Manual e Mapeamento de Segurança de Dados e Rotinas Técnicas – CAPSIRATI

Versão	1.0
Data de elaboração	01/10/2026
Referência	Manual do Pró-Gestão RPPS,
Aprovado pelo Conselho Deliberativo em	27/10/2026
Próxima revisão	Anual, ou antes, em caso de alteração normativa

Índice

1. Das disposições gerais e objetivos 03
2. Das áreas responsáveis 03
3. Das cópias de segurança (backup e restore) 04
4. Do controle de acesso lógico 05
5. Do controle de acesso físico 05
6. Da resposta a incidentes e penalidades.....06
7. Da estrutura em fluxo de resposta a incidentes (processo de urgência).....06
8. Da estrutura em fluxo de rotina de backup (processo preventivo).....07
9. Termo de responsabilidade e proteção de dados pessoais.....08

Anexo I- Fluxograma de gestão de incidentes e vazamento de dados ..... .10

Anexo II - Fluxograma de rotina de cópias de segurança 11

10. Termo de aprovação 12

MANUAL DE SEGURANÇA DE DADOS E ROTINAS TÉCNICAS – CAPSIRATI

1 DAS DISPOSIÇÕES GERAIS E OBJETIVOS

Este Manual estabelece os procedimentos normativos e práticos complementares à Política de Segurança da Informação do CAPSIRATI. Seu objetivo é fixar as regras técnicas para a manutenção de cópias de segurança (backups), controle estrito de acessos lógicos e físicos, bem como definir formalmente as áreas institucionais responsáveis por cada procedimento. Todas as diretrizes aqui expressas cumprem os ditames da Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) e da Lei de Acesso à Informação (LAI - Lei nº 12.527/2011).

2. DAS ÁREAS RESPONSÁVEIS

A governança e a execução das rotinas de segurança da informação no CAPSIRATI ficam distribuídas entre as seguintes instâncias:

Diretoria executiva: Responsável por chancelar a concessão de acessos extraordinários, autorizar a retirada física ou digital de ativos e acionar os protocolos de contingência regulamentares.

Departamento de Tecnologia da Informação (TI) do Município / Equipe Técnica Especializada Contratada: Responsável pela execução técnica operacional, o que inclui a configuração de rotinas de backup, auditoria de redes, manutenção de antivírus, gestão de credenciais lógicas e segurança dos servidores.

Agentes Públicos / Usuários Internos: Servidores, conselheiros e estagiários do CAPSIRATI respondem diretamente pela segurança diária de suas estações de trabalho, sigilo de senhas e cumprimento do bloqueio preventivo de telas.

3. DAS CÓPIAS DE SEGURANÇA (BACKUP E RESTORE)

Para salvaguardar a integridade e a disponibilidade dos dados previdenciários e sistemas informatizados do CAPSIRATI, as rotinas de backup obedecerão aos seguintes critérios:

Automatização e Janelas: Todas as cópias de segurança de bancos de dados e sistemas de gestão devem ser gerenciadas por sistemas automatizados. A execução ocorrerá obrigatoriamente fora do horário comercial (janelas de backup) para mitigar impactos na performance institucional.

Tipos de Backup:

Operacional: Voltado para a recuperação rápida e imediata de dados do cotidiano administrativo.

Contingencial: Cópias armazenadas em local geograficamente isolado (ou nuvem corporativa segura) para recuperação total em cenários de desastres físicos ou ataques cibernéticos severos.

Histórico: Retenção de dados de longo prazo para fins de cumprimento de obrigações legais de auditoria e previdência.

- **Retenção e Descarte:** Os prazos de armazenamento dos backups respeitarão o princípio da necessidade da LGPD. Dados que exaurirem sua finalidade legal deverão ser eliminados por métodos digitais seguros, impedindo qualquer possibilidade de recuperação indevida.

- **Testes de Restauração (Restore):** A equipe de TI responsável realizará testes periódicos de integridade e restauração simulada para garantir que as mídias e arquivos de backup estejam funcionais em caso de incidentes.

