MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RORAIMA
AUDITORIA INTERNA

TIPO DE AUDITORIA: AUDITORIA DE AVALIAÇÃO DE GESTÃO
EXERCÍCIO: 2016
OBJETO AUDITADO: Tecnologia da Informação
RELATÓRIO Nº: 01/2017

1. Introdução

Em cumprimento ao item 7 do Plano Anual de Atividades de Auditoria Interna - PAINT 2016, no período de 26 de dezembro de 2016 a 22 de fevereiro de 2017, foi realizada a auditoria de tecnologia da informação pelas servidoras Adriene Silva do Nascimento, Fabrícia Matte Caye e Michelle de Oliveira Barbosa Veras.

2.Objetivos da Auditoria

O objetivo da ação de controle foi avaliar a gestão de tecnologia da informação, verificando o planejamento e os procedimentos para salvaguarda da informação.

3.Escopo do Trabalho

Em função do exíguo tempo o escopo da auditoria foi reduzido. Deste modo, foram analisados os seguintes documentos: Planejamento Estratégico de Tecnologia da Informação – PETI; Plano Diretor da Tecnologia da Informação- PDTI e Política de Segurança da Informação e Comunicações - POSIC.

Também foram verificados os procedimentos realizados em 2016 pelo Comitê Gestor de Tecnologia da Informação - CGTI e pelo Comitê Gestor de Segurança da Informação – CGSI.

4. Resultado dos Exames

Para executar a auditoria foram enviadas as Solicitações de Auditoria Interna-SAI nº 077/2016 e nº 001/2017, respectivamente, para a Diretoria de Tecnologia da Informação-DTI e para o Comitê Gestor de Segurança da Informação e Comunicação-CGSIC.

Em observância às normas de auditoria aplicáveis ao Serviço Público Federal foi possível constatar o que segue:

4.1. Planejamento Estratégico de Tecnologia da Informação - PETI e o Plano Diretor da Tecnologia da Informação- PDTI desatualizados

Para obter informações sobre a atualização do Planejamento Estratégico de Tecnologia da Informação - PETI e do Plano Diretor da Tecnologia da Informação- PDTI, foram solicitadas informações do diretor de tecnologia da informação do IFRR.

Por meio do MEMO Nº. 003/2017/DTI/IFRR, de 9/1/2017, o diretor informou que:

> O PETI – Planejamento Estratégico de Tecnologia da Informação, com previsão de vigência para 2012 a 2013, não foi atualizado. Esse artefato serve como referência ideal de maturidade operacional e de governança as quais, por motivos diversos que incluem a falta de pessoal qualificado, e a baixa maturidade em governança, tanto no sentido mais geral quanto no tocante à TI do IFRR, não foi alcançado na maioria dos tópicos. Dessa forma, o PETI, como instrumento de referência estratégica, continua sendo válido e suas metas continuam atuais. Um novo PETI apenas replicaria o que ali já está posto uma vez que aquelas metas básicas devem ser alcançadas para que novas sejam estabelecidas.
>
> Já o PDTI – Plano Diretor de Tecnologia da Informação, está em processo de homologação pelo CGTI – Comitê Gestor de Tecnologia da Informação, cujo processo para submissão ao CONSUP já está aberto sob o número 23231.000613/2016-02 e a próxima reunião para finalização da minuta está marcada para o dia 13/01/2017, conforme a última ata de reunião do comitê. Como o texto ainda não está finalizado, entendemos

> não ser viável encaminhar cópia do PDTI incompleto. Após finalização do texto, encaminharemos cópia para conhecimento.

Consta no PETI 2012-2013 que ele "[...] foi elaborado visando manter-se alinhado ao Plano de Desenvolvimento Institucional 2009-2013 e à Resolução nº 51/2011 do Conselho Superior do IFRR.". Atualmente está em vigor o PDI 2014-2018 e a Resolução CONSUP nº 51/2011 vigorou até a aprovação do PDTI em 2012, conforme Art. 5º da própria resolução.

