MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO RECÔNCAVO DA BAHIA
GABINETE DO REITOR
AUDITORIA INTERNA

RELATÓRIO FINAL DE AUDITORIA Nº 04/2018

1 - IDENTIFICAÇÃO DA AUDITORIA

Realização do PAINT/2018
Área: A.7 - **Ação:** A.**7.**1-
Período de realização: 03/05/2018 a 07/08/2018
Setor Auditado: PROPLAN/COTEC
Objetivo: Avaliação objetiva sobre a gestão de TI da UFRB, destacando o planejamento existente, procedimentos para salvaguarda da informação, e avaliar o atual patamar de tecnologia da informação da Universidade, bem como o nível de adoção de práticas relacionadas a gestão de riscos em TI.

2 – ESCOPO

A auditoria teve como objetivo avaliar a Gestão de Tecnologia da Informação da UFRB, no que concerne ao planejamento das atividades, aos procedimentos para salvaguarda da informação, a capacidade de produção de sistemas e avaliação de práticas voltadas para gestão de riscos. Para cumprir o objetivo foi necessário buscar informações institucionais acerca das ações voltadas para TI na UFRB de modo a conhecer essa dinâmica na Instituição.

Para tanto foi analisado as informações constantes do PDI- Plano de Desenvolvimento Institucional para 2015-2019 e também do Relatório de Gestão de 2017, além de verificar informações constantes no sítio institucional da COTEC- Coordenadoria de Tecnologia da Informação. Realizou-se ainda, entrevista com o Coordenador de Tecnologia da Informação da UFRB com vistas a colher informações referente à gestão de TI.

Por fim, para validar o patamar de governança a gestão de TI em que se encontra a UFRB, foram formuladas questões de auditoria com base no objetivo proposto, sendo que essas questões foram adaptadas do questionário de governança do TCU- Tribunal de Contas da União referente ao ano de 2014. Essas questões foram aplicadas sob a forma de Solicitações de Auditoria, as quais foram encaminhadas para a Coordenadoria juntamente com outras solicitações, com vistas a obter informações a respeito das ações tomadas pela unidade auditada para identificar e gerir os riscos de TI.

3 – ACOMPANHAMENTO DA GESTÃO

Objetivando buscar informações quanto as boas práticas de gestão realizadas no âmbito da gestão de TI, analisou-se o sítio institucional da COTEC. Em resposta à SA n° 69/2015, referente a auditoria que fora iniciada em 2015, a COTEC informou que havia expectativa da melhoria dos serviços prestados pela COTEC com a conclusão da primeira versão do Catálogo de Serviço, (documento recomendado pelo ITIL e equivalente a Carta de Serviços), que tinha previsão de conclusão e divulgação para o primeiro trimestre de 2016. Em verificação ao sítio institucional da coordenadoria identificou-se que já consta o catalogo de serviços disponibilizados a comunidade acadêmica, o que se configura como uma boa prática de gestão e um avanço na gestão de TI da UFRB.

Na aplicação do questionário para avaliar o patamar de gestão de TI, a Coordenadoria informou que o catálogo está publicado no site, no entanto, ainda é preciso que haja uma maior integração com as atividades realizadas no dia a dia, assim a resposta a essa questão de auditoria foi validada como adota parcialmente. Este catálogo contém informações a respeito de compartilhamento de arquivos; armazenamento em nuvem; manutenção do sistema; e-mail; dentre outras informações relacionadas aos serviços prestados pela Coordenadoria à comunidade acadêmica.

Ainda em relação a aplicação do questionário para avaliar o patamar de gestão de de TI, foram aplicadas 20 questões, das quais 3 foram validadas como *adota integralmente* e 03 validadas como *adotada parcialmente* e as restantes como *não adota*, ou *iniciou plano para adota*r. As questões validadas como adota parcialmente se referem ao comitê de TI formalmente instituído, política de segurança da informação e equipe de tratamento para respostas a incidentes.

