
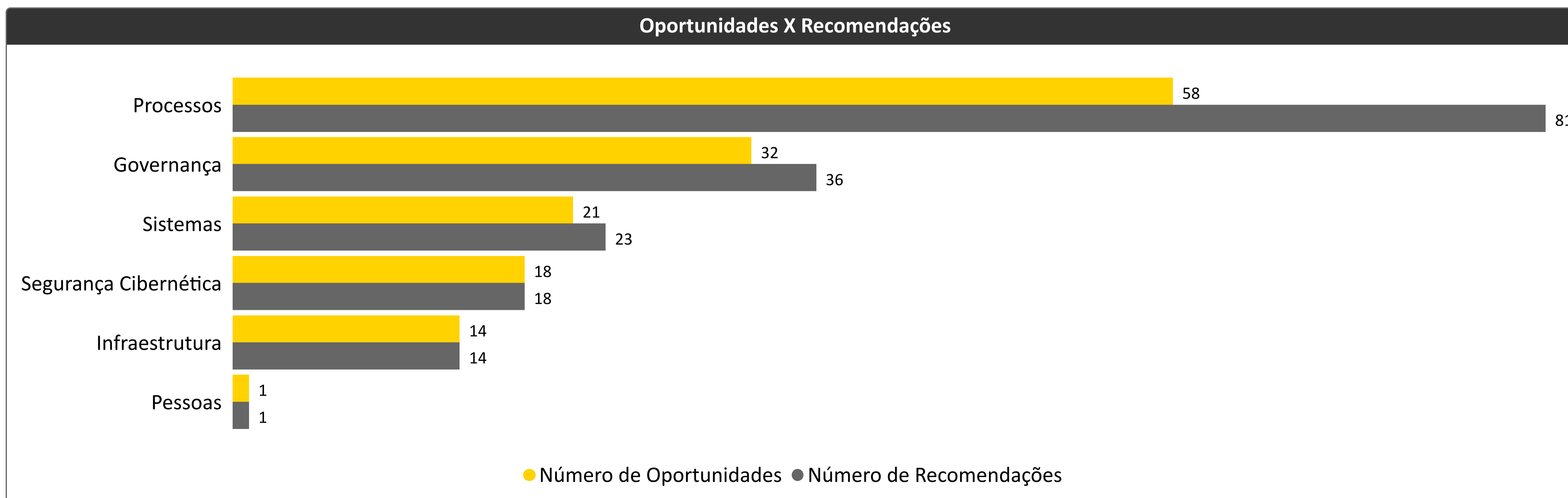
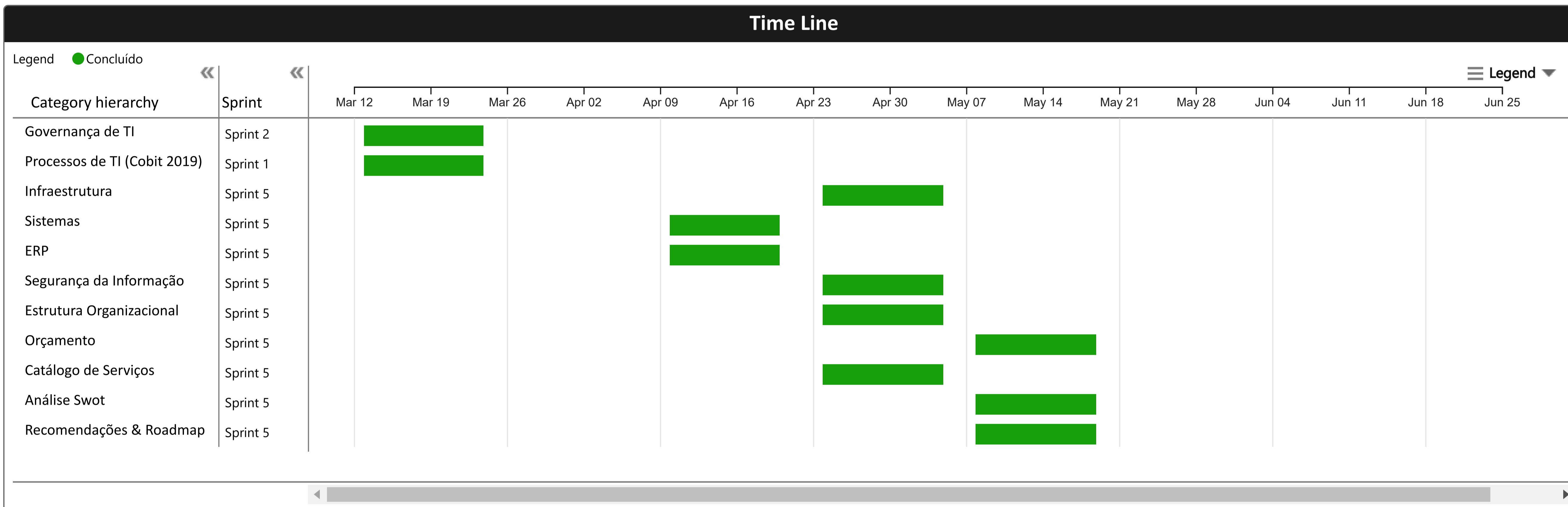


- Painel 
- Estratégia 
- Pessoas 
- Processos 
- Tecnologia 
- Orçamento 
- Roadmap 
- Anexos 



- Painel 
- Estratégia** 
- Pessoas 
- Processos 
- Tecnologia 
- Orçamento 
- Roadmap 
- Anexos 



