INSTITUTO FEDERAL
Rondônia

MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Rondônia

RELATÓRIO DE AUDITORIA

RELATÓRIO Nº : 003/2018
TIPO DE AUDITORIA : Acompanhamento
UNIDADE AUDITADA : Diretoria de Tecnologia da Informação / IFRO
CIDADE : Porto Velho/RO

Magnífico Reitor,

Em cumprimento ao Plano Anual de Atividades de Auditoria Interna – PAINT 2018, referente à Ação 8.1 Macroprocesso de Tecnologia da Informação – Governança/Segurança da Informação, apresenta-se os resultados dos exames realizados.

O início dos trabalhos se deu com o MEMORANDO nº 36/2018/REIT - AUDINT, de 22/08/2018, informando ao gestor sobre a auditoria a ser realizada, em estrita observância às normas de auditoria aplicáveis ao Serviço Público Federal. Menciona-se como fato positivo que nenhuma restrição foi imposta aos trabalhos da Auditoria Interna.

I – ESCOPO DO TRABALHO

A ação de auditoria buscou avaliar os mecanismos administrativos de controle interno da área de Governança de Tecnologia da Informação, sendo, para tanto, utilizadas as indagações do Questionário de Governança em Tecnologia da Informação (i-GovTI) a fim de coletar informações sobre a situação de governança de TI no IFRO, sendo retirados os itens relacionados a Contratos de Tecnologia da Informação, pois segundo entendimento interno trata-se de auditoria mais específica, a respeito de processo de contratação.

Para o desenvolvimento da ação de auditoria junto à área de Tecnologia da Informação, foi utilizado como ferramenta o questionário aplicado pelo Tribunal de Contas da União (ciclo 2016) – para avaliação da governança da área de TI. Entretanto, é importante esclarecer que a área auditada teve a oportunidade de responder novamente o mesmo questionário, para fins de atualização das informações fornecidas. O questionário foi dividido em duas Solicitações de Auditoria, tendo em vista que inicialmente o questionário seria aplicado parcialmente. Porém, verificou-se a necessidade de complementar o procedimento de recolhimento de informações. Dessa forma, procedeu-se em aplicar a outra parte do questionário, sendo retirados apenas os itens relativos à contratação de TI, por entendermos que se tratava de assunto mais abrangente e que necessitaria de auditoria específica.

II – OBJETIVOS

Os trabalhos desta auditoria tiveram como objetivo geral avaliar a adequação dos mecanismos de controle na área de Tecnologia da Informação e como objetivos específicos:

a) verificar se a política de governança está implementada;

b) verificar se as metas propostas no PDTI e no PDI estão alinhadas entre si e se foram alcançadas;

c) verificar a estrutura de Segurança das Informações;

d) verificar se a instituição segue boas práticas no gerenciamento de projetos e serviços de Segurança da Informação.

III – TÉCNICA E PROCEDIMENTOS DA AUDITORIA

Foi necessário adotar os seguintes procedimentos durante a realização dos trabalhos:

a) Exame dos registros: análise dos métodos e sistemas utilizados na execução dos procedimentos internos administrativos.

b) Indagação Escrita ou Oral: emissão de S.A ao setor auditado solicitando informações para averiguar a existência de mecanismos de controle interno e solicitar documentos comprobatórios, sendo ainda realizadas pequenas reuniões entre os setores envolvidos.

c) Análise documental: análise dos documentos apresentados pelo setor, quando solicitados por meio de S.A.

d) Consulta à página institucional da Tecnologia Informação: conferência dos documentos publicados.

IV – LEGISLAÇÃO APLICADA

As legislações aplicáveis ao objeto auditado foram:

1. **Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008.** Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

2. **Instrução Normativa GSI/PR nº 2, de 05 de fevereiro de 2013.** Dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.

3. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências.

4. **Acórdão TCU nº 1.603/2008 – Plenário;**

5. **Acórdão TCU nº 2.308/2010 – Plenário;**

6. **Guia de comitê de TI do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP);**

7. **Relatório - Levantamento de Governança de TI 2016 TCU – iGovTI 2016.** Avalia a situação de governança de TI na Administração Pública Federal, através de questionários que abordam práticas de governança e de gestão de TI previstas em leis, regulamentos, normas técnicas e modelos internacionais de boas práticas.

8. **Resolução nº 55/CONSUP/IFRO, de 11 de dezembro de 2014.** Dispõe sobre o Plano de Desenvolvimento Institucional do IFRO 2014-2018.

9. **Resolução nº 01/CONSUP/IFRO, de 5 de março de 2015.** Dispõe sobre o Plano Estratégico de Tecnologia da Informação – PETI do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia.

10. **Resolução nº 11/CONSUP/IFRO, de 15 de maio de 2015.** Dispõe sobre o Plano Diretor de Tecnologia da Informação 2014-2016 do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO.

11. **Resolução nº 03/CONSUP/IFRO, de 12 de janeiro de 2017.** Dispõe sobre o Plano Diretor de Tecnologia da Informação 2016-2018 do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO.

V – ANÁLISE GERAL DO QUESTIONÁRIO APLICADO

Com base nas respostas fornecidas pela área auditada no questionário aplicado, a equipe de auditoria iniciou o procedimento de análise, selecionando perguntas às quais discordava do posicionamento, ou mesmo, quando percebia a necessidade de complementar as informações.

Neste sentido, e com base nos questionamentos e informações disponibilizadas, foi possível a validação ou não das respostas informadas.

Devido a grande extensão do questionário, bem como o quantitativo de pessoal em atuação na ação, não foi possível proceder na análise de todos os itens, entretanto, foram selecionadas questões consideradas de maior relevância e que objetivam o aprimoramento da atuação da área de Tecnologia da Informação.

Item do Questionário iGovTI	RESPOSTA DA TI	ANÁLISE
1.1.a	Iniciou plano para adotar	ACEITA
1.1.b	Adota parcialmente	ACEITA*
1.1.c	Adota integralmente	ACEITA
1.1.d	Adota integralmente	ACEITA*
1.1.e	Adota parcialmente	NÃO ACEITA
1.1.f	Adota integralmente	ACEITA
1.2.a	Não adota	NÃO ACEITA
1.2.b	Adota integralmente	ACEITA*
1.2.c	Iniciou plano para adotar	ACEITA
1.2.d	Adota integralmente	NÃO ACEITA
1.3.a	Adota parcialmente	ACEITA
1.3.b	Adota parcialmente	ACEITA
1.3.c	Iniciou plano para adotar	NÃO ACEITA
1.3.d	Adota parcialmente	ACEITA*
1.3.e	Iniciou plano para adotar	ACEITA
1.4.a	Não adota	ACEITA
1.4.b	Não adota	ACEITA
1.4.c	Não adota	ACEITA
1.4.d	Não adota	ACEITA
1.5.a	Não adota	ACEITA

1.5.b	Não adota	ACEITA
1.5.c	Não adota	ACEITA
1.5.d	Não adota	ACEITA
1.5.e	Não adota	ACEITA
1.6.a	Não adota	NÃO ACEITA
1.6.b	Não adota	ACEITA
1.6.c	Não adota	ACEITA
1.6.d	Não adota	ACEITA
1.6.e	Não adota	ACEITA
2.1.a	Adota integralmente	ACEITA
2.1.b	Adota integralmente	ACEITA
2.1.c	Adota integralmente	ACEITA
2.1.d	Adota integralmente	ACEITA
2.1.e	Adota integralmente	ACEITA*
2.1.f	Adota integralmente	ACEITA
2.1.g	Adota integralmente	ACEITA
2.1.h	Adota integralmente	ACEITA
2.1.i	Adota integralmente	ACEITA
2.2.j	Adota integralmente	ACEITA
2.2.a	Adota integralmente	ACEITA
2.2.b	Adota integralmente	ACEITA*
2.2.c	Adota integralmente	ACEITA
2.2.d	Adota integralmente	ACEITA
2.2.e	Adota integralmente	ACEITA
2.2.f	Adota parcialmente	ACEITA*
2.2.g	Adota parcialmente	ACEITA
2.2.h	Adota integralmente	ACEITA
2.2.i	Adota integralmente	ACEITA*
2.2.j	Não adota	ACEITA
3.1.a	Iniciou plano para adotar	ACEITA
3.1.b	Adota parcialmente	ACEITA
3.1.c	Adota integralmente	NÃO ACEITA
3.1.d	Não adota	ACEITA
3.2.a	Adota integralmente	ACEITA
3.2.b	Iniciou plano para adotar	ACEITA
3.2.c	Iniciou plano para adotar	ACEITA
3.2.d	Iniciou plano para adotar	ACEITA
3.2.e	Iniciou plano para adotar	ACEITA
3.2.f	Iniciou plano para adotar	ACEITA
3.1.g	Iniciou plano para adotar	ACEITA
3.2.h	Iniciou plano para adotar	ACEITA
3.2.i	Iniciou plano para adotar	ACEITA
3.3.a	Iniciou plano para adotar	ACEITA
3.3.b	Adota integralmente	ACEITA
4.1.a	Adota parcialmente	ACEITA
4.1.b	Adota integralmente	ACEITA
4.1.c	Iniciou plano para adotar	NÃO ACEITA
4.1.d	Não adota	ACEITA
4.1.e	Não adota	ACEITA
4.1.f	Iniciou plano para adotar	ACEITA
4.1.g	Iniciou plano para adotar	ACEITA
4.1.h	Iniciou plano para adotar	ACEITA
4.2.a	Não adota	ACEITA
4.2.b	Não adota	ACEITA
4.2.c	Não adota	ACEITA
4.3.a	38	ACEITA
4.3.b	44	ACEITA
4.3.c	34	ACEITA
4.3.d	34	ACEITA
4.3.e	5	ACEITA
4.3.f	0	ACEITA
4.3.g	0	ACEITA
4.3.h	0	ACEITA
4.3.i	0	ACEITA
4.3.j	0	ACEITA

