INSTITUTO FEDERAL
Alagoas

AÇÃO Nº 13/2025

Governança e Gestão de Tecnologia da Informação e da Segurança da Informação

Fevereiro de 2026

Instituto Federal de Alagoas
Auditoria Interna

RELATÓRIO DE AVALIAÇÃO
Ação: 13/2025 – Governança e Gestão de Tecnologia da Informação e da Segurança da Informação
Unidade Examinada: DTI
Nº do Relatório: 04/2025

MISSÃO

Fortalecer e assessorar a gestão, bem como propor medidas para a racionalização das ações de controle no sentido de contribuir para a garantia da legalidade, da moralidade e da probidade dos atos da administração do Instituto Federal de Alagoas – Ifal.

AVALIAÇÃO

O trabalho de avaliação, como parte da atividade de auditoria interna, consiste na obtenção e na análise de evidências visando 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 Unidade Auditada, e contribuir para o seu aprimoramento.

QUAL FOI O TRABALHO REALIZADO PELA AUDITORIA INTERNA DO IFAL?

A Auditoria Interna do Ifal realizou a Ação nº 13/2025, que consistiu em avaliar a governança e gestão de tecnologia da informação e da segurança da informação, com ênfase na implementação do Programa de Privacidade e Segurança da Informação (PPSI).

POR QUE A AUDINT REALIZOU ESSE TRABALHO?

O trabalho foi executado em atendimento ao Plano Anual de Auditoria Interna (Paint/2025), cujo objetivo foi avaliar a governança e a gestão de tecnologia da informação e de segurança da informação no Ifal, com ênfase na implementação das diretrizes do Programa de Privacidade e Segurança da Informação (PPSI).

QUAIS AS CONCLUSÕES ALCANÇADAS PELA AUDINT?

Foram identificados avanços significativos, como a publicação da Política de Segurança da Informação - Resolução nº 111/2023, a criação do Comitê de Segurança da Informação, a publicação de Diretrizes Específicas da Política de Segurança da Informação e a nomeação do encarregado pelo tratamento de dados pessoais. Contudo, fragilidades foram constatadas: ausência de ato normativo para segregação de funções, implementação parcial das diretrizes específicas, falta de monitoramento sistemático e carência de mapeamento de processos e de avaliação de riscos.

QUAIS AS RECOMENDAÇÕES QUE DEVERÃO SER ADOTADAS?

A Audint recomendou: publicação de ato normativo que regulamente a segregação de funções; execução efetiva das diretrizes do PPSI com planos de ação e indicadores; elaboração de documentos formais que comprovem monitoramento; realização de treinamentos e conscientização da comunidade acadêmica quanto às boas práticas de privacidade de dados e de segurança da informação; e mapeamento de processos e avaliação de riscos.

LISTA DE SIGLAS E ABREVIATURAS

Audint - Auditoria Interna do Instituto Federal de Alagoas

CGU - Controladoria-Geral da União

CIS - Critical Security Controls v8

COBIT - Control Objectives for Information and Related Technologies

CONSUP - Conselho Superior

COSO - Committee of Sponsoring Organizations of the Treadway Commission

iESGo - Índice de Governança e Sustentabilidade

Ifal - Instituto Federal de Alagoas

ISO - International Organization of Standardization

LGPD - Lei Geral de Proteção de Dados Pessoais

MGI – Ministério da Gestão e da Inovação em Serviços Públicos

MOT - Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental do Poder Executivo Federal

Paint - Plano Anual de Auditoria Interna

PDI - Plano de Desenvolvimento Institucional

PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação

PETIC - Plano Estratégico de Tecnologia da Informação e Comunicação

PPSI - Programa de Privacidade e Segurança da Informação

SCI - Sistema de Controle Interno

SGD - Secretaria de Governo Digital

SI - Segurança da Informação

SISP - Sistema de Administração dos Recursos de Tecnologia da Informação

TCU - Tribunal de Contas da União

TI - Tecnologia da Informação

TIC - Tecnologia da Informação e Comunicação

SUMÁRIO

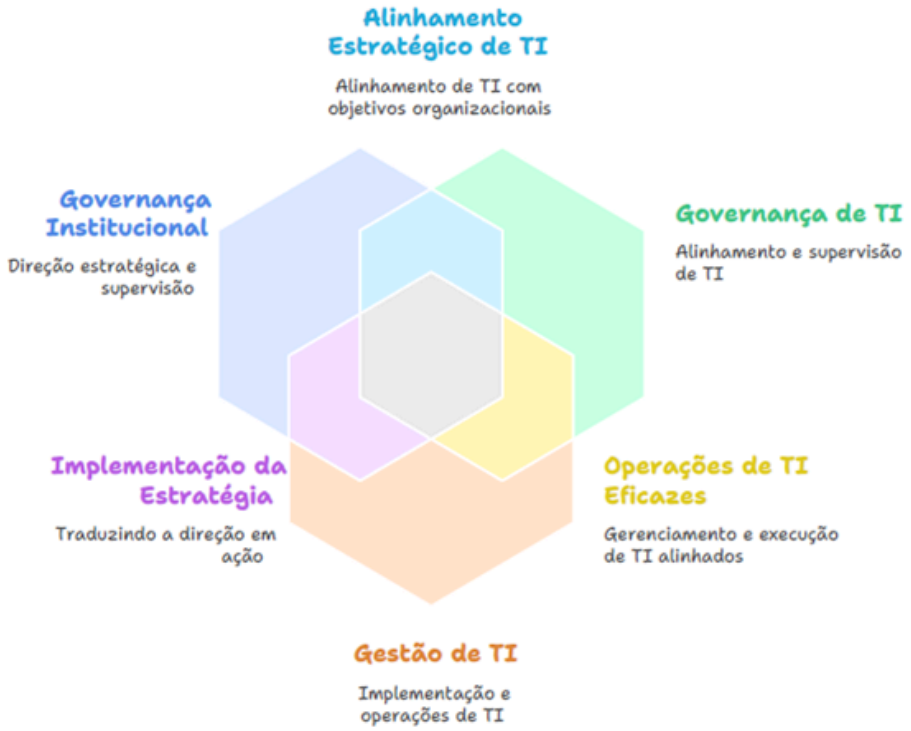
1. INTRODUÇÃO

Este Relatório refere-se à ação de auditoria nº 13/2025 - Governança e Gestão de Tecnologia da Informação e da Segurança da Informação, prevista no Plano Anual de Auditoria Interna (Paint/2025). O presente trabalho é de avaliação da governança e da gestão de tecnologia da informação e de segurança da informação no âmbito do Instituto Federal de Alagoas (Ifal), com ênfase na implementação das diretrizes do Programa de Privacidade e Segurança da Informação (PPSI).

