ESTADO DE SANTA CATARINA

MUNICÍPIO DE CAÇADOR

Instituto de Previdência Social dos Servidores Públicos Municipais de Caçador

CNPJ/MF Nº 04.272.905/0001-71

MANUAL DE PROCEDIMENTOS DE

CONTINGÊNCIAS DE TECNOLOGIA DA INFORMAÇÃO

Processo: Procedimentos de Contingência de Tecnologia da Informação

Unidade Gestora: Instituto de Previdência Social dos Servidores Públicos Municipais de Caçador – IPASC

Ente: Prefeitura Municipal de Caçador

Referências Normativas: ISO 22301, ISO 27001, ISO 27002, LGPD (Lei nº 13.709/2018)

2026

3ª Revisão

Rua General Osório, nº 52 - Centro - Caçador/SC - CEP 89.500-136
Fone (49) 3563-0216 | ipasc@cacador.sc.gov.br

SUMÁRIO

1. INTRODUÇÃO

O presente Manual de Procedimentos de Contingência de Tecnologia da Informação estabelece as diretrizes, processos e responsabilidades para garantir a continuidade dos serviços de TI do Instituto de Previdência Social dos Servidores Públicos Municipais de Caçador (IPASC), em conformidade com as melhores práticas internacionais de gestão de continuidade de negócios.

Este documento foi elaborado com base nas normas ISO 22301 (Gestão de Continuidade de Negócios), ISO 27001 (Sistema de Gestão de Segurança da Informação), ISO 27002 (Controles de Segurança da Informação) e na Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), considerando a natureza sensível dos dados previdenciários gerenciados pelo IPASC.

2. OBJETIVO

Definir e padronizar os procedimentos de recuperação após desastres e incidentes de TI, assegurando o restabelecimento das atividades do IPASC dentro de parâmetros mensuráveis de tempo e qualidade, minimizando impactos operacionais, financeiros e de conformidade legal.

2.1 Objetivos Específicos

- Estabelecer métricas de RTO (Recovery Time Objective) e RPO (Recovery Point Objective) para cada serviço crítico.
- Definir matriz de classificação de severidade de incidentes com SLAs correspondentes.
- Formalizar a cadeia de comunicação e escalonamento durante crises.
- Garantir conformidade com a LGPD na proteção dos dados dos segurados.
- Assegurar a realização periódica de testes de continuidade (tabletop exercises e simulações).

3. GLOSSÁRIO E TERMOS TÉCNICOS

Termo	Definição
Backup	Cópia de segurança dos dados, realizada de forma periódica, visando a restauração em caso de perda ou corrupção dos dados originais.
BIA (Business Impact Analysis)	Análise de Impacto nos Negócios: processo de identificação das funções críticas e do impacto que a interrupção causaria.
DRaaS	Disaster Recovery as a Service: solução de recuperação de desastres oferecida como serviço em nuvem.
IRP (Incident Response Plan)	Plano de Resposta a Incidentes: conjunto de procedimentos para detectar, conter e remediar incidentes de segurança.
LGPD	Lei Geral de Proteção de Dados (Lei nº 13.709/2018): legislação que regulamenta o tratamento de dados pessoais no Brasil.
RPO (Recovery Point Objective)	Ponto máximo de perda de dados aceitável, medido em tempo (ex.: RPO de 4h = aceita-se perder até 4h de dados).
RTO (Recovery Time Objective)	Tempo máximo aceitável para restaurar um serviço após uma interrupção.
Servidor de Arquivos	Computador conectado à rede com o objetivo de proporcionar armazenamento compartilhado de arquivos.
SLA (Service Level Agreement)	Acordo de Nível de Serviço: contrato que define métricas de desempenho e prazos entre contratante e prestador de serviços.

4. CLASSIFICAÇÃO DE SEVERIDADE DE INCIDENTES

A classificação dos incidentes em níveis de severidade permite priorizar ações de resposta e alocar recursos de forma adequada. Os SLAs definidos abaixo devem ser obrigatoriamente cumpridos pela empresa terceirizada, conforme cláusulas contratuais.

