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

2. OBJETIVO 3
2.1 Objetivos Específicos 3
3. GLOSSÁRIO E TERMOS TÉCNICOS 3
4. CLASSIFICAÇÃO DE SEVERIDADE DE INCIDENTES 4
5. MÉTRICAS DE RECUPERAÇÃO (RTO/RPO) 4
6. PLANO DE COMUNICAÇÃO DE CRISE 5
6.1 Canais de Comunicação 5
6.2 Árvore de Escalonamento 5
6.3 Lista de Contatos de Emergência 5
7. RESTAURAÇÃO DO SERVIDOR DE ARQUIVOS 6
8. RESTAURAÇÃO DO SERVIDOR DE E-MAILS 7
9. RESTAURAÇÃO DOS SERVIÇOS DE INTERNET 8
10. PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA CIBERNÉTICA 9
10.1 Tipos de Incidentes Cobertos 9
10.2 Procedimento de Resposta 9
11. POLÍTICA DE BACKUP 10
11.1 Estratégia de Backup 10
11.2 Política de Retenção 10
11.3 Segurança dos Backups 10
11.4 Testes de Restore 10
11.5 Recursos de Backup Disponíveis 10
12. GESTÃO DE FORNECEDORES E SLAs 11
12.1 SLAs Contratuais Obrigatórios 11
12.2 Plano de Contingência do Fornecedor 11
13. MONITORAMENTO PROATIVO 12
13.1 Requisitos Mínimos 12
13.2 Diagrama de Rede 12
14.1 Medidas de Proteção 12
14.2 Notificação de Incidentes 12
15.1 Tipos de Teste 13
15.2 Documentação 13

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

Estado de Santa Catarina

Município de Caçador

Instituto de Previdência Social dos Servidores
Públicos Municipais de Caçador
CNPJ 04.272.905/0001-71

PLANO DE CONTINGÊNCIA

TECNOLOGIA DA INFORMAÇÃO

IPASC

Versão 1.4 — 4ª Revisão
Fevereiro de 2026

Alinhado às normas ISO 22301, ISO 27001 e NIST CSF
Em conformidade com a Lei Geral de Proteção de Dados (LGPD — Lei 13.709/2018)

Versão	Data	Descrição	Responsável
1.0	2019	Versão inicial	IPASC
1.1	2020	1ª Revisão	IPASC
1.2	2021	2ª Revisão	IPASC
1.3	Dez/2022	3ª Revisão	IPASC
1.4	**Fev./2026**	**Revisão completa: BIA, LGPD, ISO 22301, IRP**	**IPASC / TI**

Sumário

1. OBJETIVO 4
2. APLICAÇÃO 4
3. REFERÊNCIAS NORMATIVAS 4
4. DEFINIÇÕES 5
5. COMITÊ DE GESTÃO DE CRISE 6
5.1 Composição e Responsabilidades 6
5.2 Árvore de Comunicação de Crise 6
6. ANÁLISE DE IMPACTO NO NEGÓCIO (BIA) 7
6.1 Sistemas Críticos e Métricas de Recuperação 7
7.1 Níveis de Incidentes 7
7.2 Matriz de Prioridades (Urgência × Impacto) 8
7.3 SLAs por Prioridade 8
9. RUNBOOKS — PROCEDIMENTOS OPERACIONAIS DETALHADOS 10
9.1 Problemas com Computadores Administrativos 10
9.2 Problemas de Conexão com a Rede Interna 10
9.3 Problemas de Conexão com a Internet 10
9.4 Problemas com Falta de Energia Elétrica 11
9.5 Problemas com Equipamentos de Rede e Nobreaks 11
Fase 1 — Identificação 11
Fase 2 — Contenção 12
Fase 3 — Erradicação 12
Fase 4 — Recuperação 12
Fase 5 — Lições Aprendidas 12
9.7 Incidentes Envolvendo Dados Pessoais (LGPD) 12
9.8 Problemas com Documentos Físicos 13
9.9 Demais Incidentes 13
10.1 Estratégia de Backup (Regra 3-2-1) 13
10.2 Periodicidade e Tipos de Backup 13
10.3 Testes de Restauração 13
10.4 Disaster Recovery (DR) 13
11.1 Manutenções Preventivas 14
11.2 Equipamentos Reserva 14
11.3 Segurança Cibernética 14
12. TESTES E SIMULAÇÕES 14
13.1 Quem Deve Comunicar 15
13.2 A Quem Comunicar 15
13.3 Canais de Comunicação 15

14. GESTÃO DO CONHECIMENTO 16
16. VIGÊNCIA E REVISÕES 16

1. OBJETIVO

O presente Plano de Contingência de Tecnologia da Informação tem como objetivo assegurar a continuidade dos serviços essenciais prestados pelo Instituto de Previdência Social dos Servidores Públicos Municipais de Caçador (IPASC), minimizando os impactos decorrentes de interrupções nos serviços de TI.

Este plano estabelece procedimentos estruturados para prevenção, detecção, resposta e recuperação de incidentes, alinhados às melhores práticas internacionais (ISO 22301, ISO 27001 e NIST Cybersecurity Framework) e em conformidade com a Lei Geral de Proteção de Dados (LGPD — Lei 13.709/2018).

Os objetivos específicos são:

- Definir procedimentos operacionais detalhados (runbooks) para cada cenário de incidente;
- Estabelecer métricas de recuperação (RTO e RPO) para cada sistema crítico;
- Garantir conformidade com a LGPD na gestão de incidentes envolvendo dados pessoais;
- Promover a cultura de prevenção através de testes e simulações periódicas;
- Eliminar pontos únicos de falha na estrutura de TI e na gestão de pessoas.

2. APLICAÇÃO

Este documento se aplica a todos os servidores, gestores, prestadores de serviços terceirizados, fornecedores e demais partes interessadas envolvidas com a infraestrutura de Tecnologia da Informação do IPASC.

O plano abrange todos os ativos de TI do instituto, incluindo sistemas de informação, equipamentos computacionais, infraestrutura de rede, serviços em nuvem e dados armazenados, seja em meio físico ou digital.

3. REFERÊNCIAS NORMATIVAS

Este plano foi elaborado em conformidade com as seguintes normas e legislações:

- ISO 22301:2019 — Sistemas de Gestão de Continuidade de Negócios;
- ISO 27001:2022 — Sistemas de Gestão de Segurança da Informação;
- ISO 27002:2022 — Controles de Segurança da Informação;
- NIST Cybersecurity Framework (CSF) 2.0;
- ITIL v4 — Gestão de Serviços de TI;
- Lei 13.709/2018 — Lei Geral de Proteção de Dados (LGPD);
- Decreto 10.748/2021 — Rede Federal de Gestão de Incidentes Cibernéticos;
- ABNT NBR ISO 31000:2018 — Gestão de Riscos.

