SIN210
Governança em Tecnologia de Informação

Business Case Final (Solução)

Billt - Contabilidade

Bruno Brandão Borges - 2018014331
Ivan Leoni Vilas Boas - 2018009073
Leonardo Rodrigo de Sousa - 2018015965
Lucas Tiense Blazzi - 2018003310
Thiago Marcelo Passos - 2018002850

13/07/2022

BUSINESS CASE

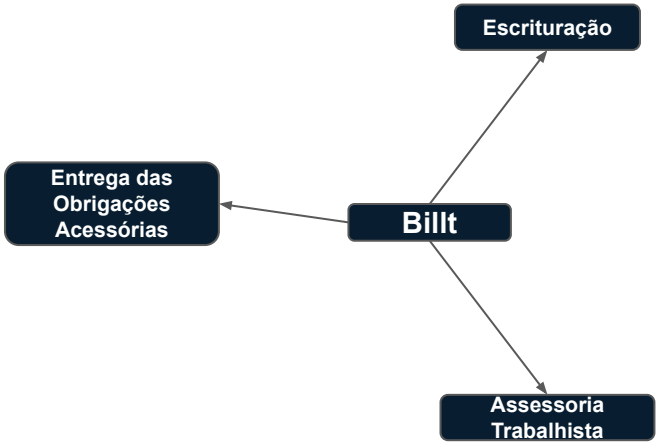
Projeto Final

Sumário

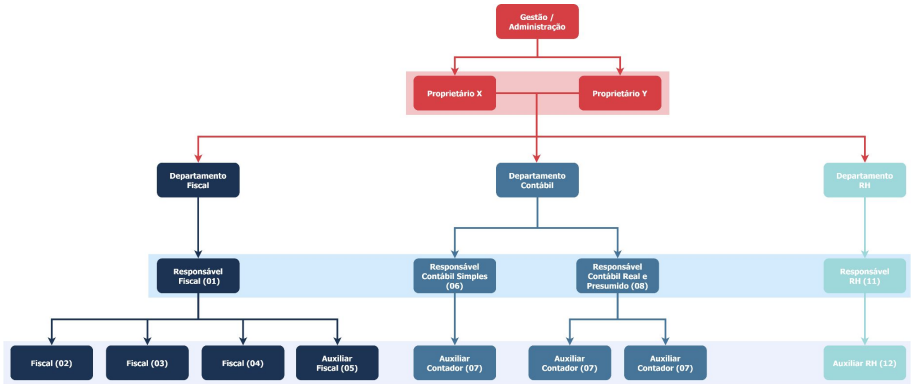
- Contextualização da empresa
- Análise do contexto - Val IT
- Fatores de Projeto - COBIT
- Cascata - Sistema de governança sob medida
- Solução - Gerenciamento de Catálogo
- Solução - Gerenciamento da Segurança
- Solução - Gerenciamento da Continuidade
- Custos da proposta
- Justificativas do investimento
- Conclusão
- Referências
- Participação dos integrantes

Contextualização

Serviços fornecidos pela Buillt

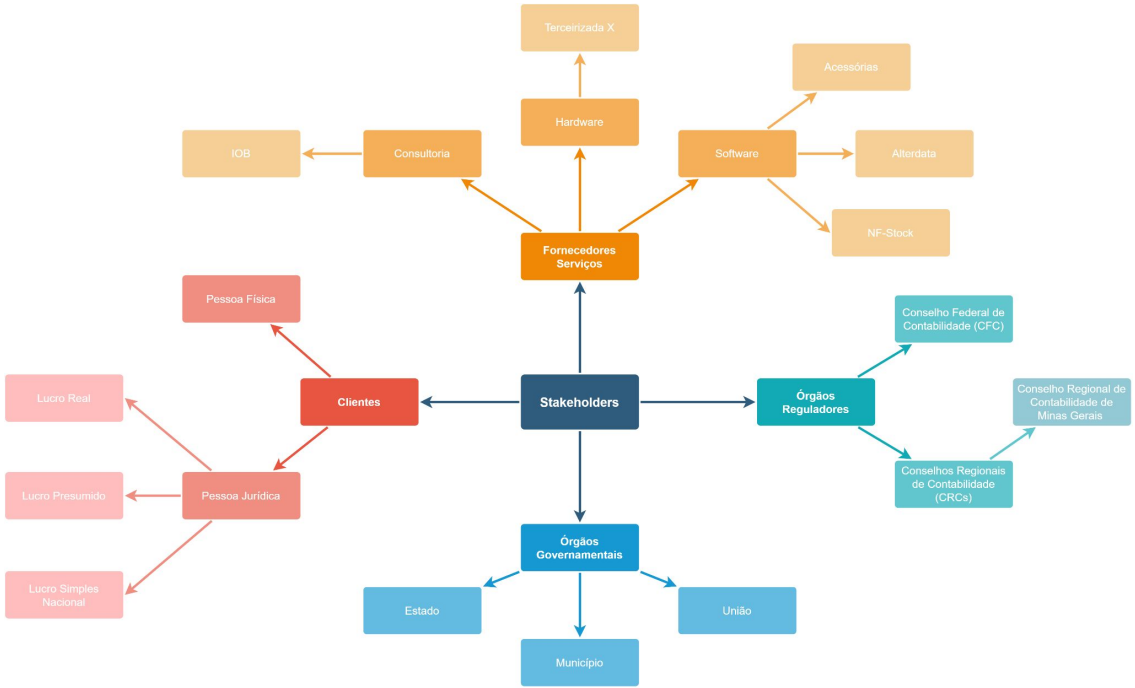


Estrutura organizacional



Contextualização

Mapa de stakeholders



Problemas encontrados

- ❌ Ausência de backups
- ❌ Ausência de softwares de proteção dos dispositivos
- ❌ Controle da transferência de arquivos pelos funcionários
- ❌ Controle de acesso em relação aos arquivos do servidor
- ❌ Conscientização / treinamento de funcionários

Contextualização

Análise dos cenários - Val IT

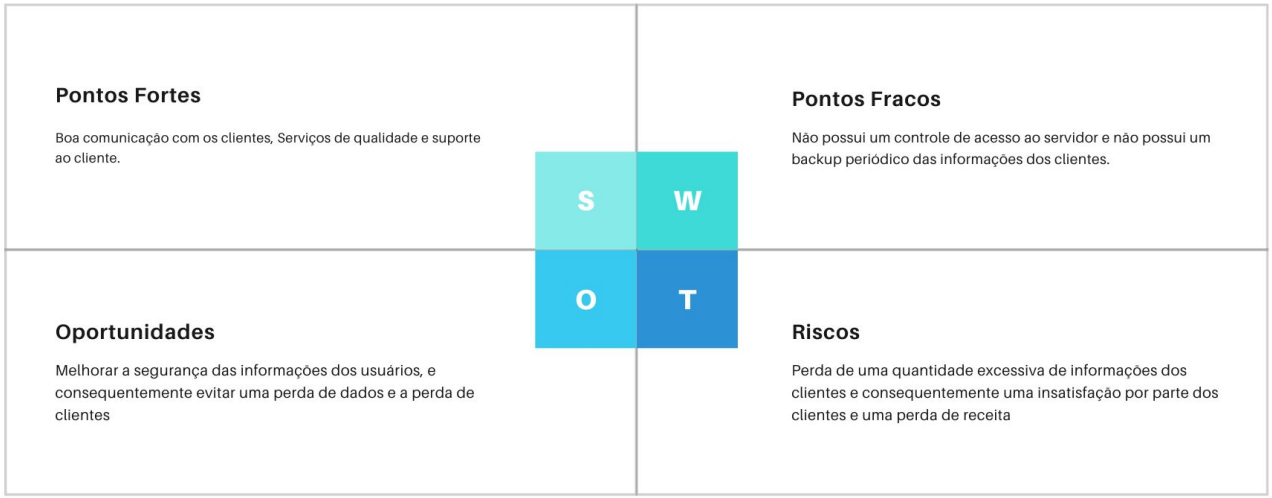
Balanced Scorecards

	Objetivos	Indicador	Iniciativas
Financeiro	Aumentar e manter a receita	Demonstrativos financeiros	Aumentar a segurança dos clientes
Cliente	- Manter a segurança das informações clientes. - Retenção dos clientes.	- Acesso as informações do cliente. - Quantidade de clientes da organização.	- Aquisição de antivírus. - Manter serviços de qualidade com segurança das informações.
Processos internos	- Controle de acesso ao sevidor. - Manter backup dos arquivos e informações dos clientes.	- número de acessos ao servidor. - Arquivos de backup.	- Aplicação para controle de acesso ao servidor. - Definir periodicidade da realização do backup
Aprendizagem	Treinar funcionários para conscientização sobre a segurança.	Conscientização em massa sobre a segurança.	Organização de treinamentos.

Análise SWOT

CONTABILIDADE

Análise SWOT de Segurança



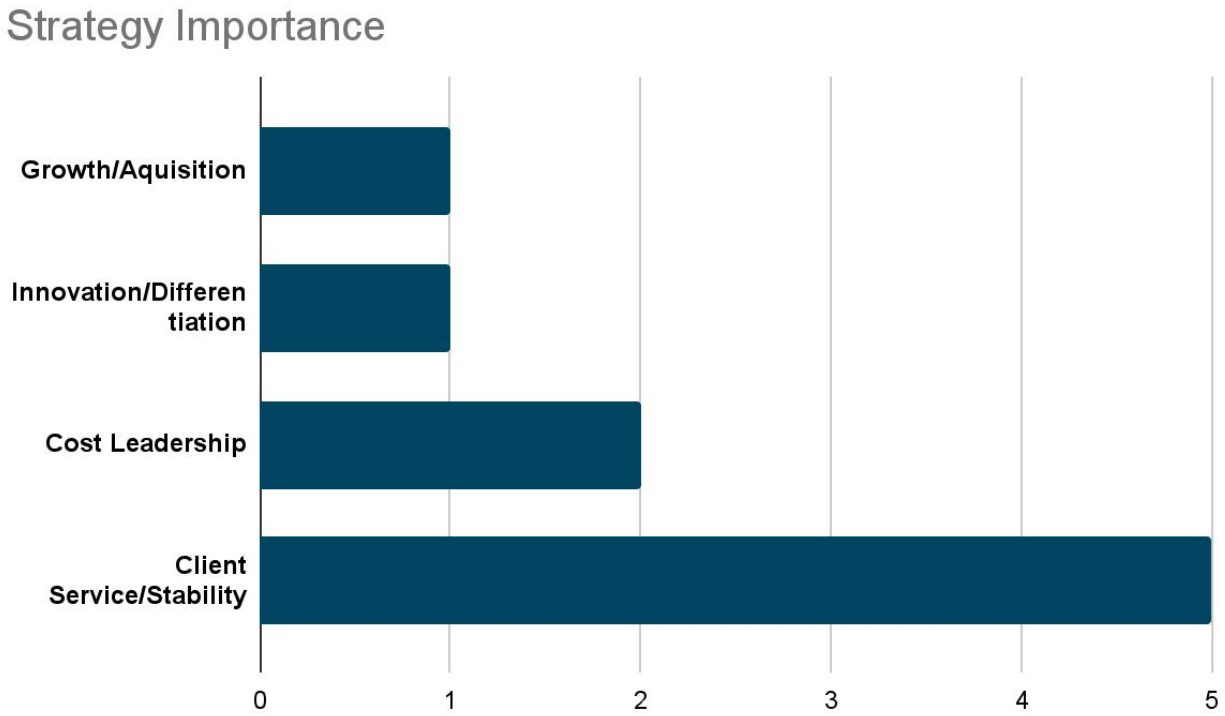
Custo benefício risco

PROBLEMA	SOLUÇÃO	BENEFÍCIOS	RISCOS
Servidores e máquinas sem uma proteção	Instalação de um antivírus nas máquinas dos funcionários e no servidor	Prevenção de um ataque ao servidor e as máquinas locais	Instalação de um antivírus com baixa proteção e servidores vulneráveis
Acesso livre aos servidores	Desenvolvimento de uma aplicação para controle de acesso ao servidor	Somente pessoas autorizadas teriam acesso ao servidor	Falha na aplicação e consequentemente uma falta de acesso ao servidor
Acesso a dados confidenciais	Treinamento para conscientização sobre segurança da informação	Funcionários com uma conscientização sobre a importância da segurança	Informações sobre como utilizar as informações de forma inapropriada
Ausência de backup das informações dos clientes	Realização automática e periódica de backup dos dados dos clientes do software alterdata no servidor	Recuperação dos dados dos clientes em caso de falha	Perda de dados entre a falha nos sistemas e a data do backup