Nível	Tempo de Resposta	Tempo de Resolução	Exemplos
CRÍTICO (P1)	15 minutos	4 horas	Servidor de arquivos fora do ar Ataque ransomware Perda total de dados
ALTO (P2)	30 minutos	8 horas	Servidor de e-mail indisponível Queda total de internet Falha no sistema de backup
MÉDIO (P3)	1 hora	24 horas	Lentidão na rede Problema em estação de trabalho individual Falha em periféricos
BAIXO (P4)	4 horas	48 horas	Solicitações de configuração Atualizações de software Criação de usuários

5. MÉTRICAS DE RECUPERAÇÃO (RTO/RPO)

As métricas de Recovery Time Objective (RTO) e Recovery Point Objective (RPO) estabelecem os limites aceitáveis de tempo de indisponibilidade e perda de dados para cada serviço crítico do IPASC.

Serviço	RTO	RPO	Criticidade
Servidor de Arquivos	4 horas	4 horas	Crítico
Servidor de E-mails	8 horas	24 horas	Alto
Acesso à Internet	2 horas	N/A	Alto
Sistema Previdenciário	2 horas	1 hora	Crítico
Banco de Dados Oracle	4 horas	1 hora	Crítico

6. PLANO DE COMUNICAÇÃO DE CRISE

Em situações de crise, a comunicação eficaz é fundamental para coordenar a resposta e minimizar impactos. Este plano define canais, responsáveis e fluxos de escalonamento.

6.1 Canais de Comunicação

Canal primário: E-mail institucional. Canal secundário: Telefone fixo e celular corporativo. Canal de emergência (quando e-mail indisponível): Grupo de mensagens instantâneas (WhatsApp/Telegram corporativo) previamente cadastrado.

6.2 Árvore de Escalonamento

Nível	Origem	Destino	Prazo
Nível 1	Qualquer servidor	Diretoria Executiva	Imediato
Nível 2	Diretoria Executiva	Empresa Terceirizada	Até 15 min
Nível 3	Empresa Terceirizada	Gerência Técnica do Fornecedor	Até 30 min
Nível 4	Diretoria Executiva	Diretor Presidente / ANPD (se dados pessoais)	Até 2 horas

6.3 Lista de Contatos de Emergência

A Diretoria Executiva deverá manter atualizada uma lista de contatos de emergência contendo: nome, cargo, telefone fixo, celular, e-mail institucional e e-mail pessoal de todos os envolvidos na cadeia de resposta a incidentes, incluindo os contatos da empresa terceirizada. Esta lista deve ser revisada mensalmente e mantida em formato impresso e digital (armazenada em local seguro fora da rede principal).

7. RESTAURAÇÃO DO SERVIDOR DE ARQUIVOS

O servidor de arquivos é um componente crítico da infraestrutura, responsável pelo armazenamento compartilhado de documentos, bases de dados, imagens e demais arquivos institucionais. Em caso de falha, o seguinte procedimento deve ser adotado:

Atividade	Responsabilidade	Detalhamento / SLA
Detecção e notificação	Qualquer servidor / Monitoramento automático	Ao verificar indisponibilidade (ou mediante alerta do sistema de monitoramento), informar imediatamente a Diretoria Executiva via e-mail ou canal de emergência. SLA: Notificação em até 15 minutos.
Acionamento da empresa terceirizada	Diretoria Executiva	Comunicar via e-mail e telefone a empresa terceirizada, abrindo chamado formal. Ponto de Atenção: Registrar número de protocolo de atendimento.
Diagnóstico e comunicação	Empresa Terceirizada	Realizar diagnóstico e informar à Diretoria: (a) causa raiz, (b) serviços afetados, (c) previsão de restabelecimento. SLA: Retorno em até 30 minutos (P1).
Comunicação aos setores	Diretoria Executiva	Informar todos os servidores sobre serviços afetados e prazo estimado de normalização, via e-mail e canal de emergência.
Manutenção corretiva	Empresa Terceirizada	Executar reparo do equipamento. Se não for possível, a empresa deverá disponibilizar equipamento substituto em até 4 horas (conforme SLA P1).
Substituição de equipamento (se necessário)	Diretoria Executiva + Empresa Terceirizada	Se necessária substituição permanente, a empresa informa via e-mail à Diretoria, que solicita compra ao setor responsável. Enquanto isso, equipamento temporário deve ser fornecido pela contratada.
Instalação de drivers e serviços	Empresa Terceirizada	Instalar sistema operacional, drivers e serviços necessários conforme documentação de configuração (baseline).
Restauração do backup	Empresa Terceirizada	Restaurar dados a partir do último backup válido, respeitando o RPO definido (4 horas). Verificar integridade dos dados restaurados via checksum.
Configuração de acessos	Empresa Terceirizada	Reconfigurar permissões de acesso dos usuários e serviços de rede (Active Directory / LDAP).
Testes de validação	Empresa Terceirizada	Testar autenticação via rede, integridade dos arquivos e performance do servidor. Emitir relatório de testes.
Encerramento do incidente	Diretoria Executiva	Registrar no log de incidentes: causa, ações tomadas, tempo de indisponibilidade e lições aprendidas.