4.3.k	0	ACEITA
4.3.l	0	ACEITA
4.3.m	-	-
5.1.a	Adota parcialmente	ACEITA
5.1.b	Não adota	ACEITA
5.1.c	Não adota	ACEITA
5.1.d	Não adota	ACEITA
5.1.e	Não adota	ACEITA
5.1.f	Não adota	ACEITA
5.1.g	Não adota	ACEITA
5.1.h	Não adota	ACEITA
5.1.i	Não adota	ACEITA
5.1.j	Não adota	ACEITA
5.1.k	Não adota	ACEITA
5.1.l	Não adota	ACEITA
5.1.m	Não adota	ACEITA
5.1.n	Não adota	ACEITA
5.2.a	Adota integralmente	NÃO ACEITA
5.2.b	Não adota	ACEITA
5.2.c	Não adota	ACEITA
5.2.d	Não adota	ACEITA
5.2.e	Não adota	ACEITA
5.2.f	Não adota	ACEITA
5.3.a	Não adota	ACEITA
5.3.b	Não adota	ACEITA
5.3.c	Não adota	ACEITA
5.3.d	Não adota	ACEITA
5.3.e	Não adota	ACEITA
5.4.a	Adota parcialmente	NÃO ACEITA
5.4.b	Iniciou plano para adotar	ACEITA
5.4.c	Iniciou plano para adotar	ACEITA
5.4.d	Iniciou plano para adotar	ACEITA
5.4.e	Adota parcialmente	NÃO ACEITA
5.4.f	Iniciou plano para adotar	ACEITA
5.4.g	Não adota	ACEITA
5.4.h	Não adota	ACEITA
5.4.i	Não adota	ACEITA
5.4.j	Não adota	ACEITA
5.4.k	Não adota	ACEITA
5.4.l	Não adota	ACEITA
5.4.m	Adota parcialmente	ACEITA
5.4.n	Não adota	ACEITA
5.4.o	Adota parcialmente	ACEITA
5.4.p	Iniciou plano para adotar	ACEITA
5.4.q	Adota parcialmente	ACEITA
5.4.r	Não adota	ACEITA
5.4.s	Adota parcialmente	ACEITA
5.4.t	Não adota	ACEITA
5.4.u	Adota integralmente	ACEITA
5.5.a	Não adota	ACEITA*
5.5.b	Não adota	ACEITA
5.5.c	Não adota	ACEITA
5.5.d	Adota parcialmente	ACEITA
5.5.e	Não adota	ACEITA
5.6.a	Adota integralmente	ACEITA
5.6.b	Adota integralmente	ACEITA
5.6.c	Adota integralmente	ACEITA
5.6.d	Não adota	ACEITA
5.6.e	Não adota	ACEITA
5.6.f	Não adota	ACEITA

Tabela 1 – Questionário aplicado junto à área de TI – SA 8.1.1 e 8.1.3
Fonte: Audint/IFRO

Legenda:
(Aceita) Indica que a informação fornecida foi aceita pela equipe de auditoria.
(Não Aceita) Indica que as informações fornecidas não foram suficientes para comprovar o item respondido.

(*) Indica que a equipe de auditoria incluiu uma observação sobre a informação fornecida.

- **Questão 1.1.b:** a organização dispõe de um comitê de direção estratégica formalmente instituído, que auxilia nas decisões relativas às diretrizes, estratégias, políticas e no acompanhamento da gestão institucional.

Resposta informada no questionário: adota parcialmente.

Solicitação de comprovação: foi incluída na resposta da SA 8.1.3.

Esclarecimentos da área auditada: Memorando nº 62/2018/REIT – DGTI.

Análise da Auditoria: por meio dos referenciais indicados na resposta, a equipe de auditoria fez a leitura do quadro referente ao Processo de Gestão da Estratégia, pág. 59 do Plano da Estratégia do IFRO, publicado no link: https://portal.ifro.edu.br/planejamentoestrategico-nav. É importante salientar que, mediante as comprovações apresentadas, as atribuições outorgadas ao Colégio de Dirigentes do IFRO (CODIR) necessitam ser atualizadas, pois não estão previstas na Resolução nº 18/2016/CONSUP/IFRO, que dispõe sobre o Regimento Interno do colegiado. Todavia, há de se considerar que o processo de planejamento estratégico do IFRO ocorreu em 2017.

- **Questão 1.1.d:** a organização dispõe de um código de ética, formalmente instituído, bem como divulga e monitora o seu cumprimento.

Resposta informada no questionário: adota integralmente.

Solicitação de comprovação: foi incluída na resposta da SA 8.1.3.

Esclarecimentos da área auditada: Memorando nº 62/2018/REIT – DGTI.

Análise da Auditoria: o documento apresentado como comprovação não se trata de um código de ética institucional, mas sim do Regimento Interno da Comissão de Ética do IFRO – Resolução nº 12/2018/CONSUP/IFRO. Apesar disso, durante a realização destes trabalhos, o Código de Ética do IFRO foi aprovado conforme a Resolução nº 81/2018/CONSUP/IFRO.

- **Questão 1.1.e:** a organização dispõe de uma política corporativa de gestão de riscos formalmente instituída como norma de cumprimento obrigatório.

Resposta informada no questionário: adota parcialmente.

Solicitação de comprovação: foi incluída na resposta da SA 8.1.3.

Esclarecimentos da área auditada: "Existe a política, mas a execução ainda não foi iniciada. http://bit.do/eBrZ5"

Análise da Auditoria: a justificativa apresentada não comprova que a Política de Gestão de Riscos iniciou sua execução no âmbito institucional. Entretanto, por a equipe de auditoria pertencer a instituição, tem-se conhecimento que a Política de Gestão de Riscos foi aprovada conforme Resolução 4/2017, sendo importante salientar que a mesma não está sendo executada em sua totalidade. Neste sentido, a equipe de auditoria interna não aceita a informação fornecida e sugere que o item seja respondido como "*Adota Integralmente*".

- **Questão 1.2.a:** o Instituto define e comunica formalmente papéis e responsabilidades mais relevantes para a governança e a gestão de TI.

Resposta informada no questionário: não adota.

Solicitação de comprovação: não foram solicitadas comprovações.

Esclarecimentos da área auditada:***

Análise da Auditoria: para a análise do presente questionamento não foi necessária a emissão de questionamentos, tendo em vista que a Auditoria Interna tem ciência que o IFRO dispõe de Regimento Geral, aprovado pela Resolução nº 65/2015/CONSUP/IFRO, onde são definidos os principais papéis da instituição e atribuídas as suas responsabilidades numa visão sistêmica de gestão, conforme a estrutura organizacional. Nesse sentido, a equipe de auditoria interna não aceita a informação fornecida e sugere que o item seja respondido como "*Adota integralmente*".

- **Questão 1.2.b:** o Instituto dispõe de um comitê de TI formalmente instituído, composto por representantes de áreas relevantes da organização.

Resposta informada no questionário: iniciou plano para adotar.

Solicitação de comprovação: apresentar convocações, atas e demais documentos que se fizerem necessários a fim de comprovar que o Plano Estratégico e o Plano Diretor de TI foram aprovados pelo Comitê Gestor de TI. Informar se há documentos mais atuais para a designação do Comitê Gestor de TI. Se houver, apresentá-los.

Esclarecimentos da área auditada: Memorando nº 62/2018/REIT – DGTI.

Análise da Auditoria: o presente questionamento se originou a partir do documento de comprovação apresentado, pois em análise à Resolução nº 27/2011/CONSUP/IFRO, que dispõe sobre o Regimento Interno do Comitê Gestor de TI, foi verificado que o presente documento se trata de uma resolução desatualizada e contendo nomes de servidores que não ocupam mais cargos de gestão no âmbito do IFRO – Portaria nº 642/2011/GR/IFRO.

Verificou-se também que após as solicitações da equipe de auditoria, a área auditada percebeu a iminente necessidade de atualização das suas normativas e tratou de iniciar discussão no âmbito da instituição, apresentando como documento comprobatório a Pauta da 47ª Reunião do Colégio dos Dirigentes. Nesse sentido, a equipe de auditoria entende que as informações fornecidas podem ser aceitas.

- **Questão 1.2.d:** o Instituto prioriza as ações de TI com apoio do comitê de TI (ou colegiado equivalente), que atua como instância consultiva da alta administração.

Resposta informada no questionário: adota integralmente.

Solicitação de comprovação: apresentar documentos, tais como convocações, atas ou portarias que comprovem que o instituto prioriza as ações de TI, com o apoio do Comitê Gestor de TI.

Esclarecimentos da área auditada: Memorando nº 62/2018/REIT – DGTI.

Análise da Auditoria: em análise à Resolução nº 27/2011/CONSUP/IFRO, verificou-se por meio da sua composição de membros, que o Comitê Gestor de TI deveria atuar em conjunto com a realização do Colégio de Dirigentes da instituição.

Entretanto, as documentações apresentadas não comprovam que as discussões sobre a Tecnologia da Informação ocorriam integralmente, o que pode ser atestado tendo em vista a ausência de discussão e acompanhamento de temas, como, por exemplo, o Plano Estratégico de TI. Desta forma, a equipe de auditoria não vê a possibilidade de validar a informação fornecida e sugere que o item seja respondido como "*Adota parcialmente*".