Em que pese a informação prestada pelo diretor de TI, no PDI vigente a dimensão tecnologia da informação possui quatro indicadores que não constam no PETI 2012-2013. Ademais, conforme o Acórdão nº 1233/2012-TCU-Plenário o PETI deve contemplar:

> [...] pelo menos: [...] objetivos, indicadores e metas para a TI organizacional, sendo que os objetivos devem estar explicitamente alinhados aos objetivos de negócio constantes do plano estratégico institucional;

Desse modo, mesmo que as metas estabelecidas no PETI estejam válidas, o documento deve ser atualizado, em virtude da existência dos indicadores e do disposto no acórdão do TCU.

Conforme consta na apresentação do PDTI 2012-2013, a revisão deve ser semestral " [...] para que seja sempre mantido seu alinhamento com o negócio institucional".

O Processo 23231.000613/2016-02, referente à elaboração do PDTI 2017/2018 foi aberto em 30/11/2016. Apesar do diretor de TI ter informado que a reunião para a finalização do PDTI ocorrerá em 13/1/2017, foi possível evidenciar, por meio da ata da 1ª Reunião Ordinária do Comitê Gestor de Tecnologia da Informação-CGTI que a reunião "[...] foi agendada para o dia 13/02/2017.".

Causa:

Falha no processo de planejamento de TI.

Consequência:

O PETI e o PDTI desatualizado pode gerar ressalvas nos relatórios de auditoria dos órgãos de controle.

Recomendação 1:

Atualizar o Planejamento Estratégico de Tecnologia da Informação – PETI, em conformidade com a jurisprudência do TCU.

Recomendação 2:

Concluir o processo de atualização do Plano Diretor da Tecnologia da Informação- PDTI.

4.2. Falta de revisão da Política de Segurança da Informação e Comunicações

A Política de Segurança da Informação e Comunicações-POSIC foi reformulada pela última vez em outubro de 2012 por meio da Resolução nº 105 do Conselho Superior. Assim, o documento está desatualizado, pois a revisão deveria ter ocorrido no período máximo de um ano.

O diretor de TI confirmou que a POSIC:

> [...] carece de atualização, que está planejada para o exercício de 2017. Lembrando que, segurança da informação não se restringe à esfera da TI, mas deve fazer parte do ambiente institucional como um todo, incluindo a TI. Vai desde o protocolo e trânsito de processos físicos até o controle das pessoas que entram e saem das dependências do IFRR. O fomento da Política de Segurança da Informação e do Comitê Gestor de Segurança da Informação tem sido encabeçada pela TI e se limitado ao seu escopo, no entanto não é isso que as boas práticas recomendam, indicando inclusive que a liderança do comitê e elaboração das políticas não fiquem a cargo do pessoal de TI, que supervisiona e mantem os sistemas, os bancos de dados, as pastas de documentos eletrônicos, as senhas etc.

Conforme estabelecido no Art. 165 do Regimento Geral do IFRR, a POSIC está a cargo do Comitê Gestor de Segurança da Informação e Comunicação - CGSIC, que possui competência definida para a Gestão da Segurança da Informação, conforme corrobora a Nota Técnica da Sefti TCU nº 07/2014. Acerca da coordenação do referido Comitê, dar-se-á na forma do §3º, Art. 3º da Portaria nº 391/2012, em consonância com os Art. 5º e 7º da IN nº 01/2008, do Gabinete de Segurança Institucional da Presidência da República.

No Guia de Orientações ao Gestor em Segurança da Informação consta que:

> Na elaboração de uma POSIC, a organização deve se preocupar não somente com aspectos técnicos, mas, também, considerar questões comportamentais e práticas do cotidiano. Afinal, as organizações enfrentam problemas de segurança que não estão necessariamente relacionados somente aos aspectos tecnológicos.
> [...]
> Todos os servidores, usuários, prestadores de serviço, contratados e colaboradores que habitualmente trabalham no órgão ou entidade [...] são responsáveis pela segurança da informação, pela segurança dos ativos e processos que estejam sob sua custódia e por todos os atos executados com suas identificações.