8. RESTAURAÇÃO DO SERVIDOR DE E-MAILS

O servidor de e-mails é responsável pelo envio, recebimento e armazenamento das comunicações eletrônicas do IPASC. Em caso de indisponibilidade, o seguinte procedimento deve ser adotado:

Atividade	Responsabilidade	Detalhamento / SLA
Detecção e notificação	Qualquer servidor / Monitoramento	Ao detectar anormalidade no e-mail, informar à Diretoria Executiva via telefone ou canal de emergência (dado que o e-mail pode estar indisponível). SLA: Notificação em até 15 minutos.
Acionamento da empresa terceirizada	Diretoria Executiva	Ligar para a empresa terceirizada abrindo chamado formal. Ponto de Atenção: Registrar número de protocolo.
Diagnóstico	Empresa Terceirizada	Identificar se o problema é local (servidor) ou no provedor de acesso. Informar diagnóstico à Diretoria. SLA: Retorno em até 30 minutos (P2).
Acompanhamento	Diretoria Executiva	Acompanhar procedimentos de reparo com atualizações a cada 2 horas.
Testes funcionais	Empresa Terceirizada	Testar envio, recebimento, acesso webmail e sincronização.
Alteração de senhas	Empresa Terceirizada + Diretoria	Se houver suspeita de comprometimento, alterar senhas de todas as contas. Comunicar usuários sobre novas credenciais via canal seguro.
Encerramento	Diretoria Executiva	Registrar incidente no log e comunicar normalização dos serviços a todos os setores.

9. RESTAURAÇÃO DOS SERVIÇOS DE INTERNET

O serviço de internet é essencial para o funcionamento dos sistemas previdenciários e comunicação institucional. Em caso de indisponibilidade, seguir o procedimento abaixo:

Atividade	Responsabilidade	Detalhamento / SLA
Detecção e notificação	Qualquer servidor / Monitoramento	Informar à Diretoria Executiva imediatamente. SLA: Notificação em até 15 minutos.
Verificação física	Diretor Adm. e Financeiro	Checar cabeamento de rede, alimentação elétrica de modem, roteadores e switches, conforme orientação da empresa terceirizada.
Diagnóstico local vs. provedor	Diretor Adm. e Financeiro + Empresa Terceirizada	Determinar se a falha é local (infraestrutura interna) ou no provedor de acesso. Realizar testes de conectividade (ping, traceroute).
Ativação do link de backup	Empresa Terceirizada	Ativar link ADSL de backup ou link dedicado de contingência. SLA: Ativação em até 30 minutos.
Contato com provedor	Diretoria Executiva	Solicitar reparo ao provedor via telefone. Ponto de Atenção: Registrar protocolo de atendimento.
Comunicação de prazo	Diretoria Executiva	Informar setores sobre prazo de normalização e serviços afetados.
Encerramento	Diretoria Executiva	Registrar no log de incidentes e retornar ao link principal quando restabelecido.

10. PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA CIBERNÉTICA

Considerando o crescimento de ameaças cibernéticas a órgãos públicos, o IPASC deve estar preparado para responder a incidentes como ransomware, phishing, vazamento de dados e ataques DDoS.

10.1 Tipos de Incidentes Cobertos

- Ransomware e malware: códigos maliciosos que criptografam ou comprometem dados.
- Phishing e engenharia social: tentativas de obter credenciais ou informações sensíveis.
- Vazamento de dados pessoais: exposição não autorizada de dados dos segurados.
- Ataques DDoS: sobrecarga intencional dos serviços de rede.
- Acesso não autorizado: invasão de sistemas ou contas de usuários.

