UNIVERSIDADE FEDERAL DA FRONTEIRA SUL

Relatório Final de Auditoria nº 01 – Governança de TIC

Ano 2024

QUAL FOI O TRABALHO REALIZADO?

Essa ação de auditoria analisou a estrutura de governança de TIC quanto aos controles internos essenciais de governança de TIC. Foram analisados os instrumentos, definidos pela SETI, para a governança, especificamente através do PDTIC, POSIC, PTD, conforme objetivos propostos e critérios de auditoria estabelecidos no Programa de Auditoria. Ainda, verificou-se a existência, aprovação e vigência do PDA, bem como a atuação do Comitê de Governança Digital, do Comitê de Segurança da Informação ou estrutura equivalente, do Gestor de Segurança da Informação e da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, além da maturidade da estrutura de controle internos e gestão de riscos de TIC.

POR QUE O TRABALHO FOI REALIZADO?

Considerada a matriz de riscos aplicada na elaboração do Paint/2023 o tema "Gestão de Demandas de TI" ficou classificado como um tema de maior risco, entretanto, a partir da análise preliminar, constatou-se ausência de adequada maturidade em relação à Governança de TIC, ainda que a SETI possua um Setor de Governança de TI (SGTI). Tomando com principal motivador os marcos regulatórios que demandam sobre a Governança de TI, observou-se que a UFFS apresenta fragilidades em relação ao cumprimento da legislação que orienta as ações de TI relacionadas à governança e, consequentemente, apresenta fragilidades nos processos que dependem de adequada governança, como é o caso do processo Gestão de demandas de TI. Assim, a proposta de ação de auditoria em "Gestão de Demandas de TI" passa a ser substituída pela ação "Governança de TIC", dada a dificuldade da avaliação da Gestão das Demandas de TI, sem que esteja implementada a Governança de TI.

QUAIS AS CONCLUSÕES ALCANÇADAS?
QUAIS RECOMENDAÇÕES FORAM EMITIDAS?

Na análise realizada, observados os critérios de avaliação definidos no escopo desta auditoria e, consideradas as documentações e informações disponibilizadas pela SETI e/ou através de consulta ao *site* da UFFS, encontrou-se fragilidades no processo de Governança de TIC, as quais são apresentadas neste relatório.

Destaca-se que tais fragilidades relacionadas à governança de TIC levam a um "apetite ao risco".

Ainda, observou-se a ausência de Mapeamento de Processos e Gestão de Riscos da área de TIC alinhada à Política de Gestão de Riscos e às normativas e diretrizes para a TIC, muito embora existam documentos e guias internos.

Observou-se, ainda, que os controles internos administrativos, referentes ao tema auditado, encontram-se em um nível básico de maturidade. Ou seja, o nível indica falha de controle, causando irregularidades que exigem imediata ação corretiva (risco alto).

As constatações/recomendações à gestão, bem como informações em destaque, encontram-se no item II deste relatório – Resultado dos Exames.

Sumário

I – INTRODUÇÃO

O presente trabalho trata dos resultados da auditoria em Governança de TIC da Universidade Federal da Fronteira Sul (UFFS).

O escopo desta auditoria se limitou à verificação da estrutura de governança de TIC, quanto aos controles internos essenciais de governança de TIC.

Foram analisados os instrumentos, definidos pela Seti, para a governança de tecnologia da informação, especificamente através do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), da Política de Segurança da Informação e Comunicações (POSIC) e do Plano de Transformação Digital (PTD), conforme objetivos propostos e critérios de auditoria estabelecidos no programa. Ainda, foi verificado o Plano de Dados abertos (PDA) quanto à sua criação pela unidade competente, aprovação pelo Comitê de Governança Digital, além da vigência.

Em relação ao Comitê de Governança Digital (Decreto nº 10.332 de 28 de abril de 2020 e Guia de Governança de TIC do SISP), ao Comitê de Segurança da Informação ou estrutura equivalente, à nomeação de Gestor de Segurança da Informação e à nomeação da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (Decreto nº 9.637, de 26 de dezembro de 2018), foram verificadas suas aprovações/nomeações pelo órgão/pessoa competente(s), além das vigências.

A maturidade da estrutura de controles internos e gestão de riscos de TIC foi avaliada através do Questionário de Avaliação de Controles Internos (QACI), da verificação da existência de mapeamentos de processos, gestão de riscos e outros instrumentos de controle analisados, conforme os objetivos propostos.

De acordo com os objetivos e questões de auditoria, estabelecidos no programa, não foi necessária determinação de amostra.

Essa ação de auditoria contou com o **objetivo geral** de verificar a adequação dos controles internos essenciais à gestão e governança de TIC, buscando-se conformidade com os marcos regulatórios que afetam a sua atuação.

Como **objetivos específicos**:

1. Verificar se os instrumentos, definidos pela Seti, para governança de tecnologia da informação, considerando-se o PDTIC, a POSIC e o PTD da UFFS existem, encontram-se vigentes e foram aprovadas pelos órgãos competentes.
2. Verificar se o PDTIC, caso vigente, encontra-se alinhado ao Plano de Desenvolvimento Institucional (PDI).

