

# Plano de Recuperação de Desastres

## 1. Metas Principais do DRP

- **Objetivo:** Restaurar as funcionalidades críticas de automação (subir/descer carretéis, controle do ar-condicionado e solda, registro de ferramentas) em um prazo aceitável após um desastre
- **Tempo Máximo de Inatividade (RTO):** 2 horas para funcionalidades críticas
- **Perda Máxima de Dados (RPO):** 1 dia (baseado na frequência de backup do servidor/configurações do ESP32)

## 2. Equipe de Recuperação

Função	Responsabilidade Primária	Membro
Desenvolvedor Backend	Recuperação do Webserver (código, BD, ambiente)	Giulia Nogueira Lopes De Sa / Gustavo Marcello Correa De Araujo
Desenvolvedor Embarcado (ESP32)	Reprogramação e reconfiguração dos ESP32, hardware	Vinicius Binda
Técnico de Infraestrutura	Rede, energia, substituição física de componentes	Guilherme Alves De Oliveira / Joao Pedro Lima Paulo

### 3. Perfil do Aplicativo

Sistema/Função	Crítico	Dependências	RTO	Notas
Controle de Carretéis	Sim	ESP32, Relés, Servidor	2 horas	Essencial para o uso seguro das bancadas.
Controle de Bancadas de Solda	Sim	ESP32, Relés, Servidor	2 horas	Essencial para segurança e economia de energia.
Registro de Ferramentas	Não	ESP32 (sensores), Servidor	2 horas	Manutenção do inventário e controle de perdas.
Controle de Ar Condicionado	Não	ESP32 (IR), Servidor	3 horas	Conforto, pode ser controlado manualmente.
Webserver	Sim	Servidor físico, Banco de dados	2 horas	Interface de comando e registro de dados.
Servidor ESP32	Sim	Conectividade Wi-Fi, Firmware	2 horas	Interface de comunicação direta com o hardware.

## 4. Perfil do Inventário

Componente	Tipo	Localização	Backup/Estoque
Webserver	Software	Servidor principal	Repositório Git, Backup do BD (Diário)
Firmware ESP32	Software	Repositório Git	SD Card de Backup (opcional)
ESP32	Hardware	Painéis de Controle	Estoque: 2 unidades sobressalente
Sensores	Hardware	Espalhados pela sala	Estoque: 2 sensores sobressalentes
Roteador Wi-Fi	Infraestrutura	Sala de Servidores	Suprimento da TI da escola

## 5. Procedimentos de Backup

- **Código-Fonte (Server e ESP32):**
  - Frequência: Após cada alteração significativa e semanalmente
  - Método: Commit e Push para um Repositório Git
- **Banco de Dados (Registro de sensores/Logs):**
  - Frequência: Diária
  - Método: Exportação do banco de dados para um armazenamento na nuvem ou drive de rede separado
- **Configurações do ESP32:**
  - Frequência: Após qualquer mudança de rede ou lógica
  - Método: Arquivo de configuração armazenado na mesma localização do código-fonte do server

## 6. Procedimentos de Recuperação de Desastres

Cenário A: Falha no Webserver

- 1. Avaliação:** Verificar logs e status do serviço
- 2. Ação 1 (Simples):** Tentar reiniciar o serviço
- 3. Ação 2 (Grave):**
  - Clonar o repositório Git no servidor de destino (original ou alternativo)
  - Restaurar o ambiente Python (instalar dependências)
  - Importar o último backup do Banco de Dados (Seção 5)
  - Verificar a comunicação com o ESP32 (ping, porta aberta)
  - Testar as funcionalidades críticas pela interface
- 4. Verificação:** Testar a comunicação

Cenário B: Falha no ESP32 (Hardware ou Firmware Corrompido)

- 1. Avaliação:** O ESP32 está offline (Webserver não comunica) ou não responde a comandos
- 2. Ação 1 (Firmware):**
  - Conectar o programador ao ESP32 defeituoso
  - Fazer download do firmware do repositório/backup
  - Reflash no ESP32
- 3. Ação 2 (Hardware):**
  - Desligar a energia do painel de controle
  - Substituir o módulo ESP32 defeituoso por um sobressalente (Seção 4)
  - Realizar o Reflash (como na Ação 1)
- 4. Verificação:** Testar a comunicação e os atuadores (relés, motores)

