



**Ministério da Educação
Universidade Federal de Viçosa
Auditoria Interna**

RELATÓRIO DE AUDITORIA Nº 02/2025:

Avaliação da Governança em Tecnologia da Informação da Universidade
Federal de Viçosa

Processo SEI nº 23114.907656/2025-30



UNIVERSIDADE FEDERAL DE VIÇOSA

Demetrius David da Silva
Reitor

Rejane Nascentes
Vice-Reitora

Marcos Ribeiro Furtado
Secretário de Órgãos Colegiados

Elilce de Figueiredo Rodrigues
Chefe de Gabinete – Reitoria

Equipe da Auditoria Interna

Luís Otávio Pacheco
Auditor Chefe

Érica Monteiro Andrade Barreto
Chefe de Expediente

Aline Xisto Rodrigues
Flávia dos Reis Arruda
Felipe Estevan Cardoso Sarmento
Laís Silva Dias
Maria Olímpia dos Santos Silva
Paula Carolina Santos Lopes

VIÇOSA 2025

Missão

Aumentar e proteger o valor organizacional, fornecendo avaliações, assessoria e conhecimento objetivo baseado em risco, que garantam o aprimoramento da governança pública.

Auditoria Interna Governamental

A auditoria interna governamental é uma atividade independente e objetiva, de avaliação e de consultoria, desenhada para adicionar valor e melhorar as operações da UFV, auxiliando-a a alcançar seus objetivos a partir da aplicação de uma abordagem sistemática e disciplinada, para avaliar e melhorar a eficácia dos processos de gerenciamento de riscos, controles internos e governança.

Avaliação

Consiste na obtenção e na análise de evidências com o objetivo de fornecer opiniões ou conclusões independentes sobre um objeto de auditoria. Objetiva também avaliar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos relativos ao objeto e à UFV, e contribuir para o seu aprimoramento.

Qual foi o trabalho realizado pela Audin?

Avaliou-se os mecanismos de Governança em TI da Universidade Federal de Viçosa, tendo como base o Guia SISP e outros normativos pertinentes ao tema.

Por que o trabalho foi realizado?

Este trabalho foi desenvolvido a partir de uma demanda da Pró-Reitoria de Planejamento e Orçamento (PPO), considerando que a auditoria em Governança de TI constitui um relevante indicador de maturidade, contemplado pelo iESGO-Índice de Governança, Sustentabilidade e Gestão nas Organizações Públicas, com o propósito de aprofundar o conhecimento sobre a situação da governança no setor público e fomentar a adoção de boas práticas.

Ao identificar avanços, lacunas e oportunidades de melhoria, o trabalho possui o potencial de contribuir para o aperfeiçoamento da estrutura de governança da UFV, fortalecendo a transparência, legitimidade e eficiência na gestão das iniciativas de TIC na instituição.

Quais as conclusões alcançadas pela Audin? Quais as recomendações deverão ser adotadas?

A análise da governança de TIC na Universidade Federal de Viçosa evidenciou avanços importantes, como o envolvimento da alta administração com iniciativas de TIC, a atuação do Comitê de Governança Digital (CGD) e a existência de instrumentos normativos que estruturam a estratégia, a priorização de investimentos e a gestão de riscos. Entretanto, identificou-se como pontos de aprimoramento, a organização e transparência das informações sobre comitês, fluxos decisórios, indicadores e portfólio de TIC, de modo a contribuir para o acompanhamento e avaliação das ações.

Em relação ao gerenciamento de risco, a POSIC e o PDTI representam avanços normativos, todavia verificou-se limitada harmonização entre esses instrumentos e a PGRC. Notou-se também que, até o momento das análises, ainda não havia um plano específico de segurança da informação.

As recomendações apresentadas, envolvem a atualização e centralização das informações institucionais, formalização de fluxos decisórios, divulgação de indicadores e resultados, elaboração de planos de gestão de riscos e alinhamento do portfólio de TIC aos objetivos estratégicos.

A adoção dessas medidas contribui para a conformidade em relação aos normativos vigentes e para a consolidação de boas práticas de governança, alinhado ao uso estratégico e eficiente dos recursos públicos e o alcance dos objetivos institucionais.

LISTA DE SIGLAS E ABREVIATURAS

Audin - Auditoria Interna

CGRC - Comitê de Governança, Integridade, Riscos e Controle

CGD- Comitê de Governança Digital

CPGD - Comitê Permanente de Governança de Dados

CSIC - Comitê de Segurança da Informação e Comunicação

CONSU - Conselho Universitário

DGI - Diretoria de Governança Institucional

DTI - Diretoria de Tecnologia da Informação

GUT - Gravidade, Urgência e Tendência

iESGO - Índice de Governança, Sustentabilidade e Gestão nas Organizações Públicas