4. DEFINIÇÕES

Termo	Definição
BIA	Business Impact Analysis — Análise de Impacto no Negócio. Processo que identifica funções críticas e determina o impacto de sua interrupção.
Contingência	Situação de risco com potencial de ocorrência, inerente às atividades, serviços e equipamentos de TI.
DataCenter	Ambiente projetado para concentrar servidores, equipamentos de processamento, armazenamento de dados e ativos de rede.
DPO	Data Protection Officer — Encarregado de Proteção de Dados, conforme previsto na LGPD.
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 de Segurança.
MTPD	Maximum Tolerable Period of Disruption — Período máximo tolerável de interrupção.
RPO	Recovery Point Objective — Ponto no tempo ao qual os dados devem ser recuperados após um incidente (perda máxima de dados aceitável).
RTO	Recovery Time Objective — Tempo máximo aceitável para restauração de um serviço após uma interrupção.
Runbook	Documento operacional com procedimentos detalhados passo a passo para resposta a incidentes específicos.
SLA	Service Level Agreement — Acordo de Nível de Serviço que define tempos e qualidade esperados.
TI	Tecnologia da Informação.

5. COMITÊ DE GESTÃO DE CRISE

O Comitê de Gestão de Crise é responsável por identificar e analisar os impactos nos processos, garantir a continuidade dos serviços e priorizar processos críticos por meio do estabelecimento de procedimentos, divisão de responsabilidades e alocação de recursos.

5.1 Composição e Responsabilidades

Função	Responsabilidades
Servidor Responsável pelo TI (Titular)	Coordenar a resposta a incidentes; mitigar impactos; executar runbooks; acionar terceiros quando necessário; documentar ações tomadas.
Substituto do Responsável pelo TI	Assumir integralmente as funções do titular em sua ausência, com acesso às mesmas credenciais, documentação e contatos de emergência.
Servidores do IPASC	Informar imediatamente o responsável pelo TI sobre qualquer anomalia detectada em sistemas, equipamentos ou infraestrutura.
Diretoria Executiva	Tomada de decisão estratégica; autorizar aquisições de emergência; comunicar partes externas; acionar o DPO quando aplicável.
Encarregado de Dados (DPO)	Avaliar incidentes envolvendo dados pessoais; orientar sobre notificação à ANPD; garantir conformidade com a LGPD durante a resposta ao incidente.
Prestadores de Serviços e Fornecedores	Atender chamados conforme SLA contratual; executar manutenções emergenciais; fornecer relatórios de incidentes.

5.2 Árvore de Comunicação de Crise

A comunicação de incidentes deve seguir a seguinte cadeia, utilizando canais primários (e-mail institucional e ramal telefônico) e alternativos (grupo de mensageria institucional via aplicativo seguro):

1. O servidor que detecta o incidente comunica imediatamente o Responsável pelo TI;
2. O Responsável pelo TI avalia o nível do incidente e, se necessário, comunica a Diretoria Executiva;
3. Para incidentes Nível III ou envolvendo dados pessoais, o DPO deve ser notificado simultaneamente;
4. A Diretoria Executiva autoriza comunicações externas (ANPD, CERT.br, imprensa) quando aplicável.

6. ANÁLISE DE IMPACTO NO NEGÓCIO (BIA)

A Análise de Impacto no Negócio (Business Impact Analysis) identifica os processos críticos do IPASC, suas dependências de TI e os parâmetros de recuperação aceitáveis. Esta análise deve ser revisada anualmente ou sempre que houver mudança significativa na infraestrutura.

6.1 Sistemas Críticos e Métricas de Recuperação

Sistema/Processo	RTO	RPO	MTPD	Criticidade
Sistema de Folha de Pagamento Previdenciária	2 horas	1 hora	4 horas	CRÍTICA
Sistema de Gestão de Benefícios	2 horas	1 hora	4 horas	CRÍTICA
Servidor de Rede / Active Directory	1 hora	30 min	2 horas	CRÍTICA
E-mail Institucional	4 horas	2 horas	8 horas	ALTA
Conexão com a Internet	30 min	N/A	2 horas	ALTA
Site Institucional / Portal do Segurado	8 horas	4 horas	24 horas	MÉDIA
Impressão e Periféricos	24 horas	N/A	48 horas	BAIXA

Legenda: RTO = Recovery Time Objective (tempo máximo para restauração); RPO = Recovery Point Objective (perda máxima de dados); MTPD = Maximum Tolerable Period of Disruption (período máximo tolerável de interrupção).

7. CLASSIFICAÇÃO DE INCIDENTES

7.1 Níveis de Incidentes

Nível	Descrição	Exemplos
I	Incidente controlado pelo responsável de TI sem interrupção das atividades do servidor.	Problema com periféricos (mouse, teclado, monitor); lentidão pontual.
II	Incidente que impede o uso do equipamento ou sistema por um ou mais servidores.	Computador que não liga; falta de acesso à sistema específico; falha de autenticação.
III	Incidente que afeta toda a infraestrutura do IPASC, impedindo o trabalho de todos.	Queda de internet; falha no servidor central; ataque cibernético; queda prolongada de energia.

7.2 Matriz de Prioridades (Urgência × Impacto)

A prioridade de atendimento é definida pela relação entre a urgência do incidente e o impacto causado, conforme o framework ITIL v4:

Urgência \ Impacto	Crítico	Alto	Médio	Baixo
Muito Alta	CRÍTICA	ALTA	ALTA	MÉDIA
Alta	ALTA	ALTA	MÉDIA	MÉDIA
Média	ALTA	MÉDIA	MÉDIA	BAIXA
Baixa	MÉDIA	MÉDIA	BAIXA	BAIXA

O impacto é definido pelo número de usuários afetados (servidores, segurados) e pela criticidade do sistema. A urgência considera a natureza da atividade e se ela pode ser interrompida (reuniões de conselhos, pregões, atendimento de segurados).

7.3 SLAs por Prioridade

Prioridade	Tempo de Resposta	Tempo de Resolução	Escalação
CRÍTICA	15 minutos	Até 2 horas	TI atua imediatamente; escala Diretoria + DPO
ALTA	30 minutos	Até 4 horas	TI atua imediatamente; escala Diretoria após 2h
MÉDIA	2 horas	Até 8 horas	TI atua imediatamente; escala Diretoria após 4h
BAIXA	4 horas	Até 48 horas	TI atua imediatamente; escala Diretoria após 24h

Nota: O Responsável pelo TI é o primeiro a atuar em todos os níveis de prioridade, por ser quem detém o conhecimento técnico para diagnóstico e resolução. A coluna de escalação indica para quem o incidente deve ser comunicado quando exigir decisões estratégicas, autorizações de aquisição emergencial ou envolver questões legais (LGPD).

8. MAPA DE RISCOS

O mapa de riscos identifica os principais cenários de ameaça, suas possíveis causas, a probabilidade de ocorrência e o impacto potencial sobre as operações do IPASC.