4. DO CONTROLE DE ACESSO LÓGICO

O acesso ao ecossistema digital do CAPSIRATI (sistemas de gestão, e-mails e arquivos em rede) é estritamente controlado de forma individual:

Identificação Nominal: Fica terminantemente proibida a criação ou utilização de contas genéricas ou compartilhadas. Cada agente público terá credenciais únicas ligadas diretamente ao seu CPF ou matrícula para fins de auditabilidade e trilha de auditoria.

Política Extensiva de Senhas: As senhas de acesso devem cumprir a complexidade mínima de 8 caracteres (letras maiúsculas, minúsculas números e caracteres especiais) e expirarão obrigatoriamente a cada 90 dias. O sistema impedirá o reaproveitamento das últimas senhas utilizadas.

Bloqueio de Tela Preventivo: É obrigação do usuário bloquear a estação de trabalho instantaneamente ao levantar-se de sua mesa através do comando *Windows + L*. Três tentativas erradas consecutivas de login resultarão no bloqueio temporário da conta para análise da TI.

Armazenamento e Periferias: Prioriza-se o uso de nuvem institucional homologada. Dispositivos removíveis particulares (como pendrives ou HDs externos) dependem de varredura prévia obrigatória do antivírus antes de qualquer conexão nos computadores da autarquia.

5. DO CONTROLE DE ACESSO FÍSICO

A proteção perimetral e física das dependências do CAPSIRATI visa impedir a manipulação indevida de hardware e documentos físicos:

Segregação de Servidores: O servidor de arquivos e equipamentos centrais de rede devem permanecer em sala ou rack fechado e isolado, dotado de refrigeração constante e proteção contra intempéries (no-breaks e

estabilizadores). O acesso físico a esse perímetro é restrito à equipe técnica autorizada.

Arquivos Físicos e Documentais: O arquivo de prontuários, processos físicos de concessão de benefícios e pastas de segurados só poderá ser acessado por servidores públicos efetivos ou cedidos lotados na autarquia. Visitantes e terceiros não possuem trânsito livre nestas áreas sem acompanhamento integral.

Retirada de Ativos: Nenhum equipamento do parque de TI (computadores, monitores, switches) ou documento institucional original poderá ser retirado do prédio do CAPSIRATI sem prévia justificativa formalizada, autorização expressa da Diretoria Executiva e preenchimento do termo de cautela correspondente.

6. DA RESPOSTA A INCIDENTES E PENALIDADES

Protocolo de Emergência: Constatada qualquer intrusão física, lógica (ataque hacker ou *ransomware*) ou perda física de dados, o servidor que identificar o fato deve isolar imediatamente o equipamento afetado da rede e comunicar a Diretoria executiva.

Penalidades: A inobservância das regras técnicas fixadas neste Manual acarretará a abertura de processo de apuração de responsabilidade administrativa, aplicando-se as penalidades previstas no Estatuto dos Servidores Públicos Municipais de Irati, além das sanções civis e criminais aplicáveis.

7. DA ESTRUTURA EM FLUXO DE RESPOSTA A INCIDENTES (PROCESSO DE URGÊNCIA)

O processo de mitigação de incidentes de segurança lógica ou vazamento de dados seguirá a sequência linear descrita nas etapas abaixo:

1. **[Início do Fluxo]** Identificação visual ou sistêmica de vírus, lentidão anormal ou mensagens de sequestro de dados (*ransomware*) pelo Usuário.
2. **[Ação de Contenção]** O Usuário desconecta imediatamente o cabo azul de rede ou desliga a rede Wi-Fi da máquina afetada (Proibido reiniciar o sistema antes deste passo).
3. **[Notificação]** O Usuário abre chamado emergencial comunicando verbalmente e por escrito a Superintendência e o Departamento de TI.
4. **[Análise Técnica]** A equipe de TI assume o controle do hardware, isola o perímetro lógico na rede corporativa e investiga a extensão do impacto.
5. **[Ponto de Decisão - LGPD]** A TI avalia se houve comprometimento de dados pessoais de ativos, aposentados ou pensionistas:
   Se SIM: O fluxo desvia para comunicação formal à ANPD e aos titulares.
   Se NÃO: O fluxo segue diretamente para a limpeza de ameaças.
6. **[Restauração]** A TI realiza a varredura completa da rede, executa o *restore* dos sistemas e emite Relatório Técnico de Incidente.
7. **[Fim do Fluxo]** Equipamento é reintegrado à produção e o processo é arquivado pela Diretoria.

