PLANO DE RECUPERAÇÃO A DESASTRES DA CONTROLADORIA E OUVIDORIA GERAL DO ESTADO DO CEARÁ – CGE/CE

CONTROLE DE APROVAÇÃO

ELABORAÇÃO	REVISÃO	APROVAÇÃO
Leonardo dos Santos Menezes Borba	Marcos Henrique de Carvalho Almeida	Marcelo de Sousa Monteiro

HISTÓRICO DE MODIFICAÇÕES

Versão	Data	Alterações em relação à edição anterior
01	06/01/2026	Edição inicial.

Controladoria e Ouvidoria Geral do Estado
Av. Gal. Afonso Albuquerque Lima – Ed. Seplag - 2ºandar - Cambeba • CEP: 60.822-325
Fortaleza / CE • Fone: (85) 3101 3471

SUMÁRIO

Controladoria e Ouvidoria Geral do Estado
Av. Gal. Afonso Albuquerque Lima – Ed. Seplag - 2ºandar - Cambeba • CEP: 60.822-325
Fortaleza / CE • Fone: (85) 3101 3471

1.INTRODUÇÃO

O Plano de Recuperação de Desastres (PRD) estabelece os procedimentos, responsabilidades e mecanismos necessários para restaurar a infraestrutura tecnológica, os sistemas corporativos e os serviços essenciais da Controladoria e Ouvidoria Geral do Estado do Ceará (CGE/CE) em situações de desastre que comprometam a continuidade das operações. Seu objetivo central é reduzir o tempo de indisponibilidade, assegurar a integridade das informações e garantir que os serviços críticos retornem ao funcionamento dentro dos prazos estabelecidos pela organização.

Este documento abrange a infraestrutura física e lógica utilizada pela CGE/CE, incluindo servidores, aplicações, bancos de dados, redes, serviços em nuvem e demais componentes que suportam os sistemas corporativos da instituição. O PRD se aplica a eventos de grande impacto, como falhas massivas de hardware, interrupções prolongadas de energia, danos físicos às instalações, incidentes cibernéticos de alto impacto ou qualquer situação que exija a reconstrução total ou parcial do ambiente tecnológico.

2. ALINHAMENTO NORMATIVO E ESTRATÉGICO

O PRD faz parta da Política de Segurança da Informação da CGE e funciona de maneira complementar ao Plano de Resposta a Incidentes (PRI). Enquanto o PRI trata da resposta imediata a incidentes de segurança, o PRD define o conjunto de ações necessárias para reconstruir ou restaurar ambientes tecnológicos quando o impacto ultrapassa a capacidade de resposta operacional rotineira.

O PRD está alinhado às diretrizes de:

- Política de Segurança da Informação e Comunicação (POSIC) da CGE/CE;
- Plano de Resposta a Incidentes da CGE/CE;

Controladoria e Ouvidoria Geral do Estado
Av. Gal. Afonso Albuquerque Lima – Ed. Seplag - 2ºandar - Cambeba • CEP: 60.822-325
Fortaleza / CE • Fone: (85) 3101 3471

- Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018);
- Normas e boas práticas de continuidade;

3. DEFINIÇÕES

Para efeito deste Plano são adotadas as seguintes definições:

a) **Ambiente Primário e Secundário:** locais ou infraestruturas destinados à operação principal e à recuperação;

b) **Ataque:** qualquer ação ou conjunto de ações deliberadas realizadas com o objetivo de comprometer a confidencialidade, integridade ou disponibilidade de um sistema, rede, ou conjunto de dados.

c) **Desastre**: evento que provoca interrupção severa dos serviços e exige ações extraordinárias de recuperação;

d) **Incidente de Segurança***:* qualquer evento ou ação que comprometa a confidencialidade, integridade ou disponibilidade dos dados ou sistemas de uma organização;

e) **Log:** processo de registro de eventos relevantes num sistema computacional;

f) **Malware:** qualquer tipo de software projetado para causar danos a um computador, servidor, rede ou dispositivo;

g) **Ransomware:** é um tipo de malware, ou software malicioso, que pode bloquear o acesso a dados ou criptografá-los, exigindo um resgate para restaurar o acesso**;**

h) **RTO (Recovery Time Objective):** tempo máximo tolerável para restabelecer um serviço;

i) **RPO (Recovery Point Objective)**: ponto máximo, em termos de tempo, a partir do qual os dados podem ser recuperados;

j) **Vírus:** programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos;

