PLANO DE CONTINGÊNCIA DE TECNOLOGIA DA INFORMAÇÃO
NITERÓI PREV

1. OBJETIVO

Estabelecer diretrizes, responsabilidades e procedimentos para garantir a continuidade dos serviços de Tecnologia da Informação do RPPS de grande porte, assegurando:

- Pagamento regular e tempestivo dos benefícios;
- Integridade, confidencialidade e disponibilidade das informações previdenciárias;
- Conformidade com normas da Secretaria de Previdência, Tribunal de Contas e LGPD;
- Minimização de impactos operacionais, financeiros e reputacionais.

2. ESCOPO

Aplica-se a:

- Sistemas previdenciários e atuariais
- Sistemas contábeis e financeiros
- Banco de dados
- Infraestrutura física e virtual
- Ambiente em nuvem
- Links de internet
- Segurança da informação
- Atendimento digital ao segurado

3. BASE NORMATIVA E CONTROLES EXIGIDOS PELA SECRETARIA DE PREVIDÊNCIA

Este plano observa as exigências aplicáveis ao RPPS, incluindo:

3.1 Governança e Controles Obrigatórios

✓ Política formal de Segurança da Informação
✓ Plano de Continuidade de Negócios (PCN)
✓ Plano de Contingência de TI formalizado

✓ Inventário atualizado de ativos de TI

✓ Controle de acesso com segregação de funções

✓ Trilhas de auditoria (logs) mantidas por no mínimo 5 anos (Deve-se observar com os administradores dos sistemas externos os períodos de retenção de logs para adequação às necessidades do relatório.)

✓ Backup periódico com testes de restauração (Sistemas externos podem possuir periodicidades próprias de backup.)

✓ Controle formal de contratos com fornecedores de TI

✓ Gestão de riscos documentada

✓ Plano de resposta a incidentes de segurança

✓ Conformidade com LGPD (encarregado/DPO designado)

4. BUSINESS IMPACT ANALYSIS (BIA)

4.1 Identificação de Processos Críticos

Processo	Impacto	Criticidade
Pagamento de benefícios	Interrupção social e legal	Crítico
Folha mensal	Multas e responsabilização	Crítico
CADPREV / envio de informações	Irregularidade previdenciária	Alto
Contabilidade	Impacto fiscal	Alto
Atendimento ao segurado	Impacto reputacional	Médio
Portal da Transparência	Risco legal	Alto

4.2 Definição de RTO e POR

Os tempos de recuperação (RTO) deverão ser validados periodicamente por testes práticos de restauração total, com registro dos tempos efetivamente obtidos.

Sistema	RTO	RPO
Sistema Previdenciário	4 horas	1 hora
Banco de Dados	2 horas	30 min

Sistema	RTO	RPO
Sistema Contábil	8 horas	2 horas
Portal do Segurado	12 horas	4 horas
E-mail Corporativo	24 horas	8 horas

4.3 Impactos Potenciais

- Suspensão de pagamento
- Multas administrativas
- Perda de Certificado de Regularidade Previdenciária (CRP)
- Danos à imagem institucional
- Vazamento de dados sensíveis

5. ESTRATÉGIAS DE CONTINGÊNCIA

O ambiente de backup encontra-se segregado logicamente do ambiente de produção, reduzindo riscos de perda simultânea em caso de falha ou incidente de segurança.

5.1 Infraestrutura

Medida	Descrição	Responsável
Data center climatizado	Controle de temperatura e umidade	TI
Host de virtualização centralizado	Ambiente físico que hospeda servidores virtuais críticos	
Servidor dedicado de backup	Equipamento independente responsável pelo armazenamento das cópias	TI
Backup local estruturado	Cópias mantidas fora do host principal	
Backup 3-2-1	3 cópias, 2 mídias, 1 externa (*)	TI
Backup externo (offsite)	Armazenamento externo seguro	TI

Medida	Descrição	Responsável
Link de internet redundante	Operadoras distintas	TI
Firewall UTM	Proteção perimetral	TI
No-break	Autonomia de 1 hora para a função de desligamento seguro dos serviços	Administração

(*) Sistemas internos não possuem backup em nuvem e no caso dos externos deve-se observar com seus administradores, as políticas de backup destes sistemas.

