Prefeitura de Cambé
UM GOVERNO PARA TODOS

Relatório de Auditoria

Objeto

Verificar o cumprimento da Política de Segurança da Informação, conforme previsão no Manual do Pró-Gestão (versão 3.5) para os níveis de certificação I e II

Identificação

Secretaria Municipal de Auditoria e Controle Interno - SEMACI
Responsável: Roberval Zamperlini / Analista - Programador
Equipe: Gislaine M. Moreno Brandelik / Contadora
Órgão dono do processo: Diretoria Executiva da Autarquia Cambé Previdência
Área auditada: Segurança da Informação
Origem: Ordem de Serviço 2/2024
Número do Processo: Auditoria 2/2024
Identificador do E-CIGA: 6b6961ca-f13d-4e6e-b64a-e1946d4ab698

Missão

Fortalecer a gestão dos recursos financeiros, patrimoniais e humanos com vista a assegurar que as políticas públicas sejam fornecidas com eficiência

Avaliação

O trabalho de avaliação, como parte da atividade de auditoria interna, consiste na obtenção e na análise de evidências com o objetivo de fornecer opiniões ou conclusões independentes sobre um objeto de auditoria. Objetiva também avaliar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos relativos ao objeto e à Unidade Auditada, e contribuir para o seu aprimoramento.

12/2024

QUAL FOI O TRABALHO REALIZADO PELA SECRETARIA?

O trabalho realizado consistiu na **auditoria de conformidade da Política de Segurança da Informação (PSI)** da **Cambé Previdência**, visando verificar a conformidade com as **normas de segurança da informação**, incluindo as diretrizes previstas no **Manual do Pró-Gestão RPPS (versão 3.5)** para os Níveis I e II e a **LGPD (Lei Geral de Proteção de Dados)**. O escopo da auditoria abrangeu:

A avaliação da **conformidade da PSI** com normas de segurança da informação, como **ISO/IEC 27001 / 27002, CIS V8 ou outras**.

A verificação dos **procedimentos de segurança de dados pessoais**, em conformidade com a **LGPD**.

A avaliação da **abrangência da Política de Segurança da Informação** para Servidores e Prestadores de Serviço.

A verificação de **regras normativas claras quanto ao uso de internet, correio eletrônico e recursos tecnológicos**.

A **implementação de procedimentos** relacionados ao controle de acesso, **contingência** e **backup**.

A Verificação de formalização de responsabilidades quanto à **gestão de TI** e segurança da informação.

POR QUE A SECRETARIA REALIZOU ESSE TRABALHO?

A auditoria foi realizada para atender à **certificação do Pró-Gestão RPPS**, especificamente **no Nível II**, conforme o **Manual do Pró-Gestão (versão 3.5)**. Essa certificação exige a **verificação da completude e do cumprimento da Política de Segurança da Informação (PSI)**, um item fundamental para assegurar que as boas práticas de segurança estão sendo seguidas, especialmente na proteção e no tratamento adequado das informações gerenciadas pela Cambé Previdência. A PSI é crucial para garantir a **confidencialidade, integridade e disponibilidade** dos dados do Regime Próprio de Previdência Social (RPPS), considerando o volume e a sensibilidade das informações pessoais e financeiras dos servidores municipais. A auditoria também foi determinada por fatores de relevância e criticidade, já que a **não conformidade** com as normas de segurança e a **LGPD** pode expor a entidade a riscos operacionais e legais significativos, além de comprometer sua capacidade de **manter a certificação do Pró-Gestão**.

QUAIS AS CONCLUSÕES ALCANÇADAS PELA SECRETARIA?

A auditoria da **PSI** da Cambé Previdência identificou que, apesar da implementação de diretrizes gerais, há **lacunas importantes** que comprometem a conformidade com **padrões reconhecidos de segurança** e a **LGPD**. As principais conclusões são:

Conformidade parcial com padrões de segurança: A PSI não atende a normas reconhecidas, aumentando os riscos de falhas.

Não conformidade com a LGPD: Ausência de inventário de dados pessoais, termos de consentimento e políticas de retenção e eliminação de dados.

Falta de responsabilidade e treinamentos: Inexistência de termos formalizados de responsabilidade e treinamento contínuo insuficiente.

Ausência de procedimentos de controle: Embora existam backups, não são realizados testes regulares de recuperação de dados e faltam planos de contingência, aumentando riscos de interrupções.

Conformidade no uso de internet e e-mail: Diretrizes adequadas ao porte da organização.

Falta de monitoramento da PSI: A ausência de um processo formal dificulta a validação do cumprimento dos requisitos e impede a determinação de conformidade.

Falta de formalização na gestão de TI: Não há uma área designada para a gestão de TI e segurança da informação, gerando incertezas sobre responsabilidades.

QUAIS AS RECOMENDAÇÕES QUE DEVERÃO SER ADOTADAS?

CONSTATAÇÃO	RECOMENDAÇÃO
A Política de Segurança da Informação da Cambé Previdência (PSI) foi criada e publicada, porém carece de conformidade com padrões e normas de segurança reconhecidas, a fim de garantir os princípios de confidencialidade, integridade e disponibilidade.	Revisar a **PSI**, incluindo a adoção formal de normas de segurança reconhecidas, como **ISO/IEC 27001, 27002** e **CIS V8 ou outras,** visando fortalecer a segurança dos dados e garantir conformidade com a Lei Geral de Proteção de Dados (**LGPD**) e demais regulamentos relacionados.
Necessidade de adequação da Política de Segurança da Informação para garantir conformidade com a LGPD.	Revisar **PSI** para atender as obrigações da **LGPD**, incluindo diretrizes específicas como por exemplo o tratamento e armazenamento de dados pessoais, inventário de dados, obtenção de consentimento, e retenção/exclusão de dados.
Servidores e prestadores de serviço acessam informações sem compromissos formais de segurança, com lacunas na conscientização e treinamento insuficiente	Criação e formalização de **termos de responsabilidade** para todos os servidores e prestadores de serviço, além da implementação de um **plano de treinamento contínuo** para capacitar todos os envolvidos sobre suas responsabilidades na segurança da informação.
Procedimentos sobre controle de acesso (físico e lógico) aos sistemas informatizados e bancos de dados não formalizados, ausência de planos de contingência adequados, com risco de perda de dados e interrupção de serviços críticos em caso de incidentes.	Criação de **procedimentos formalizados de controle de acesso (físico e lógico)**, além da implementação de **planos de contingência e recuperação de desastres**. Também é necessário formalizar uma **política de testes de backups** e **políticas de continuidade de negócios**.
Necessidade de fortalecimento da Política de Segurança da Informação com mecanismos de controle e implementação de monitoramento contínuo e transparente.	Fortalecimento da **PSI** para incluir mecanismos robustos de controle e sanções, bem como a implementação de um processo formalizado de **monitoramento contínuo** e transparente.
Inexistência de área responsável formalmente definida pela gestão da estrutura de TI.	Formalizar a gestão de TI constituindo área responsável pela gestão da TI da autarquia, com papéis e responsabilidades claros, incluindo um acordo de serviços para garantir a continuidade dos sistemas e o cumprimento das normas de segurança.