Controladoria e Ouvidoria Geral do Estado
Av. Gal. Afonso Albuquerque Lima – Ed. Seplag - 2ºandar - Cambeba • CEP: 60.822-325
Fortaleza / CE • Fone: (85) 3101 3471

k) **Worm**: programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador;

4. GOVERNANÇA E RESPONSABILIDADES

A governança do Plano de Recuperação de Desastres (PRD) estabelece a estrutura de papéis, responsabilidades, autoridades e fluxos de comunicação necessários para assegurar a execução coordenada e eficaz das ações de recuperação da infraestrutura tecnológica. O objetivo é garantir que, diante de um desastre, todas as equipes envolvidas atuem de forma organizada, seguindo a cadeia de comando definida e mantendo a rastreabilidade das decisões.

A governança do PRD é composta pelos seguintes grupos:

4.1 Coordenador do PRD

Responsável pela condução integral do plano, incluindo:

a) Coordenar a execução das etapas de recuperação;
b) Acionar as equipes envolvidas e distribuir responsabilidades;
c) Reportar o progresso à alta administração;
d) Garantir o registro de evidências e decisões;
e) Validar o cumprimento dos requisitos de recuperação (RTO/RPO).

4.2 Equipe Técnica de Infraestrutura e Operações

Equipe responsável pela execução dos procedimentos técnicos necessários para restaurar a infraestrutura, incluindo:

a) Servidores físicos e virtuais;
b) Ambientes em nuvem;
c) Redes e comunicação;
d) Bancos de dados e aplicações;
e) Restauração de backups;

Controladoria e Ouvidoria Geral do Estado
Av. Gal. Afonso Albuquerque Lima – Ed. Seplag - 2ºandar - Cambeba • CEP: 60.822-325
Fortaleza / CE • Fone: (85) 3101 3471

4.3 Encarregado de Dados (DPO/CGE)

Atua quando houver risco ou evidência de impacto sobre dados pessoais, sendo responsável por:

a) Assessorar sobre obrigações da LGPD durante a recuperação;
b) Emitir pareceres sobre mitigação de riscos à privacidade;
c) Auxiliar na tomada de decisão sobre comunicação a titulares ou ANPD;
d) Registrar impactos e medidas de proteção adotadas.

4.4 Responsáveis por Sistemas Críticos

Cada sistema essencial (ex.: Ceará Transparente, AVIA, e-Contratos, SACC, e-Parcerias e etc.) possui um responsável que deve:

a) Auxiliar na priorização da recuperação;
b) Validar a disponibilidade funcional após a restauração;
c) Garantir a comunicação com usuários das áreas finalísticas.

5. CLASSIFICAÇÃO DOS ATIVOS

A classificação dos ativos críticos tem como objetivo identificar os sistemas, serviços, dados e componentes tecnológicos cuja indisponibilidade pode causar impactos significativos às operações da Controladoria e Ouvidoria Geral do Estado do Ceará (CGE/CE). Esse processo permite definir prioridades de recuperação, estabelecer níveis adequados de proteção e orientar a execução do PRD.

5.1 Critérios de Classificação

Os ativos tecnológicos são classificados com base nos seguintes critérios:

a) Impacto na Prestação de Serviços Essenciais: Avalia a importância do ativo para a manutenção das atividades finalísticas da CGE/CE, tais como auditoria, ouvidoria, transparência e controle interno;

Controladoria e Ouvidoria Geral do Estado
Av. Gal. Afonso Albuquerque Lima – Ed. Seplag - 2ºandar - Cambeba • CEP: 60.822-325
Fortaleza / CE • Fone: (85) 3101 3471

b) **Impacto Legal e Normativo:** Considera exigências da POSIC da CGE, Lei Estadual e demais regulamentações que demandam proteção e disponibilidade dos dados;

c) **Impacto Operacional:** Analisa a dependência das áreas internas em relação ao ativo e os prejuízos causados pela indisponibilidade prolongada**.**

d) **Impacto Reputacional:** Avalia potenciais danos à confiança pública, especialmente para sistemas acessados pela sociedade (ex.: Ceará Transparente).

e) **Impacto em Dados Pessoais:** Examina a sensibilidade dos dados tratados e a probabilidade de violação de dados pessoais em caso de indisponibilidade ou perda.