5.2 Segurança da Informação

✓ Autenticação multifator (MFA)
✓ Controle de acesso por perfil
✓ Logs de auditoria ativos
✓ Criptografia de dados sensíveis
✓ Teste anual de vulnerabilidade
✓ Treinamento anual de usuários
✓ Política formal de senhas

Responsável: Gerência de TI

5.3 Banco de Dados

- Backup incremental diário
- Backup completo semanal
- Teste trimestral de restauração
- Monitoramento de integridade
- Backup realizado via servidor dedicado
- Backup de máquinas virtuais completas + backup lógico do banco
- Testes considerando restauração completa de VM
- Ambiente de contingência em nuvem (*)

(*) Temos um ambiente heterogêneo, cujos bancos de dados administrados internamente não possuem contingência em nuvem e no caso dos externos deve-se observar com seus administradores, as políticas de backup destes sistemas.

Responsável: Administrador de Banco de Dados

6. PLANO DE RESPOSTA A INCIDENTES

6.1 Classificação

Nível	Descrição
Baixo	Incidente isolado
Médio	Afeta setor específico
Alto	Afeta sistemas críticos
Crítico	Interrompe pagamento ou compromete dados

6.2 Fluxo Operacional

1. Identificação
2. Registro formal
3. Classificação
4. Comunicação à Diretoria
5. Ação corretiva
6. Recuperação
7. Relatório pós-incidente

7. MATRIZ DE RESPONSABILIDADES

Atividade	TI	Diretor	Controle Interno	Fornecedor
Backup diário	R	I	I	C
Teste de restauração	R	I	C	C

Atividade	TI	Diretor	Controle Interno	Fornecedor
Ativação da contingência	R	A	C	C
Comunicação oficial	C	R	A	I
Relatório pós-incidente	R	A	C	I
Recuperação de host de virtualização	R	I	I	C
Restauração de máquinas virtuais	R	I	I	C
Validação de Active Directory	R	I	I	C

Legenda:
R = Responsável
A = Aprovador
C = Consultado
I = Informado

8. CHECKLIST OPERACIONAL DE CONTINGÊNCIA

8.1 Checklist Diário

☐ Verificação automática de backup
☐ Verificação de logs de erro
☐ Monitoramento de antivírus
☐ Monitoramento de uso de servidor
☐ Verificação de integridade de banco

8.2 Checklist Mensal

☐ Teste de restauração parcial
☐ Atualização de patches
☐ Revisão de acessos de usuários
☐ Teste de link redundante
☐ Atualização de inventário de ativos

8.3 Checklist Trimestral

☐ Teste completo de restauração
☐ Simulação de indisponibilidade
☐ Teste de plano de resposta a incidentes
☐ Revisão de contratos de TI
☐ Auditoria de logs

8.4 Checklist Anual

☐ Simulação completa de desastre
☐ Treinamento de usuários
☐ Revisão do plano
☐ Relatório de gestão de riscos
☐ Atualização da política de segurança

8.5 Checklist em caso de desastre

☐ Classificar tipo de desastre
☐ Acionar Diretor Presidente
☐ Registrar ocorrência formal
☐ Isolar ambiente afetado
☐ Avaliar integridade dos backups
☐ Restaurar ambiente de contingência
☐ Validar sistemas críticos
☐ Comunicar partes interessadas
☐ Emitir relatório final
☐ Registrar lições aprendidas
☐ Verificar integridade do servidor de backup
☐ Validar disponibilidade do repositório de backup
☐ Definir ordem de restauração das VMs
☐ Validar funcionamento do Active Directory antes de outros sistemas

9. PLANO DE COMUNICAÇÃO EM CRISE

Em caso de incidente crítico:

1. Comunicação imediata à Diretoria
2. Comunicação ao Controle Interno
3. Comunicação ao Ente Federativo (se aplicável)
4. Comunicação formal aos segurados (se houver impacto)
5. Registro documental completo

10. TESTES E REVISÃO DESTE PLANO

- Revisão anual obrigatória
- Atualização após incidente relevante
- Registro formal de testes realizados
- Aprovação pela Diretoria Executiva

11. ROTINAS TÉCNICAS DE RECUPERAÇÃO DE DESASTRES

A classificação do incidente como desastre e a ativação formal do plano de contingência caberá ao responsável de TI, com ciência da Diretoria.

11.1 Escopo da recuperação

As rotinas deste item aplicam-se aos ativos de TI administrados internamente pela Niterói Prev, organizados conforme a seguinte arquitetura:

- **Host de virtualização principal**, responsável por hospedar os servidores:
    - Servidor de arquivos
    - Active Directory (AD)
    - Servidor de impressão
- **Servidor independente de backup**, responsável pelo armazenamento das cópias de segurança dos ambientes virtuais.

Não fazem parte deste escopo serviços externos ou sistemas gerenciados por terceiros, os quais devem seguir seus próprios procedimentos de contingência.