Sumário

1. INTRODUÇÃO

Este relatório apresenta os resultados da auditoria realizada pela Secretaria de Auditoria e Controle Interno, órgão responsável e unidade central do Sistema de Controle Interno do Município de Cambé, incluindo a Administração Indireta. Essa atuação é regulamentada pela legislação pertinente:

- **Lei nº 2.089/2006**: Lei de criação da Secretaria.
- **Lei nº 2.164/2007**: Disposição sobre a estrutura do controle interno.
- **Lei nº 2.259/2009**: Altera o sistema de controle interno.
- **Lei nº 2.530/2012**: Modifica dispositivos das Leis 2.089/2006 e 2.259/2009.
- **Lei nº 2.934/2018**: Revoga e modifica artigos das Leis 2.089/2006 e 2.164/2007 e suas alterações.

A auditoria foi realizada na **Autarquia Municipal de Previdência Social dos Servidores Públicos do Município de Cambé** (Cambé Previdência), que é a unidade gestora responsável pela operacionalização e administração dos planos de benefícios previdenciários e do respectivo plano de custeio, conforme regulamentação da **Lei Municipal nº 2.647/2014** e suas alterações, sendo o **Regime Próprio de Previdência Social (RPPS)** regulamentado pela **Lei Complementar nº 057/2021** e suas alterações.

O objetivo da auditoria foi verificar o cumprimento da **Política de Segurança da Informação (PSI)**, conforme estabelecido no **Manual do Pró-Gestão RPPS (versão 3.5)**, para os Níveis I e II de certificação. A PSI é um componente fundamental para garantir a proteção dos dados e a segurança dos sistemas informatizados da autarquia.

O trabalho de auditoria focou em avaliar a conformidade da PSI em relação às boas práticas e normas reconhecidas, incluindo a ISO/IEC 27001, ISO/IEC 27002, CIS V8 e à legislação brasileira, em especial a Lei Geral de Proteção de Dados (LGPD). A análise abrangeu o controle de acesso a sistemas, o tratamento de dados pessoais, a abrangência da política de segurança, a existência de planos de contingência e a adequação das normas internas de uso de recursos tecnológicos.

A relevância desta auditoria está associada à necessidade de garantir a conformidade com as exigências legais e regulatórias, bem como à mitigação de riscos relacionados à segurança da informação, assegurando a continuidade dos serviços e a integridade dos dados do RPPS. Este trabalho foi conduzido como parte das exigências de certificação do Pró-Gestão RPPS, Nível II,

reforçando o compromisso da Cambé Previdência com as melhores práticas de governança e gestão de TI.

2. ESCOPO DO TRABALHO

A auditoria de conformidade foi conduzida com o objetivo de verificar a completude e o cumprimento da Política de Segurança da Informação (PSI) da Cambé Previdência, focando na adequação aos requisitos normativos e legais relacionados à segurança da informação e à proteção de dados pessoais, conforme previsto no Manual do Pró-Gestão RPPS (versão 3.5) para Níveis I e II de certificação.

O trabalho de auditoria iniciou-se a partir da **ordem de serviço 02/2024** emitida pelo Secretário de Auditoria e Controle Interno, com **início em 02/10/2024**, abrangendo a análise de documentos e informações relacionadas à implementação e cumprimento da Política de Segurança da Informação instituída através **da portaria 019/2023** pela Cambé Previdência.

A técnica adotada para a realização da auditoria foi a **solicitação de auditoria através de questionário de avaliação**, complementada pelo **envio de documentos e informações** que pudessem evidenciar as respostas fornecidas. Esta metodologia visa garantir um processo de auditoria mais eficiente, estruturado e baseado em evidências concretas, assegurando a validação das práticas declaradas pelo auditado.

O questionário de auditoria foi elaborado com base nas **sete questões de auditoria** previamente definidas na **Matriz de Planejamento**, abordando pontos críticos relacionados à **Política de Segurança da Informação (PSI)** da Cambé Previdência. Cada pergunta foi formulada para avaliar aspectos específicos da conformidade da autarquia com as normas e legislações aplicáveis, como a **LGPD**, **ISO/IEC 27001, 27002, CIS V8** e as diretrizes do **Pró-Gestão RPPS**.

As perguntas solicitaram que o auditado fornecesse respostas sobre:

- **Informações detalhadas** sobre a implementação da PSI.
- **Descrição dos processos** relacionados à gestão de segurança da informação, controle de acesso, contingência e backups.
- **Responsabilidades e compromissos** de servidores e prestadores de serviços em relação à segurança dos dados.

- **Procedimentos adotados** para o monitoramento e aplicação de penalidades em caso de não conformidade.

Para garantir a **veracidade e a confiabilidade** das respostas fornecidas no questionário, foi solicitado o envio de **documentos e informações** que pudessem evidenciar o cumprimento das práticas relatadas. A Cambé Previdência foi orientada a fornecer:

- **Relação dos artigos ou anexos da PSI** que evidenciam a conformidade com a LGPD.
- **Relação dos artigos ou normas e regulamentos internos** que tratam sobre o uso de internet, correio eletrônico e recursos tecnológicos.
- **Termos de responsabilidade** assinados por servidores e prestadores de serviços.
- **Registros de incidentes** de segurança e penalidades aplicadas, caso existissem.
- **Planos de contingência** e **documentos de backup** que demonstrassem a gestão de riscos e recuperação de dados.
- **Registros de treinamentos** oferecidos aos colaboradores sobre segurança da informação.
- **Documentos que comprovem a designação formal da área ou equipe responsável** pela gestão de hardware, software e segurança da informação.

Essas evidências foram solicitadas para assegurar que as práticas mencionadas no questionário estavam efetivamente implementadas, conforme as melhores práticas de governança e segurança da informação. O envio foi realizado através do **Sistema de Gerenciamento de processos Eletrônico (e-CIGA)**, garantindo a rastreabilidade e a preservação da integridade dos documentos.

A utilização do **questionário de auditoria** combinado com o envio de documentos evidenciais permite que a auditoria:

1. **Avalie de maneira objetiva** a conformidade da PSI com as normas e regulamentos aplicáveis.
2. **Documente de forma clara** os processos, procedimentos e controles adotados pela Cambé Previdência.
3. **Valide as práticas declaradas**, cruzando as respostas com as evidências documentais apresentadas.

4. **Assegure a transparência** do processo, permitindo o acompanhamento e análise contínua das práticas de segurança da informação.

Essa técnica proporciona uma visão abrangente e detalhada da implementação da PSI, permitindo identificar potenciais lacunas e propor as melhorias necessárias para garantir a conformidade e a segurança dos dados gerenciados pela Cambé Previdência.

Com base nessas diligências e nas evidências coletadas, foram elaborados os **achados de auditoria**, que constam na **Matriz de Achados**, identificando as não conformidades e propondo recomendações para correção.