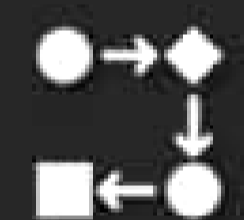
Painel



Estratégia



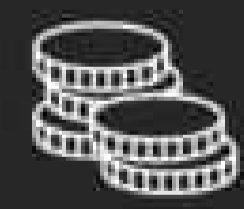
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Liderança

Planejamento

Alocação de Capital

Políticas

Coordenação e Compliance

Monitoramento e Controle

Gestão do Relacionamento com o Negócio

Descrição do Pilar

O domínio Liderança tem como objetivo estabelecer um processo formal e transparente de relacionamento com as áreas da empresa, trabalhar com as partes interessadas para entender a demanda atual e futura de Serviços de TI e estabelecer comissões que apoiam e orientam a Governança de TI.

Análise As Is

- Não foram identificadas atividades e processos direcionados à gestão do relacionamento da TI com o negócio.
 - A identificação da necessidade do negócio não ocorre de maneira proativa.
- Comunicação do negócio com a TI ocorre em âmbito operacional, quando a TI é acionada para tratamento de novas demandas.
 - Não possuem normativas sobre o desenvolvimento Low Code de sistemas pelas áreas de negócio.
- Aquisição de equipamentos de tecnologia sem a devida aprovação da área de tecnologia, nem sempre seguindo o padrão de equipamentos estipulado pela TI, porém, não foram identificados documentos que determinem estes padrões.

Recomendações To Be

- Mapear os usuários chaves de cada área da empresa que serão os pontos focais de relacionamento com a TI.
- Estabelecer processo proativo de proposição de soluções de TI para atendimento das necessidades do negócio, junto aos pontos focais identificados, definindo suas responsabilidades, frequência e forma de atuação.
 - Manter sob o domínio da TI todos os sistemas utilizados pela companhia, assim como atualizar o portfólio de sistemas.
- Estabelecer diretrizes e processo estruturado para aquisição de novos softwares e/ou desenvolvimento dos mesmos para atendimento às áreas de negócio (Processo Make or Buy).
 - Estabelecer a política padrão dos equipamentos de tecnologia e divulgar para toda companhia.



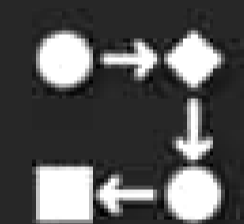
Painel



Estratégia



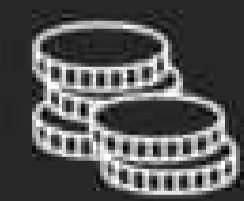
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Liderança

Planejamento

Alocação de Capital

Políticas

Coordenação e Compliance

Monitoramento e Controle

Estabelecimento de Comissões

Descrição do Pilar

O domínio Liderança tem como objetivo estabelecer um processo formal e transparente de relacionamento com as áreas da empresa, trabalhar com as partes interessadas para entender a demanda atual e futura de Serviços de TI e estabelecer comissões que apoiam e orientam a Governança de TI.

Análise As Is

- Foram identificados apenas dois comitês coordenados por TI, sendo eles: TIC (Tecnologia da Informação e Comunicação) e SI (Segurança da Informação), sendo o primeiro com encontros trimestrais e o segundo semestrais.
- A TI possui participação em outros comitês internos (Concurso, PGA - Programa de Gestão Anual) e externos (CNC - Conselho Nacional de Cartografia, CS-AEB - Conselho Superior da Agência Espacial Brasileira).
 - Não foram identificados outros comitês, como, por exemplo: Comitê de Projetos de TI e Comitê de Inovação.
- Os regimentos internos dos Comitês de TIC e SI estão aguardando aprovação da área de Governança para que os mesmos possam ser oficializados.
 - Falta de comunicação e participação das unidades regionais em comitês da TI.

Recomendações To Be

- Estabelecer Comitês que enderecem os assuntos de Governança de TI, Projetos de TI e Inovação de TI, observando suas responsabilidades, periodicidade e público-alvo. Exemplo: Comitê de Projetos de TI; Comitê de Inovação.
- Estabelecer ponto focal de TI em cada unidade regional e incluir sua participação nos comitês aplicáveis.



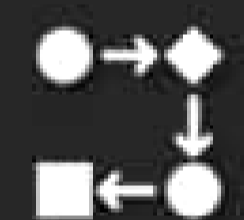
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Liderança

Planejamento

Alocação de Capital

Políticas

Coordenação e Compliance

Monitoramento e Controle

Definição do Plano Estratégico de TI

Descrição do Pilar

O domínio Planejamento atua na definição de estratégias de TI, bem como no desenvolvimento e estruturação de soluções e serviços para atingimento dos objetivos e metas organizacionais.

Análise As Is

- Ausência de um sistema de governança de TI para avaliar, direcionar e monitorar os serviços oferecidos, corrobora para a existência de lacunas as necessidades do negócio e os serviços ofertados pela TI.
- O último PDTI foi elaborado em 2015, abrangendo o período de 2015-2020. Contudo, não foram identificadas ações que evidenciem os devidos desdobramentos deste plano.
- Não foi identificado portfólio de projetos de TI.

Recomendações To Be

- Implementar e monitorar as recomendações constantes neste PDTI.
- Estabelecer Portfólio de projetos e processo de monitoramento do Portfólio de projetos de TI, mantendo o devido alinhamento com as necessidades do negócio.



