INSTITUTO DE PREVIDÊNCIA SOCIAL DO MUNICÍPIO DE ANGRA DOS REIS

CONTROLADORIA INTERNA

RELATÓRIO DE AUDITORIA 004/2025

SETOR AUDITADO:

Coordenação de Tecnologia da Informação

ANO BASE: 2024/2025

IDENTIFICAÇÃO DO SETOR AUDITADO:

Tecnologia da Informação

Endereço: Rua Dr. Orlando Gonçalves, 231 - Parque das Palmeiras, Angra dos Reis - RJ, CEP: 23906-540

Telefone: (24) 3365-5260

ASSESSORIA:

Coordenadora de Tecnologia da Informação	**Camille Gomes Dourado**
Chefe de Gabinete	**Paulo Henrique da Silva Bulé**

SUMÁRIO

HISTÓRICO DE VALIDAÇÃO

Título		**Autor**	**Elaborado em**
Relatório de Auditoria nº 004/2025		Controladoria Interna	10/09/2025
Aprovado por	**Aprovado em**	**Instrumento de Aprovação**	
Conselho de Administração	25/09/2025	Ata da Reunião Ordinária do Conselho de Administração	

1. INTRODUÇÃO

Este relatório apresenta os resultados da auditoria interna realizada no Setor de Tecnologia da Informação do Instituto de Previdência Social do Município de Angra dos Reis (ANGRAPREV). A auditoria foi conduzida em conformidade com as diretrizes estabelecidas no Plano Anual de Auditoria Interna (PAAI) de 2024, fundamentada na necessidade de assegurar a regularidade, eficiência e conformidade dos procedimentos de controle relacionados à gestão da infraestrutura tecnológica, segurança da informação, suporte técnico e conformidade com a LGPD.

A execução da auditoria considerou os seguintes normativos e boas práticas:

- Constituição Federal (Artigos 70 e 74);
- Lei Federal nº 4.320/1964 – Normas gerais de Direito Financeiro e princípios da contabilidade pública;
- Lei Complementar nº 101/2000 (Lei de Responsabilidade Fiscal - LRF);
- Normas Brasileiras de Contabilidade Aplicadas ao Setor Público (NBC T 16);
- Manual de Contabilidade Aplicado ao Setor Público (MCASP) – Secretaria do Tesouro Nacional;
- Portaria MTP nº 1.467/2022 – Diretrizes para certificação no Programa Pró-Gestão RPPS;
- Boas práticas de governança de TI e gestão de riscos.

A Coordenação de Tecnologia da Informação mantém sistemas de controle e atendimento por meio de ferramentas internas, abrangendo serviços como manutenção de site, e-mails, treinamentos e atualização de conteúdo institucional. Também são executadas rotinas de apoio à infraestrutura, segurança da informação e integração de sistemas.

A auditoria envolveu a análise de indicadores de desempenho, registros de chamados, relatórios operacionais, questionários aplicados à equipe de TI e verificação documental dos controles adotados.

Os achados aqui apresentados visam contribuir para o aprimoramento da governança de TI, fortalecendo os controles internos, promovendo maior eficiência nos serviços e assegurando a conformidade legal e regulatória aplicável ao setor.

1.1 Fundamentação Legal

A auditoria de que trata o presente relatório tem sua legitimidade conferida pela Lei nº 4.037/2021 e a Lei nº 4.350/2024, a qual atribui à Controladoria Interna a competência de exercer as auditorias orçamentária, financeira, patrimonial, operacional e contábil, programando, dirigindo, orientando e controlando as atividades a elas pertinentes. Respeitando também as Normas Brasileiras de Contabilidade e os princípios fundamentais da auditoria de Conformidade regidos pelo INTOSSAI - Normas Internacionais das Entidades Fiscalizadoras.

