

LUCAS BASTOS FRANCO – 2310622

# DevTech Solutions

## Governança em TI

Matéria: Governança de Tecnologia da  
Informação

Docente: Talles Santos

2025 – Anápolis

# SUMÁRIO

INTRODUÇÃO .....	3
SOBRE A EMPRESA .....	3
PROBLEMAS E DESAFIOS.....	3
NÍVEL DE MATURIDADE .....	3
ANÁLISE.....	3
EM SUMA .....	4
SWOT “FOFA”.....	4
FORÇAS – interno .....	4
OPORTUNIDADES – externo.....	4
FRAQUEZAS – interno .....	5
AMEAÇAS – externo .....	5
PROPOSTAS .....	5

# INTRODUÇÃO

Você é um consultor que foi contratado pela empresa DevTech com o objetivo de elevar a TI ao nível estratégico

## SOBRE A EMPRESA

Bem-vindos ao desafio da DevTech Solutions, uma empresa de desenvolvimento de software em rápido crescimento. Com 150 funcionários, a DevTech atende clientes de médio e grande porte, mas enfrenta desafios significativos em sua governança de TI.

## PROBLEMAS E DESAFIOS

1. Gestão de Processos e Projetos: Priorização ineficiente de projetos e falta de processo claro para gestão de mudanças, resultando em gargalos e retrabalho.
2. Alinhamento TI e Negócio: TI vista apenas como suporte operacional, sem participação ativa nas decisões estratégicas e sem modelo de acompanhamento de desempenho.
3. Gerenciamento de Serviços de TI: Falta de processo formalizado para atendimento de chamados e ausência de catálogo formal de serviços.
4. Gestão de Riscos e Segurança: Política de segurança não disseminada e ausência de plano estruturado de continuidade de negócios.

## NÍVEL DE MATURIDADE

### ANÁLISE

1. Gestão de Processos e Projetos: o nível dela é **ARTESANAL**, o motivo é que a empresa carece de um processo estruturado de gestão de mudança e priorização de projeto, causando gargalos e retrabalho.
2. Alinhamento TI e Negócio: o nível dela é **ARTESANAL**, o motivo é que a TI vista em suporte operacional, sem estratégias e sem KPIs<sup>1</sup>.
3. Gerenciamento de Serviços de TI: o nível dela é **EFICIENTE**, o motivo é que têm falta de processos formal de atendimento de chamados e catálogo de serviços bem definido. Entretanto, existem esforços para estruturar o setor.

---

<sup>1</sup> KPIs = Indicadores-chaves de desempenho usado para medir o sucesso de processos, serviços ou estratégia

4. Gestão de Riscos e Segurança: o nível dela é **ARTESANAL**, o motivo é que têm ausência de uma política disseminada de segurança e de plano estruturado de continuidade.

### **EM SUMA**

Com base na análise dos problemas encontrado na empresa, podemos definir que o nível dela é 1, ou seja, nível **ARTESANAL**. No nível artesanal, na área de TI, é definido por não ter processos, entretanto a empresa apresentar de priorização ineficientes. A empresa recebeu este nível, pois, a equipe de TI ainda opera sem processos e sem alinhamento. Há iniciativas em andamento, mas ainda não há uma priorização clara e metodologias bem definidas.

## **SWOT “FOFA”**

### **FORÇAS – interno**

Com base na análise, por demos perceber que:

- Crescimento acelerado
- Boa reputação no mercado
- Equipe qualificada em desenvolvimento de software
- Possui suporte operacional
- Cultura inovadora e ágil

### **OPORTUNIDADES – externo**

Com base na análise, por demos perceber que:

- Implementação de frameworks como ITIL<sup>2</sup>, COBIT<sup>3</sup> e AGILE<sup>4</sup>
- Maior participação da TI na estratégia
- Uso de ferramentas de automação
- Destaque entre seus concorrentes
- Avanço na tecnologia

---

<sup>2</sup> ITIL = Conjunto de boas práticas para gestão de serviços com foco em eficiência e qualidade

<sup>3</sup> COBIT = Framework de governança para garantir alinhamento estratégico, controle de risco e conformidade com regulamentos

<sup>4</sup> AGILE = Metodologia de desenvolvimento de software baseada em ciclos curtos

## **FRAQUEZAS – interno**

Com base na análise, por demos perceber que:

- Falta de processos estruturados
- Baixa integração da TI com o negócio
- Alinhamento da empresa
- Ausência de modelo de atendimento
- Retrabalho e atrasos impactantes

## **AMEAÇAS – externo**

Com base na análise, por demos perceber que:

- Risco de segurança devida à falta de políticas
- Impactos ao cliente por conta de atrasos
- Perda de competitividade por ineficiência
- Possível aumento de perdas de clientes
- Risco de aumento de gastos

## **PROPOSTAS**

Com base na análise, por demos implementar um framework COBIT, que fornece diretrizes para garantir alinhamento com os objetivos. Se utilizando de ITIL para estruturar processos e criar um PDTI<sup>5</sup> para estabelecer metas claras e acompanhar a evolução da governança.

Também criar um comitê estratégico de TI, envolvendo lideranças da empresa, para alinhar decisões tanto tecnológico e estratégicas aos objetivos do negócio. Definir acompanhamento KPIs e OKRs<sup>6</sup> que avaliem o impacto e adotar BSC<sup>7</sup> para traduzir a estratégia empresarial em metas de TI.

Ainda mais, podemos acrescentar uma estrutura de catálogo de serviços de TI com SLAs<sup>8</sup> bem definidos para melhorar a previsibilidade e qualidade dos serviços.

---

<sup>5</sup> PDTI = Documento estratégico que orienta investimentos, metas e ações de TI

<sup>6</sup> OKRs = Método de definição de objetivos e resultados-chave para mensurar o desempenho

<sup>7</sup> BSC = Modelo de gestão estratégica que mede o desempenho organizacional

<sup>8</sup> SLAs = Acordos de nível de serviços que estabelecem parâmetros de qualidade, tempo de resposta e disponibilidade

Adotando ferramentas como ITSM<sup>9</sup> para padronização e implementar modelos baseado em ITIL para práticas de gestão de incidentes, problemas e mudanças.

E por fim, desenvolver a disseminar uma PSI<sup>10</sup> baseada no ISO 27001<sup>11</sup>, criando um plano PCN<sup>12</sup>, seguindo a norma ISO 22301<sup>13</sup>, para garantir resiliência da empresa e promover auditorias periódicas e treinamentos sobre segurança.

---

<sup>9</sup> ITSM = Abordagem focada na entrega e gestão de serviços com qualidade, baseada em processos estruturados

<sup>10</sup> PSI = Documento que define diretrizes, normas e controle para proteger ativos de informação contra ameaças e riscos.

<sup>11</sup> ISO 27001 = norma internacional para sistemas de gestão de segurança da informação

<sup>12</sup> PCN = Estratégia que define ações e procedimentos para garantir a continuidade das operações críticas

<sup>13</sup> ISO 22301 = norma internacional que define os requisitos para uns sistemas de gestão de continuidade de negócios