Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco
Reitoria/Reitoria/Auditoria Interna

RELATÓRIO DE AUDITORIA Nº 020/2024

TIPO DE AUDITORIA	Avaliação
EXERCÍCIO	2024
MACROPROCESSO DO IFPE	Tecnologia da Informação e Comunicação
PROCESSO DE TRABALHO DO IFPE	Planejamento, Organização, Direção e Monitoramento da Gestão da Política e Diretrizes de Tecnologia da Informação
UNIDADES AUDITADAS	Reitoria, Diretoria de Tecnologia da Informação (DTI)
CÓDIGOS UG's	158136
GESTORES RESPONSÁVEIS	José Carlos de Sá (158136); Jobson Tenório do Nascimento (158136)

1. Introdução

Em atendimento ao item nº 11, anexo I do Plano Anual de Atividades da Auditoria Interna (PAINT) do exercício 2024, e à demanda prevista na Ordem de Serviço nº 020/2024 da Auditoria-Geral e consoante o estabelecido na Instrução Normativa – Secretaria Federal de Controle (IN/SFC) nº 03, de 09/06/2017, apresentamos os resultados da análise preliminar acerca do objeto de auditoria "Planejamento, Organização, Direção e Monitoramento da Gestão da Política e Diretrizes de Tecnologia da Informação".

"A análise preliminar do objeto constitui uma etapa fundamental dos trabalhos de auditoria. É necessária para ajudar os auditores internos governamentais a obter uma compreensão suficiente do objeto de auditoria e para que se estabeleçam de forma mais clara os objetivos, o escopo do trabalho, os exames a serem realizados e os recursos necessários para a realização da auditoria"[1].

É importante destacar que a seleção do objeto (Planejamento, Organização, Direção e Monitoramento da Gestão da Política e Diretrizes de Tecnologia da Informação) ocorreu com base na identificação e na avaliação dos riscos da auditoria, quando da elaboração do PAINT 2024.

No quadro a seguir, serão apresentadas informações sobre os seguintes aspectos: Macroprocesso; Processo; Atribuição do Regimento Geral do IFPE; e por fim, o risco, identificando potenciais ameaças ou incertezas que podem impactar negativamente a execução eficaz dos processos e o alcance dos objetivos institucionais.

Quadro 01 - Risco identificado pela Auditoria Interna

Macroprocesso:	Processo de Trabalho:	Atribuição do Regimento do Geral do IFPE	Risco identificado

Tecnologia da Informação e Comunicação	Planejamento, Organização, Direção e Monitoramento da Gestão da Política e Diretrizes de Tecnologia da Informação	Art. 60. Compete à Diretoria de Avaliação e Desenvolvimento de Tecnologias: [...] V - implantar e manter serviços de TI de natureza sistêmica;	Em virtude de Processos não estruturados > a Unidade poderá deixar de executar a seguinte atribuição: V - implantar e manter serviços de TI de natureza sistêmica; > Prejudicando o alcance do Objetivo Estratégico (OE-AC-1): Disponibilizar recursos de tecnologia da informação para suportar as atividades pedagógicas e institucionais, em alinhamento com a transformação digital e a evolução tecnológica.

Fonte: IFPE - PAINT 2024

As informações apresentadas no quadro fornecem uma visão sobre o risco identificado pela auditoria, associado à ausência de processos estruturados na gestão de TI no IFPE. A falta desses processos sistêmicos impacta diretamente as atividades de implementação e manutenção adequadas dos serviços de TI, comprometendo a capacidade institucional de atingir o Objetivo Estratégico (OE-AC-1), essencial para viabilizar a transformação digital e dar suporte às atividades pedagógicas e institucionais. Esse risco evidencia uma vulnerabilidade no alinhamento entre práticas operacionais e diretrizes estratégicas, resultando em possíveis impactos negativos na eficiência, continuidade e qualidade dos serviços. Para mitigar esses efeitos, torna-se fundamental priorizar a estruturação dos processos de TI, implementando mecanismos que assegurem o planejamento, monitoramento e conformidade com as políticas institucionais, além de acompanhar a evolução tecnológica.

