INSTITUTO DE PREVIDÊNCIA SOCIAL DO MUNICÍPIO DE PAULISTA-PE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO- PSI

MANUAL E MAPEAMENTO DE PROCEDIMENTO DE CONTINGÊNCIA

PREVIPAULISTA
Instituto de Previdência Social do Município do Paulista

Sumário

Rua Democrático de Souza Filho, n° 26, Bairro do Nobre. Paulista-PE
Fone: (81) 3437-0543
comunicacao@previpaulista.pe.gov.br

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
MANUAL DE PROCEDIMENTO DE CONTINGÊNCIA

A instituição possui grande volume de armazenamento de dados e histórico de todos os beneficiários do Regime Próprio de Previdência Social (RPPS). Como esses dados são imprescindíveis para a manutenção das atividades do PREVIPAULISTA e a devida manutenção das aposentadorias e pensões, a necessidade de garantir a integridade das informações e, em casos de eventualidades (incidentes, panes e catástrofes), a recuperação das informações de forma rápida e ordenada, eliminando ou mitigando os possíveis danos, apresentamos o Manual de procedimentos de contingências em complemento a **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.**

DIRETORIA EXECUTIVA

DIRETORA-PRESIDENTE
Giovanna Maria Oliveira da Conceição Cordeiro
ASSESSOR ESPECIAL
Walleska Felix Amaral
COORDENADOR DE PREVIDÊNCIA
Sandra Simplício
COORDENADOR JURÍDICO
Karla Rio Reis
COORDENADOR DE RECURSOS HUMANOS
Karime Soares
COORDENADOR ADMINISTRATIVO-FINANCEIRO
Juarez Marinheiro

Rua Democrático de Souza Filho, n° 26, Bairro do Nobre. Paulista-PE
Fone: (81) 3437-0543
comunicacao@previpaulista.pe.gov.br

1. OBJETIVO

O presente MANUAL DE CONTINGÊNCIA tem por objetivo definir as medidas preventivas e corretivas a serem adotadas para garantir a continuidade dos serviços essenciais no âmbito do INSTITUTO DE PREVIDÊNCIA SOCIAL DO MUNICÍPIO DE PAULISTA-PREVIPAULISTA, em conformidade com o Art. 21 e demais itens correlatos presentes na Política de Segurança da Informação (PSI) do próprio PREVIPAULISTA, visando a proteção das informações, dos processos e demais dados sensíveis diante de falhas técnicas, indisponibilidades, incidentes de segurança, desastres naturais ou quaisquer eventos que comprometam a normalidade das operações institucionais.

2. LEGISLAÇÃO E REFERÊNCIAS

LEI Nº 13.709/2018 – LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): Regulamenta o tratamento de dados pessoais no Brasil, incluindo o setor público.

PRINCIPAIS DEFINIÇÕES NA LGPD:

a) Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
b) Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
c) Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento
d) Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
e) Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
f) Encarregado: pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados pessoais (ANPD).
g) Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Rua Democrático de Souza Filho, n° 26, Bairro do Nobre. Paulista-PE
Fone: (81) 3437-0543
comunicacao@previpaulista.pe.gov.br

MANUAL DE PRÓ-GESTÃO RPPS – VERSÃO 4.0 (2026): Documento orientador para os RPPS, estabelecendo: Obrigatoriedade de política formal de segurança da informação abrangendo servidores e prestadores. Elaboração de manuais de contingência específicos para incidentes. Mapeamento de riscos, controles de acesso, rotinas de backup e procedimentos para incidentes. Processos de revisão e aprimoramento contínuo das políticas e controles.

3. RESPONSABILIDADES

Para assegurar a eficácia do plano de contingência, as responsabilidades de cada setor, área e participante são claramente definidas. Cada envolvido possui funções específicas, fundamentais tanto para a prevenção quanto para a adequada resposta e superação de situações de crise. Essa distribuição de papéis fortalece a governança, a agilidade nas decisões e o cumprimento de todas as etapas previstas neste manual.

