Plano de Continuidade de Negócios (BCP) - Language Masters

# 1. Introdução da empresa e seu cenário

A Language Masters é uma escola de idiomas com 3 filiais localizadas em São Paulo, oferecendo cursos presenciais e online para mais de 300 alunos. A empresa possui 300 funcionários entre professores, equipe administrativa e TI. Depende fortemente de sistemas de TI para operação dos cursos, gestão acadêmica e atendimento aos alunos.

# 2. Recursos críticos identificados

* Plataforma EAD (aulas online ao vivo e gravadas);
* Sistema de gestão acadêmica (matrículas, notas, frequência);
* Infraestrutura de rede (Wi-Fi, servidores, acesso à internet nas 3 unidades);
* Banco de dados de alunos;
* Equipe de TI e Suporte técnico;
* Energia elétrica e internet nas filiais;
* Serviços de comunicação (WhatsApp, e-mail, telefone).

# 3. Análise de Impacto nos Negócios (BIA)

* Falha de internet: paralisação imediata de aulas online e comunicação com alunos.
* Ataque cibernético (ransomware): perda de acesso ao banco de dados e sistemas essenciais.
* Desastre natural (enchente): interrupção das aulas presenciais, perda de equipamentos.
* Pane elétrica prolongada: impacto nas aulas e nos sistemas de controle administrativo.
* Falha no sistema EAD: interrupção de até 70% das atividades educacionais.

# 4. Estratégias de recuperação propostas

* Backup diário em nuvem e local dos sistemas e banco de dados;
* Redundância de internet (link secundário) em cada unidade;
* Contrato com empresa especializada em resposta a incidentes cibernéticos;
* Servidores virtualizados com failover;
* Plano de comunicação de emergência com alunos e professores via canais alternativos;
* Treinamento periódico dos colaboradores sobre resposta a incidentes.

# 5. Plano de ação detalhado

1. 1. Detecção: Equipe de TI identifica o incidente e bloqueia o acesso ao sistema afetado.
2. 2. Notificação: Acionar responsáveis internos e parceiros de segurança.
3. 3. Isolamento e análise: Isolar o sistema comprometido e iniciar análise forense.
4. 4. Ativação dos backups: Restaurar dados do último backup íntegro.
5. 5. Comunicação com alunos e funcionários explicando a situação e o tempo estimado de retomada.
6. 6. Revisão e reforço das medidas de segurança após a recuperação.

# 6. Sugestão de teste do plano

Simulação de ataque ransomware: Equipe de TI e administrativa passam por um teste simulado onde o sistema EAD é 'comprometido'.  
Objetivo: verificar tempo de resposta, comunicação interna, restauração de dados e continuidade das aulas.