- **Questão 1.3.c:** a organização define formalmente diretrizes para a avaliação de bens e serviços de TI.

Resposta informada no questionário: iniciou plano para adotar.

Solicitação de comprovação: informar as normativas utilizadas para a contratação de bens e serviços da TI e apresentar comprovantes das tratativas já realizadas que objetivem formalizar diretrizes para essa ação.

Esclarecimentos da área auditada: Memorando nº 62/2018/REIT – DGTI.

Analise da Auditoria: após a análise das informações fornecidas em resposta ao presente questionamento, não houve comprovação que o IFRO define formalmente avaliação dos bens e serviços de TI, apesar de a área de administração do IFRO realizar procedimentos internos de acompanhamento dos contratos de Tecnologia da Informação. Desta forma, a equipe de auditoria não vê a possibilidade de validar a informação fornecida e sugere que o item seja respondido como "*Não adota*".

- **Questão 1.3.d:** o Instituto define formalmente diretrizes para avaliação do desempenho dos serviços de TI.

Resposta informada no questionário: adota parcialmente.

Solicitação de comprovação: apresentar comprovações das tratativas já realizadas para comunicar sobre os resultados da gestão e uso dos recursos de Tecnologia da Informação.

Esclarecimentos da área auditada: Memorando nº 62/2018/REIT – DGTI.

Analise da Auditoria: tendo em vista que a informação foi prestada de forma incompleta, a equipe de auditoria buscou documentos da Reunião dos índices:

- 15.2 – Taxa de unidades conectadas à INFOVIA
- 15.3 – Taxa de disponibilidade de serviço
- 15.4 – Índice da infraestrutura tecnológica
- 15.5 – Taxa de implementação das ações do PDTI

Com base nos documentos verificados, atestou-se que a área auditada dispõe de indicadores e está inserida como membro da Reunião da Avaliação da Estratégia, entretanto, entende-se que a área de Tecnologia da Informação realiza o acompanhamento de seu planejamento, metas e ações, e não necessariamente dos seus serviços.

- **Questão 1.6.a:** o Instituto define formalmente diretrizes para avaliação da governança e da gestão de TI.

Resposta informada no questionário: não adota.

Solicitação de comprovação: não foram solicitadas comprovações.

Esclarecimentos da área auditada: *

Analise da Auditoria: para análise do presente questionamento, não foi necessário emitir questionamentos, tendo em vista que a Auditoria Interna, durante a realização da ação de auditoria, verificou parcialmente a definição de diretrizes para a avaliação da gestão de TI no PDTI da instituição. Cita-se como exemplo a "Taxa de implementação das ações do PDTI", que é devidamente acompanhada pela Reunião de Avaliação da Estratégia da instituição. Neste sentido, a equipe de auditoria interna não valida a informação fornecida e sugere que o item seja respondido como "*Adota parcialmente*".

- **Questão 1.6.e:** o Instituto realiza avaliação periódica de contratos de TI.

Resposta informada no questionário: não adota.

Esclarecimentos da área auditada: foram solicitados esclarecimentos à área de administração, conforme SA nº 8.1.4.

Análise da Auditoria: entretanto, utilizando-se do conhecimento geral sobre atos da instituição e conforme consulta formalizada à área de administração da instituição, foi constatado que apesar de não estarem devidamente formalizadas, são realizadas consultas aos fiscais de contratos de Tecnologia da Informação e Comunicação (TIC) quando da ocorrência de eventos de alteração contratual ou prorrogação de prazo (Solicitação de Auditoria nº 8.1.4/2018).

- **Questão 2.1.e:** a organização possui plano estratégico vigente, formalmente instituído pelo seu dirigente máximo.

Resposta informada no questionário: adota integralmente.

Solicitação de comprovação: foi incluída na resposta da SA 8.1.3.

Esclarecimentos da área auditada: *

Análise da Auditoria: apesar de a área responsável apontar o Plano de Desenvolvimento Institucional (PDI) como plano estratégico institucional visando comprovar a questão, a equipe de auditoria entende que o documento requisitado pelo item se trata do Plano Estratégico do IFRO 2018-2022, que pode ser acessado conforme link https://portal.ifro.edu.br/planejamentoestrategico-nav.

- **Questão 2.2.b:** o processo de planejamento de TI prevê a participação das áreas mais relevantes da organização.

Resposta informada no questionário: adota integralmente.

Solicitação de comprovação: apresentar documentos que comprovem a participação das áreas mais relevantes no processo de planejamento da TI (considerar portarias de designação, atas de reuniões ou demais comprovantes pertinentes).

Esclarecimentos da área auditada: Memorando nº 62/2018/REIT – DGTI.

Análise da Auditoria: apesar de o processo de planejamento de TI contar com a participação das áreas estratégicas da instituição representadas pelos pró-reitores e diretores das áreas sistêmicas, conforme previsto na Resolução nº 27/2011/CONSUP/IFRO, as portarias de designação da comissão responsável pela elaboração do documento (pág. 3 do PDTI 2016-2018 - Resolução nº 3/2017/CONSUP/IFRO), demonstra que apenas servidores da Tecnologia da Informação participam da fase de elaboração do planejamento, não sendo possível atestar que áreas fins da instituição participam do processo de levantamento de demandas institucionais. Neste sentido, a equipe de auditoria interna não valida a informação fornecida e sugere que o item seja respondido como "*Adota parcialmente*".

- **Questão 2.2.f:** o plano de TI vigente contempla objetivos, indicadores e metas para a TI, com os objetivos explicitamente alinhados aos objetivos de negócio constantes do plano estratégico institucional.

Resposta informada no questionário: adota parcialmente.

Solicitação de comprovação: não foram solicitadas comprovações.

Esclarecimentos da área auditada: *

Análise da Auditoria: cumpre esclarecer que o IFRO dispõe de novo Plano de Desenvolvimento Institucional com vigência para o período 2018-2022, sendo que o PDTI está em processo de atualização. Desta forma, não foi possível atestar o alinhamento institucional entre ambos. Entretanto, durante o período de vigência do antigo documento não houve desalinhamento.

- **Questão 2.2.i:** o plano de TI vigente vincula as ações (atividades e projetos) a indicadores e metas do negócio.

Resposta informada no questionário: adota integralmente.

Solicitação de comprovação: não foram solicitadas comprovações.

Esclarecimentos da área auditada: *

Análise da Auditoria: cumpre esclarecer que o IFRO dispõe de novo Plano de Desenvolvimento Institucional com vigência para o período 2018-2022, sendo que o PDTI está em processo de atualização. Desta forma, optou-se por não avaliar este item.

- **Questão 3.1.a:** a organização identifica e mapeia os principais processos de negócio.

Resposta informada no questionário: iniciou plano para adotar.

Solicitação de comprovação: foi incluída na resposta da SA 8.1.3.

Esclarecimentos da área auditada: ***

Análise da Auditoria: por meio da resposta apresentada pela área auditada, a equipe de auditoria fez uma rápida busca no site institucional do IFRO, e em consulta ao link https://portal.ifro.edu.br/component/phocadownload/category/1201-modernizacao-da-gestao-implantacao-do-escritorio-de-projetos-processos-e-riscos?download=5829:pp-modernizacao-da-gestao-implantacao-do-escritorio-de-gerenciamento-de-projetos-processos-e-riscos atestou a existência de Projeto Estratégico no PDI, denominado "Modernização da gestão: implantação do escritório de projetos e processo".

Esclarece-se, entretanto, que as respostas encaminhadas em atendimento às solicitações de auditoria, tanto externas quanto às internas, devem ser fornecidas de maneira completa, uma vez que a auditoria interna não possui atribuições relativas a atestar o cumprimento ou não de um normativo. Neste sentido, orienta-se que ações de auditoria devem ser respondidas com o maior zelo possível, disponibilizando todas as documentações necessárias.

- **Questão 3.1.c:** há catálogo publicado com informações atualizadas de cada um dos sistemas informatizados.

Resposta informada no questionário: adota integralmente.

Solicitação de comprovação: foi incluída na resposta da SA 8.1.3.

Esclarecimentos da área auditada: ***

Análise da Auditoria: para fins de comprovação, a área auditada disponibilizou o link: http://ifro.edu.br/catalogoservicos/, onde foi possível verificar, de maneira fácil e rápida, o acesso aos sistemas prestados pelo IFRO, podendo ser avaliado de maneira positiva. Sugere-se, entretanto, que o catálogo de serviço contenha informações tais como: conceitos dos sistemas, principais termos, condições e controles definidos em relação aos serviços prestados pela instituição, e que defina um período para revisar e atualizar as informações dispostas. É válido salientar, entretanto, a ausência do serviço de Seleção do IFRO. Neste sentido, a equipe de auditoria interna não aceita a informação fornecida e sugere que o item seja respondido como "*Iniciou plano para adotar*".

- **Questão 4.1.c:** a organização elabora, periodicamente, plano de capacitação, para suprir as necessidades de desenvolvimento de competências de TI.

Resposta informada no questionário: iniciou plano para adotar.

Solicitação de comprovação: foi incluída na resposta da SA 8.1.3.

Esclarecimentos da área auditada: ***

Análise da Auditoria: em complementação à sua resposta, a área auditada informou que não existe um plano de capacitação específico para a TI, mas sim, um plano de capacitação a nível institucional. Neste sentido, a equipe de auditoria interna não aceita a informação fornecida e sugere que o item seja respondido como "*Não adota*".

