RELATÓRIO DE AUDITORIA INTERNA Nº 06/2014

ÁREA: TECNOLOGIA DA INFORMAÇÃO

D T I C

INSTITUTO FEDERAL
SANTA CATARINA

Ministério da Educação

GOVERNO FEDERAL
BRASIL
PAÍS RICO É PAÍS SEM POBREZA

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA
UNIDADE DE AUDITORIA INTERNA – AUDITORIA GERAL
Telefone (48) 3877-9006 – e-mail: auditoria@ifsc.edu.br

RELATÓRIO DE AUDITORIA INTERNA

Nº 06/2014

Dirigentes

Magnífica Reitora Profª. Maria Clara Kaschny Schneider

Prof Andrei Zwetsch Cavalheiro (PRODIN)

Prof Emerson Ribeiro de Mello (DTIC).

Área:

Departamento de Tecnologia da Informação

Origem da Demanda: PAINT/2014

A. Introdução

A Diretoria de Tecnologia da Informação e Comunicação (DTIC) está subordinada à Pró-reitoria de Desenvolvimento Institucional (PRODIN), e tem por objetivo, desenvolver as atividades de gestão da Tecnologia de Informação e Comunicação da instituição. Cabe a DTIC o planejamento, a coordenação, a organização, em nível central, da tecnologia da informação e comunicação a fim de alinhar os objetivos, ações e metas às estratégias denidas no Plano de Desenvolvimento Institucional (PDI). Dentre as atribuições da DTIC, podemos destacar:

- Planejar e viabilizar o desenvolvimento dos projetos relacionados ao PDTI;

- Identificar as necessidades da instituição quanto a Tecnologia da Informação e Comunicação e planejar o desenvolvimento de projetos para o atendimento dessas necessidades;
- Propor políticas de Tecnologia da Informação e Comunicação e de Segurança da Informação e Comunicação para a instituição;
- Avaliar os riscos nos projetos de Tecnologia da Informação e Comunicação;
- Gerenciar os investimentos de Tecnologia da Informação e Comunicação e propor recursos para ações de Segurança da Informação e Comunicação;
- Acompanhar as investigações e avaliações dos danos decorrentes de quebras de segurança da informação no âmbito da instituição.

Por ser uma atividade estratégica e essencial à organização, de alta relevância, que nunca foi auditada em anos e trabalhos anteriores, que já foi demandada e solicitada para trabalhos de auditoria pelo CONSUP do IFSC e pela CGU, a área de TI passou a incorporar a Matriz de Risco dos trabalhos de Auditoria, inseridos no PAINT 2014, aprovado pelo Conselho Superior da Instituição e pela Controladoria Geral da União – CGU.

B. Objetivo

A presente atividade de auditoria teve por objetivo aferir e avaliar as atuais condições dos controles administrativos internos na área da Tecnologia da Informação – **em especial os controles relacionados à Segurança da Informação.** Os trabalhos foram realizados durante o mês de dezembro de 2014 pela Auditoria Geral – Reitoria. Foram utilizados diversos procedimentos e técnicas de auditoria para a consecução dos objetivos pretendidos, em especial: testes de observância e testes substantivos, englobando a conferência de documentos e dados extraídos dos sistemas operacionais de informações em uso pela unidade, especialmente SIAPE e DGP.

Em suma, o presente trabalho buscou avaliar os procedimentos, fluxos, mecanismos e ferramentas de controle utilizados e em efetivo funcionamento no âmbito da Tecnologia da Informação, em especial da Segurança da Informação no IFSC.

C. Da Metodologia

Encaminhamento de Solicitação Auditoria ao departamento envolvido; análise do material e seleção de amostras; registro das constatações e recomendações; elaboração do relatório final que ficará disponível para consulta pública no endereço eletrônico: http://www.ifsc.edu.br/menu-unai-raint em atendimento à lei de acesso à informação.

D. Período de Realização

a) Planejamento: 15/11 a 30/11/2014
b) Execução: 01/12 a 15/12/2014
c) Encerramento – Análise dos Papéis de Trabalho e Relatórios – 15/12 a 18/12/2014

E. Equipe e Horas/Atividades

AUDITORES	ATIVIDADE	HORA/ATIVIDADE
Patrick Barcelos Teixeira	Coordenação de Campo / Planejamento / Análise de Processos /Relatório Prévio	80h
João Clovis Schmitz	Planejamento / Coordenação Geral / Análise Final / Revisão	80h

1. CONSIDERAÇÕES INICIAIS

Os trabalhos foram realizados dentro dos prazos previstos, sendo que nenhuma restrição foi imposta aos nossos trabalhos. Abaixo seguem as informações e constatações verificadas no decorrer dos trabalhos de auditoria, bem como as respectivas recomendações desta Unidade de Auditoria Interna, para a avaliação, conhecimento e providências que a gestão porventura julgar oportunas, convenientes e cabíveis.