Assim, o presente relatório foi preparado com o intuito de apresentar a análise preliminar realizada pela Auditoria Interna sobre as atividades relacionadas à atribuição do Art. 60. Compete à Diretoria de Avaliação e Desenvolvimento de Tecnologias: [...] V - implantar e manter serviços de TI de natureza sistêmica.

Este relatório tem como objetivo fornecer informações essenciais para orientar ações futuras voltadas à avaliação da eficácia e da abrangência dos controles internos da unidade na mitigação dos riscos identificados pela Auditoria Interna. Além disso, busca apresentar, de forma independente e objetiva, informações relevantes apuradas pela auditoria, subsidiando a gestão em futuras tomadas de decisão.

Os trabalhos de auditoria são fundamentais para fortalecer e aprimorar continuamente o processo de gerenciamento de riscos da instituição. Com uma perspectiva imparcial, a auditoria identifica áreas que demandam aprimoramento ou ajustes nos controles de riscos.

Destaca-se que, ao evidenciar boas práticas e apontar oportunidades de melhoria, as auditorias buscam contribuir para o aperfeiçoamento contínuo do sistema de gerenciamento de riscos.

Ademais, durante a fase de coleta de informações dessa ação de auditoria, constatou-se a ausência de Plano Diretor de Tecnologia da Informação (PDTI) no IFPE, um instrumento essencial para alinhar as estratégias de Tecnologia da Informação (TI) às diretrizes organizacionais. Em razão dessa lacuna, foi elaborada a Nota de Auditoria 13/2024, recomendando, com urgência, à DTI a elaboração do PDTI.

O desenvolvimento dos trabalhos, inicialmente previsto para o período de 25 de outubro a 05 de dezembro de 2024, foi concluído em 16 de dezembro de 2024, devido ao pedido da DTI de prorrogação de prazo para atendimento das solicitações de auditoria.

As atividades foram realizadas por meio de testes, análises e consolidação de dados, em estrita observância às normas de auditoria aplicáveis ao Serviço Público Federal.

Nenhuma restrição foi imposta à realização dos exames.

2. Resultado da análise preliminar

2.1 Planejamento Anual Integrado (PAI)

Ao ser questionada sobre a elaboração do Plano de Ação (Plano de Ação Integrado ou documento equivalente) para o exercício corrente, a DTI informou que:

> "O planejamento da DTI para o exercício de 2024 foi devidamente registrado no sistema SCOPI (documento SEI nº 1521521) e contempla a atribuição de "implantar e manter serviços de TI de natureza sistêmica". Contudo, o foco principal das ações previstas está na manutenção dos serviços existentes, considerando as restrições orçamentárias e de pessoal que limitam severamente a implantação de novos serviços.
> Destaco, porém, a dificuldade de realizar o acompanhamento completo do plano de ação registrado no sistema SCOPI, especialmente no que se refere à conclusão do ciclo PDCA, o que representa um desafio adicional para a gestão e avaliação das metas estabelecidas."

A análise das informações fornecidas pela DTI revela um planejamento voltado predominantemente para a manutenção dos serviços existentes, o que reflete a realidade das restrições orçamentárias e de pessoal enfrentadas pela unidade. Embora a alocação de recursos para preservar a continuidade dos serviços de TI seja essencial, a priorização exclusiva dessa área pode comprometer a capacidade de evolução tecnológica e a ampliação dos serviços de TI de natureza sistêmica, como previsto no Regimento Geral do IFPE. Além disso, a dificuldade relatada no acompanhamento completo do plano de ação no sistema SCOPI, especialmente quanto à conclusão do ciclo PDCA, sinaliza fragilidades no monitoramento e na avaliação das metas estabelecidas.

É importante destacar que essa situação pode dificultar a identificação de possíveis desvios e ajustes necessários para o alcance dos objetivos estratégicos, reforçando a necessidade de aperfeiçoar os mecanismos de gestão, monitoramento e revisão contínua do planejamento de TI.