1.2 Escopo

Os exames obedeceram aos Princípios Fundamentais de Contabilidade elencados na Resolução n.º 750/93 do Conselho Federal de Contabilidade – CFC, tendo sido realizados com base em técnicas de amostragem aleatória e casual, bem como os princípios fundamentais da auditoria de conformidade regidos pelo INTOSSAI, na extensão que se julgou necessária.

1.3 Objeto e Periodicidade

Este relatório tem como objetivo avaliar a eficiência, eficácia e conformidade dos processos relacionados à gestão da Tecnologia da Informação no ANGRAPREV, no período de 2024 e no primeiro semestre de 2025. A auditoria concentrou-se na verificação da infraestrutura tecnológica, segurança da informação, suporte aos usuários, gestão de sistemas, bem como no alinhamento da TI com os objetivos institucionais e as boas práticas de governança.

Para a realização dos trabalhos, foram analisados documentos, sistemas e procedimentos com base em critérios de materialidade, criticidade e relevância, visando uma amostragem representativa das principais rotinas executadas pela Coordenação de Tecnologia da Informação.

O objetivo central foi avaliar a conformidade dos procedimentos operacionais, a adequação dos controles internos e a efetividade das medidas adotadas para garantir a integridade, disponibilidade e segurança dos ativos de informação do Instituto, conforme as normativas legais e as melhores práticas em gestão de tecnologia pública.

Dentre os principais aspectos avaliados, destacam-se:

- ✓ Regularidade e conformidade legal das práticas de segurança da informação e proteção de dados;
- ✓ Efetividade dos controles internos no gerenciamento de acessos, backups e atualizações de sistemas;
- ✓ Aderência às normas de governança de TI, incluindo padrões de interoperabilidade, continuidade de serviços e integridade dos dados;
- ✓ Identificação de riscos operacionais, como falhas de sistema, vulnerabilidades de segurança e indisponibilidade de serviços;
- ✓ Eficiência no suporte técnico aos usuários internos e na gestão dos contratos de TI.

A auditoria também buscou identificar oportunidades de melhoria na automação de controles, na gestão de riscos tecnológicos e no desempenho dos serviços de TI, com vistas à otimização das rotinas e ao fortalecimento da governança digital do ANGRAPREV. As recomendações propostas neste relatório estão alinhadas aos princípios da legalidade, eficiência, economicidade e inovação no setor público.

1.4 Papéis de Trabalho

A inspeção foi realizada por meio de um programa consubstanciado em papéis de trabalho, bem como entrevistas pessoais com o coordenador responsável pelo setor auditado e o Chefe de Gabinete.

1.5 Atribuições regulamentares do órgão auditado

A Coordenação de Tecnologia da Informação (COTIN) do ANGRAPREV é responsável pela gestão da infraestrutura tecnológica, suporte técnico, segurança da informação, desenvolvimento e manutenção de sistemas, bem como pela conformidade com normativos legais relacionados à tecnologia e à proteção de dados. Suas atividades são essenciais para garantir a continuidade operacional, a integridade dos dados institucionais e o suporte às funções administrativas e previdenciárias do Instituto.

A atuação da COTIN impacta diretamente a eficiência dos serviços prestados aos segurados do RPPS, à medida que assegura a disponibilidade, segurança e confiabilidade dos sistemas corporativos, além de facilitar o acesso à informação e promover a inovação tecnológica alinhada aos objetivos estratégicos do ANGRAPREV.

Os serviços de TI são operacionalizados por meio de ferramentas de controle de chamados internos, contratos com prestadores terceirizados, políticas institucionais e rotinas de backup, contingência e monitoramento. A gestão da informação e a adequação à Lei Geral de Proteção de Dados (LGPD) também fazem parte das atribuições do setor, sendo essenciais para a conformidade institucional.

