ANEXO F

PLANO DE CONTINGÊNCIA E CONTINUIDADE DE TECNOLOGIA DA INFORMAÇÃO DO INSTITUTO DE PREVIDÊNCIA DO ESTADO DE RORAIMA – IPER

Elaborado pela Gerência de Tecnologia da Informação – GTI

1. OBJETIVO

O Plano de Contingência e Continuidade de TI do IPER tem como finalidade garantir a continuidade dos serviços essenciais de tecnologia da informação em situações de incidentes, falhas, interrupções operacionais ou desastres, reduzindo impactos sobre atividades previdenciárias e protegendo dados, sistemas e documentos institucionais.

Este documento atende às diretrizes:

- ISO 22301 – Sistema de Gestão de Continuidade de Negócios;
- ISO 27001/27002;
- LGPD (Lei nº 13.709/2018);
- Pró-Gestão RPPS – Nível II;
- Portarias IPER nº 188, 189 e 190/2024.

2. ABRANGÊNCIA

O plano aplica-se a:

- Sistemas críticos (SISPREV, SEI, e-mail, Servidor de Rede, servidores);
- Infraestrutura de rede e conectividade;
- Equipamentos essenciais;
- Bases de dados;
- Usuários internos e externos;
- Prestadores de serviços;
- Ambientes físicos críticos (CPD, racks, salas técnicas).

3. PRINCÍPIOS DO PLANO DE CONTINGÊNCIA

I – Garantir a continuidade dos serviços essenciais de TI.

II – Reduzir o tempo de indisponibilidade.

III – Proteger dados e ativos críticos.

IV – Minimizar prejuízos administrativos, legais e reputacionais.

V – Estabelecer uma resposta estruturada a incidentes.

4. RISCOS E IMPACTOS

Os principais riscos mapeados incluem:

4.1. Riscos Tecnológicos

- Ataques cibernéticos (phishing, ransomware, DDoS)
- Falha de servidor
- Falhas de software crítico
- Perda de integridade de dados

4.2. Riscos de Infraestrutura

- Rompimento de fibra óptica
- Oscilações de energia
- Incêndio em instalações
- Falhas de refrigeração

4.3. Riscos Humanos

- Erro operacional
- Acesso indevido
- Uso inadequado de senhas

4.4. Riscos Naturais

- Inundação
- Tempestades
- Desastres diversos

4.5. Impactos Possíveis

- Interrupção de serviços previdenciários
- Perda de prazos legais
- Vazamento de dados pessoais
- Sanções administrativas ou legais
- Prejuízo financeiro

5. PARÂMETROS DE CONTINUIDADE (RTO / RPO)

Os seguintes parâmetros são adotados pelo IPER:

5.1. RTO – Recovery Time Objective (Tempo máximo de retorno)

- Sistemas críticos (SISPREV, SEI, e-mail): **até 24 horas**
- Sistemas de suporte administrativo: **até 48 horas**

5.2. RPO – Recovery Point Objective (Ponto de recuperação de dados)

- Bases críticas: **1 hora**
- Demais bases: **24 horas**

6. NÍVEIS DE INCIDENTES

Nível I – Baixo Impacto

- Problemas isolados sem interrupção geral
- Sem risco de perda de dados

Nível II – Médio Impacto

- Interrupções parciais
- Risco moderado aos dados
- Necessidade de ação rápida da GTI

Nível III – Alto Impacto

- Indisponibilidade generalizada
- Ataque cibernético ou falha grave
- Acionamento total do plano de contingência
- Possível comunicação à ANPD (LGPD, art. 48)

7. PROTOCOLO DE RESPOSTA A INCIDENTES

7.1. Etapas de Resposta

1. **Detecção**
   Identificação do incidente pelo usuário ou GTI.
2. **Registro**
   Abertura de ocorrência via SEI ou canal emergencial.
3. **Classificação**
   Identificação do nível (I, II ou III).
4. **Contenção**
   Isolamento do incidente para evitar propagação.
5. **Erradicação**
   Correção da causa raiz.
6. **Recuperação**
   Restauração dos serviços e sistemas.
7. **Comunicação**
   - Chefias
   - Diretoria
   - Usuários afetados
   - ANPD (se envolver dados pessoais)
   - Prestadores responsáveis