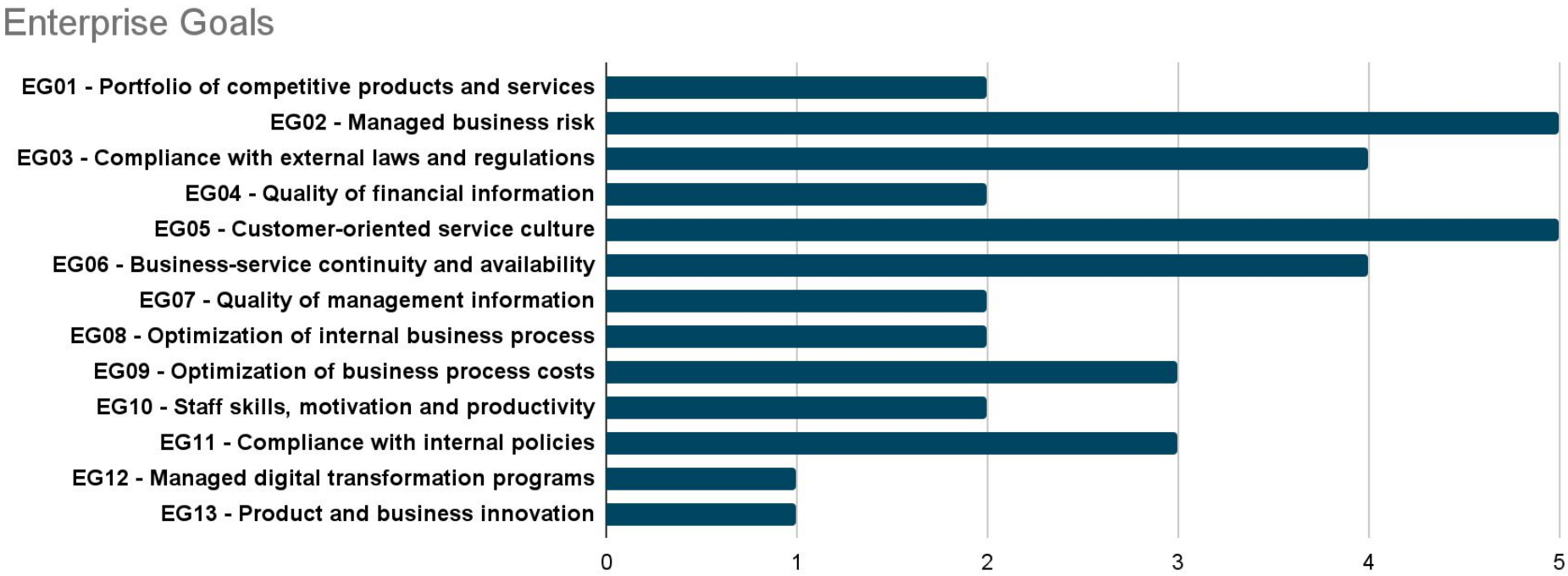
Fatores de Projeto

Mapeamento do sistema de governança e seus componentes

Estratégia da empresa



Objetivos da empresa



Perfil de risco da empresa

Risk Scenario Category	Impact (1 - 5)	Likelihood (1 - 5)	Risk Rating
IT investment decision making, portifolio definition and maintenance	4	5	◆
Program and projects lifecycle management	2	2	◆
IT cost and oversight	2	1	◆
IT Expertise, skills and behavior	2	1	◆
Enterprise/it architecture	5	4	◆
IT operational infrasctrucutre incidents	5	3	◆
Unauthorized actions	4	5	◆
Sofware adoption/usage problems	3	2	◆
Hardware incidents	4	4	◆
Software failures	5	3	◆
Logical attacks (hacking, malware, etc.)	1	1	◆
Third-party/supplier incidents	2	2	◆
Noncompliance	3	3	◆
Geopolitical issues	2	1	◆
Industrial action	2	1	◆
Acts of nature	1	1	◆
Technology-based innovation	2	2	◆
Environmental	3	3	◆
Data and information management	4	4	◆

◆	Very High Risk
◆	High Risk
◆	Normal Risk
◆	Low Risk

Problemas relacionados à informação e tecnologia

Value	Importance (1 - 3)	Baseline
Frustration between different IT entities across the organization because of a perception of low contribution to business value	1	2
Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business value	3	2
Significant IT-related incidents, such as data loss, security breaches, project failure and application errors, linked to IT	3	2
Service delivery problems by the IT outsourcer(s)	1	2
Failures to meet IT-related regulatory or contractual requirements	2	2
Regular audit findings or other assesment reports about poor IT performance or reported IT quality or service problems	1	2
Substential hidden and rogue IT spending, that is, IT spending by user departments outside the control of the normal IT investment decision mechanisms and approved budgets	1	2
Duplications or overlaps between various initiatives, or other forms of wasted resources	1	2
Insufficient IT resources, staff with inadequate skills or staff burnout/dissatisfaction	3	2
IT-enabled changes or projects freequently failing to meet business needs and delivered late or over budget	1	2
Reluctance by board members, executives or senior management to engage with IT, or lack of committed business sponsorshop for IT	3	2
Complex IT operating model and/or unclear decision mechanisms for IT-related decisions	2	2
Excessively high cost of IT	1	2
Obstrucured or failed implementation of new initiatives or innovations caused by the current IT architecture and systems	2	2

Value	Importance (1 - 3)	Baseline
Gap between business and technical knowledge, which leads to business users and information and/or technology specialists speaking different languanges	3	2
Regular issues with data quality and integration of data across various sources	1	2
High level of end-user computing, creating (among other problems) a lack of oversight and quality control over the applications that are being developed and put in operation	2	2
Business departments implementing their own information solutions with little or no involvment of the enterprise IT department	3	2
Ignorance of and/or noncompliance with privacy regulations	3	2
Inability to exploit new technologies or innovate using I&T	2	2

1	No Issue
2	Issue
3	Serious Issue

Aplicação da cascata - Sistema de Governança sob medida

Objetivos da empresa→ Objetivos de alinhamento

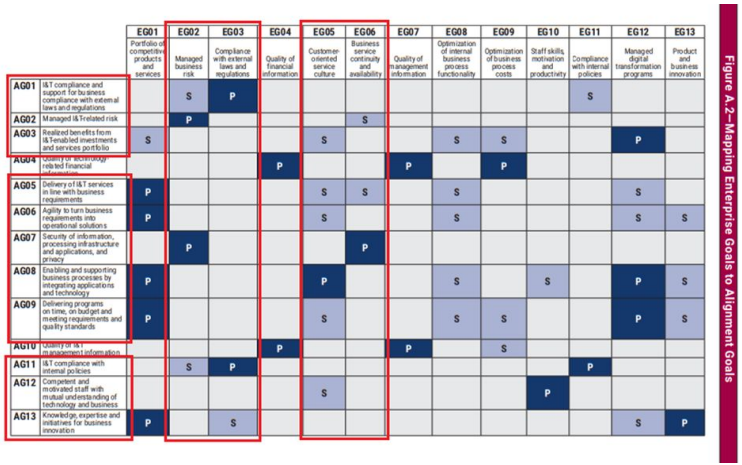


Figure A.2—Mapping Enterprise Goals to Alignment Goals

	EG01 Portfolio of competitive products and services	EG02 Managed business risk	EG03 Compliance with external laws and regulations	EG04 Quality of financial information	EG05 Customer-oriented service culture	EG06 Business service continuity and availability	EG07 Quality of management information	EG08 Optimization of internal business process functionality	EG09 Optimization of business process costs	EG10 Staff skills, motivation and productivity	EG11 Compliance with internal policies	EG12 Managed digital transformation programs	EG13 Product and business innovation
AG01 I&T compliance and support for business compliance with external laws and regulations		S	P								S		
AG02 Managed I&T-related risk		P				S							
AG03 Realized benefits from I&T-enabled investments and services portfolio	S				S			S	S			P	
AG04 Quality of technology-related financial information				P			P		P				
AG05 Delivery of I&T services in line with business requirements	P				S	S		S				S	
AG06 Agility to turn business requirements into operational solutions	P				S			S				S	S
AG07 Security of information, processing infrastructure and applications, and privacy		P				P							
AG08 Enabling and supporting business processes by integrating applications and technology	P				P			S		S		P	S
AG09 Delivering programs on time, on budget and meeting requirements and quality standards	P				S			S	S			P	S
AG10 Quality of I&T management information				P			P		S				
AG11 I&T compliance with internal policies		S	P								P		
AG12 Competent and motivated staff with mutual understanding of technology and business					S					P			
AG13 Knowledge, expertise and initiatives for business innovation	P		S									S	P

