Plano de Recuperação de Desastres (Disaster Recovery Plan)

Código do Documento: PLN-DST-RCV-025	Versão: 1.0
Data de Emissão: Janeiro de 2026	Classificação de Informação: Uso Interno / Clientes / Auditoria
Área Responsável: Infraestrutura, Cloud & DevOps	Aplica-se a: Todos os Serviços, Bancos de Dados e Aplicações

1. OBJETIVO

Este documento estabelece a política, os procedimentos e as diretrizes técnicas de Recuperação de Desastres (*Disaster Recovery*) aplicáveis aos serviços prestados pela organização. Seu propósito é assegurar a restauração das operações em caso de indisponibilidades críticas, falhas catastróficas de infraestrutura, desastres naturais ou incidentes graves de segurança.

2. ESTRATÉGIA DE INFRAESTRUTURA EM NUVEM (AWS)

A arquitetura de hospedagem adota serviços gerenciados nativos da Amazon Web Services (AWS), projetada com redundância e alta disponibilidade por padrão:

- Computação (ECS / Fargate): Contêineres de aplicação implantados de forma distribuída em múltiplas Zonas de Disponibilidade (Multi-AZ), garantindo resiliência contra falhas em data centers individuais.
- Banco de Dados (Amazon RDS / MySQL): Utilização de instâncias Multi-AZ com replicação síncrona automática para um ambiente secundário e criação de snapshots periódicos gerenciados pelo AWS Backup.
- Entrega e Armazenamento (CloudFront & S3): Distribuição global de conteúdo estático via CDN (CloudFront) e armazenamento resiliente de objetos com replicação de dados.

3. MÉTRICAS CHAVE DE CONTINUIDADE (RPO E RTO)

O plano de recuperação fundamenta-se nas seguintes metas de nível de serviço para ambientes críticos de produção sendo as métricas e definições em documento próprio.

4. PROCEDIMENTOS DE BACKUP E RESTAURAÇÃO

4.1. Política de Backup Automatizado

- Snapshots de Banco de Dados: Capturas diárias retidas por 30 dias com habilitação de *Point-in-Time Recovery* (PITR), permitindo a restauração do banco de dados para qualquer segundo dentro do período de retenção.
- Infraestrutura como Código (IaC): Definições de infraestrutura, redes e contêineres mantidas em repositórios controlados no GitHub, permitindo a reconstrução automatizada do ambiente.
- Criptografia e Proteção: Todos os dados em repouso e backups são criptografados utilizando chaves gerenciadas via AWS KMS.

4.2. Fluxo de Restauração em Caso de Desastre

1. Identificação e Declaração de Incidente: Detecção do evento crítico via monitoramento de disponibilidade e acionamento da equipe de DevOps.
2. Isolamento da Origem: Bloqueio das entradas comprometidas ou redirecionamento de tráfego de rede via DNS/CloudFront.
3. Restauração da Base de Dados: Provisionamento de uma nova instância RDS a partir da réplica limpa ou do snapshot mais recente (PITR).
4. Redeployment dos Serviços: Execução das pipelines de CI/CD para subir os contêineres das aplicações no ECS Fargate apontando para a nova base.
5. Validação e Testes de Fumaça: Verificação da integridade das rotas, serviços de autenticação e persistência de dados antes da liberação.
6. Redirecionamento de Tráfego: Alteração dos registros de DNS para restabelecer o serviço para os usuários finais.

5. TESTES E AUDITORIA PERIÓDICA

A eficácia do Plano de Recuperação de Desastres é validada periodicamente por meio de:

- Simulação de Restauração: Testes semestrais de recuperação da base de dados e reprovisionamento de contêineres em ambiente de homologação (*Stage*);
- Revisão de Políticas: Atualização anual deste documento ou sempre que houver mudanças relevantes na arquitetura do sistema.

Revisão #3
Criado 2026-09-03 19:53:38 UTC por Marcio Klitzke
Atualizado: 2026-09-04 17:51:33 UTC por Marcio Klitzke