PREVIJUNO

Manual 008
TECNOLOGIA
Da Informação

FUNDO MUNICIPAL DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DE JUAZEIRO DO NORTE/CE – PREVIJUNO

CONSELHO DELIBERATIVO

Vandir Menezes Lima
José Erivaldo Oliveira dos Santos
Hellen Karine Soares Lira
Edivan Alexandre Ferreira
Ana Cláudia Fulgêncio de Lima
Francisco Fraudiê Barbosa de Medeiros

CONSELHO FISCAL

Mário Malzoni Neto
Clênia Beane Brito de Oliveira
Janaclea Rodrigues Gomes

DIRETORIA EXECUTIVA

Jesus Rogério de Holanda
Tiago César da Silva Viana
José Ivan Silva Alves
Marcos Aurélio Gonçalves Silva

CONTROLE INTERNO
OUVIDORIA INSTITUCIONAL

Clênia Beane Brito de Oliveira

Rua do Cruzeiro, 163/167, Centro, Juazeiro do Norte, Ceará
(088) 3512 5088 | (088) 3511 4139
faleconosco@previjuno.com

SUMÁRIO

Manual - 008
Tecnologia da Informação

Histórico das Alterações		
Revisão	**Data**	**Descrição**
00	05/10/2022	Elaboração Inicial
01	07/07/2025	Revisão geral

1 RESPONSÁVEL PELO PROCESSO

A Diretoria Previdenciária de Gestão e Benefícios, por meio do Setor de Tecnologia da Informação (TI), é a responsável pela execução e gestão dos procedimentos aqui descritos.

2 REGULAMENTAÇÃO

Este manual está fundamentado nas seguintes normativas:

Lei Nº 13.709, de 14 de agosto de 2018 (Geral de Proteção de Dados);
Portaria MTP nº 1.467, de 02 de junho de 2022;
Política de Segurança da Informação – PSI, aprovada pelo Decreto nº 728/2022.

3 OBJETIVO

Estabelecer diretrizes e padronizar os procedimentos operacionais relacionados à infraestrutura, segurança, acesso e contingência no âmbito da Tecnologia da Informação do PREVIJUNO, promovendo eficiência, rastreabilidade, segurança e conformidade com os princípios legais e institucionais.

4 PROCEDIMENTOS OPERACIONAIS

4.1 Controle de Acesso Físico

O sistema **SISPREV WEB** está hospedado em ambiente de nuvem no data center da empresa **Agenda**, que assegura infraestrutura redundante e proteção física avançada.

No ambiente **local (on-premises)** do PREVIJUNO, mantêm-se os seguintes equipamentos essenciais para a operação:

Equipamento	**Função Principal**
Firewall	Protege a rede interna contra acessos indevidos, ataques cibernéticos e tráfego não autorizado.
Servidor de Dados Linux (Samba AD)	Controla o acesso a arquivos e autenticação centralizada de usuários por meio do Samba Active Directory.

Equipamento	Função Principal
Servidor Windows (Painel Administrativo)	Gerencia permissões, políticas de acesso e auditorias via Active Directory.
Computadores com Windows 7 (Sistemas Legados)	Executam sistemas antigos que requerem este sistema operacional. O acesso é remoto e restrito.

Nota: Devido à obsolescência do Windows 7, são aplicadas medidas rigorosas de isolamento de rede e monitoramento.

Backups:
Todos os dados críticos possuem backups automáticos realizados por horário, com armazenamento em dispositivos externos e ambientes seguros, garantindo recuperação eficiente em caso de incidentes.

Segurança Física:
O servidor central está fisicamente instalado no setor de TI, com acesso controlado por técnicos autorizados. A sala permanece trancada e, em caso de manutenção externa, o acesso é previamente autorizado pelo Conselho de Administração, sendo os serviços acompanhados por equipe interna.

