PLANO DE RECUPERAÇÃO DE DADOS

SUMÁRIO

1. INTRODUÇÃO

1.1. Dos serviços essenciais de Tecnologia da Informação

Documento Nº: **371943/2023**
MINUTA - proposta de minuta alteração IN 06/2018

I – Sistemas de eleição, durante o período eleitoral;
II – Sistemas de atendimento ao eleitor/cadastro;
III – Processo Judicial Eletrônico (PJE);
IV - Diário de Justiça Eletrônico (DJE);
V – Sistemas de processo administrativo digital (PAD e SEI);
VI - Serviços de e-mail e colaboração em nuvem;
VIII – Sistema de Acompanhamento de Documentos e Processos (SADP).

1.2. Matriz de serviços essenciais de negócio

Serviço	Criticidade	RPO[1]	RTO[2]	Descrição
Sistemas de eleição	Alta	24 horas	4 horas	Perda de acesso aos sistemas eleitorais
Sistemas de atendimento ao eleitor	Alta	24 horas	4 horas	Perda de acesso aos sistemas de atendimento ao eleitor
PJE	Alta	24 horas	4 horas	Perda de acesso ao sistema
DJE	Alta	24 horas	4 horas	Perda de acesso ao sistema
PAD / SEI	Alta	Último backup válido	4 horas	Perda de acesso aos sistemas de processo administrativo digital
Keycloak	Alta	Último backup válido	4 horas	Perda de acesso aos sistemas
Google Workspace	Alta	24 horas	4 horas	Serviço de e-mail / storage indisponíveis
Intranet	Média	24 horas	12 horas	Perda de acesso à intranet
Portal do Servidor	Baixa	24 horas	24 horas	Perda de acesso à intranet

[1] Recovery Point Objective: quantidade limite de dados que uma organização toleraria perder em caso de pane ou de paralisação, decorrente de uma iminente **ameaça de invasão.**

[2] Recovery Time Objective: período máximo de tempo que o sistema levará para voltar a operar após uma parada ou pane.

1.3. Matriz de serviços essenciais de infraestrutura

Serviço	Criticidade	RPO[3]	RTO[4]	Descrição
Virtualização	Alta	Último backup válido	4 horas	Perda de acesso aos sistemas
Servidores de aplicação	Alta	Último backup válido	4 horas	Perda de acesso aos sistemas
Serviços de rede	Alta	Último backup válido	4 horas	Perda de acesso à rede, sistemas e internet
Serviços de storage	Alta	Último backup válido	4 horas	Perda de acesso aos dados
Serviços de monitoramento	Alta	Último backup válido	4 horas	Perda de acesso ao monitoramento ativo
DHCP	Alta	Ambiente de contingência	4 horas	Perda de acesso à rede, sistemas e internet
DNS	Alta	Ambiente de contingência	4 horas	Perda de acesso à rede, sistemas
Data Center	Alta	Ambiente de contingência	4 horas	Perda de acesso ao ambiente computacional

1.4. Matriz de serviços essenciais de segurança da informação

Serviço	Criticidade	RPO[5]	RTO[6]	Descrição
Firewall	Alta	Ambiente de contingência	4 horas	Perda de acesso à rede, sistemas e internet
WAF / F5	Alta	Ambiente de	4 horas	Perda de acesso ao sistema