8. DA ESTRUTURA EM FLUXO DE ROTINA DE BACKUP (PROCESSO PREVENTIVO)

O processo de salvaguarda de bancos de dados previdenciários e arquivos obedecerá ao ciclo contínuo de trabalho descrito abaixo:

1. **[Início do Fluxo]** Abertura automática do sistema de agendamento na "Janela de Backup" (horário noturno ou fins de semana).
2. **[Processamento]** Geração em lote das três matrizes de proteção: Backup Operacional, Contingencial e Histórico.

3. **[Ponto de Decisão - Validação]** O sistema faz a checagem binária se os arquivos gerados estão corrompidos ou válidos:
   Se HOUVER ERRO: O sistema gera log de falha e dispara alerta sms/e-mail para a equipe técnica de TI iniciar intervenção manual imediata.
   Se SUCESSO: O fluxo avança para replicação.
4. **[Replicação Criptografada]** Envio automático da cópia contingencial para o servidor em nuvem corporativa homologada da autarquia.
5. **[Fim do Fluxo]** Gravação final dos registros de sucesso no painel de controle de auditoria da TI.

9. TERMO DE RESPONSABILIDADE E PROTEÇÃO DE DADOS PESSOAIS (ANEXO INTEGRANTE)

"Eu, _____, inscrito no CPF sob nº _____, ocupante do cargo/função de _____, atuando no âmbito da Caixa de Aposentadoria e Pensão dos Servidores Municipais de Irati (CAPSIRATI), declaro ter pleno conhecimento das normas e procedimentos descritos neste Manual de Segurança da Informação e na Política de Segurança da Informação da autarquia. Comprometo-me formalmente a:

1. Reconhecer que, no exercício de minhas atribuições, terei acesso a dados pessoais, dados sensíveis e informações previdenciárias confidenciais de segurados, aposentados e pensionistas, assumindo o compromisso de utilizá-los estritamente para as finalidades legais permitidas.
2. Guardar sigilo absoluto e manter a confidencialidade de minhas credenciais lógicas de acesso (login e senha), que são de uso pessoal, nominal e intransferível, sob pena de responsabilização direta por qualquer ato praticado sob minha identificação.
3. Efetuar o bloqueio imediato da tela da minha estação de trabalho (comando Tecla Windows + L) sempre que me afastar do equipamento, ainda que por curto período, impedindo o acesso visual ou operacional de terceiros não autorizados.

4. Não utilizar, conectar ou transferir arquivos institucionais por meio de dispositivos de armazenamento removíveis particulares (pendrives ou HDs externos) sem a prévia e obrigatória varredura por software antivírus corporativo da autarquia.
5. Não instalar, baixar ou executar softwares, programas ou sistemas não licenciados ou não homologados formalmente pela equipe de TI nas estações de trabalho do CAPSIRATI.
6. Comunicar de maneira imediata à Superintendência e ao Departamento de TI qualquer indício, suspeita ou confirmação de violação das regras de segurança, incidentes cibernéticos ou potencial vazamento de dados de segurados.
7. Reconhecer que a inobservância de qualquer obrigação técnica ou de confidencialidade disposta neste termo e no manual ensejará a imediata abertura de procedimento administrativo para apuração de responsabilidades funcionais, sem prejuízo das sanções cíveis e penais previstas na legislação federal vigente.

Irati, xxx de xxxx de xxxx

_____ _____

Assinatura do Servidor/Agente Público"