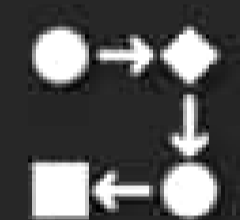
Painel



Estratégia



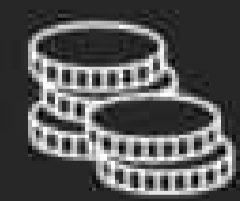
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Liderança

Planejamento

Alocação de Capital

Políticas

Coordenação e Compliance

Monitoramento e Controle

Definição do Plano Estratégico de TI



Descrição do Pilar

O domínio Planejamento atua na definição de estratégias de TI, bem como no desenvolvimento e estruturação de soluções e serviços para atingimento dos objetivos e metas organizacionais.

Análise As Is

- Ausência de um sistema de governança de TI para avaliar, direcionar e monitorar os serviços oferecidos, corrobora para a existência de lacunas as necessidades do negócio e os serviços ofertados pela TI.
- O último PDTI foi elaborado em 2015, abrangendo o período de 2015-2020. Contudo, não foram identificadas ações que evidenciem os devidos desdobramentos deste plano.
- Não foi identificado portfólio de projetos de TI.

Recomendações To Be

- Implementar e monitorar as recomendações constantes neste PDTI.
- Estabelecer Portfólio de projetos e processo de monitoramento do Portfólio de projetos de TI, mantendo o devido alinhamento com as necessidades do negócio.



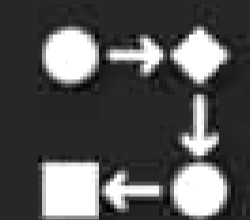
Painel



Estratégia



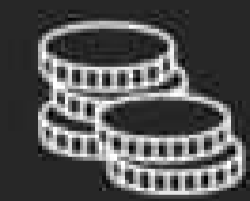
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Liderança

Planejamento

Alocação de Capital

Políticas

Coordenação e Compliance

Monitoramento e Controle

Definição do Plano Estratégico de TI



Descrição do Pilar

O domínio Planejamento atua na definição de estratégias de TI, bem como no desenvolvimento e estruturação de soluções e serviços para atingimento dos objetivos e metas organizacionais.

Análise As Is

- Ausência de um sistema de governança de TI para avaliar, direcionar e monitorar os serviços oferecidos, corrobora para a existência de lacunas as necessidades do negócio e os serviços ofertados pela TI.
- O último PDTI foi elaborado em 2015, abrangendo o período de 2015-2020. Contudo, não foram identificadas ações que evidenciem os devidos desdobramentos deste plano.
- Não foi identificado portfólio de projetos de TI.

Recomendações To Be

- Implementar e monitorar as recomendações constantes neste PDTI.
- Estabelecer Portfólio de projetos e processo de monitoramento do Portfólio de projetos de TI, mantendo o devido alinhamento com as necessidades do negócio.



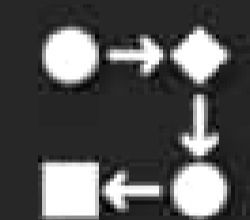
Painel



Estratégia



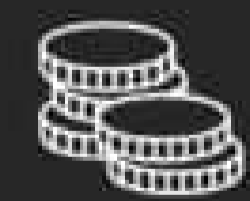
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Liderança

Planejamento

Alocação de Capital

Políticas

Coordenação e Compliance

Monitoramento e Controle

Definição da Estratégia de Terceirização

Descrição do Pilar

O domínio Planejamento atua na definição de estratégias de TI, bem como no desenvolvimento e estruturação de soluções e serviços para atingimento dos objetivos e metas organizacionais.

Análise As Is

- Ausência de estratégia para a adoção de serviços de TI terceirizados.
- Contratações de profissionais terceirizados ad-hoc.

Recomendações To Be

- Definir estratégia de terceirização de fornecedores, considerando os tipos de serviço e as responsabilidades que devem ser mantidas com a equipe interna de TI ou repassadas a terceiros.



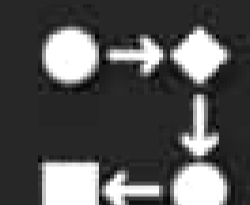
Painel



Estratégia



Pessoas



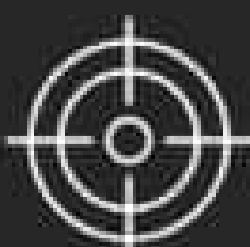
Processos



Tecnologia



Orçamento



Roadmap

Liderança

Planejamento

Alocação de Capital

Políticas

Coordenação e Compliance

Monitoramento e Controle

Organização, Planejamento e Desenho de Soluções e Serviços

Descrição do Pilar

O domínio Planejamento atua na definição de estratégias de TI, bem como no desenvolvimento e estruturação de soluções e serviços para atingimento dos objetivos e metas organizacionais.

Análise As Is

- Ausência de método para o planejamento e desenho de soluções e serviços para atendimento às necessidades do negócio.

Recomendações To Be

- Implementar o comitê de Inovação para possibilitar o desenho de soluções alinhadas à necessidade do negócio.
- Estabelecer processo para revisão periódica do Catálogo de Serviços para atendimento às necessidades do negócio, validando os serviços existentes, os ANSs (Acordos de Nível de Serviço) e ANOs (Acordos de Nível Operacional).