PDI - Plano de Desenvolvimento Institucional

PDTI - Plano Diretor de Tecnologia da Informação

POSIC - Política de Segurança da Informação e Comunicação

PGRC - Política de Governança, Integridade, Riscos e Controle

PAINT- Plano Anual de Atividades de Auditoria Interna

PPO - Pró-Reitoria de Planejamento e Orçamento

TCU - Tribunal de Contas da União

TIC - Tecnologia da Informação e Comunicação

SA - Solicitação de Auditoria

SISP- Sistema de Administração dos Recursos de Tecnologia da Informação

SEI - Sistema Eletrônico de Informações

UFV - Universidade Federal de Viçosa

Sumário

1. INTRODUÇÃO	1
1.1. Visão geral do objeto	1
2. METODOLOGIA.....	2
3. RESULTADOS DO TRABALHO	4
3.1. Envolvimento da alta administração em ações de TIC com fragilidades na transparência das ações e no desenvolvimento de competências	4
3.2. Especificação dos direitos decisórios de TIC com fragilidade nos fluxos formais de decisão.....	5
3.3. Formalização dos comitês de TIC com fragilidade na comunicação e transparência de suas ações	6
3.4. Fragilidade no gerenciamento de riscos de TIC	8
3.5. Alinhamento das ações de TIC aos objetivos estratégicos com fragilidade na divulgação do portfólio.....	10
3.6. Existência de canais de comunicação com fragilidade na transparência das ações de governança em TIC	11
3.7. Fragilidade no monitoramento e avaliação das ações de TIC.....	11
4. RECOMENDAÇÕES	12
5. CONCLUSÃO.....	14
APÊNDICE A.....	16

1. INTRODUÇÃO

O presente trabalho de avaliação foi desenvolvido em atendimento à Ordem de Serviço nº 7/2025/AIN/RTR, item 1 do quadro 2 de serviços previstos no [Plano Anual de Atividades de Auditoria Interna \(PAINT 2025\)](#) e teve como objetivo avaliar a governança de Tecnologia da Informação e Comunicação (TIC) da Instituição.

Embora inicialmente estivesse prevista a avaliação conjunta da gestão e da governança em TIC, a abrangência dos temas levou à delimitação do escopo apenas à governança, de modo a garantir maior precisão analítica e viabilidade no alcance dos objetivos propostos. A escolha deve-se ao caráter estratégico da governança, que fortalece a gestão ao alinhar-se aos objetivos e metas organizacionais e manter coerência com a cultura institucional.

As questões de auditoria foram estabelecidas com base nos normativos que regulamentam as boas práticas de governança de TIC no setor público, com destaque para o Guia de Governança de TIC do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), do Ministério do Planejamento, Desenvolvimento e Gestão.

Ressalta-se que o trabalho foi conduzido em estrita observância às normas de auditoria aplicáveis ao serviço público e que não houve nenhuma limitação para a sua realização.

1.1. Visão geral do objeto

De acordo com o [Ministério das Comunicações](#) a governança de TIC compreende um conjunto de práticas e processos voltados para assegurar que a tecnologia da informação seja gerida de forma eficiente, segura e em consonância com os objetivos estratégicos da organização. Esse modelo envolve a definição clara de responsabilidades, o processo decisório, o acompanhamento do desempenho e a mitigação de riscos, com o propósito de otimizar a utilização dos recursos de TIC e garantir a conformidade regulatória.

O Guia de Governança de TIC (GovTIC), elaborado pela Secretaria de Tecnologia da Informação e Comunicação do Ministério do Planejamento, Desenvolvimento e Gestão (SETIC/MP), no âmbito do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), define princípios e diretrizes que devem ser observados por órgãos e entidades integrantes do Sistema na implementação ou evolução da governança de TIC.

A metodologia adotada nesta avaliação baseou-se no modelo de governança de TIC do SISP, que reúne dez práticas voltadas ao fortalecimento da governança institucional. Essas práticas visam consolidar a estrutura de governança, reforçar o papel estratégico da alta administração e promover o uso eficiente dos recursos de TIC. São elas: (1) Envolvimento da alta administração nas iniciativas de TIC; (2) Definição dos direitos decisórios sobre TIC; (3) Comitê de TIC; (4) Gestão de riscos de TIC; (5) Portfólio de TIC; (6) Alinhamento estratégico; (7) Comunicação e transparência; (8) Conformidade do ambiente de TIC; (9) Monitoramento do desempenho da TIC; e (10) Avaliação do uso da TIC. Essas práticas não operam isoladamente, mas de maneira integrada, o que potencializa seus efeitos e amplia a efetividade da governança de TIC.

2. METODOLOGIA

Para cumprir o objetivo proposto, o trabalho foi estruturado com base nos três eixos norteadores da governança: Liderança, Estratégia e Controle, conforme estabelecido pelo [Decreto nº 9.203/2017](#), e considerando os instrumentos normativos e orientadores pertinentes à área, incluindo a [Portaria SGD/ME nº 778/2019](#) e suas alterações, bem como o [Guia de Governança em TIC do SISP](#), versão 2.0, como suporte para a definição de práticas e diretrizes adotadas.

A partir desses eixos, foram identificados os riscos-chave com base nas 10 práticas de governança de TIC do *Guia de Governança em TIC do SISP*, os quais foram validados com a unidade auditada por meio de reuniões com os interlocutores, que ocorreram via o *google meet*. Ademais, destaca-se que o próprio relatório de auditoria, produto desse trabalho, constitui-se evidência concreta da Prática 8, cujo artefato principal são relatórios de conformidade.