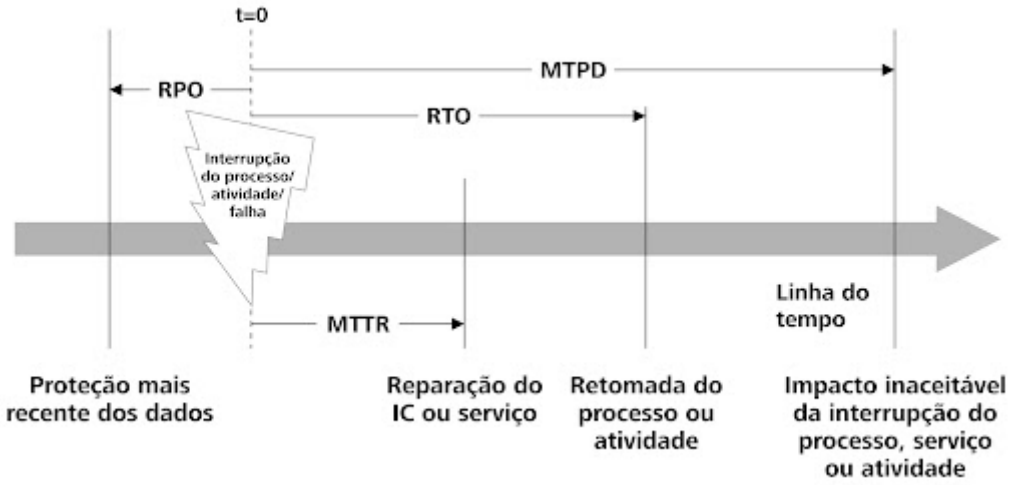
[3] Recovery Point Objective: quantidade limite de dados que uma organização toleraria perder em caso de pane ou de paralisação, decorrente de uma iminente **ameaça de invasão.**

[4] Recovery Time Objective: período máximo de tempo que o sistema levará para voltar a operar após uma parada ou pane.

[5] Recovery Point Objective: quantidade limite de dados que uma organização toleraria perder em caso de pane ou de paralisação, decorrente de uma iminente **ameaça de invasão.**

[6] Recovery Time Objective: período máximo de tempo que o sistema levará para voltar a operar após uma parada ou pane.

		contingência		
Segurança de endpoints	Alta	Ambiente de contingência	4 horas	Perda de acesso ao sistema
Análise de vulnerabilidade	Alta	Ambiente de contingência	4 horas	Perda de acesso ao sistema



1.5. Objetivo do PRD

1.5.1. O objetivo deste plano é assegurar a restauração das operações no ambiente principal após a ocorrência de uma crise ou cenário de desastre, concentrando-se nos ativos, conexões e configurações específicas do ambiente. Os objetivos do PRD são os seguintes:

1.5.2. Avaliar os danos aos ativos e conexões do datacenter e fornecer meios para sua recuperação.

1.5.3. Restaurar o ambiente computacional em prazo tolerável.

1.6. Escopo e abrangência

1.6.1. Abrange servidores de aplicações, bancos de dados e serviços computacionais essenciais.

1.7. Papéis e responsabilidades

1.7.1. Equipe de instalações / ambiente

1.7.1.1. Composta por servidores do Tribunal Regional Eleitoral que são responsáveis pelas instalações físicas que abrigam o ambiente computacional (envolve a infraestrutura predial além da infraestrutura de TI).

1.7.2. Equipe de conectividade

1.7.2.1. Fornecimento e manutenção da infraestrutura de rede.

1.7.3. Equipe de infraestrutura / aplicações

1.7.3.1. Fornecimento e manutenção da infraestrutura de servidores físicos e virtuais necessária para execução de operações e processos essenciais durante um desastre.

1.7.4. Equipe de operações

1.7.4.1. Responsável pelo ambiente colaborativo, de forma a garantir as ferramentas necessárias para que os servidores desempenhem suas funções da forma mais rápida e eficiente possível.

1.7.5. Equipe de comunicação

1.7.5.1. Responsável pela comunicação durante um desastre. Repassa informações aos setores competentes do Tribunal.

1.7.6. Equipe de backup

1.7.6.1. Análise e mapeamento de dados perdidos, tempo de recuperação, além da formulação de estratégias de recuperação.

1.7.7. Equipe de testes

1.7.7.1. Responsável pelos testes de ambiente de forma a auxiliar na elaboração de cronogramas, bem como informar o marco temporal de recuperação.

1.7.8. Equipe de segurança da informação

1.7.8.1. Fornecimento e manutenção de mecanismos de segurança no ambiente principal e alternativo, resguardar dados e evitar desdobramentos de segurança que afetem o acionamento da continuidade.