3. RESULTADO DOS EXAMES

A auditoria realizada na **Cambé Previdência** resultou na identificação de dois tipos de constatações: **Boas Práticas**, que são achados positivos destacando medidas que atendem os critérios de avaliação estabelecidos, e **Achados de Auditoria**, que refletem áreas onde há necessidade de aprimoramento ou correção para garantir a conformidade com normas e boas práticas de gestão e segurança da informação.

A seguir, são apresentados os detalhes de cada achado, classificados entre **Boas Práticas** e **Achados de Auditoria**, com suas respectivas análises, conclusões e recomendações.

3.1. BOAS PRÁTICAS

3.1.1. A PSI da Cambé Previdência estabelece regras normativas gerais sobre o uso de internet, correio eletrônico e recursos tecnológicos, adequadas ao porte da organização

A **Política de Segurança da Informação (PSI) da Cambé Previdência** estabelece **regras normativas gerais** sobre o uso de internet, correio eletrônico e recursos tecnológicos, consideradas **adequadas ao porte da organização**. Essas diretrizes cumprem as exigências de segurança da informação e são apropriadas para a estrutura e os recursos disponíveis na autarquia, sendo vistas como uma boa prática no contexto de gestão tecnológica.

A avaliação foi realizada a partir da resposta à questão de auditoria e encaminhamento de informações e documentos pelo auditado, conforme segue abaixo:

Questão de auditoria: Existem regras normativas claras quanto ao uso de internet, correio eletrônico e recursos tecnológicos do RPPS?

Resposta do auditado: Sim.

INFORMAÇÕES REQUERIDAS	INFORMAÇÕES, DOCUMENTOS OU JUSTIFICATIVAS ENVIADAS PELO AUDITADO
RELAÇÃO DOS ARTIGOS OU ANEXOS DA PSI, COMO NORMAS E REGULAMENTOS INTERNOS QUE TRATAM SOBRE O USO DE INTERNET, CORREIO ELETRÔNICO E RECURSOS TECNOLÓGICOS	Anexo 5.1: Portaria 019/2023 – Artigos 6º ao 10º.

Durante a auditoria realizada na **Cambé Previdência**, a equipe buscou verificar se existiam **regras normativas claras** sobre o uso de internet, correio eletrônico e recursos tecnológicos dentro da organização, conforme descrito na **Política de Segurança da Informação (PSI)**. A autarquia forneceu a **Portaria 019/2023**, que, em seus Artigos 6º ao 10º, define diretrizes específicas para o uso desses recursos. O trabalho de auditoria foi realizado para assegurar que essas normativas fossem adequadas ao porte da entidade e seguissem boas práticas de segurança da informação, garantindo a conformidade com os critérios estabelecidos.

A **PSI da Cambé Previdência** contém **regras normativas claras** sobre o uso de internet, correio eletrônico e outros recursos tecnológicos, conforme descrito nos Artigos 6º ao 10º da **Portaria 019/2023**. Embora o detalhamento não seja extenso, essas diretrizes são consideradas suficientes e adequadas ao porte e às necessidades operacionais da autarquia, sem apresentar lacunas significativas. O critério utilizado para essa avaliação foi a **adequação dessas normas ao porte da organização**, em conformidade com boas práticas de segurança da informação, como as recomendadas pela **ISO/IEC 27001**, que sugere políticas que assegurem o uso seguro desses recursos para minimizar riscos operacionais e proteger as informações da entidade.

A adequação das regras normativas sobre o uso de internet e correio eletrônico garante a **segurança das informações** e o **uso correto dos recursos tecnológicos** na Cambé Previdência. Como resultado, a autarquia consegue manter o controle sobre os recursos digitais, minimizar riscos relacionados ao uso indevido e garantir a **proteção dos dados**. Este achado positivo reflete uma abordagem proativa em relação à governança de TI.

Recomenda-se que a **Cambé Previdência** mantenha o monitoramento contínuo e revisões periódicas dessas normas para garantir que permaneçam adequadas às **necessidades operacionais** e às **evoluções tecnológicas**, assegurando a proteção contínua das informações e o uso eficiente dos recursos tecnológicos.

3.2. ACHADOS DE AUDITORIA

3.2.1. A Política de Segurança da Informação da Cambé Previdência foi criada e publicada, porém carece de conformidade com padrões e normas de segurança reconhecidas, a fim de garantir os princípios de confidencialidade, integridade e disponibilidade.

A **Política de Segurança da Informação (PSI)** da Cambé Previdência foi avaliada com o objetivo de verificar se sua elaboração seguiu padrões e diretrizes reconhecidas nacional e internacionalmente, como as normas **ISO/IEC 27001**, **ISO/IEC 27002** e **CIS Controls v8, ou outras**. Esses padrões são fundamentais para garantir os princípios de **confidencialidade, integridade e disponibilidade** das informações, essenciais para proteger os dados sob custódia da autarquia.

A avaliação foi realizada a partir da resposta à questão de auditoria e encaminhamento de informações e documentos pelo auditado, conforme segue abaixo:

Questão de auditoria: A Política de Segurança da Informação da Cambé Previdência foi elaborada com base em padrões, normas e diretrizes reconhecidas nacionalmente ou internacionalmente, como a ISO/IEC 27001, ISO/IEC 27002, CIS - Critical Security Controls v8, ou outra, a fim de garantir os princípios de confidencialidade, integridade e disponibilidade?

Resposta do auditado: Sim.

INFORMAÇÕES REQUERIDAS	INFORMAÇÕES, DOCUMENTOS OU JUSTIFICATIVAS ENVIADAS PELO AUDITADO
DOCUMENTAÇÃO QUE MENCIONE OS PADRÕES E NORMAS SEGUIDOS NA ELABORAÇÃO DA PSI OU REFERÊNCIA EXPLÍCITA A ISO/IEC 27001, ISO/IEC 27002, CIS - CRITICAL SECURITY CONTROLS V8, OU OUTROS PADRÕES	Guia de Boas Prática / LGPD / Governo Federal. https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf Por se tratar de um documento de iniciativa própria, além da menção no artigo 21 – parágrafo Único da Portaria 019/2023 que trata da PSI - não disponibilizamos outros documentos que contenham, explicitamente, as motivações da utilização das normas da ABNT bem como a utilização do Guia acima, disponibilizado pelo Governo Federal. (Anexo 1.1 – Print do Artigo 21 – Parágrafo Único da Portaria 019-2023 – PSI)

Após análise, constatou-se que, embora o **Artigo 21 – Parágrafo Único da Portaria 019-2023** da PSI da Cambé Previdência mencione tanto a **ISO/IEC 27002** quanto a **LGPD**, essa referência é limitada ao contexto do **armazenamento e acesso de arquivos físicos** e **não abrange os controles necessários** para garantir a proteção abrangente da informação. Também **não está alinhada** ao **Guia de Boas Práticas da LGPD** citado pelo auditado, especialmente em relação ao **tratamento seguro de dados pessoais**, **consentimento dos titulares** e **políticas de retenção e eliminação de dados**.