Com base nesses referenciais, a auditoria foi conduzida a partir de seis questões centrais, uma delas desdobrada em duas subquestões, conforme sistematizado a seguir:

1. Há envolvimento da alta administração com iniciativas de TIC?
 - 1.1 A alta administração se envolve efetivamente com questões de governança da TIC?
 - 1.2 Os processos decisórios de TIC, especialmente quanto à priorização de projetos e investimentos, envolvem todas as partes interessadas e estão formalizados?
2. O comitê de TIC está formalmente instituído e contribui efetivamente para a avaliação, direcionamento e monitoramento da governança de TIC?
3. O gerenciamento de riscos de TIC é realizado de modo a contribuir para o alcance dos objetivos de TIC e organizacionais?
4. As ações de TIC estão alinhadas aos objetivos estratégicos da instituição?
5. As ações e resultados de TIC são comunicados de forma satisfatória?
6. As ações de TIC são monitoradas e avaliadas adequadamente?

Para responder a essas questões, foram aplicados procedimentos de auditoria baseados em testes substantivos, os quais compreenderam:

- **Análise documental** de normativos, planos, políticas e registros relacionados à governança de TIC da UFV (tais como Plano de Desenvolvimento Institucional – PDI; Política de Gestão de Riscos e Controles – PGRC; Plano Diretor de Tecnologia da Informação – PDTI; Resoluções e deliberações dos colegiados de TIC);
- **Indagação escrita**, utilizada para esclarecer pontos específicos junto à unidade auditada;
- **Indagação oral**, realizada em reuniões com interlocutores designados para facilitar a comunicação entre a unidade auditada e a equipe de auditoria.

O detalhamento das questões de auditoria e os elementos de verificação a elas associados, encontra-se sistematizado no **APÊNDICE A**.

3. RESULTADOS DO TRABALHO

A seguir, apresentamos os principais resultados das análises, tendo como base as questões de auditoria que nortearam a execução do trabalho.

3.1. Envolvimento da alta administração em ações de TIC com fragilidades na transparência das ações e no desenvolvimento de competências

A análise sobre o envolvimento da alta administração com iniciativas de TIC buscou identificar a existência de práticas institucionais formais, a participação da alta gestão em comitês da área, a definição de papéis e responsabilidades e a adoção de mecanismos de capacitação voltados ao tema.

Inicialmente, ressalta-se que, conforme a [Resolução Consu nº 02/2020](#) a Diretoria de Tecnologia da Informação (DTI) está formalmente vinculada à Pró-Reitoria de Planejamento e Orçamento (PPO), o que evidencia a integração da área de TIC à alta gestão e reforça seu papel estratégico na instituição.

Complementarmente, a [Resolução Consu nº 11/2022](#) instituiu o Comitê de Governança Digital (CGD), órgão colegiado máximo de decisões em TIC, de caráter estratégico e permanente. Composto por representantes multicampi da alta gestão, o CGD exerce funções normativas, consultivas e deliberativas sobre governança digital e TIC, evidenciando o envolvimento da alta administração nas iniciativas da área. Vinculado à Reitoria, o colegiado tem por finalidade desenvolver e monitorar políticas e diretrizes estratégicas transversais de governança digital assegurando o alinhamento com os objetivos institucionais.

Quanto à atuação do CGD, os registros de atas, convocações e pautas demonstram o cumprimento de suas atribuições normativas, com a abordagem de temas alinhados à sua finalidade, voltados a ampliar a eficiência e estruturar a governança em tecnologias da informação. Assim, as deliberações confirmam a prática consistente de governança de TIC, abrangendo estratégia e planejamento (PDTI e Plano de Transformação Digital), priorização de investimentos (matriz de priorização de sistemas e projetos), gestão de riscos e continuidade (Plano de Continuidade de Negócios, privacidade e segurança da informação, Política de Gestão de Vulnerabilidades, Norma de Gestão de Ativos de Informação), além de transparência e controle (Planos de Dados Abertos, regimentos, evidências iESGo, indicadores iGovSISP).

Apesar da existência de práticas formais de governança organizacional e da participação da alta administração em questões de TIC, constatou-se que a documentação disponível não está devidamente organizada nem acessível de forma clara às partes interessadas. A página eletrônica da DTI disponibiliza a resolução de criação do CGD e a lista de seus membros titulares, porém não apresenta informações atualizadas sobre o Comitê Permanente de Governança Digital (CPGD) e o Comitê de Segurança da Informação e Comunicação (CSIC), o que compromete a transparência das instâncias colegiadas de governança em TIC.

Embora tenha sido constatado o envolvimento da alta administração nas iniciativas de TIC, não foram identificadas ações de capacitação em governança de TI voltadas aos gestores de TIC e aos demais envolvidos, no período analisado. A unidade auditada informou que os últimos treinamentos realizados se concentraram no aprimoramento técnico das equipes de TIC, especificamente na área de segurança da informação. Tal situação pode decorrer da fragilidade do planejamento institucional voltado ao desenvolvimento de competências em governança de TIC.

Assim, observa-se como oportunidade de melhoria a atualização e organização dos dados de governança, bem como a elaboração de um plano de capacitação voltado à alta administração, gestores de TIC e demais envolvidos, promovendo maior transparência e o fortalecimento das competências em governança corporativa.

3.2. Especificação dos direitos decisórios de TIC com fragilidade nos fluxos formais de decisão

No que se refere à priorização de projetos e investimentos buscou-se verificar se os processos decisórios de TIC, estavam devidamente formalizados e se envolviam todas as partes interessadas relevantes (áreas de negócio, área de TIC e alta administração).

