação está planejada por etapas, devido ao alto custo financeiro, pois envolve a troca dos switches e dos pontos de acessos por novos, do tipo gerenciáveis."(Ofício SIn no.062/2014)

MANIFESTAÇÃO DA AUDiN: O "plano de contingência" requer um estudo e planejamento para amenizar os riscos inerentes à área de TI, o que engloba ações mais amplas, não somente ações pontuais como a autenticação da rede cabeada ou a troca de Ativos das redes, mas uma adequação, como

exemplo - às exigências da ISO 27005 no que diz respeito ao processo de gestão de riscos, quais sejam: ativo, ameaça, vulnerabilidade e impacto. Portanto, entendemos que o processo ainda está em sua fase inicial e a SIn deve intensificar ações pró-ativas na área de PSI (Política de Segurança da Informação).

3.2.2 CONSTATAÇÃO: Ausência efetiva de estímulos para a implantação e utilização dos "softwares livres" na Universidade.

MANIFESTAÇÃO DO AUDITADO: Um plano inicial está sendo adotado. Estamos preparando cursos e treinamentos para software livres, que serão oferecidos à comunidade tão logo estejam prontos.

ANÁLISE DA AUDITORIA INTERNA: A adoção do Software Livre por parte do Estado é amparada principalmente pelos princípios de Impessoalidade, Eficiência e Razoabilidade[1].

Quanto à utilização de software livre nos órgãos públicos, o TCU fez as seguintes considerações:

> ***Acórdão 1598/2006 Plenário***
>
> *Abstenha-se de proceder a 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:*
>
> *• 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 a 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 a contratante.*
>
> *Com isso, dispensa-se a necessidade de pagar patentes e contratar diretamente as mesmas empresas, fornecedoras exclusivas de sistemas, para atualização.*
>
> ***Acórdão 1521/2003 Plenário***
>
> *Não obstante a indicação de marca, desde que circunstanciadamente motivada, possa ser aceita em observância ao principio da padronização, este como aquela não devem ser obstáculo aos estudos e a efetiva implantação e utilização de software livre no âmbito da administração Publica Federal, vez que essa alternativa poderá trazer vantagens significativas em termos de economia de recursos, segurança e flexibilidade.*

3.2.2.1 RECOMENDAÇÃO: Que o PDTI contemple ações para adoção do uso de "software livre" na Universidade com vistas à eliminação de mudanças compulsórias que os modelos proprietários impõem periodicamente a seus usuários, em face da descontinuidade de suporte a versões ou soluções, bem como eliminação de despesas referentes a licenças de uso.

---

[1] *O artigo 37 da Constituição da República apresenta os Princípios Basilares da Administração Pública: legalidade, impessoalidade, moralidade, publicidade e eficiência. O princípio da razoabilidade possui fundamentação implícita, sendo evidenciado em algumas Constituições Estaduais.*

MANIFESTAÇÃO DO AUDITADO NO RELATÓRIO PRELIMINAR: "*Conforme já manifestado, foi adotado um plano para oferecer cursos e treinamentos para software livres. Este processo teve início com a última licitação ocorrida com a compra de periféricos de informática compatíveis com software livre."(Ofício SIn no.062/2014)*

MANIFESTAÇÃO DA AUDiN: *Permanecem a recomendação 3.2.2.1 diante da ausência de dados e informações relevantes e detalhadas na resposta do auditado: "Que o PDTI contemple ações para adoção do uso de "software livre" na Universidade com vistas à eliminação de mudanças compulsórias que os modelos proprietários impõem periodicamente a seus usuários, em face da descontinuidade de suporte a versões ou soluções, bem como eliminação de despesas referentes a licenças de uso."*

3.2.3 CONSTATAÇÃO: Inexistência de Inventário de ativos de Informação em desacordo com a NBR ISO/IEC 27.002 item 7.

MANIFESTAÇÃO DO AUDITADO: "...Sim, no âmbito SIn. Externo a SIn o procedimento deve ser realizado, salvo melhor juízo, pelo Departamento de Patrimônio."

ANÁLISE DA AUDITORIA INTERNA: Há um equívoco no entendimento e interpretação do que seja inventário de ativos de informação. Segundo item 7.1 da NBR ISO/IEC 27.002, há vários tipos de ativos, sendo que os "ativos físicos" são apenas um dos tipos de ativos, conforme já citado nos seguintes Acórdãos – TCU: AC-2613-40/11-P, AC-0592-08/11-P, AC-0594-08/11-P que versam sobre a matéria.

3.2.3.1 RECOMENDAÇÃO: Que a SIn estabeleça procedimento de inventário de ativos de informação, de maneira a que todos os ativos de informação sejam inventariados e tenham proprietário responsável, observando o item 7.1 da NBR ISO/IEC 27.002.

B) Política de Gestão da Infraestrutura de Software e Hardware

3.2.4 CONSTATAÇÃO: Intempestividade/morosidade na aprovação do PDTI pela Administração superior.

MANIFESTAÇÃO DO AUDITADO: "...Embora não aprovado é a base para o desenvolvimento na área de TI".

ANÁLISE DA AUDITORIA INTERNA: O Plano Diretor de Tecnologia da Informação 2013/2015, ainda não foi aprovado pela CATI – Câmara Assessora de Tecnologia de Informação. Embora a CATI tenha sido aprovada em reunião da COAD em 03/05/2013, ainda não houve a "primeira" reunião que contemple a aprovação do PDTI-UFSCar. Portanto, há uma morosidade no processo de implementação do PDTI, citamos por exemplo, ausência de planejamento de ações relacionadas ao novo campus Lagoa do Sino.

3.2.4.1 RECOMENDAÇÃO: Que administração superior juntamente com o presidente da CATI – Câmara Assessora de Tecnologia de Informação envide esforços para a premente necessidade de apreciação do PDTI-UFSCar.

C) Política de Gestão da Infraestrutura Administrativa (Peopleware)

3.2.5 CONSTATAÇÃO: Ausência de planos de ações efetivos que contemplem a capacitação continuada dos servidores atuantes na SIn.

MANIFESTAÇÃO DO AUDITADO: "A capacitação é sob demanda. Anualmente, um levantamento é realizado na SIn e encaminhado à Administração para providenciar sua realização".

"Não tivemos nenhum curso neste ano. O nosso pedido depende da aprovação da PROAD, pois é RP. Não sabemos quando serão oferecidos, se neste ano ou no ano próximo".

ANÁLISE DA AUDITORIA INTERNA: Apesar da resposta do auditado: "... *não houve nenhum curso de capacitação para os servidores lotados na SIn até a presente data.*" Identificamos no sistema SIAFI a realização de um curso de capacitação em LINUX referente ao Campus Araras. O PDTI-UFSCar contempla a necessidade de cursos de capacitação, entretanto, houve uma incipiente ação da SIn na busca de inovação, atualização de novos conhecimentos necessários para os seus servidores numa área tão estratégica da administração.

Mesmo que os 'pedidos' dependam de aprovação da ProAd, pois são recursos próprios, consta no PDTI as necessidades de distribuição de recursos.

3.2.5.1 RECOMENDAÇÃO: Que a SIn avalie/concilie no PDTI as previsões entre necessidades/recursos e proceda ações para sua efetiva realização em atenção às disposições contidas no Decreto nº 5.707/2006, art. 5º, 2º, c/c Portaria MP nº 208/2006, art. 2º, I e art. 4º.

São Carlos, 23 de outubro de 2014.

Wania Maria Recchia
SIAPE - 424881

Felizardo Delgado
SIAPE - 1572938