Plano de Recuperação de Desastres (DRP) - Software Controlap

Projeto: Controlap - Sistema de Controle de Franquias da Cacau Show
Versão: 1.0
Data: 05 de Novembro de 2025

1. Principais objetivos de um plano de recuperação de desastres

O principal objetivo deste **Plano de Recuperação de Desastres (DRP)** é garantir a **continuidade de negócios** para as franquias da Cacau Show, minimizando o impacto de qualquer interrupção nos sistemas de informação do software **Controlap**. O Controlap é um sistema de missão crítica que gerencia o estoque e o ambiente (luz, AC, prateleiras) das lojas.

As metas de recuperação são definidas para atender à **baixa tolerância a riscos** das franquias e do Patrocinador:

Métrica	Objetivo	Descrição
RTO (Recovery Time Objective)	**4 horas**	Tempo máximo aceitável para restaurar as funções críticas do sistema (controle de estoque e PDV) após uma interrupção.
RPO (Recovery Point Objective)	**15 minutos**	Perda máxima de dados aceitável. Os backups devem ser realizados e replicados a cada 15 minutos.
Disponibilidade	**99.9%**	Garantir que o sistema esteja operacional na maior parte do tempo, refletindo a baixa tolerância a riscos operacionais.

2. Pessoal (Equipe de Recuperação de Desastres)

A equipe de recuperação é a primeira linha de defesa e é composta por membros-chave com responsabilidades específicas durante uma crise.

Papel	Responsabilidade Primária no DRP	Membro da Equipe	Contato de Crise
Gerente de Crise (GC)	Liderar a resposta, comunicar o status às partes interessadas e autorizar a execução do DRP.	Gerente de Projeto (Bruno Costa Dourado)	[Telefone/Email de Crise]
Líder Técnico (LT)	Coordenar a equipe técnica, diagnosticar a causa raiz e supervisionar a execução dos procedimentos de recuperação.	Líder Técnico	[Telefone/Email de Crise]
Equipe de Infraestrutura (EI)	Restaurar a infraestrutura de rede, servidores e conectividade IoT.	Gerente de Infra	[Telefone/Email de Crise]
Equipe de Desenvolvimento (ED)	Restaurar e validar o software, aplicar patches e garantir a integridade dos dados.	Arquiteto de Software	[Telefone/Email de Crise]

Procedimento de Notificação: Em caso de desastre, o GC será notificado pelo monitoramento automático ou por reclamações de franquias. O GC acionará o LT e a EI em até 15 minutos.

3. Perfil do aplicativo (Controlap)

O Controlap é um sistema de **missão crítica** com os seguintes módulos:

Módulo	**Função Crítica**	**Impacto de Falha (Classificação de Risco)**
Estoque e PDV	Sincronização de vendas e inventário em tempo real.	**Extremo** (Perda de vendas e controle)
IoT	Controle de sensores de luz, temperatura (AC) e prateleiras.	**Extremo** (Perda de controle operacional)
Segurança	Autenticação, criptografia e proteção de dados sensíveis.	**Alto** (Vazamento de dados)

4. Perfil de estoque (Infraestrutura Crítica)

A infraestrutura do Controlap é híbrida (Cloud + On-Premise nas lojas).

Item	**Tipo**	**Localização**	**Requisito de Recuperação**
Servidor Central	Servidor de Aplicação/Banco de Dados	Data Center (Cloud)	Redundância e Failover Automático (Hot Site)
Dispositivos IoT	Sensores, Controladores de AC, Gateways	Franquias (Lojas)	Redundância de Sensores (TEC-001)
Rede de Comunicação	Internet (Principal) e Backup (Rede Móvel)	Franquias (Lojas)	Backup de Conexão (TEC-002)
Backup de Energia	UPS/Geradores	Franquias (Lojas)	Mitigação de Interrupção de Energia (EXT-001)

5. Procedimentos de backup dos serviços de informação

O procedimento de backup é fundamental para garantir o RPO de 15 minutos.

1. **Backup de Dados (Banco de Dados):**
    - **Frequência:** Backups incrementais a cada **15 minutos**. Backups completos diários.
    - **Localização:** Armazenamento primário no Data Center principal e replicação imediata para um Data Center geograficamente distinto (estratégia de Mitigação/Prevenção).
2. **Backup de Configuração e Código:**
    - **Frequência:** Backup do código-fonte e arquivos de configuração (incluindo chaves de criptografia) é realizado a cada *commit* no repositório Git e espelhado em um serviço de armazenamento seguro.
3. **Teste de Restauração:** Um teste de restauração completo é realizado **trimestralmente** para validar o RPO e o RTO.

6. Procedimentos de recuperação de desastres (Cenários de Resposta)

Estes procedimentos detalham a resposta a desastres de alta prioridade.