3. Verificar se o PDTIC, a POSIC e o PTD da UFFS estão alinhados minimante aos normativos externos correspondentes.

4. Verificar, conforme o art. 3º do Decreto nº 10.332, de 28 de abril de 2020, se o PDA existe, encontra-se vigente e aprovado pelo órgão competente.

5. Verificar como se encontra a atuação do Comitê de Governança Digital, do Comitê de Segurança da Informação ou estrutura equivalente, do Gestor de Segurança da Informação e da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos.

6. Verificar a maturidade da estrutura de controles internos e gestão de riscos de TIC.

Para atender aos objetivos do trabalho foram estabelecidas as seguintes **questões de auditoria**:

1. Os instrumentos, definidos pela Seti, para a governança de tecnologia da informação e comunicação, considerando-se o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), a Política de Segurança de Informação e Comunicação (POSIC) e o Plano de Transformação Digital (PTD), existem e encontram-se vigentes e aprovadas pelos órgãos competentes?

2. O PDTIC está alinhado ao Plano de Desenvolvimento Institucional (PDI)?

3. Os instrumentos, definidos pela Seti, para governança de tecnologia da informação (PDTIC – POSIC e PTD) da UFFS, estão minimamente alinhados aos normativos externos correspondentes?

4. Considerado o art. 3º do Decreto nº 10.332, de 28 de abril de 2020, além do PDTIC, da POSIC e do PTD, existe Plano de Dados Abertos (PDA) e este se encontra vigente e aprovado pelo órgão competente?

5. Como se encontra a atuação do Comitê de Governança Digital, do Comitê de Segurança da Informação ou estrutura equivalente, do Gestor de Segurança da Informação e da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos?

6. Como se encontra a maturidade da estrutura de controles internos e gestão de riscos de TIC?

Para a inspeção foram realizados os seguintes **procedimentos e técnicas de auditoria**:

- Indagações informais, através de reunião via *Meet* e conversas de *WhatsApp*.
- Indagação escrita/formal – Solicitações de Auditoria (Processo 23205.008428/2024-85) e e-mail.
- Consulta no *site* da UFFS.

- Análise Legislativa e Normativa.
- Análise documental através dos registros institucionais apresentados.

A análise documental ocorreu de forma cem por cento digital, através do *site* da UFFS, de processo de solicitações de auditoria e respostas a estas, bem como resposta à e-mail, além de documentos disponibilizados no Sipac/Mesa Virtual.

A avaliação ocorreu através da análise documental e/ou de informações repassadas pela gestão, confrontando-as com a legislação e normativas vigentes.

Além da análise de conformidade com a legislação e normativos específicos, analisou-se o ambiente e as atividades de controles internos administrativos (atividades, rotinas e procedimentos interligados), bem como a existência ou não da formalização da gestão de riscos dos processos de governança de TIC.

II – RESULTADOS DOS EXAMES

1. Constatações

Constatação 01 – Documentos Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) e Política de Segurança de Informação e Comunicação (POSIC) com vigência expirada ou sem revisão/atualização

Fato

Em análise, observou-se que os documentos PDTIC (2019 a 2021 – Versão 1.0 – Dezembro de 2019) e POSIC (Última POSIC publicada em 09/03/2018) estão com a vigência expirada ou sem revisão/atualização.

Quanto ao PDTIC, o último documento publicado tem vigência de 2019 a 2021 (Versão 1.0 – Dezembro de 2019).

Quanto à POSIC, o último documento foi publicado em 09/03/2018.

Causa/Critério/Consequência

A causa desta constatação se deve às falhas na observância da legislação e normativas aplicáveis, aliado a fragilidades no controle interno institucional.

Como critério de análise do PDTIC, foi verificada a legislação, em especial o Decreto nº 10.332, de 28 de abril de 2020 (Art. 3º – II) e alterações, a Portaria nº 778, de 4 de abril de 2019 (implantação da Governança de Tecnologia da Informação e Comunicação nos órgãos e entidades pertencentes ao Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal – SISP) e alteração, bem como a Instrução Normativa PR/GSI nº 1, de 27 de maio de 2020, em comparativo com o documento.

Como critério de análise da POSIC, destaca-se a verificação do Decreto nº 9.637, de 26 de

dezembro de 2018 (institui a Política Nacional de Segurança da Informação) e da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 (Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal), em comparativo com o documento.

Na análise, verificou-se que:

Quanto ao PDTIC, de acordo com a Portaria nº 778, de 4 de abril de 2019, o documento deve *"VI – ter vigência mínima de dois anos com revisão anual"*. Ainda, conforme informação constante na página da UFFS, seu período de validade é de três anos, sendo que a cada ano são feitas até duas revisões, dependendo da necessidade de adequações do documento.

Quanto à POSIC, segundo a Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, Art. 12. VII - § 1º *"[...] A periodicidade para a revisão da Política de Segurança da Informação não deve exceder 4 (quatro) anos"*. Ainda, de acordo com o § 2º *"A Política de Segurança da Informação, quando necessário, deve ser complementada por normas, metodologias e procedimentos"*. Ademais, a Portaria nº 216/GR/UFFS/2018, Art. 33, estabelece que *"Os Instrumentos normativos gerados a partir da POSIC/UFFS, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 03 (três) anos"*.