A avaliação realizada identificou que a governança de TIC da instituição apresenta avanços relevantes, especialmente no que diz respeito à existência de instrumentos normativos, comitês formalizados e critérios definidos para priorização de investimentos. No entanto, foram verificadas fragilidades que

limitam a transparência e a efetividade do processo decisório, podendo impactar a legitimidade das deliberações e a eficiência na gestão de recursos.

Quanto aos fluxos de decisão, embora a resposta emitida pela unidade auditada à solicitação de auditoria (SA) tenha descrito como se dá a tomada de decisão em TIC, não foi localizada a formalização desse fluxo em documento oficial ou em publicações acessíveis às partes interessadas. A inexistência de fluxos formalmente instituídos e publicados pode resultar em falta de clareza quanto às responsabilidades e etapas decisórias e favorecer a morosidade, o retrabalho e as indefinições na condução de demandas. Além disso, a ausência de um instrumento de referência claro pode comprometer a previsibilidade e dificultar o acompanhamento por parte da comunidade acadêmica e da sociedade.

Em relação à definição de competências, observou-se que a Resolução Consu nº 11/2022 detalha a composição do CGD, que abrange representantes da alta gestão, setores administrativos, divisões acadêmicas e os campi descentralizados, garantindo pluralidade e legitimidade às decisões. No que se refere às atas das reuniões do CGD e do CPGD, verificou-se que, embora as deliberações dessas instâncias estejam alinhadas às atribuições regimentais previstas, os registros não são disponibilizados de forma sistemática e padronizada no site da DTI, o que dificulta o acesso às informações pela comunidade acadêmica e pela sociedade.

Em relação à priorização de investimentos em TIC, o [Plano Diretor de Tecnologia da Informação \(PDTI\) 2024-2029](#) adotou a matriz GUT como metodologia oficial de priorização, garantindo maior objetividade e consistência na análise das demandas. Apesar desse avanço, a influência das restrições orçamentárias pode comprometer o alinhamento entre planejamento e execução, privilegiando soluções imediatas em detrimento de projetos estratégicos e de maior impacto institucional.

3.3. Formalização dos comitês de TIC com fragilidade na comunicação e transparência de suas ações

A partir da análise documental e das interações com os interlocutores do trabalho, verificou-se a existência de três instâncias colegiadas ativas relacionadas à TIC: o Comitê de Governança Digital (CGD), vinculado à Reitoria;

o Comitê Permanente de Governança de Dados (CPGD), subordinado ao CGD; e o Comitê de Segurança da Informação e Comunicação (CSIC), vinculado à PPO.

As análises abrangeram aspectos como a instituição formal dos comitês, a existência de regimentos internos, a definição e divulgação de pautas e calendários de reuniões, bem como a elaboração e disponibilização das atas de deliberação. Constatou-se, assim, a formalização, a atuação e o nível de transparência das instâncias colegiadas de TIC instituídas pela universidade.

Na constituição dos colegiados, verificou-se que apenas o CSIC prevê a suplência de membros, tendo estes sido nomeados recentemente pela [Portaria nº 0713/2025, de 19 de setembro de 2025](#). Observou-se que o CPGD foi instituído por portaria, enquanto o CGD e o CSIC foram criados por resolução do Consu. Quanto aos regimentos internos, apenas o CGD e o CSIC os possuem, permanecendo o CPGD sem normativo próprio. Apesar de a [Portaria RTR/UFV nº 37/2025](#) definir objetivos, competências e composição do CPGD, não estabelece regras de funcionamento nem a frequência das reuniões. Constatou-se, ainda, que embora os comitês tenham sido formalmente instituídos, as informações disponíveis encontram-se desatualizadas e desorganizadas, como exemplifica a página institucional da DTI, que ainda apresenta dados de colegiados já extintos.

No exame das competências, observou-se que cada colegiado tem foco específico — CGD na governança de TIC, CPGD na governança de dados e CSIC na segurança da informação e comunicação. Observou-se que alguns aspectos são abordados pelos três colegiados, especialmente em relação a transparência, abertura de dados, continuidade de negócios e alinhamento estratégico, o que evidencia a convergência em relação a temas de caráter estratégico no âmbito da governança em TIC.

Em relação às pautas e calendários de reuniões, as informações se mostraram parciais, uma vez que apenas o CGD e o CSIC definiram periodicidade em seus regimentos, mas sem indicar datas em um calendário anual. Quanto às pautas, verificou-se que, no CGD, elas são incluídas nos atos de convocação, mas sem evidência de disponibilização prévia. No CPGD, a primeira reunião (processo 23114.907806/2025-13) registrou pauta, porém também sem comprovação de envio antecipado aos membros.

Acerca das atas, observou-se que, os registros já existentes (CGD e CPGD) apresentam qualidade adequada, com síntese das discussões, clareza nas decisões, fundamentação em evidências, definição de planos de ação, responsáveis, prazos e sugestões de pautas futuras. O CSIC, por estar em fase inicial de funcionamento, ainda não possui reuniões registradas, como destacado anteriormente seus membros foram recentemente nomeados.