Evento	Possíveis Causas	Probabilidade	Impacto	Nível de Risco
Interrupção de energia elétrica	Fator externo (concessionária); fator interno (curto-circuito, incêndio, infiltrações)	Média	Alto	**ALTO**
Falha na conexão de internet	Problema na operadora; rompimento de fibra; falha no roteador	Média	Alto	**ALTO**
Indisponibilidade de rede interna	Rompimento de cabeamento; falha em switch/roteador; obras internas	Baixa	Alto	**MÉDIO**
Falha de hardware	Fim de vida útil; superaquecimento; defeito de fábrica; surto elétrico	Média	Médio	**MÉDIO**
Ataque cibernético	Ransomware; phishing; DDoS; exploração de vulnerabilidades	Média	Crítico	**CRÍTICO**
Vazamento de dados pessoais	Acesso indevido; engenharia social; configuração incorreta	Baixa	Crítico	**ALTO**
Falha humana	Erro de configuração; exclusão acidental; manuseio inadequado	Média	Médio	**MÉDIO**
Desastre natural/sinistro	Inundação; vendaval; incêndio	Baixa	Crítico	**ALTO**

9. RUNBOOKS — PROCEDIMENTOS OPERACIONAIS DETALHADOS

Cada cenário de incidente possui um runbook específico com procedimentos passo a passo, responsáveis, tempos-alvo e critérios de escalação. Estes runbooks devem ser impressos e mantidos acessíveis para consulta offline.

9.1 Problemas com Computadores Administrativos

Prioridade padrão: Nível I ou II | SLA: 4 a 8 horas

a) O servidor comunica o problema ao responsável pelo TI via e-mail institucional. Se o e-mail estiver indisponível, utilizar o ramal telefônico ou canal de mensageria alternativo;

b) O responsável registra o chamado em planilha de controle de incidentes (data, hora, descrição, servidor afetado);

c) Se o problema impedir o trabalho, o responsável realiza diagnóstico in loco em até 30 minutos;

d) Tentativa de solução imediata: reinicialização, verificação de cabos, drivers e configurações;

e) Se não solucionado: disponibilizar computador reserva ao servidor e agendar assistência técnica externa;

f) Documentar a resolução e atualizar o inventário de ativos se houver substituição.

9.2 Problemas de Conexão com a Rede Interna

Prioridade padrão: Nível II ou III | SLA: 2 a 4 horas

a) Identificar se o problema é localizado (uma estação) ou generalizado (toda a rede);

b) Verificar indicações físicas: LEDs dos switches, estado dos patch panels, integridade dos cabos;

c) Testar conectividade via Ping para o gateway padrão e servidor DNS;

d) Se problema localizado: substituir cabo de rede ou porta do switch; reiniciar ponto de rede;

e) Se problema generalizado: reiniciar switch/roteador principal; verificar configurações DHCP e VLAN;

f) Caso não seja solucionado em 1 hora: acionar empresa contratada para manutenção de rede;

g) Registrar o incidente com diagnóstico e solução aplicada.

9.3 Problemas de Conexão com a Internet

Prioridade padrão: Nível III | SLA: até 2 horas

a) Verificar se o problema afeta todos os equipamentos ou apenas alguns;

b) Testar conectividade: Ping para DNS externo (8.8.8.8); verificar status do modem/roteador;

c) Verificar se há manutenção programada pela operadora;
d) Abrir chamado de suporte com a operadora, registrando número do protocolo;
e) Se a previsão de reparo exceder o RTO: avaliar ativação de link de contingência (modem 4G/5G institucional);
f) Comunicar todos os servidores sobre a indisponibilidade e previsão de retorno.

9.4 Problemas com Falta de Energia Elétrica

Prioridade padrão: Nível III | SLA: conforme duração

a) Identificar se a queda é interna (disjuntor, curto) ou externa (concessionária);
b) Se interna: desligar equipamentos de TI preventivamente e informar a Diretoria;
c) Se externa com duração estimada até 30 minutos: os nobreaks mantenham os servidores e equipamentos críticos em operação;
d) Se a interrupção ultrapassar 30 minutos: realizar shutdown controlado dos servidores de rede e sistemas, seguindo ordem de prioridade inversa (menos críticos primeiro);
e) Quando a energia for restabelecida: religar equipamentos na ordem de prioridade (servidores primeiro, depois estações);
f) Verificar integridade dos dados e sistemas após o religamento;
g) Registrar o incidente e, se necessário, solicitar laudo técnico à concessionária.

9.5 Problemas com Equipamentos de Rede e Nobreaks

Prioridade padrão: Nível I a III, conforme abrangência

a) Identificar o equipamento com falha (switch, roteador, nobreak, estabilizador);
b) Verificar se há equipamento reserva disponível para substituição imediata;
c) Realizar a substituição minimizando o tempo de indisponibilidade;
d) Se não houver reserva: acionar fornecedor para reparo ou aquisição emergencial;
e) Para nobreaks: monitorar autonomia da bateria e, se em estado crítico, realizar shutdown preventivo dos equipamentos conectados;
f) Atualizar o inventário de ativos e registrar o incidente.

9.6 Incidentes de Segurança e Ataques Cibernéticos

Prioridade padrão: Nível III | SLA: resposta imediata

Este runbook segue as fases do NIST Cybersecurity Framework:

Fase 1 — Identificação

a) Monitoramento contínuo de tráfego de rede pela empresa contratada;
b) Ao detectar anomalia, a empresa emite alerta imediato ao responsável pelo TI;
c) Classificar o tipo de ataque: ransomware, phishing, DDoS, invasão, malware;
d) Registrar o horário de detecção e os sistemas afetados.

Fase 2 — Contenção

a) Isolar imediatamente os equipamentos comprometidos da rede (desconectar cabo de rede ou desativar porta do switch);

b) Não desligar os equipamentos comprometidos para preservar evidências voláteis (memória RAM, processos em execução);

c) Alterar credenciais de acesso administrativo;

d) Comunicar imediatamente a Diretoria Executiva e o DPO.

Fase 3 — Erradicação

a) Identificar a causa raiz do incidente;

b) Remover malware, fechar vulnerabilidades exploradas;

c) Aplicar patches de segurança pendentes;

d) Realizar varredura completa com antimalware atualizado em todos os equipamentos.

Fase 4 — Recuperação

a) Restaurar sistemas a partir dos backups mais recentes, respeitando o RPO definido;

b) Validar a integridade dos dados restaurados;

c) Reconectar gradualmente os equipamentos à rede, monitorando anomalias;

d) Restabelecer o acesso dos usuários com novas credenciais.

Fase 5 — Lições Aprendidas

a) Elaborar relatório pós-incidente (post-mortem) em até 5 dias úteis;

b) Documentar timeline completa, ações tomadas e resultados;

c) Identificar melhorias nos controles de segurança;

d) Atualizar este plano com base nas lições aprendidas.