A ausência de vigência/revisão/atualização dos documentos fragiliza o processo de governança de TIC, além de fragilizar as diversas áreas da UFFS, uma vez que a TI é um importante parceiro estratégico institucional por possuir transversalidade em áreas-chave da instituição.

Quando o órgão não observa as leis e normas a serem seguidas e/ou não tem controles internos bem estruturados para atender aos princípios de governança de TIC, aumentam-se os riscos em sua atuação.

Constatação 02 – Documento Plano de Transformação Digital (PTD) em desacordo com a legislação

Fato[1]

Na página da UFFS consta o documento PTD com vigência para o período de 2020 a 2022, entretanto, a publicação da Versão 1.1 ocorreu somente em maio de 2022. Acrescenta-se ao fato, que os documentos de monitoramentos, apresentados pela Seti, possuem data inicial em janeiro de 2022 (anterior à publicação do PTD).

Documento sem revisão/atualização a partir da publicação do Decreto nº 11.260, de 22 de novembro de 2022, sobretudo quanto ao acréscimo da ação "Segurança e Privacidade".

Documento com equívocos textuais, principalmente quanto à padronização dos termos utilizados nas tabelas.

Documento sem referenciação de siglas no campo "Ação", constante na primeira coluna do item "XI – Ações previstas".

Inexistência de documento de aprovação do PTD pelo Comitê de Governança Digital.

Inexistência, no documento, de definição de estratégias de monitoramento das ações do PTD, pactuadas com a Secretaria Especial de Modernização do Estado da Secretaria-Geral da Presidência da República.

Documento, apontado como válido pela gestão, sem formalização da prorrogação de vigência.

Causa/Critério/Consequência

A causa desta constatação se deve às falhas na observância da legislação aplicável, além de falhas na observância das boas práticas de governança de TIC, aliado a fragilidades no controle interno institucional.

Como critério de análise foi verificada a legislação aplicável, em especial a Lei nº 14.129, de 29 de março de 2021 (Lei do Governo Digital) e o Decreto nº 10.332, de 28 de abril de 2020, alterado pelos decretos 10.996, de 14 de março de 2022 e 11.260, de 22 de novembro de 2022 (institui a Estratégia de Governo Digital). Ainda, observou-se as orientações constantes no

[1] Analisado apenas o PTD, mesmo que o documento se encontre com a vigência expirada e a gestão da Seti tenha afirmado, em resposta ao Ofício nº 37/2023 – AUDIN, de 26/07/2023 (Processo Sipac 23205.021631/2023-66), quando da análise preliminar, que *"O Plano de Transformação Digital faz parte da Estratégia de Governo Digital é uma ação continuada, está em fase de elaboração o novo plano em conjunto entre UFRN e Cooperadas, a UFFS está entre estas IFES. Previsão de publicação até, 31 de outubro de 2023"*. Isso porque a gestão alegou, em resposta à SA 02/2024-AUDIN (de 02/04/2024) e SA 04/2024-AUDIN (de 16/04/2024) que "[…] é o documento vigente até a implantação dos módulos participantes da integração", que *"[...] a conclusão das ações do PTD 2020-2022 continua dependendo da implantação de módulos do sistema"* e, que, *"[...] Entre novembro de 2022 e março de 2023, o PTD 2.0 esteve em negociação, onde novos serviços seriam integrados ao Gov.br. Contudo, o novo governo optou por não priorizar isto e o projeto foi abandonado. Considerando que o projeto com a UFRN não teve continuidade em 2023, as ações previstas não foram alteradas. Por esse motivo, acredito que a gestão anterior não criou um novo PTD para a UFFS"*.

Guia de Governança de TIC do SISP – v 2.0.

O PTD carece de coerência em relação às datas de vigência e monitoramentos ou, esclarecimento em relação ao desencontro, além revisão/atualização sempre que surgirem novas legislações e/ou necessidades advindas de adequações no caminho seguido ou de falhas textuais observadas no documento. Para além, é necessária a definição de estratégias de monitoramento das ações do PTD, pactuadas com a Secretaria Especial de Modernização do Estado da Secretaria-Geral da Presidência da República (Decreto nº 10.332, de 28 de abril de 2020, Art. 3º § 3º), bem como, documento de aprovação pelo Comitê de Governança Digital (Decreto nº 10.332, de 28 de abril de 2020, Art. 3º § 1º – II). Finalmente, considerado o entendimento exposto pela Seti de que o documento é prorrogável e, havendo base legal e normativa para fundamentar o entendimento, é necessária a prorrogação formal.

Assim, o PTD precisa estar em conformidade com a legislação, a fim do bom andamento do processo de transformação digital da UFFS, cujo eixo central direciona para a simplificação dos relacionamentos das pessoas com a instituição, a partir da transformação do ambiente digital que conhecemos em um cenário ainda mais intuitivo, interativo e agradável. Feito isso, faz-se necessário um ambiente de controle interno administrativo adequado, com atividades de controle capazes de gerenciarem os riscos do processo.