Entre as principais atribuições da COTIN, destacam-se:

a) Gerenciar os recursos tecnológicos do Instituto, incluindo redes, servidores, sistemas, e estações de trabalho;

b) Prestar suporte técnico aos usuários internos, por meio de sistema de chamados e atendimento presencial;

c) Monitorar os níveis de segurança da informação, com adoção de medidas preventivas e reativas contra incidentes;

d) Implementar e supervisionar políticas de backup e recuperação de dados;

e) Gerir os contratos de serviços terceirizados em TI (ex: manutenção do site, e-mails, hospedagens, consultoria);

f) Garantir a conformidade com a LGPD, em especial no tratamento de dados sensíveis em sistemas do RPPS;

g) Assegurar a atualização contínua da infraestrutura tecnológica, propondo aquisições e substituições de equipamentos obsoletos;

h) Apoiar os setores do ANGRAPREV em demandas tecnológicas específicas, promovendo a integração entre sistemas e a automação de processos;

i) Registrar, acompanhar e resolver as solicitações e incidentes por meio de ferramentas adequadas de controle;

j) Fornecer informações e relatórios técnicos às auditorias internas e externas, aos órgãos de controle e à alta administração.

A atuação efetiva da Coordenação de TI é indispensável para garantir a estabilidade, disponibilidade e integridade dos ativos tecnológicos do Instituto, contribuindo para a

governança, a proteção das informações e a melhoria contínua dos serviços prestados à comunidade segurada do RPPS.

1.6 Riscos da Auditoria

Risco de auditoria é a possibilidade de o auditor vir a emitir uma opinião tecnicamente inadequada sobre a matéria auditada. Para determinar o risco desta auditoria alguns critérios foram avaliados, tais como, a estrutura do órgão, as políticas de pessoal, o sistema de registro de informações e as limitações de acesso físico e aos relatórios.

Considerando a análise preliminar dos tópicos mencionados, entendemos que o risco de auditória é **baixo**.

2. EXECUÇÃO DOS TRABALHOS

2.1 Etapas

O trabalho de auditoria constou de três fases: planejamento, execução e conclusão.

As análises documentais foram realizadas com o objetivo de validar os dados constantes nos sistemas de controle utilizados pela Coordenação de Tecnologia da Informação (COTIN), incluindo registros de chamados internos, relatórios operacionais, contratos de prestação de serviços, questionários respondidos pela equipe e relatórios mensais de indicadores de desempenho.

A execução caracterizou-se pela aplicação de procedimentos de auditoria e coleta de evidências voltadas à identificação de fragilidades, boas práticas e oportunidades de melhoria nos processos relacionados à infraestrutura de TI, suporte técnico, segurança da informação, conformidade com a LGPD e prestação de serviços terceirizados. O período auditado abrange o exercício de 2024 e o 1º semestre de 2025.

Para alcançar os objetivos estabelecidos na presente auditoria utilizaremos das técnicas disponíveis de Auditoria, em especial:

Indagação Escrita ou Oral: Utilização de entrevistas envolvendo o responsável pela Coordenação de Compensação Previdenciária para obtenção de dados e informações.

Análise documental: Análise da documentação, dos processos e dos registros, em especial os relacionados à tramitação e procedimentos de controle para a abertura, análise de requerimentos e atendimento às exigências.

Observações das atividades e condições: Verificação das atividades com a finalidade de detectar erros, problemas ou deficiências através dos seguintes elementos de observação: identificação da atividade; observação da sua execução; comparação do comportamento com algum padrão já verificado; avaliação e conclusão.

Cálculo: conferência da exatidão numérica, confrontando-se dados de diferentes procedências com vistas a identificar a congruência das informações.

As eventuais impropriedades formais e/ou materiais detectadas são apresentadas na análise das áreas, bem como sugestões para sua otimização. A conclusão é apresentada no final do presente relatório.

2.2 Metodologia Aplicada

2.2.1 Avaliação dos Controles Internos

Efetuamos um exame com vistas à avaliação da capacidade e efetividade dos sistemas de controles internos. Avaliamos os procedimentos, processos administrativos, políticas e registros que compõem o controle, com o objetivo de constatar se estes proporcionam razoável segurança de que as atividades e operações se realizam de forma a possibilitar o atendimento das metas, em termos satisfatórios.