A seguir, apresenta-se a relação detalhada das atribuições dos principais responsáveis pelo plano de contingência, contemplando desde a gestão estratégica até a atuação operacional no contexto do **PREVIPAULISTA**:

3.1 DIRETORIA EXECUTIVA: Cabe a Diretoria Executiva aprovar formalmente o Plano de Contingência e suas revisões. Supervisionar periodicamente a execução dos testes, treinamentos e simulações do plano. Garantir os recursos necessários (humanos, tecnológicos e financeiros) para a implantação/atualização do plano. Tomar decisões estratégicas durante eventos críticos, autorizando ações especiais, aquisição de novos serviços/produtos de emergência e comunicação institucional com órgãos externos. Promover a integração entre os setores envolvidos, assegurando o cumprimento das rotinas estabelecidas. Avaliar e homologar os relatórios de incidentes, acompanhando os planos de melhoria.

3.2 CONTROLE INTERNO: Compete ao Controle Interno dar conformidade, atualizar em conjunto com a Diretoria o Plano de Contingência para os sistemas e dados. Implementar rotinas de backup, testar periodicamente a eficácia dos backups e documentar as evidências dos testes.

3.3 COLABORADORES: É responsabilidade do(a) colaborador(a) cumprir rigorosamente as rotinas estabelecidas no Plano de Contingência, inclusive durante simulações e treinamentos. Notificar imediatamente a área de Controle Interno e/ou Diretoria Executiva sobre qualquer ocorrência de falha, indisponibilidade ou suspeita de incidente de segurança da informação. Colaborar em treinamentos e exercícios simulados, participando ativamente das ações propostas para garantir o conhecimento prático do plano. Preservar o ambiente em caso de sinistros,

Rua Democrático de Souza Filho, n° 26, Bairro do Nobre. Paulista-PE
Fone: (81) 3437-0543
comunicacao@previpaulista.pe.gov.br

evitando manipular sistemas ou equipamentos até a autorização da área responsável.

3.4 PRESTADORES DE SERVIÇOS EXTERNOS: cabe aos prestadores auxiliar no suporte técnico especializado à área de TI no processo de restauração de sistemas e serviços contratados. Cumprir prazos previamente estabelecidos para atendimento emergencial em situações de indisponibilidade, conforme cláusulas contratuais. Fornecer rapidamente informações técnicas e orientações necessárias para o retorno das atividades essenciais ou esclarecimentos sobre falhas ocorridas nos sistemas ou contratos sob sua responsabilidade. Participar de revisões do plano quando envolver sistemas, infraestruturas ou processos terceirizados, sugerindo melhorias quando necessário.

3.5 TÉCNICOS INTERNOS (PREVIPAULISTA OU PREFEITURA) - Monitorar continuamente possíveis riscos tecnológicos e alertar a diretoria sobre eventuais vulnerabilidades ou necessidades de atualização de procedimentos. Executar tecnicamente os procedimentos de resposta em caso de sinistros: desligamento seguro dos sistemas, restauração de backups e reestabelecimento dos serviços. Manter inventário atualizado dos ativos de tecnologia (hardware, software, sistemas críticos, redes) e registrar as ações realizadas durante incidentes. Orienta os demais colaboradores e setores sobre os protocolos de segurança da informação e sobre as instruções a serem seguidas em situações emergenciais.

3.6 . DEFINIÇÕES GERAIS

a) Áreas Sensíveis: áreas que se forem atingidas podem provocar grandes danos ao patrimônio;
b) Backup: Cópia de um sistema completo ou de um ou mais arquivos guardados em diferentes dispositivos de armazenamento;
c) Banco de dados: coleção organizada de informações e dados estruturados da instituição
d) PREVIPAULISTA, armazenados eletronicamente em um sistema de computador físico ou virtual e acessado ou modificado pelos usuários padrão;
e) Contingência: situação potencial com risco de danificar sistemas, equipamentos ou
f) Infraestrutura;
g) Setor de Tecnologia da Informaçao:projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados;
h) Equipamento de acesso: qualquer equipamento capaz de se conectar ao banco de dados, de forma física (através de cabos) ou remota (através de rede wi-fi ou bluetooth), como desktops, notebooks, smartphones e tablets;