4.1.1 Controle de Acesso aos equipamentos eletrônicos

O acesso lógico aos ativos de TI segue um modelo de **autenticação centralizada**, com base nos princípios da **Política de Segurança da Informação (PSI)**.

a) Autenticação Centralizada:
- Gerenciada via Active Directory (AD);
- Senhas obrigatoriamente complexas e com periodicidade de troca;
- Contas de usuário personalizadas e auditáveis.

b) Controle de Acesso por Camadas:
- **Firewall:** Monitora e restringe tráfego de rede;
- **Samba AD:** Controla permissões em arquivos e pastas;
- **Sistemas legados:** Acesso remoto exclusivo a usuários autorizados.

c) Acesso a Sistemas Específicos:
- **SISPREV WEB:** Acesso via login seguro em ambiente em nuvem;
- **Painel Administrativo:** Restrito à equipe de TI;
- **Sistemas Legados:** Restringido a máquinas específicas.

d) Monitoramento e Auditoria:
- Registros de acesso mantidos em logs centralizados;
- Tentativas indevidas são bloqueadas e notificadas;
- Sessões remotas criptografadas e inativas por tempo determinado são encerradas automaticamente.

O compartilhamento de arquivos segue o **princípio do menor privilégio**, com autorizações formais para acessos especiais.

4.2 Controle de Acesso Lógico

4.2.1 Solicitação de Acesso

As solicitações de criação, alteração ou exclusão de acesso à rede, internet e sistemas devem ser formalizadas via abertura de chamado no portal eletrônico <https://glpi.previjuno.com/index.php>

4.2.2 Recebimento de solicitação

1. Recebimento da solicitação pelo setor de TI;
2. Verificação da autorização;
3. Registro da solicitação no sistema de chamados;
4. Encaminhamento ao técnico responsável;
5. Verificação do perfil funcional e concessão de acesso de acordo com diretrizes da Diretoria Administrativa e Financeira;
6. Registro da execução no sistema e notificação ao solicitante.

4.3 Plano de Contingência

O plano de contingência é elaborado para garantir a **continuidade das operações críticas** e a integridade das informações em casos de falhas, incidentes de segurança ou desastres.

4.3.1 Elaboração do Plano

O setor de TI é responsável pela elaboração do plano, contemplando, no mínimo, os seguintes riscos:

- Quedas de energia elétrica;
- Indisponibilidade de internet;
- Falha humana ou operacional;
- Ataques cibernéticos;
- Falhas de hardware;
- Desastres naturais ou incêndios;
- Ameaças internas.

O plano é submetido à **apreciação e aprovação da Diretoria Executiva**, em conformidade com a PSI.

4.3.2 Execução do Plano

A execução é de responsabilidade do setor de TI, incluindo:

- Adoção imediata das medidas de contenção e recuperação;
- Ativação de backups e redundâncias necessárias;
- Comunicação com a gestão para tomada de decisão.