5.2 Níveis de Criticidade

Os ativos são classificados em três níveis:

a) **Crítico**: Ativos cuja interrupção compromete diretamente serviços essenciais, gera riscos legais, afetando operações de controle interno, auditoria, ouvidoria ou transparência. A recuperação deve observar os menores RTO e RPO definidos;

b) **Importante**: Ativos relevantes para as operações, mas cuja indisponibilidade, embora impactante, não inviabiliza totalmente a atividade fim.

c) **Operacional**: Ativos de apoio, administrativos ou auxiliares, cuja interrupção possui impacto limitado e possui alternativas temporárias.

5.3 Inventário dos Ativos Tecnológicos

O inventário de ativos está disposto no caminho **G:\CEINS\Datacenter\Inventário de VM's e Servers.xlsx** e contempla os seguintes tipos de ativos:

a) Sistemas corporativos (internos e externos);
b) Servidores físicos e virtuais;
c) Serviços em nuvem (ETICE, AWS, Azure);
d) Bancos de dados;

Controladoria e Ouvidoria Geral do Estado
Av. Gal. Afonso Albuquerque Lima – Ed. Seplag - 2ºandar - Cambeba • CEP: 60.822-325
Fortaleza / CE • Fone: (85) 3101 3471

e) Componentes de rede;
f) Serviços de autenticação (AD, LDAP, IAM etc.);
g) Repositórios de backup;
h) Equipamentos (racks, storages, switches, firewalls).

5.4 Matriz de Criticidade dos Ativos

A Matriz de Criticidade dos Ativos, apresentada no caminho **G:\Gestao\Qualidade\Procedimentos\N.COTIC.002_PRD\Anexo II.xlsx** deste Plano, consolida os sistemas, serviços, componentes de infraestrutura e demais ativos tecnológicos da CGE/CE classificados conforme seu nível de importância para a continuidade operacional da instituição. A matriz organiza, de forma objetiva, informações como classificação de criticidade, tempos de recuperação (RTO), pontos de recuperação aceitáveis (RPO), áreas responsáveis e dependências tecnológicas, permitindo definir prioridades de restauração em cenários de desastre.

5.5 Priorização para Recuperação

Com base na matriz de criticidade, os ativos devem ser priorizados da seguinte forma:

a) Serviços Críticos essenciais ao cumprimento da missão institucional;
b) Sistemas que suportam atividades regulatórias, legais e de controle;
c) Sistemas corporativos de uso interno;
d) Aplicações administrativas e de apoio;

5.6 Revisão Periódica da Classificação

A classificação dos ativos críticos deve ser revisada:

a) sempre que houver inclusão ou descontinuação de sistemas;
b) quando houver mudanças na arquitetura de TI;
c) após incidentes significativos;
d) ao menos **uma vez por ano**;

6. PROCEDIMENTOS DE RECUPERAÇÃO

Controladoria e Ouvidoria Geral do Estado
Av. Gal. Afonso Albuquerque Lima – Ed. Seplag - 2ºandar - Cambeba • CEP: 60.822-325
Fortaleza / CE • Fone: (85) 3101.3471

Os Procedimentos de Recuperação descrevem, de forma detalhada e operacional, as ações necessárias para restabelecer a infraestrutura tecnológica, os sistemas corporativos e os serviços essenciais da CGE/CE após a ocorrência de um desastre. Esses procedimentos orientam tecnicamente as equipes responsáveis, garantindo padronização, previsibilidade e rastreabilidade das atividades realizadas. Cada etapa deve ser registrada em formulários próprios, assegurando documentação adequada para auditoria, melhoria contínua e governança de TIC.

6.1 Recuperação de Servidores Físicos

Inclui servidores dedicados, appliances de segurança, equipamentos críticos de armazenamento e dispositivos essenciais para sustentação do ambiente.

Seguem as principais ações:

a) **Inspeção física completa dos equipamentos**: Verificar condições do ambiente (temperatura, umidade, presença de água/fumaça), Checar integridade visual do servidor (painéis, LEDs de alerta, cabos, portas) e Confirmar disponibilidade de energia elétrica estável e funcionamento de no-breaks/UPS;
b) **Validação de componentes críticos:** Verificar funcionamento de controladoras RAID e status dos discos, Checar fontes redundantes, ventiladores, módulos de memória e placas de expansão e Certificar integridade do storage local (LUNs, volumes, saúde de discos)**.**
c) **Reativação segura do equipamento**: Iniciar boot observando mensagens de erro críticas no POST, Acessar BIOS/UEFI para verificar integridade, hora do sistema e configurações padrão e Aplicar atualizações de firmware se documentado nos procedimentos.
d) **Restauração do sistema operacional**: Restaurar imagem do servidor (bare metal recovery), quando aplicável, Reconfigurar drivers, pacotes e serviços essenciais e Revalidar partições, volumes lógicos e mapeamento **de discos;**
e) **Testes pós-restauração**: Validar conectividade (rede, DNS, gateway), Testar autenticação no domínio/serviços de identidade e Confirmar funcionamento dos serviços hospedados.