Rua Democrático de Souza Filho, n° 26, Bairro do Nobre. Paulista-PE
Fone: (81) 3437-0543
comunicacao@previpaulista.pe.gov.br

i) Incidente: evento inesperado ou situação que altera a ordem normal das coisas, capaz de causar danos leves ou mau funcionamento aos sistemas e equipamentos; toda ocorrência anormal, que foge ao controle de um processo, sistema ou atividade;
j) Intervenção: é a atividade de atuar durante a emergência, seguindo o plano de ação para corrigir ou minimizar os possíveis danos aos equipamento e sistemas de TI;
k) Servidor físico: equipamento que armazena o banco de dados da instituição, contendo todos os softwares e hardwares necessários para a proteção dos dados, inclusive com espelhamento de backup. Das empresas contratadas da área de tecnologia ou de banco de dados do Previpaulista.
l) Servidor virtual: servidor remoto (nuvem) onde será feito o backup dos dados do servidor físico para garantir a integridade das informações e dados em caso de pane no servidor físico;
m) Situação de Emergência: Situação gerada por evento em um sistema ou equipamento que resulte ou possa resultar em danos graves, parada ou mau funcionamento dos próprios sistemas ou equipamentos ou ao desempenho do trabalho dos usuários;
n) TI: Tecnologia da Informação.

4. ETAPAS DA EXECUÇÃO DO PLANO DE CONTINGÊNCIA

4.1 IDENTIFICAÇÃO E CLASSIFICAÇÃO DE RISCOS

a) Cibersegurança e Ameaças Cibernéticas: Inclui ataques como *ransomware*, *phishing*, *malware* e ataques de negação de serviço (DDoS) que podem paralisar operações.
b) Violação de Dados (Data Breach): Roubo ou vazamento de informações confidenciais de clientes, fornecedores ou propriedade intelectual da empresa.
c) Riscos Operacionais e de Infraestrutura: Falhas em hardware, bugs de software, erros humanos e problemas de disponibilidade dos sistemas (servidores fora do ar).
d) Riscos Estratégicos e de Governança: Desalinhamento da TI com os objetivos de negócios, falta de investimento, ou falha na adoção de tecnologias adequadas.
e) Riscos de Compliance e Regulatórios: Não conformidade com leis de proteção de dados (como LGPD), gerando multas e danos à reputação.

Rua Democrático de Souza Filho, n° 26, Bairro do Nobre. Paulista-PE
Fone: (81) 3437-0543
comunicacao@previpaulista.pe.gov.br

f) Ameaças Internas: Funcionários ou terceiros com acesso autorizado que abusarão desses privilégios para vazar ou roubar dados
g) Qualquer evento em potencial que está relacionado à área de tecnologia da informação e pode impactar a TI e o negócio.

Esta etapa consiste em analisar cuidadosamente todos os processos, ativos e áreas críticas no âmbito do **PREVIPAULISTA**, buscando identificar possíveis ameaças que possam comprometer a continuidade dos serviços, como falhas de sistemas, interrupções elétricas, ataques digitais, eventos naturais, erros operacionais ou humanos.

Após a identificação, é realizada a classificação desses riscos segundo critérios de probabilidade de ocorrência e impacto potencial, priorizando os que exigem resposta mais rápida e efetiva. Essa classificação orienta as ações subsequentes do plano, garantindo que os recursos e esforços estejam focados naquilo que é mais essencial para o funcionamento do regime previdenciário.

4.2 CLASSIFICAÇÃO DE RISCO (MATRIZ IMPACTO X PROBABILIDADE)

A priorização dos riscos geralmente segue uma matriz que cruza a probabilidade de ocorrência com o impacto no negócio, com níveis comuns sendo:

a) **Baixo/Leve:** Pequeno impacto operacional, fácil mitigação.
b) **Moderado:** Impacto perceptível, exige resposta rápida.
c) **Severo/Alto:** Interrupção significativa dos serviços ou vazamento de dados sensíveis.
d) **Crítico/Massivo:** Parada total de atividades essenciais, perdas financeiras enormes (recursos previdenciários), danos graves à reputação

4.3 ELABORAÇÃO DAS ESTRATÉGIAS DE CONTINGÊNCIA

Para reduzir a exposição ao risco, recomenda-se:

- **Plano de Contingência:** Elaborar estratégias de recuperação após desastres.
- **Segurança da Informação:** Adotar criptografia e controle de acesso rígido.
- **Atualização de Hardware/Software:** Manter os sistemas atualizados para evitar bugs e vulnerabilidades.
- **Treinamento:** Capacitar funcionários contra ataques de engenharia social (phishing)

Nesta fase, são definidos detalhadamente os procedimentos preventivos e corretivos a serem adotados diante de cada tipo de risco identificado. Isso inclui o passo a passo para o desligamento seguro dos sistemas, a conservação dos dados

Rua Democrático de Souza Filho, n° 26, Bairro do Nobre. Paulista-PE
Fone: (81) 3437-0543
comunicacao@previpaulista.pe.gov.br

e a proteção das informações e dos dados sensíveis, a fim de evitar a ocorrência de qualquer tipo de dano, ou, caso o incidente aconteça, atenuar sua gravidade, seja este patrimonial, intelectual ou moral, que possa afetar direta ou indiretamente o PREVIPAULISTA, seus colaboradores, segurados e prestadores de serviços.

