



Instituto de Previdência Social dos Servidores Públicos do Município de Balneário Piçarras – IPRESP.

MANUAL DO PLANO DE CONTINGÊNCIA DOS SISTEMAS INFORMATIZADOS DO INSTITUTO DOS SERVIDORES PÚBLICOS DO MUNICÍPIO DE BALNEÁRIO PIÇARRAS – IPRESP

ESTE DOCUMENTO FOI ASSINADO EM: 10/09/2025 10:57 -03:00 - 03
PARA CONFERÊNCIA DO SEU CONTEÚDO ACESSAR <https://ic.ipm.com.br/pe581c6163a82>.



Manual do Plano de Contingência dos Sistemas Informatizados	VERSÃO	APROVADO
	1.0	09/2025
Diretoria Executiva e Departamento de Tecnologia da Informação		



1. INTRODUÇÃO

O Instituto dos Servidores Públicos do Município de Balneário Piçarras – IPRESP, é uma autarquia municipal e presta serviços de previdência para os funcionários do município de Balneário Piçarras. 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 órgão e o devido pagamento das aposentadorias e pensões, há 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.

2. OBJETIVOS

- Garantir a rápida recuperação do banco de dados em casos de incidentes;
- Eliminar ou mitigar os possíveis danos;
- Reestabelecer plenamente o sistema de informações.

3. DOCUMENTOS COMPLEMENTARES

- Manual de Controle de Acesso aos Sistemas Informatizados do IPRESP¹;
- Instrução Normativa do Controle Interno 004/2025²;
- Política de Segurança da Informação do IPRESP (PSI)³.

4. APLICAÇÃO

Este documento será aplicado a todos os serviços e sistemas de Tecnologia da Informação que são providos ou mantidos pelo IPRESP, sejam em sua sede ou qualquer outra dependência, inclusive em servidores virtuais.

¹ <https://ipresp.sc.gov.br/controles-internos/mapeamento-manualizacao/>

² <https://ipresp.sc.gov.br/controles-internos/politica-de-seguranca-da-informacao/>

³ <https://ipresp.sc.gov.br/controles-internos/politica-de-seguranca-da-informacao/>





5. DEFINIÇÕES

Áreas Sensíveis: áreas que se forem atingidas podem provocar grandes danos ao patrimônio;

Backup: Cópia de um sistema completo ou de um ou mais arquivos guardados em diferentes dispositivos de armazenamento;

Banco de dados: coleção organizada de informações e dados estruturados da instituição IPRESP, armazenados eletronicamente em um sistema de computador físico ou virtual e acessado ou modificado pelos usuários padrão;

Contingência: situação potencial com risco de danificar sistemas, equipamentos ou infraestrutura;

Data Center: ou Centro de Processamento de Dados, é um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados;

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*;

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;

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;

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*. O servidor físico será instalado em sala com temperatura controlada e com sistema





contra falta de energia;

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;

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;

TI: Tecnologia da Informação.

6. RESPONSABILIDADES

As responsabilidades pela manutenção, monitoramento e recuperação do banco de dados em casos de incidentes estão distribuídas de acordo com o nível de competência de cada usuário e sistema.

Diretoria Executiva: Responsável pela definição das funções de cada área e usuário. Também, pela destinação de recursos para elaboração, implementação e execução do plano.

Gestor de Informações Lógicas: Responsável pelo monitoramento do plano, baseado nas informações recebidas pelos usuários e pela solicitação da execução em caso de incidentes.

Área de Tecnologia de Informação: Deve executar o Plano de Contingência com a maior brevidade possível assim que acionada pelo Gestor de Informações e conter ou mitigar os impactos decorrentes de emergências que afetem os sistemas, equipamentos ou infraestrutura do IPRESP.

Usuário padrão: Responsável por informar o Gestor de Pessoas ou a área de TI qualquer incidente, anomalia ou emergência que detectem, a qualquer momento, nos sistemas e equipamentos do IPRESP.



7. NÍVEIS DE INCIDENTES

- **Nível I:** incidente que pode ser controlado pelo próprio usuário, pelo Gestor de Informações ou pela equipe de TI e que não afeta o andamento dos trabalhos.

Exemplo: problemas com equipamentos periféricos de computadores;

- **Nível II:** incidente que impede a utilização de equipamentos ou sistemas e acaba impedindo a continuação dos trabalhos.

Exemplo: problema com o funcionamento do computador (não liga, travado, etc.) ou ainda, sistemas off-line impedindo o uso do mesmo;

- **Nível III:** incidente que impede o uso de sistemas ou equipamentos de todo o IPRESP, impedindo o desenvolvimento dos trabalhos de todos os usuários ou perda de dados de forma isolada.