Quanto à disponibilização do conteúdo das reuniões do CGD (pautas e atas) este se encontra no site da DGI, compartilhado com os documentos do Comitê de Governança, Integridade, Riscos e Controle (CGRC), em razão da realização conjunta das reuniões de ambos os colegiados, todavia o acesso não é intuitivo. Assim, identifica-se como ponto de melhoria a comunicação mais eficaz sobre os comitês, oferecendo maior clareza sobre sua composição, funcionamento e atuação. Tais medidas podem contribuir para a transparência ativa, fortalecendo a legitimidade das instâncias colegiadas e reforçando a estrutura de governança de TIC na UFV.

3.4. Fragilidade no gerenciamento de riscos de TIC

No âmbito do gerenciamento de riscos de TIC na UFV, buscou-se avaliar se o processo de gestão de riscos é realizado de forma estruturada e eficaz, de modo a contribuir para o alcance dos objetivos institucionais. Foram considerados aspectos como a formalização de política de segurança da informação, a participação da alta administração em deliberações sobre riscos, a identificação e tratamento dos principais riscos de TIC, a existência de plano específico de gestão de riscos de segurança da informação, bem como a implementação de mecanismos de conformidade com a Lei Geral de Proteção de Dados (LGPD).

Constatou-se que a [Resolução Consu nº 12/2024](#) institucionalizou a Política de Segurança da Informação e Comunicação (POSIC), que tem como objetivo orientar a UFV quanto à gestão de riscos e ao tratamento de incidentes de segurança, assegurando a conformidade legal e regulatória. Essa política estabelece diretrizes gerais para adoção de mecanismos de segurança da informação, representando um avanço significativo no campo normativo da instituição.

Em relação à participação da alta gestão em deliberações voltadas à gestão de risco, observou-se seu envolvimento tanto nos trabalhos de gestão de risco institucional quanto na elaboração do PDTI 2024-2029, o qual contempla um plano de gestão de riscos de TIC.

No que se refere à identificação e ao tratamento dos principais riscos de TIC, verificou-se que o PDTI estabeleceu um plano de gestão de riscos, enquanto a página da Diretoria de Governança Institucional (DGI) apresentou riscos de TIC mapeados. Contudo, observa-se um desalinhamento entre ambos: os riscos identificados no PDTI estão associados ao alcance de suas metas, ao passo que os registrados na página da DGI estão vinculados aos processos operacionais de TIC.

Na análise do plano de gestão de riscos de TIC constante no PDTI em comparação com a [Política de Gestão de Riscos e Controles Internos da UFV](#) (PGRC), foram constatadas divergências, principalmente quanto à nomenclatura e aos critérios adotados para definição dos níveis de aceitação. Enquanto a PGRC utiliza o nível de risco como referência, o PDTI adota a categoria do risco como critério. Também foram identificadas diferenças na classificação de probabilidade, impacto e na metodologia de pontuação empregada para definição dos níveis de risco.

Além disso, não foram identificados mapeamentos de processos estratégicos na unidade, notadamente aqueles vinculados à governança de TIC. Essa ausência de mapeamento compromete a visão sistêmica das atividades críticas, dificultando a identificação de riscos, a implementação de controles internos, a definição clara de responsabilidades e a padronização dos procedimentos.

Adicionalmente, constatou-se a inexistência de um plano específico de Gestão de Riscos de Segurança da Informação, assim como do respectivo relatório de tratamento dos riscos. A ausência do referido instrumento fragiliza a capacidade da instituição de tratar riscos críticos de segurança da informação de forma sistemática e alinhada às diretrizes normativas vigentes. A POSIC estabelece que tais instrumentos devem ser aprovados pelo Gestor de Segurança da Informação e Comunicação (GSIC), recentemente nomeado pela [Portaria RTR 713/2025](#).

Em relação à LGPD, a universidade iniciou a adequação em 2021 com a criação de um grupo de trabalho, que apoiou auditorias externas, aplicou diagnósticos de maturidade e identificou fragilidades institucionais, constatando um estágio inicial de implementação. Em 2022, com a criação do Comitê de Governança Digital (CGD), as responsabilidades do referido grupo foram absorvidas por estruturas permanentes, incluindo a nomeação do Encarregado de Dados (ETDP) e a definição de responsabilidades normativas. Desde então, a universidade tem fortalecido a governança em privacidade e segurança da informação, revisando políticas e normas, criando comitês técnicos, estruturando o Programa de Governança em Privacidade (PGPriv) e elaborando planos estratégicos (PDTIC 2025–2029 e Plano de Dados Abertos 2025–2027). Essas ações representam avanços significativos, embora a maturidade institucional ainda precise evoluir para assegurar plena conformidade com a LGPD.

3.5. Alinhamento das ações de TIC aos objetivos estratégicos com fragilidade na divulgação do portfólio

Sobre o alinhamento das ações de TIC aos objetivos estratégicos da UFV, buscou-se verificar a definição e publicação do portfólio de TIC, o alinhamento do PDTI ao PDI e a participação dos comitês de TIC nos processos decisórios e de acompanhamento.

Constatou-se, inicialmente, a definição e publicação parcial do portfólio de TIC. Embora haja referência a iniciativas e investimentos, não foi identificado documento atualizado e amplamente divulgado que apresente clara vinculação entre necessidades institucionais, programas e projetos de TIC. Essa lacuna dificulta a transparência das ações e o acompanhamento da execução orçamentária e financeira voltada à área.