O próprio **Guia de Boas Práticas da LGPD,** na página 54, itens 4.2.2, 4.2.3 e página 49, recomenda seguir as normas e padrões aqui citados, porém, após análise verificou-se que a PSI também **não atende completamente as diretrizes da ISO/IEC 27001**, que estabelece um Sistema de Gestão de Segurança da Informação, nem da **ISO/IEC 27002**, que fornece diretrizes para a implementação de controles de segurança da informação, abrangendo uma vasta gama de requisitos para proteger a **confidencialidade, integridade e disponibilidade** das informações. Da mesma forma, a política não reflete práticas críticas do **CIS Controls v8**, como inventário de ativos e resposta a incidentes.

A falta de adoção de normas reconhecidas afeta diretamente a capacidade da autarquia de **garantir a segurança dos dados** que administra. Além disso, essa lacuna pode expor a Cambé Previdência a **riscos legais**, uma vez que a **Lei Geral de Proteção de Dados (LGPD)** exige que os dados pessoais sejam tratados com o mais alto nível de segurança disponível, o que inclui a adoção de padrões de mercado. A **certificação no Pró-Gestão RPPS**, que exige conformidade com boas práticas, também pode ser impactada, colocando em risco a integridade da operação e a proteção dos dados.

Em resumo, a PSI existente não está em conformidade com padrões amplamente aceitos, o que resulta em falhas potenciais nos controles de segurança, portanto, **recomenda-se** que a Cambé Previdência **revise e atualize a sua política**, alinhando-a formalmente a normas como **ISO/IEC 27001**, **ISO/IEC 27002, CIS Controls v8 ou outras formalmente reconhecidas**. Além disso, a adoção dessas diretrizes deve ser formalizada e documentada para garantir que os controles de segurança sejam eficazes e que a autarquia atenda tanto às exigências do **Pró-Gestão RPPS** quanto às da **LGPD**.

3.2.1.1. Manifestação da Unidade Auditada

A unidade auditada reconheceu a relevância do achado e consentiu com sua implementação, destacando o compromisso em adotar as medidas recomendadas para aprimorar os processos de segurança da informação e conformidade.

3.2.2. Necessidade de adequação da Política de Segurança da Informação para garantir conformidade com a Lei Geral de Proteção de Dados (LGPD)

A **Política de Segurança da Informação (PSI) da Cambé Previdência** não está totalmente em conformidade com as exigências da **Lei Geral de Proteção de Dados (LGPD)**, especialmente no que se refere ao **tratamento, armazenamento, proteção e eliminação de dados pessoais**. A PSI carece de procedimentos claros para o **consentimento dos titulares**, a **classificação de dados pessoais**, a **retenção e descarte de informações** e os **procedimentos de resposta a incidentes** que envolvem dados sensíveis, colocando a autarquia em **risco de não conformidade legal**.

A avaliação foi realizada a partir da resposta à questão de auditoria e encaminhamento de informações e documentos pelo auditado, conforme segue abaixo:

Questão de auditoria: A Política de Segurança da Informação da Cambé Previdência está em conformidade com as obrigações estabelecidas pela LGPD no que se refere ao tratamento, armazenamento e proteção de dados pessoais?

Reposta do auditado: Parcialmente

INFORMAÇÕES REQUERIDAS	INFORMAÇÕES, DOCUMENTOS OU JUSTIFICATIVAS ENVIADAS PELO AUDITADO
RELAÇÃO DOS ARTIGOS OU ANEXOS DA PSI QUE EVIDENCIAM ACONFORMIDADE COM A LGPD	A PSI não detalha como os dados pessoais são tratados, armazenados e protegidos
INVENTÁRIO E CLASSIFICAÇÃO DE DADOS PESSOAIS	A PSI não detalha sobre o inventário de dados pessoais, categorizando-os conforme sua sensibilidade e indicando as medidas de proteção conforme LGPD
POLÍTICAS DE CONSENTIMENTO	A PSI não traz em seu teor “Termo de Consentimento dos titulares de dados.”
PROCEDIMENTOS DE RESPOSTA A	Anexo 2.1 – Portaria 019 /2023. Artigos 32 ao 34

INCIDENTES DE SEGURANÇA	
POLÍTICAS DE RETENÇÃO E ELIMINAÇÃO DE DADOS	A PSI não trata sobre tempo de guarda dos documentos

Durante a auditoria, com base nas informações fornecidas pelo auditado, bem como em análises documentais, foi verificado que a **PSI** da Cambé Previdência não contempla adequadamente as exigências da **LGPD**, gerando lacunas nos processos de **tratamento, armazenamento e proteção de dados pessoais**. A PSI não detalha os procedimentos para obter o **consentimento explícito** dos titulares de dados, tampouco apresenta um **inventário de dados** que classifique informações pessoais conforme sua sensibilidade.

Além disso, não foram encontradas diretrizes claras sobre a **retenção e eliminação** de dados, o que deixa a Cambé Previdência em desacordo com a LGPD, que exige o descarte seguro de informações após o término de sua finalidade. A ausência de políticas robustas de **resposta a incidentes de segurança**, especialmente aqueles que envolvem dados pessoais, também compromete a capacidade da organização de cumprir integralmente a legislação.

A **LGPD** estabelece que as organizações devem garantir a **confidencialidade, integridade e proteção** dos dados pessoais, assegurando os direitos dos titulares. Entre os requisitos estão: a **obtenção de consentimento explícito**, a **classificação de dados pessoais** conforme sua sensibilidade, a implementação de **políticas de retenção e eliminação de dados**, e **procedimentos de resposta a incidentes de segurança**.

Esses critérios visam garantir que os dados sejam tratados com segurança, conforme as melhores práticas e exigências legais. A análise da PSI da Cambé Previdência foi realizada com base nesses padrões, avaliando se a política atendia às diretrizes da LGPD.

A incompletude da **PSI** da Cambé Previdência pode resultar no **descumprimento de diversos artigos da LGPD**, como a ausência de **consentimento adequado** dos titulares, **retenção indevida** de dados além do período necessário e **má gestão** de dados pessoais. Esses fatores aumentam significativamente o risco de **incidentes de segurança**, como vazamentos de dados, e expõem a autarquia a **sanções regulatórias** impostas pela Autoridade Nacional de Proteção de Dados **(ANPD)**, além de comprometer a proteção dos direitos dos titulares.

Em resumo, a **Política de Segurança da Informação (PSI)** da Cambé Previdência **não está em conformidade** com as exigências estabelecidas pela **LGPD** no que se refere ao **tratamento, armazenamento e proteção de dados pessoais**. A ausência de políticas claras para o **consentimento adequado**, a **retenção e eliminação de dados** e a **gestão de incidentes** compromete a segurança e a privacidade dos dados, expondo a autarquia a **riscos legais** e operacionais significativos. É essencial que a PSI seja revisada e ajustada para garantir a conformidade legal e a proteção eficaz dos dados pessoais sob sua custódia.