Cenário C: Perda de Conectividade de Rede (Wi-Fi/Rede Local)

- 1. Avaliação:** Webserver e ESP32 não se comunicam
- 2. Ação:** Verificar o Roteador Wi-Fi (status, energia) e as configurações de IP (estáticas ou DHCP) do ESP32 e do Webserver

## 7. Plano de Recuperação para Site Móvel

- **Não aplicável (NA):** O sistema é ligado ao laboratório de ferramentas
- **Alternativa:** Caso a automação falhe, o plano é reverter para operação manual imediata:
  - Carreais: Subir/descer manualmente
  - Solda: Ligar/desligar manualmente as tomadas das bancadas
  - Ferramentas: Registro manual em papel
  - Ar Condicionado: Controle pelo controle remoto original.
- **Comunicação:** A equipe de recuperação notifica o professor/usuário do laboratório sobre a necessidade de operação manual até a recuperação total

## 8. Plano de Recuperação para Hot Site

- **Hot Site (Ambiente de Backup):** Uso de um Computador alternativo na rede da escola com o Webserver pré-instalado (ou script de instalação rápida)
- **Procedimento:** Se o servidor principal falhar, o plano é implantar o Webserver (Seção 6, Ação 2) no Hot Site. O endereço IP do Webserver deve ser atualizado no firmware do ESP32 (necessita de reflashing) ou ser um endereço DNS que possa ser reconfigurado rapidamente

## 9. Restaurando Todo o Sistema

- **Propósito:** Restaurar completamente o Webserver e o ESP32, incluindo dados e configurações, a partir do zero
1. Preparar um novo servidor
  2. Instalar o Sistema Operacional e dependências (Python, Flask, etc.)
  3. Clonar o código-fonte do Git (Seção 5)
  4. Restaurar o Banco de Dados (Seção 5)
  5. Preparar um novo ESP32 (ou reflash no existente)
  6. Fazer upload do Firmware ESP32 (Seção 5)
  7. Verificação completa de todas as funcionalidades (Carreais, Solda, Ferramentas, AC)

## 10. Processo de Reconstrução

- **Propósito:** Avaliar a causa raiz da falha (hardware, software, rede) e evitar recorrências
1. **Avaliação de Danos:** Documentar a falha (hora, causa, impacto).
  2. Correção: Implementar o procedimento de recuperação apropriado (Seção 6)
  3. **Análise Pós-Incidente:** Reunir a Equipe (Seção 2) para identificar as fragilidades
  4. **Atualização do DRP:** Se o processo de recuperação revelou falhas no DRP, atualizar as seções 4, 5 e 6

## 11. Testando o Plano de Recuperação

- **Frequência:** Após grandes mudanças no sistema
- **Tipos de Teste:**
  - **Teste de Restauração de Backup:** Tentar restaurar o banco de dados e o código-fonte em um ambiente de teste
  - **Simulação de Falha do Servidor:** Desligar o servidor Flask e cronometrar o RTO para o Hot Site (Seção 8)
  - **Simulação de Falha do ESP32:** Trocar um ESP32 em funcionamento por um "defeituoso" e cronometrar o RTO para a recuperação de firmware/hardware (Seção 6, Cenário B)
- **Documentação:** Registrar os tempos de RTO e RPO atingidos e as lições aprendidas

## 12. Reconstrução das Instalações em Caso de Situação Grave

- **Adaptação:** Aplica-se à reconstrução física dos painéis de controle e da fiação do laboratório
- **Planta Baixa:** Manter uma cópia digital da planta de fiação e localização dos relés/ESP32 em um local seguro
- **Requisitos:**
  - Alimentação elétrica para os motores dos carretéis e bancadas de solda
  - Rede Wi-Fi

## 13. Registro das Alterações ao Plano

- **Propósito:** Manter o DRP sempre atualizado e refletindo a configuração atual.

Data	Seção Afetada	Descrição da Alteração
Anualmente	4, 5, 6	Adicionado novo módulo de relé, atualizado procedimento de backup para BD
Anualmente	2, 11	Mudança na Equipe de Recuperação e cronograma de testes.
Quando houver grandes mudanças	7, 8, 9, 10	Mudança nos planos de recuperação física