A Governança e a Gestão da tecnologia da informação (TI) e da segurança da informação (SI) são elementos estratégicos importantes para assegurar a integridade das informações, a proteção de dados sensíveis e a continuidade dos serviços prestados à sociedade - ao mesmo tempo em que previnem prejuízos financeiros, danos à imagem, maior segurança a ataques cibernéticos e riscos institucionais. No contexto do Ifal, TI e SI adquirem relevância adicional diante do aumento da dependência de soluções digitais e do imperativo de conformidade com normativos legais.

A imagem a seguir ilustra, de forma integrada, elementos e inter-relações entre governança e gestão. Ela representa como diretrizes estratégicas, processos de gestão, controles internos e recursos tecnológicos se articulam para assegurar a continuidade e a confiabilidade dos serviços prestados.

Figura 1 - Integração entre Governança Institucional, Governança de TI, Gestão de TI e Objetivos Estratégicos para alcançar Valor Organizacional



Fonte: imagem criada através do Napkin IA.

A Política de Governança da Administração Pública Federal, instituída pelo Decreto nº 9.203/2017, estabelece que a governança compreende os mecanismos de liderança, estratégia e controle para avaliar, direcionar e monitorar a gestão. A governança possui como função principal definir diretrizes, avaliar resultados e monitorar o desempenho institucional, enquanto a gestão executa essas diretrizes por meio da entrega de produtos e serviços, bem como do controle operacional das atividades.

Na área da tecnologia da informação e da segurança da informação, essa distinção permanece: a governança de TI e SI estabelece o direcionamento estratégico e define os mecanismos de tomada de decisão, ao passo que a sua gestão operacionaliza essas diretrizes, garantindo que os recursos tecnológicos sejam utilizados de forma eficaz, eficiente e alinhada aos objetivos institucionais.

À luz da Lei n.º 14.129/2021, que estabelece princípios, regras e instrumentos para o governo digital e para o aumento da eficiência da administração pública, observa-se que a efetividade da governança e da gestão da tecnologia da informação e da segurança da informação no Ifal demanda avanços. Esses avanços passam pela implementação de mecanismos que assegurem a integridade, a disponibilidade e a confiabilidade dos dados. Esses mecanismos incluirão, no mínimo, formas de acompanhamento de resultados, soluções para a melhoria do desempenho das organizações e instrumentos de promoção do processo decisório fundamentado em evidências. O art. 3º da referida Lei prevê, entre seus princípios e diretrizes, a promoção da transparência, da eficiência e da inovação na prestação de serviços públicos, pilares que somente serão alcançados mediante a consolidação de práticas robustas de segregação de funções, monitoramento contínuo e gestão de riscos.

Por sua vez, a Portaria SGD/MGI nº 852/2023 institui o Programa de Privacidade e Segurança da Informação (PPSI), cuja adesão é obrigatória para todos os órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP). O PPSI estrutura-se em cinco eixos: governança, metodologia, maturidade, pessoas e tecnologia, e visa elevar o grau de proteção da informação, com foco em privacidade, resiliência e continuidade dos serviços públicos.

Mais recentemente, o Decreto nº 12.198 de 2024 institui a Estratégia Federal de Governo Digital para o período de 2024 a 2027 e a Infraestrutura Nacional de Dados, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. O referido Decreto traz no seu art. 5º que os “órgãos e as entidades da administração pública federal direta, autárquica e fundacional instituirão Comitê de Governança Digital ou colegiado equivalente, para deliberar sobre os assuntos relativos à implementação das ações de governo digital e ao uso de recursos de tecnologia da informação e comunicação”.

O Acórdão nº 2387/2024 – Plenário do Tribunal de Contas da União (TCU) reforça a necessidade de que os órgãos públicos federais promovam avaliações sistemáticas da maturidade de sua governança de TI e SI, com base em referenciais reconhecidos e aderentes

ao PPSI, à LGPD e ao CIS Controls v8. O TCU destaca que a ausência de mecanismos efetivos de controle e de gestão integrada dos riscos relacionados à segurança da informação representa vulnerabilidade crítica à integridade institucional.

Cabe destacar ainda que a realização desta atividade possui como objetivo geral avaliar a governança e a gestão de tecnologia da informação e de segurança da informação no âmbito do Instituto Federal de Alagoas (Ifal), com ênfase na implementação das diretrizes do Programa de Privacidade e Segurança da Informação (PPSI).

Conforme orientações da Controladoria-Geral da União (MOT, 2017), os objetivos devem consistir, basicamente, nas questões a que a auditoria se propõe a responder ao longo do trabalho. Assim como, devem ser considerados aspectos como a extensão dos procedimentos, a profundidade dos testes, o tempo necessário, os recursos disponíveis, a metodologia adotada e a natureza da auditoria, a fim de delimitar de forma adequada a sua abrangência e garantir a sua execução. No presente trabalho, foram delineados os seguintes objetivos geral e específicos:

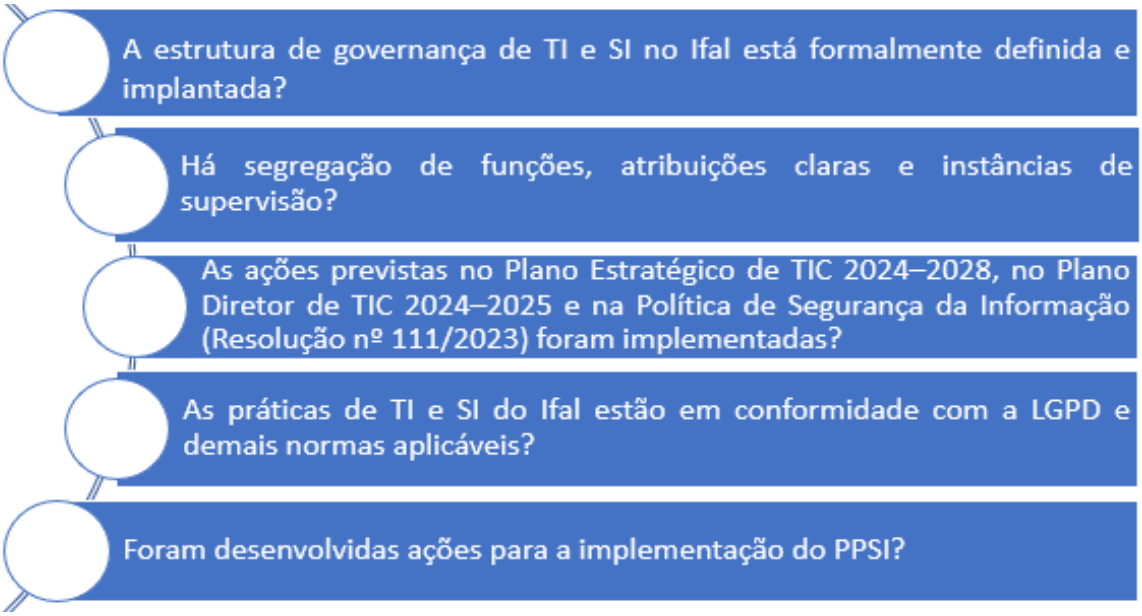
Objetivo Geral

- Avaliar a governança e a gestão de Tecnologia da Informação e da Segurança da Informação no âmbito do Instituto Federal de Alagoas (Ifal).

Objetivos Específicos

- Avaliar a conformidade da estrutura de governança de TI e de segurança da informação com os documentos normativos institucionais, especialmente: Plano Estratégico de TIC 2024–2028; Plano Diretor de TIC 2024–2025 e Política de Segurança da Informação (Resolução nº 111/2023);
- Avaliar a existência, implementação e eficácia de controles internos relacionados à segurança da informação, o que inclui: Políticas e normativos internos; Processos de gestão de acessos; Monitoramento e resposta a incidentes; Continuidade de serviços de TI; Gestão de acessos e identidades, e Proteção de dados pessoais;
- Analisar as ações de autoavaliação, planejamento e acompanhamento da implementação do PPSI.

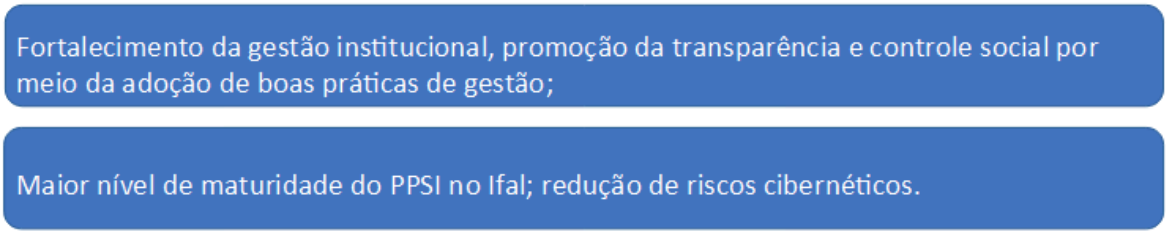
As questões que nortearam o trabalho da Auditoria Interna para alcance dos objetivos propostos são as reproduzidas a seguir:



1.1 BENEFÍCIOS ESPERADOS

A implementação das recomendações apresentadas neste relatório pretende alcançar os seguintes benefícios para o Instituto Federal de Alagoas (Ifal):

- Fortalecimento da governança e da gestão da segurança da informação no Ifal;
- Redução do risco de concentração indevida de funções e de conflitos de interesse;
- Alinhamento com normativos e boas práticas de gestão pública; maior efetividade do PPSI;
- Maior capacidade institucional de proteção da informação;
- Redução ou mitigação dos riscos relacionados à segurança da informação;
- Alinhamento com normativos e boas práticas nacionais e internacionais;



2. RESULTADOS DOS EXAMES

A equipe da Audint recorreu metodologicamente aos documentos oficiais e às boas práticas de gestão pública para legitimar os achados identificados, os quais subsidiaram as respostas para as questões de auditoria aludidas na introdução deste trabalho. Logo, as fontes utilizadas como critério de auditoria estão amparadas em atos normativos no âmbito do Ifal e na legislação vigente de âmbito federal.

Para a Auditoria, o achado é o resultado da comparação entre um critério preestabelecido pela equipe de auditoria durante a fase de planejamento e a condição real encontrada durante a realização dos exames, comprovada por evidências. O critério, por sua vez, sustenta-se em procedimentos e normas legais e é o parâmetro que serve para comparar com a situação encontrada. Inicialmente, houve levantamento de informações, estudos preliminares e realização de reunião com o diretor da Diretoria de Tecnologia e Informação (DTI).

Cabe destacar, entretanto, que a execução desta ação de auditoria passou por limitações. Foi elaborada uma Solicitação de Auditoria (SA) com questionário específico destinado à obtenção de informações relevantes para subsidiar os trabalhos. Mesmo após as prorrogações de prazo, as respostas não foram encaminhadas pela unidade auditada. Diante disso, a equipe decidiu prosseguir com a elaboração do relatório sem as informações da SA. Para tanto, recorreu à análise documental de atos e normativos disponíveis no site do Ifal, bem como da reunião realizada com o diretor da DTI.

Isso dito, as evidências relativas aos achados que subsidiaram a opinião da Audint e as considerações concernentes ao desenvolvimento do presente relatório são expostas nas subseções subsequentes.

2.1 Fragilidades no que se refere à segregação de funções

A Resolução nº 111/2023 - Consup/Ifal, em seu Art. 5º, inciso III, apresenta a seguinte redação:

> As normas e diretrizes da Política de Segurança da Informação do Ifal deverá se guiar pelos seguintes princípios:
> Segregação de função: funções de planejamento, execução e controle devem ser segregadas de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos;

Apesar da previsão normativa da Resolução nº 111/2023 quanto à necessidade de segregação de funções, não há documentos publicados que estabeleçam formalmente essa estrutura. Portanto, não foram identificadas portarias de nomeação ou outros documentos que comprovem a segregação de funções.

