



Plano de Continuidade de Negócios

Kicol Tecnologia e Serviços LTDA

Documento:	Plano de Continuidade de Negócios
Versão:	1.0
Data de aprovação:	03 de março de 2026
Próxima revisão:	Março de 2027
Aprovado por:	Eduardo Macedo — Diretor / Responsável Técnico
Classificação:	Uso interno

CNPJ: 64.973.433/0001-06

Rua Alcindo Guanabara, 17, Sala 1313, Centro, Rio de Janeiro - RJ, 20031-130

1. Objetivo

Definir as estratégias e procedimentos para garantir a continuidade dos serviços prestados pela Kicol Tecnologia e Serviços LTDA em caso de interrupções, desastres ou eventos que comprometam a operação normal da empresa.

2. Escopo

Este plano se aplica a todos os serviços e sistemas mantidos pela empresa para seus clientes, incluindo aplicações web, integrações, bancos de dados e infraestrutura de hospedagem.

3. Análise de Impacto no Negócio (BIA)

Os processos críticos da empresa e seus requisitos de recuperação foram identificados:

Processo	Criticidade	RPO	RTO	WRT
Aplicações web em produção	Alta	24 horas	4 horas	2 horas
Bancos de dados de produção	Alta	24 horas	4 horas	2 horas
Repositórios de código	Média	0 (versionado)	1 hora	30 minutos
Integrações com APIs	Média	N/A	4 horas	1 hora
E-mail e comunicação	Baixa	N/A	24 horas	1 hora

RPO (Recovery Point Objective): quantidade máxima de dados que pode ser perdida, medida em tempo. Com backups diários, o RPO é de 24 horas.

RTO (Recovery Time Objective): tempo máximo aceitável para restaurar o serviço após uma interrupção.

WRT (Work Recovery Time): tempo necessário para verificar a integridade dos dados e validar o funcionamento após a restauração.

4. Cenários de Interrupção e Estratégias

4.1 Falha no servidor de hospedagem

- O provedor de hospedagem (Hostinger) possui infraestrutura redundante e SLA de disponibilidade;

- Em caso de indisponibilidade prolongada, o sistema pode ser restaurado em outro provedor a partir dos backups e do código versionado no GitHub;
- Tempo estimado de recuperação: até 4 horas.

4.2 Perda ou corrupção de banco de dados

- Restauração a partir do backup diário mais recente;
- Verificação de integridade dos dados restaurados;
- Perda máxima de dados: até 24 horas (RPO);
- Tempo estimado de recuperação: até 4 horas.

4.3 Comprometimento de segurança (invasão)

- Ativação do Plano de Resposta a Incidentes de Segurança;
- Isolamento do ambiente comprometido;
- Restauração a partir de backup íntegro anterior ao comprometimento;
- Rotação de todas as credenciais e chaves de acesso;
- Notificação ao cliente conforme previsto no Plano de Resposta a Incidentes.

4.4 Indisponibilidade do responsável técnico

Em caso de indisponibilidade temporária do responsável técnico (doença, emergência), as seguintes medidas estão previstas:

- Documentação técnica atualizada de todos os projetos e acessos;
- Credenciais de emergência armazenadas em gerenciador de senhas com acesso de recuperação configurado;
- Contato de parceiro técnico de confiança para suporte emergencial, quando necessário;
- Comunicação proativa ao cliente sobre prazos afetados.

4.5 Falha no equipamento de trabalho

- Todo o código-fonte está versionado no GitHub (repositórios privados), independente do equipamento local;
- As credenciais estão no gerenciador de senhas (Bitwarden), acessível de qualquer dispositivo;
- O acesso aos servidores é por chave SSH, que pode ser reconfigurada em novo equipamento;
- Tempo estimado para retomada: até 4 horas com novo equipamento.

5. Testes do Plano

O plano de continuidade é testado semestralmente por meio de simulações de restauração de backup e verificação dos procedimentos de recuperação. Os resultados são registrados com data, cenário testado e eventuais melhorias identificadas.

6. Comunicação de Crise

Em caso de interrupção que afete os serviços de um cliente, a comunicação é feita diretamente pelo responsável técnico ao ponto de contato do cliente, informando:

- Natureza da interrupção;
- Impacto estimado;
- Ações em andamento;
- Previsão de restabelecimento;
- Atualizações regulares até a resolução.

7. Revisão

Este plano será revisado anualmente ou após qualquer evento que ative os procedimentos de continuidade.

Versão	Data	Descrição	Responsável
1.0	03/03/2026	Versão inicial do documento	Eduardo Macedo

8. Aprovação

Eduardo Macedo

Diretor / Responsável Técnico

Kicol Tecnologia e Serviços LTDA

03 de março de 2026