7.2. Comunicação Emergencial

Canais:

- E-mail institucional
- Telefone da GTI
- Canal de contingência (Spark, WhatsApp)
- Registro no SEI

8. PLANO DE AÇÃO POR TIPO DE INCIDENTE

8.1. Interrupção de Energia

Ações:

- Acionamento de nobreaks
- Acompanhamento do restabelecimento
- Verificação de integridade dos servidores

8.2. Ataque Cibernético

Ações:

- Isolamento imediato da rede afetada
- Bloqueio de tráfego suspeito no firewall
- Troca de senhas críticas
- Acionamento da empresa de suporte, se necessário
- Comunicação à ANPD se houver risco a titulares

8.3. Indisponibilidade da Internet

Ações:

- Acionar redundância de link
- Comunicar operadora
- Ativar plano *offline*

8.4. Falha em Servidor Crítico

Ações:

- Recuperação via backup
- Restauração da última versão íntegra conforme RPO

9. PLANO OFFLINE (OPERAÇÃO MANUAL)

Em caso de falha total de sistemas:

I – Atendimento previdenciário será registrado manualmente.

II – Documentos serão produzidos em formulários impressos.

III – A equipe deve manter:

- formulários manuais padronizados,
- carimbos,
- checklists emergenciais.

IV – Assim que os sistemas forem restabelecidos, a equipe deve:

- digitalizar documentos
- registrar manualmente os atendimentos
- normalizar os fluxos no SEI / SISPREV

10. BACKUP E RESTAURAÇÃO

10.1. Rotina de Backup

- Backups diários automáticos
- Retenção mínima: **30 dias**
- Réplicas off-site em ambiente seguro
- Proteção por criptografia

10.2. Testes de Restauração

- Realizados **mensalmente**
- Relatórios registrados no SEI

10.3. Responsabilidade

GTI é responsável pela integridade e execução do ciclo de backup/restauração.

11. ATIVAÇÃO DO PLANO

O plano será ativado quando:

- houver incidente de nível III
- houver indisponibilidade superior a 2 horas
- a diretoria solicitar acionamento
- houver determinação da Presidência

A GTI se tornará o núcleo operacional de resposta.

12. EQUIPE DE CONTINGÊNCIA (Núcleo de Continuidade)

Composição:

- Gerente de TI (coordenador do plano)
- Técnico de informática
- Técnico de infraestrutura
- Suporte de sistemas
- Representantes das diretorias
- Prestador terceirizado responsável

13. DOCUMENTAÇÃO DE EVIDÊNCIAS

Todos os incidentes devem ser registrados no SEI com:

- Relatório de ocorrência
- Cronologia dos fatos
- Ações executadas
- Evidências técnicas (logs, prints, arquivos)
- Parecer técnico da GTI
- Plano de prevenção futura

14. TREINAMENTOS E TESTES DO PLANO

I – Testes de contingência devem ocorrer **semestralmente**.

II – Servidores devem ser treinados anualmente.

III – Simulados práticos devem ocorrer com:

- falha de rede
- ataque cibernético
- operação offline
- restauração completa

15. RELATÓRIO ANUAL DE CONTINUIDADE

A GTI elaborará relatório contendo:

- Incidentes ocorridos no ano
- Ações e correções
- Indicadores de disponibilidade

- Recomendações de melhoria
- Avaliação da maturidade

16. ATUALIZAÇÃO DO PLANO

O plano será revisado:

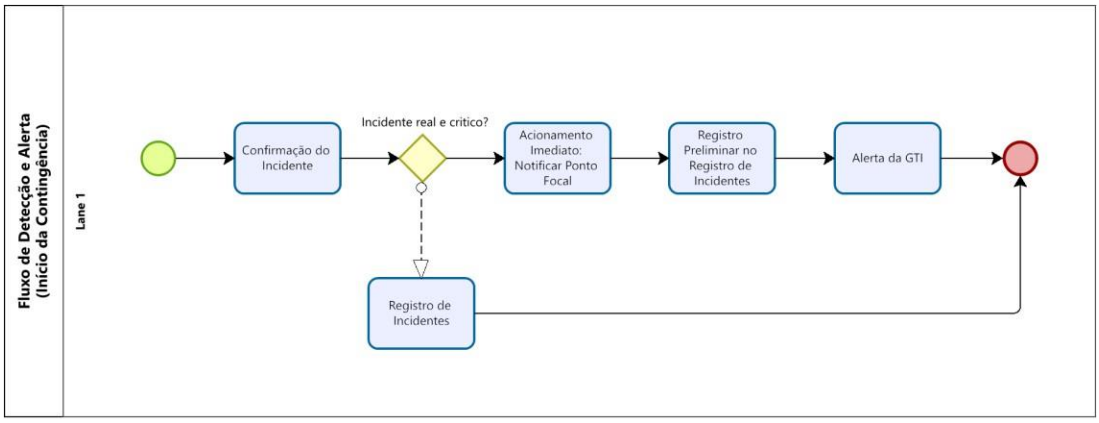
- A cada **2 anos**, ou quando houver alterações significativas na infraestrutura, sistemas ou legislação.

17. VIGÊNCIA

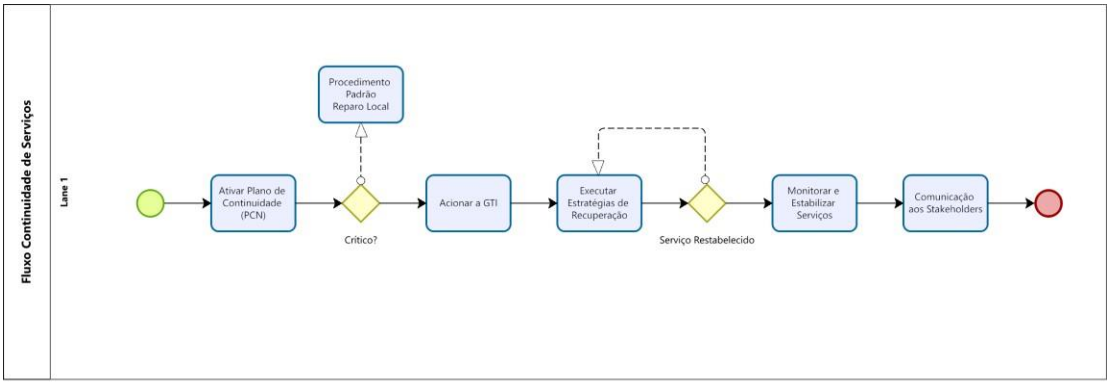
Este Plano de Contingência entra em vigor na data de sua aprovação e integra o conjunto de documentos oficiais de governança do IPER.

18. ANEXOS - FLUXOS

18.1 PLANO DE AÇÃO POR TIPO DE INCIDENTE



18.2 FLUXO DE CONTINUIDADE DE SERVIÇOS



SEÇÃO – INDICADORES GERAIS DE SEGURANÇA DA INFORMAÇÃO

1. Finalidade

Os indicadores gerais visam medir a eficácia da Política de Segurança da Informação, da gestão de riscos, do Plano de Contingência, da cultura organizacional e da proteção de dados no IPER.

2. Indicadores Estratégicos

2.1. Taxa de Incidentes de Segurança da Informação (TISI)

Descrição: Mede a quantidade de incidentes registrados em determinado período.

Fórmula:
TISI = (Incidentes registrados no período / total de usuários ativos) × 100

Meta: ≤ 2% ao mês **Periodicidade:** Mensal **Responsável:** GTI
Registro: SEI – "Indicadores – Segurança da Informação".

2.2. Tempo Médio de Resposta a Incidentes (TMRI)

Descrição: Tempo entre a detecção e o início da contenção do incidente.

Fórmula:
TMRI = Soma dos tempos de resposta / total de incidentes

Meta: ≤ 2 horas **Periodicidade:** Mensal **Responsável:** GTI
Origem: Registros de incidente (Anexo F – item 13)

2.3. Tempo Médio de Recuperação (MTTR – Mean Time to Recover) Descrição: Tempo médio para restaurar serviços após falha.

Fórmula:
MTTR = Soma dos tempos de recuperação / número total de incidentes **Meta:** Dentro do RTO previsto no Plano de Contingência **Periodicidade:** Mensal
Responsável: GTI
Origem: Plano de Contingência – item 5 (RTO/RPO)

2.4. Índice de Disponibilidade dos Sistemas Críticos

Descrição: Mede o tempo que os sistemas essenciais (SISPREV) ficam disponíveis.