Controladoria e Ouvidoria Geral do Estado
Av. Gal. Afonso Albuquerque Lima – Ed. Seplag - 2ºandar - Cambeba • CEP: 60.822-325
Fortaleza / CE • Fone: (85) 3101 3471

6.2 Recuperação de Máquinas Virtuais (VMs)

Inclui máquinas virtuais hospedadas em ambientes de virtualização locais ou em nuvem, contemplando servidores, aplicações e serviços essenciais. Seguem as principais ações:

a) Verificação inicial do ambiente virtual:

- Confirmar se o servidor de virtualização (hypervisor) está funcionando normalmente;
- Checar se o armazenamento onde ficam os discos das VMs está íntegro e acessível;
- Validar se há recursos disponíveis (CPU, memória e rede) para iniciar ou recuperar a VM.

b) Avaliação do estado da máquina virtual:

- Verificar se os discos virtuais, snapshots ou pontos de restauração estão íntegros;
- Checar as configurações de rede virtual (interface, VLAN e conectividade);
- Confirmar se a configuração da VM (CPU, memória, disco) está compatível com o ambiente atual.

c) Reativação segura da VM:

- Iniciar a máquina virtual observando possíveis mensagens de alerta durante o boot;
- Verificar se o sistema operacional inicia corretamente e se não há erros críticos;
- Aplicar ajustes necessários, como ferramentas de integração ou drivers recomendados pelo hypervisor.

d) Restauração da VM, caso necessário:

- Restaurar a VM a partir de backup, snapshot ou imagem mais recente disponível;

Controladoria e Ouvidoria Geral do Estado
Av. Gal. Afonso Albuquerque Lima – Ed. Seplag - 2ºandar - Cambeba • CEP: 60.822-325
Fortaleza / CE • Fone: (85) 3101 3471

- Revalidar configurações de hardware virtual após a restauração;
- Ajustar serviços, aplicações e configurações internas que possam ter sido impactadas.

e) Testes pós-restauração:

- Validar conectividade de rede, DNS, gateway e comunicação com demais sistemas;
- Confirmar login, autenticação e funcionamento do sistema operacional;
- Garantir que todos os serviços e aplicações hospedados na VM funcionem corretamente.

6.3 Recuperação de Banco de Dados

Inclui ambientes de banco de dados executados em servidores físicos, máquinas virtuais ou infraestrutura em nuvem, especificamente para PostgreSQL e Microsoft SQL Server.

Seguem as principais ações:

a) Verificação inicial do ambiente:

- Confirmar se o servidor ou máquina virtual onde o banco está instalado está funcionando corretamente;
- Verificar se o armazenamento onde ficam os arquivos do banco está íntegro e acessível;
- Validar se há recursos suficientes (CPU, memória e espaço em disco) para reativação.

b) Avaliação do estado do banco de dados:

- Checar se os arquivos de dados e logs estão íntegros e sem sinais de corrupção;
- Garantir que os serviços do PostgreSQL ou SQL Server estejam disponíveis para iniciar a recuperação;
- Validar conexões de rede, portas e permissões necessárias para o funcionamento do banco.

c) Reativação segura do serviço:

Controladoria e Ouvidoria Geral do Estado
Av. Gal. Afonso Albuquerque Lima – Ed. Seplag - 2ºandar - Cambeba • CEP: 60.822-325
Fortaleza / CE • Fone: (85) 3101 3471

- Iniciar o banco de dados observando possíveis alertas ou mensagens de erro durante o processo;
- Validar configurações essenciais, como caminhos dos arquivos, parâmetros de inicialização e permissões;
- Aplicar ajustes ou atualizações previstas nos procedimentos, caso necessário.

d) Restauração dos dados:

- Restaurar o banco a partir do backup mais recente disponível (completo, incremental ou ponto no tempo);
- Reaplicar arquivos de log ou etapas de recuperação para garantir que o banco volte ao estado mais próximo possível do momento do incidente;
- Validar a consistência dos dados após a restauração.

e) Testes pós-restauração:

- Confirmar acesso ao banco e às credenciais de autenticação;
- Validar leitura e gravação de dados para garantir funcionamento adequado;
- Testar as aplicações que dependem do banco e confirmar que todas conseguem se conectar normalmente.