Recomenda-se que a **Cambé Previdência** revise e atualize sua **Política de Segurança da Informação** para garantir conformidade com a **LGPD**, implementando minimamente as seguintes ações:

- **Consentimento dos titulares**: Incluir procedimentos claros para obter e documentar o **consentimento explícito** dos titulares de dados pessoais, conforme exigido pela LGPD.

- **Inventário e classificação de dados**: Estabelecer um **inventário de dados pessoais**, categorizando-os conforme sua sensibilidade e aplicando medidas de proteção adequadas a cada tipo de dado.

- **Políticas de retenção e eliminação de dados**: Definir políticas específicas para a **retenção e eliminação** de dados, garantindo que as informações sejam mantidas apenas pelo tempo necessário e eliminadas de forma segura ao fim de sua utilização.

- **Gestão de incidentes de segurança**: Implementar e documentar procedimentos robustos para a **detecção, resposta e mitigação** de incidentes de segurança que envolvam dados pessoais, garantindo conformidade com os prazos e exigências da **ANPD**.

Estas medidas são essenciais para reduzir os riscos legais e operacionais, proteger os direitos dos titulares de dados e assegurar a conformidade da Cambé Previdência com a **LGPD**.

3.2.2.1. Manifestação da Unidade Auditada

A unidade auditada reconheceu a relevância do achado e consentiu com sua implementação, destacando o compromisso em adotar as medidas recomendadas para aprimorar os processos de segurança da informação e conformidade.

3.2.3. Servidores e prestadores de serviço acessam informações sem compromissos formais de segurança, com lacunas na conscientização e treinamento insuficiente

A **Política de Segurança da Informação (PSI) da Cambé Previdência** não define, de forma clara e formal, as **responsabilidades** de todos os servidores e prestadores de serviço que acessam informações do **RPPS**. Verificou-se que esses usuários possuem acesso aos dados sem a exigência de **termos de responsabilidade formalmente assinados** e sem a implementação de um programa estruturado de **conscientização e treinamento em segurança da informação.**

A avaliação foi realizada a partir da resposta à questão de auditoria e encaminhamento de informações e documentos pelo auditado, conforme segue abaixo:

Questão de auditoria: A Política de Segurança da Informação da Cambé Previdência abrange todos os servidores e prestadores de serviço que acessam informações do RPPS, indicando claramente as responsabilidades de cada um quanto à segurança da informação?

Reposta do auditado: A PSI atende parcialmente.

INFORMAÇÕES REQUERIDAS	INFORMAÇÕES, DOCUMENTOS OU JUSTIFICATIVAS ENVIADAS PELO AUDITADO
RELAÇÃO DOS ARTIGOS OU ANEXOS DA PSI QUE EVIDENCIAM A ABRANGÊNCIA DE TODOS OS SERVIDORES E PRESTADORES DE SERVIÇO QUE ACESSEM INFORMAÇÕES DO RPPS	Anexo 3.1 – Portaria 019/2023 – Artigos 1º e 2º
TERMOS DE RESPONSABILIDADE ASSINADOS POR SERVIDORES E PRESTADORES DE SERVIÇO	Anexo 3.2: Não dispomos de Termo de recebimento, porém a informação é explicitada no Termo de Referência que é parte integrante nos processos licitatórios
REGISTROS DE TREINAMENTO E CONSCIENTIZAÇÃO	Além da publicação em órgão oficial do município da Portaria 019 de 26 de outubro de 2023 -PSI - e, ainda, publicação permanente do documento na página da internet desta Autarquia Municipal - Cambé Previdência - não há plano de ação para treinamentos periódicos para servidores e prestadores de serviços acerca das práticas e responsabilidades explicitadas na política de segurança da informação

A avaliação realizada, teve como objetivo verificar se a **Política de Segurança da Informação** abrange todos os **servidores e prestadores de serviço** que acessam informações do **RPPS**, indicando claramente suas **responsabilidades** em relação à segurança da informação. A questão central da auditoria foi verificar se existem **termos de responsabilidade assinados** e se a autarquia promove **treinamentos periódicos** para conscientização e capacitação dos colaboradores.

Para isso, o auditado foi solicitado a apresentar a **relação dos artigos da PSI** que tratam dessas responsabilidades, **termos de responsabilidade assinados** por servidores e prestadores de serviço, bem como **registros de treinamentos** realizados. A Cambé Previdência respondeu que a PSI **atende parcialmente**, enviando a **Portaria 019/2023** (Artigos 1º e 2º) como evidência, mas informou que **não dispõe de termos de recebimento** assinados pelos servidores e prestadores. Além disso, não foi identificado um **plano de ação para treinamentos periódicos**, o que demonstra **lacunas na conscientização e capacitação** sobre segurança da informação.

A auditoria identificou que a **PSI da Cambé Previdência** não formaliza claramente as responsabilidades de **servidores e prestadores de serviço** que acessam informações do **RPPS**. **Termos de responsabilidade assinados** não foram apresentados, e não há um **plano de treinamentos periódicos** para conscientização sobre segurança da informação. A publicação da PSI no portal oficial não garante que os colaboradores compreendam plenamente suas responsabilidades, deixando a organização vulnerável a **acessos indevidos** e **uso inadequado das informações**.

O critério utilizado para avaliar a **PSI da Cambé Previdência** foi baseado nas **melhores práticas de segurança da informação**, exigindo que a política abrangesse todos os **servidores e prestadores de serviço** que acessam informações do **RPPS**, com a devida **formalização de responsabilidades** e a realização de **treinamentos periódicos**.

A falta de **formalização de responsabilidades** e a ausência de **treinamentos periódicos** expõem a Cambé Previdência a **riscos significativos**, como **acessos indevidos**, **uso inadequado de informações** e **vazamentos de dados**. Sem esses controles, a autarquia fica vulnerável a falhas de segurança que podem comprometer a **proteção dos dados do RPPS**,

gerando possíveis **sanções** e **não conformidade** com a **LGPD** e as diretrizes do **Pró-Gestão RPPS**.

Recomenda-se que a Cambé Previdência formalize os compromissos de segurança, estabelecendo e implementando **termos de responsabilidade assinados** por todos os servidores e prestadores de serviço que acessam informações do RPPS, garantindo que cada colaborador compreenda suas obrigações em relação à segurança da informação. Além disso, deve-se implementar um **programa contínuo de treinamento e conscientização**, desenvolvendo e aplicando **treinamentos periódicos** sobre boas práticas de segurança da informação, a fim de reforçar a importância da segurança e mitigar riscos operacionais.

3.2.3.1. Manifestação da Unidade Auditada

A unidade auditada reconheceu a relevância do achado e consentiu com sua implementação, destacando o compromisso em adotar as medidas recomendadas para aprimorar os processos de segurança da informação e conformidade.

3.2.4. Procedimentos sobre controle de acesso (físico e lógico) aos sistemas informatizados e bancos de dados não formalizados, ausência de planos de contingência adequados, com risco de perda de dados e interrupção de serviços críticos em caso de incidentes

Os procedimentos de **controle de acesso (físico e lógico)** aos sistemas informatizados e bancos de dados da Cambé Previdência **não estão formalizados**, assim como os **planos de contingência** e recuperação de desastres. Essa ausência de documentação e procedimentos claros coloca em risco a continuidade dos serviços críticos e aumenta a vulnerabilidade a **perda de dados** em caso de incidentes graves, além de comprometer a segurança e integridade dos sistemas.

