Infraestrutura

Documentação de Continuidade de Negócios e Segurança

Definições de RTO/RPO

1. Resumo da Infraestrutura

A plataforma SISMETRO utiliza atualmente o motor de banco de dados MySQL 8.4 hospedado na Amazon Web Services (AWS) na região São Paulo (sa-east-1).
A arquitetura foi desenhada para garantir que os dados estejam sempre disponíveis e protegidos contra falhas de hardware ou desastres geográficos.

2. Objetivos de Recuperação (Métricas Principais)

Métrica	Objetivo	Descrição
RTO (Tempo de Recuperação)	**1 Hora**	Tempo máximo para o sistema voltar a operar após uma falha crítica na instância principal.
RPO (Ponto de Recuperação)	**Próximo a Zero**	Quantidade máxima de dados que podem ser perdidos. Graças à replicação síncrona, a perda é virtualmente nula.

3. Estratégias de Resiliência Aplicadas

A. Alta Disponibilidade (Multi-AZ)
Diferente de servidores convencionais, o nosso banco de dados opera em modo Multi-AZ (Multi-Availability Zones).

- **Replicação Síncrona:** Cada dado gravado no banco principal (sa-east-1a) é replicado instantaneamente para uma instância de reserva (standby) em uma zona isolada (sa-east-1c).
- **Failover Automático:** Se a zona principal sofrer uma interrupção, o AWS RDS detecta a falha e redireciona todo o tráfego para a reserva automaticamente em cerca de 60 segundos, sem necessidade de intervenção manual ou alteração de configurações pelos usuários.

B. Política de Backup e Retenção
Utilizamos o AWS Backup para garantir camadas extras de proteção:

- **Snapshots Diários e Horários:** Mantemos um histórico rigoroso de snapshots (capturas de estado) criados automaticamente a cada hora.

- **Point-in-Time Recovery (PITR):** Podemos restaurar o banco de dados para qualquer segundo específico dos últimos 7 dias. Isso protege o cliente não apenas contra falhas técnicas, mas também contra erros humanos (como exclusões acidentais de dados).

C. Performance e Segurança
Armazenamento gp3: Utilizamos volumes SSD de última geração com IOPS provisionados, garantindo que a recuperação e o processamento de dados ocorram na velocidade máxima permitida pela tecnologia atual.

Criptografia: Todos os dados, tanto em repouso quanto nos backups, são criptografados usando chaves AES-256 (AWS KMS).

Atualizado 18/03/2026.

Separação de dados Multi-tenant

A arquitetura de isolamento por chaves de identificação (também conhecida como *Logical Multi-tenancy* ou *Row-Level Isolation*) é uma estratégia robusta e eficiente para sistemas SaaS que utilizam uma base de dados compartilhada.

1. O Conceito de Isolamento Lógico

Diferente de modelos onde cada cliente tem seu próprio banco de dados (o que elevaria drasticamente o custo de infraestrutura no AWS RDS), o SISMETRO utiliza um Banco de Dados Consolidado.

- **A Chave de Identificação:** Cada tabela que contém dados sensíveis ou de clientes possui uma coluna identificadora (tenant_id).
- **Filtro em Camada de Aplicação:** O isolamento ocorre no nível do código (Aplicação). Toda e qualquer consulta ao banco de dados é automaticamente "carimbada" com o ID do cliente logado (tenant_id), garantindo que um Cliente A jamais visualize registros do Cliente B, mesmo estando na mesma tabela física.

2. Vantagens Estratégicas para o Cliente

Ao descrever isso para um fornecedor ou auditoria, os pontos de destaque são:

- **Segurança de Dados:** O isolamento é garantido por políticas globais no código, o que minimiza o erro humano de esquecer um filtro em uma consulta específica.
- **Performance Consistente:** Utilizando de instâncias potentes, replicadas e armazenamento extensível, o ganho de escala beneficia todos os clientes. O banco de dados consegue gerenciar índices globais de forma muito mais performática do que centenas de pequenos bancos separados.
- **Agilidade em Atualizações:** Quando é atualizada a estrutura do banco (migrações), todos os clientes recebem as melhorias de segurança e performance simultaneamente.