Business Continuity Plan

Kicol Tecnologia e Serviços LTDA

Document:	Business Continuity Plan
Version:	1.0
Approval date:	March 3, 2026
Next review:	March 2027
Approved by:	Eduardo Macedo — Director / Technical Lead
Classification:	Internal use

CNPJ: 64.973.433/0001-06

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

1. Purpose

To define the strategies and procedures to ensure the continuity of services provided by Kicol Tecnologia e Serviços LTDA in the event of disruptions, disasters or events that compromise normal operations.

2. Business Impact Analysis (BIA)

Process	Criticality	RPO	RTO	WRT
Web applications in production	High	24 hours	4 hours	2 hours
Production databases	High	24 hours	4 hours	2 hours
Code repositories	Medium	0 (versioned)	1 hour	30 minutes
API integrations	Medium	N/A	4 hours	1 hour
Email and communication	Low	N/A	24 hours	1 hour

RPO (Recovery Point Objective): maximum acceptable data loss, measured in time. With daily backups, the RPO is 24 hours.

RTO (Recovery Time Objective): maximum acceptable time to restore service after a disruption.

WRT (Work Recovery Time): time needed to verify data integrity and validate operation after restoration.

3. Disruption Scenarios and Strategies

3.1 Hosting server failure

- The hosting provider (Hostinger) has redundant infrastructure and availability SLA;
- In case of prolonged outage, the system can be restored on another provider from backups and versioned code on GitHub;
- Estimated recovery time: up to 4 hours.

3.2 Database loss or corruption

- Restoration from the most recent daily backup;
- Restored data integrity verification;
- Maximum data loss: up to 24 hours (RPO);

- Estimated recovery time: up to 4 hours.

3.3 Security compromise (breach)

- Activation of the Security Incident Response Plan;
- Isolation of the compromised environment;
- Restoration from an intact backup prior to the compromise;
- Rotation of all credentials and access keys;
- Client notification as specified in the Incident Response Plan.

3.4 Technical lead unavailability

- Updated technical documentation for all projects and access;
- Emergency credentials stored in a password manager with configured recovery access;
- Trusted technical partner contact for emergency support when needed;
- Proactive client communication about affected timelines.

3.5 Work equipment failure

- All source code is versioned on GitHub (private repositories), independent of local equipment;
- Credentials are in the password manager (Bitwarden), accessible from any device;
- Server access is via SSH key, which can be reconfigured on new equipment;
- Estimated time to resume: up to 4 hours with new equipment.

4. Plan Testing

The continuity plan is tested semi-annually through backup restoration simulations and recovery procedure verification.

5. Crisis Communication

In case of disruption affecting a client's services, communication is made directly by the technical lead to the client's point of contact, informing the nature of the disruption, estimated impact, ongoing actions, restoration forecast and regular updates until resolution.

6. Review

This plan will be reviewed annually or after any event that activates continuity procedures.

Version	Date	Description	Owner
1.0	03/03/2026	Initial version	Eduardo Macedo

7. Approval

_____

Eduardo Macedo
Director / Technical Lead
Kicol Tecnologia e Serviços LTDA
March 3, 2026