Cenário A: Falha Crítica de Hardware/Software no Servidor Central (Extremo)

Passo	**Ação de Recuperação**	**Responsável**
1. Detecção e Acionamento	GC é notificado. Aciona o DRP.	GC
2. Failover	EI inicia o processo de *failover* para o servidor de *standby* no Hot Site.	EI
3. Restauração de Dados	ED verifica a integridade dos dados e aplica o último backup (RPO de 15 minutos).	ED
4. Validação	LT e ED validam as funções críticas (Estoque e IoT) e liberam o acesso.	LT, ED

Cenário B: Falha Massiva de Sensores IoT em uma Franquia (Extremo)

Passo	Ação de Recuperação	Responsável
1. Detecção	Sistema identifica perda de comunicação com múltiplos sensores (TEC-001).	LT
2. Modo Manual	GC instrui a franquia a operar os sistemas de luz e AC em **modo manual** (procedimento de contingência).	GC
3. Substituição	EI aciona o fornecedor para a substituição imediata dos sensores.	EI

7. Plano de recuperação para o site móvel (Procedimento de Contingência Local)

O "site móvel" refere-se à capacidade de uma franquia operar em um modo degradado ou manual em caso de falha total da conectividade ou do sistema IoT local.

1. **Ativação do Modo de Contingência:** Se a conectividade principal e o backup falharem (TEC-002), a franquia deve:
    - **Estoque/PDV:** Utilizar o PDV em modo *offline* (se suportado) ou registrar vendas manualmente.
    - **IoT:** Operar luzes e AC manualmente (instrução do GC).
2. **Registro de Transações:** Todas as transações manuais devem ser registradas em um log local para posterior sincronização.
3. **Sincronização:** Assim que a conectividade for restaurada, a ED deve garantir que o log de transações manuais seja sincronizado com o servidor central.

8. Plano de recuperação para hot site (Estratégia de Data Center)

O Controlap utiliza uma estratégia de **Hot Site** para o servidor central, garantindo o RTO de 4 horas.

- **Definição:** Um ambiente de Data Center secundário, totalmente configurado e pronto para assumir a carga de trabalho em caso de falha do Data Center principal.
- **Tecnologia:** Utilização de replicação de banco de dados em tempo real e *load balancing* para redirecionar o tráfego automaticamente.

- **Acionamento:** O *failover* para o Hot Site é o primeiro passo no Cenário A (Falha Crítica de Servidor).

9. Restaurando todo o sistema

O procedimento de restauração completa é acionado após um desastre que exija a reconstrução total do ambiente.

1. **Reconstrução da Infraestrutura:** A EI provisiona novos servidores e infraestrutura de rede no Data Center de recuperação.
2. **Restauração do Sistema Operacional e Aplicação:** A EI instala o sistema operacional e a ED implanta a última versão do software Controlap a partir do backup de código-fonte.
3. **Restauração de Dados:** A ED restaura o backup de dados mais recente (RPO de 15 minutos) no novo banco de dados.
4. **Validação Pós-Restauração:** O LT executa um conjunto completo de testes de regressão e validação de dados antes de liberar o sistema para as franquias.

10. Processo de reconstrução (Retorno ao Site Principal)

Após a recuperação no Hot Site (Seção 8), o processo de reconstrução visa restaurar o Data Center principal e retornar as operações a ele.

1. **Análise da Causa Raiz:** O LT e a EI analisam a falha no site principal e corrigem o problema.
2. **Reconstrução do Site Principal:** A EI reconstrói a infraestrutura do site principal.
3. **Replicação Reversa:** Os dados atualizados no Hot Site são replicados de volta para o site principal.
4. **Failback:** O LT e a EI agendam uma janela de manutenção para realizar o *failback* (retorno das operações) para o site principal, garantindo que o processo seja transparente para as franquias.

11. Testando o plano de recuperação de desastres

O teste é crucial para garantir a eficácia do DRP.

Tipo de Teste	Frequência	Objetivo	Responsável
Teste de Mesa (Walkthrough)	Semestral	Revisar o DRP com a equipe, garantindo que todos conheçam seus papéis.	GC
Teste de Simulação	Anual	Simular um desastre (ex: Cenário A) e executar o DRP sem interromper as operações reais.	LT
Teste de Restauração	Trimestral	Validar o RPO e o RTO, restaurando dados em um ambiente isolado.	ED

12. Reconstrução do site do desastre (Procedimento Pós-Desastre)

Este procedimento é executado após a estabilização das operações no site de recuperação (Hot Site).

1. **Avaliação de Danos:** O GC e a EI avaliam os danos físicos e lógicos no site do desastre.
2. **Aquisição de Equipamentos:** A EI adquire e instala novos equipamentos, se necessário.
3. **Configuração:** A EI configura o novo ambiente para que ele possa servir como o novo Hot Site ou retornar à função de site principal (Seção 10).
4. **Documentação:** O GC documenta todas as lições aprendidas e os custos incorridos.

13. Registro de mudanças de plano

O DRP é um documento vivo. Qualquer alteração deve ser registrada e aprovada.

Data	**Versão**	**Descrição da Mudança**	**Autor da Mudança**	**Aprovação (GC)**
12/09/2025	1.0	Criação inicial do Plano de Gerenciamento de Riscos (Base para o DRP).	Bruno Costa Dourado	Pedro
05/11/2025	2.0	Inclusão das 13 seções do guia IBM e detalhamento dos planos de Hot Site e Site Móvel.	João Vitor Leão Bonifácio	Pedro