



# METHODOLOGY AND PLAN FOR IT RISK MANAGEMENT

This document is a simplified version for technical portfolio demonstration purposes, focusing on strategic structure and alignment with COBIT, ISO, or ITIL frameworks.



**Company Name:** BioHealth Systems

**Document Type:** Methodology and Plan for  
IT Risk Management

**Reference Framework:** ISO/IEC 27005 e ISO 31000



## ● Risk Assessment Process

We follow the ISO 27005 flow:

- **Identification:** Mapping of assets (e.g., electronic medical records, cloud servers), threats (e.g., ransomware), and vulnerabilities (e.g., outdated systems).
- **Analysis:** Determination of Probability (P) and Impact (I).
- **Assessment:** Calculation of Risk Level ( $R = P \times I$ ).



## ● Impact Criteria (Example Matrix)

For BioHealth, the impact is measured in four dimensions:

- **Operational:** Interruption of surgeries or exams.
- **Legal/Compliance:** Fines from the ANPD (LGPD).
- **Reputational:** Loss of patient trust.
- **Financial:** Loss of revenue and remediation costs.

# ● Risk Register Sample

Below is a simulation of how risks are prioritized:

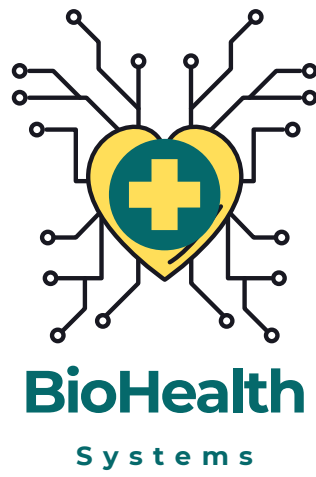
ID	Threat	Potential Impact	P	I	Level	Treatment Strategy
R-01	Ransomware Attack	Unavailability of Medical Records	4	5	20 (Critical)	Mitigate: Implement offline backups and MFA.
R-02	Data Leak	LGPD Fines and Patient Exposure	3	5	15 (High)	Mitigate: Database encryption
R-03	Power Failure (Data Center)	Temporary local system outage	2	4	8 (Medium)	Transfer: Migrate load to the cloud (SaaS).



## ● Heat Map

Risks are plotted on a 5x5 matrix:

- **Red Area (15-25):** Requires immediate action and reporting to the Executive Committee.
- **Orange Area (8-14):** Actions planned for the next quarter.
- **Yellow Area (1-7):** Accepted or monitored risk.



## ● Continuous Monitoring

Risks are not static. BioHealth conducts reviews every six months or whenever there are significant changes in the IT infrastructure.



## ● Disclaimer

This document represents a fictional case developed for professional and educational purposes and does not reflect any real organization.