A ocorrência de falhas nas tarefas principais (avaliar, direcionar, monitorar) para a boa governança da TIC, aumentam os riscos de contratempos na construção de uma UFFS eficiente, confiável, transparente e aberta à sociedade.

Constatação 03 – Ausência de regimento interno, de atas das reuniões do Comitê de Governança Digital e desatualização da Portaria nº 1035/GR/UFFS/2017

Fato

Inexistência de regimento interno do Comitê de Governança Digital, de registros das reuniões ocorridas em 2023 e desatualização da Portaria nº 1035/GR/UFFS/2017 ao citar o Decreto 8.638, de 15 de janeiro de 2016, o qual já foi revogado pelo Decreto nº 10.332, de 28 de abril de 2020.

Causa/Critério/Consequência

A causa da ausência se deve à inobservância da legislação e normativas, aliada às fragilidades no controle interno institucional.

Como critério de análise foi verificada a página da UFFS em relação à legislação e normativas, bem como, solicitação de informações à Seti.

É orientação da Portaria nº 1035/GR/UFFS/2017, Art. 5º, que *"O regimento interno definirá*

as regras de funcionamento do CGD". Outrossim, no Guia de Governança de TIC do SISP – v 2.0 consta a orientação de que o Comitê possua regimento interno e confeccione as atas de reunião do Comitê. Ademais, entende-se como boa prática o cuidado e constante atualização dos documentos internos.

Tal estratégia auxilia no ambiente de controle interno administrativo e beneficia a atuação do Comitê de Governança Digital, diminuindo os riscos em sua atuação.

Constatação 04 – Ausência de ato que defina a forma de funcionamento do Comitê de Segurança da Informação e desatualização da portaria de designação dos membros

Fato

Em análise à página da UFFS não foi encontrado ato que defina a forma de funcionamento do Comitê de Segurança da Informação. Ainda, a portaria de designação dos membros encontra-se desatualizada[2].

Causa/Critério/Consequência

A causa das falhas se deve à inobservância da legislação, aliada às fragilidades do controle interno institucional.

Como critério de análise foi verificada a página da UFFS em relação à legislação, qual seja, o Art. 16 do Decreto 9.637, de 26 de dezembro de 2018, que rege para que *"Os órgãos e as entidades da administração pública federal editarão atos para definir a forma de funcionamento dos respectivos comitês de segurança da informação, observado o disposto neste Decreto e na legislação"*, bem como, solicitação de informações à Seti.

O Comitê carece, por força da legislação, de definição de sua forma de funcionamento. Ademais, é importante a atualização constante da portaria de designação dos membros.

Tais fatos fragilizam a atuação do Comitê de Segurança da Informação e aumentam os riscos na atuação.

Constatação 05 – Ausência de Mapeamento de processos de TIC

Fato

Segundo resposta da Seti à Solicitação de Auditoria nº 05/2024 – AUDIN, não há processo mapeado homologado. Também, em consulta ao *site* oficial da UFFS (www.uffs.edu.br > Acesso a Informação > Transparência e Prestação de Contas > Administrativo > Mapa de Processos), não se encontrou mapas de processos institucionalizados.

---

[2] Conforme resposta da própria gestão em resposta à SA Nº 03-2024 – AUDIN.

Causa/Critério/Consequência

A causa desta constatação se deve às falhas na observância das normas aplicáveis, em especial às relacionadas à governança de TIC, à Política de gestão de Riscos e Controles Internos da UFFS e Plano de Gestão de Riscos e Controles Internos da UFFS, aliado a fragilidades no controle interno institucional.

Os conceitos traduzidos/apresentados pelo COSO I, os Princípios de Gestão e Governança Pública, a Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016 (que dispõe sobre os controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal), a Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021, o Decreto nº 9.637, de 26/12/2018 em seu artigo 17, incisos V, VII, VIII e § 2º e o Guia de Governança de TIC do SISP v 2.0, enfatizam a necessidade de gerenciamento de riscos, o que, na UFFS, é realizado a partir do mapeamento de processos.

Ainda, de acordo com a Política de Gestão de Riscos da UFFS, no Art. 8° *"A operacionalização da Gestão de Riscos deverá partir do mapeamento de riscos referentes aos objetivos institucionais da UFFS, presentes no Plano de Desenvolvimento Institucional (PDI)"*. Finalmente, para mais do que documentar, perpetuar e difundir o conhecimento sobre como o trabalho é realizado, padronizar a execução das atividades, agir em conformidade com as normas e ser transparente, o mapeamento de processos tem as finalidades de racionalizar a tomada de decisões, definir papéis e responsabilidades, realizar avaliação de riscos de forma mais eficaz, gerenciar competências, suportar treinamentos e capacitações, analisar o processo para o seu gerenciamento e estabelecer padrões de busca de melhoria contínua.

A ausência do mapeamento dos principais processos da área de TIC fragiliza a ação da TI e da instituição como um todo.