A UFRB possui desde 2014 sua Política de Segurança da Informação e Comunicação- POSIC, ela foi criada através da emissão da Nota Técnica 02/2014. Essa política fornece diretrizes, normas, critérios, monitoramento e controle para a preservação da autenticidade, confiabilidade, disponibilidade e integridade dos dados e das informações processadas, armazenadas e dos recursos de TIC custodiados pela UFRB. Atualmente existe um processo solicitando a composição do grupo de trabalho para revisão e atualização da POSIC. Há ainda um núcleo de segurança da informação que atua onde atualmente existe um núcleo de segurança de informação que atua com esta finalidade.

Quanto às respostas ao questionário que foram validadas como adota parcialmente, estavam: A política de cópias de segurança de informação, onde foi informado que tal procedimento está sendo reformulado através do processo de número 23007.00002630/2018-91; Processo de monitoramento do uso de recursos de TI para detectar as atividades não autorizadas sendo apontado que já fora definido os procedimentos técnicos para o serviço de e-mail e para identificação de acesso não autorizado, no entanto ainda necessita de ampliação; e Gerenciamento do catálogo de serviços, a COTEC possui catálogo publicado no site, no entanto precisa integrar o catálogo às atividades realizados no dia a dia, como já citado anteriormente.

4– CONSTATAÇÕES, ANÁLISE E RECOMENDAÇÕES DA AUDITORIA INTERNA:

A partir do questionário aplicado, foram consideradas como objeto de constatações as respostas apresentadas como '*não adota'*, com vistas a destacar os impactos desta não adoção e a relevância de adotar tais ações. Ademais, foram aplicadas questões para avaliar o patamar de gestão de riscos de TI, que obtiveram respostas, que não se constituíram sob a forma de constatação devido às boas práticas.

Deste modo, solicitou-se informações com vistas a verificar o patamar de gestão de riscos em Tecnologia da Informação em que se encontra a Universidade Federal do Recôncavo da Bahia, bem como o nível de adoção da prática e formalização da Gestão de Riscos em TI, com apresentação das devidas justificativas e documentações comprobatórias. Neste sentido, ao se questionar, à unidade de TI, quanto a existência de política de gestão de riscos formalmente instituída, verificou-se que a unidade não adota práticas nesse sentido. Verificando que tal apontamento é conseqüência da própria ausência de estrutura de gestão de riscos na UFRB como um todo. No entanto, isso não isenta a unidade de TI do desenvolvimento de práticas relacionadas a gestão de riscos.

Quanto a isto, foi questionada a unidade sobre questões mais práticas em relação a riscos, como a identificação e avaliação de riscos; a elaboração de mapa de riscos; e plano de ação para mitigação de incidentes, sendo respondido que a organização, especificamente a gestão de TI, iniciou plano para adotar. Esse plano refere-se a ações iniciadas este ano, onde foi realizado o levantamento de riscos por *brainstorming(técnica para desenvolvimento de novas idéias ou resolução de problemas)* envolvendo todos os técnicos da COTEC e a pontuação dos riscos com chefes de núcleo da COTEC.

Atualmente a unidade está em processo de classificação dos riscos por níveis de tratamento e definição de ações técnicas e recomendações para a administração e a conclusão do relatório, que é o resultado do processo. Além disso, os documentos elaborados foram encaminhados para esta Auditoria. Dentre esses documentos, foi apresentado um que contempla a descrição dos riscos a serem sanados, os riscos a serem minimizados e os riscos a serem aceitos, que foram definidos a partir de uma escala de numeração e com a indicação das respectivas soluções caso o risco se concretize.

Foi elaborado pela COTEC também um fluxograma com a indicação das ações necessárias para o gerenciamento dos riscos de TI, que perpassa pela identificação do risco a partir de relatórios de anos anteriores, a classificação dos riscos através de documentos de Riscos de TI, a definição do plano de ação e por fim a elaboração do relatório final. Da análise das respostas obtidas verificou-se que duas das etapas definidas para o gerenciamento de riscos já foram definidas.

Tais ações demonstram um avanço na gestão de riscos da Universidade, considerando que o nível de governança ainda não estabeleceu uma estrutura de gerenciamento de riscos, a COTEC é uma das pioneiras no desenvolvimento de práticas relacionadas a gestão de riscos, pois até o momento só a Auditoria Interna apresentou a experiência na confecção da matriz de riscos. Resta agora desenvolver as outras etapas para finalizar o relatório e colocar em prática o mapa elaborado, como uma maneira de impulsionar a gestão na formalização da política, além de servir como referência para desenvolvimento em outras unidades que podem adaptar o mapa elaborado as suas realidades.