Ademais, conforme a Norma Complementar Nº 03/IN01/DSIC/GSIPR a POSIC deve ser elaborada por:

> [...] Grupo de Trabalho constituído por representantes dos diferentes setores do órgão ou entidade [...]como por exemplo: segurança patrimonial, tecnologia da informação, recursos humanos, jurídico, financeiro e planejamento.

Em razão disso, servidores da área de TI podem participar da elaboração da POSIC.

Com relação à divulgação, o presidente do CGSIC informou que a Política de Segurança da Informação do IFRR está disponível "[...]no link http://reitoria.ifrr.edu.br/dti/POSICIFRRNova.pdf [...]". No entanto, está previsto no item 24.2 da POSIC do IFRR que "Nos seis primeiros meses de vigência da política deverão

serão (sic) desenvolvidas ações para que os usuários tomem conhecimento da política e possam se adequar a ela.".

Com relação ao Plano de Continuidade de Negócios (PCN); Plano de Gerenciamento de Incidentes (PGI) e Plano de Recuperação de Negócios (PRN), o diretor informou que:

> Não possuímos Plano de Continuidade de Negócio (PCN), Plano de Gerenciamento de Incidentes (PGI) e Plano de Recuperação de Negócio (PRN). Não dispomos de pessoal qualificado para elaboração desses documentos, ou mesmo em quantidade suficiente para compor as posteriores equipes que executarão essas atividades, depois de planejadas, sem que haja comprometimento das atividades já exercidas pelos servidores atualmente lotados na Diretoria de TI. Tal expertise não é comum na formação dos profissionais de TI, sendo adquirida a posteriori através de qualificação pessoal corporativa. É importante mencionar que, os planos acima referidos devem estar relacionados ao escopo de "negócio" da TI, o qual é fomentar o negócio do IFRR naquilo que couber à TI. Nesse sentido, "incidente" está sendo compreendido como de TI e, apesar de não haver um PGI, há o registro e tratamento através do módulo de suporte do SUAP, desenhado para atender um PGI oriundo do IFRN. Já os Planos de Continuidade e de Recuperação de negócio do IFRR, vão além da TI e não podem ser determinados por esta Diretoria ou mesmo pelo CGTI. Os planos que se referirem apenas ao escopo de atuação da TI devem existir mas não são suficientes para garantir a continuidade e recuperação do negócio do IFRR. Deveriam, portanto, ser uma seção nos Planos de Continuidade e Recuperação de Negócio do IFRR e este um documento criado por comissão designada especialmente para esse fim.

Em que pese a informação prestada pelo diretor de TI, consta no item 16.2. da POSIC que o Plano de Continuidade de Negócio – PCN "[...] será definido pelo Comitê Gestor de Segurança da Informação com base na análise de riscos e terá a aprovação do Conselho Superior."

O item 15 da POSIC do IFRR estabelece as Diretrizes para Gestão de Risco e Tratamento de Incidentes. No item 10.2 da Política há informações sobre recuperação de ativos:

> A documentação dos ativos deverá conter informações que permitam sua recuperação após um desastre, incluído o tipo de ativo, formato, localização, informações sobre cópias de segurança e informações sobre a importância do ativo para a instituição.

Consta no Relatório de Auditoria Anual de Contas nº 201108748, emitido pela equipe de auditores da CGU-RR, que:

> " A Política de Segurança da Informação deverá conter, no mínimo, os seguintes requisitos:
> [...]
> f) referências a documentações que possam apoiar a política, como:
> [...]
> - Programa de Gestão de Continuidade de Negócios, contendo Plano de Gerenciamento de Incidentes (PGI), Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Negócios (PRN);"

O presidente do CGSIC informou que os documentos que apoiam a POSIC do IFRR são: o Decreto nº 3.505 2000; a IN GSI/PR Nº 1/2008; a Lei nº 12.527/2011; o Decreto nº 7.724/2012; a ABNT NBR ISO/IEC 27001:2006 e a ABNT NBR ISO/IEC 27002:2005.