2.2.2 Exame da Documentação Original

O exame foi efetuado para a comprovação da situação dos requerimentos que por exigências legais ou de controle são evidenciadas por documentos comprobatórios.

Verificamos a autenticidade, ou seja, se a documentação é fidedigna e merece crédito; a normalidade, constatando se a análise refere-se à operação normal e de acordo com os objetivos do ANGRAPREV; a aprovação, verificando se os documentos foram aprovados por pessoa autorizada e, finalmente, o registro, comprovando se este foi adequado e se a documentação é hábil.

2.2.3 Entrevistas

Realizamos perguntas e obtivemos respostas de forma informal, as quais foram devidamente registradas nos papéis de trabalho, que serão arquivados nesta Unidade de Controle.

2.2.4 Amostragem

O tipo de amostragem escolhida foi a "Amostragem não probabilística ou por julgamento", onde os itens a serem testados não permitem a utilização de amostragem estatística ou os motivos da realização da auditoria tornam desnecessária a imparcialidade. Nesses casos, os testes a serem realizados baseiam-se no julgamento pessoal do auditor, que efetua a seleção dos itens subjetivamente, calcada principalmente em sua capacidade física, de pessoal, e experiência profissional.

A amostragem por julgamento é utilizada na extração de amostras, independentemente das bases estatísticas, sem nenhuma base de sustentação técnica quanto a seu tamanho e método de seleção, para tanto, utilizou-se como critério de seleção para compor uma amostra a análise de vulnerabilidade, risco potencial inerente e importância relativa.

3. GESTÃO DE RISCOS

Gestão de Riscos no Coordenação de Tecnologia da Informação

A gestão de riscos no Setor de Tecnologia da Informação é essencial para garantir a continuidade dos serviços institucionais, a segurança dos dados, a conformidade com a legislação vigente (especialmente a LGPD) e a eficiência no atendimento das demandas internas e externas. Uma abordagem eficaz de gerenciamento de riscos em TI contribui para a resiliência operacional, proteção da informação e sustentabilidade das operações do ANGRAPREV.

Durante esta auditoria, foram avaliados os relatórios de chamados internos e externos, as entrevistas com a equipe da COTIN, os relatórios mensais de desempenho e os controles operacionais vigentes. O foco esteve na identificação de vulnerabilidades relacionadas à infraestrutura tecnológica, segurança da informação, controle de acessos, conformidade contratual e gestão de continuidade dos serviços.

A análise considerou o grau de exposição do Instituto a riscos operacionais e legais associados ao uso da tecnologia, e resultou na identificação de riscos específicos, apresentados a seguir:

3.1 – Gestão de Riscos no Setor de Tecnologia da informação

3.1.1 – Falta de evidências documentadas da atuação do Comitê de Segurança da Informação

- **Risco:** Existência apenas formal do comitê, sem comprovação de atividades deliberativas ou estratégicas relacionadas à segurança da informação**.**
- **Impacto:** Fragilidade na governança de TI, ausência de diretrizes atualizadas e comprometimento da aderência ao Nível IV do Pró-Gestão.
- **Mitigação:** Registro formal de atas, planos de ação, deliberações e revisões periódicas da Política de Segurança da Informação pelo Comitê, com arquivamento e disponibilização das evidências para controle interno e auditorias externas.

3.1.2 - Falta de divulgação ampla da Política e das Normas de Segurança da Informação

- **Risco**: Desconhecimento ou descumprimento das normas por parte de servidores e prestadores.
- **Impacto**: Aumento da vulnerabilidade institucional e possibilidade de incidentes por falha humana.
- **Mitigação**: Divulgação ativa e permanente da Política e das Normas de Segurança da Informação, com disponibilização em canais internos, site e materiais explicativos.