Fórmula:
Disponibilidade (%) = (Tempo total disponível / tempo total do período) × 100

Meta: ≥ 99%
Periodicidade: Mensal
Responsável: GTI / Operadoras / Fornecedores

3. Indicadores de Conformidade e Governança

3.1. Taxa de Adesão aos Termos Obrigatórios (TATO)

Abrange: Termos dos Anexos C, D, E e G.
Fórmula:
TATO = (Total de usuários com termos assinados / total de usuários obrigados)
× 100

Meta: 90% **Periodicidade:** Trimestral **Responsável:** RH + GTI

3.2. Percentual de Usuários com Acessos Validados na Auditoria Semestral

Fórmula:
% = (Usuários validados pelas gerências / total de usuários ativos) × 100

Meta: 100% **Periodicidade:** Semestral **Responsável:** GTI
Origem: Item 2.4.3 da PSI (auditoria semestral).

3.3. Índice de Conformidade LGPD (IC-LGPD)

Descrição: Avalia conformidade com medidas de privacidade e proteção de dados.

Parâmetros:

Existência de consentimento Tratamento mínimo necessário Controle de acesso
Medidas de segurança aplicadas

Ausência de vazamentos

Fórmula:
IC-LGPD = (Itens conformes / total de itens avaliados) × 100

Meta: ≥ 95%

Responsável: GTI / Consultoria Jurídica
Periodicidade: Semestral

4. Indicadores de Cultura e Treinamento

4.1. Participação no Treinamento Anual Obrigatório (PTAO)

Fórmula:
PTAO = (Participantes / total de usuários obrigados) × 100

Meta: 100% **Periodicidade:** Anual **Responsável:** GTI **Origem:** Item 3.4.7 da PSI.

4.2. Índice de Engajamento em Campanhas de Segurança (IECS) Descrição: Mede acessos, cliques, visualizações ou respostas às campanhas.

Fórmula:
IECS = (Usuários que interagiram / total de usuários alcançados) × 100

Meta: ≥ 70%
Periodicidade: Trimestral
Responsável: Comunicação + GTI

5. Indicadores do Plano de Contingência

5.1. Índice de Sucesso dos Testes de Contingência (ISTC)

Fórmula:
ISTC = (Testes bem-sucedidos / testes realizados) × 100

Meta: ≥ 90% **Periodicidade:** Semestral **Responsável:** GTI

5.2. Taxa de Atualização do Plano de Contingência Fórmula:

% = (Atualizações realizadas / atualizações previstas) × 100

Meta: 100% (a cada 2 anos)
Responsável: GTI
Origem: Item 16 – Atualização do Plano.

6. Indicadores de Backups e Integridade

6.1. Índice de Sucesso de Backups (ISB)

Descrição: Mede quantos backups foram executados com sucesso.

Fórmula:
ISB = (backups bem-sucedidos / total de backups) × 100

Meta: 100% **Periodicidade:** Mensal **Responsável:** GTI
Origem: Item 10 – Backup e Restauração.

6.2. Índice de Sucesso dos Testes de Restauração (ISTR) Descrição: Mede a eficácia dos testes de restauração.

Fórmula:
ISTR = (restaurações bem-sucedidas / total de testes) × 100

Meta: ≥ 95% **Periodicidade:** Mensal **Responsável:** GTI

7. Indicadores de Acesso e Autenticação

7.1. Contas Inativas Eliminadas no Prazo (CIEP)

Fórmula:
CIEP = (Contas inativas eliminadas / contas inativas encontradas) × 100

Meta: ≥ 95% **Periodicidade:** Semestral **Responsável:** GTI
Origem: PSI – Auditoria de acessos.

7.2. Índice de Senhas Fortes (ISF)

Descrição: Mede se usuários seguem os critérios de senha.

Fórmula:
ISF = (Senhas conformes / total de verificações) × 100

Meta: 100% **Periodicidade:** Semestral **Responsável:** GTI