O presidente do comitê também corroborou a ausência dos planos do Programa de Gestão de Continuidade de Negócios:

> O Comitê [...] não realizou nenhuma ação quanto ao Plano de Continuidade de Negócio (PCN), Plano de Gerenciamento de Incidentes (PGI) ou Plano de Recuperação de Negócio (PRN) [...]Outro problema para elaboração de tais documentos é a qualificação do pessoal que compõe o comitê, especialmente quanto a aplicação das normas ISO 27001:2013, 27002:2013 e 27005:2011.

Causa:

Falha no controle do processo de segurança da informação do IFRR.

Consequência:

Risco potencial de comprometer os objetivos organizacionais, em virtude da ausência de ações de segurança da informação.

Recomendação 3:

Apresentar cronograma para implantação do Programa de Gestão de Continuidade de Negócios, contendo Plano de Gerenciamento de Incidentes (PGI), Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Negócios (PRN).

Recomendação 4:

Revisar a Política de Segurança da Informação e Comunicações-POSIC do IFRR, com o apoio do Plano de Gerenciamento de Incidentes (PGI), do Plano de Continuidade de Negócios (PCN) e do Plano de Recuperação de Negócios (PRN).

4.3. O Comitê Gestor de Tecnologia da Informação-CGTI e o Comitê Gestor de Segurança da Informação e Comunicação-CGSIC não estão exercendo as competências formalmente atribuídas

O Comitê Gestor de Tecnologia da Informação-CGTI, com atribuições definidas no Regimento Geral do IFRR, possui como função de alinhamento e regulação das ações de TI ao planejamento institucional, de forma a apoiar ações, projetos, oportunidades de melhoria em tecnologia da informação. Acerca do seu funcionamento em 2016, o Diretor de Tecnologia da Informação apresentou a Ata de apenas uma reunião que ocorreu em 09 de dezembro de 2016, com próxima reunião para 13/02/2017.

Acerca da manifestação do envio de cópia do Regimento Interno do CGTI, o Diretor de TI apresentou uma minuta, ainda não aprovada pelo Conselho Superior. No entanto, a Portaria nº 512/2011, em seu art. 4º informa que o "Comitê deverá elaborar proposta de regimento interno no prazo de 60 dias contados a partir da designação de seus membros", e esta designação ocorreu por meio do Portaria nº 1936 de 2013.

De acordo com a Portaria nº 0391/2012, o Comitê Gestor de Segurança da Informação e Comunicação – CGSIC possui entre suas atribuições "promover, gerir e rever periodicamente a Política de Segurança da Informação e Comunicação – POSIC do IFRR (...); propor recursos necessários às ações de Segurança da Informação e Comunicação".

Acerca do funcionamento do CGSIC, foi solicitado do Diretor de Tecnologia da Informação o envio de cópia de atas das reuniões realizadas em 2016, no entanto, foram encaminhadas apenas duas atas de reuniões realizadas em 2012. Conforme informado pelo presidente do comitê, no exercício de 2016 não ocorreu reunião do CGSIC. O presidente informou ainda que:

> [...] Os atuais integrantes do Comitê foram designados pela portaria 1010/GR, de 22 de junho de 2015, tendo um titular e um suplente da DTI, da DGP e de cada Pró-Reitoria do IFRR. Não há representantes dos campi integrando o Comitê e grande parte de seus membros já não pertencem aos setores aos quais representavam. Desta forma há a necessidade de designar novamente os membros do CGSIC, incluindo representantes de cada campi. [...]

O Art.3º da Portaria nº 391/2012, estabelece que os integrantes do CGSIC são representantes

> [...] dos seguintes setores [...]: Diretoria de Tecnologia da Informação; Diretoria de Gestão de Pessoas; Pró-Reitorias de Ensino, Pós-Graduação e Pesquisa e Extensão; Pró-Reitorias de Administração e Planejamento e Desenvolvimento Institucional.