CONSTATAÇÃO 04
Ausência de Planejamento Formal nas Ações de TI

Em continuidade aos trabalhos de auditoria foi emitida a solicitação de Auditoria de n° 242/2018 com vistas a colher informações quanto ao atual patamar de gestão de Tecnologia da Informação em que a Universidade se encontra. Desta forma, destacou-se os pontos que não são adotadas ações nesse sentido, a saber:

- Apoio do comitê de TI
- Plano de TI vigente, formalmente instituído (com objetivos, indicadores e metas e acompanhamento do Plano de TI quanto ao alcance das metas)
- Definição de diretrizes para avaliação de desempenho dos serviços de TI
- Avaliação Periódica dos Sistemas de Informação

Assim, foi informado que a UFRB não prioriza as ações de TI com apoio do comitê de TI, que *a priori*, deveria atuar como instância consultiva da alta administração, pois esse comitê deve estar envolvido na priorização das ações de TI, onde para desenvolver uma ação de TI ela deveria passar primeiro por reunião e aprovação do comitê. Corrobora com isso o fato de que no Relatório de Gestão da UFRB referente ao ano de 2017 consta a informação de que no ano de 2017 o Comitê de Governança digital não realizou reuniões nem emitiu decisões. Demonstrando que de fato o Comitê pode não estar atuando como instância consultiva. Ademais, como não houve reuniões, não foi possível analisar as atas de reuniões para levantar as ações discutidas no âmbito do Comitê.

O referido Comitê é formado por Pró-Reitores, Vice Reitor, Coordenador de da Unidade de TI, representante dos Gerentes Técnicos e representante dos Diretores dos Centros de Ensino, que são representantes da administração estratégica, justamente para assegurar que a governança de TI seja considerada como parte da governança corporativa e fazer com que a formulação e a implementação das estratégias e planos de TI estejam harmonizadas com os objetivos organizacionais da alta administração.

Entre as atividades que devem ser desempenhadas pelo Comitê de acordo com o Guia de Comitê de TI do SISP- Sistema de Administração dos Recursos de Tecnologia da Informação estão a definição de prioridades para projetos e ações de TI, a tomada de decisão em relação aos recursos orçamentários para a viabilização da implementação dos

planos e deliberação sobre estratégias, planos e políticas de TI para a organização. Corrobora com isto o fato de que esse Comitê de Governança Digital é atualmente responsável pela elaboração do PDTI- Plano Diretor de TI, que objetiva orientar as ações institucionais na área de TI, o que já foi apontado no Relatório de Gestão da UFRB em 2017, onde foi informado que foi criada uma comissão para elaboração do PDTI em 2016, entretanto ainda não houve reunião, o que foi confirmado pela COTEC em resposta a SA n° 240/2018.

Deste modo, faz-se necessário que esse Comitê se articule para elaborar o Plano Diretor de TI, pois não há que se justificar a ausência do PDTI devido a ausência de um PDI- Plano de Desenvolvimento Institucional, visto que este plano encontra-se vigente de 2015 a 2019, o que permite realizar o alinhamento do Plano Diretor de TI com o Plano de Desenvolvimento Institucional. No entanto, de acordo com o Guia de PDTI do Sistema de Administração dos Recursos de Tecnologia da Informação- SISP, além do PDTI ser alinhado às metas da organização, deve ser alinhado ao período de execução. Se for considerado que o PDI da UFRB tem vigência de 2015 a 2019 e que estamos em meados de 2018 e ainda não foi elaborado o PDTI, quando da sua elaboração pode haver um descompasso que acarrete dificuldades no acompanhamento da execução e do alcance das metas de TI e a comparação com os objetivos do planejamento estratégico.

Do mesmo modo, ainda não foi elaborado o Plano Estratégico de TI (PETI), que também deve ser alinhado ao Plano de Desenvolvimento Institucional O ultimo PETI elaborado foi referente ao ano de 2012 a 2014 e apresentava os objetivos estratégicos e as metas a serem atingidas para cada objetivo, quanto a isso a COTEC informou que a ação de elaboração do PETI depende de uma visão estratégica e que ainda não há uma definição por parte da gestão de TI se o mesmo será incluído no PDTI ou se será um documento a parte.