Exemplo: falha na conexão com a internet ou queda de energia elétrica, ou ainda problema técnico em algum servidor de rede que controla a conexão interna;

- **Nível IV:** perda de dados parcial ou total do banco de dados.

Exemplo: queima do HD do servidor ou apagamento acidental das informações.

8. PRINCIPAIS RISCOS

RISCOS	CAUSAS	MITIGAÇÃO DO RISCO
Interrupção de energia elétrica	Fator externo: falha na rede da concessionária.	Nobreak para proteger e manter os servidores em funcionamento.
	Fator interno: falha na rede interna da sala ou prédio.	Nobreak para proteger e manter os servidores em funcionamento.



Indisponibilidade de rede	Fator externo: falha na rede da concessionária.	Acionamento imediato da empresa prestadora do serviço.
	Fator interno: falha na rede interna da sala ou prédio.	Acionamento imediato do setor de TI.
Falha humana	Acidentes ao manusear equipamentos.	Treinamento contínuo e conscientização dos riscos.
Ataques cibernéticos	Ataque virtual que comprometa o funcionamento da instituição; roubo de dados; apagamento de dados.	Antivírus; Firewall; Criptografia.
Apagamento de dados	Falha humana; Dano irreparável ao servidor.	Backup no servidor; Backup na nuvem.
Superaquecimento do servidor	Elevada temperatura do ambiente.	Instalação de ar-condicionado na sala do servidor.

9. PROCEDIMENTOS PARA BACKUP

Com o objetivo de assegurar a integridade e a disponibilidade das informações, foi estabelecida a seguinte política de cópias de segurança: diariamente, às 21:00 horas, é realizado o espelhamento completo dos arquivos do servidor principal para um servidor secundário.

Como medida adicional de proteção (*disaster recovery*), uma cópia integral dos dados é mantida em um servidor virtual em nuvem. Este procedimento visa garantir a recuperação das informações na eventualidade de uma falha simultânea dos discos rígidos locais.

Ressaltamos que é imprescindível que todos os dados de propriedade do IPRESP sejam armazenados pelos usuários exclusivamente no servidor, visto que não há rotina de backup para os computadores de mesa ou notebooks.

9.1 RESTAURAÇÃO E TESTE

A restauração de dados deve ser solicitada pelo usuário padrão ao Gestor de Informações lógicas. Este solicitará ao setor de TI a realização de acordo com os procedimentos

Avenida Emanuel Pinto, nº 1962, sala 01 - Centro, Balneário Piçarras - SC, CEP 88380-000
Tel (47) 3345-3286



específicos do mesmo. A verificação e o teste de restauração serão realizados com as ferramentas (softwares e hardwares) apropriadas e disponibilizadas pela área de TI.

10. COMUNICAÇÃO

Em caso de pane ou incidente de qualquer natureza, os usuários padrão deverão comunicar imediatamente o Gestor de Informações lógicas ou o setor de TI, através dos números de telefone disponibilizados ou através do aplicativo WhatsApp, abrindo posteriormente o processo digital para registrar a ação, conforme mapeamento em anexo.