Objetivos de alinhamento → Objetivos de governança e gestão

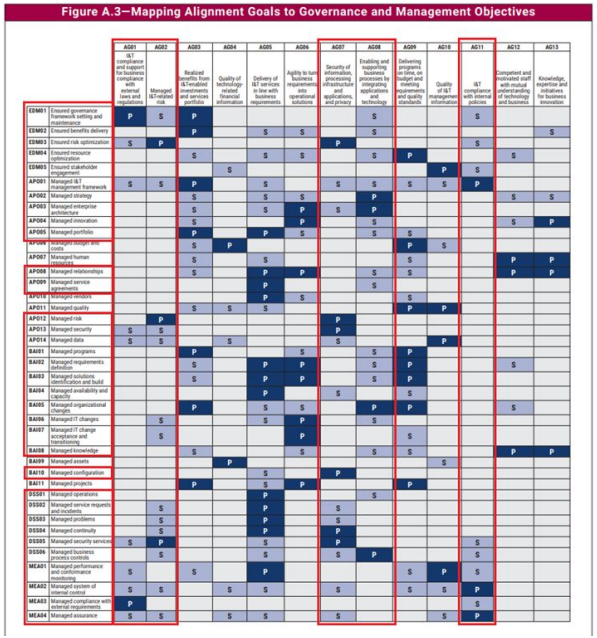


Figure A.3—Mapping Alignment Goals to Governance and Management Objectives

	AG01 I&T compliance and support for business compliance with external laws and regulations	AG02 Managed I&T-related risk	AG03 Realized benefits from I&T-enabled investments and services portfolio	AG04 Quality of technology-related financial information	AG05 Delivery of I&T services in line with business requirements	AG06 Agility to turn business requirements into operational solutions	AG07 Security of information, processing infrastructure and applications, and privacy	AG08 Enabling and supporting business processes by integrating applications and technology	AG09 Delivering programs on time, on budget and meeting requirements and quality standards	AG10 Quality of I&T management information	AG11 I&T compliance with internal policies	AG12 Competent and motivated staff with mutual understanding of technology and business	AG13 Knowledge, expertise and initiatives for business innovation
EDM01 Ensured governance framework setting and maintenance	P	S	P					S			S		
EDM02 Ensured benefits delivery			P		S	S		S					S
EDM03 Ensured risk optimization	S	P					P				S		
EDM04 Ensured resource optimization			S		S	S		S	P			S	
EDM05 Ensured stakeholder engagement				S						P	S		
APO01 Managed I&T management framework	S	S	P		S		S	S	S	S	P		
APO02 Managed strategy			S		S	S		P				S	S
APO03 Managed enterprise architecture			S		S	P	S	P					
APO04 Managed innovation			S			P		S				S	P
APO05 Managed portfolio			P		P	S		S	S				
APO06 Managed budget and costs			S	P					P	S		P	P
APO07 Managed human resources			S		S				S			P	P
APO08 Managed relationships			S		P	P		S	S				
APO09 Managed service agreements					P			S					
APO10 Managed vendors					P	S			S				
APO11 Managed quality			S	S	S				P	P			
APO12 Managed risk		P					P						
APO13 Managed security	S	S					P						
APO14 Managed data	S	S		S			S			P			
BAI01 Managed programs			P			S		S	P				
BAI02 Managed requirements definition			S		P	P		S	P			S	
BAI03 Managed solutions identification and build			S		P	P		S	P				
BAI04 Managed availability and capacity					P		S		S				
BAI05 Managed organizational changes			P		S	S		P	P			S	
BAI06 Managed IT changes		S			S	P		S					
BAI07 Managed IT change acceptance and transitioning		S				P			S				
BAI08 Managed knowledge			S			S		S	S			P	P
BAI09 Managed assets				P						S			
BAI10 Managed configuration					S		P						
BAI11 Managed projects			P		S	P			P				
DSS01 Managed operations					P			S					
DSS02 Managed service requests and incidents		S			P		S						
DSS03 Managed problems		S			P		S						
DSS04 Managed continuity		S			P		P						
DSS05 Managed security services	S	P			S		P				S		
DSS06 Managed business process controls		S			S		S	P			S		
MEA01 Managed performance and conformance monitoring	S		S		P				S	P	S		
MEA02 Managed system of internal control	S	S		S	S		S		S	S	P		
MEA03 Managed compliance with external requirements	P										S		
MEA04 Managed assurance	S	S		S	S		S			S	P		

Aplicação da cascata - Sistema de Governança sob medida

Filtragem do perfil de risco

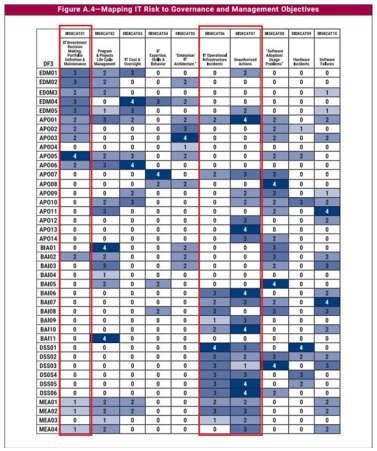


Figure A.4—Mapping IT Risk to Governance and Management Objectives

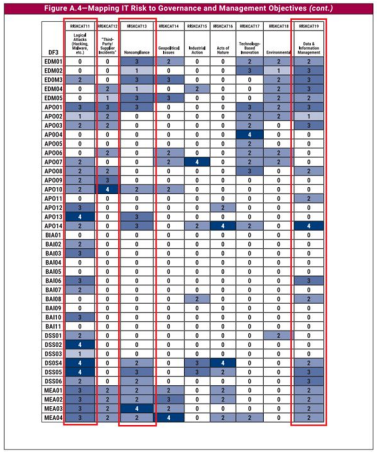


Figure A.4—Mapping IT Risk to Governance and Management Objectives (cont.)

Filtragem dos problemas de tecnologia e informação

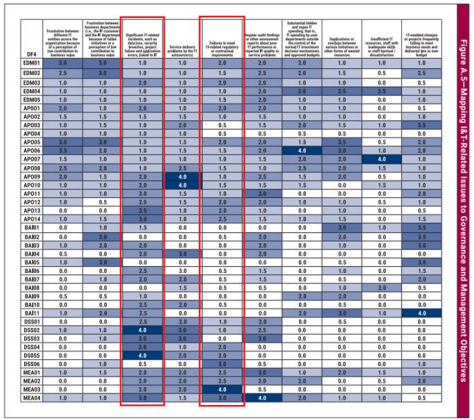


Figure A.5—Mapping I&T-Related Issues to Governance and Management Objectives

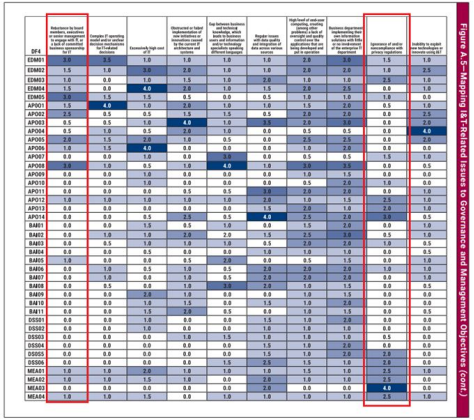
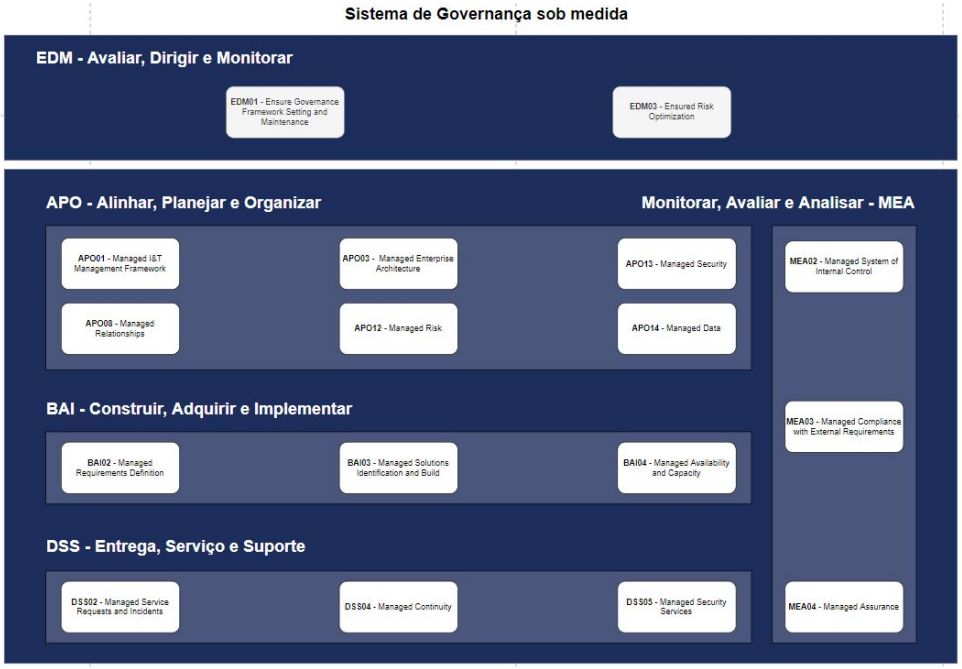


Figure A.5—Mapping I&T-Related Issues to Governance and Management Objectives (cont.)

Aplicação da cascata - Sistema de Governança sob medida

Refinamento → Sistema de governança sob medida



Solução

Contextualização

Proposta de solução

Definição dos serviços de Segurança → Gerenciamento do catálogo de serviços

Controle de acesso, antivírus e treinamentos → Gerenciamento de segurança da informação

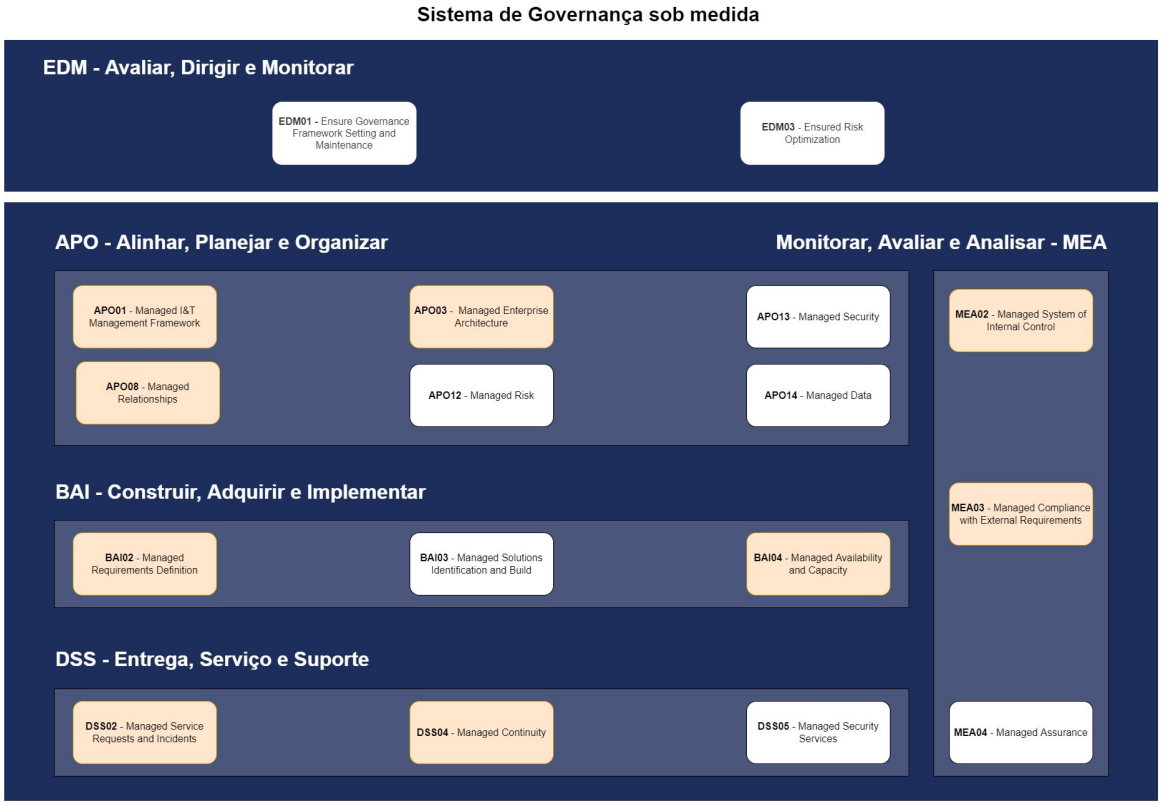
Plano de backup e restauração do servidor → Gerenciamento de continuidade