Outro quesito que teve a classificação *não adota* foi a avaliação periódica dos sistemas de informação e avaliação de desempenho, o que se constitui em risco para a gestão de TI, pois uma vez que os sistemas e os serviços não são avaliados não é possível mensurar a sua qualidade e realizar possíveis melhorias e sanar as falhas identificadas pelos usuários.

Inclusive, estava previsto para 2016 uma pesquisa de levantamento das necessidades dos usuários para identificar as demandas dos usuários do serviço, no entanto até o momento atual esta pesquisa ainda não foi realizada. Conforme resposta a SA n°240/2018, a pesquisa não foi realizada por questões orçamentárias e estratégicas, e que foi solicitado aos técnicos dos Centros de Ensino este levantamento com apresentação por *webconf* para PROPLAN, no entanto foi cancelada decorrente de problemas elétricos, mas há a previsão de realização desse levantamento ainda em julho do ano corrente. .

Essas avaliações possibilitam a identificação de gargalos e uma maior eficiência nos processos informatizados visando atender as expectativas dos usuários, o que pode ser feito inclusive por meio de softwares específicos. O fato da Universidade ser Multicampi coaduna com esta necessidade pois, muitas vezes pelo distanciamento da Reitoria e da Coordenadoria de Tecnologia da Informação, a COTEC não conheça as demandas dos Centros.

A própria ausência de um PDTI e de um PETI implica em dificuldades para a avaliação de desempenho de TI, visto que se não há formalização das metas e objetivos a serem atingidas na área de TI não é possível se ter parâmetros para comparar os resultados apresentados numa pesquisa de satisfação, por exemplo, com um cenário requerido, não sendo possível avaliar os serviços de TI. Então uma questão acaba culminando em outra, a limitação de atuação do comitê de governança digital implica na não elaboração do PDTI e do PETI e consequentemente na ausência avaliação dos sistemas de informação e da avaliação do desempenho dos serviços de TI.

MANIFESTAÇÃO DA UNIDADE AUDITADA

Sobre a elaboração do PDTI: Uma proposta/minuta do plano esta sendo analisada pela Pro-reitoria de Planejamento para verificação da capacidade orçamentaria da instituição e posterior debate junto a Reitoria.

Sobre a ausência de um PETI: A proposta de criação do PDTI, conforme guia de elaboração do STI/MPDG, já engloba elementos de nível estratégico e tático tornando desnecessária a confecção do PETI.
Link para minuta do PDTI - https://arquivos.ufrb.edu.br/index.php/s/Kt0SwPb2fsj6zqo

- **Análise da Auditoria Interna**

Conforme resposta da unidade auditada, há uma proposta de elaboração do PDTI, a qual foi enviada para esta auditoria, o que confirma a necessidade de elaboração desse plano. Como já há iniciativas da gestão de TI no que concerne a elaboração desse plano, resta a apenas análise junto à pro-reitoria de planejamento e da Reitoria para finalização. Ademais, a unidade auditada não se manifestou no tocante a atuação do comitê de Governança Digital e a avaliação dos serviços de Tecnologia da Informação. Deste modo, a constatação será mantida para acompanhamento posterior através do plano de providência da auditoria interna.

RECOMENDAÇÃO 17
Recomenda-se que haja um maior envolvimento do comitê de Governança Digital no desenvolvimento e priorização de ações de TI

RECOMENDAÇÃO 18
Recomenda-se o desenvolvimento de ações para finalizar a elaboração do PDTI- Plano Diretor de Tecnologia da Informação.

RECOMENDAÇÃO 19
Recomenda-se que seja realizada avaliação dos serviços de Tecnologia de Informação pela comunidade acadêmica

Cruz das Almas, 07/08/2018

Aline Barbosa de Oliveira
Auditoria Interna
Matrícula SIAPE 2323921

Ciente em ___/___/_____
Simea Azevedo Brito Borges
Matrícula SIAPE
Chefe da Auditoria Interna