2. RESULTADOS DOS TRABALHOS

INFORMAÇÃO 1: **Existência de rotina de realização de testes.**

Foi verificado que existe uma rotina de realização de testes semanais para aferição do correto funcionamento do grupo gerador e no-break, bem como existe um servidor designado para o acompanhamento das rotinas de verificações. Foram apresentadas informações que buscaram evidenciar que os servidores blade, storage e backup apresentam funcionamento correto.

Recomendação A: criar uma rotina ou procedimento de documentar e historizar as verificações periódicas de funcionamento dos servidores.

Recomendação B: aprimorar a rotina de realização de testes, de forma que as verificações sejam efetivadas de maneira tempestiva e periódica, de acordo com as necessidades técnicas de cada equipamento.

INFORMAÇÃO 2: **Realização de backup na Reitoria e no CERFEAD.**

Foi verificado que existe a rotina de realização de cópias de segurança dos dados armazenados nos servidores da Reitoria, através de software próprio, com backups incrementais diários e completos uma vez à semana. Entretanto, com relação aos equipamentos do CERFEAD foi verificado que ocorreu uma mudança na administração e gestão dos seus equipamentos, que até o mês de julho de 2014 ficavam a cargo de um grupo de bolsistas contratados para tal finalidade e atualmente está sob a responsabilidade da DTIC, o que ocasionou um hiato onde inexiste um procedimento implementado e validado de realização de cópias de segurança. Ademais, foi informado que o CERFEAD possui uma tape library porém os backups não são realizados na fita pois inexiste um software para tanto; igualmente foi informado que o procedimento de

armazenamento das cópias chegou a ser realizado através do RSNAPSHOT, porém tal procedimento passou por um processo de descontinuidade quando da mudança da administração e gestão dos indigitados equipamentos.

Recomendação A: que seja implementado um procedimento de realização e armazenamento de cópias de segurança dos equipamentos do CERFEAD, seja através da aquisição de software e registro na tape library própria ou de qualquer outro meio tecnicamente viável e seguro que garanta a efetividade dos backups.

Recomendação B: que seja garantida a segurança e a eficiência dos backups realizados, e que sejam de fato testados, conforme indicam as melhores práticas na área de segurança em TI, em especial que seja evitado o armazenamento e arquivamento das cópias de segurança nos mesmos locais e espaços (prédios/campus) dos servidores e equipamentos que foram copiados, evitando que em caso de sinistro tanto os dados e informações primárias e originais, quanto suas respectivas cópias, sejam perdidos.

CONSTATAÇÃO 1: **Ausência de gerenciamento de riscos de TI.**

Inexiste a realização de gerenciamento de riscos, de acordo com um processo formalizado, de forma a mitigar e reduzir possíveis e eventuais impactos negativos, em especial o não atingimento de metas e necessidades, constantes no PDTI 2014-2015.

Recomendação 1.1:

Elaborar um procedimento formalizado de gerenciamento de riscos de TI, de acordo com o PDTI biênio 2014-2015, e executá-lo conforme as necessidades técnicas da área e institucionais, visando a mitigação e redução dos riscos residuais e inerentes à área de TI.

CONSTATAÇÃO 2: **Ausência de ferramenta de revogação de acesso (e-mail).**

Verificou-se que existem fluxos pré-definidos de inclusão, manutenção e exclusão de acessos aos sistemas DGP e SIG, contudo inexiste política e mecanismo implementado para revogação de acessos às listas de e-mail, somente uma prática de concessão das listas de e-mail, alteração de senha de administração da lista e registro, arquivamento e armazenamento dos logs de trocas de senhas, no sistema DGP/LDAP/Listas. Como exemplo cita-se o e-mail "erico@ifsc.edu.br", que pertencia ao servidor Érico de Ávila Madruga, que não integra mais o quadro funcional do IFSC, todavia ainda está no rol de e-mails das listas "dam" e "todos.reitoria".

Recomendação 2.1:

Criar, implementar e manter sempre atualizado os procedimentos, ferramentas e meios de revogação de acessos às listas de e-mail, bem como do próprio e-mail institucional, daqueles servidores que não mais integrem ou laborem no IFSC, independente do gênero do rompimento do vínculo, seja por exoneração, demissão, cessão, etc, especialmente através de um fluxo e uma rotina que envolva a comunicação tempestiva da DGP à DTIC das alterações das situações funcionais dos servidores, para que esta possa executar as alterações e especialmente as revogações de maneira célere.