No que tange ao alinhamento estratégico, o exame realizado permite concluir que o PDTI 2024-2029 está em consonância com o PDI 2024-2029, traduzindo diretrizes institucionais em metas e ações voltadas para governança digital, modernização administrativa, infraestrutura tecnológica, inclusão e suporte aos macroprocessos acadêmicos e de inovação. Ressalta-se, entretanto, a necessidade de monitoramento contínuo e do aperfeiçoamento dos indicadores

para assegurar que os benefícios esperados sejam efetivamente mensurados e entregues.

Por fim, verificou-se que o CGD participou ativamente da elaboração do PDTI 2024-2029, conforme registrado nas atas de 2023, incluindo a priorização de sistemas de TI e o acompanhamento de projetos.

3.6. Existência de canais de comunicação com fragilidade na transparência das ações de governança em TIC

Neste aspecto, avaliou-se a existência de canais de prestação de contas e a clareza das informações para gestores e sociedade, bem como se as informações de TIC estavam acessíveis de forma clara e transparente para as partes interessadas.

Com relação à prestação de contas, constatou-se que há canais de comunicação que promovem a transparência. No site da DTI, encontram-se disponíveis o campo “dados abertos da UFV” e o “painel de dados”, que permitem acesso a informações gerais da instituição, inclusive financeiras. Há também o Plano de Dados Abertos, além da Ouvidoria, que possibilita manifestações da comunidade. Além disso, o [Relatório de Gestão](#), constitui um relevante instrumento anual de comunicação e prestação de contas, pois reúne de forma clara e objetiva as principais ações, resultados e uso dos recursos públicos pela instituição. Como ponto de melhoria, retoma-se a necessidade de sistematização e melhor comunicação e transparência de informações relacionadas à governança em TIC, sobretudo no que diz respeito à atuação dos comitês, reforçando os achados dos itens 3.1, 3.2 e 3.3.

3.7. Fragilidade no monitoramento e avaliação das ações de TIC

No que se refere ao monitoramento e à avaliação das ações de TIC, buscou-se identificar a existência de mecanismos formais de acompanhamento do desempenho, como indicadores, métricas de qualidade e de prestação de serviços, além da realização de avaliações periódicas dos resultados. Constatou-se atendimento parcial, uma vez que, embora existam mecanismos regulares de monitoramento e avaliação de TIC, não foram identificadas métricas voltadas à mensuração do retorno dos investimentos realizados na área.

Quanto ao monitoramento dos serviços, em resposta à SA foi informado que a UFV acompanha continuamente a qualidade e o desempenho dos serviços de TIC por meio de indicadores vinculados a processos-chave, com metas e fatores críticos de sucesso que permitem avaliar a efetividade dos processos, tais como atendimento a usuários, gestão de incidentes, disponibilidade de sistemas e segurança da informação. Ainda conforme informado, a análise periódica desses resultados favorece a identificação de melhorias, evidenciando uma governança de TIC orientada por métricas objetivas e alinhada às demandas institucionais. Todavia, os indicadores mencionados encontram-se disponíveis apenas até 2021, não tendo sido localizados registros atualizados.

Em relação às avaliações periódicas sobre o uso e os resultados da TIC, a unidade auditada informou que a instituição realiza o monitoramento das ações principalmente por meio do PDTI, de indicadores de desempenho dos serviços e dos Relatórios de Gestão anuais, o que possibilita o acompanhamento do progresso de projetos e a avaliação qualitativa dos resultados. Esses mecanismos oferecem revisões periódicas (anuais ou semestrais) e ajustes operacionais, com reporte aos comitês de governança. Todavia, não existe processo formal para mensurar o retorno sobre investimento (ROI) específico da TIC, sendo que as avaliações estão distribuídas entre diferentes instrumentos. As avaliações externas, como as do TCU, analisam de forma indireta a maturidade da governança de TI.

Adicionalmente, destaca-se que, ao acessar a aba 'Monitoramento' na página eletrônica da DTI, todos os links apresentaram erro, o que impossibilitou a consulta. Na aba 'PDTI', por sua vez, é possível acessar métricas das ações previstas no plano, bem como informações sobre TIC e investimentos constantes no Relatório de Gestão da instituição.

4. RECOMENDAÇÕES

Com base nas análises realizadas e nos resultados obtidos neste estudo sobre a governança de TI na Universidade Federal de Viçosa, apresentam-se as seguintes recomendações:

1. Aprimorar a transparência das informações sobre governança em TIC

Promover a atualização e a sistematização das informações sobre governança em TIC na página institucional da DTI, disponibilizando, de forma centralizada e

acessível, dados referentes à criação, composição, regimentos, calendário de reuniões, pautas, atas e deliberações dos comitês de TIC na aba “Governança”, de modo a aprimorar a transparência e facilitar o acompanhamento pelas partes interessadas.

Item 3.1; 3.2; 3.3, 3.6

2. Desenvolver capacidades técnicas e gerenciais

Elaborar e implementar um plano de capacitação voltado aos gestores e demais atores envolvidos com a área de TIC, de forma a fortalecer competências e promover um ambiente propício à consolidação da governança de TIC.

Item 3.1

3. Aprimorar a transparência e a padronização das decisões em TIC

Formalizar e disponibilizar, em meio oficial e de fácil acesso, os fluxos decisórios da área de TIC, assegurando clareza quanto às instâncias responsáveis, etapas e critérios adotados nos processos de decisão.