6.4 Recuperação da Infraestrutura de Rede

a) Checagem inicial:

- Verificar se os equipamentos de rede estão ligados e funcionando;
- Conferir cabos, portas, energia e links de internet/VPN.

b) Avaliar o estado dos equipamentos:

- Ver se as configurações de switches, firewalls e roteadores estão OK;
- Confirmar se serviços básicos (DHCP, DNS interno, VLANs, regras de firewall) estão ativos.

c) Reativação da rede:

- Reiniciar equipamentos com falha, se necessário;

Controladoria e Ouvidoria Geral do Estado
Av. Gal. Afonso Albuquerque Lima – Ed. Seplag - 2ºandar - Cambeba • CEP: 60.822-325
Fortaleza / CE • Fone: (85) 3101.3471

- Restaurar configurações de backup caso algo tenha sido perdido;
- Validar rotas internas e externas.

d) Restauração de componentes:

- Reaplicar configurações importantes (ACLs, NAT, VPNs, segmentação);
- Garantir que conexões entre sites e túneis VPN voltem ao normal.

e) Testes finais:

- Testar comunicação entre servidores, sistemas e usuários;
- Verificar acesso à internet, VPN, aplicações e serviços internos;
- Monitorar a rede para confirmar estabilidade.

7. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

A Gestão de Riscos de Segurança da Informação constitui um componente essencial para garantir a resiliência, a continuidade e a proteção dos ativos tecnológicos da Controladoria e Ouvidoria Geral do Estado do Ceará (CGE/CE). Este processo permite identificar, avaliar, tratar e monitorar riscos que possam comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, especialmente em cenários de desastre.

A gestão de riscos aplicada ao PRD tem como principais objetivos:

a) **Identificar ameaças** capazes de gerar indisponibilidade significativa dos ambientes de TI.
b) **Avaliar vulnerabilidades** que possam aumentar o impacto de incidentes ou desastres.
c) **Determinar impactos operacionais, legais, de privacidade e reputacionais**, especialmente quando o desastre envolve tratamento de dados pessoais.
d) **Definir ações de mitigação**, preventivas e corretivas, que aumentem a resiliência da infraestrutura.
e) **Apoiar a priorização de ativos**, permitindo orientar o RTO (Recovery Time Objective) e o RPO (Recovery Point Objective).

Controladoria e Ouvidoria Geral do Estado
Av. Gal. Afonso Albuquerque Lima – Ed. Seplag - 2ºandar - Cambeba • CEP: 60.822-325
Fortaleza / CE • Fone: (85) 3101 3471

f) **Fornecer insumos para decisões estratégicas**, assegurando que a recuperação seja baseada em critérios de risco.

Os riscos de segurança da informação relacionados ao ambiente da CGE/CE encontram-se mapeados, analisados e classificados no documento localizado no caminho G:\CEINS\Gestão de Riscos\gestão de riscos de segurança da informação.xls.

8. CONTROLE DE REGISTRO DA QUALIDADE

Identificação	Armazenamento	Proteção	Recuperação		Retenção	Disposição
			Indexação	Acesso		
Plano de Recuperação a Desastres da CGE	Arquivo digital: diretório de rede da Cotic e Codip	Backup	Cronológica	Cotic e Codip	Permanente	Manutenção em backup

9. REVISÃO

Esta norma será validada ou revisada sempre que necessário, em decorrência do processo de melhoria contínua do Sistema de Gestão da Qualidade.

10. APROVAÇÃO

NOME	FUNÇÃO
Marcelo de Sousa Monteiro	Presidente do Comitê de Integridade, Riscos e Qualidade

11. REFERÊNCIAS BIBLIOGRÁFICAS

Decreto Estadual nº 33.805, de 09 de novembro de 2020. Institui a Política de Gestão de Riscos do Poder Executivo do Estado do Ceará;

Decreto Estadual 34.100/2021. Institui a Política Estadual de Segurança da Informação do Poder Executivo do Estado do Ceará.

Controladoria e Ouvidoria Geral do Estado
Av. Gal. Afonso Albuquerque Lima – Ed. Seplag - 2ºandar - Cambeba • CEP: 60.822-325
Fortaleza / CE • Fone: (85) 3101.3471