A Estratégia deve ser elaborada e aplicada considerando cada caso concreto, com foco em alcançar a melhor solução para a situação de forma célere e eficaz, de modo a impedir a ocorrência de danos, ou, caso já tenham ocorrido, mitigar sua gravidade. Busca-se, assim, garantir o bom funcionamento das atividades e o bem-estar de todos os envolvidos.

Para situações como vazamento de dados, acesso indevido, erro humano e outros riscos, devem ser estabelecidos planos de resposta específicos, abrangendo desde simples falhas operacionais até grandes interrupções causadas por sinistros, incidentes de segurança ou indisponibilidade total da infraestrutura. Também são organizadas alternativas de continuidade, visando a minimizar o tempo de paralisação e os prejuízos para o Instituto.

4.4 COMUNICAÇÃO

A comunicação eficaz é fundamental durante qualquer situação de contingência. Por isso, define-se um fluxo claro e oficial para que incidentes sejam prontamente comunicados à Diretoria Executiva, à equipe de Controle Interno e aos principais colaboradores.

Neste contexto, devem estar definidos os responsáveis por iniciar a comunicação e os canais que serão utilizados para tal, como o uso de e-mail, telefones, aplicativos, reuniões presenciais ou virtuais e demais meios de comunicação pertinentes ao caso concreto que se julgue necessário para a resolução do incidente.

Se faz necessário também definir claramente os níveis de notificação (riscos) e os critérios para acionar, quando necessário, as autoridades, órgãos reguladores, segurados ou fornecedores, conforme previsto na legislação. Salienta-se que todo o histórico das comunicações deve ser arquivado para caso se julgue necessário, a realização de uma posterior análise e/ou prestação de contas.

4.5 EXECUÇÃO DE ROTINAS DE BACKUP E RECUPERAÇÃO

O sucesso do plano de contingência depende da existência de políticas robustas e bem executadas de backup e recuperação. Aqui, são estabelecidas rotinas de backup dos dados críticos do **PREVIPAULISTA**, definindo a frequência apropriada e os tipos de backup (completo, incremental, diferencial), bem como a localização e a proteção desses arquivos (em mídia física externa, servidores

Rua Democrático de Souza Filho, n° 26, Bairro do Nobre. Paulista-PE
Fone: (81) 3437-0543
comunicacao@previpaulista.pe.gov.br

remotos ou na nuvem). São agendadas rotinas para teste e validação dos backups por meio de simulações reais de restauração, para garantir que a recuperação será possível e eficiente quando necessário.

4.6 TESTES, ATUALIZAÇÕES E TREINAMENTOS

Para que o plano seja realmente efetivo, é indispensável realizar exercícios práticos (simulados de crise ou testes de mesa) periodicamente, a fim de treinar os envolvidos e identificar pontos de melhoria. Sempre que houver um incidente real, uma mudança tecnológica ou organizacional relevante, ou novo requisito na legislação, o plano deve ser revisto e atualizado, garantindo que permaneça aderente à realidade. Uma rotina obrigatória de capacitação dos colaboradores sensibiliza e prepara todos para agir com precisão e responsabilidade em situações de emergência.

4.7 RETORNO À NORMALIDADE

Encerrado o incidente, inicia-se o processo de avaliação do retorno à normalidade. São verificados todos os sistemas, dados e serviços para certificar a estabilidade e a integridade das operações. Essa etapa envolve a documentação do que ocorreu, das ações tomadas e dos resultados, produzindo relatório detalhado e recomendações para prevenção de situações futuras. As lições aprendidas são compartilhadas formalmente, alimentando um ciclo contínuo de aprimoramento do plano e elevação do nível de maturidade da gestão de riscos do **PREVIPAULISTA**.

