Instituto de Previdência dos
Servidores do Distrito Federal

PROCEDIMENTOS DE CONTINGÊNCIA DE CÓPIAS DE SEGURANÇA DOS SISTEMAS INFORMATIZADOS

2026 Brasília - DF

GOVERNO DO DISTRITO FEDERAL

Governadora
Celina Leão

INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES DO DISTRITO FEDERAL

Diretora-presidente
Raquel Galvão Rodrigues da Silva

Diretora de Governança, Projetos e Compliance
Sylvia Neves Alves

Diretora de Administração e Finanças
Elaine De Fatima De Almeida Lima

Diretor de Previdência
Pedro Henrique Araújo Nabarrete Gabini

Diretor Jurídico
Radam Nakai Nunes

Diretor de Investimentos
Thiago Mendes Rodrigues

Controladoria
Maurílio de Freitas

Unidade de Atuária
Jucelina Santana da Silva

Unidade de Comunicação Social
Hadassa da Rocha Marques

Elaboração
Filipe Silva Santos
Helber do Nascimento Soares
Coordenação de Gestão e Tecnologia da Informação

EDIÇÃO GRÁFICA

Unidade de Comunicação Social
Raphaela Satiko Reis Watanabe

Sumário

INTRODUÇÃO

A modernização institucional do IPREV-DF pressupõe a transição de um modelo de gestão funcional e fragmentado para uma abordagem por processos. Esta visão sistêmica permite que a tecnologia da informação atue como o elo de integração entre as diversas unidades administrativas, substituindo a burocracia rígida por fluxos de trabalho fluidos, transparentes e orientados a resultados para o segurado do Regime Próprio de Previdência Social (RPPS).

Nesse cenário, a manualização consolida-se como um instrumento estratégico de governança. Este documento tem por finalidade traduzir as rotinas operacionais de forma clara e padronizada, servindo como um guia indispensável tanto para os servidores, na condição de executores, quanto para os usuários que dependem da segurança e integridade dos sistemas previdenciários.

O presente Manual de Controle de Contingência de cópias de Segurança dos sistemas Informatizados e Bancos de Dados foi estruturado com o objetivo de organizar e proteger os ativos de informação do Instituto. Ele atua como um mecanismo gerencial que facilita a compreensão da arquitetura de nossos sistemas e garante a rastreabilidade necessária para a conformidade com as normas de segurança vigentes.

Cabe destacar que esta versão inicial retrata o diagnóstico do cenário atual (As-Is) dos procedimentos operacionais. Com base neste mapeamento, a Coordenação, em colaboração estreita com as gerências de cada setor, conduzirá uma análise criteriosa para a identificação de melhorias e a implementação de novas camadas de eficiência tecnológica, assegurando a evolução contínua da infraestrutura digital do IPREV-DF

OBJETIVO

Estabelecer procedimentos de contingência no âmbito do IPREV-DF, contemplando a existência de cópias de segurança dos sistemas informatizados e dos bancos de dados garantindo a continuidade dos serviços essenciais.

ABRANGÊNCIA

Aplica-se a todos os:

- Sistemas informatizados do IPREV-DF;
- Bancos de dados institucionais;
- Ambientes físicos críticos (Processamento de dados, redes, telecomunicações);
- Servidores, colaboradores e prestadores de serviço).

BASE NORMATIVA

- Política de Segurança da Informação do IPREV-DF (POSIC);
- Normativos internos vigentes;
- Boas práticas de Governança de TI.

RESPONSABILIDADES

Por ser Autarquia que faz uso e possui serviços providos pelo Centro de Dados Corporativo Privado do Distrito Federal (CeTIC-DF), na forma do Decreto Distrital nº 40.015, de 14 de agosto de 2019, o IPREV/DF segue o disposto na Resolução Nº 02, de 29 de abril de 2024, que aprova a Política de Backup e Recuperação de Dados do Governo do Distrito Federal.

PROCEDIMENTOS DE CONTIGÊNCIA

DIRETRIZES GERAIS

A Política de Backup e Recuperação de Dados objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pela SEEC/DF, por intermédio da sua Secretaria Executiva de Tecnologia da Informação e Comunicação – SETIC, formalmente definidos como de necessária salvaguarda, para se manter a continuidade do negócio. É fundamental que sejam estabelecidos mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças.

Backup e restore são cópias de segurança, tendo por objetivo que os usuários se resguardem de uma ocasional perda de arquivos originais, seja por ações do próprio usuário ou mau funcionamento dos sistemas, permitindo assim a restauração das informações ou dados eventualmente perdidos.

Os procedimentos de contingência têm como finalidade assegurar a continuidade dos serviços e a recuperação das informações em caso de falhas, incidentes ou desastres.