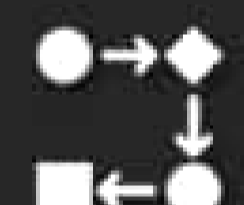
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Liderança

Planejamento

Alocação de Capital

Políticas

Coordenação e Compliance

Monitoramento e Controle

Definição de capital necessário

Descrição do Pilar

O domínio Alocação de Capital está relacionado à gestão financeira, de recursos da estrutura de trabalho de TI, e do orçamento necessário para desenvolvimento das ações de TI, objetivando a entrega efetiva de Serviços.

Análise As Is

- Ausência de definições sobre as características das soluções, equipamentos e demais ativos que estão pertinentes a TI, como: hardwares, softwares e serviços tecnológicos.
- Ausência de critérios para definição de investimento em TI.
- A divisão de TI (DIINFO) submete para aprovação o orçamento anual através do Projeto de Lei Orçamentária - PLOA e a Diretoria de Infraestrutura Geocientífica (DIG) define o orçamento da divisão.

Recomendações To Be

- Estabelecer política que atribua exclusivamente a TI todo o orçamento a ser destinado a ativos e serviços tecnológicos.
 - Estabelecer critérios de priorização de investimento em TI.
 - Definir estratégia para alocação de recursos das soluções de TI.
- Estabelecer processo de revisão prévia do plano orçamentário anual da TI com a diretoria responsável e com as áreas de negócio aplicáveis.



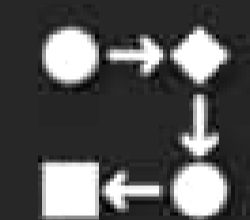
Painel



Estratégia



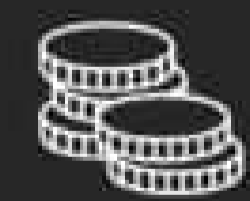
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Liderança

Planejamento

Alocação de Capital

Políticas

Coordenação e Compliance

Monitoramento e Controle

Gestão de Recursos



Descrição do Pilar

O domínio Alocação de Capital está relacionado à gestão financeira, de recursos da estrutura de trabalho de TI, e do orçamento necessário para desenvolvimento das ações de TI, objetivando a entrega efetiva de Serviços.

Análise As Is

- A TI realiza o planejamento anual orçamentário previsto no Projeto de Lei Orçamentária - PLOA e o Plano Anual de Trabalho - PAT registra o planejamento dos programas, projetos e atividades. Não foram identificados critérios, classificação e planejamento para o orçamento disponibilizado. Este orçamento definido pela DIG é comumente inferior ao solicitado pela DIINFO. O orçamento disponibilizado para a TI no ano de 2023 foi cerca de 74% do solicitado.
- Ausência de processos de showback e chargeback.

Recomendações To Be

- Estipular a estratégia para gestão de recursos disponibilizados, refletindo o atual cenário orçamentário da TI, contemplando procedimentos para a priorização orçamentária.
- Prover transparência dos custos relacionados a TI por meio do processo de showback e, posteriormente, seguir a estratégia definida para a gestão de recursos (chargeback ou não).



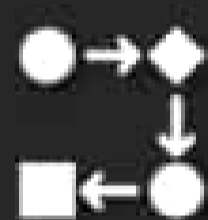
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Liderança

Planejamento

Alocação de Capital

Políticas

Coordenação e Compliance

Monitoramento e Controle

Definição de Políticas e Procedimentos de TI

Descrição do Pilar

O domínio Políticas é responsável pela definição e estabelecimento dos processos, procedimentos e práticas da TI para atingimento dos objetivos definidos no domínio Planejamento.

Análise As Is

- Políticas, procedimentos e normas da TI não abordam principais temas de TI, como: Gestão de Acesso; Trabalho Remoto; Armazenamento de Dados; etc.
- Não existe processo definido para verificação periódica de políticas, normas e procedimentos.

Recomendações To Be

- Estabelecer, através da governança, processo para atualização e/ou criação de políticas, procedimentos e normas da TI, divulgando-os para toda a companhia através dos canais oficiais de comunicação (e-mail, intranet etc.).
- Atualizar normativos existentes da TI.



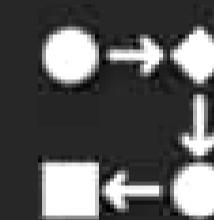
Painel



Estratégia



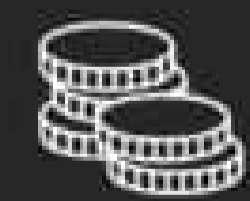
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Liderança

Planejamento

Alocação de Capital

Políticas

Coordenação e Compliance

Monitoramento e Controle

Assegura o cumprimento dos padrões e obrigações de TI

Descrição do Pilar

O domínio Coordenação e Compliance atua para que as políticas, normas e procedimentos sejam cumpridos, além de identificar, classificar e mitigar os riscos da TI relacionados ao Negócio.

Análise As Is

- Não foram identificados processos formais para verificação do cumprimento dos procedimentos operacionais de TI.

Recomendações To Be

- Implementar processos formais para verificação dos procedimentos operacionais de TI, conforme as recomendações apontadas na análise de capacidade dos processos de TI.
- Utilizar o comitê de TIC para monitorar a implementação das recomendações.



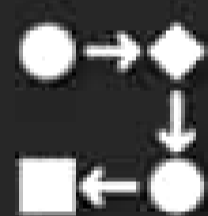
Painel



Estratégia



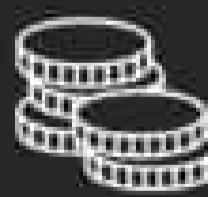
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Liderança

Planejamento

Alocação de Capital

Políticas

Coordenação e Compliance

Monitoramento e Controle

Gestão de Riscos



Descrição do Pilar

O domínio Coordenação e Compliance atua para que as políticas, normas e procedimentos sejam cumpridos, além de identificar, classificar e mitigar os riscos da TI relacionados ao Negócio.