Item 3.2

4. Fortalecer a atuação dos comitês como instância de governança

Elaborar o regimento interno do Comitê Permanente de Governança de Dados (CPGD), em conformidade com as diretrizes do Guia de Comitê de TIC do SISP.

Item 3.3

5. Fortalecer a governança e gestão de riscos de TIC

5.1 Realizar análise comparativa entre a PGRC institucional e o PDTI para avaliar a conveniência de ajustes e harmonização dos critérios adotados para aceitação e tratamento dos riscos;

5.2 Elaborar e institucionalizar o Plano de Gestão de Riscos de Segurança da Informação, em conformidade com as diretrizes da IN GSI/PR nº 3/2021, incluindo a formalização do relatório de tratamento de riscos.

5.3 Mapear e formalizar os processos estratégicos da unidade, com destaque para aqueles relacionados à governança institucional.

Item 3.4

6. Aprimorar a transparência e o alinhamento estratégico dos investimentos em TIC

Atualizar e divulgar, na página institucional da DTI, o portfólio de TIC, contemplando programas e projetos em andamento ou planejados, com vinculação explícita às necessidades institucionais e aos objetivos estratégicos da organização.

Item 3.5

7. Aprimorar a transparência do monitoramento e a avaliação da atuação da TIC

Atualizar a página institucional da DTI, de forma contínua, divulgando os principais indicadores de desempenho da área de TIC, garantindo a acessibilidade e a clareza das informações para acompanhamento pela gestão e demais partes interessadas. E ainda, verificar a pertinência de implementar métricas formais para avaliar o retorno dos investimentos em TIC, ao invés de apenas monitorar e avaliar os resultados.

Item 3.7

5. CONCLUSÃO

O trabalho de avaliação realizado na Universidade Federal de Viçosa teve como objetivo verificar a governança de Tecnologia da Informação e Comunicação (TIC) da instituição, considerando, principalmente, o Decreto nº 9203/2017, a Portaria SGD/ME nº 778/2019 e suas alterações, e o Guia de Governança em TIC do SISP. A metodologia adotada contemplou análise documental, indagações escritas e orais, além da verificação de registros, planos, políticas e comitês vinculados à gestão de TIC, o que possibilitou identificar práticas consolidadas, avanços e oportunidades de melhoria.

Os resultados evidenciam avanços significativos da instituição em relação à governança em TIC, mas também apontam oportunidades de melhoria em algumas dimensões estratégicas e operacionais. A análise revelou que a alta administração está formalmente envolvida nas iniciativas de TIC, por meio da vinculação da Diretoria de Tecnologia da Informação (DTI) à Pró-Reitoria de Planejamento e Orçamento (PPO) e da atuação do Comitê de Governança Digital (CGD). Esse alinhamento estratégico, reforçado por comitês colegiados e instrumentos normativos, evidencia a preocupação institucional com a governança, a priorização de investimentos, a gestão de riscos, a continuidade de negócios, a transparência e a segurança da informação

Entretanto, verificou-se que a documentação e as informações sobre governança e processos decisórios ainda carecem de organização e de facilidade de acesso ao público. A ausência de fluxos decisórios formalizados, a divulgação não sistematizada das atas e pautas dos comitês na página oficial da DTI, a atualização irregular de indicadores de desempenho e a dispersão de

informações sobre portfólio e resultados de TIC comprometem a transparência e dificultam o acompanhamento da execução e do impacto das ações.

No âmbito do gerenciamento de riscos, a institucionalização da Política de Segurança da Informação e Comunicação (POSIC) e a inclusão de um plano de gestão de riscos de TIC no PDTI representam avanços normativos. Todavia, a ausência de harmonização entre os diferentes instrumentos de gestão de riscos e a falta de um plano específico voltado à segurança da informação constituem lacunas significativas, que podem comprometer a capacidade da instituição de tratar riscos críticos de forma estruturada e consistente.

Diante desse cenário, as recomendações propostas - como a atualização e centralização das informações sobre governança e comitês, a formalização dos fluxos decisórios, a divulgação sistemática de indicadores e resultados, a elaboração de planos de gestão de riscos e o alinhamento do portfólio de TIC aos objetivos estratégicos - têm o potencial de consolidar a transparência, a legitimidade e a eficiência da governança de TIC na UFV. A adoção destas medidas vai ao encontro do cumprimento das normas legais e regulatórias e do fortalecimento da cultura de *accountability* e do uso estratégico dos recursos públicos, assegurando que as ações de TIC contribuam efetivamente para o alcance dos objetivos institucionais.

Em síntese, a UFV apresenta avanços relevantes na governança em TIC, com estruturas e normas que fortalecem a gestão e a tomada de decisão. Ainda assim, destaca-se a relevância da instituição adotar as recomendações propostas, de modo a aprimorar a transparência, apoiar o desenvolvimento de capacidades técnicas e gerenciais, fortalecer a gestão de riscos e integrar os instrumentos de governança, alinhando-se às melhores práticas nacionais e internacionais.

APÊNDICE A

Quadro 2: Detalhamento das questões de auditorias, e testes, segundo as práticas do Guia SISP.