CONSTATAÇÃO 3: **Ausência de gestão de segurança da informação e TI.**

Foi constatado que inexiste uma política de segurança da informação bem como a gestão de continuidade de negócio relativa aos serviços de TI. Não foi criado e implementado no IFSC um Comitê de Segurança da Informação, que contemple, por óbvio, a segurança em tecnologia da informação.

Recomendação 3.1:

A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas

organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos.

Dessa forma, recomendamos a criação imediata do Comitê de Segurança da Informação no âmbito da organização, que contemple a área de segurança em tecnologia da informação, bem como as áreas de segurança física, patrimonial, etc, constituído por uma equipe multidisciplinar de servidores. E que a partir daí, se institua e formalize uma política se segurança da informação e gestão de continuidade de negócio relativos aos serviços/processos de TI.

Na impossibilidade de atendimento total da recomendação, que ao menos se crie um setor/coordenação, com objetivos e competências definidas, que seja responsável por implementar e manter mecanismos de controle que visem mitigar as fragilidades existente na segurança de informação dos processos de TI.

CONSTATAÇÃO 4: **Ineficiência da gestão de revogação de acessos no SIG.**

Constatou-se que, apesar da DTIC informar que existem procedimentos de rotina para manutenção e exclusão de direitos de acessos ao sistema SIG, diversos servidores que já não mais integram o quadro funcional do IFSC continuam com cadastros ativos no sistema, com diversos privilégios e direitos nos módulos SIGRH, SIPAC, SIGAA e SIGADMIN. Como exemplo se citam os ex-servidores Morgana Machado Jorge, Haroldo Gomes Nogueira Júnior e Pierri Eduardo Batista Rodrigues, todos já exonerados e com cadastros em atividade.

Recomendação 4.1:

Aplicar e manter sempre atualizado os procedimentos, ferramentas e meios de revogação de acessos aos sistemas institucionais daqueles servidores que não mais integrem ou laborem no IFSC, independente do gênero do rompimento do vínculo, seja por exoneração, demissão, cessão, etc, especialmente através de um fluxo e uma rotina que envolva a comunicação tempestiva da DGP à DTIC das alterações das situações

funcionais dos servidores, para que esta possa executar as alterações e especialmente as revogações de maneira célere.

Recomendação 4.2:

Evitar atribuir uma quantidade muito grande de direitos de acessos e privilégios a um mesmo servidor, buscando atender e respeitar o Primado da Segregação de Funções que é mandamental e fundamental na Administração Pública.

CONSTATAÇÃO 5: **Falta de atendimento a necessidades do PDTI 2014-2015.**

Verificou-se que algumas necessidades constantes no item 4.2 do PDTI biênio 2014-2015 ainda não foram totalmente cumpridas e atendidas, ou sequer iniciadas. Foram selecionadas para auditoria as necessidades (ligadas à área de segurança de TI) de números 6 (aquisição de certificado digital), 9 (enlace redundante para a Reitoria), 14 (manual com procedimento para ocupação para espaço físico), 15 (políticas de uso para os serviços de TIC), 23 (política de segurança da informação), 26 (desenvolvimento de sítio web padrão para eventos), 27 (políticas de TIC para guiar atividades das CTICs), 30 (construção de um novo datacenter DTIC adequado) e 33 (política para renovação do parque computacional).

Da totalidade das necessidades escolhidas para análise apenas a de número 6 encontra-se plenamente atendida, algumas estão em andamento e a maioria os trabalhos para atendimento sequer foram iniciados ou se encontram sem previsão de conclusão por falta de recursos humanos, financeiros, espaço físico, entre outros fatores.

Recomendação 5.1:

Iniciar as tratativas e trabalhos para atendimento das necessidades que ainda não possuem qualquer encaminhamento, em especial as necessidades 15 e 27, com brevidade e celeridade, e concluir os processos para atendimento daquelas necessidades que já foram iniciadas e por algum motivo não finalizadas, especialmente realizando as aquisições e contratações necessárias para as necessidades 9 e 26,

dando encaminhamentos efetivos nos trabalhos dos GT e comissões das necessidades 14, 23 e 33, e reforçando com a alta administração a importância e relevância do atendimento da necessidade 30.

CONSTATAÇÃO 6: **Vulnerabilidade na segurança física e ambiental.**

Constatou-se que o datacenter do IFSC apresenta algumas vulnerabilidades e carências com relação aos aspectos atinentes à segurança física e ambiental do local. Em suma, foi verificado que o controle de acesso à sala precisa ser aprimorado, haja vista que a fechadura da porta (Coord de Redes e Sistemas) que antecede a sala principal do datacenter está estragada e a porta do próprio datacenter contêm apenas uma fechadura simples. Ademais, a chave da fechadura do datacenter fica de propriedade de alguns servidores, de mais de uma área inclusive (redes, suporte, etc), que têm absoluto controle e carga da chave.