9.7 Incidentes Envolvendo Dados Pessoais (LGPD)

Prioridade padrão: CRÍTICA | Notificação ANPD: até 72 horas

a) Ao identificar possível vazamento ou acesso indevido a dados pessoais, notificar imediatamente o DPO;

b) O DPO realiza avaliação preliminar: tipos de dados afetados, número de titulares, abrangência do incidente;

c) Classificar os dados: dados pessoais comuns ou dados pessoais sensíveis (saúde, biometria);

d) Se confirmado risco ou dano relevante aos titulares: comunicar a ANPD em até 72 horas, conforme Art. 48 da LGPD;

e) Comunicar os titulares afetados, informando: a descrição do incidente, os dados afetados, as medidas adotadas e as recomendações para mitigação;

f) Preservar todas as evidências (logs, registros de acesso, capturas de tela);

g) Elaborar relatório de incidente de dados pessoais e arquivar conforme política de retenção.

9.8 Problemas com Documentos Físicos

Nos casos de extravio de documento físico, o servidor deve relatar à Diretoria Executiva por protocolo formal. Se o documento gerar efeitos em outros documentos, seus efeitos devem ser cessados imediatamente. O incidente deve ser registrado e, se envolver dados pessoais, o DPO deve ser notificado.

9.9 Demais Incidentes

Para problemas como configurações de e-mail, impressoras, acesso com login e senha e outros não previstos nos runbooks acima, deve-se observar a Política de Segurança da Informação do IPASC e seguir o fluxo padrão de comunicação ao responsável pelo TI.

10. POLÍTICA DE BACKUP E RECUPERAÇÃO

10.1 Estratégia de Backup (Regra 3-2-1)

A política de backup do IPASC segue a regra 3-2-1, reconhecida como boa prática pela indústria:

- 3 cópias dos dados (produção + 2 backups);
- 2 tipos de mídia diferentes (disco local + nuvem/fita);
- 1 cópia offsite (armazenada em local geograficamente distinto ou em nuvem).

10.2 Periodicidade e Tipos de Backup

Tipo	Frequência	Retenção	Armazenamento
Incremental	Diário (após expediente)	30 dias	Datacenter contratado + nuvem
Completo (Full)	Semanal (domingo)	90 dias	Datacenter contratado + nuvem
Completo (Arquivamento)	Mensal	5 anos	Nuvem + mídia offsite

10.3 Testes de Restauração

A integridade dos backups deve ser validada por meio de testes periódicos de restauração (restore), obedecendo ao seguinte cronograma:

- Teste de restore parcial: mensal (verificar ao menos um sistema crítico);
- Teste de restore completo: trimestral (simular recuperação total do ambiente);
- Todos os testes devem ser documentados com data, resultado, tempo de recuperação real e responsável.

10.4 Disaster Recovery (DR)

A empresa contratada para prestação de serviços de infraestrutura computacional e datacenter deve manter solução de Disaster Recovery as a Service (DRaaS), garantindo:

- Replicação contínua ou periódica dos sistemas críticos para ambiente secundário;
- Failover automatizado ou semi-automatizado com tempo de ativação compatível com o RTO definido na BIA;
- Testes de failover semestrais, documentados e com medição do tempo real de recuperação.

11. CONTROLES PREVENTIVOS

11.1 Manutenções Preventivas

- Inspeção mensal de antivírus/antimalware em todas as estações de trabalho;
- Atualização periódica de sistemas operacionais e aplicações (patch management);
- Verificação trimestral do estado físico dos equipamentos (limpeza, ventilação, temperatura);
- Teste mensal de autonomia dos nobreaks;
- Revisão semestral do cabeamento de rede estruturada.

11.2 Equipamentos Reserva

O IPASC deve manter disponíveis para substituição imediata, no mínimo:

- 1 (um) computador completo configurado e pronto para uso;
- 1 (um) nobreak compatível com as estações de trabalho;
- 1 (um) switch de rede;
- 1 (um) modem 4G/5G para contingência de internet;
- Cabos de rede, cabos de força e acessórios básicos.

11.3 Segurança Cibernética

- Firewall configurado e monitorado pela empresa contratada;
- Filtragem de conteúdo web e controle de acesso por perfil;
- Política de senhas fortes com troca periódica (mínimo a cada 90 dias);
- Autenticação multifator (MFA) para acessos administrativos e remotos;
- Conscientização dos servidores sobre phishing e engenharia social (treinamento anual);
- Monitoramento de logs de acesso e alertas automatizados para atividades suspeitas.

12. TESTES E SIMULAÇÕES

A eficácia do Plano de Contingência somente pode ser comprovada por meio de testes periódicos. O IPASC adotará o seguinte programa de testes:

Tipo de Teste	Frequência	Descrição
Tabletop Exercise	Semestral	Simulação em mesa com o comitê de crise, percorrendo cenários hipotéticos para validar ações e identificar lacunas.
Teste de Restore	Trimestral	Restauração real de dados a partir do backup para verificar integridade e medir o tempo efetivo de recuperação.
Teste de Failover (DR)	Semestral	Ativação real do ambiente de DR para validar a continuidade dos sistemas críticos.
Simulação de Phishing	Anual	Envio controlado de e-mails simulando ataques de phishing para medir a maturidade dos servidores.

Os resultados de todos os testes devem ser documentados em relatório específico, incluindo: cenário testado, participantes, cronologia, resultado (sucesso/falha), tempo real versus tempo esperado, e ações de melhoria identificadas. Os relatórios alimentam o ciclo PDCA (Plan-Do-Check-Act) para melhoria contínua deste plano.

13. COMUNICAÇÃO

13.1 Quem Deve Comunicar

Qualquer servidor que detecte problema relacionado a sistemas, equipamentos ou infraestrutura de TI deve comunicar imediatamente o responsável pelo TI.

13.2 A Quem Comunicar

Situação	Comunicar a	Prazo
Incidentes Nível I e II	Responsável pelo TI	Imediato
Incidentes Nível III	Responsável pelo TI + Diretoria Executiva	Imediato
Incidentes com dados pessoais	Responsável pelo TI + DPO + Diretoria	Imediato
Notificação à ANPD	DPO + Diretoria Executiva	Até 72 horas
Comunicação ao CERT.br	Responsável pelo TI	Até 24 horas

13.3 Canais de Comunicação

Para garantir a comunicação mesmo em cenários de indisponibilidade da infraestrutura, os seguintes canais devem ser utilizados:

- Canal primário: e-mail institucional e ramal telefônico;
- Canal secundário: grupo de mensageria institucional (aplicativo seguro como Signal ou similar);
- Canal terciário: telefone celular pessoal dos membros do Comitê de Crise (lista atualizada trimestralmente).

14. GESTÃO DO CONHECIMENTO

Para eliminar a dependência de pessoa única e garantir a continuidade do conhecimento técnico, o IPASC deve manter:

- Base de conhecimento (knowledge base) documentada e atualizada, com procedimentos de configuração, senhas administrativas (em cofre digital seguro), diagramas de rede e inventário de ativos;
- Designação formal de substituto para o responsável pelo TI, com acesso às mesmas credenciais e documentação;
- Treinamento cruzado: o substituto deve participar de pelo menos 2 manutenções por trimestre acompanhando o titular;
- Revisão semestral da documentação técnica para garantir atualidade.