Constatação 06 – Ausência de Gestão de Riscos de TIC

Fato

Segundo resposta da Seti à Solicitação de Auditoria nº 05/2024 – AUDIN, existe uma gestão de riscos devidamente formalizada, submetida à análise do Comitê de Governança, Riscos e Controles da UFFS. Ademais, em consulta ao *site* oficial da UFFS/Comitê de Governança, Riscos e Controles, não se encontrou mapa de riscos e/ou informações que subsidiassem a realização de gerenciamento dos riscos de TIC. Logo, não ficou evidenciada aplicação da política de gestão de riscos aos processos de TIC.

Causa/Critério/Consequência

A causa desta constatação se deve às falhas na observância das normas aplicáveis, em especial

às relacionadas à governança de TIC, aliado a fragilidades no controle interno institucional. Os conceitos traduzidos/apresentados pelo COSO I, os Princípios de Gestão e Governança Pública, a Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016 (que dispõe sobre os controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal), a Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021, o Decreto nº 9.637, de 26/12/2018 em seu artigo 17, incisos V, VII , VIII e § 2º e o Guia de Governança de TIC do SISP v 2.0, enfatizam a necessidade de gerenciar riscos, uma vez que são inerentes a qualquer atividade e, assim, o ideal é que haja a identificação dos riscos da atividade e o seu gerenciamento.

O gerenciamento de riscos provê as ferramentas necessárias para planejar, identificar, qualificar, quantificar, responder e monitorar os riscos, sendo apropriado a todos os processos. Conhecer os riscos e saber identificá-los como positivos ou negativos fará um grande diferencial no seu tratamento.

Uma gestão de riscos ineficiente pode afetar na tomada de decisões e, consequentemente, maximizar as perdas e diminuir os ganhos. Por isso, deve-se assegurar que a gestão de riscos seja implementada e incorporada para apoio à melhoria contínua dos processos de TIC da UFFS.

Constatação 07 – Geral– Falhas na transparência ativa

Fato

Em consulta à página da Seti, bem como no espaço “Acesso à informação”, observou-se falhas na publicação da totalidade dos documentos produzidos pela Seti, a exemplo de instruções, informações, portarias de aprovação, constituição e designação e demais documentos que tratem da atuação da Seti em relação ao PDTIC, POSIC, PTD, PDA, Comitê de Governança Digital, Comitê de Segurança da Informação ou estrutura equivalente, Gestor de Segurança da Informação e Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos.

Causa/Critério/Consequência

A causa desta constatação se deve às falhas na observância das normas aplicáveis, em especial às relacionadas à publicidade e transparência, aliado a fragilidades no controle interno institucional.

Como critério de análise foi verificada a página da UFFS (Seti e Acesso à informação) em relação à legislação, em especial ao estabelecido na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à informação), a qual rege que todas as informações de interesse público de-

vem ser publicadas. Ainda, a edição da Estratégia de Governo Digital (EGD) para o período de 2020 a 2022, enfatiza a transparência ao afirmar que *"o desempenho, os custos, riscos e resultados das ações empreendidas pela área de TIC deverão ser medidos pela função de gestão de TIC e reportados à alta administração da organização e à sociedade por meio de canais de comunicação adequados, provendo transparência à aplicação dos recursos públicos em iniciativas de TIC e propiciando amplo acesso e divulgação das informações (grifo nosso)"*.

Pelo exposto, destaca-se que, além da obrigatoriedade da disponibilização da totalidade das informações, é necessário que a divulgação seja feita de forma organizada, detalhada e de fácil localização e compreensão, ou seja, não basta que as informações estejam publicadas/divulgadas, é preciso que estejam transparentes.

As falhas na transparência ativa dificultam a participação popular e o controle social, podendo gerar a busca pela transparência passiva.

2. Recomendações

A seguir, apresentam-se as recomendações da auditoria, as quais, após a emissão deste relatório, iniciam processo de monitoramento. Assim, estabelece-se como **data limite do monitoramento deste relatório o dia 29/11/2024**.

Para o monitoramento das recomendações, a auditoria interna entrará em contato com a gestão, a fim de apresentar o sistema de monitoramento (e-Aud) e orientar como utilizá-lo para a emissão de manifestação em relação às recomendações aqui relatadas.

É de responsabilidade da unidade auditada o cumprimento das recomendações emitidas pela Audin, ou, então, a aceitação formal do risco correspondente, caso decida não implementá-las (assunção de riscos). No caso de optar pela não implementação da recomendação/assunção de riscos, esta opção deve ser comunicada à Audin através da manifestação do gestor no sistema e-Aud.

Recomendação 01 – corretiva – Constatação 01 (monitoramento 29/11/2024)

Confeccionar novo PDTIC, alinhado ao PDI e aos normativos externos correspondentes (Decreto nº 10.332, de 28 de abril de 2020 (Art. 3º – II), Portaria nº 778, de 4 de abril de 2019, Instrução Normativa PR/GSI nº 1, de 27 de maio de 2020 e informação constante na página da Seti, espaço PDTIC), aprovando-o pelo órgão competente (Decreto nº 10.332, de 28 de abril de 2020 (Art. 3º – II, § 1º II).