2. IDENTIFICAÇÃO DE RISCOS

2.1. Lista de potenciais desastres

Evento	Possíveis causas
Indisponibilidade de rede / circuitos	Rompimento de fibra óptica, desastres naturais (tempestades), falha de equipamento de rede
Perda de dados	Falha de hardware (disco rígido, memória), ataque de malware, erro humano (exclusão acidental)
Interrupção de energia elétrica	Queda de linhas de energia, sobrecarga na rede elétrica, falha de equipamento de energia
Incêndio nas instalações	Curto-circuito elétrico, vazamento de produtos inflamáveis, falha no sistema de prevenção de incêndios
Inundação nas instalações	Vazamento de encanamento, tempestades intensas
Ataque cibernético	Malware, phishing, engenharia social, exploração de vulnerabilidades de software
Falha do sistema de refrigeração	Falha do equipamento de refrigeração, obstrução dos dutos de ventilação, vazamento de gás refrigerante

3. INVENTÁRIO DE RECURSOS

3.1. Lista de ativos críticos

3.1.1. Servidores físicos, servidores virtuais, armazenamento de dados, máquinas virtuais, bancos de dados.

3.2. Detalhes de configuração e localização física

3.2.1. Configurações específicas de máquinas virtuais, localização física dos servidores no data center, detalhes de armazenamento virtualizado.

4. PROCEDIMENTOS DE BACKUP

4.1. Frequência e métodos de backup

4.1.1. Backup diário de máquinas virtuais, armazenamento de snapshots para rápida recuperação.

4.2. Armazenamento seguro e locais alternativos

4.2.1. Armazenamento em storage virtualizado e replicação em data centers secundários.

4.3. Testes regulares de restauração

4.3.1. Testes bimestrais de restauração para garantir a integridade dos backups.

5. COMUNICAÇÃO E NOTIFICAÇÃO

5.1. Lista de contatos de emergência

5.1.1. Números de telefone e endereços de e-mail da equipe de recuperação e contatos no data center.

5.2. Procedimentos de comunicação interna e externa

5.2.1. Uso de canais de comunicação seguros e definidos para notificar a equipe e o data center em caso de desastres.

5.3. Cadeia de comando durante uma crise

5.3.1. Hierarquia de comunicação clara entre os membros da equipe.

6. MANUTENÇÃO E ATUALIZAÇÃO

6.1. Revisão periódica do PRD

6.1.1. Revisão anual do documento para refletir alterações na infraestrutura de virtualização.

6.2. Atualização conforme mudanças na infraestrutura

6.2.1. Inclusão de novas máquinas virtuais, atualizações de hipervisores e outras alterações no ambiente virtualizado.

6.3. Treinamento contínuo das equipes

6.3.1. Garantir que todos estejam familiarizados com os procedimentos específicos de recuperação em ambientes virtualizados.

7. DOCUMENTAÇÃO DE INCIDENTES

7.1. Registro de eventos críticos

7.1.1. Documentação detalhada de incidentes, incluindo impacto nas máquinas virtuais e nas operações.

7.2. Análise pós-incidente

7.2.1. Avaliação das ações tomadas, identificação de pontos fortes e áreas de melhoria para ambientes virtualizados.

7.3. Ações corretivas e preventivas

7.3.1. Implementação de medidas para fortalecer a segurança em máquinas virtuais e prevenir futuros incidentes similares.

8. MACROPROCESSOS DO PLANO DE CONTINUIDADE DE TI

8.1. Identificação e declaração de desastre;

8.2. Ativação do Plano de Recuperação de Desastres (DRP)

8.2.1. Ativação do plano de recuperação de desastres.

8.3. Avaliação da Situação

8.3.1. Avaliar a extensão dos danos e os sistemas afetados pelo desastre.

8.3.2. Priorizar a recuperação com base na criticidade dos sistemas e na necessidade de negócio.

8.4. Comunicação com as Partes Interessadas

8.4.1. Comunicação constante entre as partes interessadas internas e externas, com atualização da situação e das medidas de recuperação em andamento.

8.5. Provisionamento de Recursos de Recuperação

8.5.1. Alocar os recursos necessários para iniciar a recuperação, como hardware de reposição, software, pessoal de suporte, etc.