2.2 Sistemas de TI utilizados pelo IFPE

Foi solicitado à DTI informações sobre os sistemas de TI utilizados pelo IFPE, como a propriedade, manutenção/atualização, backups. As informações recebidas foram consolidadas da imagem a seguir:

Imagem 01 - Sistema utilizados pelo IFPE

Fonte: Elaboração própria a partir das informações da DTI (1516249)

Os dados apresentados na imagem 01, retratam a diversidade e complexidade dos sistemas de TI utilizados pelo IFPE, abrangendo desde sistemas próprios desenvolvidos pela instituição até sistemas contratados ou oriundos de cooperação técnica. **A predominância de sistemas próprios de código aberto reflete uma estratégia de autossuficiência tecnológica, mas também apresenta desafios significativos em termos de manutenção, atualização e suporte, uma vez que a maioria desses sistemas opera com periodicidade de manutenção "não regular" ou apenas sob demanda.**

As informações detalhadas sobre todos os sistemas utilizados no IFPE (finalidade, proprietário, procedimento de backup e recuperação de dados, periodicidade de manutenção e atualização) podem ser consultadas no **Apêndice A** deste relatório.

2.3 A prática da Gestão de Riscos na DTI

Ao ser questionada sobre a adoção da prática da gestão de riscos em seus processos, a DTI informou que ainda não adota tal prática. Além disso, informou as seguintes dificuldades enfrentadas para adoção da prática no setor:

- Falta de Processos Estruturados: Não há uma abordagem sistemática ou documentação padronizada para a gestão de riscos.
- Recursos Limitados: A escassez de pessoal especializado e ferramentas adequadas dificulta a implementação de um processo eficaz de gestão de riscos.
- Ausência de Capacitação: A equipe não possui treinamento específico para lidar com as práticas de identificação e mitigação de riscos.
- Integração com Outras Áreas: A comunicação e colaboração com outras áreas da instituição para identificar riscos mais amplos ainda são limitadas.
- Falta de Monitoramento Contínuo: Não há um acompanhamento contínuo dos riscos após sua identificação, dificultando a ação preventiva. DTI (1516249)

Conforme relatado pela DTI, o setor enfrenta desafios na gestão de riscos devido à ausência de processos

estruturados, falta de recursos especializados, integração limitada com outras áreas e ausência de monitoramento contínuo. Esses fatores comprometem a eficiência na identificação e mitigação de riscos, exigindo investimentos em políticas formalizadas, capacitação da equipe, ferramentas adequadas e uma abordagem mais estratégica e colaborativa.

Ressalta-se que essa informação sobre a não adoção da prática da gestão de riscos corrobora com as informações constantes do Relatório de Auditoria 015/2024, que conclui-se que o nível de maturidade da **gestão de risco do IFPE se encontra em estágio "inicial" (1,85)**. Evidenciando que, apesar de o processo de gerenciamento de riscos do IFPE encontrar-se normatizado, ainda carece de efetiva implementação operacional.

2.4 Identificação das atividades desenvolvidas pela DTI

Foram solicitadas informações à DTI para esclarecer as atividades que a mesma realiza em conformidade com suas atribuições regimentais. No quadro a seguir são apresentadas as atividades informadas pela DTI para cumprir as atribuições estabelecidas no Regimento Geral do IFPE. São apresentados, ainda, os problemas relacionados à execução dessas atividades, bem como os fatores ou causas que podem contribuir para esses problemas durante sua realização. Além disso, serão informados os mecanismos utilizados para evitar, mitigar ou corrigir tais problemas.

Quadro 02 - Atividades relacionadas à atribuição de implantar e manter serviços de TI de natureza sistêmica

Aspectos relacionados à atribuição do Regimento Geral do IFPE			
Macroprocesso relacionado (Resolução nº 18/2019 CGRC): 13. Tecnologia da Informação e Comunicação			
Processo (Resolução nº 18/2019 CGRC) ou descrição do objeto: 1. Planejamento, Organização, Direção e Monitoramento da Gestão da Política e Diretrizes de Tecnologia da Informação			
Atribuição do Regimento Geral do IFPE: Art. 60. Compete à Diretoria de Avaliação e Desenvolvimento de Tecnologias: **[...]** **V - implantar e manter serviços de TI de natureza sistêmica;**			
Identificar as Atividades necessárias para realização da atribuição do Regimento Geral do IFPE	**Identificar os problemas relacionados à execução das atividades**	**Identificar os fatores ou as causas que podem ocasionar o surgimento dos problemas durante a execução das atividades.**	**Identificar os mecanismos utilizados para evitar, mitigar ou corrigir os problemas relacionados à execução das atividades.**