15. PUBLICAÇÃO

Este documento deverá ser publicado no site institucional do IPASC e disponibilizado internamente a todos os servidores e prestadores de serviços. Uma cópia impressa deve ser mantida na sala do datacenter para consulta em situações de indisponibilidade de sistemas.

16. VIGÊNCIA E REVISÕES

Este plano tem validade de 5 (cinco) anos a partir da data de sua assinatura, com revisões obrigatórias conforme os seguintes gatilhos:

- Revisão anual ordinária;
- Mudança significativa na infraestrutura de TI;
- Após a ocorrência de incidente de Nível III;
- Após resultado insatisfatório em testes de simulação;
- Alterações na legislação aplicável (LGPD, normas técnicas).

Caçador, ____de _____de 2026.

_____
Diretor(a) Presidente do IPASC

_____
Responsável pela Tecnologia da Informação

_____
Encarregado de Proteção de Dados (DPO)

ESTADO DE SANTA CATARINA | MUNICÍPIO DE CACADOR

Instituto de Previdência Social dos Servidores Públicos Municipais de Caçador

CNPJ 04.272.905/0001-71

POLITICA DE SEGURANÇA DA INFORMAÇÃO

PSI - IPASC

Versão 2.0 | fevereiro de 2026

Elaborado por:	Setor de Informática / Diretoria Executiva
Aprovado por:	Diretoria Presidente e Diretoria Administrativa e Financeira
Data de emissão:	Fevereiro de 2026
Próxima revisão:	Fevereiro de 2026 (revisão anual obrigatória)
Classificação:	Interna (20) - Uso exclusivo dos servidores do IPASC
Substitui:	PSI IPASC versão 1.0 de 13 de marco de 2023

Sumário

1. APRESENTAÇÃO E ABRANGÊNCIA 4
2. OBJETIVO E BASE LEGAL 5
2.1 Objetivo 5
2.2 Base Legal e Normativa 5
3. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO 5
3.1 Ciclo de Gestão de Riscos 5
3.2 Matriz de Riscos 6
4. PROTEÇÃO DE DADOS PESSOAIS - LGPD 6
4.1 Encarregado de Dados (DPO) 6
4.2 Mapeamento de Dados (Data Mapping) 6
4.3 Relatório de Impacto (RIPD) 6
4.4 Resposta a Incidentes com Dados Pessoais 7
5. CLASSIFICAÇÃO DA INFORMAÇÃO 7
6. INVENTÁRIO DE INFORMACOES POR SETOR 8
6.1 Arrecadação 8
6.2 Benefícios 8
6.3 Contabilidade 8
6.4 Investimentos 9
6.5 Recursos Humanos 9
6.6 Jurídico 9
6.7 Atendimento 9
7. GESTÃO DE IDENTIDADES E ACESSOS (IAM) 10
7.1 Política de Senhas 10
7.2 Autenticação Multifator (MFA/2FA) 10
7.3 Ciclo de Vida de Acessos 11
8. TRATAMENTO DA INFORMAÇÃO 11
8.1 Transmissão e Divulgação 11
9. CONTINUIDADE DE NEGOCIOS E BACKUP 12
9.1 Objetivos de Recuperação (RTO e RPO) 12
9.2 Política de Backup 12
9.3 Plano de Resposta a Incidentes (IRP) 12
10. CONTROLES TECNICOS DE SEGURANÇA 13
10.1 Gestão de Vulnerabilidades e Patches 13
10.2 Segmentação de Rede e Controles Perimetrais 13
10.3 Monitoramento e Log Management (SIEM) 13
10.4 Segurança em Nuvem (Cloud Security) 13
10.5 Antivírus e Endpoint Protection (EDR) 13
11. POLITICA DE USO ACEITAVEL DE RECURSOS 14

11.1 Internet e Navegação Web 14
11.2 Correio Eletrônico Institucional 14
11.3 Aplicativos de Mensagens Instantâneas 14
11.4 Dispositivos Moveis e Trabalho Remoto 14
12. PROGRAMA DE CONSCIENTIZAÇÃO EM SEGURANÇA (SECURITY AWARENESS) ... 15
13. AUDITORIA, CONFORMIDADE E RESPONSABILIDADES DOS GESTORES 15
13.1 Auditorias de Acesso 15
13.2 Responsabilidades dos Gestores 15
13.3 Indicadores de Segurança (KPIs) 16
14. PENALIDADES E MATRIZ DE SEVERIDADE 16
15. DISPOSIÇOES FINAIS E REVISÃO 17

1. APRESENTAÇÃO E ABRANGÊNCIA

A Política de Segurança da Informação (PSI) do Instituto de Previdência Social dos Servidores Públicos Municipais de Caçador - IPASC estabelece os princípios, diretrizes e responsabilidades para a proteção dos ativos de informação do Instituto, em conformidade com a ISO/IEC 27001:2022, a Lei Geral de Proteção de Dados Pessoais (LGPD - Lei 13.709/2018), a Resolução CNPS e demais normativos aplicáveis aos Regimes Próprios de Previdência Social (RPPS).

Esta política se aplica a:

- Todos os servidores efetivos, comissionados, contratados, estagiários e colaboradores temporários;
- Prestadores de serviços, fornecedores e terceiros que acessem sistemas, dados ou instalações do IPASC;
- Todos os ativos de informação, sistemas, dispositivos e infraestrutura tecnológica do Instituto;
- Atividades realizadas internamente ou em regime de trabalho remoto (teletrabalho).

> Princípio Fundamental
> A informação é um ativo estratégico do IPASC. Sua proteção adequada é responsabilidade de todos, independentemente do cargo ou função, e é essencial para a continuidade dos serviços previdenciários e a confiança dos segurados.

2. OBJETIVO E BASE LEGAL

2.1 Objetivo

Garantir a disponibilidade, integridade, confidencialidade, autenticidade, legalidade, irretratabilidade e auditabilidade das informações necessárias para o cumprimento da missão institucional do IPASC, mitigando riscos cibernéticos e assegurando conformidade legal.

2.2 Base Legal e Normativa

1. ISO/IEC 27001:2022 - Sistemas de Gestão de Segurança da Informação;
2. ISO/IEC 27002:2022 - Controles de Segurança da Informação;
3. ISO/IEC 27005:2022 - Gestão de Riscos de Segurança da Informação;
4. Lei 13.709/2018 - Lei Geral de Proteção de Dados (LGPD);
5. NIST Cybersecurity Framework (CSF) 2.0;
6. Instrução Normativa MPS/SPS e resoluções do CNPS aplicáveis aos RPPS;
7. Lei 12.527/2011 - Lei de Acesso à Informação (LAI).

3. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

O IPASC adota uma abordagem estruturada e cíclica de gestão de riscos baseada na ISO/IEC 27005:2022 e no NIST Risk Management Framework (RMF), integrando identificação, analise, avaliação, tratamento e monitoramento continuo de riscos.