8.6. Restauração de Sistemas Críticos

8.6.1. Priorizar a restauração dos sistemas críticos para a continuidade das operações essenciais da organização.

8.7. Recuperação de Dados

8.7.1. Restaurar os dados a partir de backups recentes e verificar a integridade dos dados recuperados.

8.8. Teste de Funcionalidade

8.8.1. Após a restauração dos sistemas e dados, aplicar testes visando avaliação da funcionalidade dos sistemas para garantir que estejam operacionais e atendam às necessidades de negócio.

8.9. Verificação da Segurança

8.9.1. Verificar se os sistemas restaurados estão protegidos contra ameaças de segurança, como malware, vulnerabilidades de software, etc.

8.10. Validação da Recuperação

8.10.1. Validar se os sistemas estão funcionando conforme o esperado e se os dados estão acessíveis.

8.11. Reintegração ao Ambiente de Produção

8.11.1. Após confirmar que a recuperação foi bem-sucedida, reintegrar os sistemas recuperados ao ambiente de produção.

8.12. Revisão e Atualização do Plano de Recuperação de Desastres

8.12.1. Após o término da recuperação, revisar o plano de recuperação de desastres para identificar áreas de melhoria e atualizar conforme necessário com base nas lições aprendidas.

9. EXECUÇÃO DO PLANO DE DESASTRES

9.1. Procedimentos

9.1.1. Identificar ativos danificados / serviços indisponíveis

9.1.1.1. As equipes de instalação / backup / infraestrutura / conectividade deverão identificar e listar todos os ativos danificados

9.1.2. Identificar acessos indisponíveis

9.1.2.1. A equipe de conectividade deverá identificar as interrupções de conexões e acessos gerados após o desastre, informando a abrangência (rede local, rede WAN ou provedor).

9.1.3. Identificar serviços indisponíveis

9.1.3.1. A equipe do PRD deverá mapear os serviços indisponíveis abrangendo todos os componentes necessários à plena operação dos serviços essenciais como máquinas virtuais, banco de dados, firewall, plataforma de colaboração, roteadores, switches, equipamentos de microinformática, bem como rotas, dns, vlans, etc.

9.1.4. Elaborar cronograma de recuperação

9.1.4.1. Após o mapeamento de perdas e impactos será elaborado um breve cronograma de recuperação das aplicações.

9.1.5. Substituição de ativos e equipamentos

9.1.5.1. Em caso de perda de ativos deverá ser realizada estimativa de tempo para aquisição e o quanto isso impacta no RTO de cada serviço.

9.1.6. Reconfiguração de ativos e equipamentos

9.1.6.1. A equipe de instalações deverá verificar as configurações de forma a garantir pleno funcionamento dos serviços.

9.1.7. Teste de ambiente

9.1.7.1. Realização de testes do ambiente alternativo;

9.1.7.2. Realização de testes do ambiente principal antes de recuperação de dados, quando for o caso;

9.1.7.3. Validar configurações e funcionalidades dos sistemas;

9.1.7.4. Quando possível incluir testes automatizados de monitoramento de serviços.

9.1.8. Encerramento do PRD

9.1.8.1. Consolidar informações em parecer específico com o tempo de restabelecimento de cada serviço ou equipamento, bem como lista de procedimentos realizados e fornecedores eventualmente acionados.

10. ANEXOS

10.1. Mapas de rede

10.1.1. Diagramas mostrando a interconexão das máquinas virtuais e servidores físicos.

10.2. Listas de fornecedores de serviços de recuperação

10.2.1. Contatos de empresas especializadas em recuperação de desastres em ambientes virtualizados.

IC / Serviço	Contato	E-mail	Telefone
Operadora 1			
Operadora 2			

10.3. Documentação técnica adicional

10.3.1. Manuais detalhados para configuração de hipervisores, políticas de segurança virtual e outros detalhes específicos de ambientes virtualizados.

10.4. Cronograma de testes

10.4.1. Previsão de realização de simulação no ambiente nos dias 23 e 24 de março de 2024, para os serviços essenciais do Tribunal Regional Eleitoral do Paraná, conforme documento PAD **371943/2023.**

10.4.2. Previsão de realização de 3 testes por ano.

10.5. Documento de validação e teste

Data / Horário	Serviço / Sistema	Tipo	Descrição	Status
		Teste de mesa / Teste automatizado / simulação no ambiente		Falha / Sucesso