5. APROVAÇÃO

A aprovação deste Manual de Contingência é de responsabilidade da Diretoria Executiva do **PREVIPAULISTA**, a quem cabe analisar a aderência do documento à legislação vigente, às diretrizes do Pró-Gestão RPPS e às necessidades operacionais e tecnológicas da instituição. A Diretoria Executiva avalia o conteúdo do manual, revisa suas rotinas e estratégias, e só após sua validação formal o procedimento é instituído como norma interna e passa a vigorar em toda a Unidade Gestora do **PREVIPAULISTA**.

Essa aprovação deve ser realizada por meio de despacho, ata ou termo específico, devidamente assinado pelo(s) responsável(eis) da Diretoria Executiva, garantindo a legitimidade e validade do documento para toda a equipe. Recomenda-se, ainda, que o manual aprovado seja amplamente divulgado para todos os colaboradores e que sua existência e última revisão fiquem registradas em controles internos do RPPS.

Rua Democrático de Souza Filho, n° 26, Bairro do Nobre. Paulista-PE
Fone: (81) 3437-0543
comunicacao@previpaulista.pe.gov.br

A cada revisão, atualização ou modificação do manual, um novo processo formal de aprovação deverá ser conduzido pela Diretoria Executiva, reafirmando seu compromisso com a governança, segurança institucional e continuidade dos serviços previdenciários.

Rua Democrático de Souza Filho, n° 26, Bairro do Nobre. Paulista-PE
Fone: (81) 3437-0543
comunicacao@previpaulista.pe.gov.br

RESPONSABILDADES

PARTICIPANTES	RESPONSABILIDADE
DIRETORIA EXECUTIVA	Aprovar, supervisionar e monitorar o plano de contingência
CONTROLE INTERNO	Dar conformidade,
COLABORADORES/SOLICITANTE	Cumprir rotinas estabelecidas e comunicar quaisquer incidentes
PRESTADORES DE SERVIÇOS/RESPONSÁVEL PELO TRATAMENTO DOS DADOS	Apoiar tecnicamente na restauração e manutenção dos sistemas

PROCEDIMENTOS

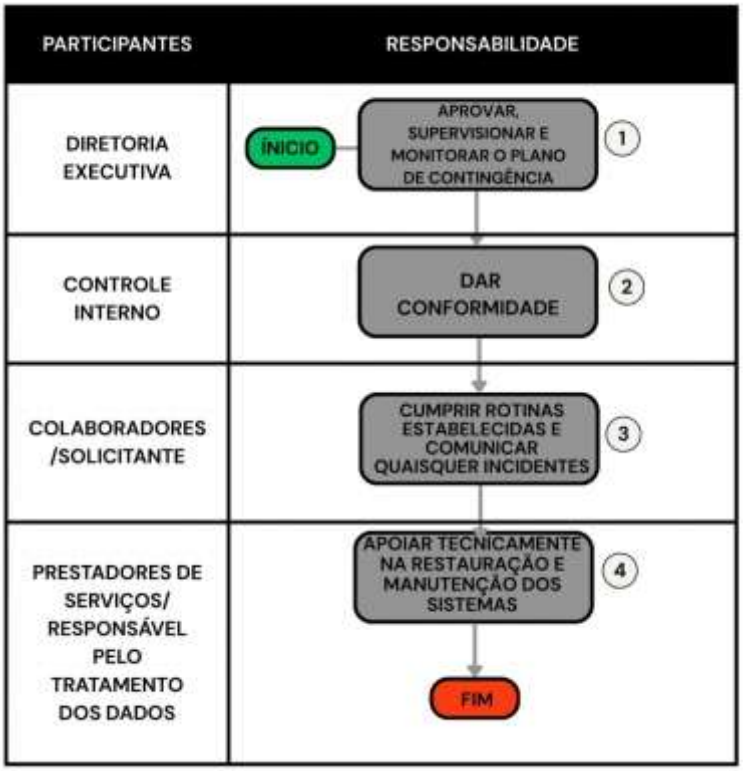
PARTICIPANTES	RESPONSABILIDADE
SOLICITANTE	Faz a solicitação ao responsável pela PSI (Setor de controle Interno)
RESPONSÁVEL PELO TRATAMENTO DOS DADOS	Autua a solicitação e decide se é necessário dar continuidade ou não, caso não seja necessário arquiva e comunica o solicitante
RESPONSÁVEL PELO TRATAMENTO DOS DADOS	Se sim, encaminhar os dados para Diretor Presidente
DIRETOR(A) PRESIDENTE	Analisa se está de acordo com as medidas da PSI Se não - solicitar as ações necessárias de retificação Se sim – Ratificar o plano e encaminhar para recuperação
CONTROLE INTERNO	Dar a conformidade
RESPONSÁVEL PELO TRATAMENTO DOS DADOS	Se não – Analisar e aplicar as correções Se sim – Implementar Plano de recuperação das informações e monitorar a execução