Planejamento	● Falta de Clareza nos Objetivos; ● Insuficiência de Dados e Informações; ● Estimativa Inadequada de Recursos; ● Cronogramas Irrealistas; ● Desconsideração de Riscos; ● Comunicação Ineficiente; ● Falta de Acompanhamento e Revisão; ● Centralização Excessiva no Planejamento;	● Objetivos mal definidos ou não alinhados às metas estratégicas; ● Comunicação ineficaz entre as partes envolvidas; ● Ausência de direcionamento ou priorização clara; ● Dados desatualizados ou inconsistentes; ● Falta de análise detalhada sobre as demandas e recursos disponíveis; ● Pressão para encurtar prazos sem avaliar a complexidade das atividades; ● Subestimação da quantidade de trabalho envolvido; ● Falta de análise de riscos no planejamento; ● Otimismo excessivo sobre o sucesso das atividades; ● Falta de reuniões regulares entre as partes interessadas; ● Uso inadequado de ferramentas de comunicação; ● Sobreposição de prioridades que desviam a atenção do plano inicial;	● Utilizar ferramentas como SMART Goals para definir objetivos específicos, mensuráveis, alcançáveis, relevantes e com prazo; ● Realizar análises preliminares e buscar validação das informações antes de utilizá-las no planejamento; ● Realizar análise de capacidade (Capacity Planning) para dimensionar corretamente os recursos necessários; ● Construir cronogramas colaborativos com envolvimento da equipe; ● Utilizar metodologias ágeis para gerenciar mudanças e ajustar prazos durante a execução; ● Monitorar riscos ao longo da execução do plano; ● Estabelecer pontos de controle (milestones) para revisar o progresso; ● Utilizar o ciclo PDCA (Planejar, Fazer, Checar, Agir) para revisões contínuas;
Implantação	● Definição Inadequada de Requisitos; ● Falta de Planejamento e Cronograma Irrealista; ● Resistência à Mudança por Parte dos Usuários; ● Infraestrutura Inadequada; ● Falhas na Integração com Sistemas Existentes; ● Testes Insuficientes; ● Sobrecarga na Equipe de TI; ● Monitoramento e Suporte Pós-Implantação Insuficientes;	● Comunicação deficiente entre os stakeholders e a equipe técnica; ● Pressão para entregar rapidamente, sem considerar complexidades técnicas; ● Medo de perda de controle ou aumento de complexidade; ● Recursos de hardware ou rede insuficientes; ● Sistemas legados com documentação deficiente; ● Falta de envolvimento de usuários reais na fase de testes; ● Equipe insuficiente ou sobrecarregada com outras demandas; ● Recursos insuficientes para suporte técnico no período inicial;	● Utilizar técnicas como documentação de casos de uso e prototipação para validar as necessidades; ● Realizar análises de viabilidade e estimativas detalhadas de esforço e tempo; ● Oferecer treinamentos completos antes e após a implantação; ● Investir em atualizações de hardware ou software quando necessário; ● Garantir que a equipe técnica tenha acesso a documentação e suporte necessário; ● Incluir os usuários finais no processo de homologação; ● Priorizar tarefas para evitar sobrecarga durante períodos críticos; ● Avaliar a necessidade de contratar temporariamente ou terceirizar partes do projeto; ● Solicitar feedback contínuo dos usuários para ajustes e melhorias;
Manutenção Preventiva	● Falhas de Comunicação entre as Partes Interessada; ● Insuficiência de Recursos Humanos e Técnicos; ● Atualizações Mal Planejadas;	● Especificações de manutenção pouco claras; ● Falta de pessoal; ● Equipamentos ou infraestrutura desatualizados; ● Falta de compatibilidade entre versões de sistemas e outros serviços;	● Documentar procedimentos e manter um histórico de interações para referência; ● Realizar análises de capacidade e ajustar alocações de recursos conforme a demanda; ● Criar um plano de gerenciamento de mudanças para testar atualizações em ambientes controlados;