Solução

Mapeamento dos serviços e seus aspectos

Gerenciamento do catálogo de Serviços

Associação entre governança e gestão



ITIL

Gerenciamento do catálogo de serviços na contabilidade

Estratégia de Implantação - Planejamento

COBIT

APO- Alinhar, planejar e organizar

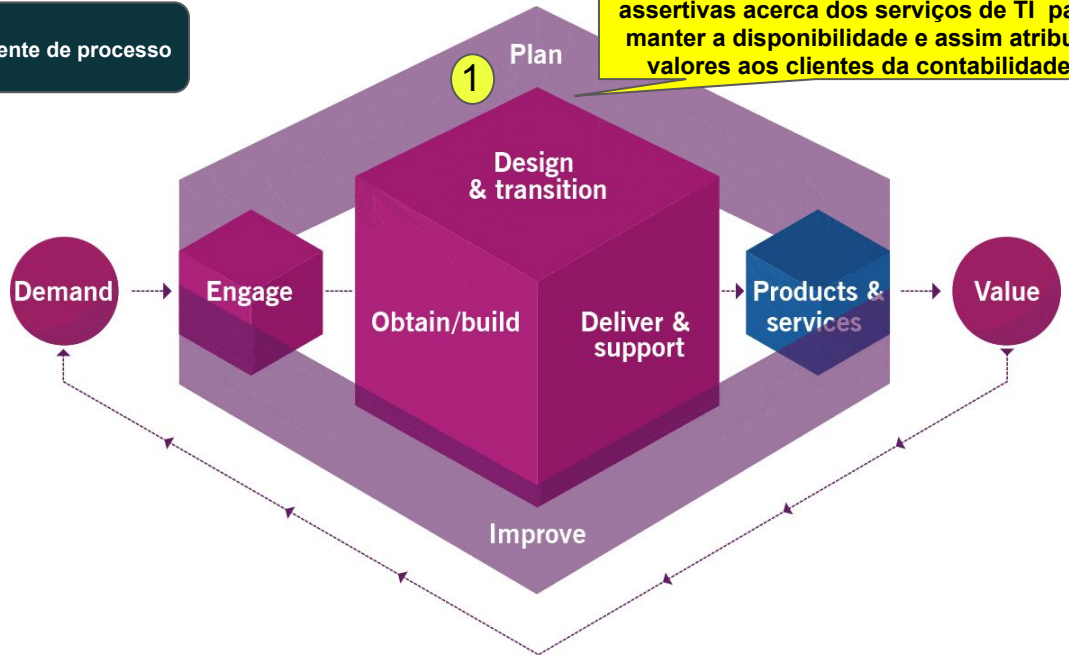
- **APO01 Gerenciar a Estrutura de Gestão**
  - Definir Políticas;
    Definir processos;
    Analisar Ferramentas;
    Analisar riscos;
    Definir metas;
    Definir indicadores;
    Raci
- **APO03 Gerenciar a Arquitetura**
  - Identificação de:
    -Tecnologia;
    - Infraestrutura;
    - Capacidade
    - Demanda

ITIL

- Gerenciamento de estratégia
- Gerenciamento financeiro
- Gerência de Mudanças organizacional
- Gerenciamento de talento e força de trabalho
- Análise de Negócio
- Gerenciamento de Arquitetura

Gerente de processo

Aplicar as estratégias de negócio da contabilidade através dos serviços de TI fornecendo todos os detalhes sobre todos os serviços requeridos pela empresa, a fim de que os funcionários tenham proatividade e tomem decisões assertivas acerca dos serviços de TI para manter a disponibilidade e assim atribuir valores aos clientes da contabilidade



Estratégia de Implantação - Desenho e Transição

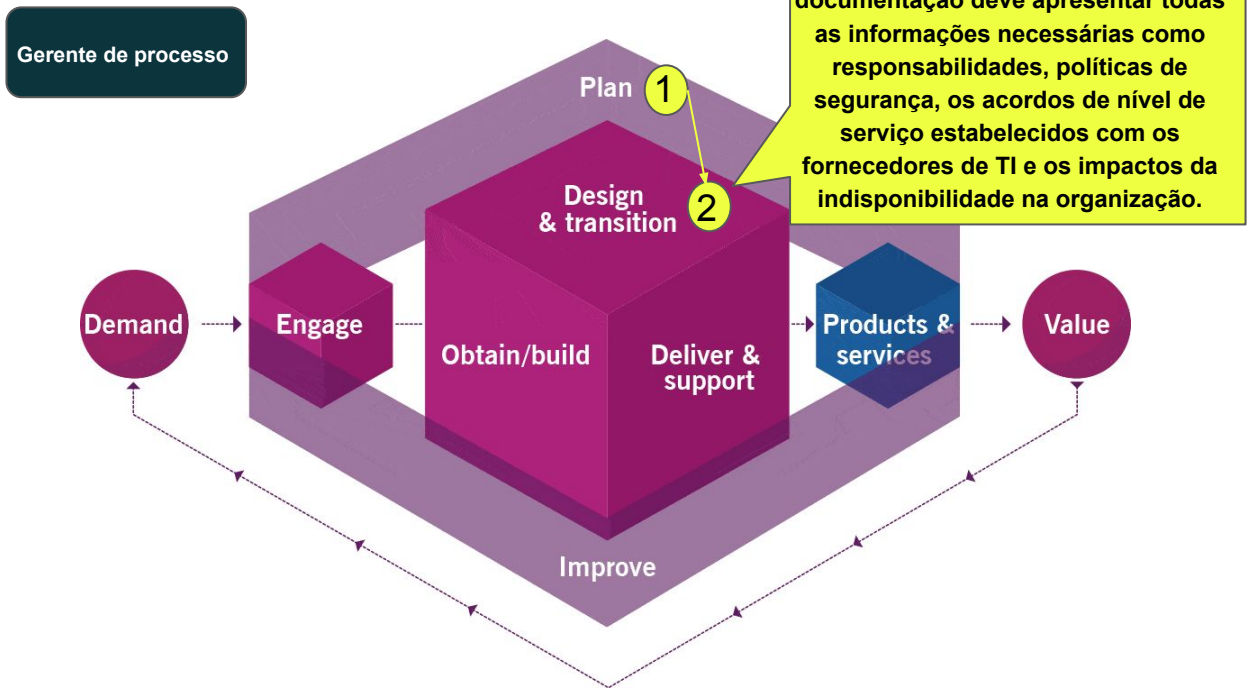
COBIT

BAI- Construir, adquirir e implementar

BAI02 Gerenciar a definição de Requisitos	BAI04 Gerenciar Disponibilidade e Capacidade

ITIL

- Desenho de Serviço
- Gerenciamento de Disponibilidade
- Gerenciamento de nível de serviço
- Gerenciamento de Risco



Estratégia de Implantação - Obter e Construir

COBIT

BAI- construir, adquirir e implementar

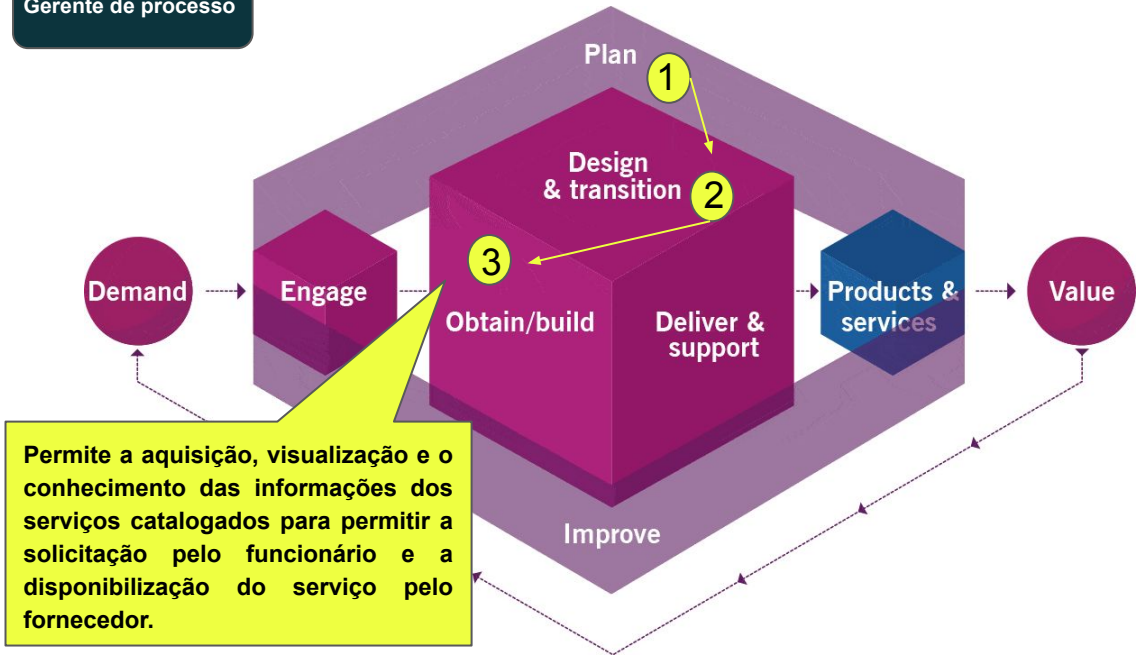
BAI02 Gerenciar a definição de Requisitos

BAI04 Gerenciar Disponibilidade e Capacidade

ITIL

Gerenciamento do conhecimento

Gerente de processo



Permite a aquisição, visualização e o conhecimento das informações dos serviços catalogados para permitir a solicitação pelo funcionário e a disponibilização do serviço pelo fornecedor.

Estratégia de Implantação - Engajar

COBIT

APO- Alinhar, planejar e organizar

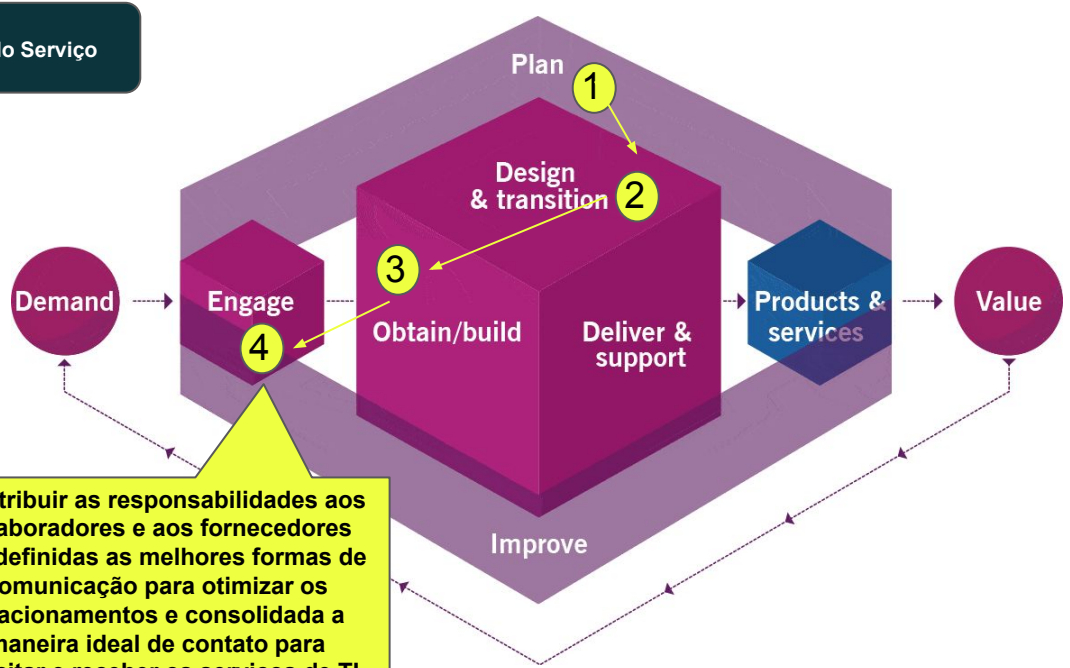
PO08 Gerenciar Relacionamentos

ITIL

Gerenciamento de Fornecedores

Gerenciamento de Relacionamento

Dono do Serviço



Ao atribuir as responsabilidades aos colaboradores e aos fornecedores são definidas as melhores formas de comunicação para otimizar os relacionamentos e consolidada a maneira ideal de contato para solicitar e receber os serviços de TI catalogados