- **Questão 5.2.a:** a organização mantém um catálogo publicado e atualizado dos serviços de TI oferecidos às áreas clientes, incluindo os níveis de serviço definidos.

Resposta informada no questionário: adota integralmente.

Solicitação de comprovação: foi incluída na resposta da SA 8.1.3.

Esclarecimentos da área auditada: ***

Análise da Auditoria: no item **5.2.a** a área auditada informa que "*Adota integralmente*" quando questionada se o IFRO mantém um catálogo publicado e atualizado dos serviços de TI oferecidos, contendo ainda os níveis dos serviços definidos. Entretanto, logo abaixo, no item 5.2.b, é informado que o IFRO não dispõe de níveis de serviços formalmente definidos entre as áreas de TI e as áreas clientes.

Neste sentido, a equipe de auditoria interna não aceita a informação fornecida e sugere que o item seja respondido como "*Adota parcialmente*".

- **Questão 5.4.a:** a organização dispõe de uma política de segurança da informação formalmente instituída como norma de cumprimento obrigatório.

Resposta informada no questionário: adota parcialmente.

Solicitação de comprovação: apresentar minuta da Política de Segurança da Informação.

Esclarecimentos da área auditada: Memorando nº 62/2018/REIT – DGTI.

Análise da Auditora: em análise à informação fornecida pela área auditada, a instituição não dispõe de uma política de segurança da informação formalmente instituída, tendo em vista que o documento apresentado trata-se apenas de uma minuta. É importante salientar ainda que a última versão do documento foi inserida no SEI em 14/12/2017, e, a partir de então, não foram dados novos encaminhamentos.

Foi evidenciado pela área auditada que a instituição não dispõe de uma política de segurança da informação, tendo em vista que o documento apresentado trata-se de uma minuta de política de segurança da informação. Neste sentido, a equipe de auditoria interna não valida a informação fornecida e sugere que o item seja respondido como "*Iniciou plano para adotar*".

- **Questão 5.4.e:** a organização dispõe de política de cópias de segurança (*backup*) formalmente instituída como norma de cumprimento obrigatório.

Resposta informada no questionário: adota parcialmente.

Solicitação de comprovação: detalhar os procedimentos realizados para realizar cópias de segurança (backup) dos sistemas institucionais. Os procedimentos são feitos com base em algum normativo? Se sim, indicar quais são.

Esclarecimentos da área auditada: Memorando nº 62/2018/REIT – DGTI.

Análise da Auditora: apesar de entender como positivas as rotinas realizadas pela área auditada, verifica-se a necessidade de a organização dispor de formalizações documentais, tais como Políticas de Segurança da Informação, Políticas de Controle de Acesso, Políticas de Cópias de Segurança, Análises de Riscos e Planos de Continuidade do Negócio, devidamente formalizadas e divulgadas no âmbito institucional.

Neste sentido, a equipe de auditoria interna não valida a informação fornecida e sugere que o item seja respondido como "*Iniciou plano para adotar*".

- **Questão 5.5.a:** a organização executa um processo de software, com o objetivo de assegurar que o software a ser desenvolvido, direta ou indiretamente, atenda às suas necessidades.

Resposta informada no questionário: não adota.

Solicitação de comprovação: foi incluída na resposta da SA 8.1.3.

Esclarecimentos da área auditada: Memorando nº 62/2018/REIT – DGTI.

Análise da Auditoria: no item **5.5.a** a área auditada informa que não executa processo de software, entretanto, no item **5.5.d** é informado que a organização possui pessoal capacitado para gerir a execução do processo de software e que o referido processo é feito de maneira parcial. Complementa-se que regularmente os servidores recebem *e-mail's* institucionais informando atualização de sistemas como, por exemplo, o *e-mail* datado de 17/02/2017 com título: "Processo de implantação do Sistema RAD".

Esclarece-se, entretanto, que as respostas encaminhadas em atendimento às solicitações de auditoria, tanto externas quanto às internas, devem ser fornecidas de maneira completa, uma vez que a auditoria interna não possui atribuições relativas a atestar o cumprimento ou não de um normativo. Desta maneira, orienta-se que ações de auditoria devem ser respondidas com o maior zelo possível, disponibilizando todas as documentações necessárias. Neste sentido, a equipe de auditoria interna não valida a informação fornecida e sugere que o item seja respondido como "*Adota parcialmente*".

VI – RESULTADO DOS EXAMES

ACHADOS DE AUDITORIA: GERAL

CONSTATAÇÃO 001: Desconhecimento dos documentos institucionais.

FATO: Durante o preenchimento do questionário aplicado pela equipe de auditoria ocorreram divergências nas respostas informadas, conforme itens apresentados abaixo.

- Item **1.2.a** que questiona se o IFRO define e comunica papéis e responsabilidades mais relevantes para a governança e a gestão de TI, sendo respondido como "Não adota". Entretanto, em seu Regimento Geral (Resolução nº 65/2015/CONSUP/IFRO), o IFRO possui o detalhamento da estrutura organizacional, as competências das unidades administrativas e as atribuições dos respectivos dirigentes.
- Item **1.6.a** que questiona se o IFRO define formalmente diretrizes para avaliação da governança e da gestão de TI, sendo respondido como "Não adota". Entretanto, mesmo que não realize formalmente, possui devidamente definido no item nº

1.9 do Plano Diretor de TI 2016/2018 a forma como se dará o monitoramento das ações propostas.

- Item **1.6.e** que questiona se o IFRO realiza avaliação periódica de contratos de TI, sendo respondido como "Não adota". Entretanto, em consulta formalizada a área de administração da instituição, foi constatado que apesar de não estar devidamente formalizada e mesmo que de maneiras sucintas, são realizadas consultas aos fiscais de contratos de Tecnologia da Informação e Comunicação (TIC) quando da ocorrência de eventos de alteração contratual ou prorrogação de prazo (Solicitação de Auditoria nº 8.1.4/2018).
- Item **2.1.e** que questiona se o IFRO possui plano estratégico institucional vigente, formalmente instituído pelo seu dirigente máximo, sendo respondido como "Adota integralmente" e apontado como documento comprobatório o Plano de Desenvolvimento Institucional. Entretanto, a equipe de auditoria entende que o documento requisitado na questão se trata do Plano Estratégico do IFRO 2018-2022, que pode ser acessado conforme link https://portal.ifro.edu.br/planejamentoestrategico-nav.
- Item **5.5.a** que questiona se o IFRO executa processo de software, com o objetivo de assegurar que o software a ser desenvolvido, direta ou indiretamente, atenda às necessidades da instituição, sendo respondido como "Não adota". Entretanto, além da própria área responder no item 5.5.d que o referido processo é executado de maneira parcial, a equipe de auditoria, por integrar a instituição e consequentemente acompanhar as atividades desenvolvidas, percebe que regularmente os servidores recebem *e-mails* institucionais informando sobre diversas atualizações em sistemas.

Importante esclarecer que o achado em questão será tratado pela Auditoria Interna como necessidade de capacitação a fim de suprir a lacuna existente.

MANIFESTAÇÃO DO SETOR AUDITADO: Neste sentido, quando questionado se a atual gestão da área de Tecnologia da Informação recebeu capacitação gestora, a área informou, conforme Memorando nº **62/2018/REIT - DGTI/REIT**:

> Sim, recentemente. O FORTI promoveu negociações junto a ENAP e foi criado uma turma específica para os gestores de TI dos institutos Federais no curso Lideranças em Tecnologia da Informação e Comunicações - Turma exclusiva (Conif) nos dias 22 a 26/10/2018 e 19 a 23/10/2018.

ANÁLISE DA AUDITORIA INTERNA: Há de se considerar que a atual gestão da área auditada possui pouco de tempo de experiência enquanto gestor. Mesmo assim, faz-se necessária à devida atenção e zelo para responder questões que estão sob a ótica de uma auditoria. Avalia-se como positiva a capacitação ministrada conforme informado e acompanhado por esta equipe, mas, ainda assim, e ao considerar o repertório de documentos que a instituição possui, reflete-se quanto à necessidade de iniciar ações onde os servidores tenham conhecimento dos próprios documentos institucionais. Por fim, aproveita-se para sugerir que a recomendação desta constatação seja estendida a todos os colaboradores do IFRO.

RECOMENDAÇÃO 001: Iniciar ações internas para que os servidores do IFRO tenham conhecimento dos documentos institucionais.

***

CONSTATAÇÃO 002: Ausência de envolvimento das áreas responsáveis durante o processo de resolução do questionário iGovTI.

FATO: Durante os procedimentos de auditoria verificou-se que o Levantamento de Governança de TI contém diversos temas que, apesar de estarem relacionados à área de Tecnologia da Informação, necessitam do envolvimento de outras áreas da instituição. Contudo, percebeu-se que os questionários eram respondidos apenas pela área de TI.

MANIFESTAÇÃO DO SETOR AUDITADO: Em relação a presente constatação, o setor auditado informou (conforme Memorando nº 70/2018/REIT-DGTI): "Informamos que, em consulta ao servidor responsável pelas respostas dadas ao iGovTI 2016, o diretor de TI anterior, as perguntas eram encaminhadas informalmente, sem o registro por documentos.".

ANÁLISE DA AUDITORIA INTERNA: Em 2010, o Tribunal de Contas da União (TCU) aplicou o primeiro questionário voltado a conhecer melhor a situação da governança no setor público, especificamente na área de TI. Seu objetivo era avaliar o nível de governança nesta área e estimular as organizações públicas a adotarem boas práticas de funcionamento. Para que fosse possível mensurar o resultado deste levantamento, bem como induzir estas melhorias de governança de TI no âmbito da Administração Pública Federal, foi criado o Índice de Governança de TI ou iGovTI.