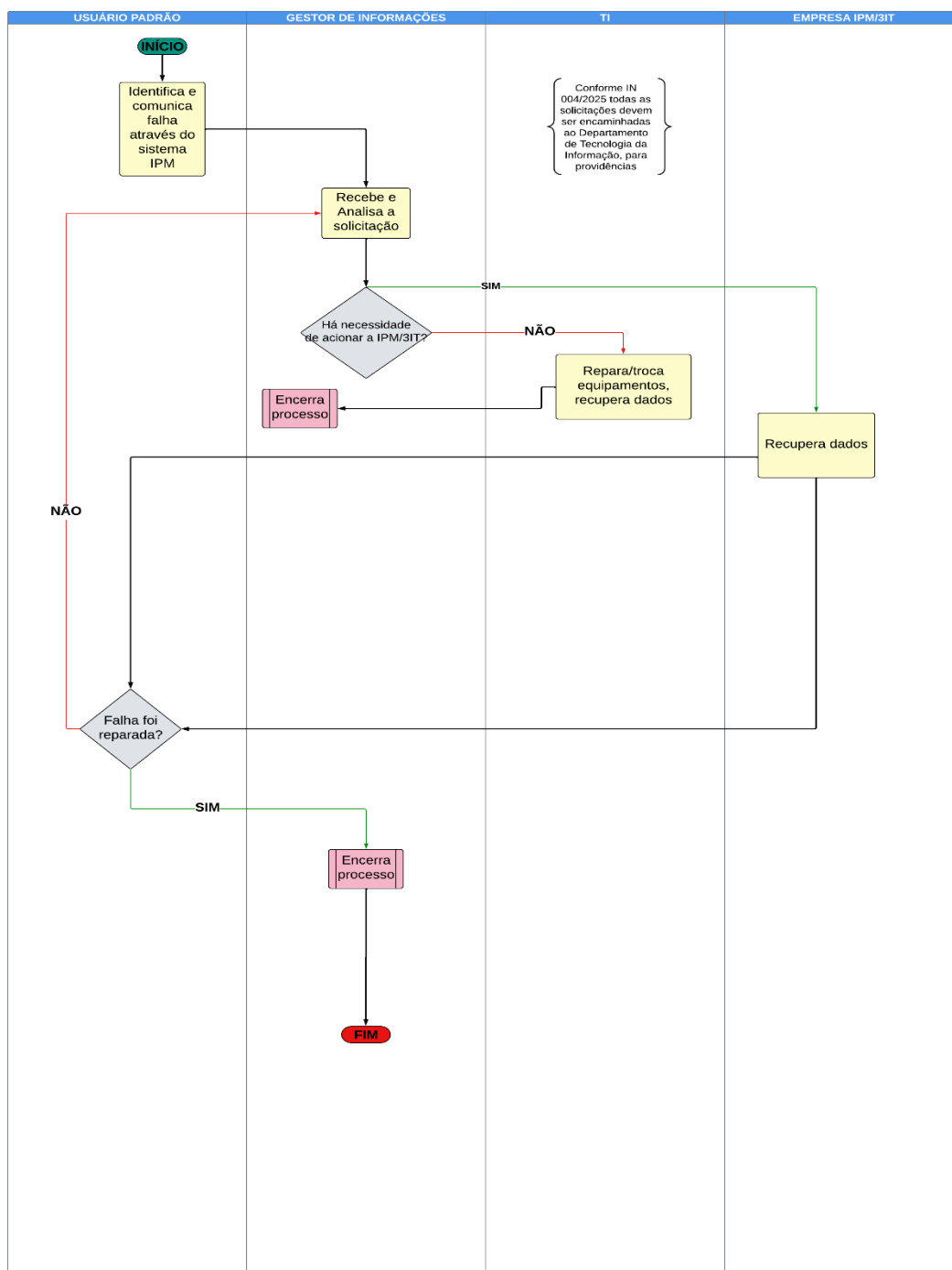
11. DETALHAMENTO DO PROCESSO DE RECUPERAÇÃO DE DADOS

ETAPA	ATIVIDADE	RESPONSÁVEL	DETALHAMENTO
1	Identificação e comunicação de falha nos sistemas.	Usuário padrão	-
2	Análise da comunicação	Gestor de Informações lógicas	Verifica se há necessidade de acionar a TI e/ou iniciar o Plano de Contingência, caso necessário.
3	Conserto ou troca de equipamentos ou recuperação de dados, de acordo com o Plano de Contingência.	TI	Disponibiliza pessoal e ferramentas para reparar, trocar equipamentos ou recuperar os dados salvos no Backup.
4	Verificar se a falha foi reparada satisfatoriamente.	Usuário padrão	Analisa se os trabalhos poderão retornar a sua rotina normal.
5	Encerramento do processo.	Gestor de informações lógicas	-



12. ANEXO

MAPEAMENTO DO PLANO DE CONTINGÊNCIA



13. REVISÃO

Este manual deverá ser revisado a qualquer momento por solicitação da Diretoria Executiva, sempre que quaisquer usuários ou o setor de TI identificar possíveis falhas ou melhorias nos processos, ou a cada dois anos.

Manual de Padronização dos Processos da Área de Tecnologia da Informação.

Aprovado por:

Rosani Cesário Pereira
Presidente do IPRESP

Silvana Dallagnol
Diretora Financeira e Administrativa

Renan Luiz de Souza
Diretor de Benefícios

Juliano Carlos da Costa
Assessor de Tecnologia da Informação
Gestor de Informações lógicas

Jéssica Prigol
Coordenadora do Pró-Gestão

Leonardo Abido
Gestor de Informações Físicas e Digitais

Caroline Braganholo
Contadora do IPRESP

Matheus Hilgert Rodrigues
Gestor de Pessoas do IPRESP