Eixo	Questão de Auditoria	Subquestão de Auditoria	Prática do Guia de GovTIC do SISP	Teste
Liderança	1. Há envolvimento da alta administração com iniciativas de TIC?	1.1 - A alta administração se envolve efetivamente com questões de governança da TIC?	Prática 01 - Envolvimento da alta administração com iniciativas de TIC Prática 06 – Alinhamento Estratégico	1 - Verificar a existência de práticas (atos, portarias) de governança organizacional e de governança de TIC.
				2 - Verificar a instituição e cumprimento das atribuições do Comitê de Governança Digital.
				3 - Verificar a formalização dos papéis e responsabilidades acerca da tomada de decisão sobre a governança de TIC, bem como se as informações necessárias para tomada de decisão são definidas.
				4 - Verificar a instituição de mecanismos para o desenvolvimento de competências relacionadas à governança de TIC para alta administração, gestores de TIC e demais envolvidos com o tema.
		1.2 - Os processos decisórios de TIC, especialmente em relação à priorização de projetos e investimentos, envolvem todas as partes interessadas relevantes (áreas de negócio, área de TI, alta administração) e estão formalizados?	Prática 02 - Especificação dos direitos decisórios sobre TIC	1 - Verificar a existência de fluxos formais do processo decisórios de TIC da organização, bem como seu embasamento legal/normativo.
				2 - Verificar se a definição das competências sobre as decisões de TIC envolve todas as partes interessadas relevantes.
				3 - Verificar se a execução das atividades e das tomadas de decisão pela área de TIC estão de acordo com as competências atribuídas.
				4 - Verificar a utilização de critérios formalizados ao

				realizar a priorização de projetos e investimentos de TIC.
Estratégia	2. O comitê de TIC está formalmente instituído e contribui efetivamente na avaliação, direcionamento e monitoramento da governança de TIC?		Prática 03 - Comitê de TIC Prática 07 – Sistema de Comunicação e Transparência	1. Verificar se os comitês de TIC foram formalmente instituídos, com ato que define competências, composição, papéis, estrutura de apoio, membros e suplentes em nível hierárquico adequado.
				2 - Verificar se o Regimento Interno dos comitês de TIC está estabelecido, e detalha regras para o funcionamento do comitê; se existem mecanismos para que as partes interessadas, internas e externas à organização, sejam ouvidas no comitê de TI.
				3 - Verificar se o cronograma anual de reuniões ordinárias do comitê está estabelecido.
				4 – Verificar se as reuniões seguem o previsto, considerando a antecedência e adequação das convocações e pautas, a pertinência dos assuntos tratados, o cumprimento do cronograma e a frequência de participação dos membros.
				5 - Verificar se as atas registram de forma clara as discussões e decisões, fundamentam as deliberações em evidências, definem planos de ação com responsáveis e prazos e apresentam sugestões de pautas futuras.
	3. O gerenciamento de riscos de TIC é realizado de modo a contribuir		Prática 04 - Riscos de TIC	6 – Verificar se as informações e documentos do comitê estão publicados, organizados e acessíveis às partes interessadas. 1 - Verificar a formalização de uma política de gestão de riscos de TIC que assegure a conformidade legal e regulatória e que esteja

	efetivamente para o alcance dos objetivos de TIC e organizacionais?			<p>alinhada à gestão de riscos organizacionais, sendo de fácil acesso a todos na organização.</p> <p>2- Verificar o registro em ata, com participação da alta administração, de deliberações sobre os riscos de TIC definidos.</p> <p>3- Verificar se há levantamento dos principais riscos de TIC, definição dos níveis de aceitação e mecanismos que orientem seu tratamento.</p> <p>4- Verificar a existência de Plano de gestão de Riscos de segurança da informação e o relatório de tratamento de riscos de segurança da informação</p> <p>5 - Verificar a implementação de mecanismos para garantir alinhamento às obrigações da LGPD.</p>
	4. As ações de TIC estão alinhadas aos objetivos estratégicos da instituição?		<p>Prática 05 – Portfólio de TIC</p> <p>Prática 06 – Alinhamento Estratégico</p>	<p>1 - Verificar a definição e publicação do Portfólio de TIC e se ele está atualizado</p> <p>2. Quais são os procedimentos para a priorização dos investimentos em TIC?</p> <p>3. Verificar se o PDTIC está alinhado ao Planejamento Estratégico Institucional (PDI)</p> <p>4. O comitê participa da aprovação do PDTIC, priorização de investimentos e acompanhamento de projetos</p>
	5. As ações e resultados de TIC são comunicados de forma satisfatória?		Prática 07 – Sistema de Comunicação e Transparência	1. Existem canais de comunicação para prestação de contas (transparência interna e externa)? As informações de TIC estão acessíveis de forma clara e compreensível para gestores e sociedade (quando aplicável)?
Controle	6. As ações de TIC são		Prática 09 – Monitoramento	1. Há mecanismos formais de monitoramento do

	monitoradas e avaliadas adequadamente?		do desempenho da TIC Prática 10 – Avaliação do uso da TIC	desempenho da TIC (ex.: indicadores, painéis, indicadores da qualidade e desempenho dos serviços prestados, tempo de resposta)? São realizadas avaliações periódicas sobre uso e resultados da TIC?
				2. Existe indicadores para o monitorar as ações (prestação de serviço, investimento)? É realizada avaliação dos resultados das ações?