A avaliação foi realizada a partir da resposta à questão de auditoria e encaminhamento de informações e documentos pelo auditado, conforme segue abaixo:

Questão de auditoria: A Cambé Previdência possui procedimentos mapeados e manualizados sobre controle de acesso (físico e lógico) aos sistemas informatizados e bancos de dados, e possui procedimentos de contingência formalizados que garantam a existência de planos de recuperação de desastres, cópias de segurança (backups) e continuidade dos serviços críticos em caso de incidentes?

Reposta do auditado: Não há procedimentos mapeados e manualizados sobre o controle físico e lógico do banco de dados.

INFORMAÇÕES REQUERIDAS	INFORMAÇÕES, DOCUMENTOS OU JUSTIFICATIVAS ENVIADAS PELO AUDITADO
PROCEDIMENTOS DOCUMENTADOS DE CONTROLE DE ACESSO (FÍSICO E LÓGICO)	Todos os servidores que atuam nesta Autarquia, dispõe de usuários e senhas próprias para acessos a todos os sistemas, bem como ao servidor de arquivos.
PLANOS DE CONTINGÊNCIA E RECUPERAÇÃO DE DESASTRES	Não dispomos de procedimentos formalizados para gerenciar incidentes graves.
REGISTROS DE BACKUPS	Possuímos backup – mas não dispomos de testes completos de restauração.
POLÍTICAS DE CONTINUIDADE DE NEGÓCIOS	Não dispomos de políticas que descrevam as estratégias e procedimentos adotados para manter os serviços críticos funcionando durante incidentes.

A questão analisada teve o objetivo de avaliar a existência e a adequação dos **procedimentos de controle de acesso** (físico e lógico) aos sistemas informatizados e bancos de dados, bem como a implementação de **planos de contingência** e **recuperação de desastres**. A equipe de auditoria solicitou ao auditado a documentação que comprovasse a formalização desses procedimentos e os registros de backups e políticas de continuidade de negócios.

O auditado indicou que, embora os servidores possuam usuários e senhas próprias, **não há procedimentos formalizados** para gerenciar incidentes graves, **testes de restauração** completos de backups, nem **políticas de continuidade de negócios** que assegurem o funcionamento dos serviços críticos durante incidentes. A ausência desses elementos representa um risco significativo para a segurança e a operacionalidade da autarquia, podendo afetar diretamente a proteção dos dados do RPPS.

Ficou constatado que a **Cambé Previdência** não possui **procedimentos formalizados** de controle de acesso, tanto físico quanto lógico, aos sistemas informatizados e bancos de dados. Além disso, não foram implementados **planos de contingência** ou **procedimentos de recuperação de desastres** para garantir a continuidade dos serviços críticos em caso de incidentes. Embora realizem backups, não há registros de**testes completos** que assegurem a recuperação eficaz dos dados, nem políticas adequadas de **continuidade de negócios**, o que compromete a segurança e a eficiência operacional da autarquia.

Os padrões estabelecidos pelas **boas práticas de segurança da informação** e normas como a **ISO/IEC 27001** e **ISO/IEC 27002** determinam que as organizações devem adotar **procedimentos formalizados de controle de acesso** a sistemas e dados, implementar **planos de contingência** para garantir a recuperação rápida em caso de incidentes, e realizar **testes periódicos de backups**. Esses critérios garantem a **continuidade dos serviços críticos** e a **proteção contra a perda de dados**, sendo exigidos também pelo **Pró-Gestão RPPS**.

A ausência de procedimentos formalizados de **controle de acesso** e **planos de contingência** coloca a Cambé Previdência em situação de vulnerabilidade. Sem esses mecanismos, há um risco elevado de **perda de dados**, **interrupção dos serviços críticos** e **exposição a ataques**

cibernéticos. Além disso, a falta de políticas adequadas pode resultar em **demora na recuperação de incidentes graves**, comprometendo a **continuidade operacional** e a **proteção das informações** do RPPS, com possíveis consequências legais e operacionais.

A **Cambé Previdência** possui fragilidades operacionais devido à falta de **procedimentos formalizados** para o controle de acesso aos sistemas e dados, assim como à ausência de **planos de contingência** e mecanismos de recuperação em situações de crise. Esses fatores elevam o risco de interrupções nos serviços essenciais e expõem os dados do RPPS a vulnerabilidades que podem resultar em perdas irreversíveis. A implementação de políticas robustas para assegurar a **continuidade dos serviços** e a proteção das informações é uma medida necessária e urgente para mitigar esses riscos e garantir a resiliência da autarquia diante de incidentes críticos.

Recomenda-se que a **Cambé Previdência**, defina e formalize os procedimentos abaixo, inclusive mapeando e manualizando:

- **Controle de acesso (físico e lógico)** aos sistemas informatizados e bancos de dados, garantindo que todas as etapas de acesso sejam claramente documentadas, monitoradas e auditáveis, para assegurar a proteção das informações e evitar acessos indevidos.
- **Planos de contingência e recuperação de desastres**, detalhando os procedimentos necessários para gerenciar incidentes graves, assegurando a continuidade dos serviços críticos e a rápida recuperação dos sistemas em caso de falhas.
- **Testes periódicos de backups**, para verificar a eficácia dos backups e garantindo que os dados possam ser recuperados integralmente em caso de incidentes, assegurando a integridade e disponibilidade das informações.
- **Políticas de continuidade de negócios**, descrevendo detalhadamente as estratégias e ações a serem tomadas durante incidentes, com o objetivo de minimizar interrupções nos serviços críticos e assegurar a proteção das informações e a resiliência operacional da autarquia.

3.2.4.1. Manifestação da Unidade Auditada

A unidade auditada reconheceu a relevância do achado e consentiu com sua implementação, destacando o compromisso em adotar as medidas recomendadas para aprimorar os processos de segurança da informação e conformidade.

3.2.5. Necessidade de fortalecimento da Política de Segurança da Informação com mecanismos de controle e implementação de monitoramento contínuo e transparente

A **PSI da Cambé Previdência** apresenta ausência de **mecanismos formalizados de controle e monitoramento contínuo**, incluindo registros de incidentes de segurança e ações de conformidade. Essa falta de monitoramento impede que a organização acompanhe e avalie de forma contínua o cumprimento da PSI e aplique sanções em caso de não conformidade, o que compromete a integridade dos processos de segurança da informação.

A avaliação foi realizada inicialmente a partir da resposta à questão de auditoria e solicitação de documentos, como segue:

Questão de auditoria: A Política de Segurança da Informação e seus procedimentos estão sendo cumpridos de acordo com os requisitos estabelecidos, e as penalidades previstas estão sendo aplicadas em casos de não conformidade?

Reposta do auditado: Atualmente, não possuímos relatórios de incidentes para apresentar.