11.2 Hipóteses de acionamento

A recuperação deverá ser acionada em caso de:

- falha total da máquina host de virtualização;
- indisponibilidade de uma ou mais máquinas virtuais críticas;
- corrupção de dados ou perda de volumes;
- falha do Active Directory;
- falha grave no sistema operacional do host ou das VMs;
- incidente de segurança que comprometa integridade, disponibilidade ou autenticidade dos dados.

11.3 Objetivos de recuperação

Devem ser respeitados os seguintes parâmetros mínimos:

- **Banco de dados:**
    - RTO: até 2 horas
    - RPO: até 30 minutos
- **Active Directory:** recuperação prioritária, anterior aos sistemas dependentes;
- **Servidor de arquivos:** recuperação conforme criticidade dos dados administrativos e operacionais.

11.4 Estratégia geral de recuperação

A estratégia adotada baseia-se em:

- restauração de máquinas virtuais a partir do **servidor dedicado de backup**;
- priorização da recuperação por dependência técnica dos serviços;
- isolamento do ambiente comprometido antes da restauração.

11.5 Sequência de recuperação

A recuperação deverá seguir a seguinte ordem obrigatória:

1. Infraestrutura física e host de virtualização

2. Active Directory (autenticação e serviços básicos)
3. Servidor de banco de dados
4. Servidor de arquivos
5. Serviços auxiliares (impressão etc)
6. Validação geral e liberação

11.6 Procedimento de recuperação do host de virtualização

Em caso de falha do host principal:

a) avaliar necessidade de substituição ou reinstalação do host físico;
b) reinstalar o hipervisor ou restaurar sua configuração;
c) reestabelecer conectividade com o servidor de backup;
d) validar acesso aos repositórios de backup;
e) iniciar o processo de restauração das máquinas virtuais.

11.7 Procedimento de restauração das máquinas virtuais

11.7.1 Etapas gerais

Para cada servidor virtual:

a) selecionar o backup íntegro mais recente;
b) validar consistência da imagem de backup;
c) restaurar a máquina virtual no host disponível;
d) garantir configuração correta de rede, IP e integração ao ambiente;
e) iniciar a VM em modo controlado para validação.

11.8 Procedimento de restauração do Active Directory

11.8.1 Prioridade

O Active Directory deve ser restaurado antes dos sistemas dependentes.

11.8.2 Etapas

a) restaurar a VM do controlador de domínio a partir do backup;
b) validar integridade do **System State**, SYSVOL e base do AD;
c) verificar funcionamento de DNS e políticas de grupo (GPO);

d) testar autenticação com usuário administrativo e usuário padrão;
e) validar acesso aos recursos de rede.

11.8.3 Critério de liberação

O AD será considerado operacional quando:

- autenticação estiver funcional;
- políticas aplicadas corretamente;
- resolução de nomes funcionando;
- acesso aos serviços dependentes habilitado.

11.9 Procedimento de restauração do sistema de banco de dados

11.9.1 Etapas

a) restaurar banco de dados a partir do último backup válido;
b) aplicar incrementais/logs, se aplicável;
c) validar integridade da base;
d) testar funcionamento do sistema com usuário autorizado.

11.9.2 Critério de aceitação

- sistema acessível;
- dados consistentes;
- operações críticas funcionando (consulta, processamento etc).

11.10 Procedimento de restauração do servidor de arquivos

a) restaurar VM do servidor de arquivos;
b) restaurar volumes e diretórios;
c) validar permissões de acesso;
d) testar compartilhamentos críticos.

11.11 Procedimentos pós-recuperação

Após a restauração:

- revisar contas administrativas e permissões;

- redefinir senhas críticas, se necessário;
- verificar presença de ameaças ou persistência maliciosa;
- validar backups futuros;
- monitorar o ambiente de forma intensiva nas primeiras 24/48 horas.

11.12 Failback (retorno à operação normal)

Caso a recuperação ocorra em ambiente alternativo:

a) sincronizar dados atualizados;
b) validar integridade;
c) retornar operação ao host principal após estabilização;
d) registrar formalmente o encerramento do incidente.

11.13 Registro e rastreabilidade

Todas as ações devem ser registradas, contendo:

- data e hora;
- ativo afetado;
- tipo de falha;
- backup utilizado;
- responsáveis técnicos;
- tempo de recuperação;
- validações realizadas;
- lições aprendidas.

12. DISPOSIÇÕES FINAIS

Este plano entra em vigor na data de sua aprovação e deve ser amplamente divulgado aos responsáveis.