3.1 Ciclo de Gestão de Riscos

8. Identificação de ativos de informação e mapeamento de ameaças e vulnerabilidades;
9. Analise quantitativa e qualitativa de riscos com cálculo de probabilidade e impacto;
10. Definição de apetite ao risco e critérios de aceitação pela Diretoria Executiva;
11. Elaboração e execução de Planos de Tratamento de Risco (PTR);
12. Revisão anual obrigatória ou sempre que ocorrerem mudanças significativas na infraestrutura ou no ambiente de ameaças.

3.2 Matriz de Riscos

Catégoria de Risco	Probabilidade	Impacto	Nível de Risco
Ransomware e malware	Alta	Critico	**CRÍTICO**
Vazamento de dados pessoais (LGPD)	Media	Critico	**ALTO**
Acesso não autorizado a sistemas	Media	Alto	**ALTO**
Falha de backup e perda de dados	Baixa	Critico	**MEDIO**
Engenharia social e phishing	Alta	Alto	**ALTO**
Uso indevido de privilégios (Insider Threat)	Media	Alto	**ALTO**

4. PROTEÇÃO DE DADOS PESSOAIS - LGPD

O IPASC, na qualidade de Controlador de dados pessoais nos termos da Lei 13.709/2018, trata dados pessoais e dados pessoais sensíveis de seus segurados, servidores e dependentes. O tratamento desses dados ocorre exclusivamente com base nas hipóteses legais previstas nos Art. 7 e Art. 11 da LGPD.

4.1 Encarregado de Dados (DPO)

O IPASC deverá nomear formalmente um Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer - DPO), responsável por:

- Receber comunicações dos titulares e da Autoridade Nacional de Proteção de Dados (ANPD);
- Orientar servidores e terceiros sobre práticas de proteção de dados;
- Executar as demais atribuições previstas no Art. 41 da LGPD.

4.2 Mapeamento de Dados (Data Mapping)

O IPASC deverá manter um Registro de Atividades de Tratamento (RAT) atualizado, contemplando: finalidade, base legal, catégoria dos dados, retenção, destinatários e medidas de segurança aplicadas para cada fluxo de dados pessoais.

4.3 Relatório de Impacto (RIPD)

Para tratamentos de dados que apresentem risco elevado aos direitos dos titulares - especialmente dados sensíveis como informações medicas de perícia, dados financeiros e biométricos - o IPASC deve elaborar o Relatório de Impacto a Proteção de Dados Pessoais (RIPD) conforme Art. 38 da LGPD.

4.4 Resposta a Incidentes com Dados Pessoais

Em caso de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, o IPASC deverá comunicar a ANPD e os titulares afetados em prazo razoável, conforme Art. 48 da LGPD. O prazo recomendado pela ANPD e de até 72 horas para notificação preliminar.

Dados Pessoais Confidenciais

Todos os dados pessoais de servidores, segurados, pensionistas e dependentes são classificados como CONFIDENCIAIS (nível 40). Dados sensíveis (Art. 5, II da LGPD), como dados de saúde das pericias medicas, recebem tratamento diferenciado com controles adicionais de criptografia, acesso restrito e log de auditoria.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

E de responsabilidade do Gestor de cada área estabelecer e manter a classificação das informações produzidas e custodiadas, seguindo a tabela abaixo. O nível de classificação deve ser indicado no canto superior direito de todos os documentos e no cabeçalho de mensagens eletrônicas.

Tipo	Classificação	Nível	Descrição
Publica	10	Baixo	Informações que podem ser de conhecimento público, sem restrições de acesso.
Interna	20	Moderado	Informações de uso exclusivo dos servidores do IPASC, divulgáveis externamente apenas mediante autorização do Gestor ou exigência legal.
Restrita	30	Alto	Informações que requerem cuidados especiais. Sua divulgação indevida sujeita o IPASC a riscos consideráveis.
Confidencial	40	Critico	Informações pessoais, estratégicas e sensíveis. Sua divulgação pode causar grandes impactos financeiros, de imagem ou operacionais.

6. INVENTÁRIO DE INFORMACOES POR SETOR

6.1 Arrecadação

Processo	Informação	Destino	Classificação
Arrecadação	Ofícios de cobrança PMC	PMC / Arquivo	**20**
Arrecadação	Ofícios de retenção FPM	Banco / Arquivo	**20**
Arrecadação	Lista de servidores cedidos	Arquivo	**20**
Arrecadação	Lista de servidores licenciados	Arquivo	**20**
Arrecadação	Guias de recolhimento individual	Servidor / Arquivo	**30**

6.2 Benefícios

Processo	Informação	Destino	Classificação
Benefícios	Pedidos de simulação	Arquivo	**20**
Benefícios	Processos de aposentadoria	Arquivo	**20**
Benefícios	Processos de pensão	Arquivo	**20**
Benefícios	Pericias medicas	Arquivo	**40**
Benefícios	Pedidos de CTC	Arquivo	**20**
Benefícios	Pedidos de averbação	Arquivo	**20**
Benefícios	Pedidos de revisão	Arquivo	**20**

6.3 Contabilidade

Processo	Informação	Destino	Classificação
Contabilidade	Balancetes	Arquivo	**20**
Contabilidade	Demonstrativos	Arquivo	**20**
Contabilidade	Demonstrações contábeis	Arquivo	**20**
Contabilidade	Prestação de contas	Arquivo	**20**
Contabilidade	Conciliações bancarias	Arquivo	**30**

6.4 Investimentos

Processo	Informação	Destino	Classificação
Investimentos	Política de investimentos	Gestor / Arquivo	**10**
Investimentos	Estudo ALM	Gestor / Arquivo	**20**
Investimentos	Relatório de investimentos	Gestor / Arquivo	**10**
Investimentos	APR	Gestor / Arquivo	**20**
Investimentos	Credenciamento	Gestor / Arquivo	**20**

6.5 Recursos Humanos

Processo	Informação	Destino	Classificação
RH	Relatórios de gastos mensais	Arquivo	**20**
RH	Pastas de servidores do IPASC	Arquivo	**40**
RH	Relatórios da folha	Contabilidade	**20**
RH	Folha de pagamento inativos	Portal da Transparência	**10**
RH	Comprovante envio DIRF / RAIS	Arquivo	**30**

6.6 Jurídico

Processo	Informação	Destino	Classificação
Jurídico	Documentos de ações judiciais	Arquivo	**40**
Jurídico	Pareceres administrativos	Arquivo	**20**
Jurídico	Relatórios jurídicos	Arquivo	**20**

6.7 Atendimento

Processo	Informação	Destino	Classificação
Atendimento	Carta de margem	Destinatário / Arquivo	**30**
Atendimento	Informe de Rendimento	Destinatário / Arquivo	**30**
Atendimento	Folha de pagamento	Servidor / Arquivo	**30**
Atendimento	Declaração de viagem	Servidor / Arquivo	**30**
Atendimento	Correspondências e Ofícios	Destinatário / Arquivo	**10**

7. GESTÃO DE IDENTIDADES E ACESSOS (IAM)

O IPASC adota o modelo de controle de acesso baseado em função (Role-Base Access Control - RBAC) e o princípio do menor privilegio (Least Privilege), garantindo que cada usuário acesse apenas os recursos necessários ao desempenho de suas atribuições.