10.2 Procedimento de Resposta

Atividade	Responsabilidade	Detalhamento / SLA
Detecção	Monitoramento / Qualquer servidor	Identificar sinais de comprometimento (comportamento anômalo, alertas de antivírus/EDR, notificações de usuários).
Isolamento	Empresa Terceirizada	Isolar imediatamente os sistemas afetados da rede para conter a propagação. SLA: Ação em até 15 minutos após detecção.
Notificação interna	Diretoria Executiva	Acionar a cadeia de escalonamento. Em caso de dados pessoais, preparar notificação à ANPD.
Investigação forense	Empresa Terceirizada	Coletar evidências, identificar vetor de ataque, escopo de comprometimento e dados afetados. Preservar logs.
Erradicação	Empresa Terceirizada	Remover a ameaça, aplicar patches, alterar credenciais comprometidas.
Recuperação	Empresa Terceirizada	Restaurar sistemas a partir de backups limpos (verificados). Monitorar comportamento pós-restauração.
Notificação ANPD/Titulares	Diretoria Executiva + Jurídico	Se houver vazamento de dados pessoais, notificar a ANPD e os titulares conforme Art. 48 da LGPD, no prazo regulamentar.
Pós-incidente	Diretoria Executiva + Empresa Terceirizada	Elaborar relatório de incidente (post-mortem), identificar lições aprendidas e implementar melhorias preventivas.

11. POLÍTICA DE BACKUP

A política de backup do IPASC segue a regra 3-2-1: três cópias dos dados, em dois tipos de mídia diferentes, sendo uma cópia offsite (fora do local físico da instituição).

11.1 Estratégia de Backup

Tipo	Frequência	Destino	Escopo
Backup Completo (Full)	Semanal (Domingo)	Servidor + Offsite	Todos os dados
Backup Incremental	Diário (Seg-Sáb)	Servidor + Nuvem	Alterações desde o último backup
Backup de Banco de Dados	A cada 4 horas	Servidor + Nuvem	Oracle / bancos críticos
Snapshot de VMs	Diário	Servidor de Backup	Máquinas virtuais completas

11.2 Política de Retenção

- Backups diários: retenção de 30 dias.
- Backups semanais: retenção de 12 semanas.
- Backups mensais: retenção de 12 meses.
- Backups anuais: retenção de 5 anos (conforme exigências legais previdenciárias).

11.3 Segurança dos Backups

- Todos os backups devem ser criptografados com AES-256, tanto em repouso quanto em trânsito.
- As chaves de criptografia devem ser armazenadas separadamente dos dados.
- Pen-drives não são considerados mídia aceitável para backup institucional.
- Acesso aos backups restrito apenas a pessoal autorizado, com registro em log de auditoria.

11.4 Testes de Restore

Testes de restauração (restore) devem ser realizados trimestralmente para validar a integridade e a capacidade de recuperação dos backups. Cada teste deve ser documentado com: data, responsável, dados restaurados, tempo de recuperação atingido e resultado (sucesso/falha). Os resultados devem ser apresentados à Diretoria Executiva.

11.5 Recursos de Backup Disponíveis

I. Servidor com principais serviços pré-instalados (Linux, Oracle).
II. Servidor com cópia das máquinas virtuais (E-mail, Web, bancos de dados).
III. Nobreaks para continuidade elétrica.
IV. Link ADSL de backup.
V. Link dedicado de backup pela empresa contratada.

12. GESTÃO DE FORNECEDORES E SLAs

A dependência de empresa terceirizada para serviços críticos de TI exige gestão rigorosa de SLAs e mecanismos de contingência para o caso de indisponibilidade do próprio fornecedor.

12.1 SLAs Contratuais Obrigatórios

- Tempo de resposta para incidentes críticos (P1): máximo de 15 minutos.
- Tempo de resolução para incidentes críticos (P1): máximo de 4 horas.
- Disponibilidade mínima dos serviços gerenciados: 99,5% mensal.
- Relatório mensal de nível de serviço com métricas de MTTR (Mean Time to Repair) e MTBF (Mean Time Between Failures).
- Cláusulas de penalidade por descumprimento de SLA.