Quando do monitoramento desta auditoria, devem ser apresentadas as ações referentes ao recomendado.

Recomendação 02 – corretiva – Constatação 01 (monitoramento 29/11/2024)

Revisar/atualizar a POSIC, alinhando-a aos normativos externos correspondentes (Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, Art. 12. VII - § 1º e § 2º, Portaria nº 216/GR/UFFS/2018, Art. 33) e aprovando-a pelo órgão competente (Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, Art. 9º).

Quando do monitoramento desta auditoria, devem ser apresentadas as ações referentes ao recomendado.

Recomendação 03 – estruturante – Constatação 02 (monitoramento 29/11/2024)

Revisar o PTD, retificando os equívocos textuais, adequando/atualizando-o à legislação e normativas (Lei nº 14.129, de 29 de março de 2021, Decreto nº 10.332, de 28 de abril de 2020, alterado pelos decretos 10.996, de 14 de março de 2022 e 11.260, de 22 de novembro de 2022 e as orientações constantes no Guia de Governança de TIC do SISP – v 2.0.) e acrescentando a definição de estratégias de monitoramento das ações, pactuadas com a Secretaria Especial de Modernização do Estado da Secretaria-Geral da Presidência da República.

Quando do monitoramento desta auditoria, devem ser apresentadas as ações referentes ao recomendado.

Recomendação 04 – estruturante – Constatação 02 (monitoramento 29/11/2024)

Após a revisão do PTD, efetuar a aprovação formal pelo Comitê de Governança Digital, bem como, prorrogar a sua vigência, formalmente.

Quando do monitoramento desta auditoria, devem ser apresentadas as ações referentes ao recomendado.

Recomendação 05 – estruturante – Constatação 03 (monitoramento 29/11/2024)

Atender aos atos administrativos e às diretrizes do Sistema de Administração dos Recursos de Tecnologia da Informação (Portaria nº 1035/GR/UFFS/2017, Art. 5º e Guia de Governança de TIC do SISP – v 2.0), confeccionando o regimento interno do Comitê de Governança Digital.

Quando do monitoramento desta auditoria, devem ser apresentadas as ações referentes ao recomendado.

Recomendação 06 – estruturante – Constatação 03 (monitoramento 29/11/2024)

Atender à diretriz estabelecida no Sistema de Administração dos Recursos de Tecnologia da Informação (Guia de Governança de TIC do SISP – v 2.0), confeccionando as atas de registro

das reuniões do Comitê de Governança Digital.
Quando do monitoramento desta auditoria, devem ser apresentadas as ações referentes ao recomendado.

Recomendação 07 – corretiva – Constatação 03 (monitoramento 29/11/2024)
Atualizar a Portaria nº 1035/GR/UFFS/2017.
Quando do monitoramento desta auditoria, devem ser apresentadas as ações referentes ao recomendado.

Recomendação 08 – corretiva – Constatação 04 (monitoramento 29/11/2024)
Atender à legislação (Art.16 do Decreto nº 9.637, de 26 de Dezembro de 2018), confeccionando ato que defina a forma de funcionamento do Comitê de Segurança da Informação.
Quando do monitoramento desta auditoria, devem ser apresentadas as ações referentes ao recomendado.

Recomendação 09 – corretiva – Constatação 04 (monitoramento 29/11/2024)
Atualizar a Portaria N° 2331/GR/UFFS/2022, a qual designa (Art.15, IV, do Decreto 9.637, de 26 de Dezembro de 2018) os membros do Comitê de Segurança da Informação.
Quando do monitoramento desta auditoria, devem ser apresentadas as ações referentes ao recomendado.

Recomendação 10 – estruturante – Constatação 05 (monitoramento 29/11/2024)
Confeccionar e publicar o mapeamento dos principais processos da área de TIC, com alinhamento às normas específicas de TIC (COSO I, os Princípios de Gestão e Governança Pública, a Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016, a Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021, o Decreto nº 9.637, de 26/12/2018 em seu artigo 17, incisos V, VII, VIII e § 2º e o Guia de Governança de TIC do SISP v 2.0) quanto ao tema e, com alinhamento às diretrizes institucionais da UFFS quanto ao mapeamento de processos.
Quando do monitoramento desta auditoria, devem ser apresentadas as ações referentes ao recomendado.

Recomendação 11 – estruturante – Constatação 06 (monitoramento 29/11/2024)
Aplicar a Gestão de Riscos da área de TIC, alinhada à Política de Gestão de Riscos da UFFS,

observando as normativas e diretrizes para a TIC quanto ao tema.
Quando do monitoramento desta auditoria, devem ser apresentadas as ações referentes ao recomendado.