O princípio da segregação de funções, previsto no Art. 5º, inciso III, da Resolução nº 111/2023 – Consup/Ifal, constitui medida importante para a mitigação de riscos no âmbito da segurança da informação. Tal diretriz decorre do entendimento de que as funções de planejamento, execução e controle não devem concentrar-se em um único indivíduo ou até mesmo em um setor, pois essa sobreposição de responsabilidades aumenta a possibilidade de ocorrência de ações que comprometem a integridade, a confidencialidade e a disponibilidade dos ativos.

Ao promover a separação clara dessas funções, reduz-se a probabilidade de modificação indevida, uso não autorizado ou manuseio não intencional das informações e recursos. Além disso, possibilita maior transparência, rastreabilidade e responsabilização nas atividades, o que fortalece os mecanismos de governança e de gestão.

A segregação de funções não deve ser pensada apenas como uma exigência normativa. Trata-se de um instrumento estruturante para a efetividade da Política de Segurança da Informação no Ifal. Invariavelmente, ela contribui diretamente para a resiliência institucional, conforme a Resolução nº 111/2023 - Consup/Ifal, inciso VII, que estabelece que “os sistemas e processos devem ser projetados para poderem resistir ou se recuperarem dos efeitos de um desastre e retornar à normalidade das operações”.

Por sua vez, o MOT (pág. 136, 2017) vai afirmar que a segregação de funções “consiste na separação de funções de tal forma que estejam segregadas entre pessoas diferentes, a fim de reduzir o risco de erros ou de ações inadequadas, ou fraudulentas.” Portanto, a segregação de funções é um instrumento relevante do controle interno e da governança, por estabelecer a separação de atribuições. Ao tentar impedir que uma mesma pessoa detenha controle sobre todas as etapas de um processo – do planejamento à execução e ao controle –, essa prática reduz significativamente a probabilidade de erros não detectados, bem como de condutas inadequadas.

A ausência de normativos internos sobre o referido tema indica que o Ifal não possui, até o momento, uma estrutura organizacional definida para tratar de forma clara e formal a governança da segurança da informação, em descumprimento aos princípios da Resolução nº 111/2023. Por isso, é importante adotar, como boa prática, a implementação de normativos internos sobre segregação de funções com definição clara de papéis e responsabilidades.

Diante desse contexto, as seguintes causas, consequências, recomendações e benefícios esperados são apresentados em razão das fragilidades no que se refere à segregação de funções:

Possíveis causas

Número insuficiente de servidores no setor e inexistência de regulamentação interna que defina a estrutura de governança em segurança da informação, em especial à segregação de funções.

Possível consequência

Fragilidade na governança de segurança da informação.

Recomendação

Elaborar, publicar e implementar ato normativo que estabeleça a estrutura de governança da segurança da informação, com definição clara das atribuições dos agentes envolvidos, para atender ao princípio da segregação de funções previsto na Resolução nº 111/2023 - Consup/Ifal.

Benefícios esperados

Fortalecimento da governança e da gestão da segurança da informação no Ifal; redução do risco de concentração indevida de funções e de conflitos de interesse; alinhamento com normativos e boas práticas de gestão pública.

Manifestação da Gestão

Esta Diretoria se manifesta de acordo com os achados apresentados pelo Relatório Preliminar referente à Ação de Auditoria nº 13/2025.

Análise da Auditoria Interna

Reitera-se a importância da elaboração, publicação e implementação de ato normativo que estabeleça a estrutura de governança da segurança da informação, com definição clara das atribuições dos agentes envolvidos, para atender ao princípio da segregação de funções previsto na Resolução nº 111/2023 - Consup/Ifal. Dessa forma, diante da manifestação apresentada pela gestão em que corrobora o achado de auditoria, mantém-se a recomendação em monitoramento até que seja efetivada a medida indicada.

Assim sendo, esta Audint considerará atendida a recomendação quando constatar a sua efetiva implementação através de trabalhos futuros de monitoramento.

2.2. Implementação parcial das ações previstas nos instrumentos estratégicos e normativos relacionados à segurança da informação

O Programa de Privacidade e Segurança da Informação do Ifal (PPSI) conta com uma base normativa consolidada nos últimos anos, tendo como eixo principal a Resolução nº 111/2023 e os planos estratégicos da área de TIC – PETIC 2024–2028 e PDTIC 2024–2025. Entre 2024 e 2025, o Instituto publicou um conjunto de diretrizes específicas por meio de portarias normativas, contemplando temas como tratamento da informação, segurança física e do ambiente, gestão de incidentes de segurança da informação, gestão de ativos, gestão do uso dos recursos operacionais e de comunicação, controle de acesso, gestão de riscos e gestão de continuidade.

Esse arcabouço normativo representa um avanço significativo em termos de governança e gestão. Contudo, ao analisar sua execução, verificou-se que a aplicação prática permanece incipiente ou sem comprovação documental suficiente. Não foram identificados planos de ação vinculados às diretrizes específicas, indicadores de desempenho ou relatórios de acompanhamento. Da mesma forma, não foram localizados controles internos como, por exemplo, registros de ações de simulação (como resposta a incidentes ou testes de continuidade) ou outras evidências que atestem a efetiva aplicação das diretrizes previstas.

Portanto, embora se reconheça o progresso obtido no campo normativo, persistem lacunas relevantes na operacionalização do PPSI, o que pode comprometer a proteção de dados sensíveis, a continuidade das operações críticas e a conformidade institucional frente à Lei Geral de Proteção de Dados (LGPD) e demais legislações aplicáveis. Desse modo, entre as boas práticas a serem adotadas, destacam-se a estruturação de mecanismos eficazes de monitoramento, a realização periódica de testes (como simulações de resposta a incidentes), a capacitação contínua de pessoal e a divulgação de relatórios de execução.

