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

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)