INFORMAÇÕES REQUERIDAS	INFORMAÇÕES, DOCUMENTOS OU JUSTIFICATIVAS ENVIADAS PELO AUDITADO
REGISTROS DE INCIDENTES DE SEGURANÇA	Anexo 6.1: Portaria 019/2023 – PSI - Artigos 12º e 13º
AÇÕES DISCIPLINARES APLICADAS	Não enviado
RELATÓRIOS DE NÃO CONFORMIDADE	Não enviado

O objetivo da questão e os documentos solicitados, teve como objetivo saber se existe um acompanhamento para verificar se as diretrizes da PSI estão sendo cumpridas, e quais medidas foram ou serão tomadas em caso de não cumprimento.

A resposta do auditado não ficou evidente se a ausência de relatórios de incidentes e penalidades aplicadas se dá pelo cumprimento total da PSI ou pela falta de mecanismos de controle e monitoramento, então foi realizada uma nova solicitação de auditoria nº **03/2024**, onde foi solicitado resposta a uma nova questão de auditoria e envio de evidências, como segue abaixo:

Questão de auditoria: A Cambé Previdência possui mecanismos de monitoramento contínuo e formalizado para garantir o cumprimento da Política de Segurança da Informação (PSI), incluindo o registro de incidentes de segurança, avaliação periódica e aplicação de penalidades em caso de não conformidade?

Reposta do auditado: Não possuímos manual para registros de monitoramento, conformidade e /ou que evidencie incidentes.

Documentos solicitados: Documentação do processo de monitoramento, evidências de conformidade, registros de incidentes monitorados;

Como a questão foi respondida pelo auditado como critério não atendido, não foram encaminhados os documentos solicitados.

A auditoria realizada teve o objetivo de verificar se a **PSI** está sendo cumprida e se as penalidades previstas são aplicadas em caso de não conformidade. O auditado relatou a inexistência de relatórios de incidentes de segurança e de ações disciplinares, o que indicou uma possível ausência de mecanismos formalizados de monitoramento. Diante disso, solicitou-se uma avaliação mais detalhada sobre os métodos de controle utilizados para garantir o cumprimento da PSI.

A partir da resposta enviada através do **ofício 442/2024** referente ao segundo questionamento, foi confirmado que a **Cambé Previdência** não possui procedimentos formalizados para o **monitoramento contínuo do cumprimento da PSI**, incluindo a falta de registros de incidentes de segurança e de avaliações periódicas de conformidade, o que dificulta a aplicação de sanções quando necessário. Essa ausência de monitoramento impossibilita a identificação de não conformidades e a aplicação de ações corretivas em tempo hábil.

O critério estabelecido para esta avaliação é que a **Cambé Previdência** deve implementar um **sistema formal de monitoramento** que permita o acompanhamento contínuo do cumprimento da PSI, incluindo registros de incidentes e aplicação de ações corretivas e de sanções, conforme recomendam as boas práticas de segurança da informação e o **Manual do Pró-Gestão RPPS**, para garantir a segurança dos dados e a continuidade dos serviços.

A ausência de um monitoramento contínuo do cumprimento da PSI expõe a autarquia a riscos elevados, como a possibilidade de **incidentes de segurança não identificados**, ausência de registros para análise de conformidade e **falhas no cumprimento das diretrizes de segurança da informação**. Isso aumenta a vulnerabilidade da Cambé Previdência a ataques cibernéticos e a potenciais sanções por não conformidade com as normas de segurança.

Recomenda-se que a **Cambé Previdência** estabeleça um **processo de monitoramento formalizado**, que inclua registros de incidentes de segurança, avaliações periódicas de conformidade e um protocolo de resposta a incidentes para aplicação de sanções, quando necessário. Esse processo deve abranger:

1. **Implementação de uma rotina de monitoramento contínuo** para verificar o cumprimento da PSI, documentando cada etapa e responsáveis.
2. **Registro de incidentes de segurança** e acompanhamento de ações corretivas.
3. **Auditorias internas periódicas** para assegurar o cumprimento das normas estabelecidas pela PSI e verificar a eficácia das ações de segurança implementadas.

3.2.5.1. Manifestação da Unidade Auditada

Por meio do **Ofício 487/2024**, a unidade auditada solicitou reconsideração quanto ao achado, especificamente no que se refere à suposta inexistência de penalidades indicadas na **PSI**. Na manifestação, foi citado o **Artigo 27 da Portaria 019/2023**, que estabelece sanções administrativas aplicáveis em casos de descumprimento das diretrizes da PSI.

3.2.5.2. Análise da equipe de auditoria

Com base na análise realizada, esclarecemos que **o achado não apontou a inexistência de penalidades** indicadas na Política de Segurança da Informação (PSI). Reconhecemos que o Artigo 27 da PSI prevê sanções administrativas para casos de descumprimento.

O achado **trata-se da necessidade de fortalecer os mecanismos de controle e acompanhamento**, assegurando que as sanções previstas sejam efetivamente aplicadas, quando cabíveis, com base em evidências documentais e processos claros.

Assim, **mantemos o entendimento descrito no relatório** quanto à necessidade de melhorias nesses aspectos.

3.2.6. Inexistência de área responsável formalmente definida pela gestão da estrutura de TI

A **Cambé Previdência** não possui uma **área formalmente designada** para a **gestão da estrutura de TI**, incluindo hardware, software e segurança da informação. A gestão de TI é realizada de maneira informal com o apoio do corpo técnico da **Prefeitura de Cambé**, sem que haja documentos que formalizem as responsabilidades e atribuições de gestão, o que pode comprometer a segurança e a continuidade dos serviços de TI.

A avaliação foi realizada a partir da resposta à questão de auditoria e solicitação de documentos, como segue:

Questão de auditoria: Existe área responsável formalmente definida pela gestão da estrutura de TI da Cambé Previdência, incluindo hardware, software e segurança da informação?

Reposta do auditado: Não há área de TI, formalmente responsável pelos processos de segurança da informação no âmbito da Autarquia Cambé Previdência. Desde a criação desta Autarquia, contamos com o apoio do corpo técnico da Prefeitura Municipal de Cambé.

Documentos solicitados: Documentação que Defina Formalmente a Área Responsável pela Gestão de TI, Organograma de TI, Atribuições de Papéis e Responsabilidades, Contratos de Terceirização (se aplicável).

Como a questão foi respondida pelo auditado como critério não atendido, não foram encaminhados os documentos solicitados.

O objetivo da questão de auditoria foi verificar se havia uma **área formalmente definida** para a **gestão da estrutura de TI**, responsável por garantir o funcionamento adequado de hardware, software e segurança da informação. O foco era analisar se a gestão de TI estava devidamente estruturada, com papéis e responsabilidades claramente definidos, conforme as boas práticas de segurança e continuidade de TI.