Diante exposto, as seguintes causas, consequências, recomendações e benefícios esperados são apresentados em razão da implementação parcial das ações previstas nos instrumentos estratégicos e normativos relacionados à segurança da informação:

Possíveis causas

Programa ainda em fase de adequação à Política de Segurança da Informação; inexistência de instrumentos de monitoramento e avaliação, mesmo na etapa de implementação; e limitações de pessoal e de recursos para a execução das ações previstas.

Possíveis Consequências

Não alinhamento entre os instrumentos normativos e sua aplicação prática; manutenção de vulnerabilidades operacionais e riscos à integridade, confidencialidade e disponibilidade das informações institucionais; e fragilidades na resposta a incidentes e na continuidade das operações de TIC.

Recomendações

Executar as diretrizes específicas da Política de Segurança da Informação; Acompanhar, por meio de indicadores, as diretrizes específicas da Política de Segurança da Informação; e realizar treinamentos de pessoal.

Benefícios esperados

Maior efetividade do PPSI; elevação da capacidade institucional de proteção da informação; redução ou mitigação dos riscos relacionados à segurança da informação; alinhamento com normativos e boas práticas nacionais e internacionais.

Manifestação da Gestão

Esta Diretoria se manifesta de acordo com os achados apresentados pelo Relatório Preliminar referente à Ação de Auditoria nº 13/2025.

Análise da Auditoria Interna

Reitera-se a importância de planos de ação vinculados às diretrizes específicas, indicadores de desempenho e relatórios de monitoramento. Tais lacunas na operacionalização do PPSI podem comprometer a proteção de dados sensíveis, a continuidade das operações críticas e a conformidade institucional frente à Lei Geral de Proteção de Dados (LGPD) e demais legislações aplicáveis. Dessa forma, diante da manifestação apresentada pela gestão em que corrobora o achado da auditoria, mantém-se a recomendação em monitoramento até que sejam efetivadas as medidas indicadas.

Assim sendo, esta Audint considerará atendida a recomendação quando constatar a sua efetiva implementação através de trabalhos futuros de monitoramento.

2.3. Fragilidade no monitoramento das diretrizes específicas da Política de Segurança da Informação, devido à ausência de registros formais

À luz das diretrizes do COBIT, que estabelece uma estrutura para a governança e gestão da tecnologia da informação; dos conceitos previstos no COSO ERM, que estabeleceu o gerenciamento de riscos, não como uma função ou departamento, mas como a cultura, os

recursos e as práticas que as organizações integram com a estratégia definida e executada, visando gerenciar o risco na criação, preservação e valorização; da Instrução Normativa Conjunta MP/CGU nº 01, de 10 de maio de 2016, que trata dos controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal; da Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021; e do Guia de Governança de TIC do SISP v. 2.0, evidencia-se a necessidade de um gerenciamento efetivo da tecnologia da informação e da segurança da informação, considerando sua relevância para o alcance dos objetivos institucionais.

Neste mesmo contexto, o Decreto nº 7.579, de 11 de outubro de 2011, apresenta diretrizes relevantes para a implementação da governança de TI, por meio do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP, abrangendo o planejamento, a coordenação, a organização, a operação, o controle e a supervisão dos recursos de tecnologia da informação dos órgãos e entidades da administração pública federal direta, autárquica e fundacional. Além dos normativos já mencionados, destacam-se também o Decreto nº 12.573, de 4 de agosto de 2025, que institui a Estratégia Nacional de Cibersegurança; a Portaria SGD/MGI nº 852, de 28 de março de 2023, que dispõe sobre o Programa de Privacidade e Segurança da Informação – PPSI; a Lei 14.129/2021, que dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública; e a ISO 27001, norma internacional que estabelece requisitos para um Sistema de Gestão de Segurança da Informação (SGSI). Esses instrumentos, somados a outras legislações nacionais e internacionais, reforçam a necessidade de uma governança e gestão de TI e SI eficazes.

No âmbito do Ifal, observa-se a existência de diversos normativos voltados à proteção dos dados sob sua responsabilidade — em especial os sensíveis, pessoais e estratégicos — ao longo de todo o seu ciclo de vida, segundo a Lei Geral de Proteção de Dados Pessoais (LGPD). Destaca-se, nesse contexto, a Portaria Normativa nº 31/2022 – REIT, que regulamenta o uso institucional de dados pessoais, além de outras legislações aplicáveis. Tais dispositivos podem ser consultados nas Portarias Normativas e Diretrizes Específicas disponíveis no site da instituição (https://www2.ifal.edu.br/o-ifal/tecnologia-da-informacao/comites). Ressalta-se, ainda, que a Política de Segurança da Informação no âmbito do Instituto Federal de Alagoas – Ifal está normatizada pela Resolução nº 111/2023 – CONSUP/IFAL.

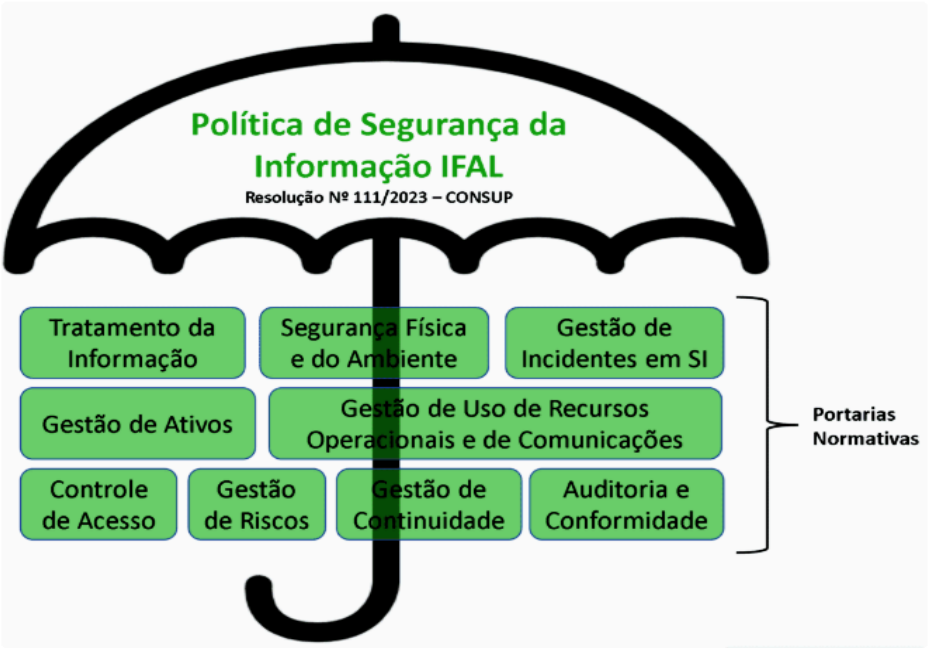
A Política estabelece normas, diretrizes e princípios destinados a assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações do Ifal. Em seu art. 7º, apresenta as seguintes diretrizes específicas:

> I – tratamento da informação;
> II – segurança física e ambiental;
> III – gestão de incidentes em segurança da informação;
> IV – gestão de ativos;
> V – gestão do uso de recursos operacionais e de meios de comunicação, como e-mail, acesso à internet, mídias sociais, computação em nuvem, entre outros;
> VI – controles de acesso;

VII – gestão de riscos;
VIII – gestão da continuidade; e
IX – auditoria e conformidade

Conforme ilustrado na Figura 2, a Estrutura da Política de Segurança da Informação do Ifal organiza, de forma sistêmica, as diretrizes específicas estabelecidas pela Resolução nº 111/2023 – Consup/Ifal.

Figura 2 – Estrutura da Política de Segurança da Informação do Ifal



Fonte: Site institucional do Ifal

Embora a Política de Segurança da Informação e os demais normativos estejam estabelecidos, não foram identificados documentos, como atas, registros, relatórios de conformidade e não conformidade, riscos identificados ou cronogramas que comprovem a efetiva implementação e o monitoramento das ações previstas nessas diretrizes relacionadas à TI e à SI.

Ressalta-se, ainda, que o TCU, por meio do relatório individual da autoavaliação - iESGo2024, Acórdão 1913/2024 - TCU - Plenário, aponta como inexpressiva a capacidade do Ifal de gerir os riscos de tecnologia da informação e de segurança da informação, conforme apresentado pelo *Indicador: RiscosTISegInfo - Capacidade em gerir riscos de tecnologia da informação e da segurança da informação*

Em reunião com o Gestor de TI, referente aos pontos mencionados, foi verificado que alguns já estão implementados, enquanto outros encontram-se em fase de implementação. Segundo o Gestor, a ausência de evidências sobre a implementação e o acompanhamento efetivo das ações estabelecidas decorre do número reduzido de servidores no setor.

Considerando que a conformidade com a LGPD exige uma abordagem integrada entre diferentes áreas, combinando processos de governança eficientes, políticas e normativos, controles internos e monitoramento contínuo, o acompanhamento insuficiente das diretrizes

estabelecidas pode fragilizar a segurança da informação e a tomada de decisões, além de gerar prejuízos à instituição e à sociedade, comprometendo seus objetivos institucionais.

Diante exposto, as seguintes causas, consequências, recomendações e benefícios esperados são apresentados em razão da ausência de monitoramento das diretrizes específicas relacionadas à Política de Segurança da Informação:

Possível causa

Número reduzido de servidores no setor de TI/SI.

Possíveis Consequências

Fragilidades na segurança da informação e na tomada de decisões, podendo, ainda, levar a prejuízos para a instituição e para a sociedade – além de comprometer os objetivos institucionais.

Recomendação

Elaborar documentos formais (atas, registros, relatórios, cronogramas, etc) que comprovem e permitam aos órgãos de controle avaliar a implementação e o efetivo acompanhamento das diretrizes estabelecidas na Política de Segurança da Informação.

Benefícios esperados

Fortalecimento da gestão institucional, promoção da transparência e controle social por meio da adoção de boas práticas de gestão.

Manifestação da Gestão

Esta Diretoria se manifesta de acordo com os achados apresentados pelo Relatório Preliminar referente à Ação de Auditoria nº 13/2025.

Análise da Auditoria Interna

Embora a Política de Segurança da Informação e demais normativos estejam estabelecidos; a não elaboração de documentos, como atas, registros, relatórios de conformidade e não conformidade, riscos identificados ou cronogramas que comprovem a efetiva implementação e o monitoramento das ações previstas nas diretrizes relacionadas à TI e à SI, podem levar a prejuízos para a instituição na tomada de decisões, e para a sociedade – além de comprometer os objetivos institucionais.

Dessa forma, diante da manifestação apresentada pela gestão em que corrobora o achado da auditoria, mantém-se a recomendação em monitoramento até que sejam efetivadas as medidas indicadas.

Assim sendo, esta Audint considerará atendida a recomendação quando constatar a sua efetiva implementação através de trabalhos futuros de monitoramento.

2.4. Fragilidades na implementação do Programa de Privacidade e Segurança da Informação (PPSI)

Pensado para elevar a maturidade e a resiliência dos órgãos e entidades da administração pública federal no que se refere à privacidade e à segurança da informação, especialmente nas unidades que integram o SISP – conforme estabelece o art. 3º da Portaria SGD/MGI nº 852 –, o PPSI está estruturado em cinco áreas temáticas: governança, maturidade, metodologia, pessoas e tecnologia. Para atender a essas áreas, o Ifal já definiu sua Política de Segurança da Informação, instituiu o Comitê de Segurança da Informação, regulamentou as diretrizes específicas, nomeou o encarregado pela proteção de dados pessoais e iniciou a implantação de um software de apoio à execução dos processos do programa.

Entretanto, apesar desses avanços, ainda não foram realizados o mapeamento de processos, a avaliação de riscos nem as ações de treinamento e conscientização da comunidade acadêmica sobre boas práticas relacionadas ao PPSI — aspectos fundamentais para assegurar a proteção de dados e a segurança da informação. Ademais, não foram encontradas evidências formais de avaliação, análise ou planejamento voltados à plena implementação do Programa de Privacidade e Segurança da Informação.

Conforme o Guia do Framework de Privacidade e Segurança da Informação da Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos — que orienta as instituições públicas na identificação, acompanhamento e tratamento de lacunas relacionadas à privacidade, proteção de dados pessoais e segurança da informação —, é necessário estabelecer controles efetivos nesse processo.