3.1.3 – Ausência de ações periódicas de conscientização em Segurança da Informação

- **Risco**: Baixo nível de sensibilização dos usuários quanto à importância da proteção da informação.
- **Impacto**: Maior exposição à fraudes, vazamentos e violações à LGPD.
- **Mitigação**: Promoção de campanhas educativas, treinamentos regulares e dinâmicas informativas voltadas a servidores e prestadores de serviços.

3.1.4 – Inexistência de projetos estruturados para fortalecimento da Segurança da Informação

- **Risco**: Estagnação dos processos e ausência de evolução nos controles de segurança.
- **Impacto**: Obsolescência de práticas, aumento do passivo tecnológico e exposição institucional.
- **Mitigação**: Proposição e execução de projetos estratégicos voltados à modernização da segurança da informação, como auditoria de acessos, implantação de firewalls, criptografia e revisão de políticas.

3.1.5 – Ausência de política formal de classificação da informação

- **Risco**: Tratamento inadequado de documentos sigilosos ou sensíveis.
- **Impacto**: Violações de confidencialidade, responsabilidade institucional e infração à LGPD.
- **Mitigação**: Elaboração, normatização e institucionalização de política de classificação da informação, com definição clara de níveis de acesso e responsabilidades.

3.1.6 – Falta de definição de temporalidade para guarda e descarte das informações

- **Risco**: Armazenamento indefinido de dados ou descarte prematuro de registros importantes.
- **Impacto**: Riscos legais, excesso de dados não úteis e falhas na rastreabilidade.
- **Mitigação**: Inclusão de critérios de temporalidade na política de gestão da informação, em conformidade com a legislação arquivística e a LGPD.

3.1.7 – Falta de testes documentados de backup e restauração

- **Risco**: Incerteza sobre a efetividade das cópias de segurança.
- **Impacto**: Risco real de perda de dados em caso de falha sem recuperação.
- **Mitigação**: Implementação de rotina temporal de testes de restauração com registro e avaliação dos resultados.

3.1.8 – Inexistência de indicadores formais de segurança da informação

- **Risco**: Dificuldade de mensurar riscos, tomar decisões preventivas e garantir conformidade com o Pró-Gestão.
- **Impacto**: Inabilidade para identificar anomalias e justificar investimentos na área.

- **Mitigação**: Criação e monitoramento de indicadores específicos: número de incidentes, tempo médio de resposta, índice de conformidade com políticas internas.

3.2 *Compliance* e Conformidade

3.2.1 *Compliance* com a Portaria 1467/2022

A Portaria MTP nº 1.467/2022 estabelece diretrizes para o aprimoramento da governança, controle interno e transparência dos Regimes Próprios de Previdência Social (RPPS), incluindo o adequado gerenciamento das receitas previdenciárias, como contribuições, aportes e compensações financeiras.

No contexto da Coordenação de Tecnologia da Informação, o *compliance* representa a adoção sistemática de procedimentos voltados à conformidade legal, à segurança da informação e à rastreabilidade dos dados e processos digitais, assegurando que os sistemas, aplicações e infraestruturas estejam em conformidade com as normas vigentes e melhores práticas do setor.

A conformidade com as diretrizes regulatórias implica no monitoramento contínuo dos sistemas e serviços de TI, no fortalecimento dos controles de acesso e integridade dos dados, na observância de prazos legais e contratuais, bem como na documentação adequada das rotinas tecnológicas. Essas práticas contribuem para a eficiência operacional, a proteção dos ativos digitais e a integridade das informações institucionais.

A observância dessas diretrizes fortalece a segurança jurídica e tecnológica da organização, permitindo que o ANGRAPREV exerça com eficiência o controle e a governança sobre os recursos tecnológicos utilizados no suporte aos processos administrativos e previdenciários.