Estratégia de Implantação - Entrega e suporte

COBIT

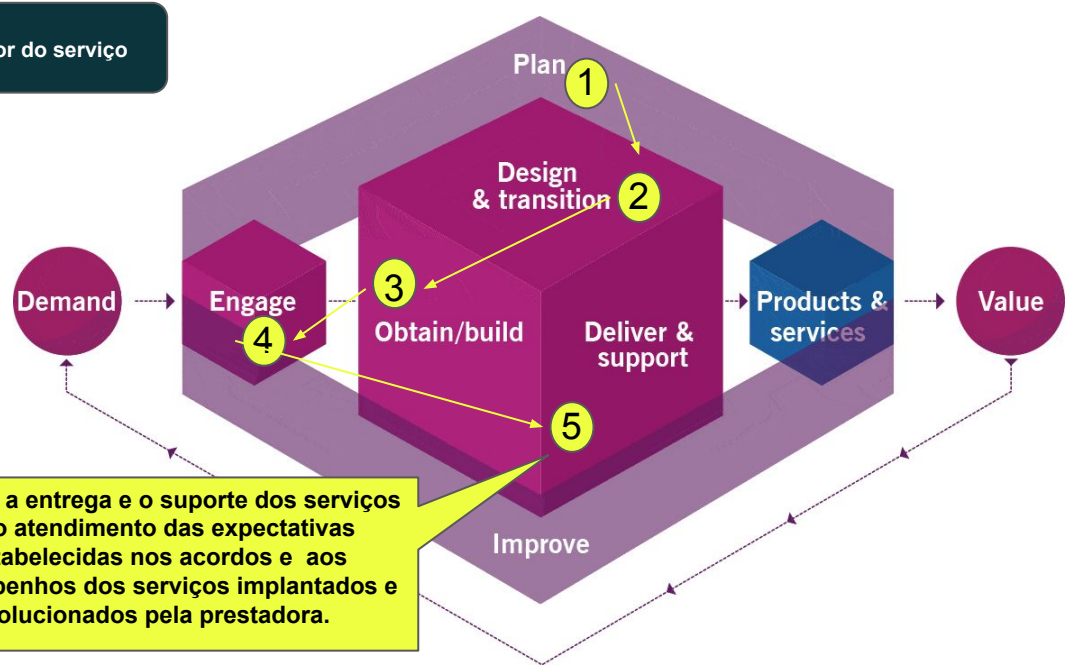
DSS- Entregar, servir e suportar

DSS02 Gerenciar Solicitação de Serviços e Incidentes

ITIL

- Gerenciamento de Continuidade
- Gerenciamento de nível de serviço
- Gerenciamento de Requisição de Serviços
- Gerenciamento de Incidentes
- Gerenciamento do Desempenho

Fornecedor do serviço



Otimiza a entrega e o suporte dos serviços pelo atendimento das expectativas estabelecidas nos acordos e aos desempenhos dos serviços implantados e solucionados pela prestadora.

Estratégia de Implantação - Melhorar

COBIT

MEA Monitorar, Avaliar e Analisar

MEA02 Monitorar, Avaliar e Analisar o Sistema de Controle Interno

MEA03 Monitorar, Avaliar e Analisar a Conformidade com Requisitos Externos

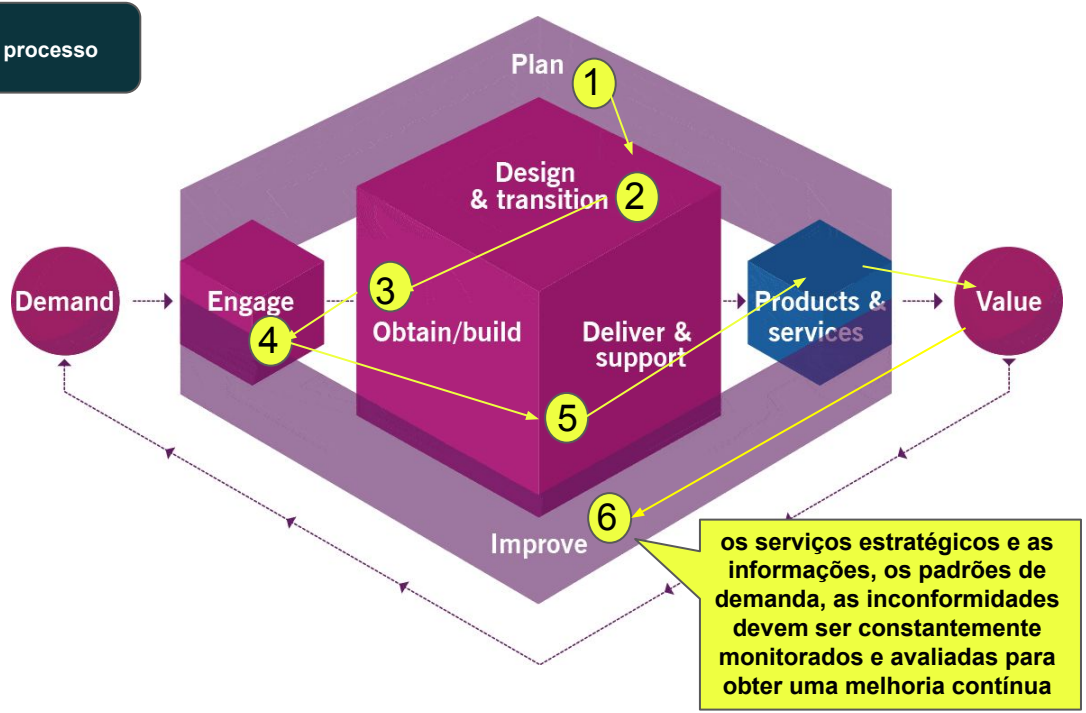
ITIL

Melhoria Contínua

Controle de mudanças

Medição e Relatório

Dono do processo



Gerenciamento do Catálogo de Serviço:

Políticas	
Serviços	**O serviço de TI deve ser claramente definido para que se possa mensurar a sua relevância na contabilidade e o seu papel na cadeia de serviço, possibilitando aos colaboradores possuírem conhecimento das capacidades da empresa e de suas responsabilidades, e ainda permitindo mais eficácia na requisição de um novo serviço ou na resolução de incidentes**
Catálogo	**Deve garantir que os prestadores e principalmente os colaboradores tenham conhecimento de todos os serviços prestados pela TI. Por se tratar de um processo "vivo", essas validações garantem que os serviços estejam atualizados e que eles tenham responsáveis definidos.**
Publicação	**O Catálogo de Serviços pode ser utilizado para fins de gestão do serviço e com a finalidade de apresentar aos funcionários e aos prestadores de serviços informações referentes aos serviços acordados que são providos pela TI e garantem a geração do valor de negócio da contabilidade.**

Gerenciamento do Catálogo de Serviço: RACI

Atividades do catálogo	Dono do Processo Maria	Gerente de Processo Maria	Gerente de Mudança Glauciano	Dono do serviço colaboradores
ALTERAR informações	-	R/A	C	C
INSERIR informações	-	R/A	C	C
ATUALIZAR	I	R/A	-	C
PUBLICAR nova versão	I	R/A	I	I
Selecionar itens	R	A	-	-
Gerar relatório de inconsistências	-	R/A	I	C
Levantar dados de indicadores	R	A	-	-
Analisar indicadores	-	R/A	-	-
Gerar relatório de indicadores	-	R/A	-	-
Apresentar resultados	I	R/A	-	-

Gerenciamento do Catálogo de Serviço: Riscos

Riscos do Catálogo

- Inexatidão das informações do negócio da contabilidade;
- Inexatidão das informações da terceirizada de TI com relação aos serviços e de suas capacidades;
- Inexatidão dos dados no catálogo
- Os serviços não estarem sob rigoroso controle de mudanças;
- A Baixa aceitação do catálogo de serviços e sua consequente não utilização em todos os processos operacionais;
- Ferramentas e recursos ineficientes necessários para manter as informações do catálogo;
- Pouco acesso ao gerenciamento de mudanças, às informações e aos processos do catálogo.

Gerenciamento do Catálogo de Serviço

Tipo	ENTRADAS	SAÍDAS
Gerenciamento	• Requisição de mudança; • Reporte de outros processos; • Novos serviços estratégicos requeridos pelos stakeholders.	• Requisição de Mudança atualizada; • Catálogo de Serviços atualizado. • Definição do serviço.
Auditoria	• Catálogo de serviços; • Informações de indicadores e metas.	• Registro RDM • Relatório de Indicadores; • Relatório de inconsistência

Exemplos de Métricas para melhorias do Catálogo

Descrição	**Porcentagem de inconsistências auditadas do catálogo publicado**
Período	**semestral**
Meta	**3%**
Cálculo	**(Total de Inconsistências / Quant. Total de serviços) x 100**

Descrição	**Percentual de servidores que têm desconhecimento do Catálogo de Serviços**
Período	**Trimestral**
Meta	**0%**
Cálculo	**Total de ausências assinaturas / total de colaboradores da contabilidade**

Exemplo de relatório para Gerenciamento do Catálogo

Total de Serviços de TI catalogados: 42			Data: 03/07/2022 Período do relatório: De 01/01/22 até 30/06/22	
Id	**Serviço**	**Pacote**	**Responsável**	**Descrição**
01	S20- Realizar restauração do backup e tratamento de falha relacionado ao backup quando solicitado	Backup	Glauciano	O serviço pode ser dividido em dois: 1 voltado apenas a Restauração e outro apenas para tratar falhas que venham ocorrer no processo do backup
Número total de Inconsistências		1	Porcentagem de Inconsistências (meta 3%)	(1/42) x 100= 2,38%
Meta de inconstância atingida: Informar dono do serviço e encaminhar RDM ao gerente de mudanças				
Número total de Servidores		Números de Servidores Com assinaturas de conhecimento do catálogo		Percentual de desconhecimento dos colaboradores
12		9		(3/12) x 100=25%
Meta Não atingida: Informar os colaboradores com desconhecimento e ou procurar melhor alternativa além do mural de aviso da empresa.				

Solução

Redução de problemas de segurança da informação

Gerenciamento de segurança da informação

Gerenciamento de segurança da informação de TI

Objetivo:

- Gerenciar as atividades de segurança voltadas aos dados contábeis dos clientes.