Também como resultado desse primeiro levantamento, foi expedido pelo TCU o Acórdão nº 1.603/2008 – Plenário, onde se percebe que a governança de TI passou a ser objeto de avaliação dos órgãos de controle. Ressalta-se ainda que, para o bom funcionamento da TI e com o objetivo de assegurar que seu uso agregue valor ao negócio, com riscos e custos aceitáveis, faz-se necessário o bom funcionamento de um conjunto de mecanismos dentro da organização, ou seja, cabe o envolvimento de outras áreas a fim de contribuir com que a perspectiva da área de tecnologia seja efetivamente alcançada.

Entretanto, foi perceptível que as áreas responsáveis pelos temas arrolados no Questionário iGovTI não foram envolvidas, são elas: a Pró-Reitoria de Desenvolvimento Institucional com atuação direta de sua Diretoria de Planejamento, a Autoridade de Monitoramento que é responsável pelo cumprimento da Lei de Acesso à Informação, a Diretoria de Gestão de Pessoas, a Comissão de Ética do IFRO e ainda a própria Auditoria Interna.

Neste sentido, recomendamos que seja indispensável a participação de todas estas áreas, bem como de outras que forem detectadas posteriormente, com o devido acompanhamento da autoridade máxima da instituição, para que seja possível compartilhar demandas detectadas e aprimorar a atuação da área de TI.

RECOMENDAÇÃO 002: Criar metodologias ações a fim de envolver todas as áreas responsáveis pelos temas discutidos no Questionário iGovTI, de forma a aperfeiçoar a atuação da área de Tecnologia da Informação no âmbito do IFRO, bem como aprimorar os processos de governança institucional.

***

INFORMAÇÃO 001: Composição da equipe de Tecnologia da Informação

FATO: Dentro da dimensão "Pessoas", um dos quesitos avaliados por meio do Questionário iGovTI é a composição da equipe de trabalho da área de Tecnologia da Informação, se a gestão da TI está nas mãos de pessoal pertencente ao quadro permanente da organização.

No caso do IFRO, percebe-se que não há percentual de terceirizados e/ou estagiários envolvidos na execução de tarefas dentro da área de TI. Dos 34 (trinta e quatro) servidores lotados na TI, apenas 1 (um) não se encontra na instituição, por estar afastado para cursar doutorado.

***

INFORMAÇÃO 002: Nível de qualificação da equipe de Tecnologia da Informação.

FATO: Em relação à qualificação, os servidores lotados na área de TI (*campi* e Reitoria) tem se distribuído no seguinte percentual, conforme gráfico abaixo demonstrado:

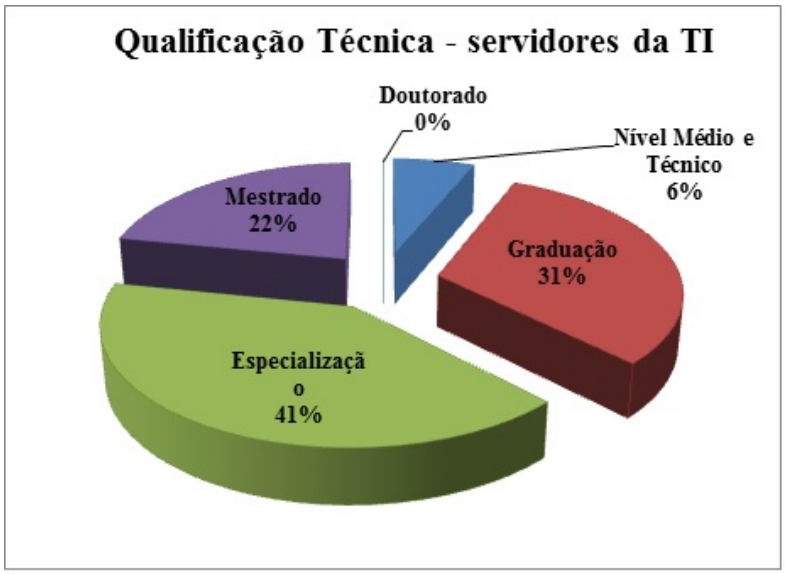

Imagem 1: Qualificação técnica – servidores da TI.
Fonte: Elaborada pela equipe de auditoria com base nos dados fornecidos.

***

CONSTATAÇÃO 003: Necessidade de mapear e planejar metodologias para o desenvolvimento de competências na área de TI.

FATO: Ausência de planejamento que desenvolva as aptidões dos servidores lotados na área de Tecnologia da Informação.

MANIFESTAÇÃO DO SETOR AUDITADO: Em resposta à Solicitação de Auditoria nº 8.1.3, a área auditada encaminhou relatório informando que: "Existe um plano de capacitação anual para todos os servidores, que insere os serviços de TI. Não existe um plano de capacitação específico de TI, porém deseja-se produzir o documento para o ano de 2019.".

ANÁLISE DA AUDITORIA INTERNA: Considera-se positivo que algumas unidades do IFRO, tais como a Reitoria, realizem um plano de capacitação anual para atender às demandas de qualificação de seus servidores. Inclusive, percebe-se que um grande percentual de servidores da área de Tecnologia da Informação (*campi* e Reitoria) foi capacitado em 2017 e 2018. Entretanto, cumpre ressaltar quanto à necessidade de haver um plano onde estejam mapeadas as necessidades de capacitação exclusivamente da área em questão, podendo desta maneira estabelecer um efetivo planejamento a fim de desenvolver as competências da área de TI, sanando ou diminuindo assim as lacunas existentes.

Contudo, e ao considerar que a área já se manifestou informando que o presente documento será elaborado em 2019, a equipe de auditoria acompanhará esta emissão.

RECOMENDAÇÃO 003: Elaborar planejamento a fim de desenvolver as competências no âmbito da área de TI.

***

ACHADOS DE AUDITORIA: GOVERNANÇA

CONSTATAÇÃO 004: Necessidade de aprimorar o processo de elaboração do planejamento de TI.

FATO: Em análise às documentações apresentadas pela área auditada, no que diz a respeito à elaboração do planejamento de Tecnologia da Informação, percebe-se que não houve o envolvimento de outros seguimentos da instituição, se não servidores com conhecimento na área de TI.

MANIFESTAÇÃO DO SETOR AUDITADO: Em atenção ao presente questionamento, a área auditada informou:

> Para o PDTI 2016-2018 o grupo de trabalho foi estruturado pelos representantes de TI de todos os campi com a proposta de que nos campi, o coordenador de gestão de TI local ficou responsável por realizar o alinhamento com a gestão local e na Reitoria, o Diretor de TI responsável pelo alinhamento com o Ensino, Pesquisa, Extensão e Administração, porém, sem integrantes destas áreas compondo o grupo.
>
> Já para este novo PDTIC, 2019-2021, com o intuito de envolver ainda mais as áreas-fim no processo de planejamento e construção do PDTIC, foi definido a elaboração do PDTI através de um compôs-se a comissão com os representantes de TI dos campi, dentre eles, dois campi contam com docentes atuando nesta coordenação, integrantes da DGTI, integrante da área de planejamento e da administração.
>
> Segue em anexo o plano do Projeto de Elaboração do PDTI juntamente com a portaria de composição da comissão.
>
> Salientamos que ainda atualizaremos a portaria da comissão, incluindo integrantes da PROEN, PROEX, PROPESP e DGP.

ANÁLISE DA AUDITORIA INTERNA: Para melhor entendimento deste achado, a equipe de auditoria descreveu abaixo algumas das etapas identificadas no processo para elaboração e aprovação do Plano Diretor de TI:

- Era nomeada uma comissão com servidores da TI (*campi* e Reitoria) responsável pelo levantamento de demandas locais e também pela elaboração do documento final para apresentação.
- Posteriormente, o documento era discutido no Colégio de Dirigentes da instituição, que deveria atuar como Comitê Gestor de TI segundo a Resolução nº 27/2011/CONSUP/IFRO.
- Finalmente, o documento era efetivamente aprovado pelo Conselho Superior, resultando na emissão de uma resolução, como, por exemplo, a Resolução nº 03/2017/CONSUP/IFRO, alterada pela Resolução nº 40/2018/CONSUP/IFRO, que trata do último PDTI da instituição.

Há de se considerar que a possível atuação de um comitê responsável por discutir demandas da área de Tecnologia da Informação composto por membros que são dirigentes das diversas unidades e áreas do IFRO contribui para que estas decisões sejam tomadas de maneira mais abrangente.

Entretanto, quando se percebe que a equipe responsável por realizar os levantamentos locais e elaborar os respectivos documentos de planejamento é composta apenas por servidores da área técnica, como pode ser atestado conforme página 03 do PDTI em vigência, constata-se a necessidade de incluir demais áreas relevantes que possam alavancar os resultados deste planejamento.

Enfatiza-se que incluir membros de outras áreas relevantes, tais como o próprio ensino, pesquisa e extensão, contribuiria para a emissão de um documento mais conciso e também mais próximo da realidade institucional. Cita-se, inclusive, que este procedimento já era realizado, conforme Portaria nº 981/2014/GR/IFRO.

RECOMENDAÇÃO 004: Aprimorar o processo de planejamento da área de Tecnologia da Informação, incluindo representantes das áreas relevantes.

***

CONSTATAÇÃO 005: Desalinhamento institucional do Comitê Gestor de TI.

FATO: Funcionamento do Comitê Gestor de TI em desacordo com os documentos institucionais.