Recomendação 12 – estruturante – Geral (monitoramento 29/11/2024)
Atender à legislação (Lei nº 12.527, de 18 de novembro de 2011) e a edição da Estratégia de Governo Digital (EGD) para o período de 2020 a 2022, procedendo à publicização, de forma transparente, da totalidade dos documentos que tratam da atuação da Seti em relação ao PDTIC, POSIC, PTD, PDA, Comitê de Governança Digital, Comitê de Segurança da Informação ou estrutura equivalente, Gestor de Segurança da Informação e Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos.
Quando do monitoramento desta auditoria, devem ser apresentadas as ações referentes ao recomendado.

3. Informações

Informação 01 – Quanto à verificação do **alinhamento do PDTIC, caso vigente, ao Plano de Desenvolvimento Institucional (PDI)**, uma vez que o PDTIC se encontra com a vigência expirada (vigência de 2019 a 2021 – Versão 1.0 – Dezembro de 2019), conforme análise na página da UFFS e confirmação pela Seti[3] bem como o PDI (período de 2019 a 2023), não foi realizada a verificação do alinhamento do PDTIC ao PDI.

Informação 02 – Quanto à verificação se o **Plano de Dados Abertos (PDA) existe, está vigente e foi aprovado pelo órgão competente (Comitê de Governança Digital)**, observou-se que o PDA foi elaborado e aprovado pelo Reitor (conforme Art. 6º da Resolução nº 3, de 13 de outubro de 2017 – *"Os Planos de Dados Abertos deverão ser aprovados e instituídos pelo dirigente máximo do órgão ou entidade e publicados em transparência ativa, na seção 'Acesso à Informação' do sítio eletrônico de cada órgão [...]"*), bem como, encontra-se vigente (julho de 2023 a julho de 2025, conforme Art. 3º da Resolução nº 3, de 13 de outubro de 2017 – *"Os PDAs devem ter vigência de dois anos, a contar da publicação"*). Ainda, o documento está publicado, bem como a Portaria de aprovação (Portaria nº 2937/GR/UFFS/2023).

[3] SA Nº 02-2024 – AUDIN.

Informação 03 – Quanto à verificação se o **PDTIC, a POSIC e o PTD da UFFS estão alinhados minimante aos normativos externos correspondentes e foram aprovados pelos órgãos competentes**, uma vez que os documentos PDTIC e POSIC encontram-se com a vigência expirada ((PDTIC com vigência de 2019 a 2021 – Versão 1.0 – Dezembro de 2019, POSIC com a última publicação em 09/03/2018)), não foi realizada a análise do alinhamento dos documentos aos normativos externos correspondentes, nem verificada a aprovação pelos órgãos competentes.

III – CONCLUSÃO

Na análise realizada, observados os critérios de avaliação definidos no escopo desta auditoria, consideradas as documentações e informações disponibilizadas pela Seti e/ou no *site* institucional, encontrou-se evidências de fragilidades quanto à governança de TIC.

Quanto às respostas às questões de auditoria:

1. Os instrumentos, definidos pela Seti, para a governança de tecnologia[4] da informação e comunicação, considerando-se o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), a Política de Segurança de Informação e Comunicação (POSIC) e o Plano de Transformação Digital (PTD), existem e encontram-se vigentes e aprovadas pelos órgãos competentes?

Constatou-se que o PDTIC existe, está disponível para a consulta, entretanto, está com vigência expirada (PDTIC 2019-2021). Quanto à POSIC, constatou-se que não ocorreu revisão desde a publicação (2018). Em relação ao PTD, na página da UFFS consta o documento PTD com vigência para o período de 2020 a 2022, documento este, apontado como válido pela gestão e, portanto, efetuada a análise do Critério 3.

2. O PDTIC está alinhado ao Plano de Desenvolvimento Institucional (PDI)?

Constatada a expiração do prazo de validade do documento, ainda em 2021, não foi realizada a análise do alinhamento do documento com o PDI.

3. Os instrumentos, definidos pela Seti, para governança de tecnologia da informação (PDTIC – POSIC e PTD) da UFFS, estão minimamente alinhadas aos normativos externos[5] correspondentes?

---

[4] *"[...] III – governança de TIC: sistema pelo qual o uso atual e futuro de TIC é dirigido e controlado, mediante avaliação e direcionamento, para atender às necessidades prioritárias e estratégicas da organização e monitorar sua efetividade por meio de planos, incluída a estratégia e as políticas de uso de TIC no âmbito da organização; [...]"* (Portaria nº 778, de 4 DE abril DE 2019).

[5] Descritos nos critérios de auditoria deste programa.

Constatado que o PDTIC e a POSIC estão com prazo de vigência expirado, não foi realizada a análise do alinhamento aos normativos externos.

Em relação ao PTD, constatou-se que documento está em desacordo com a legislação.

4. Considerado o art. 3º, do Decreto nº 10.332, de 28 de abril de 2020, além do PDTIC, POSIC e PTD, existe Plano de Dados Abertos (PDA) e este se encontra vigente e aprovado pelo órgão competente?

Observou-se que o PDA está vigente (julho de 2023 a julho de 2025), encontra-se disponível para a consulta (https://www.uffs.edu.br/atos-normativos/portaria/gr/2023-2937) e foi aprovado pelo órgão competente (Portaria nº 2937/GR/UFFS/2023).