Para tanto, o documento apresenta o modelo de Sistema de Controle Interno estruturado em três linhas, consoante a Instrução Normativa nº 3, de 9 de junho de 2017, da Controladoria-Geral da União (CGU):

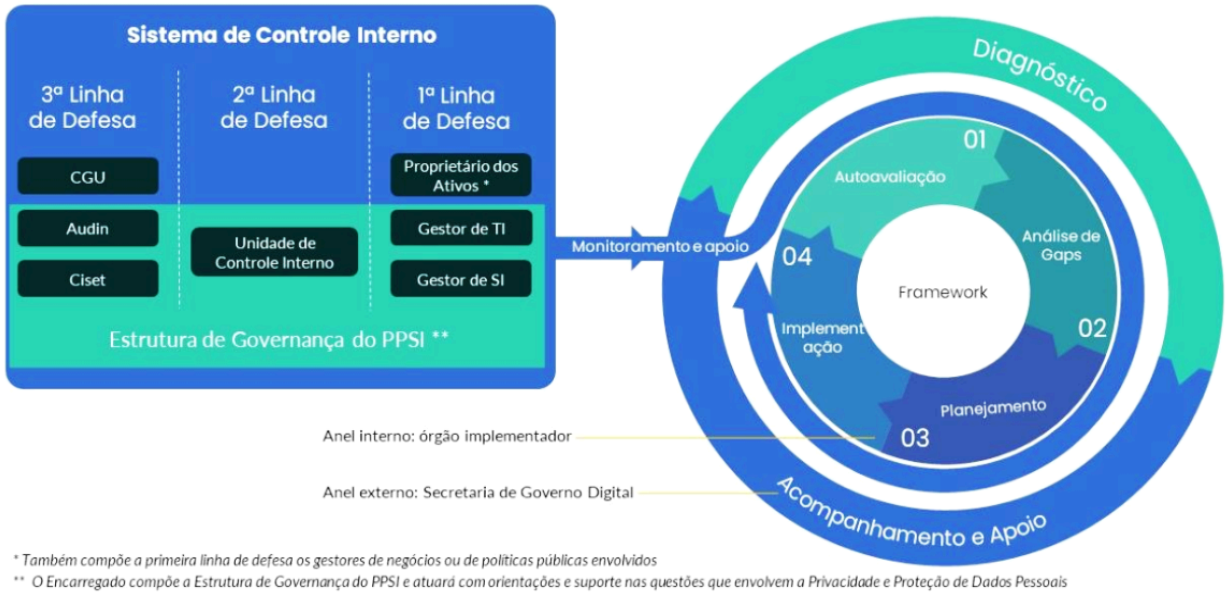
> Primeira linha – responsável por identificar, avaliar, controlar e mitigar os riscos, no sentido de atingimento de metas e objetivos da instituição;
>
> Segunda linha – objetiva assegurar que as atividades realizadas pela primeira linha sejam desenvolvidas e executadas de forma adequada.
>
> Terceira linha – representada pela atividade de auditoria interna governamental. Presta serviços de avaliação e de consultoria com base nos pressupostos de autonomia técnica e de objetividade.

O Guia destaca ainda que a gestão de privacidade e segurança da informação se fundamenta na política de governança da Administração Pública Federal direta, autárquica e fundacional, prevista no Decreto nº 9.203, de 22 de novembro de 2017. Esse decreto define governança pública como o conjunto de mecanismos de liderança, estratégia e controle destinados a avaliar, direcionar e monitorar a gestão, com foco na condução de políticas públicas e na prestação de serviços de interesse da sociedade.

Além disso, apresenta a gestão de riscos como um processo contínuo, instituído, direcionado e acompanhado pela alta administração, que envolve a identificação, avaliação e tratamento de eventos que possam impactar a organização. Esse processo busca oferecer segurança razoável quanto ao alcance dos objetivos institucionais, fornecendo direcionadores para que a alta administração estabeleça, mantenha, monitore e aperfeiçoe sistemas de gestão de riscos e de controles internos. O objetivo é possibilitar a identificação, avaliação, tratamento, monitoramento e análise crítica de riscos que possam comprometer a execução da estratégia e o cumprimento da missão institucional.

Dessa forma, é fundamental observar os papéis de cada linha no processo de desenvolvimento e implementação do Framework do PPSI. A Figura 3 apresenta, de maneira resumida, a metodologia de implementação do Framework, destacando sua integração ao Sistema de Controle Interno (SCI), os principais atores envolvidos e as atividades a serem desenvolvidas.

Figura 3 – Metodologia de Implementação do Framework



Fonte: Guia do Framework de Privacidade e Segurança da Informação

O Guia também destaca a importância do treinamento e da conscientização de todos os envolvidos no processo, como forma de assegurar a conformidade e a correta execução de cada etapa da implementação. Recomenda-se, sobretudo, que o órgão estabeleça e mantenha procedimentos de monitoramento voltados ao acompanhamento da execução dos controles e das medidas planejadas.

Além disso, o Decreto nº 12.573, de 4 de agosto de 2025, que institui a Estratégia Nacional de Cibersegurança, dispõe em seu art. 4º que a proteção e a conscientização do cidadão e da sociedade devem contemplar, no mínimo, as seguintes ações:

> IV - incentivo à capacitação de professores e gestores, públicos e privados, em cibersegurança;
>
> V - incentivo à inclusão de temas relacionados à cibersegurança nos currículos de todos os níveis educacionais;

Nesse sentido, o Plano Estratégico de Tecnologia da Informação e Comunicação do Ifal (PETIC 2024–2028) contempla, no âmbito do Objetivo Estratégico de TIC 11 (Aprimorar a Segurança da Informação e Comunicação), a abrangência das campanhas de conscientização de segurança da informação e comunicação direcionadas. Esse compromisso está expresso no Indicador Estratégico de TIC 11.2, que estabelece metas progressivas para execução, o que demonstra alinhamento direto com as diretrizes normativas.