MANIFESTAÇÃO DO SETOR AUDITADO: Quando questionada se o IFRO dispunha de comitê de TI formalmente instituído, a área auditada informou como "Adota integralmente", apresentando a Resolução nº 27/2011/CONSUP/IFRO em complemento a sua resposta. Percebida a desatualização documental, a equipe de auditoria solicitou documentos que comprovassem a atuação do referido comitê, e conforme Memorando nº **62/2018/REIT - DGTI/REIT** foi informado que:

> A opção "adota integralmente" foi selecionada em virtude de ter sido nomeado Comitê Gestor de TI no ano de 2011 através da resolução Nº 27/CONSUP/IFRO, porém esse comitê nomeado não foi reconstituído com a substituição dos membros que deixaram de compor os quadros de representatividade das pró-reitorias, diretorias sistêmicas e até o cargo de Reitor. A atuação do comitê de TI não alcançou a efetividade esperada, em virtude das mudanças de seus componentes e a não definição de um novo comitê através de portaria e com regulamentação própria.

Por fim, a área auditada complementou:

> Com o objetivo de suprir as demandas de alinhamento estratégico de TI com a estratégia geral do IFRO, a DGTI irá encaminhar a solicitação de nomeação de novos membros ao Comitê Gestor de Tecnologia da Informação e atualização do regimento interno do comitê para submissão ao CODIR conforme convocação para a 47ª reunião ordinária e posterior aprovação no CONSUP.

ANÁLISE DA AUDITORIA INTERNA: A documentação entregue para comprovar a existência e o funcionamento do Comitê Gestor de TI – Resolução nº 27/2011/CONSUP/IFRO e a Portaria nº 642/2011/GR/IFRO de nomeação dos membros, são documentações desatualizadas, como a própria área auditada reconhece em sua manifestação.

E, apesar dos esforços envidados em demonstrar que há um funcionamento pelo menos parcial do comitê de TI, a equipe de auditoria constatou um desalinhamento institucional entre a normativa supracitada e o próprio Regimento Geral do IFRO, pois em atenção ao Art. 32 da Resolução nº 65/2015/CONSUP/IFRO, transcrita abaixo, a instituição deve dispor do Comitê de Tecnologia da Informação e Comunicação:

> Art. 32. O Comitê de Tecnologia da Informação e Comunicação (CTIC) é órgão de caráter consultivo e propositivo dos assuntos inerentes às áreas de Tecnologia da Informação e Comunicação, tendo sua organização, composição, competências e funcionamento regulados neste Regimento Geral e no seu Regimento Interno.

Ou seja, a existência do Comitê Gestor de TI (COGIT) não está em conformidade com os documentos institucionais mais atuais. Inclusive, o Regimento Geral atribui ao Diretor de Tecnologia da Informação a competência para presidir o referido comitê, conforme Parágrafo Único também do Art. 32.

Enfatiza-se a necessidade de os servidores terem maior conhecimento sobre seus regulamentos, conforme já narrado na Constatação 001 do presente relatório. Todavia, a área auditada já demonstrou organizações internas a fim de regularizar a situação. Neste sentido, aproveita-se para recomendar que o Regimento Interno que irá dispor quanto ao funcionamento do Comitê de Tecnologia da Informação e Comunicação tenha como base as orientações expedidas pela Secretaria de Logística e Tecnologia da Informação (SLTI).

RECOMENDAÇÃO 005: Fomentar ações para que o Comitê Gestor de TI seja ativado em sua totalidade, com base nas orientações expedidas pela Secretaria de Logística e Tecnologia da Informação (SLTI).

***

CONSTATAÇÃO 006: Necessidade de efetivar o monitoramento.

FATO: Quando indagada, a área auditada informou que não é realizado monitoramento com avaliação periódica de governança e gestão da TI e de sistemas de informação.

MANIFESTAÇÃO DO SETOR AUDITADO: O setor auditado discorre sobre alguns percalços para efetivar ações de monitoramento, conforme informado no Memorando nº **62/2018/REIT - DGTI/REIT**:

> "No tópico 3.1 "Organograma da DGTI" presente no PETI 2015-2019 do IFRO, é apresentado o organograma atual da diretoria e informado com base no Acordão no 1200/2014 - TCU Plenário, que aprova o diagnóstico da situação da estrutura de recursos humanos alocadas na área de Tecnologia da Informação, quanto a necessidade de adequação da estrutura administrativa do IFRO:
>
> Contudo, a percepção da necessidade de adequação, somada com a organização interna praticada, indica que há a necessidade da adequação da estrutura administrativa da DGTI. Dessa forma, garante-se o atendimento efetivo trabalhado quanto ao identificado pelo acórdão do TCU (PETI IFRO, 2015).
>
> Baseado no trecho extraído do PETI, a ausência de setor específico no organograma tem gerado prejuízo às ações de governança, sendo necessária a reestruturação para adequação à estratégia de TI.
>
> Como encaminhamento, será solicitado ao Comitê Gestor de TI, após sua reconstituição, a reestruturação do organograma da Diretoria de Gestão da Tecnologia da Informação (DGTI) inserindo setor de governança de TI."

ANÁLISE DA AUDITORIA INTERNA: A ausência de monitoramento contribui para o aumento do nível de risco de um possível desalinhamento da TI com o negócio da instituição, pois conforme Relatório iGovTI – Exercício 2016, um processo de monitoramento devidamente estabelecido permite à alta administração acompanhar efetivamente o cumprimento dos planos organizacionais.

Neste mesmo sentido, a norma da ABNT NBR ISO/IEC nº 38500/2009 orienta que "Convém que os dirigentes monitorem até que ponto a TI dá suporte ao negócio. Convém que os dirigentes monitorem até que ponto as políticas, tais como aquelas relacionadas com a exatidão dos dados e a eficiência do uso da TI, são seguidas corretamente".

RECOMENDAÇÃO 006: Efetivar as ações de monitoramento junto à área de Tecnologia da Informação, de forma a possibilitar a correção oportuna dos objetivos institucionais com a direção do IFRO.

***

ACHADOS DE AUDITORIA: SEGURANÇA DA INFORMAÇÃO

CONSTATAÇÃO 007: **Ausência de Política de Segurança da Informação.**

FATO: Mediante a análise das respostas e documentos disponibilizados, foi verificada a ausência de política de segurança da informação em vigor e inexistências de discussões para a regularização do tema.

MANIFESTAÇÃO DO SETOR AUDITADO: O setor auditado apresentou documentos institucionais em andamento para demonstrar o processo de regularização da política de segurança da informação, conforme manifestação constante no Memorando nº **62/2018/REIT - DGTI/REIT**:

> O plano de trabalho para a construção da política de Segurança da Informação foi construído e o pode ser acessado através do Link http://estrategia.ifro.edu.br/si/plano-de-trabalho/ além dos documentos em anexo (0397111) porém o último encaminhamento relativo ao processo foi o encaminhamento ao gabinete (protocolo 503287/2015-62 no sistema http://siga-adm.ifro.edu.br).
>
> Planeja-se após a redefinição do comitê gestor de TI, recompor a comissão, realizar a revisão e submeter para aprovação da política.

E quando solicitado esclarecimento sobre a não efetivação da política, não souberam informar, conforme Memorando nº 70/2018/REIT - DGTI/REIT:

> Processo de criação da política foi iniciado em 2015 porém não foi concluído e encontra-se paralisado desde então. Ao se questionar um dos membros da comissão de elaboração da POSIC, não soube indicar com certeza o motivo da não conclusão do processo.

ANÁLISE DA AUDITORIA INTERNA: Segundo o Decreto nº 3.505, de 13/06/2000, foi instituída a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, sendo conceituada conforme o inciso II de seu Art. 2º, transcrito:

> Art. 2º Para efeitos da Política de Segurança da Informação, ficam estabelecidas as seguintes conceituações:
>
> (...)
>
> II - Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das

> comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.

Conforme orientações dispostas na norma da ABNT NBR ISO/IEC 17799:2005:

> As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por código malicioso, *hackers* e ataques de *denial of service* estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

Nesse sentido, o Decreto nº 3.505, de 13/06/2000 determina:

> Art. 3º São objetivos da Política da Informação:
>
> I - dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;
>
> II - eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;
>
> III - promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;
>
> IV - estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação;
>
> V - promover as ações necessárias à implementação e manutenção da segurança da informação;
>
> VI - promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação;
>
> VII - promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a segurança da informação; e
>
> VIII - assegurar a interoperabilidade entre os sistemas de segurança da informação.

Verifica-se, portanto, que diversas normativas primam por orientar as organizações públicas a zelar pela segurança da informação, pois sua definição é requisito indispensável para reconhecer sua importância no âmbito institucional. Desta maneira, instituições privadas ou públicas, assim como o IFRO, têm o dever de aprimorar essa ação objetivando proteger a informação de ameaças como as supramencionadas, a fim de garantir a continuidade do negócio, minimizar o risco e maximizar oportunidades.

Percebeu-se que a assessoria desta Auditoria Interna àquela área de TI, por ocasião do desenvolvimento do presente trabalho, conseguiu alcançar um dos seus principais objetivos: contribuir com a conscientização referente à implantação da política em discussão.

Aproveita-se para recomendar que a nova política de segurança da informação seja elaborada com base nas recomendações expedidas pelo Departamento de Segurança da Informação e Comunicação (DSIC), bem como seja ativado o Comitê Gestor de Segurança da Informação e Comunicação (CGSIC), órgão responsável pela elaboração e revisão periódica da Política de Segurança da Informação e Comunicação (POSIC), conforme o Art. 34 do Regimento Geral do IFRO – Resolução nº 65/2015/CONSUP/IFRO.