5. Como se encontra a atuação do Comitê de Governança Digital, do Comitê de Segurança da Informação ou estrutura equivalente, do Gestor de Segurança da Informação e da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos?

Em relação ao Comitê de Governança Digital, constatou-se que não há registro de um documento que defina o Regimento Interno do Comitê, tampouco atas das reuniões no ano de 2023, além do fato de a Portaria nº 1035/GR/UFFS/2017 estar desatualizada.

No que concerne ao Comitê de Segurança da Informação, constatou-se que não há documentos que definam sua forma de funcionamento e a Portaria n° 2331/GR/UFFS/2022 encontra-se desatualizada.

Em relação ao Gestor de Segurança da Informação, observou-se que o mesmo foi oficialmente designado pela Portaria N° 3259/GR/UFFS/2024 (18/01/2024).

Sobre a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos, observou-se que a mesma foi estabelecida pela Portaria n° 2535/GR/UFFS/2022 e os membros designados pela Portaria n° 2536/GR/UFFS/2022, com alterações feitas pela Portaria n° 2631/GR/UFFS/2023. As atribuições da ETIR estão descritas em sua Portaria de constituição.

6. Como se encontra a maturidade da estrutura de controle internos e gestão de riscos de TIC?

Em relação à maturidade, tendo em visto o constante nesse relatório, sobre os critérios, sobre a ausência de mapeamento de processos e gestão de riscos formalmente institucionalizados (muito embora existam documentos e guias internos) e através da aplicação do QACI, observou-se que os controles internos administrativos referentes ao tema auditado se encontram em um nível básico de maturidade. Ou seja, indica falha de controle, causando irregularidades que exigem imediata ação corretiva (risco alto).

Pelo exposto até aqui, consideradas as análises quanto aos controles internos administrativos/institucionais estarem adequados de forma a cumprir os objetivos de governança de TIC, ainda que tenham sido citadas formas de controles, este fica fragilizado.

Destaca-se que as atividades de controle são aquelas que, quando executadas a tempo e maneira adequados, permitem a redução ou administração dos riscos, sendo que podem ser de prevenção (como exemplo: segregação de funções, aprovações e/ou autorizações, sistemas informatizados, normativos internos) ou de detecção (como por exemplo: conciliação, revisão de desempenho, sistemas informatizados).

Uma cultura de controle interno e gerenciamento de riscos adequada (formalizada), pauta-se no fato dos servidores e gestores serem conhecedores dos processos, ou seja: servidores e responsáveis sabem o que deve ser feito? Se sim, eles sabem como fazê-lo? Se sim, eles querem e possuem capacidade operacional para fazê-lo?

Aplicado o QACI, observou-se que os controles internos administrativos referentes ao tema auditado se encontram em um nível básico de maturidade. Ou seja, indica falha de controle, causando irregularidades que exigem imediata ação corretiva (risco alto).

No que se refere aos resultados e benefícios desta auditoria, considerando a IN SFC n° 4, de 11 de junho de 2018 (anexo I), entende-se que esta ação de auditoria poderá gerar ***"benefícios não financeiros"***, ou seja, *"benefícios que embora não seja passível de representação monetária, demonstra impacto positivo na gestão de forma estruturante, tal como melhoria gerencial, melhoria nos controles internos e aprimoramento de normativos e processos".* Sendo que, dentro de sua classificação dimensão ***"pessoas, infraestrutura e/ou processos internos"***, venha a afetar os processos de apoio e/ou gerenciais da instituição, com repercussão ***"estratégica",*** onde, o benefício trazido pelas providências a serem adotadas pelo gestor digam respeito às atividades internas e/ou operacionais da unidade examinada, bem como possam gerar alterações institucionais.

Quanto aos resultados e benefícios, sejam estes financeiros ou não financeiros, cabe observar que estes só ocorrem no momento em que a gestão atende as recomendações emitidas pela unidade de auditoria interna.

Por fim, salienta-se que os encaminhamentos e publicações deste relatório de auditoria seguem o fluxo do Mapa de Processo nº 92/EP/UFFS/2022, encaminhando-se esse relatório ao Reitor (através do Sipac/Mesa Virtual), com cópia, através de e-mail, à Secretaria Especial de Tecnologia e Informação. Posteriormente, não havendo restrições de informações, publica-se o relatório e encaminha-se para conhecimento: à CGU (através do e-Aud), ao Concur, ao

Consuni/Capgp, à Pró-Reitoria de Planejamento (responsável pelo apoio ao Comitê de Governança Riscos e Controles) e à Assessoria Especial de Governança e Integridade.

Chapecó, 08 de julho de 2024.

MARISA ZAMBONI PIEREZAN
Chefe da Dataudin

De acordo.

DEISI MARIA DOS SANTOS KLAGENBERG
Auditora-Chefe

Auditoria Interna
Universidade Federal da Fronteira Sul - UFFS
Rodovia SC 484 - Km 02, Fronteira Sul, Chapecó (SC)
Sala 03 (Subsolo) - Prédio da Biblioteca - CEP: 89815-899
WhatsApp Institucional (49) 2049-3131/3132/3144.