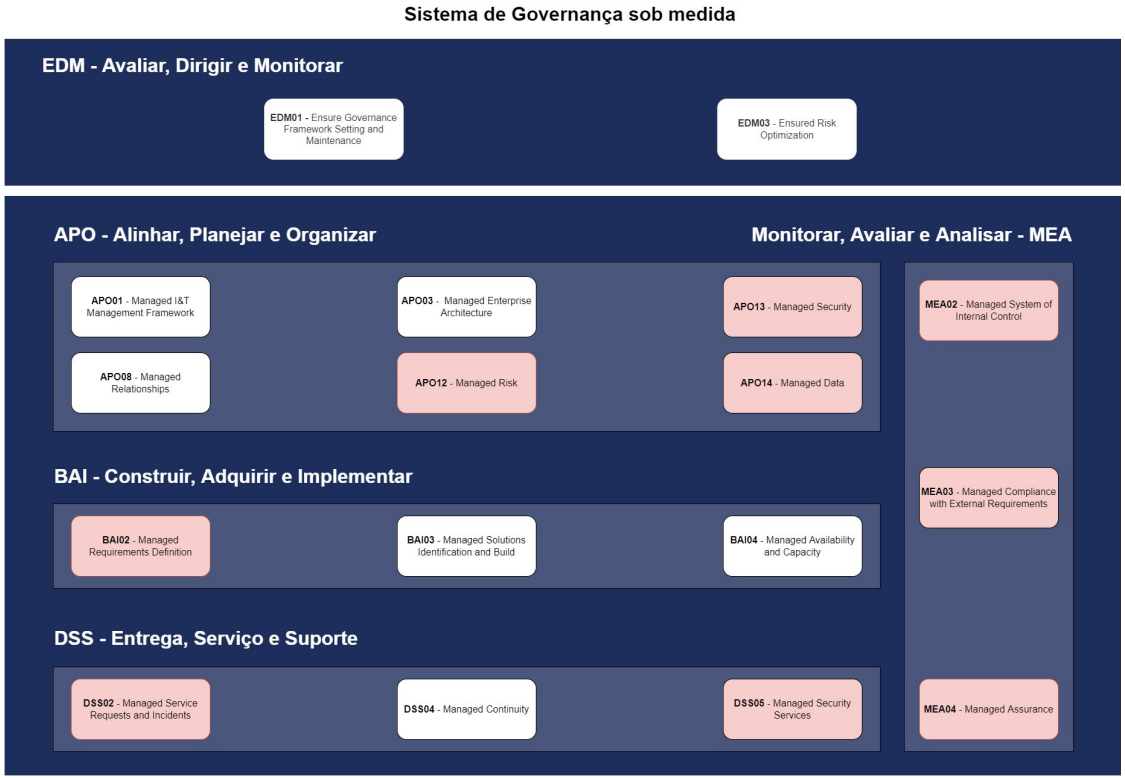
Entradas

- Novas regulamentações de órgãos reguladores
- Novos direcionamentos organizacionais
- Adição de questões de segurança de dados

Saídas

- Políticas de segurança de informação
- Implementação de controles de segurança
- Documentação de procedimentos adotados

Associação entre governança e gestão



ITIL

Gerenciamento da segurança da informação

Diretrizes COBIT x Atividades chave ITIL

COBIT

Monitorar, Avaliar e Analisar

MEA02 - Managed System of Internal Control

MEA03 - Managed Compliance with External Requirements

MEA04 - Managed Assurance

ITIL

Monitoramento de medidas detectivas

Gerenciamento de violações de segurança

COBIT

Alinhar, planejar e organizar

APO12 - Managed Risk

APO13 - Managed Security

APO14 - Managed Data

ITIL

Avaliação de riscos e exposição de riscos

Conceber medidas de segurança apropriadas

Estabelecer e distribuir documentação sobre gerenciamento de dados

Desenvolvimento de processos facilitadores para o seguimento de políticas

Diretrizes COBIT x Atividades chave ITIL

COBIT

Construir, Adquirir e Implementar

BAI02 - Managed Requirements Definition

ITIL

Alocar recursos de TI para atender a regulamentação

Conscientizar sobre dados

Estipular medidas preventivas

COBIT

Entrega, Serviço e Suporte

DSS02 - Managed Service Requests and Incidents

DSS05 - Managed Security Services

ITIL

Estipular medidas redutivas

Estipular medidas corretivas

Garantir proteção lógica e física

Matriz RACI

Atividades propostas	Dono	Gestor do setor de contabilidade	Auxiliar da contabilidade	Responsável pela Soluções T.I.	Técnico de Soluções T.I.
Conceber medidas de segurança	I	-	-	R+A	C
Conceber documentação sobre gerenciamento de dados	I	-	-	R+A	C
Desenvolver processos facilitadores para gerenciamento de dados	I	-	-	R+A	C
Treinamentos de segurança	I	I	I	A	R
Estabelecimento de direitos de acesso	I	I	I	R+A	R
Implantação de backups automatizados	I	-	-	A	R
Proteção lógica de dados com antivírus	I	-	-	A	R

Exemplo de relatório

Documento de Políticas de Segurança da Informação:

5.2. Armazenamento de dados

Os dados relevantes para a realização do trabalho dos funcionários devem ser armazenados no servidor interno da empresa. Com exceção de dados públicos, nenhum outro dado (dentro da classificação do Item 4) pode ser mantido armazenado na máquina local.

5.3. Realização de backup

O backup dos dados deverá acontecer somente sobre os dados armazenados no servidor interno. Dados armazenados localmente nas estações de trabalho individuais não terão backups realizados pela equipe de T.I.

A tarefa de realização de backup deverá ser automatizada pelos fornecedores de serviços de T.I., não havendo necessidade de alocar algum funcionário para a realização da tarefa.

A periodicidade da realização do backup dos dados deverá ser acordada entre os prestadores de serviços de segurança de T.I. e os sócios-proprietários da empresa de contabilidade e será revista sempre que os sócios-proprietários acharem necessário. No momento, a periodicidade é diária.

Métricas

Descrição	**Maior conscientização sobre a política de segurança e seu conteúdo em toda a organização**
Atividades	• **Elaboração do Documento de Políticas de Segurança da Informação** • **Distribuição do documento, via PDF, no servidor da empresa.**
Cálculo	**Total de funcionários / Nº de funcionários conhecedores do Documento de Políticas de Segurança da Informação**
Total de funcionários	**12 pessoas**
Funcionários afetados	**12 pessoas**

Métricas

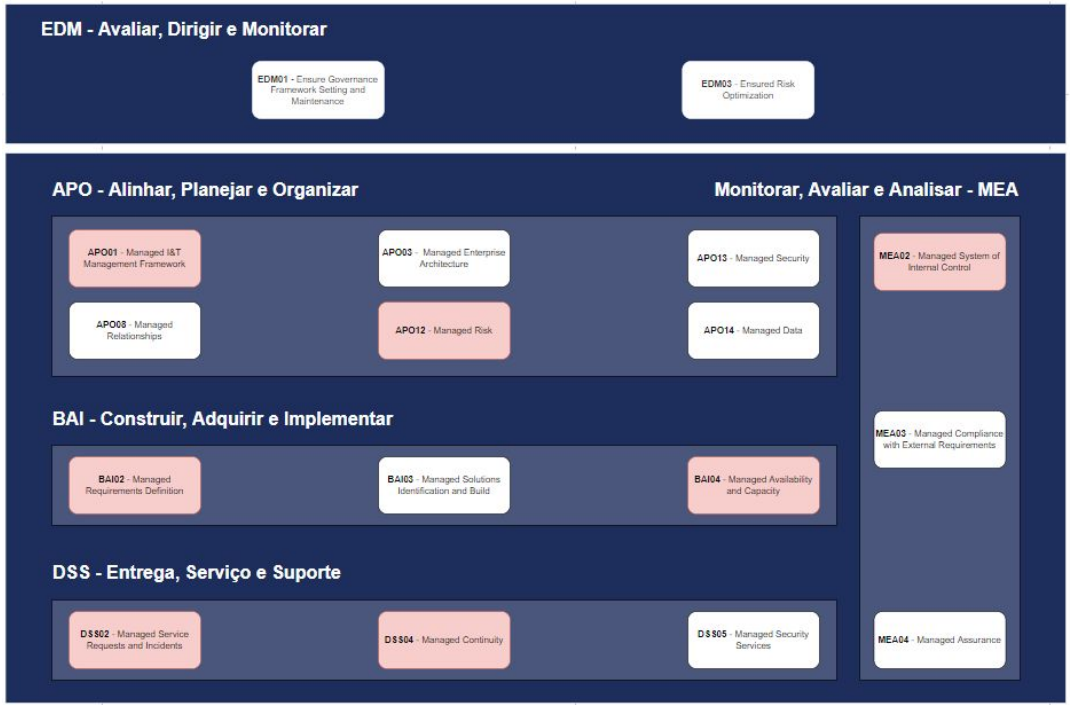
Descrição	**Diminuição do número de não conformidades de segurança detectadas**
Atividades	• **Elaboração do Documento de Políticas de Segurança da Informação** • **Definição de controles através do Documento de Políticas de Segurança da Informação**
Cálculo	**Nº de problemas encontrados no contexto da segurança da informação na empresa / Nº de problemas atendidos pelo Documento de Políticas de Segurança da Informação**
Total de não conformidades detectadas	**13** **problemas / pontos de não conformidade com regulamentação externa**
Não conformidades atendidas / regulamentadas	**7 (53,8%)** **pontos atendidos pelo Documento de Políticas de Segurança da Informação e os controles nele estabelecidos.**

Solução

Proposta para a continuidade e redução de risco dos serviços

Gerenciamento da continuidade dos serviços

Associação entre governança e gestão



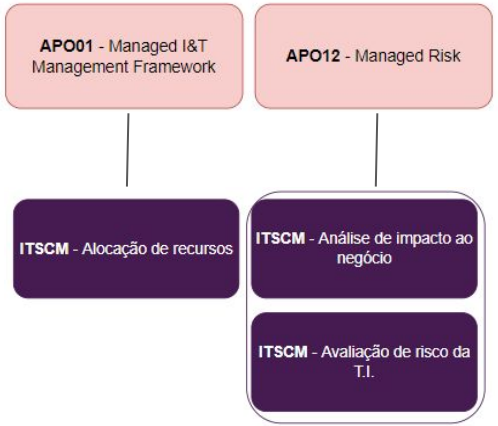
ITIL

Gerenciamento da continuidade dos serviços de TI

Estratégia de Implantação - Alinhamento e Planejamento

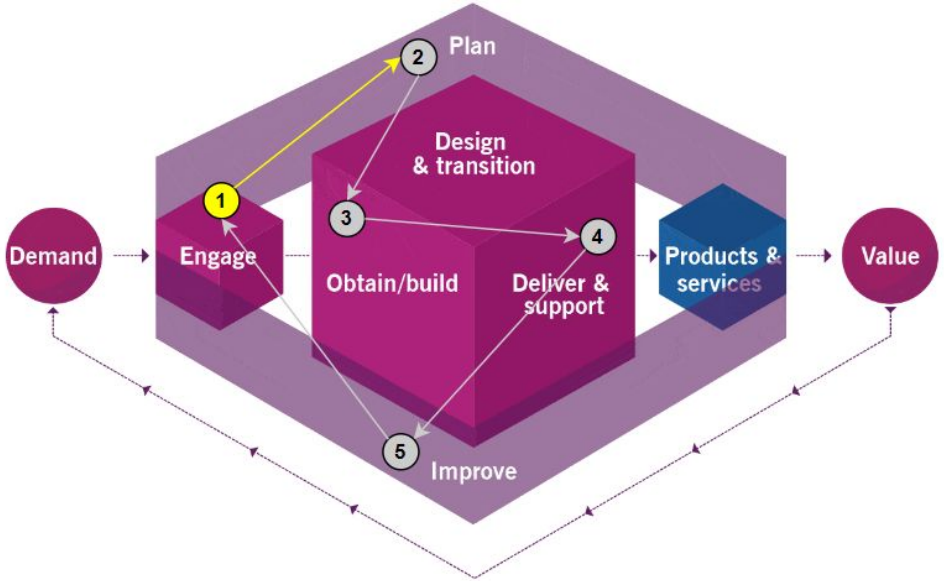
COBIT

Alinhar, planejar e organizar



ITSCM - Iniciação e estratégia

ITIL

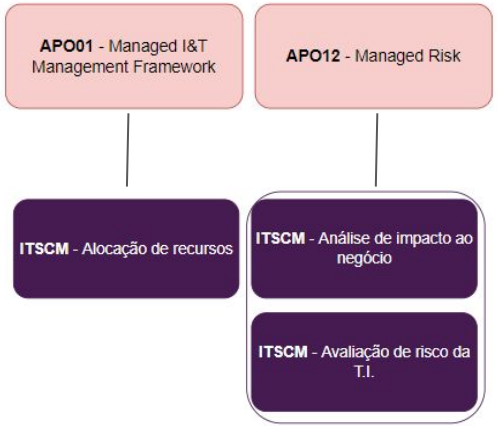


- Contato com Francisco (responsável pela Soluções T.I.) para agendamento de suporte com os serviços de T.I.