4.3.3 Monitoramento da Execução do Plano

1. Monitoramento periódico da execução dos backups;

2. Testes regulares de restauração de dados;

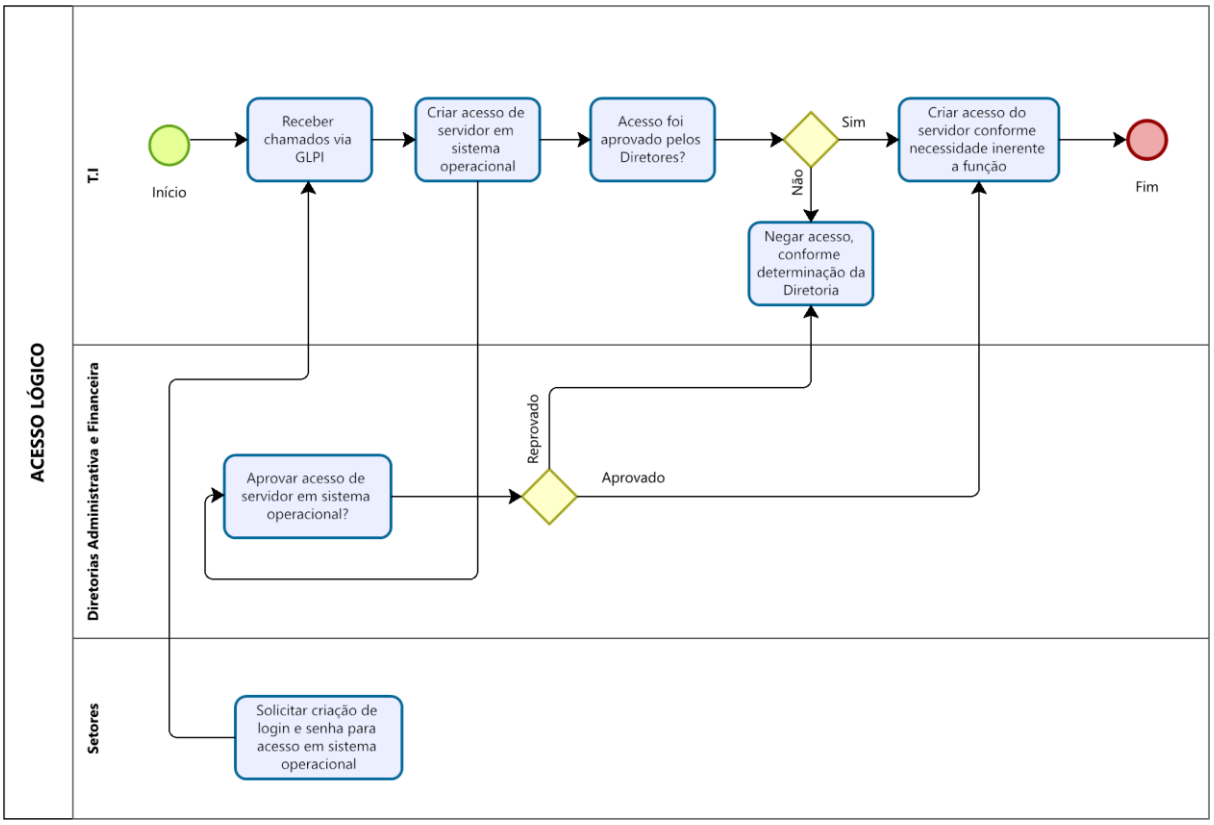
3. Acompanhamento de falhas ou incidentes com registro e análise das ocorrências;