RECOMENDAÇÃO 007: Elaborar e efetivar as ações dispostas na Política de Segurança da Informação.

RECOMENDAÇÃO 008: Implementar, conforme Regimento Geral do IFRO, o Comitê Gestor de Segurança da Informação e Comunicação.

***

CONSTATAÇÃO 008: **Ausência de planejamento para gerir continuidade de serviço de TI.**

FATO: Quando questionada, a área auditada informou que não dispõe de política institucional e não realiza procedimentos a fim de evitar a descontinuidade dos serviços prestados pela área de Tecnologia da Informação.

MANIFESTAÇÃO DO SETOR AUDITADO: Quando questionada a respeito da não implementação de um planejamento para gerir a continuidade de serviços de TI, a área auditada informou suas dificuldades: “Capacitação da equipe, alta demanda de atividades do setor em relação ao quantitativo de servidores, necessidade de reestruturar DGTI através da criação de setor para tratar especificamente a governança de TI.”.

ANÁLISE DA AUDITORIA INTERNA: Segundo a Norma da ABNT NBR ISO/IEC 17799/2005, o objetivo da gestão da continuidade do negócio é não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, além de assegurar a sua retomada em tempo hábil, caso necessário.

Ainda conforme a norma supramencionada convém que uma estrutura básica dos planos de continuidade do negócio (PCN) seja mantida para assegurar que todos os planos são consistentes, para contemplar os requisitos de segurança da informação e para identificar prioridades para testes e manutenção.

A ausência de um plano para manter a continuidade dos serviços demonstra que a instituição não está preparada para recuperar ou manter suas atividades caso ocorram situações que interrompam os serviços prestados. Assim, segundo a ata do Acórdão do TCU nº 1.603/2008 - Plenário:

> A ausência de PCN na organização é um indício de falta de conscientização em nível estratégico com os riscos de interrupção de serviços. Sem planejamento dessa natureza, a organização fica vulnerável quando da ocorrência de desastres (naturais ou por sabotagem) e interrupções de serviços. Eventos que poderiam ser resolvidos sem grande perda, acabam por comprometer toda a base atual e histórica de informações da organização. Pode ser até que o PCN nunca precise ser acionado, mas se houver a necessidade e ele não existir, isso pode significar risco à continuidade da existência da organização.

Por fim, destaca-se a necessidade de que o processo de gestão da continuidade do negócio seja implementado para minimizar um impacto sobre a organização e recuperar perdas de ativos da informação (que pode ser resultante de, por exemplo, desastres naturais, acidentes, falhas de equipamentos e ações intencionais) a um nível aceitável através da combinação de ações de prevenção e recuperação.

RECOMENDAÇÃO 009: Realizar ações para implantar a gestão da continuidade dos serviços de Tecnologia da Informação.

***

CONSTATAÇÃO 009: **Ausência de gestão de mudanças.**

FATO: Quando questionada, a área auditada informou que não dispõe de política e não realiza procedimentos a fim de gerir mudanças no ambiente de TI.

MANIFESTAÇÃO DO SETOR AUDITADO: Quando questionada a respeito da não implementação de um gerenciamento de mudanças, a área auditada informou suas dificuldades: “Capacitação da equipe, alta demanda de atividades do setor em relação ao quantitativo de servidores, necessidade de reestruturar DGTI através da criação de setor para tratar especificamente a governança de TI.”.

ANÁLISE DA AUDITORIA INTERNA: De acordo com o Cobit 4.1 AI6:

> Todas as mudanças, incluindo manutenções e correções de emergência, relacionadas com a infraestrutura e as aplicações no ambiente de produção são formalmente gerenciadas de maneira controlada. As mudanças (incluindo procedimentos, processos, parâmetros de sistemas e de serviço) devem ser registradas, avaliadas e autorizadas antes da implementação e revisadas em seguida, tendo como base os resultados efetivos e planejados. Isso assegura a mitigação de riscos de impactos negativos na estabilidade ou na integridade do ambiente de produção.

Por fim, o Tribunal de Contas da União (TCU) confirma a importância desta ação conforme ata do Acórdão 1.603/2012 – Plenário:

> A realização de mudanças no ambiente de TI sem o devido controle é causa comum de instabilidade e falhas de segurança. Isso porque há mudanças frequentes e necessárias no ambiente de TI que oferecem risco à disponibilidade das informações: a atualização de versões de produtos de software, a oferta de novos sistemas ou módulos de sistemas, a atualização de sistemas operacionais e a atualização de aplicativos, dentre outros. Caso um novo produto não adequadamente testado seja disponibilizado no ambiente, há um risco de comprometer o funcionamento de outras soluções de TI. Além disso, as mudanças devem ser registradas tanto para possibilitar auditoria quanto para restaurar situações anteriores a uma mudança inadequada.

RECOMENDAÇÃO 010: Realizar ações que implantem gerenciamento de mudanças na área de TI.

***

CONSTATAÇÃO 010: Ausência de gestão de riscos em TI.

FATO: Conforme questionário aplicado, a área auditada declarou não ter, formalmente instituído, processo de gestão de riscos em TI, além de também não executar ações de identificação, avaliação e tratamento de riscos.

MANIFESTAÇÃO DO SETOR AUDITADO: Conforme o Memorando nº 70/2018/REIT – PRODIN/REIT, de 10/12/2018, a área auditada manifestou-se informando que: "Não havia a política institucional de gestão de riscos, não possuía capacitação da equipe e alta demanda de atividades do setor em relação ao quantitativo de servidores.".

ANÁLISE DA AUDITORIA INTERNA: O Relatório de Levantamento – Fiscalização nº 55/2016, emitido pelo TCU, conceitua riscos de TI como eventos capazes de impedir, em certo grau, que a gestão de TI cumpra sua missão de auxiliar a organização a alcançar seus objetivos institucionais, estando relacionados.

Seguindo a mesma referência, os riscos de TI estarão relacionados, em grande maioria, à ocorrência de obstáculos, perdas e prejuízos. Desta maneira, é imprescindível que a organização gerencie seus riscos de TI pela execução das atividades de identificação, avaliação e tratamento desses riscos, a fim de que sejam mantidos em níveis e custos aceitáveis pela corporação.

Por fim, salienta-se que o Acórdão nº 2.135/2017 - Plenário já tratou de recomendar que se avalie a conveniência e a oportunidade de estabelecer e implementar um processo de gestão de riscos de TI, com vistas a maximizar os benefícios de suas ações.

RECOMENDAÇÃO 011: Implementar ações que busquem o gerenciamento de risco na área de TI, bem como formalizar procedimentos institucionais para normatização do assunto.

***

CONSTATAÇÃO 011: Ausência de execução e formalizações em relação ao processo de software.

FATO: Quando indagada a área auditada informou que não dispõe de documento formalizando o processo de software e que não executa procedimentos que visem assegurar que o software desenvolvido atenderá as necessidades da instituição.

MANIFESTAÇÃO DO SETOR AUDITADO: Quando questionada sobre a não realização de processo de software, a área auditada esclareceu que:

> Em relação ao processo de software, não se possui documento formalizando o processo de desenvolvimento contudo, a Coordenação de Desenvolvimento de sistemas gerencia o desenvolvimento das soluções através da ferramenta https://git.ifro.edu.br que concentra os projetos de desenvolvimento dos sistemas, onde realiza-se as alterações do código e versionamento. Este desenvolvimento segue convenções e boas práticas, envolvendo reuniões com as áreas demandantes para levantamento dos requisitos, prototipação, disponibilização para ambiente de testes, homologação em ambiente de Quality Assurance - QA, e após a validação das implementações disponibiliza-se em ambiente de produção a nova versão do sistema. Contudo, ainda não possuímos uma formalização deste processo, mas observamos a necessidade e incluiremos em nosso plano de trabalho.

ANÁLISE DA AUDITORIA INTERNA: Um processo de software é, portanto, um conjunto de atividades que transformam requisitos de usuários (entrada do processo) em um produto de software. Por oportuno, chamamos a atenção para o fato de que o produto de software não é composto apenas dos programas de computadores, mas inclui outros itens. Mais ainda, destacamos que os diversos itens que compõem o produto de software são gerados ao longo da execução do processo de software (Ata do Acórdão TCU nº 1.233/2012 - Plenário).

No caso do IFRO, a área auditada depois de ter informado que "Não adota" o procedimento de software, complementou sua resposta esclarecendo que executa parcialmente o processo tendo em vista que a capacitação de seu pessoal é insuficiente perante a demanda de inovação tecnológica e que realiza ações mesmo que sem as devidas formalizações processuais.

Todavia, faz-se necessário considerar que as operações realizadas, principalmente as da área de TI, precisam ser construídas com base no negócio da instituição e que tal situação poderá melhor ser detectada quando realizada a análise e o estudo de um processo antes de sua implantação. Vejamos o que o item AI2 do Cobit 4.1 diz em se tratando de software:

> (...) devem ser disponibilizados em alinhamento com os requisitos do negócio. Este processo contempla o projeto das aplicações, a inclusão de controles e requisitos de segurança apropriados, o desenvolvimento e a configuração de acordos com padrões. Isso permite às organizações apoiarem de forma adequada as operações do negócio com as aplicações corretas.

Assim sendo, espera-se da TI do IFRO, que prime pelo desenvolvimento ou aquisição de um software, eficiente, ágil e de fácil manuseio, visando seus principais clientes.

Neste sentido, entende-se que uma ausência de execução e/ou definição de um processo de software pode acarretar em retrabalhos de uma equipe, justamente por haver um maior risco em relação ao não alinhamento com o negócio institucional.