Análise As Is

- Não foi identificado processo definido para gestão de riscos.

Recomendações To Be

- Mapear e monitorar os riscos relacionados a TI.
- Incluir os riscos mapeados pela TI, no plano de riscos corporativos.
- Implementar demais recomendações apontadas na análise de capacidade do processo APO12.



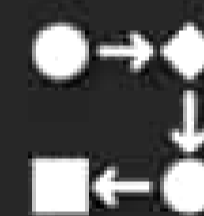
Painel



Estratégia



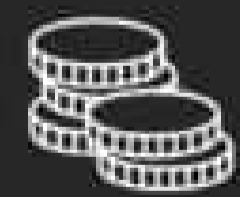
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Liderança

Planejamento

Alocação de Capital

Políticas

Coordenação e Compliance

Monitoramento e Controle

Monitoramento do Desempenho

Descrição do Pilar

O domínio Monitoramento e Controle tem como objetivo realizar a gestão de todos os serviços suportados pelo departamento de TI, monitorando indicadores de desempenho e demais processos relacionados à Operação de Serviços.

Análise As Is

- Há apenas 02 metas definidas para o acompanhamento operacional de TI, que embora derivadas do Plano Estratégico de Negócio, não são suficientes para a visão geral do desempenho da TI.

Recomendações To Be

- Estabelecer KPIs e OKRs que possibilitem medir e monitorar o desempenho e a evolução de TI.



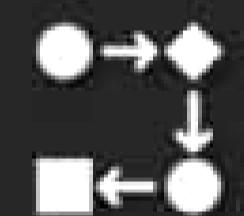
Painel



Estratégia



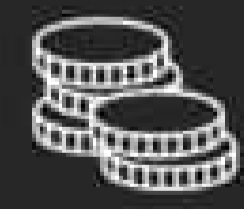
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Liderança

Planejamento

Alocação de Capital

Políticas

Coordenação e Compliance

Monitoramento e Controle

Melhoria Contínua



Descrição do Pilar

O domínio Monitoramento e Controle tem como objetivo realizar a gestão de todos os serviços suportados pelo departamento de TI, monitorando indicadores de desempenho e demais processos relacionados à Operação de Serviços.

Análise As Is

- Ausência de processos formais para melhoria contínua de indicadores, processos e atividades de TI.

Recomendações To Be

- Estabelecer governança para os processos, atividades e indicadores de TI, medindo e monitorando o seu desempenho.



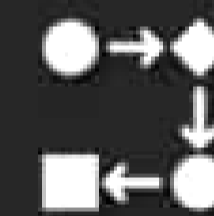
Painel



Estratégia



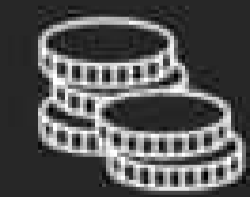
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Liderança

Planejamento

Alocação de Capital

Políticas

Coordenação e Compliance

Monitoramento e Controle

Gestão de Penalidades

Descrição do Pilar

O domínio Monitoramento e Controle tem como objetivo realizar a gestão de todos os serviços suportados pelo departamento de TI, monitorando indicadores de desempenho e demais processos relacionados à Operação de Serviços.

Análise As Is

- Contratos estabelecidos entre a TI e fornecedores possuem penalidades previstas, porém, não foram identificadas práticas e nem processos formais para aplicação das penalidades previstas, quando aplicáveis.

Recomendações To Be

- Estabelecer processo de monitoramento dos serviços contratados.
- Na ocorrência de fatos geradores de penalidades previstas em contrato, acionar departamento jurídico e avaliar sua aplicabilidade.
- Aplicar as penalidades previstas em contrato, mediante entendimento junto ao departamento jurídico.



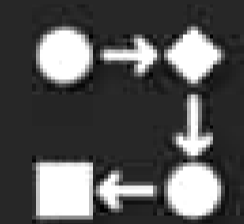
Painel



Estratégia



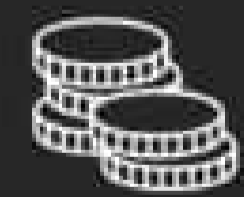
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Liderança

Planejamento

Alocação de Capital

Políticas

Coordenação e Compliance

Monitoramento e Controle

Gestão de Conhecimento

Descrição do Pilar

O domínio Monitoramento e Controle tem como objetivo realizar a gestão de todos os serviços suportados pelo departamento de TI, monitorando indicadores de desempenho e demais processos relacionados à Operação de Serviços.

Análise As Is

- Ausência de processos para registrar o conhecimento e disponibilizar para a equipe de TI.
- Ausência de processos para disponibilizar conhecimento aos usuários finais sobre soluções de problemas de baixa complexidade.

Recomendações To Be

- Implementar uma base de conhecimento da própria TI, como: Catálogo de lições aprendidas; Soluções de problemas; Scripts; etc.
 - Disponibilizar um FAQ para os usuários finais.
- Estabelecer processo de revisão para a base de conhecimento da TI e FAQ.