Rua Democrático de Souza Filho, n° 26, Bairro do Nobre. Paulista-PE
Fone: (81) 3437-0543
comunicacao@previpaulista.pe.gov.br

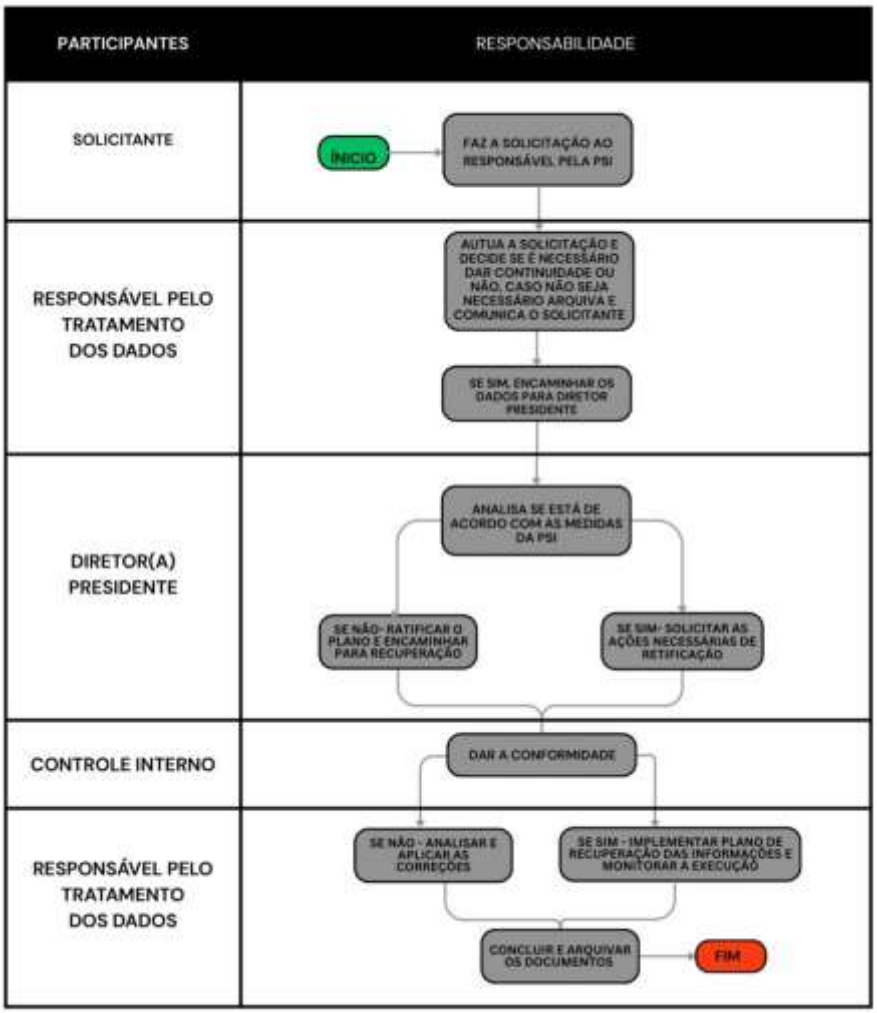
RESPONSÁVEL PELO TRATAMENTO DOS DADOS	Concluir e arquivar os documentos

Rua Democrático de Souza Filho, n° 26, Bairro do Nobre. Paulista-PE
Fone: (81) 3437-0543
comunicacao@previpaulista.pe.gov.br

6. MAPEAMENTOS (FLUXOGRAMAS)



Rua Democrático de Souza Filho, n° 26, Bairro do Nobre. Paulista-PE
Fone: (81) 3437-0543
comunicacao@previpaulista.pe.gov.br



Rua Democrático de Souza Filho, n° 26, Bairro do Nobre. Paulista-PE
Fone: (81) 3437-0543
comunicacao@previpaulista.pe.gov.br