O auditado informou que, desde a criação da autarquia, a gestão de TI é realizada com o apoio do corpo técnico da **Prefeitura Municipal de Cambé**, sem apresentar documentos de formalização de uma área ou equipe específica para desempenhar essa função. Esse arranjo gera **lacunas na responsabilização** e falta de clareza na execução de ações relacionadas à TI, essenciais para o bom funcionamento dos sistemas da autarquia.

Durante a auditoria, constatou-se que a **Cambé Previdência** não conta com uma **estrutura formalizada** para a **gestão de tecnologia da informação** e não tem um organograma que detalhe as atribuições específicas para a administração dos sistemas e da segurança da

informação. O suporte técnico atual é realizado pela **Prefeitura de Cambé**, mas essa parceria não está documentada formalmente, o que pode resultar em **ineficiências na gestão da TI** e expor os sistemas a vulnerabilidades, devido à falta de clareza nas responsabilidades.

A ausência de uma área formalmente designada para a gestão de TI na **Cambé Previdência**, aliada à dependência informal do suporte técnico da **Prefeitura de Cambé**, gera **riscos operacionais** significativos. Essa falta de clareza nas responsabilidades pode resultar em **falhas na administração dos sistemas informatizados**, **vulnerabilidades de segurança** e **ineficiências** na implementação de soluções tecnológicas. Além disso, a falta de um processo estruturado dificulta a **tomada de decisões rápidas** em situações críticas, prejudicando a continuidade dos serviços essenciais. Para mitigar esses riscos e garantir a **proteção e eficiência dos sistemas da autarquia**, é crucial formalizar uma equipe ou área específica para a gestão de hardware, software e segurança da informação.

Recomenda-se que a **Cambé Previdência** adote as seguintes medidas para formalizar e fortalecer a gestão de TI, incluindo hardware, software e segurança da informação:

- Realizar um estudo para avaliar a melhor alternativa a ser implantada para a **gestão da estrutura de TI** e segurança da informação, considerando possíveis cenários como: **constituir uma área de TI própria**, que assumiria a responsabilidade pela gestão de hardware, software e segurança da informação, garantindo o monitoramento, controle e revisão das políticas de segurança e a continuidade dos serviços; **manter o apoio técnico da Prefeitura de Cambé**, formalizando essa parceria através de um **acordo de serviços (SLA)** que defina claramente as responsabilidades, níveis de serviço, tempos de resposta e medidas de segurança; ou ainda, buscar **outras opções que satisfaçam o critério** de ter uma área responsável pela gestão de TI, em conformidade com normas de segurança como a **ISO/IEC 27001** e atendendo às exigências do **Pró-Gestão RPPS**, assegurando a **proteção dos dados** e a **continuidade dos serviços informatizados**.
- **Definir e documentar os papéis e responsabilidades** de todos os envolvidos na gestão de TI, seja uma equipe interna, área de TI da prefeitura, ou outra, assegurando que a cadeia de comando seja clara e que haja **processos documentados** para a resolução de incidentes, manutenção de sistemas e execução de atualizações.

3.2.6.1. Manifestação da Unidade Auditada

A unidade auditada reconheceu a relevância do achado e consentiu com sua implementação, destacando o compromisso em adotar as medidas recomendadas para aprimorar os processos de segurança da informação e conformidade.

4. CONCLUSÃO

A criação de uma **Política de Segurança da Informação (PSI)** representa um avanço significativo, atendendo às exigências do **Pró-Gestão RPPS** e contribuindo para a conquista da **certificação de nível II**. Essa certificação destaca o empenho da gestão em estruturar e

promover um ambiente seguro para dados e serviços, refletindo a importância dada à governança e proteção das informações no contexto da autarquia.

As recomendações deste relatório visam fortalecer ainda mais as iniciativas já realizadas, destacando pontos de melhoria que podem ampliar a **eficiência e a segurança** dos sistemas de TI e otimizar a gestão das informações da autarquia. Embora caiba à alta administração da **Cambé Previdência** decidir pela adoção e implementação das recomendações, tais ações contribuirão para robustecer o controle e a continuidade dos serviços informatizados, consolidando o compromisso com a **proteção de dados** e a **segurança institucional**.

Em relação ao destaque apresentado no **Ofício 487/2024**, a secretaria de controle interno enfatiza que cabe à gestão da autarquia avaliar como as recomendações serão implantadas. Caso considere necessário que a regulamentação municipal da LGPD também contemple a Cambé Previdência, sugere-se que a autarquia dialogue com a gestão municipal para verificar a viabilidade dessa inclusão.

Ao adotar essas recomendações, a **Cambé Previdência** poderá reforçar ainda mais sua estrutura de segurança da informação, mantendo-se alinhada às melhores práticas e garantindo uma governança mais eficaz em benefício de toda a organização e de seus usuários.

Por fim, a equipe de auditoria agradece à **Cambé Previdência** pela colaboração e prontidão em fornecer as informações solicitadas ao longo do trabalho. O apoio e comprometimento da autarquia foram fundamentais para a realização desta auditoria, reforçando o compromisso conjunto com a **segurança da informação** e a **eficiência organizacional**.

5. ENCAMINHAMENTO

Com base nos achados da auditoria e visando assegurar a **melhoria contínua dos processos de segurança da informação** da Cambé Previdência, será iniciado o processo de encaminhamento de um modelo de **plano de ação** e um **cronograma de execução**, a serem desenvolvidos pela autarquia. Ressaltamos que a adesão e a implementação das recomendações, seguindo o modelo de plano de ação proposto, cabe exclusivamente à decisão da gestão da autarquia. O plano deve detalhar as medidas corretivas necessárias, prazos, responsáveis pela execução e métricas de acompanhamento para avaliar a eficácia das ações implementadas.

Caso a gestão opte por implementar as recomendações, a **Secretaria de Auditoria e Controle Interno** realizará um monitoramento estruturado para assegurar sua execução adequada dentro dos prazos estabelecidos. Esse acompanhamento envolverá revisões periódicas, reuniões de alinhamento e a coleta de evidências que comprovem a implementação das ações propostas.

A adesão e execução eficaz do plano de ação reforçará o compromisso da autarquia com o **cumprimento das diretrizes do Manual do Pró-Gestão** (versão 3.5) para os níveis de certificação I e II, garantindo a **conformidade com normas de segurança da informação**, bem como com os requisitos da **LGPD**. Isso fortalecerá a proteção dos dados e a **eficiência na**

gestão dos processos internos, promovendo a transparência e a integridade na administração pública.

Cambé, 04 de dezembro de 2024.

Roberval Zamperlini
Responsável

Gislaine M. Moreno Brandelik
Equipe

Homologado por

Vilson Rico

Secretário de Auditoria e Controle Interno


e-Ciga
Ciga
Assinado digitalmente por:
GISLAINE MARGARETE MORENO BRANDELIK
•••.099.559-••
Data: 04/12/2024 10:03
e-Ciga
Ciga
Assinado digitalmente por:
ROBERVAL ZAMPERLINI
•••.061.039-••
Data: 04/12/2024 10:11
e-Ciga
Ciga
Assinado digitalmente por:
VILSON RICO
•••.060.509-••
Data: 04/12/2024 11:00