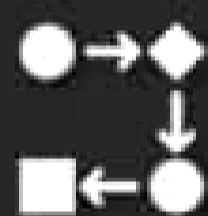
Painel



Estratégia



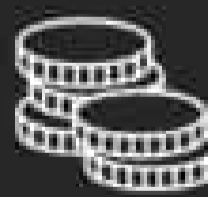
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Liderança

Planejamento

Alocação de Capital

Políticas

Coordenação e Compliance

Monitoramento e Controle

Gestão de Qualidade



Descrição do Pilar

O domínio Monitoramento e Controle tem como objetivo realizar a gestão de todos os serviços suportados pelo departamento de TI, monitorando indicadores de desempenho e demais processos relacionados à Operação de Serviços.

Análise As Is

- Não foram identificados processos formais de Gestão de Qualidade.
- Não foi identificada a realização de pesquisas de satisfação do usuário.

Recomendações To Be

- Definir critérios para a avaliação da qualidade dos serviços de TI, conforme os KPIs e OKRs definidos.
 - Definir processos formais para o monitoramento da qualidade dos serviços de TI.
- Implementar pesquisas de satisfação do usuário na finalização de chamados e periodicamente (pesquisa sazonal).

Clientes/Usuários da TI

Estratégia de transformação d...

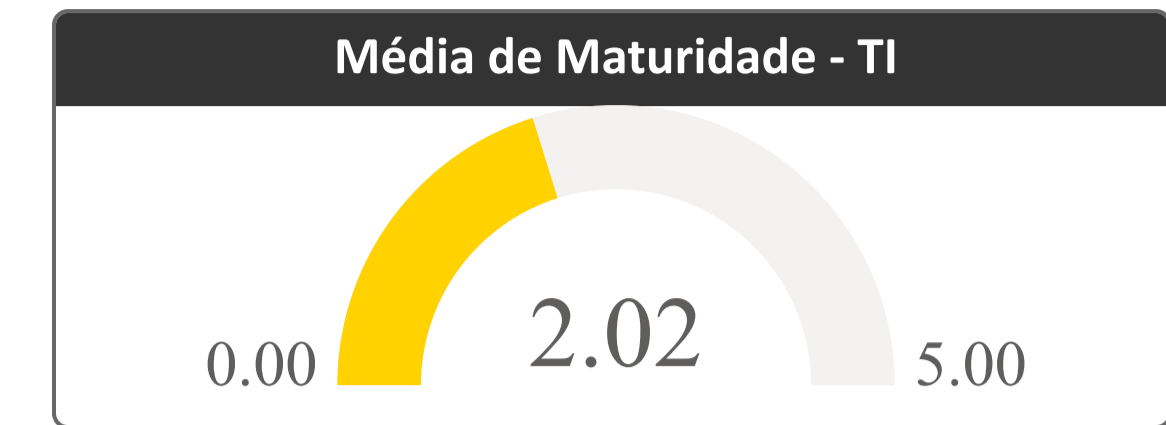
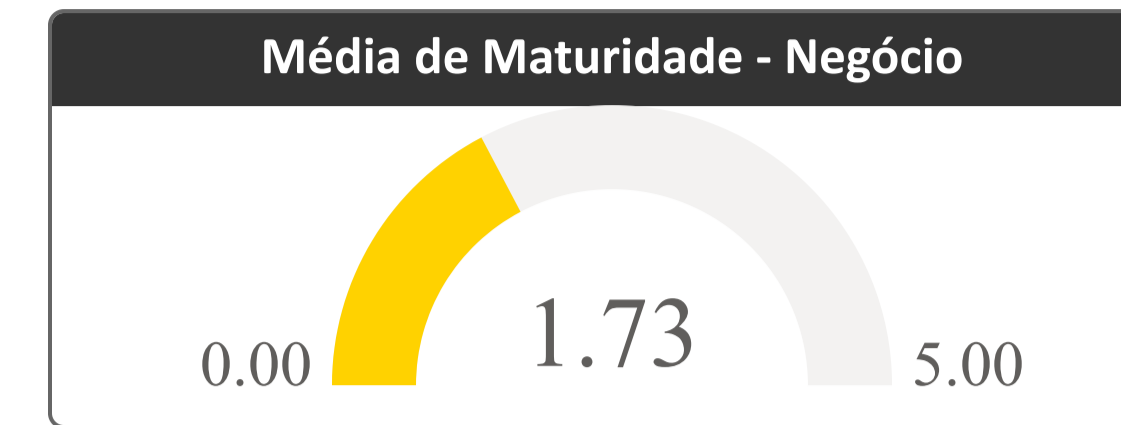
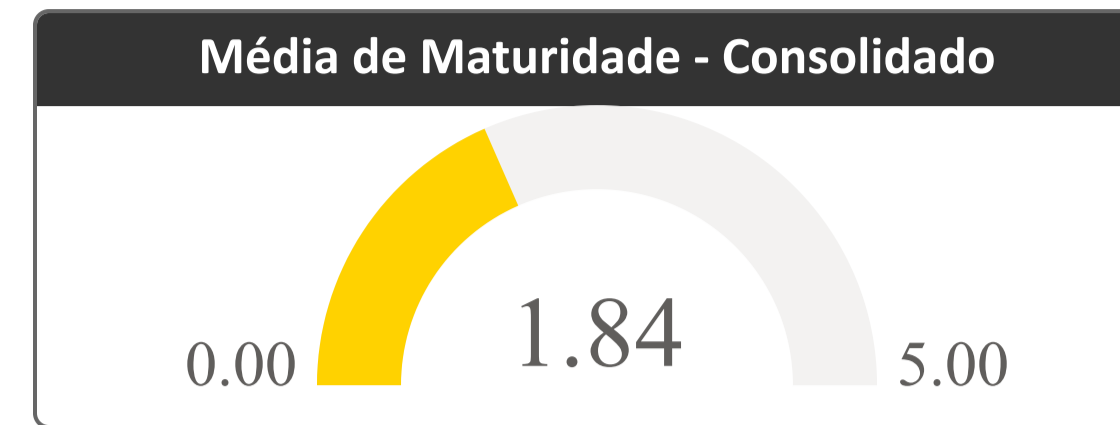
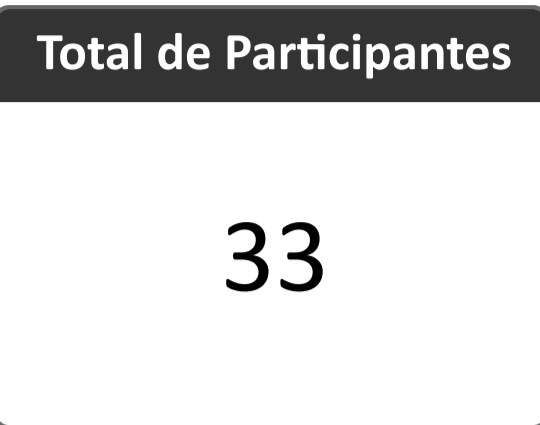
Gerenciamento da TI