CÓPIAS DE SEGURANÇA (BACKUP)

Abrangência - São realizadas cópias de segurança dos seguintes ativos:

- Sistemas informatizados;
- Bancos de dados;
- Arquivos institucionais relevantes;

Periodicidade:

- Backups realizados de forma periódica (diária, semanal ou conforme criticidade do sistema);

Tipos de Backup:

- Completo (full);
- Incremental ou diferencial (quando aplicável);

Armazenamento:

- Em ambiente seguro;
- Preferencialmente segregado do ambiente principal;

Testes de Restauração:

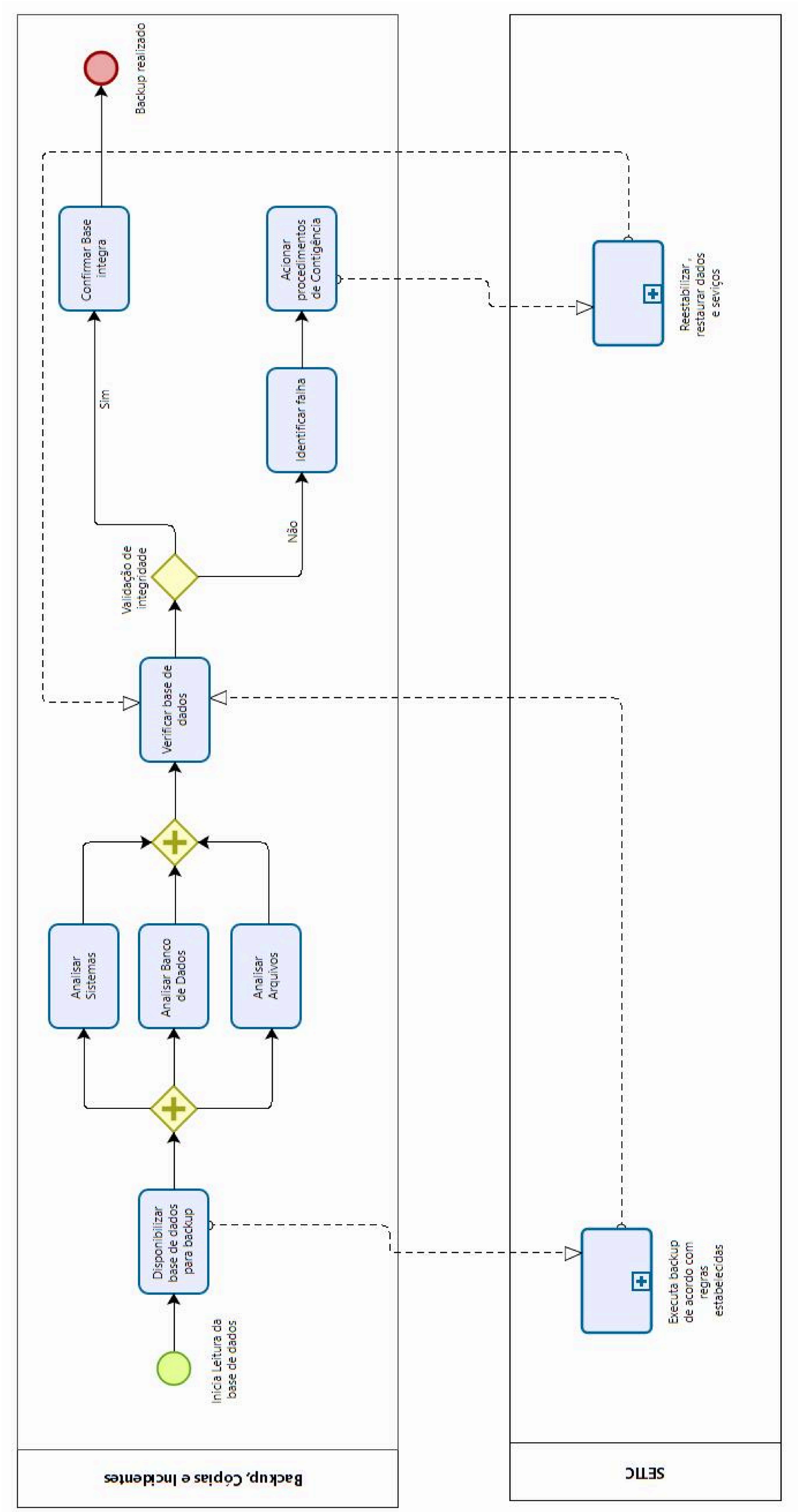
- Realização periódica de testes de recuperação;
- Validação da integridade dos dados;

PROCEDIMENTOS EM CASO DE INCIDENTE

Em caso de falha ou indisponibilidade:

1. Identificação do incidente;
2. Comunicação imediata à SETIC;
3. Avaliação do impacto;
4. Acionamento dos procedimentos de contingência;
5. Restauração dos dados a partir do backup;
6. Restabelecimento dos serviços;

FLUXOGRAMA


Backup realizado
Confirmar Base integra
Acionar procedimentos de Contigência
Identificar falha
Sim
Não
Validação de integridade
Verificar base de dados
Analisar Sistemas
Analisar Banco de Dados
Analisar Arquivos
Disponibilizar base de dados para backup
Inicia Leitura da base de dados
Reestabilizar , restaurar dados e seviços
Executa backup de acordo com regras estabelecidas
Backup, Cópias e Incidentes
SETIC

DISPOSIÇÕES FINAIS

Este manual formaliza os procedimentos de contingência no âmbito do IPREV-DF, atendendo às diretrizes de segurança da informação e às boas práticas de governança, garantindo a proteção dos ativos institucionais e a continuidade dos serviços.

IPREV DF

Instituto de Previdência dos
Servidores do Distrito Federal