Irati, xx de outubro de 2026

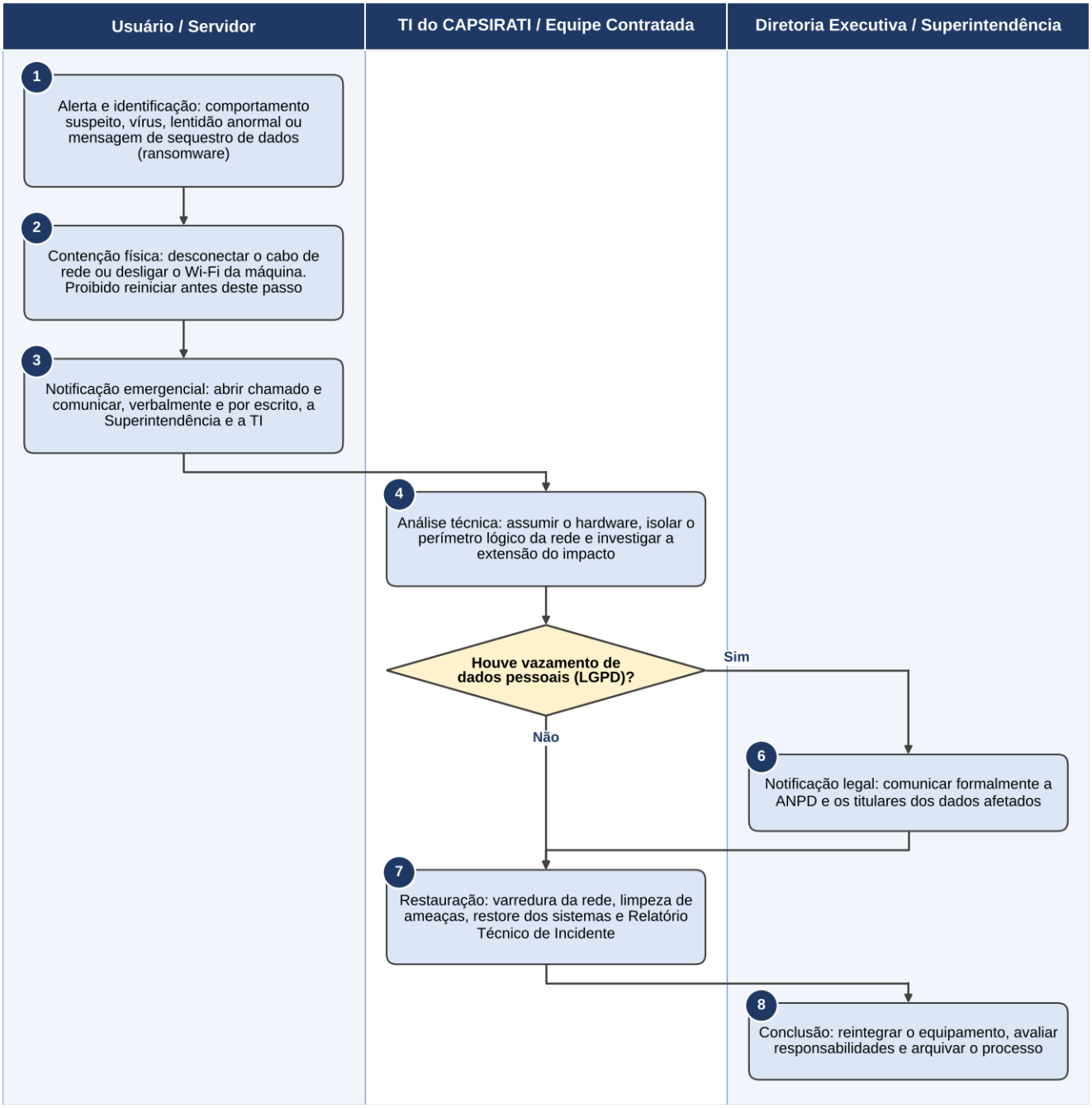
.....