Conforme Art. 6º da Portaria 0391/2012, "as reuniões do CGSI serão realizadas ordinariamente a cada dois meses e, extraordinariamente, quando necessário, por convocação do Coordenador ou solicitação de pelo menos um terço de seus membros". Nesse sentido, observa-se que o Comitê não está funcionando conforme previsto.

Ademais, observa-se que no Relatório de Auditoria Anual de Contas nº 201108748, o setor auditado foi instado a se manifestar acerca da ausência de área específica, como um comitê gestor da segurança da informação, responsável pela implementação da política de segurança da informação na Unidade. Percebe-se que foram criados o CGTI e o CGSIC, porém não estão em adequado funcionamento. No mesmo relatório, o setor auditado informou que "a responsabilidade da implantação está dividida entre a DTI/CTIs", o que condiz com a Ata da 1ª reunião do CGSIC realizada em 2012, ao ficar esclarecido que "as políticas criadas pelo comitê serão implementadas pela DTI e CTI nos campi."

De acordo com o Acórdão TCU 2.471/2008-Plenário " um comitê estratégico de TI tem como funções básicas assegurar que a governança de TI seja adequadamente tratada, aconselhar a direção estratégica de TI e revisar os grandes investimentos (...)". Acerca do comitê de direção de TI, este "tem como atribuições típicas priorizar os investimentos de TI em alinhamento com a estratégia e as prioridades do negócio do ente (...)". Conforme o referido acórdão, as auditorias realizadas pelo Tribunal na área de TI tem identificado que em parte dos auditados o comitê não estava instituído e em outra parte estava instituído, mas não era atuante. Nesse sentido, percebe-se a importância da atuação efetiva do CGTI e do CGSIC para os objetivos estratégicos institucionais.

Causa:

Falta de reuniões periódicas do CGTI e do CGSIC.

Consequência:

Ausência de reuniões do CGTI e do CGSIC pode gerar ressalvas nos relatórios de auditoria dos órgãos de controle.

Recomendação 5:

Enviar ao Conselho Superior do IFRR a minuta do Regimento Interno do CGTI para apreciação e aprovação do colegiado.

Recomendação 6:

Designar servidores para integrarem o Comitê Gestor de Segurança da Informação e Comunicação-CGSIC.

Recomendação 7:

Criar o Regimento Interno do Comitê Gestor de Segurança da Informação e Comunicação-CGSIC.

Recomendação 8:

Oferecer as condições necessárias para que o Comitê Gestor de Tecnologia da Informação-CGTI e o Comitê Gestor de Segurança da Informação e Comunicação-CGSIC realizem reuniões periódicas.

5. Conclusão

Por meio da ação de controle foi possível evidenciar a ausência de atualização do Planejamento Estratégico de Tecnologia da Informação – PETI e do Plano Diretor da Tecnologia da Informação- PDTI, bem como de revisão da Política de Segurança da Informação e Comunicações – POSIC.

Também foi possível evidenciar a falta de reuniões periódicas do CGTI e do CGSIC e de divulgação das ações de segurança da informação e comunicação aos usuários.

Ademais, foi constatada a inexistência dos planos do Programa de Gestão de Continuidade de Negócios, o que pode ameaçar a segurança da informação e comunicação e impactar negativamente as ações e os objetivos organizacionais.

Não foi enviada manifestação formal da Diretoria de Tecnologia da Informação referente às constatações do relatório preliminar de auditoria nº 001/2017. No entanto, o Diretor de TI compareceu à reunião de busca conjunta de soluções, realizada no dia 16 de fevereiro de 2017.

Boa Vista-RR, 22 de fevereiro de 2017

ADRIENE SILVA DO NASCIMENTO
Auditora Interna/Portaria 724/2010

FABRICIA MATTE CAYE
Economista

MICHELLE DE OLIVEIRA BARBOSA VERAS
Economista