4 - RESULTADOS DOS EXAMES REALIZADOS NO SETOR

Com vistas a facilitar a compreensão, os resultados dos exames, separados por assunto, serão apresentados para cada achado de auditoria julgado relevante, na forma que segue:

TESTE DE CONFORMIDADE:

SITUAÇÃO DE ANÁLISE:

EVIDÊNCIAS:

RISCOS:

RECOMENDAÇÃO:

4.1 – Teste de Conformidade: Testes de Backup e Restauração de Dados

Situação de Análise: O backup é realizado diariamente em servidor local, com registros documentais arquivados com testes de restauração validados via logs. Contudo, não há implantação de solução de backup em nuvem, o que representa uma vulnerabilidade significativa frente a riscos como falhas físicas no servidor local, desastres naturais ou ataques cibernéticos que possam comprometer a disponibilidade dos dados.

Evidência: Registros documentais e logs em servidor local que comprovam a execução e a validação dos testes de restauração. Não há documentação ou comprovação de utilização de solução de backup em nuvem.

Risco: A ausência de backup em nuvem aumenta a vulnerabilidade da organização a falhas físicas no servidor local, desastres naturais ou ataques cibernéticos, podendo resultar em perda irreparável de dados e comprometimento da continuidade operacional.

Recomendação: Avaliar e implementar uma solução de backup em nuvem, preferencialmente com criptografia e alta disponibilidade, para garantir maior segurança e resiliência dos dados.

4.2 - Teste de Conformidade: Temporalidade de Guarda e Descarte da Informação

Situação de Análise: Existe uma política vigente que estabelece critérios para a guarda e descarte de dados físicos e digitais; entretanto, identifica-se um déficit específico no tratamento e descarte adequado dos dados sensíveis, comprometendo a conformidade e a segurança dessas informações.

Evidência: Regulamento com tabela de temporalidade e guarda de documentos.

Risco: Risco legal, possibilidade de vazamento ou manuseio inadequado de dados sigilosos.

Recomendação: Reforçar a implementação e o monitoramento contínuo da política de guarda e descarte, com especial atenção ao tratamento diferenciado dos dados sensíveis. Isso inclui estabelecer procedimentos claros e específicos para a classificação, armazenamento seguro, acesso restrito e descarte adequado desses dados, em conformidade com a legislação vigente, como a LGPD.

4.3 - Teste de Conformidade: Projetos Estruturados de Segurança da Informação

Situação de Análise: Não existe nenhum projeto em andamento voltado à modernização da segurança da informação, nem há planejamento formal com metas, prazos ou orçamento definido.

Evidência: Não foram encontrados planos de ação ou registros no setor de TI.

Risco: Estagnação tecnológica, práticas desatualizadas e aumento do risco cibernético.

Recomendação: Desenvolver e implementar projetos estratégicos, como implantação de firewalls, controle de acessos, criptografia e auditoria de acessos. Estes devem incluir metas claras, cronograma e clareza de responsáveis**.**

4.4 – Teste de Conformidade: Ações Periódicas de Conscientização em Segurança da Informação

Situação de Análise: Não há cronograma formal nem evidências de treinamentos ou campanhas educativas sobre segurança da informação realizadas periodicamente.

Evidência: Não foram encontrados registros de treinamentos.

Risco: Baixa conscientização dos usuários, com exposição a fraudes, vazamento de dados e descumprimento da LGPD.

Recomendação: Elaborar plano anual de capacitação com treinamentos regulares sobre segurança da informação para servidores e prestadores com acesso institucional**.**

4.5 – Teste de Conformidade: Existência e funcionamento do Comitê de Segurança da Informação

Situação de Análise: Não foi possível identificar registros documentais de reuniões, atas, deliberações ou planos de ação do Comitê de Segurança da Informação. Em algumas entrevistas, mencionou-se a existência informal de discussões sobre segurança da informação, porém sem sistematização nem registros oficiais.

Evidência: Ausência de portaria de nomeação dos integrantes e inexistência de documentos arquivados que comprovem reuniões ou revisões da Política de Segurança da Informação.