Informação e Análise de dados

Operações e Suporte da TI

Resiliência, Riscos e Seguran...

Serviços e Soluções da TI


Classificação por Domínio

Domínio	Negócio	TI	Total
Estratégia de transformação da TI	1.04	1.63	1.26
Informação e Análise de dados	1.83	2.10	1.94
Serviços e Soluções da TI	1.93	2.06	1.98
Gerenciamento da TI	2.00	2.02	2.00
Resiliência, Riscos e Segurança da TI	1.93	2.12	2.02
Clientes/Usuários da TI	2.02	2.24	2.11
Operações e Suporte da TI	2.17	2.45	2.27
Total	1.73	2.02	1.84

Domínio por Função

Domínio	G	C	D	Total
<input type="checkbox"/> Operações e Suporte da TI	2.38	2.27	2.12	2.27
<input type="checkbox"/> Clientes/Usuários da TI	2.00	2.44	1.94	2.11
<input type="checkbox"/> Resiliência, Riscos e Segurança da TI	2.08	2.22	1.62	2.02
<input type="checkbox"/> Gerenciamento da TI	1.94	2.53	1.61	2.00
<input type="checkbox"/> Serviços e Soluções da TI	2.10	2.19	1.43	1.98
<input type="checkbox"/> Informação e Análise de dados	1.95	2.42	1.40	1.94
<input type="checkbox"/> Estratégia de transformação da TI	1.57	1.29	0.71	1.26
Total	1.95	2.05	1.46	1.84

Legenda: G - Gerente C - Coordenador D - Demais funções

Capacidade dos Domínios

Capacidades	Média
Campanhas da TI	2.92
Administração de identidade e acesso do usuário	2.82
Estratégia de entrega e suporte de serviços da TI	2.45
Plano de Comunicação da TI	2.40
Estratégia de informação e análise de dados	2.30
Implementações/lançamentos de serviços e soluções	2.29
Locais e instalações da TI	2.25
Desempenho dos serviços da TI	2.24
Gerenciamento de Serviços e Suporte da TI	2.23
Estratégia de transformação do cliente	2.22
Operações de suporte da TI	2.22
Gerenciamento de serviços da TI	2.21
Arquitetura de dados	2.18
Estratégia de Resiliência da TI	2.17
Gerenciamento de riscos da TI e resposta a crises	2.11
Gerenciamento de recursos de infraestrutura da TI	2.11
Relacionamento com o cliente	2.10
Gestão e Administração da TI	2.05
Estratégia e gerenciamento de terceiros de TI	2.04
Total	1.84

Detalhes das Perguntas

Perguntas	Média
Quão eficiente é o processo de gestão de identidade e acesso aos usuários?	3.07
Quão eficiente são as medidas técnicas e procedimentos estabelecidos para garantir que todos os usuários (internos, externos e temporários), e suas atividades em sistemas de TI (aplicativo de n...	3.00
Quanto as campanhas de TI geram valor aos seus clientes?	2.92
Qual o grau de uso de terceiros na estratégia de entrega de serviços?	2.86
Quão eficiente é o processo de solicitação de direitos de acesso do usuário?	2.71
Qual o grau de uso de terceiros na estratégia de suporte de serviços?	2.64
Quão automatizados são as medições dos níveis de serviço?	2.59
Quão eficiente é o tratamento das mudanças emergenciais ?	2.55
Quão atualizadas estão as identidades de usuário e direitos de acesso?	2.53
O quão integrada a gestão de riscos de privacidade está em relação ao processo de gestão de riscos corporativos?	2.50
Quanto os requisitos legais e/ou regulamentares estão implementados nas soluções sistêmicas que a TI oferece?	2.50
Quão eficiente é a arquitetura de dados?	2.50
Quão eficiente é sua estratégia de relacionamento com o cliente?	2.50
Quão estruturado está o processo de identificação e remediação de vulnerabilidades envolvendo identificação, comunicação, correção e rastreabilidade?	2.50
Quão eficiente é o Modelo de Entrega e Suporte de Serviços de TI?	2.47
Qual o nível de maturidade referente a inteligência de ameaças organizacionais e cibernéticas? (Este domínio ajuda uma organização a determinar se o seu programa de inteligência de ameaças est...	2.44
Quanto dos problemas ocorridos foram analisados as causas raízes?	2.44
Quão eficiente é o processo de avaliação de riscos de segurança?	2.44
Quão estável é o ambiente produtivo frente as mudanças planejadas e implementadas?	2.44
Total	1.84



Análise SWOT

A análise SWOT proporciona um diagnóstico completo da situação da própria empresa e dos ambientes que estão no seu entorno, de maneira que ajude a correr menos riscos e aproveitar as oportunidades.