Estratégia de Implantação - Alinhamento e Planejamento

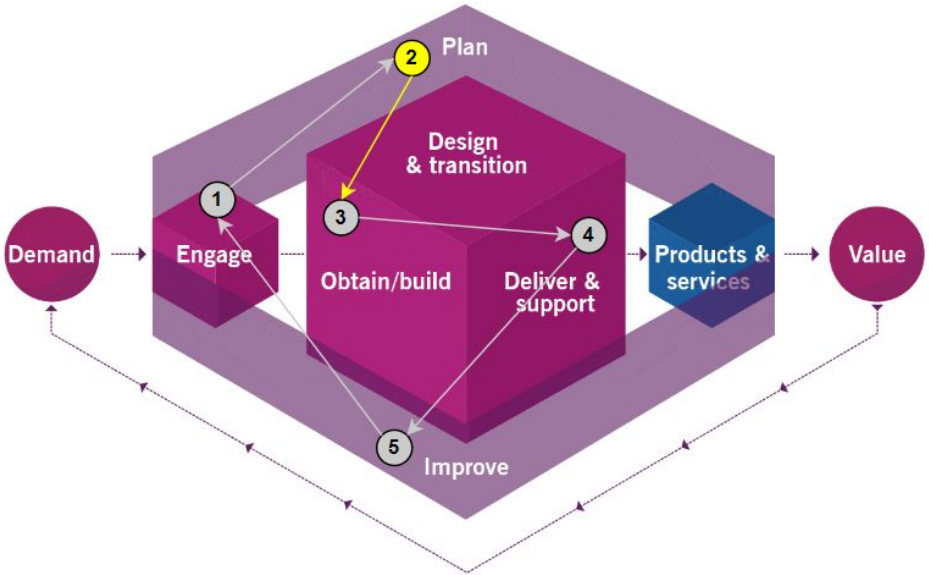
COBIT

Alinhar, planejar e organizar



ITSCM - Iniciação e estratégia

ITIL



- Maria e gestores dos departamentos realizam a definição da análise de impacto ao negócio
- Alfredo (técnico da soluções T.I.) faz a análise de risco dos serviços de TI

Estratégia de Implantação - Alinhamento e Planejamento

COBIT

Alinhar, planejar e organizar

APO01.04 – Definir a estrutura organizacional
Quem vai participar do processo

APO01.05 – Definir papéis e responsabilidades
Definir papéis no gerenciamento

APO01.01 – Planejamento do sistema
Definir o risco dos processos e seus serviços
Definir prioridades na implementação

APO01.02 – Comunicação dos objetivos de gerenciamento
Alinhamento dos objetivos com stakeholders

APO012.01 – Coletar dados
Elaborar a análise de impacto ao negócio para mapeamento de riscos

APO012.02 – Analisar o risco
Definir como os riscos do negócio são impactados pela T.I.

APO012.06 – Responder ao risco
Definir os métodos de redução de risco dado a prioridade

ITIL

ITSCM - Iniciação e estratégia

Alocação de recursos e responsáveis

Análise de impacto ao negócio

Avaliação do risco da T.I.

Estratégia de Implantação - Saídas

Matriz RACI - Gerenciamento de continuidade

	Atividades Críticas	Responsáveis					
		Dono (Maria)	Gestor do dpto. de contabilidade (Bruno)	Auxiliar da contabilidade (João)	Responsável pela Soluções T.I. (Francisco)	Técnico da Soluções T.I. (Alfredo)	Colaboradores
Organização	Definir os responsáveis pelo plano de continuidade	R	A+C	C	A	I	I
	Definir participantes para suporte da continuidade dos serviços	R	I	I	A	I	C
	Definir terceiro responsável por auxiliar na elaboração das estratégias	R	I	-	-	-	-
	Definir alocação de hora de colaboradores	R	I	-	-	-	I
Estratégia	Implementar a análise de impacto ao negócio (BIA)	R	R+A	A+I	-	-	C
	Desenvolver a análise de risco dos serviços de T.I.	A	A	-	R	C	-
	Definir as soluções possíveis para redução de risco e recuperação	A	A	-	R	C	-
	Escolher as soluções com base no custo-benefício para implementação	R+A	I	-	R	C	-
Implementação	Desenvolver os planos de continuidade dos serviços de T.I.	A	R	I	I	C	-
	Comprar os equipamentos necessários para a redução de risco com base na estratégia escolhida	A	I	-	A+C	R	-
	Implementar os serviços de redução de risco e recuperação	A	I	-	A+C	R	-
	Definir o fluxo de comunicação para o plano de continuidade	A	R	I	C+I	I	-

	Atividades Críticas	Responsáveis					
		Dono (Maria)	Gestor do dpto. de contabilidade (Bruno)	Auxiliar da contabilidade (João)	Responsável pela Soluções T.I. (Francisco)	Técnico da Soluções T.I. (Alfredo)	Colaboradores
Entrega	Fornecer os planos de continuidade para os colaboradores	A	R	C	-	-	I
	Testar os planos de continuidade	I	A+C	R	A	R	-
	Testar a eficiência dos serviços de redução de risco	I	A	-	A+C	R	-
	Definir as métricas que serão coletadas para avaliar a continuidade dos serviços	C+A	R	I	-	C	-
	Atualizar o catálogo de serviços com as soluções propostas e implementadas	R	C+A	-	I	-	-
Manutenção	Realizar o gerenciamento de mudanças	A	R	I	I	C	-
	Realizar as auditorias trimestrais das soluções propostas	A	R	C	-	I	I
	Educar e treinar os responsáveis pelo plano de continuidade	A	R	C	-	R+C	I
	Coletar as métricas propostas para o gerenciamento da continuidade dos serviços	A	R	I	-	C	-
	Avaliar a evolução das metricas coletadas para propor novas soluções e garantir o desenvolvimento contínuo	I	R	I	A	C	C

Estratégia de Implantação - Saídas

Análise de impacto ao negócio

Processo de negócio	Dependências	Prioridade ao negócio	Impacto da indisponibilidade	Necessidade de recuperação
Declaração de IR	Software Externo – Gov Servidor	Alto	Irregularização do cliente Impossibilidade de entrega dos documentos no prazo adequado Perda de vantagem competitiva Dano a reputação	1-3 horas
Conciliação bancária	Software Externo - Acessorias Servidor	Médio	Impossibilidade de registro de conciliação Perda de vantagem competitiva	1-2 dias
Registro de Balanço Patrimonial	Software Externo - IOB Servidor	Alto	Impossibilidade de desenvolvimento do BPA Perda de vantagem competitiva	1-3 horas
Processamento da folha de pagamento	Servidor	Baixo	Invalidez de pagamentos Dano a reputação	1-3 dias
Documentação de admissão e demissão	Servidor	Médio	Trava de processo de contratação	1-6 horas
Cadastro geral de empregados	Servidor	Médio	Trava de processo de contratação	1-2 dias

Estratégia de Implantação - Saídas

Avaliação de risco do servidor

Serviço	Risco	Impacto	Possibilidade de Ocorrer	Necessidade de recuperação	Ação recomendada
Servidor	**Corrompimento de disco**	**Alto**	**Médio**	**Imediato**	**Execução de backups recorrentes e definição de planos de recuperação**
Servidor	Indisponibilidade de rede	Médio	Médio	Imediato	Validação das conexões e alinhamento do nível de serviço com o provedor externo
Servidor	Acesso não autorizado	Alto	Alto	Alto	Definição de políticas de controle de acesso por usuário / departamento
Servidor	Danos físicos	Alto	Baixo	Alto	Isolamento físico do servidor em relação ao ambiente de trabalho
Servidor	**Ataque ransomware**	**Alto**	**Médio**	**Imediato**	**Execução de backups recorrentes, definição de planos de recuperação e utilização de antivírus**
Servidor	Problema funcional por falta de atualização	Médio	Baixo	Moderado	Verificação e instalação recorrente de atualizações dos serviços envolvidos
Servidor	Indisponibilidade por falta de fonte de energia	Alto	Baixo	Moderado	Utilização de nobreaks de alta potência ou geradores em caso severo
Servidor	Comprometimento de credenciais	Alto	Médio	Baixo	Definição de políticas de criação e não compartilhamento de senhas
Servidor	Superaquecimento do ambiente	Médio	Baixo	Imediato	Monitoramento da temperatura e adoção de mecanismos adequados para seu controle

Estratégia de Implantação - Implementação

COBIT

Construir, Adquirir e Implementar

BAI02 - Managed Requirements Definition

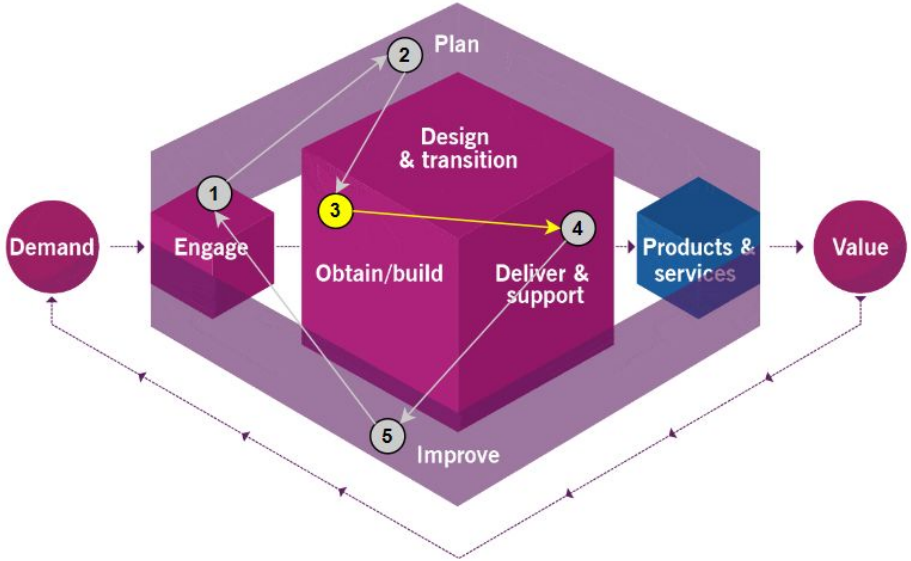
BAI04 - Managed Availability and Capacity

ITIL

ITSCM - Implementação

ITSCM - Redução de risco

ITSCM - Medidas de Recuperação



- Alfredo propõe as soluções adequadas para redução de risco do sistema
- Maria faz a validação de custo-benefício e aprova a solução mais viável
- Alfredo faz a aquisição dos equipamentos necessários e repassa as instruções necessárias para Bruno (responsável pelo setor da contabilidade)

Estratégia de Implantação - Implementação

COBIT

Construir, Adquirir e Implementar

BAI02.02 – Análise de viabilidade das soluções
Levantamento das soluções de redução de risco

BAI02.04 – Aprovação da solução
Integração entre o dono e a terceirizada para solução mais viável

BAI04.02 – Avaliar o impacto ao negócio
Compor a viabilidade da solução dado a análise de impacto

ITIL

ITSCM - Implementação

Mapeamento das soluções de redução de risco
- Implementação da realização de backups

Mapeamento das medidas de recuperação
- Método de recuperação dos dados do servidor por backup