12.2 Plano de Contingência do Fornecedor

Deve constar em contrato um exit plan (plano de saída) que inclua: transferência de conhecimento, entrega de documentação técnica completa, migração de dados e período de transição mínimo de 90 dias. Caso a empresa terceirizada esteja indisponível em situação de crise, a Diretoria Executiva deve acionar fornecedor alternativo previamente cadastrado.

13. MONITORAMENTO PROATIVO

O IPASC deve implementar solução de monitoramento proativo da infraestrutura de TI, substituindo a detecção manual de problemas por alertas automáticos.

13.1 Requisitos Mínimos

- Monitoramento de disponibilidade (uptime) de todos os servidores e serviços críticos.
- Monitoramento de performance (CPU, memória, disco, rede).
- Alertas automáticos via e-mail e SMS/mensagem instantânea.
- Dashboard centralizado com visão do estado de todos os ativos.
- Ferramentas recomendadas: Zabbix, PRTG, Nagios ou equivalente.

13.2 Diagrama de Rede

A empresa terceirizada deverá manter atualizado um diagrama topológico da rede do IPASC, incluindo: servidores, switches, roteadores, firewalls, links de internet, links de backup e segmentação de rede (VLANs). O diagrama deve ser revisado a cada alteração na infraestrutura e disponibilizado à Diretoria Executiva.

14. CONFORMIDADE COM A LGPD

O IPASC, como controlador de dados pessoais de servidores públicos municipais e seus beneficiários, deve assegurar que todos os procedimentos de contingência estejam em conformidade com a Lei Geral de Proteção de Dados.

14.1 Medidas de Proteção

- Criptografia de dados pessoais em repouso e em trânsito.
- Controle de acesso baseado em função (RBAC) para dados sensíveis.
- Logs de auditoria para todas as operações de acesso a dados pessoais.
- Avaliação de impacto (RIPD) para novos sistemas ou alterações significativas.

14.2 Notificação de Incidentes

Em caso de incidente de segurança que envolva dados pessoais, a Diretoria Executiva deverá, com apoio do encarregado de dados (DPO), notificar a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares afetados no prazo regulamentar, conforme Art. 48 da LGPD. A notificação deverá conter: descrição da natureza dos dados afetados, medidas técnicas adotadas, riscos e medidas de mitigação.

15. TESTES E SIMULAÇÕES DE CONTINUIDADE

Para garantir a efetividade deste manual, devem ser realizados testes periódicos que validem os procedimentos e identifiquem oportunidades de melhoria.

15.1 Tipos de Teste

Tipo de Teste	Frequência	Descrição
Tabletop Exercise	Semestral	Simulação teórica de cenário de crise com todos os envolvidos, discutindo ações e decisões sem intervenção real nos sistemas.
Teste de Restore	Trimestral	Restauração efetiva de dados a partir dos backups para validar integridade e medir tempo de recuperação.
Teste de Failover de Internet	Semestral	Simulação de queda do link principal para verificar ativação automática/manual do link de backup.
Simulação de Incidente Cibernético	Anual	Simulação de ataque (ex.: phishing test, simulação de ransomware) para avaliar resposta da equipe.

15.2 Documentação

Todos os testes devem ser documentados com: data, participantes, cenário testado, resultados, não-conformidades identificadas e plano de ação corretiva. Os relatórios devem ser arquivados por um período mínimo de 5 anos.

16. CONTROLE DE REVISÕES

Este manual deve ser revisado anualmente ou sempre que houver alterações significativas na infraestrutura de TI, nos processos do IPASC ou na legislação aplicável.

Versão	Data	Descrição	Responsável
1.0	2020	Versão inicial	Fernanda Fiorelli
1.1	2021	1ª revisão	Fernanda Fiorelli
1.2	2022	2ª revisão	Fernanda Fiorelli
2.0	2026	3ª revisão – reestruturação completa com inclusão de: matriz de severidade, RTO/RPO, plano de comunicação de crise, resposta a incidentes cibernéticos, política de backup 3-2-1, gestão de SLAs, monitoramento proativo, conformidade LGPD, testes de continuidade	

_____

Serviços Seccionais de Controle Interno

_____ **Antônio Carlos Castilho** Diretor Presidente	_____ **Fábio Deniz Casagrande** Diretor Administrativo e Financeiro