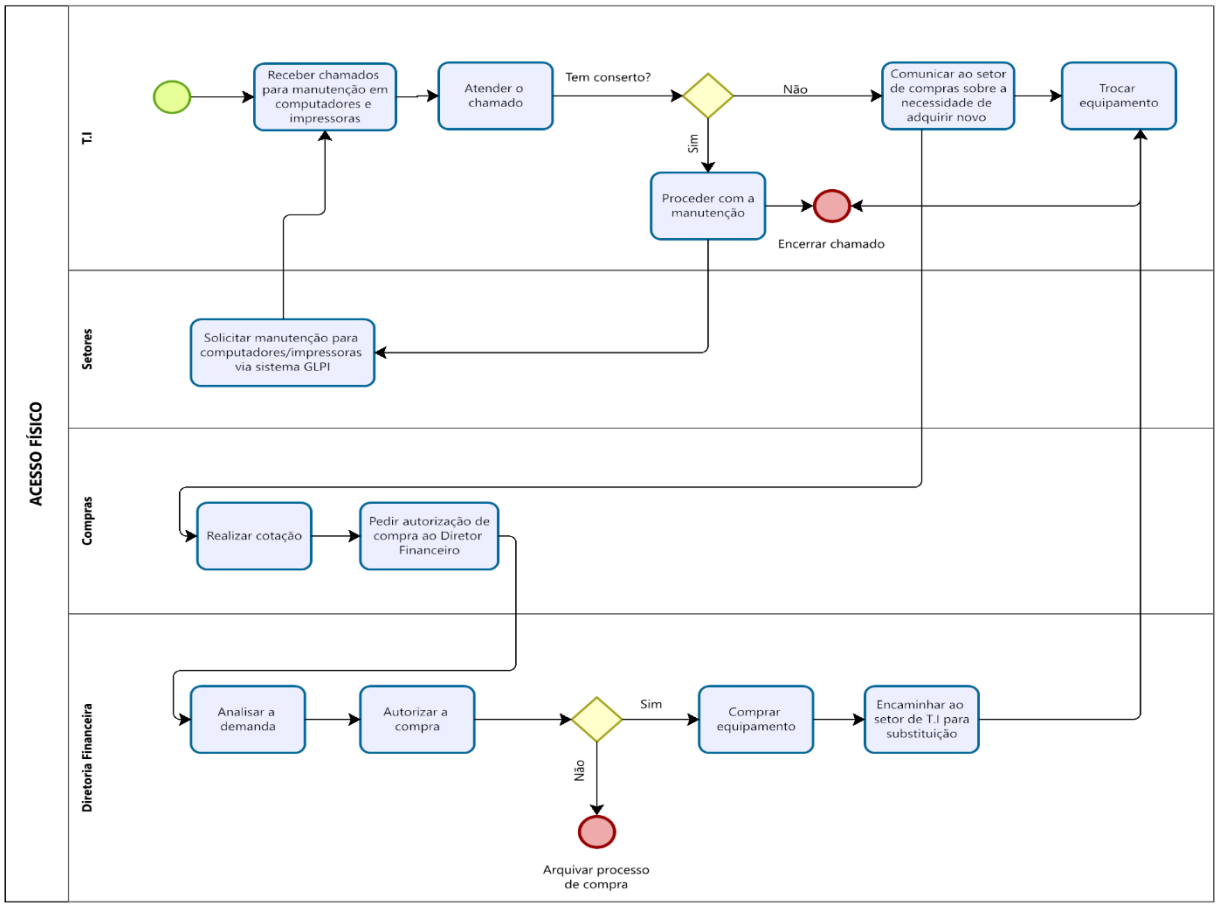
4. Adoção de ações corretivas e preventivas contínuas.

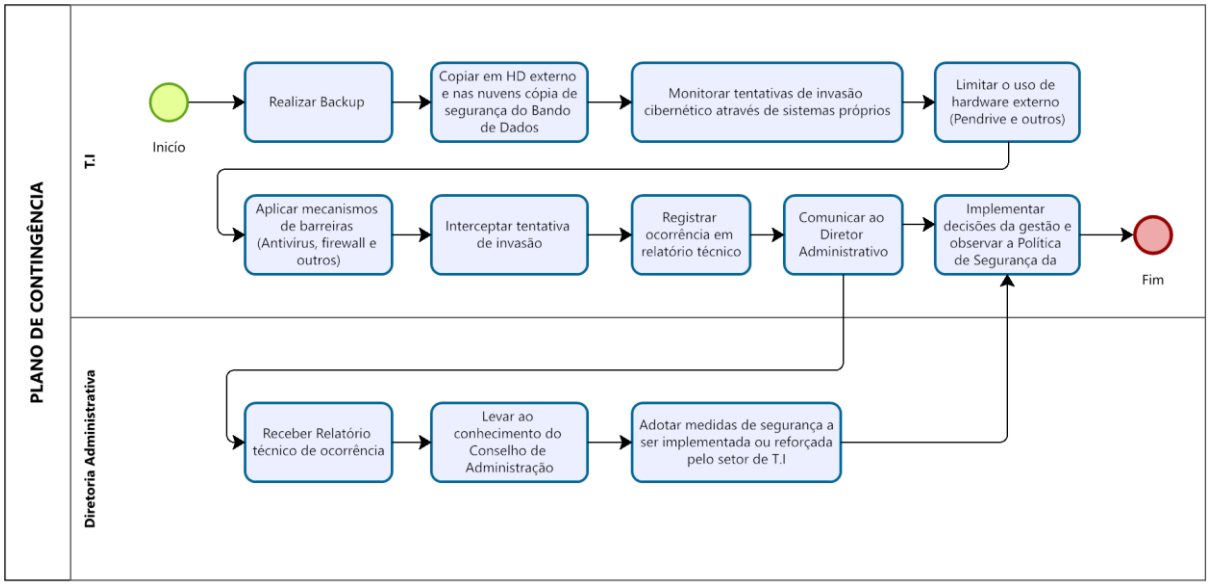
5 MAPEAMENTO DAS ATIVIDADES

A seguir, apresenta-se o mapeamento das principais atividades operacionais do Setor de Tecnologia da Informação:

Etapa	Descrição da Atividade	Responsável	Documento/Registro Gerado
1	Solicitação de acesso a sistemas ou rede	Usuário solicitante	Chamado via sistema GLPI
2	Verificação e autorização do acesso	Setor de TI	Registro no GLPI
3	Concessão de acesso conforme perfil	Técnico de TI	Registro técnico e auditoria
4	Execução de backup automatizado	Técnico de TI	Log de backup
5	Monitoramento de acessos	Técnico de TI	Logs de autenticação e acesso
6	Elaboração do plano de contingência	Coordenador de TI	Documento oficial aprovado
7	Testes de recuperação de dados	Técnico de TI	Relatório de testes


ACESSO LÓGICO
T.I
Diretorias Administrativa e Financeira
Setores
Início
Receber chamados via GLPI
Criar acesso de servidor em sistema operacional
Acesso foi aprovado pelos Diretores?
Sim
Não
Criar acesso do servidor conforme necessidade inerente a função
Fim
Negar acesso, conforme determinação da Diretoria
Aprovar acesso de servidor em sistema operacional?
Reprovado
Aprovado
Solicitar criação de login e senha para acesso em sistema operacional
Powered by bizagi Modeler


ACESSO FÍSICO
T.I
Setores
Compras
Diretoria Financeira
Receber chamados para manutenção em computadores e impressoras
Atender o chamado
Tem conserto?
Não
Sim
Comunicar ao setor de compras sobre a necessidade de adquirir novo
Trocar equipamento
Proceder com a manutenção
Encerrar chamado
Solicitar manutenção para computadores/impressoras via sistema GLPI
Realizar cotação
Pedir autorização de compra ao Diretor Financeiro
Analisar a demanda
Autorizar a compra
Sim
Não
Comprar equipamento
Encaminhar ao setor de T.I para substituição
Arquivar processo de compra


PLANO DE CONTINGÊNCIA
T.I
Diretoria Administrativa
Início
Realizar Backup
Copiar em HD externo e nas nuvens cópia de segurança do Bando de Dados
Monitorar tentativas de invasão cibernético através de sistemas próprios
Limitar o uso de hardware externo (Pendrive e outros)
Aplicar mecanismos de barreiras (Antivírus, firewall e outros)
Interceptar tentativa de invasão
Registrar ocorrência em relatório técnico
Comunicar ao Diretor Administrativo
Implementar decisões da gestão e observar a Política de Segurança da
Fim
Receber Relatório técnico de ocorrência
Levar ao conhecimento do Conselho de Administração
Adotar medidas de segurança a ser implementada ou reforçada pelo setor de T.I

REFERENCIAS

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL. Lei nº 9.717, de 27 de novembro de 1998, que dispõe sobre regras gerais para a organização e o funcionamento dos regimes próprios de previdência social dos servidores públicos da União, dos Estados, do Distrito Federal e dos Municípios, dos militares dos Estados e do Distrito Federal e dá outras providências.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018 (Geral de Proteção de Dados).

BRASIL. Ministério do Trabalho e Previdência. Secretaria de Previdência Social – SPREV. Subsecretaria dos Regimes Próprios de Previdência Social-SRPPS. Portaria nº 1.467, de 02 de junho de 2022.

JUAZEIRO DO NORTE. Lei Complementar nº 23/2007, que institui o Regime Próprio de previdência Social do Município de Juazeiro do Norte/CE e dá outras providências.

JUAZEIRO DO NORTE. Política de Segurança da Informação – PSI, aprovada pelo Decreto nº 728/2022.