Manutenção Corretiva	● Falhas de Comunicação entre as partes Interessada; ● Insuficiência de Recursos Humanos e Técnicos; ● Identificação Tardia de Problemas; ● Dependência Excessiva de Sistemas Legados; ● Problemas de Segurança; ● Dificuldade em Diagnosticar Problemas Complexos; ● Atrasos na Resolução de Incidentes; ● Ausência de Planos de Contingência; ●	● Informações insuficientes ou imprecisas sobre os problemas relatados; ● Falta de pessoal; ● Equipamentos ou infraestrutura desatualizados; ● Prioridades conflitantes devido à sobrecarga da equipe; ● Dificuldade em integrar sistemas legados com tecnologias mais recentes; ● Uso inadequado dos sistemas pelos usuários, como senhas fracas ou acessos indevidos; ● Ambientes de TI muito complexos, com várias dependências; ● Realizar reuniões regulares para alinhamento entre a equipe de TI e os usuários; ● Realizar análises de capacidade e ajustar alocações de recursos conforme a demanda; ● Garantir redundância de equipamentos e ferramentas para evitar paradas prolongadas; ● Planejar a substituição gradual de sistemas legados por tecnologias modernas; ● Capacitar os usuários em práticas seguras para utilização dos sistemas;	● Informações insuficientes ou imprecisas sobre os problemas relatados; ● Falta de pessoal; ● Equipamentos ou infraestrutura desatualizados; ● Prioridades conflitantes devido à sobrecarga da equipe; ● Dificuldade em integrar sistemas legados com tecnologias mais recentes; ● Uso inadequado dos sistemas pelos usuários, como senhas fracas ou acessos indevidos; ● Ambientes de TI muito complexos, com várias dependências; ● Realizar reuniões regulares para alinhamento entre a equipe de TI e os usuários; ● Realizar análises de capacidade e ajustar alocações de recursos conforme a demanda; ● Garantir redundância de equipamentos e ferramentas para evitar paradas prolongadas; ● Planejar a substituição gradual de sistemas legados por tecnologias modernas; ● Capacitar os usuários em práticas seguras para utilização dos sistemas;
Suporte ao Usuário	● Baixa Qualidade no Atendimento ao Usuário; ● Demora na Resolução dos Chamados; ● Insatisfação dos Usuários com as Soluções Oferecidas; ● Falta de Ferramentas de Suporte Adequadas; ● Sobrecarregamento da Equipe de Suporte;	● Falta de treinamento adequado da equipe de suporte; ● Sobrecarga da equipe de suporte; ● Falta de acompanhamento para verificar se a solução implementada resolveu o problema; ● Ferramentas de monitoramento e diagnóstico ineficazes; ● A equipe de suporte não consegue lidar com todos os tickets devido à falta de pessoal;	● Desenvolver e manter uma base de conhecimento com respostas detalhadas para problemas comuns; ● Implementar soluções de automação para diagnosticar problemas comuns ou simples; ● Estabelecer um processo de feedback para verificar se a solução fornecida foi eficaz; ● Investir em ferramentas de atendimento e suporte mais robustas e adequadas às necessidades da equipe de TI; ● Realizar análises de carga de trabalho e ajustar a equipe conforme necessário;
Gestão de Segurança	● Falta de Conscientização e Treinamento dos Colaboradores; ● Vulnerabilidades em Sistemas e Infraestrutura; ● Falhas de Segurança em Redes e Comunicações; ● Falta de Compliance com Normas e Regulamentos de Segurança;	● A falta de uma cultura organizacional focada em segurança cibernética; ● Sistemas desatualizados ou não corrigidos com os últimos patches de segurança; ● Equipamentos de rede desatualizados ou com configurações inadequadas; ● Não estar em conformidade com leis e regulamentos relacionados à segurança;	● Estabelecer campanhas periódicas de sensibilização sobre ameaças cibernéticas; ● Implementar uma política de atualização contínua, aplicando patches e correções de segurança de maneira tempestiva; ● Estabelecer políticas de segurança claras e documentadas, garantindo que todos os colaboradores as compreendam e sigam;

Fonte: Elaborado pela DTI (1516249)