Além disso, é indispensável o atendimento aos órgãos de controle que já estabeleceram a obrigatoriedade de formalizar um processo de software, observando as boas práticas, conforme o Acórdão do TCU nº 1.233/2012 – Plenário.

RECOMENDAÇÃO 012: Efetivar procedimentos de software, bem como documentá-los.

***

CONSTATAÇÃO 012: **Ausência de gestão de incidentes.**

FATO: A área auditada não dispõe de política e não realiza procedimentos a fim de gerenciar possíveis incidentes.

MANIFESTAÇÃO DO SETOR AUDITADO: Quando questionada a respeito da não implementação de uma gestão de incidentes, a área auditada informou suas dificuldades: "Capacitação da equipe, alta demanda de atividades do setor em relação ao quantitativo de servidores, necessidade de reestruturar DGTI através da criação de setor para tratar especificamente a governança de TI.".

ANÁLISE DA AUDITORIA INTERNA: Segundo a norma da ABNT NBR ISO/IEC nº17799/2005, o objetivo da Gestão de Incidentes de Segurança da Informação é assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.

Ainda segundo o que preconiza a NBR ISO/IEC 17799/2005, convém que um procedimento de notificação formal seja estabelecido para relatar os eventos de segurança da informação, junto com um procedimento de resposta a incidente e escalonamento, estabelecendo a ação a ser tomada ao se receber a notificação de um evento de segurança da informação.

Por fim, chama-se atenção para que a área responsável formalize e realize ações de treinamento e alerta a fim de definir procedimentos que gerenciem possíveis ocorrências de incidentes, tais como: a) perda de serviço, equipamento ou recursos; b) mau funcionamento ou sobrecarga de sistema; c) erros humanos; d) não conformidade com políticas ou diretrizes; e) violações de procedimentos de segurança física; f) mudanças descontroladas de sistemas; g) mau funcionamento de software ou hardware; h) violação de acesso.

RECOMENDAÇÃO 013: Realizar ações para implantação da gestão de incidentes.

***

CONSTATAÇÃO 013: **Ausência de processo de gerenciamento de ativos.**

FATO: Quando questionada, a área auditada informou que não dispõe de política e não realiza procedimentos a fim de gerenciar os ativos relativos à Tecnologia da Informação.

MANIFESTAÇÃO DO SETOR AUDITADO: Em resposta à S.A 8.1.2 o setor auditado se manifestou informando:

"Foi realizada uma ação conjunta com as CGTI's dos campi e o levantamento de ativos de TI. Ressaltamos que atendemos ao convite da CGU para Pesquisa elaborada para avaliar a Gestão de Ativos de Tecnologia da Informação e Comunicação (TIC) e o questionário foi enviado no dia 26/10/2018. A consolidação do documento encontra-se em anexo (0397145)."

Além disso, conforme Memorando nº 70/2018/REIT-DGTI, a área auditada afirmou suas dificuldades: "Capacitação da equipe, alta demanda de atividades do setor em relação ao quantitativo de servidores, necessidade de reestruturar DGTI através da criação de setor para tratar especificamente a governança de TI.".

ANÁLISE DA AUDITORIA INTERNA: Uma das definições de ativos é expressamente estabelecida pela norma da ABNT NBR nº 27002/2005:

> "**Ativos** representam todos os itens da organização onde informações **são** criadas, processadas, armazenadas, transmitidas ou descartadas. O gerenciamento de **ativos é** fundamental para priorizar investimentos **e** concentrar esforços nos **ativos** mais críticos, que sustentam os processos da organização."

Em análise, foi possível verificar que a área auditada iniciou levantamento de ativos do tipo físico: equipamentos computacionais e de comunicação, o que pode ser considerado positivo. Entretanto, e ao considerar o foco deste trabalho remetido ao tema de segurança da informação, segundo a NBR ISO/IEC 17799:2005 da ABNT, constata-se o rol de ativos que

se faz necessário levantar, são eles: ativos de software, ativos de informação, serviços, pessoas e suas qualificações, habilidades e experiências; intangíveis tais como a reputação e imagem da organização.

RECOMENDAÇÃO 014: Realizar ações que estabeleçam o gerenciamento de ativos.

***

CONSTATAÇÃO 014: Ausência de gerenciamento e acompanhamento do nível de serviço em TI.

FATO: Quando questionada, a unidade auditada informou que não dispõe de níveis de serviço formalmente definidos, consequentemente, a área não dispõe de indicadores para mensurar o nível dos serviços prestados, bem como não monitora seu alcance e não programa possíveis ações corretivas a serem implementadas, caso necessário.

MANIFESTAÇÃO DO SETOR AUDITADO: Quando questionada a respeito da ausência de gestão responsável por acompanhar níveis dos serviços de TI, a área auditada manifestou suas dificuldades: "Necessidade de reestruturação do organograma da DGTI através da criação de setor que trate especificamente o atendimento/suporte aos usuários de serviços de TI, alta demanda de atividades do setor em relação ao quantitativo de servidores.".

ANÁLISE DA AUDITORIA INTERNA: A resposta da área auditada corrobora com o resultado obtido na verificação de alguns dos processos de trabalho que apoiam a gestão de níveis de serviço, são eles: o plano de continuidade de negócios, a gestão de mudanças e ainda o catálogo de serviços.

A gestão dos níveis de serviço de TI objetiva garantir que esses serviços sejam prestados em conformidade com as expectativas e necessidades da organização.

A necessidade de um gerenciamento no nível de serviço de TI é tratada em inúmeros documentos, leis e normativos. Segundo o Acórdão TCU nº 1.603/2008:

> A ausência da gestão de acordo de níveis de serviço em percentual tão expressivo indica que grande parte dos pesquisados não realiza a negociação da qualidade dos serviços de TI com os seus clientes. A consequência disso é uma dificuldade em ajustar expectativas: as áreas de TI não sabem se estão atendendo às necessidades de qualidade de serviço dos seus clientes, nem tampouco os clientes sabem, ao pedir um serviço de TI, qual o nível de qualidade que podem esperar. Os resultados podem ser áreas de TI cujos esforços e investimentos não estão sintonizados com as necessidades e expectativas dos seus clientes.

Os processos de gestão de serviços, conforme definidos na NBR ISO/IEC nº 20000-2, compreendem diversos aspectos relacionados ao fornecimento dos serviços, tais como a organização de um catálogo de serviços de TI, o estabelecimento de Acordo de Nível de Serviço (ANS) entre a área de TI e as áreas de negócio e o monitoramento do alcance dos níveis de pactuados. Convém destacar que os ANS estabelecem os parâmetros sob os quais aquele serviço deverá operar e ser avaliado. Em geral, o referido acordo é estabelecido entre a unidade de TI da instituição e as unidades de negócio beneficiadas por seus serviços. Quando o ajuste é firmado entre a instituição e um fornecedor ou prestador de serviços contratado, o instrumento é denominado contrato com nível de serviço. (Acórdão do TCU nº 2.135/2017 – Plenário)

Desta maneira, entende-se a necessidade de haver um gerenciamento e um acompanhamento quanto ao nível de serviços em TI prestados, objetivando monitorar o grau de eficiência e o alcance da missão da TI dentro da organização e assegurando que a qualidade adequada de serviços seja entregue aos clientes.

É válido ressaltar que apesar da área auditada apresentar página institucional contendo o rol dos serviços prestados pela instituição, e indicando-a como o catálogo de informações, faz-se necessário constar documento contendo a respectiva indicação desses serviços, as principais informações sobre os mesmos e os requisitos para se obter acesso. Por fim, o documento deve ter rotina de atualização e estar devidamente publicado em site institucional.

RECOMENDAÇÃO 015: Implantar gerenciamento para definir e monitorar níveis de serviço.

RECOMENDAÇÃO 016: Aprimorar a gestão do catálogo de serviço utilizado pela instituição.

***

VII – CONCLUSÃO

O presente relatório teve como objetivo avaliar a adequação dos mecanismos de controle na área de Tecnologia da Informação. Em relação aos objetivos específicos elencados no item II deste relatório, não foi possível aferir o alinhamento entre PDTI e

PDI, tendo em vista que o IFRO já dispõe de novo PDI, enquanto que a área de TI ainda em processo de elaboração do seu novo PDTI.

Enfatiza-se que a gestão propiciou à auditoria interna apoio técnico mediante a disponibilização de um servidor com amplo conhecimento na área de Tecnologia da Informação conforme Portaria nº 2.563/2018/REIT - CGAB/IFRO, desta maneira, a análise dos documentos e informações fornecidas pela área auditada foi realizada em conjunto. Por fim, ressalta-se que a Auditoria Interna percebeu a iminente necessidade de capacitar sua equipe para que seja possível melhor assessorar um órgão de alto nível estratégico como a área de Tecnologia da Informação, e para tanto já incluiu no próximo Plano Anual de Auditoria Interna solicitação de capacitação.

Os critérios adotados no presente documento foram os de: orientar, acompanhar e avaliar os diversos setores da Instituição, visando à eficiência e eficácia dos controles.

Porto Velho/RO, 17 de dezembro de 2018.

Documento assinado eletronicamente por **Romualdo Souza de Lima**, **Auditoria Interna**, em 21/12/2018, às 15:18, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Gleiciane Santos Oliveira Xavier de Mesquita**, **Contador(a)**, em 21/12/2018, às 15:23, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ifro.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0434683** e o código CRC **D55150F8**.

Referência: Processo nº 23243.025271/2018-58 SEI nº 0434683