Risco: Fragilidade na governança de TI, ausência de diretrizes claras e atualizadas, não conformidade com os requisitos do Pró Gestão RPPS – Nível IV.

Recomendação:

Instituir formalmente o Comitê de Segurança da Informação por meio de ato normativo, com representantes de áreas estratégicas. Estabelecer cronograma regular de reuniões, registrar todas as deliberações em atas e revisar a Política de Segurança da Informação a cada 4 anos, garantindo arquivamento e disponibilização das evidências.

4.6 – Teste de Conformidade: Divulgação da Política e Normas de Segurança da Informação

Situação de Análise: A Política de Segurança da Informação e suas normas associadas estão desatualizadas e não são amplamente divulgadas aos servidores e prestadores de serviço. Embora os documentos existam, não há comunicação institucional ampla e efetiva.

Evidência: Não foram identificadas campanhas estruturadas de divulgação nem registros formais de ciência por parte dos usuários. Além disso, o documento publicado da política encontra-se desatualizado sem revisões recentes.

Risco: Desconhecimento ou descumprimento das normas, aumento de vulnerabilidade institucional e falhas operacionais por erro humano.

Recomendação: Atualizar e disponibilizar a Política e normas no ambiente digital acessível a todos os colaboradores. Promover campanhas permanentes de conscientização sobre segurança da informação.

4.7 – Teste de Conformidade: Atualização dos manuais e procedimentos operacionais da área de Tecnologia da Informação

Situação de Análise: Embora existam manuais e procedimentos operacionais formalmente instituídos na Coordenação de Tecnologia da Informação, constatou-se que parte significativa desses documentos encontra-se desatualizada ou não reflete plenamente as práticas atuais.

Evidência: Análise dos procedimentos operacionais e confronto com as práticas atuais, que demonstraram defasagem de conteúdo e ausência de revisão periódica. Também não há histórico de atualização formal registrada nos documentos.

Risco: Desalinhamento entre as rotinas documentadas e as práticas executadas, comprometendo a padronização, dificultando treinamentos e prejudicando a rastreabilidade e o controle das atividades. A defasagem pode gerar interpretações equivocadas, reduzir a efetividade dos controles e impactar a continuidade operacional.

Recomendação: Revisar e atualizar os manuais da área de TI, incorporando as rotinas atuais e garantindo aderência às normas de segurança da informação, governança e boas práticas operacionais. Estabelecer periodicidade mínima de revisão documental e registro formal das atualizações, assegurando a consistência entre o que está documentado e o que é executado.

4.8 – Teste de Conformidade: Avaliação de Bens obsoletos/inservíveis

Situação de Análise: Foi identificado que a organização possui bens patrimoniais de TI inservíveis ou obsoletos, incluindo equipamentos antigos guardados para retirada de peças. Essa prática, além de comprometer o espaço físico disponível, contribui para a desorganização do patrimônio e dificulta a gestão eficiente dos ativos. A falta de processos formalizados e atualizados para identificação, segregação e destinação desses bens impacta negativamente a eficiência operacional e o desempenho dos colaboradores.

Evidência: Inventário físico apontou existência de equipamentos e materiais fora de uso, sem registros atualizados de baixa ou destinação; inexistência de documentação formalizada referente à triagem e descarte desses bens. A inspeção realizada durante a auditoria constatou a presença de desktops ultrapassados que apresentam lentidão que impactam o desempenho dos colaboradores.

Risco: Manter bens obsoletos ou inservíveis sem controle adequado pode gerar desperdício de espaço físico, custos adicionais com manutenção desnecessária, além de riscos legais decorrentes da gestão inadequada do patrimônio público. A manutenção de equipamentos obsoletos impacta negativamente a eficiência operacional, reduz a produtividade e pode ocasionar falhas técnicas.