A análise das informações fornecidas revela um cenário complexo, com diversos fatores que impactam negativamente a eficiência das atividades de TI no setor. Três pontos críticos destacam-se como prioritários para tratamento:

a) Ausência de planejamento estruturado e alinhado às metas estratégicas

A falta de clareza nos objetivos, a existência de cronogramas irrealistas para as ações executadas e a ausência de um gerenciamento adequado de riscos aumentam significativamente a probabilidade de um planejamento deficiente. Essa situação compromete o alinhamento das atividades de TI com as metas estratégicas institucionais, reduzindo a eficácia na implantação e manutenção de serviços sistêmicos. A adoção de metodologias como SMART Goals e de ciclos como o PDCA é recomendada, porém, a falta de aplicação prática dessas ferramentas evidencia um problema crítico na gestão estratégica, que necessita ser corrigido com urgência.

b) Infraestrutura e Recursos Humanos Insuficientes

A insuficiência de recursos técnicos e humanos é recorrente em várias dimensões (implantação, manutenção preventiva e corretiva, e suporte ao usuário). A falta de equipamentos atualizados, infraestrutura inadequada e equipes sobrecarregadas tornam o setor vulnerável a falhas operacionais. Essa limitação também dificulta a resolução de incidentes, compromete a continuidade das operações e aumenta o risco de atrasos em entregas críticas. A priorização de investimentos em recursos tecnológicos e na capacitação e ampliação da equipe de TI é essencial para garantir a sustentabilidade das atividades.

c) Falhas de Segurança e Gestão de Riscos

As vulnerabilidades em sistemas, redes e infraestrutura indicam fragilidades na gestão de segurança cibernética. A falta de conscientização, treinamento de colaboradores e compliance com normas de segurança pode resultar em incidentes graves, como vazamentos de dados ou interrupções críticas nos serviços. A implementação de uma política robusta de segurança cibernética, com campanhas regulares de sensibilização e monitoramento contínuo de ameaças, é indispensável para mitigar esses riscos e proteger os ativos institucionais.

2.5 Indicadores relacionados ao processo “implantar e manter serviços de TI de natureza sistêmica” (art. 60, V)

Ao ser questionada sobre a adoção de indicadores para as atividades relacionadas à implantação e manutenção de serviços de TI de natureza sistema (Regimento Geral do IFPE, art. 60, V), a DTI informou que não possui indicadores formalmente estabelecidos, destacando as seguintes dificuldades para implementação:

- Ausência de Definição de Metas Claras: As metas para as atividades de implantação e manutenção de serviços não estão claramente definidas, o que dificulta a criação de indicadores precisos e mensuráveis.
- Recursos Limitados para Monitoramento: A falta de ferramentas adequadas para monitoramento de performance impede a coleta e análise de dados em tempo real sobre o desempenho das atividades de TI.
- Falta de Capacitação em Gestão de Desempenho: A equipe da DTI pode não ter a formação necessária para implementar e utilizar efetivamente indicadores de desempenho.
- Integração Deficiente com Outras Áreas: A falta de integração com outras áreas da instituição dificulta a definição de indicadores que considerem a totalidade dos serviços e necessidades institucionais.
- Mudanças Constantes nas Prioridades: As constantes mudanças de prioridades, devido a fatores orçamentários ou operacionais, dificultam a definição de KPIs de longo prazo. DTI (1516249)

A ausência de indicadores de desempenho (KPIs) formalmente estabelecidos na Diretoria de Tecnologia da Informação (DTI) para as atividades de implantação e manutenção de serviços de TI de natureza sistêmica evidencia fragilidades significativas na gestão de desempenho e na capacidade de monitorar e avaliar a eficiência das operações. Os fatores apontados, como a ausência de metas claras, recursos limitados para monitoramento, falta de capacitação da equipe, integração deficiente com outras áreas e mudanças constantes nas prioridades, revelam a necessidade urgente de uma abordagem estruturada para superar esses desafios. A definição de metas alinhadas aos objetivos estratégicos, a alocação de ferramentas adequadas, a capacitação do time em gestão de desempenho e a promoção de maior integração intersetorial são elementos fundamentais para estabelecer KPIs que contribuam para um gerenciamento mais eficiente e alinhado às necessidades institucionais. Sem essas ações, a instituição permanece vulnerável à falta de visibilidade sobre o desempenho de suas atividades, comprometendo a tomada de decisões baseadas em dados e a melhoria contínua dos serviços de TI.