Análise de viabilidade das soluções

Estratégia de Implantação - Entrega

COBIT

Entrega, Serviço e Suporte

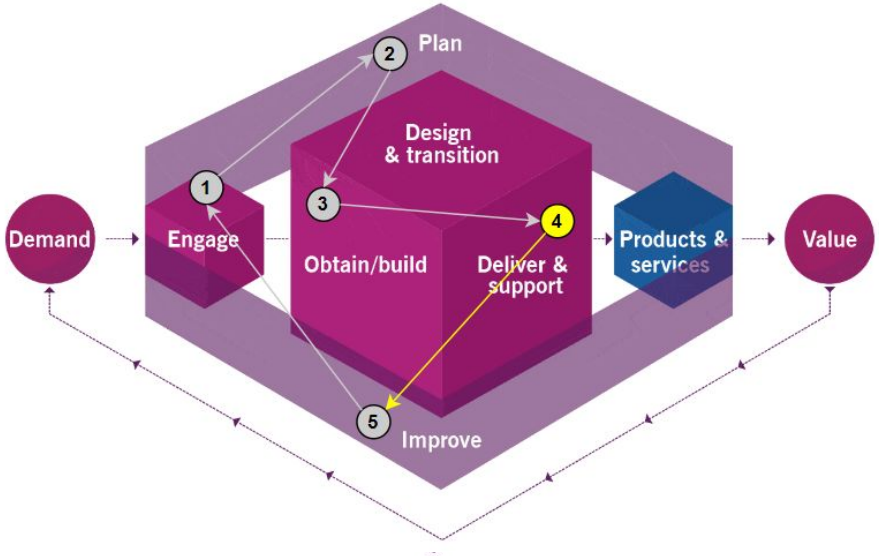
DSS02 - Managed Service Requests and Incidents

DSS04 - Managed Continuity

ITIL

ITSCM - Entrega

ITSCM - Planos de continuidade



- Bruno desenvolve o plano de continuidade e repassa para João que será responsável por executar o plano
- João recebe o treinamento pela soluções T.I. para executar o plano de continuidade
- Alfredo testa a eficiência e os conhecimentos de João em relação ao plano

Estratégia de Implantação - Entrega

COBIT

Construir, Adquirir e Implementar

DSS02.01 – Definir os responsáveis pelos incidentes

DSS02.05 - Recuperação em relação aos incidentes
Definição do plano de continuidade

DSS04.02 – Manter a resiliência do negócio
Elaborar medidas de recuperação a partir da priorização

DSS04.03 – Desenvolver procedimento de resposta
Definir o passo a passo do plano de recuperação e o plano de comunicação

DSS04.05 – Revisar, manter e melhorar os planos de continuidade
Auditoria frequente dos planos de continuidade

DSS04.06 – Conduzir o treinamento dos planos de continuidade

ITIL

ITSCM - Entrega

Desenvolvimento dos planos de continuidade
- Passo a passo
- Responsável pelo plano
- Plano de comunicação

Treinamento do funcionário para execução do plano

Teste da eficiência do plano

Estratégia de Implantação - Saídas

Plano de recuperação de dados para continuidade do servidor

Detalhes do time de recuperação	Nome	Posição	Telefone	Responsabilidades
	Bruno de Almeida	Gestor do departamento contábil	(35) 91234-5102	Execução do plano de recuperação
	João Aparecido	Auxiliar do departamento contábil	(35) 96194-1415	Auxílio da execução do plano de recuperação
	Maria Santos	Dono	(35) 97124-5123	Contato de comunicação interno
	Alfredo de Oliveira	Técnico – Soluções T.I.	(35) 98612-5912	Contato de comunicação externo
	Francisco	Dono – Soluções T.I.	(35) 97412-4512	Contato de comunicação externo – emergência
Invocação de responsáveis	João Aparecido – Responsável pela recuperação do servidor (detalhes de contato acima) Bruno de Almeida – Contato de comunicação interna (detalhes de contato acima) Alfredo de Oliveira – Contato de comunicação externa (detalhes de contato acima)			
Plano de contingência	Notificar o contato de comunicação externo e interno que o plano será executado Localizar o HD de backup e o HD auxiliar no armário da sala do departamento contábil Identificar a data do backup e documentá-la no plano Conectar o HD auxiliar no servidor e transferir os dados atuais para o HD auxiliar Formatar o disco do servidor Conectar o HD de backup no servidor formatado e iniciar a transferência dos dados Verificar a normalidade dos serviços utilizados Solicitar ao contato de comunicação externo a recuperação dos dados do HD auxiliar Confirmar, verbalmente, a estabilidade dos serviços pelos colaboradores do departamento contábil Em caso de problemas o contato de comunicação interno deverá ser acionado			
Distribuição	Esse documento deverá estar disponível com os demais arquivos referentes aos planos de recuperação no servidor, devendo estar armazenado na máquina dos responsáveis pelo plano de recuperação e auxiliares, como: Todos os chefes dos departamentos Os responsáveis pela execução do plano de recuperação O dono da empresa O contato terceirizado responsável pelas soluções de T.I.			

Estratégia de Implantação - Manutenção

COBIT

Monitorar, Avaliar e Analisar

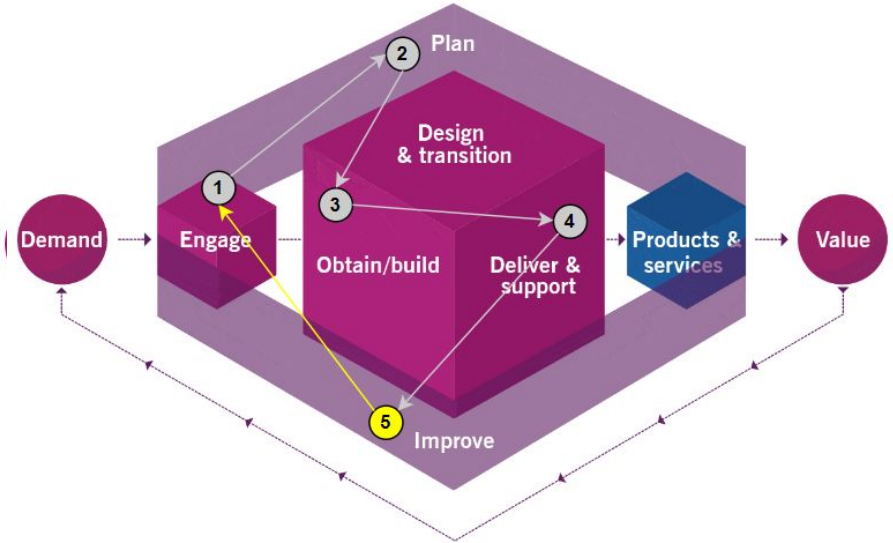
MEA02 - Managed System of Internal Control

ITIL

ITSCM - Manutenção

ITSCM - Gerenciamento de mudanças

ITSCM - Testes dos planos



- Bruno coleta as informações documentadas e avalia mensalmente a diminuição da interrupção dos serviços da empresa pelos serviços de T.I.
- Bruno verifica se os serviço de TI foram modificados para realizar o gerenciamento de mudanças e iniciar um novo plano de continuidade

Estratégia de Implantação - Manutenção

COBIT

Construir, Adquirir e Implementar

ME02.01 – Revisar a eficiência dos processos de negócio
Avaliar se o impacto da T.I. nos processos do negócio esta baixa

MEA02.03 – Realizar a avaliação das soluções próprias
Determinar se os planos de continuidade estão conforme o planejado

ITIL

ITSCM - Entrega

Educação dos envolvidos no plano de continuidade

Revisão e auditoria do plano de continuidade

Gerenciamento de mudanças

Métrica → Avaliação da redução do impacto da TI no negócio

Métrica e saídas

Descrição	**Variação mensal do impacto da indisponibilidade da TI para o negócio**
Período	**Mensal**
Meta	**0%**
Método	**Soma das horas descritas nos relatórios de execução de continuidade**
Cálculo	**Total de horas indisponíveis no mês atual / total de horas indisponíveis no mês anterior**
Responsável / Divulgação	**Bruno / Envio de email para todos funcionários**

- Mapeamento do impacto da TI no negócio
- Avaliação de risco para futuras melhorias
- Solução de backup para redução de risco
- Plano de continuidade para restauração dos dados do servidor

Estimativas da solução

Esclarecimento dos custos e benefícios

Estimativa de custos adicionais de aquisição e operação

Serviços de segurança a serem implantados na contabilidade	Opção 01 - Interno		Opção 02 - Externo	
	Custos Inicial	Custo mensal	Custos Inicial	Custo mensal
Treinamento em segurança	0,00	0,00	72,00	1,00
Controle de acesso	0,00	0,00	108,00	3,00
Instalação Kaspersky + Licenças	1.039,48	0,00	1.156,48	1,50
Atualização Kaspersky	0,00	0,00	0,00	117,00
Realização de Backup (controle e teste) + HD	200,00	0,00	200,00	216,00
Restauração do Backup + Falhas	0,00	0,00	0,00	432,00
Custos Totais	1.239,48	0,00	1.536,48	770,50
	1.239,48		2.306,98	

Pontos X nº ocorrências (catálogo)

Acordado que: cada ponto 1 Real

Custo Hora Colaborador R$ 471,63 Diferença de 174,67

Diferença de R$ 1.067,50

Justificativa do investimento

- **A empresa é responsável juridicamente pelo que ocorre em seu contexto no que tange a segurança dos dados dos clientes**
- **A não execução de backups recorrentes pode gerar a perda de todos os dados da empresa, podendo ocasionar sua descontinuidade**
- **A falta do controle de acesso pode gerar vazamento de informação dos clientes**
- **O não conhecimento da segurança da informação pelos funcionários pode levar a ações que prejudiquem a empresa nesse contexto**
- **A falta de controles mínimos de segurança como antivírus podem facilitar a ocorrência de um ataque**

- **Equivalência de investimento com base em cenário abstrato:**
  - A multa prevista pela LGPD é de 2% do faturamento global anual da empresa
    - Billt → Faturamento anual = R$600 mil → Custo = R$12 mil
  - Indisponibilidade do servidor impacta todos os serviços e empregados
    - 12 funcionários * R$9,37 hora = R$112,44 por hora (hora do iniciante)
    - Impossibilidade de entregar o produto para os clientes → Negócio indisponível → Queda de valor
  - Risco de perder todos os dados do servidor

Conclusão

- **Melhoria do relacionamento entre a empresa e o provedor de TI**
- **Melhoria no gerenciamento dos serviços de TI**
- **Melhoria da segurança dado a responsabilidade da empresa**
- **Redução do impacto da indisponibilidade da TI nos processos do negócio**
- **Redução do risco de problemas de TI a partir de um baixo investimento**
- **Maior controle do acesso aos dados na empresa**
- **Maior controle dos serviços de TI para proposta de novas soluções**
- **Maior conscientização dos colaboradores em relação a segurança da informação**
- **Possibilitar uma infraestrutura inicial para regulamentação completa em segurança no futuro**

Referências

ITIL - Service Design - 2011 Edition - The Stationery Office

ITIL Foundation - ITIL 4 Edition - The Stationery Office

COBIT 2019 - Design Guide - ISACA

COBIT 2019 - Framework Governance and Management Objectives - ISACA

ISACA - COBIT 2019 - Implementation Guide

Nancy Judith Cruz-Hinojosa, José Antonio Gutiérrez-de-Mesa, Literature review of the situation research faces in the application of ITIL in Small and Medium Enterprises, Computer Standards & Interfaces, Volume 48, 2016.

Ana Rita Fernandes de Sousa, Service Design e as boas práticas ITIL - o caso de estudo da SONAE Indústria, 2013

Responsabilidades

Bruno Brandão Borges

- Contextualização

Ivan Leoni Vilas Boas

- Gerenciamento de catálogo de serviços
- Mapeamento de custos
- Mapeamento de soluções

Leonardo Rodrigo de Sousa

- Gerenciamento de segurança da informação
- Mapeamento de soluções

Lucas Tiense Blazzi

- Gerenciamento de continuidade dos serviços
- Modelo de Governança e fatores de projeto COBIT
- Mapeamento de soluções

Thiago Marcelo Passos

- Análise de cenários Val IT