Superintendente

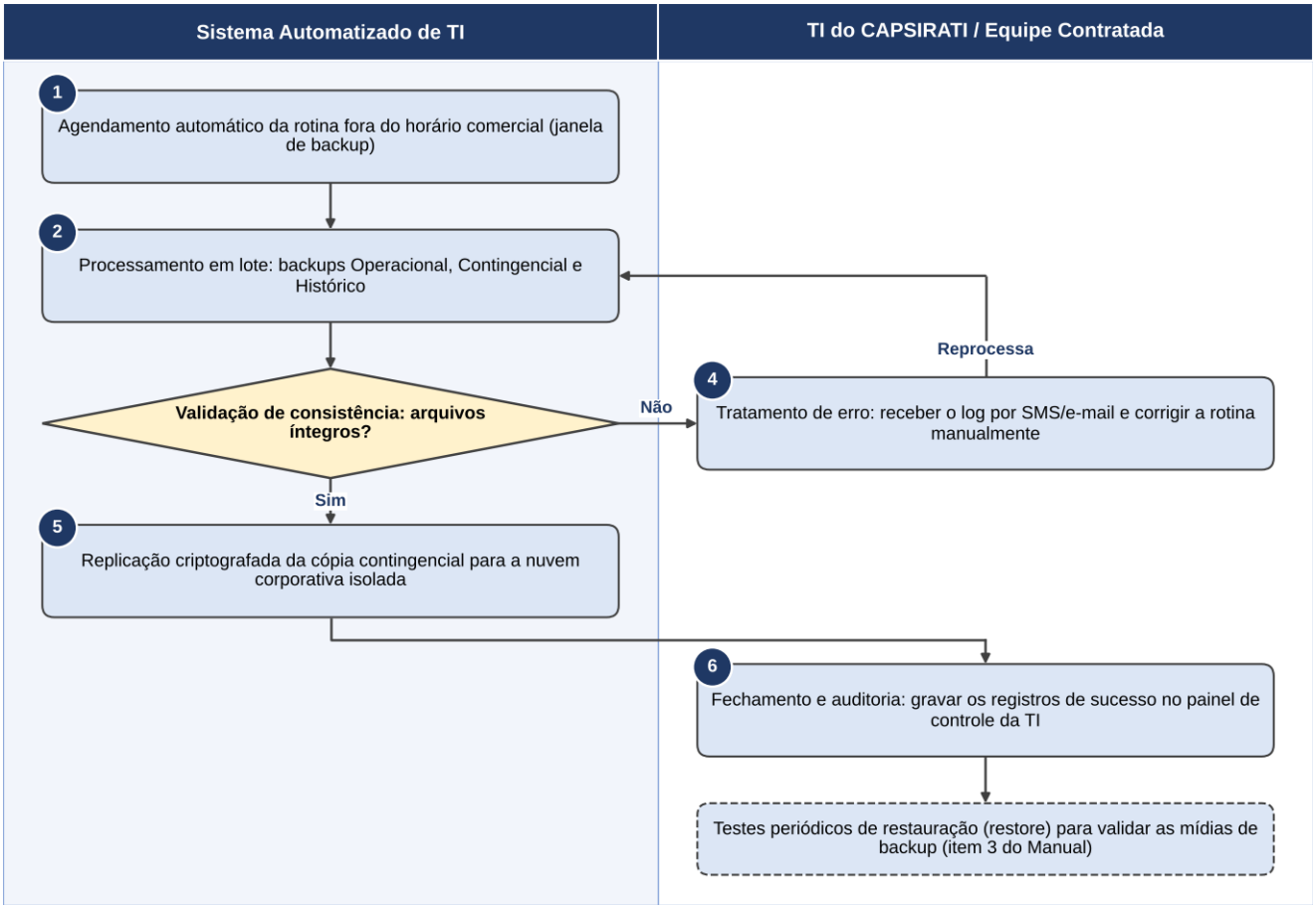
.....

Presidente do Conselho

ANEXO I – FLUXOGRAMA: GESTÃO DE INCIDENTES E VAZAMENTO DE DADOS (URGÊNCIA)



ANEXO II – FLUXOGRAMA: ROTINA DE CÓPIAS DE SEGURANÇA (BACKUP – PREVENTIVO)



10. TERMO DE APROVAÇÃO E VIGÊNCIA

As revisões são formalmente aprovadas pelo Conselho de Administração, com registro em ata e publicação da versão atualizada no site do CAPSIRATI.

Versão	Data	Alteração	Aprovação (ata)
1.0	[__/__/____]	Elaboração inicial	[nº da ata]

Irati, xxx de outubro de 2026

Rozenilda Romaniw Bárbara

_____

Superintendente
Caixa de Aposentadoria e Pensão dos Servidores Municipais de Irati (CAPSIRATI)

Cleide Aparecida da Cruz Andrade

_____

Presidente do Conselho de Administração
Caixa de Aposentadoria e Pensão dos Servidores Municipais de Irati (CAPSIRATI)