3. Identificação de riscos e controles

A auditoria interna realizada teve como objetivo assessorar na identificação dos riscos associados ao Macroprocesso de Tecnologia da Informação (DTI) do IFPE. A partir da análise, foram identificados riscos específicos que, se não mitigados, podem comprometer o desempenho e a continuidade dos serviços tecnológicos essenciais para a instituição. Vale destacar que os riscos apresentados a seguir foram identificados exclusivamente pela auditoria, não sendo um rol taxativo, ou seja, outros riscos podem e devem ser considerados pela gestão no processo contínuo de avaliação e mitigação. O relatório também sugere controles que, se implementados, podem fortalecer a governança de TI e minimizar os impactos dos riscos identificados.

Quadro 03 - Identificação de riscos e controles relacionados ao processo Implantação, manutenção e suporte de serviços de TI

Processo	Objetivo do processo	Riscos identificados	Possíveis controles	Sugestão de objetivos de futuras ações de auditoria

Implantação, manutenção e suporte de serviços de TI de natureza sistêmica no IFPE.	Garantir que as atividades de TI estejam alinhadas às metas institucionais, com infraestrutura adequada, segurança eficiente e desempenho consistente para suportar os objetivos pedagógicos e estratégicos da instituição.	R1. Alinhamento Estratégico Comprometido: A ausência de um Plano Diretor de Tecnologia da Informação (PDTI) expõe a organização ao risco de desalinhamento entre as estratégias de TI e os objetivos institucionais. Sem um direcionamento claro, as atividades de TI podem priorizar apenas a manutenção de serviços existentes, deixando de lado iniciativas estratégicas essenciais para a evolução tecnológica e a ampliação dos serviços. R2. Interrupções Operacionais: A infraestrutura tecnológica inadequada e a insuficiência de recursos humanos e técnicos aumentam o risco de falhas operacionais, interrupções nos serviços e atrasos em entregas críticas. A falta de periodicidade na manutenção e a sobrecarga das equipes dificultam a identificação preventiva de problemas, expondo a instituição a períodos de inatividade que impactam diretamente suas operações e a satisfação dos usuários. R3. Incidentes de Segurança Cibernética: As vulnerabilidades na gestão de segurança cibernética, como a ausência de políticas robustas, a falta de conscientização dos colaboradores e sistemas desatualizados, elevam o risco de ataques cibernéticos, vazamento de dados e acessos não autorizados.	C1.1.Elaboração e Implementação do PDTI: Priorizar a criação de um Plano Diretor de Tecnologia da Informação que alinhe as iniciativas de TI às metas estratégicas do IFPE. C1.2 Governança de TI: Estabelecer um comitê de TI para supervisionar e alinhar projetos de TI com os objetivos institucionais. C1.3 Revisões Periódicas: Realizar revisões anuais para garantir que as atividades de TI permaneçam alinhadas às metas organizacionais. C2.1 Plano de Manutenção Preventiva: Desenvolver um cronograma de manutenção preventiva e corretiva para os sistemas e infraestrutura tecnológica. C2.2 Gestão de Recursos: Realizar análise de capacidade e priorizar a alocação de recursos humanos e técnicos para áreas críticas. C2.3 Planos de Contingência: Elaborar planos de contingência para minimizar o impacto de interrupções operacionais. C3.1 Política de Segurança da Informação: Desenvolver e implementar políticas abrangentes de segurança cibernética, alinhadas às normas e melhores práticas. C3.2 Capacitação em Segurança: Realizar treinamentos regulares para conscientizar colaboradores sobre boas práticas de segurança, como o uso de senhas fortes e detecção de phishing. C3.3 Ferramentas de Segurança: Investir em firewalls e softwares antivírus/antimalware.	1 . Analisar a eficiência do planejamento das atividades de TI e seu alinhamento às metas institucionais. 2 . Avaliar a adequação da infraestrutura e dos recursos humanos às demandas de TI da instituição. 3 . Propor melhorias para fortalecer os controles internos e mitigar os riscos identificados.

Fonte: Elaboração própria

A análise dos riscos identificados pela auditoria revela que existem áreas críticas que exigem atenção para garantir o alinhamento estratégico da TI com as metas institucionais e a continuidade operacional dos serviços tecnológicos. Os riscos apontados, como o desalinhamento estratégico devido à falta de um Plano Diretor de Tecnologia da Informação (PDTI) e a vulnerabilidade decorrente de infraestrutura inadequada e falta de recursos humanos, são pontos que merecem consideração urgente, mas não representam uma lista exaustiva de todos os riscos possíveis.