Outro aspecto que merece destaque é a política e a rotina de procedimentos de controle de acesso ao datacenter. Foi esclarecido que a sala permanece sempre fechada e só é aberta quando existe a necessidade da realização de algum serviço em seu interior, e, ainda, quando tal serviço é executado por algum agente externo/estranho à organização é sempre acompanhada a execução por algum servidor da DTIC. Todavia, esta UNAI identificou ao longo dos trabalhos de campo alguns dias e períodos em que a sala do datacenter permaneceu destrancada e aberta, sem qualquer servidor ou movimento na sala e ante sala, o que nos parece uma fragilidade importante e que merece atenção.

Com relação a segurança ambiental do local não foram identificados extintores de incêndio apropriados e adequados para algum controle de sinistro em equipamentos de informática e eletrônicos. Igualmente, não foi esclarecida se existe uma rotina de limpeza específica dos materiais e da sala, ficou entendido que tais atividades são executadas esporadicamente.

Por fim, foi também percebido que o espaço físico destinado ao datacenter encontra-se no limite, sendo essencial o atendimento da necessidade de número 30 do PDTI 2014-2015.

Recomendação 6.1:

Fortalecer e aprimorar os mecanismos e ferramentas atinentes à segurança física e ambiental do datacenter da instituição, em especial aqueles que dizem respeito aos controles de acesso (portas com fechaduras seguras, controle por senha, utilização e distribuição criteriosa de chaves, etc) de forma que o datacenter jamais permaneça destrancado e aberto senão durante a realização de alguma atividade em seu interior e sob a supervisão de um servidor responsável.

Recomendação 6.2:

Com relação a segurança ambiental do local recomenda-se adquirir extintores de incêndio apropriados e adequados, para controle de sinistros em equipamentos de informática e eletrônicos, bem como estabelecer uma rotina de limpeza específica dos materiais e da sala, de maneira que a vida útil dos equipamentos possa ser prolongada e o ambiente apresente condições adequadas para o melhor funcionamento dos servidores.

Recomendação 6.3:

Priorizar o atendimento da necessidade 30 do PDTI, haja vista que o espaço físico destinado ao datacenter da organização encontra-se próximo do seu limite de ocupação.

3. REFERÊNCIAS

ABNT NBR ISO/IEC 27001:2006. Sistemas de gestão de segurança da informação.
ABNT NBR ISO/IEC 27002:2005. Código de prática para a gestão da segurança da informação.
Decreto nº 3.505/2000. Institui Política de Segurança da Informação na Administração Federal.
COBIT 4.1.
Manual de Boas Práticas em Segurança da Informação do Tribunal de Contas da União – 2012.
PDTI IFSC 2014-2015.

4. CONSIDERAÇÕES FINAIS

Após a finalização dos trabalhos de análises em campo, na área da Tecnologia da Informação – Segurança da Informação, esta Unidade de Auditoria Interna/UNAI/IFSC, encaminha o presente relatório para a PRODIN-DTIC, indicando as principais inconsistências encontradas.

A Unidade de Auditoria Interna irá acompanhar e monitorar as recomendações propostas durante o ano de 2015 visando ampliar e melhorar os controles administrativos internos na área da Tecnologia da Informação.

Em geral, os controles internos ora auditados merecem uma atenção especial por parte da equipe diretiva da PRODIN e DTIC, principalmente os relacionados à segurança da informação que carecem de uma política efetivamente aprovada e implantada.

Independente das recomendações que serão objeto de monitoramento pela UNAI, cabe à equipe de gestores a análise de cada item destacado neste Relatório, sendo que

o acatamento das sugestões contidas neste Relatório constitui interesse exclusivo dos gestores.

Por fim, a equipe de auditores, abaixo identificada, agradece à PRODIN e a DTIC pela disponibilidade das informações e materiais requisitados e acolhida da equipe, e se coloca a disposição para elucidar quaisquer inconsistências ou inconformidades relatadas, visando, sobretudo, o fortalecimento dos controles internos do IFSC.

Florianópolis-SC, 16/12/2014.

Patrick Barcelos Teixeira
Auditor Interno da Reitoria
Auditoria Geral – UNAI/IFSC
Matrícula SIAPE: 2032943

De acordo,

João Clovis Schmitz
Auditor-Chefe
Matrícula SIAPE 1742259

*OBS: O documento original encontra-se assinado.