7.1 Política de Senhas

Todos os usuários do IPASC devem observar os seguintes requisitos mínimos para credenciais de acesso, em conformidade com o NIST SP 800-63B:

- Comprimento mínimo de 12 caracteres;
- Uso obrigatório de combinação de letras maiúsculas, minúsculas, números e caracteres especiais;
- Troca obrigatória a cada 90 dias e imediatamente em caso de suspeita de comprometimento;
- Proibição de reutilização das últimas 10 senhas;
- Bloqueio automático apos 5 tentativas de login fracassadas;
- Uso de gerenciador de senhas corporativo recomendado para senhas complexas.

7.2 Autenticação Multifator (MFA/2FA)

A autenticação multifator e obrigatória para:

- Acesso a sistemas de aprovação financeira e previdenciária;
- Acesso remoto (VPN) a recursos do IPASC;
- Acesso ao painel administrativo de servidores e banco de dados;
- Contas com privilégios elevados (administradores de sistema);
- Acesso a ambientes de nuvem e plataformas de backup.

São aceitos como segundo fator: aplicativos TOTP (Time-based One-Time Password), tokens de hardware ou certificados digitais ICP-Brasil.

7.3 Ciclo de Vida de Acessos

Evento	Ação Requerida
Admissão	RH comunica a Diretoria; TI cria credenciais com perfil mínimo necessário; usuário assina termo de responsabilidade.
Mudança de função	RH notifica TI; revisão e ajuste de privilégios dentro de 24 horas; revogação dos acessos anteriores incompatíveis.
Afastamento temporário	Suspensão temporária de credenciais para afastamentos superiores a 30 dias.
Exoneração / Demissão	RH notifica TI imediatamente; revogação de TODOS os acessos no mesmo dia; devolução de dispositivos e credenciais.
Revisão periódica	Auditoria semestral de todos os acessos ativos, validada pelos gestores de cada setor.

8. TRATAMENTO DA INFORMAÇÃO

O tratamento da informação abrange todo o seu ciclo de vida: criação, classificação, manuseio, armazenamento, transmissão, retenção e descarte seguro. As diretrizes abaixo se aplicam a todos os níveis de classificação.

8.1 Transmissão e Divulgação

Canal	10-Publica	20-Interna	30-Restrita	40-Confidencial
Correio físico	Sem restrições	Correspondência registrada e rastreável	Desaconselhado; somente com anuência da Diretoria, com AR	**Proibido**
E-mail corporativo (interno)	Sem restrições	Sem restrições	Utilizar com precaução	**Desaconselhado**
E-mail corporativo (externo)	Sem restrições	Com autorização do Gestor	Utilizar com precaução e criptografia	**Proibido**
E-mail pessoal	**Proibido para dados institucionais**	**Proibido**	**Proibido**	**Proibido**
Aplicativos de mensagens (WhatsApp etc.)	Somente informações já publicas	**Vedado para dados institucionais**	**Proibido**	**Proibido**

9. CONTINUIDADE DE NEGOCIOS E BACKUP

9.1 Objetivos de Recuperação (RTO e RPO)

Com base na Análise de Impacto nos Negócios (BIA - Business Impact Analysis), o IPASC define os seguintes objetivos:

Sistema / Processo	Criticidade	RTO	RPO
Sistema SIPREV (folha / benefícios)	Critica	4 horas	24 horas
Banco de dados principal	Critica	4 horas	24 horas
Sistema de e-mail corporativo	Alta	8 horas	48 horas
Documentos e arquivos administrativos	Media	24 horas	72 horas

9.2 Política de Backup

13. Backup diário automatizado dos sistemas integrados e servidores de rede, sob responsabilidade da empresa contratada;
14. Backup mensal de fechamento do Sistema Integrado, realizado após comunicação formal da Contabilidade;
15. Retenção local de copias de VMs: 15 dias no ambiente XenServer;
16. Replica diária de versionamento de arquivos na nuvem;
17. Copia mensal de VMs completas para ambiente de nuvem (Disaster Recovery);
18. Testes de restauração obrigatórios a cada 3 meses, com registro documentado dos resultados;
19. Criptografia obrigatória de todos os backups em repouso (AES-256) e em trânsito (TLS 1.2+).

9.3 Plano de Resposta a Incidentes (IRP)

O IPASC deve manter um Plano de Resposta a Incidentes (Incident Response Plan - IRP) estruturado nas seguintes fases:

20. PREPARACAO: equipe de resposta definida, ferramentas disponíveis, treinamentos realizados;
21. IDENTIFICACAO: detecção e triagem do incidente com classificação de severidade (P1 a P4);
22. CONTENCAO: isolamento do ativo comprometido para limitar propagação;
23. ERRADICACAO: remoção da causa raiz (malware, acesso indevido, vulnerabilidade);
24. RECUPERACAO: restauração dos serviços com validação de integridade;
25. LICOES APRENDIDAS: relatorio pós-incidente em até 15 dias, com acoes corretivas documentadas.

Incidentes criticos (P1/P2) devem ser comunicados a Diretoria Executiva em até 2 horas. Incidentes com dados pessoais devem seguir adicionalmente o protocolo LGPD (item 4.4).

10. CONTROLES TECNICOS DE SEGURANÇA

10.1 Gestão de Vulnerabilidades e Patches

- Varreduras de vulnerabilidades mensais em toda a infraestrutura com ferramentas especializadas;
- SLA para aplicacao de patches: Criticos em até 72h, Altos em 7 dias, Medios em 30 dias;
- Manutenção de inventario atualizado de todos os ativos de TI (ITAM - IT Asset Management);
- Sistemas sem suporte do fabricante (End of Life) devem ser substituídos ou segmentados.

10.2 Segmentação de Rede e Controles Perimetrais

- Segmentação de rede por VLANs separando: usuários internos, servidores, dispositivos IoT e DMZ;
- Firewall com regras de mínimo acesso, revisadas semestralmente;
- Sistema de Detecção e Prevenção de Intrusões (IDS/IPS) na borda da rede;
- VPN com MFA obrigatória para todos os acessos remotos;
- Filtragem de DNS para bloqueio de domínios maliciosos conhecidos.

10.3 Monitoramento e Log Management (SIEM)

- Coleta centralizada de logs de todos os sistemas críticos em solução de SIEM;
- Retenção mínima de logs: 12 meses online, 5 anos em arquivo frio;
- Alertas automáticos para comportamentos anômalos: tentativas de acesso fora do horário, volumes incomuns de download, acessos de IPs não autorizados;
- Revisão semanal dos alertas pelo responsável de TI.