A auditoria sugeriu controles para mitigar esses riscos, como a criação de um PDTI e a implementação de políticas de segurança cibernética, porém não foi realizada uma análise sobre a existência ou não desses

controles na prática. Dessa forma, recomenda-se que a gestão realize uma revisão detalhada dos controles internos atuais e avalie a implementação das sugestões apresentadas, além de considerar outros riscos que possam surgir no futuro.

4. Considerações Finais

A auditoria interna realizou o levantamento de informações referente ao macroprocesso Tecnologia da Informação e Comunicação. De acordo com o Regimento Geral do IFPE, artigo 60, compete à Diretoria de Avaliação e Desenvolvimento de Tecnologias, implantar e manter serviços de TI de natureza sistêmica.

A presente análise evidenciou desafios críticos enfrentados pela Diretoria de Tecnologia da Informação (DTI) do IFPE, que impactam significativamente a capacidade de alinhar as estratégias de TI às metas institucionais e de garantir a eficiência e segurança das operações. A ausência de um Plano Diretor de Tecnologia da Informação (PDTI), instrumento essencial para o planejamento estratégico, foi identificada como uma fragilidade central, sendo recomendada sua elaboração com urgência por meio da Nota de Auditoria 13/2024.

O foco predominante no planejamento para manutenção de serviços existentes, aliado à falta de um monitoramento robusto e de avaliação contínua, compromete a evolução tecnológica e o cumprimento das metas previstas no Regimento Geral do IFPE. As fragilidades no ciclo PDCA e na utilização do sistema SCOPI reforçam a necessidade de aprimoramento nos mecanismos de gestão e revisão do planejamento. Além disso, a predominância de sistemas próprios de código aberto reflete uma estratégia de autossuficiência que, embora positiva, apresenta desafios em termos de manutenção, atualização e suporte, agravados por recursos humanos e técnicos insuficientes.

A análise destacou ainda a inexistência de processos estruturados de gestão de riscos, a falta de recursos especializados e a limitada integração com outras áreas, dificultando a identificação e mitigação de riscos. A ausência de KPIs formalizados para as atividades de implantação e manutenção de serviços de TI é outra lacuna que compromete a gestão de desempenho e a melhoria contínua.

Diante do exposto, este relatório reforça a urgência na adoção de medidas estratégicas para reverter o cenário dos riscos identificados. **A priorização na elaboração do PDTI, no fortalecimento da infraestrutura e recursos humanos, e na implementação de políticas de segurança cibernética é essencial**.

Adicionalmente, **sugere-se** a adoção de metodologias como SMART Goals, ciclos PDCA e a definição de indicadores de desempenho alinhados às metas estratégicas institucionais. Essas ações são indispensáveis para garantir a eficiência das operações de TI, promover a evolução tecnológica e proteger os ativos institucionais, assegurando a continuidade e a qualidade dos serviços prestados pelo IFPE.

Relatório elaborado pela auditora Wenia Ventura de Farias Caldas, SIAPE 2746091 e revisado pelo auditor David Lima Vilela SIAPE 1867177.

Encaminhe-se ao Magnífico Reitor do IFPE, na condição de Presidente do Conselho Superior do IFPE e ao Diretor de Tecnologia da Informação.

Recife, 19 de dezembro de 2024.

David Lima Vilela
Titular Unidade de Auditoria Interna
SIAPE 1867177

[1} * Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal, pág 64.

Disponível em: https://repositorio.cgu.gov.br/bitstream/1/64815/11/Manual_de_orientacoes_tecnicas_2017.pdf

[1] Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal, pág 64. Disponível em: https://repositorio.cgu.gov.br/bitstream/1/64815/11/Manual_de_orientacoes_tecnicas_2017.pdf

Documento assinado eletronicamente por **David Lima Vilela**, **Auditor**, em 19/12/2024, às 15:37, conforme art. 6º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade do documento pode ser conferida no site https://sei.ifpe.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1571486** e o código CRC **EA940E1B**.