Recomendação: Implementar procedimentos claros e atualizados para avaliação e destinação dos bens obsoletos e inservíveis, incluindo critérios de armazenamento temporário e descarte final para bens destinados à retirada de peças alinhados às normas vigentes. Recomenda-se ainda a substituição de desktops ultrapassados por modelos atualizados que atendam às necessidades operacionais, visando aumentar a produtividade e a eficiência.

4.9 – Teste de Conformidade: Fragilidade na Estrutura Organizacional e Capacidade Operacional da Área de Tecnologia da Informação

Situação de Análise: Durante a análise da estrutura de Tecnologia da Informação (TI) do instituto, constatou-se que o setor é composto por apenas duas pessoas: uma Coordenadora de Tecnologia da Informação e uma estagiária. Além disso, a área encontra-se subordinada diretamente à Chefia de Gabinete, o que limita sua autonomia decisória e gerencial.

Evidência: Organograma institucional e registros funcionais.

Risco: A composição reduzida e a subordinação atual podem comprometer a efetividade da governança de TI e a segurança da informação, aumentando a vulnerabilidade a incidentes, falhas de controle, atrasos na execução de atividades críticas e descumprimento de requisitos relacionados ao Programa Pró-Gestão RPPS. Tais fragilidades podem impactar diretamente a continuidade dos serviços, a proteção dos dados e a conformidade com normas e boas práticas de gestão de TI.

Recomendação: Recomenda-se que seja avaliada a reestruturação do setor de Tecnologia da Informação, com vistas a ampliar o quadro de pessoal, incluindo pelo menos um profissional adicional com formação compatível para apoiar as demandas técnicas e de segurança da informação e revisar a subordinação hierárquica, assegurando maior autonomia e independência ao setor de TI.

5. CONCLUSÃO

A auditoria realizada na Coordenação de Tecnologia da Informação do Instituto de Previdência Social do Município de Angra dos Reis (ANGRAPREV) evidenciou a existência de uma estrutura básica de governança tecnológica, com rotinas operacionais que asseguram a continuidade dos serviços e o suporte às demais áreas do Instituto. Todavia, foram identificadas lacunas significativas no que tange à formalização de diretrizes estratégicas, à segurança da informação e à conformidade com os requisitos do Pró-Gestão RPPS – Nível IV.

A ausência de um Comitê de Segurança da Informação instituído efetivamente, a falta de políticas atualizadas e divulgadas demonstram fragilidades na gestão estratégica da área. Ademais, a baixa institucionalização de ações de conscientização ampliam a exposição a riscos operacionais e a vulnerabilidades de segurança, especialmente frente às exigências da LGPD.

Apesar dessas deficiências, observa-se que o setor apresenta potencial de evolução, sendo perceptível o comprometimento da equipe técnica com a continuidade dos serviços. Recomendam-se, entretanto, ações estruturadas e graduais, com foco na institucionalização de boas práticas de governança de TI, na automação de backups críticos, na formalização de processos operacionais, na definição clara de responsabilidades e na modernização da infraestrutura tecnológica. Tais medidas contribuirão para o aumento da eficiência, mitigação de riscos operacionais e fortalecimento dos serviços de TI.

A adoção das medidas propostas neste relatório contribuirá significativamente para o fortalecimento da governança digital do ANGRAPREV, promovendo maior integridade, confiabilidade e segurança aos ativos informacionais da autarquia, em conformidade com os preceitos da administração pública eficiente, transparente e orientada a resultados.

gov.br
Documento assinado digitalmente
DAYANE ALVES REIS
Data: 08/10/2025 09:02:21-0300
Verifique em https://validar.iti.gov.br

Dayane Alves Reis
Coordenadora de Auditoria
Matr. 2500331

gov.br
Documento assinado digitalmente
GIOVANNA MARTINS VALLADAO SOARES
Data: 06/10/2025 16:17:13-0300
Verifique em https://validar.iti.gov.br

Giovanna Martins V. Soares
Controladora Interna
Matr. 2500310