10.4 Segurança em Nuvem (Cloud Security)

- Criptografia de dados em repouso (AES-256) e em trânsito (TLS 1.2 ou superior);
- Gestão de chaves criptográficas com rotação periódica;
- Avaliação anual do modelo de responsabilidade compartilhada com o provedor de nuvem;
- Controle de acesso ao ambiente de nuvem com MFA e princípio do menor privilegio.

10.5 Antivírus e Endpoint Protection (EDR)

- Solução de proteção de endpoints (EDR - Endpoint Detection and Response) instalada em todas as estacoes;
- Atualização automática de assinaturas em tempo real;
- Proibido desabilitar a proteção de endpoint sob qualquer circunstância;
- Varredura completa semanal agendada em todos os dispositivos.

11. POLITICA DE USO ACEITAVEL DE RECURSOS

11.1 Internet e Navegação Web

O acesso à Internet e autorizado exclusivamente para atividades relacionadas as funções profissionais. E terminantemente proibido acessar:

- Sites de conteúdo pornográfico, violento ou que promovam atividades ilegais;
- Plataformas de streaming de mídia não relacionadas ao trabalho;
- Serviços de armazenamento em nuvem pessoais (Google Drive pessoal, Dropbox pessoal) para dados institucionais;
- Sites identificados como maliciosos pelo sistema de filtragem de DNS;
- Realizar downloads de softwares sem autorização expressa do responsável de TI.

11.2 Correio Eletrônico Institucional

O e-mail corporativo e de uso pessoal e intransferível. E proibido o envio de mensagens com conteúdo difamatório, ofensivo, pornográfico, correntes, spam ou qualquer conteúdo que comprometa a imagem do Instituto. O usuário e o único responsável pelo conteúdo enviado pelo seu endereço.

E vedado o uso de contas de e-mail pessoais (Gmail, Hotmail etc.) para tratativas institucionais ou transmissão de dados do IPASC.

11.3 Aplicativos de Mensagens Instantâneas

Aplicativos de mensagens pessoais (WhatsApp, Telegram etc.) não devem ser utilizados para transmissão de informações institucionais de nível Interno (20) ou superior. O IPASC deve disponibilizar canal de comunicação corporativo adequado para comunicações internas.

11.4 Dispositivos Moveis e Trabalho Remoto

- Dispositivos de propriedade do IPASC não podem ter sua configuração alterada pelo usuário sem autorização de TI;
- Em caso de furto ou perda, registrar boletim de ocorrência e comunicar a Diretoria Executiva e ao responsável de TI imediatamente para bloqueio remoto;
- Trabalho remoto somente e permitido através de VPN corporativa com MFA ativo;
- E proibido conectar dispositivos do IPASC a redes Wi-Fi públicas sem o uso de VPN.

12. PROGRAMA DE CONSCIENTIZAÇÃO EM SEGURANÇA (SECURITY AWARENESS)

A assinatura desta política e condicionada a participação no programa de conscientização. O treinamento em segurança da informação e obrigatório, periódico e documentado para todos os colaboradores.

Atividade	Descrição	Periodicidade
Treinamento obrigatório	Capacitação em PSI, LGPD, engenharia social e boas práticas de senha.	Anual + onboarding
Simulação de phishing	Campanha controlada para medir e reduzir a suscetibilidade dos servidores a ataques de engenharia social.	Trimestral
Boletins de segurança	Comunicados sobre ameaças emergentes, novas políticas e lembretes de boas práticas.	Mensal
Treinamento avançado (TI)	Capacitação técnica em resposta a incidentes, hardening e análise de logs para equipe de TI.	Semestral

13. AUDITORIA, CONFORMIDADE E RESPONSABILIDADES DOS GESTORES

13.1 Auditorias de Acesso

O responsável pela Informática realizara auditorias periódicas dos acessos aos sistemas, verificando conformidade com os perfis atribuídos, histórico de acesso, alterações de privilégios e anomalias. As auditorias devem ser documentadas e os relatórios encaminhados a Diretoria Executiva.

13.2 Responsabilidades dos Gestores

- Definir e manter atualizados os perfis de acesso dos servidores de sua área;
- Validar semestralmente a lista de acessos ativos dos subordinados;
- Notificar imediatamente o setor de TI sobre mudanças de função ou desligamento de servidores;
- Assegurar que a política de mesa limpa seja observada em sua área;
- Relatar incidentes ou suspeitas de violação de segurança sem demora.

13.3 Indicadores de Segurança (KPIs)

O IPASC devera monitorar e reportar anualmente os seguintes indicadores:

- Número de incidentes de segurança registrados e tempo médio de resolução (MTTR);
- Percentual de servidores com treinamento de conscientização concluído;
- Percentual de ativos com patches críticos aplicados no prazo;
- Resultados das simulações de phishing (taxa de clique e notificação);
- Resultados dos testes de restauração de backup.

14. PENALIDADES E MATRIZ DE SEVERIDADE

O não cumprimento desta Política de Segurança da Informação constitui falta grave. As penalidades serão aplicadas de forma proporcional a gravidade da violação, conforme a matriz abaixo:

Nível	Exemplos de Violação	Penalidades Aplicáveis
BAIXO	Não bloquear estação ao se ausentar; deixar documentos na impressora.	Advertência verbal; novo treinamento obrigatório.
MEDIO	Compartilhar senha; instalar software não autorizado; uso de e-mail pessoal para dados institucionais.	Advertência formal escrita; suspensão de privilégios de acesso; abertura de processo administrativo.
ALTO	Acesso não autorizado a dados de nível Restrito ou Confidencial; violação de LGPD.	Processo administrativo disciplinar; suspensão; possível rescisão contratual; comunicação ao Ministério Público.
CRÍTICO	Vazamento intencional de dados; sabotagem de sistemas; uso de malware ou ação criminosa.	Exoneração / Rescisão imediata; responsabilidade civil e criminal; registro em Boletim de Ocorrência.

15. DISPOSIÇOES FINAIS E REVISÃO

26. Esta política entra em vigor na data de sua assinatura, revogando a versão anterior de 13/03/2023;
27. A revisão desta política e obrigatória anualmente ou sempre que ocorrer: incidente critico de segurança, mudança legislativa relevante, alteração significativa na infraestrutura tecnológica ou reorganização administrativa;
28. Todos os colaboradores devem assinar o Termo de Responsabilidade e Ciência da PSI como condição para o exercício de suas funções. Nenhum servidor poderá ser admitido sem tal assinatura;
29. O Encarregado de Dados (DPO) e o responsavel de TI sao corresponsáveis pela gestao e atualizacao desta politica;
30. Casos omissos serão analisados pela Diretoria Executiva com suporte jurídico e técnico, podendo resultar em aditivos ou normativas complementares.

Caçador (SC), Fevereiro de 2026

Diretor Presidente do IPASC	Diretor Administrativo e Financeiro do IPASC

Encarregado de Dados (DPO)
Nome / Matricula