Em reunião com o Gestor de TI, verificou-se que os pontos anteriormente destacados ainda não foram implementados devido ao número reduzido de servidores. Considerando que a privacidade e a segurança da informação devem estar integradas à cultura organizacional do Ifal, torna-se necessária uma abordagem multidisciplinar que envolva normativos, tecnologia, colaboração institucional, capacitação e conscientização dos envolvidos, com atenção especial ao monitoramento e à melhoria contínua em face à constante evolução dos riscos cibernéticos.

Ressalta-se que a ausência de mapeamento de processos, de avaliação de riscos e de ações de treinamento e conscientização voltadas a servidores, colaboradores e estudantes pode aumentar a exposição a ataques cibernéticos, o risco de vazamento de dados, além de causar danos à imagem institucional e comprometer o alcance dos objetivos estratégicos.

Diante exposto, as seguintes causas, consequências, recomendações e benefícios esperados são apresentados em razão das fragilidades na implementação do Programa de Privacidade e Segurança da Informação:

Possível causa

Número insuficiente de servidores na área de TI e SI.

Possíveis Consequências

Aumento de vulnerabilidades a ataques cibernéticos, vazamento de dados, danos à imagem da instituição e comprometimento de objetivos.

Recomendações

Desenvolver treinamento e conscientização de servidores, alunos e colaboradores quanto às boas práticas de privacidade e segurança da informação. Como também, mapear processos e avaliar riscos relacionados à privacidade de dados e à segurança da informação.

Benefícios esperados

Maior nível de maturidade do PPSI no Ifal e redução de riscos cibernéticos.

Manifestação da Gestão

Esta Diretoria se manifesta de acordo com os achados apresentados pelo Relatório Preliminar referente à Ação de Auditoria nº 13/2025.

Análise da Auditoria Interna

Reitera-se a importância do mapeamento dos processos, da avaliação de riscos e de ações de treinamento e conscientização voltadas a servidores, colaboradores e estudantes quanto às boas práticas de privacidade e segurança da informação. Tais lacunas podem aumentar a exposição a ataques cibernéticos e o risco de vazamento de dados, além de causar danos à imagem institucional e comprometer o alcance dos objetivos estratégicos. Dessa forma, diante da manifestação apresentada pela gestão em que corrobora o achado da auditoria, mantém-se a recomendação em monitoramento até que sejam efetivadas as medidas indicadas.

Assim sendo, esta Audint considerará atendida a recomendação quando constatar a sua efetiva implementação através de trabalhos futuros de monitoramento.

RECOMENDAÇÕES

Recomendação relacionada ao Achado 2.1: Fragilidades no que se refere à segregação de funções

3.1	Elaborar, publicar e implementar ato normativo que estabeleça a estrutura de governança da segurança da informação, com definição clara das atribuições dos agentes envolvidos, de forma a atender ao princípio da segregação de funções previsto na Resolução nº 111/2023 - Consup/Ifal.

Recomendações relacionadas ao Achado 2.2: Implementação parcial das ações previstas nos instrumentos estratégicos e normativos relacionados à segurança da informação

3.2	Executar as diretrizes específicas da Política de Segurança da Informação.
3.3	Acompanhar, por meio de indicadores, as diretrizes específicas da Política de Segurança da Informação.
3.4	Realizar treinamento de pessoal.

Recomendação relacionada ao Achado 2.3: Fragilidade no monitoramento das diretrizes específicas da Política de Segurança da Informação, devido à ausência de registros formais

3.5	Elaborar documentos formais (atas, registros, relatórios, cronogramas, etc) que comprovem e permitam aos órgãos de controle avaliar a implementação e o efetivo acompanhamento das diretrizes estabelecidas na Política de Segurança da Informação.

Recomendações relacionadas ao Achado 2.4: Fragilidades na implementação do Programa de Privacidade e Segurança da Informação (PPSI)

3.6	Promover treinamento e conscientização de servidores, estudantes e colaboradores quanto às boas práticas de privacidade de dados e segurança da informação.
3.7	Mapear processos e avaliar riscos relacionados à privacidade de dados e à segurança da informação.

CONCLUSÃO

A presente auditoria permitiu avaliar práticas de governança e gestão da Tecnologia da Informação e da Segurança da Informação no Instituto Federal de Alagoas (Ifal), com foco na implementação das diretrizes do Programa de Privacidade e Segurança da Informação (PPSI).

Os exames evidenciaram avanços normativos significativos, como a publicação da Resolução nº 111/2023, a criação do Comitê de Segurança da Informação, a elaboração de diretrizes específicas e a nomeação do encarregado pelo tratamento de dados pessoais. Contudo, foram identificadas fragilidades que comprometem a efetividade das ações e a mitigação dos riscos. Destacam-se: a ausência de normativos que formalizam a segregação de funções; a implementação parcial das diretrizes previstas nos instrumentos estratégicos e normativos; a ausência de evidências de monitoramento sistemático das ações de segurança da informação; e a oportunidade de melhorias na implementação do Programa de Privacidade e Segurança da Informação.

Tais gargalos decorrem, em alguma medida, de limitações de pessoal e de recursos, mas também da ausência de mecanismos consolidados de acompanhamento e monitoramento. As consequências potenciais incluem vulnerabilidades operacionais, riscos à confidencialidade, integridade e disponibilidade das informações, bem como fragilidade na resposta a incidentes.

Assim, as recomendações apresentadas buscam fortalecer a governança e a gestão por meio da elaboração de ato normativo que regulamente a segregação de funções, da execução efetiva das diretrizes publicadas, do estabelecimento de indicadores e planos de ação, da formalização de registros e relatórios de acompanhamento, do desenvolvimento de treinamentos e ações de conscientização sobre privacidade de dados e segurança da informação e da gestão de riscos.

Em consonância com o trabalho desenvolvido pela Audint, a Gestão manifestou concordância com os achados apresentados no relatório da Ação de Auditoria nº 13/2025. As recomendações emitidas serão objeto de monitoramento em auditorias futuras.

Por fim, como atividade de assessoramento e fortalecimento da Gestão, a Auditoria possui caráter preventivo e busca agregar valor à Instituição.

Atenciosamente,

Jefferson Gerlânio do Nascimento
Auditor

José Emiliano dos Santos
Auditor

Sócrates Mesquita Bomfim
Auditor/Titular da Auditoria Interna do Ifal