O resultado da análise é uma matriz 2x2, chamada de Matriz SWOT, que divide os quatro pontos de análise: Forças, Fraquezas, Oportunidades e Ameaças.

Forças (Strengths)

Referem-se às iniciativas internas que estão com um bom desempenho. São os pontos positivos, que podem ser considerados como vantagens competitivas.

S

W

Fraquezas (Weaknesses)

Questões internas que podem ser ruins para o negócio ou iniciativas que estão com desempenho abaixo do esperado.

Oportunidades (Opportunities)

Fatores internos ou externos que podem influenciar positivamente, criando potencial de fazer crescer a vantagem competitiva.

O

T

Ameaças (Threats)

Aspectos negativos com potencial de comprometer o desempenho do negócio. Podem prejudicar o planejamento estratégico e os resultados.



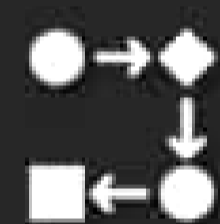
Painel



Estratégia



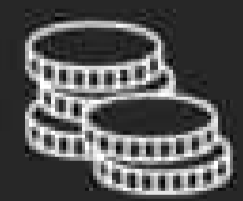
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Análise SWOT
Forças

- Infraestrutura descentralizada.
- Estrutura organizacional robusta.
- Resiliência da Equipe de TI.
- Diretoria incentiva a melhoria da TI.
- Todas as aplicações utilizam-se de modelos de arquitetura considerados seguros.
- 80% das aplicações administrativas possuem hospedagem em Cloud.

Fraquezas

- Relacionamento da TI com as áreas de negócio, para identificação de suas necessidades, incipiente.
- As áreas de negócio abrem chamados diretamente com fornecedores, sem que haja controle integrado para o acompanhamento pela TI.
 - Contratação de serviços e equipamentos de TI sem a anuência da TI.
 - Ausência de formalização dos Processos de TI.
 - Portifólio de Projetos de TI inexistente.
- Política de Segurança da Informação ainda não aprovada e implementada.
- Ausência de um plano de Continuidade do Negócio e Recuperação de Desastres.
- Ausência de indicadores para medição de monitoramento de alguns serviços.
 - Sistemas não integrados.
- 50% das aplicações possuem hospedagem On Premise (tanto data center interno quanto colocation).
 - 17% das aplicações utilizam banco de dados obsoletos.
- 18% das aplicações utilizam banco de dados que são hospedadas em servidor(es) com Sistema Operacional que já está obsoleto ou cujo ciclo de vida (EoL) está próximo.
- 70% das aplicações são hospedadas em servidor(es) com Sistema Operacional que já está obsoleto ou cujo ciclo de vida (EoL) está próximo.

Oportunidades

- A ausência ou simplicidade dos processos atuais da TI geram oportunidade para que pequenos ajustes alinhados às boas práticas viabilizem resultados significativos mais rapidamente.
- A consolidação de aplicações em uma plataforma centralizada e integrada tende a aumentar a eficiência do orçamento.
- Alinhamento das atividades da célula disruptiva ao modelo de governança definido pela TI.
 - Estreitamento da comunicação e relacionamento da TI com o negócio.
 - Migração da hospedagem das aplicações atualmente On Premise para Cloud.
 - Estruturação e Padronização do modelo de governança de dados.

Ameaças

- Mudanças na Legislação obrigando a TI a se adaptar.
- Ataques de hacking, explorando brechas e fragilidades em aplicações e sistemas operacionais não mais suportados.
- Interrupção prolongada das operações na ocorrência de desastres e/ou falhas catastróficas devido a ausência de Plano de Continuidade do Negócio e Recuperação de Desastre.



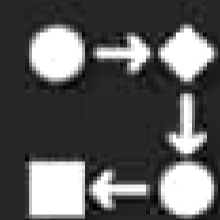
Painel



Estratégia



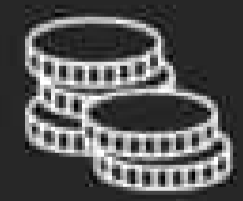
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

- Painel 
- Estratégia 
- Pessoas** 
- Processos 
- Tecnologia 
- Orçamento 
- Roadmap 
- Anexos 

ESTRUTURA ORGANIZACIONAL

Estrutura Atual

Designs Praticados no Mercado

Estrutura Proposta

O presente documento foi elaborado considerando princípios metodológicos da EY, conforme apresentado abaixo, focado no pilar de estratégia para desenhar a estrutura organizacional atual e sugerir a estrutura futura.

GESTÃO E INFORMAÇÃO

Governança nos mostra a clareza dos papéis e responsabilidades no processo decisório de forma transversal.

Sistema de Gerenciamento – Nível de alinhamento das obrigoriedades envolvendo acordo com sindicatos, terceirização, contratos, políticas e regulamentos.

Tecnologia e Informação influencia a forma como as pessoas trabalham, automatizam atividades e devem ser geridas por pessoas.

ALINHAMENTO ESTRATÉGICO

Estratégia deve balizar o desenho da estrutura organizacional trazendo alinhamento de como a TI se organiza com as prioridades das áreas e reflexo na estrutura.

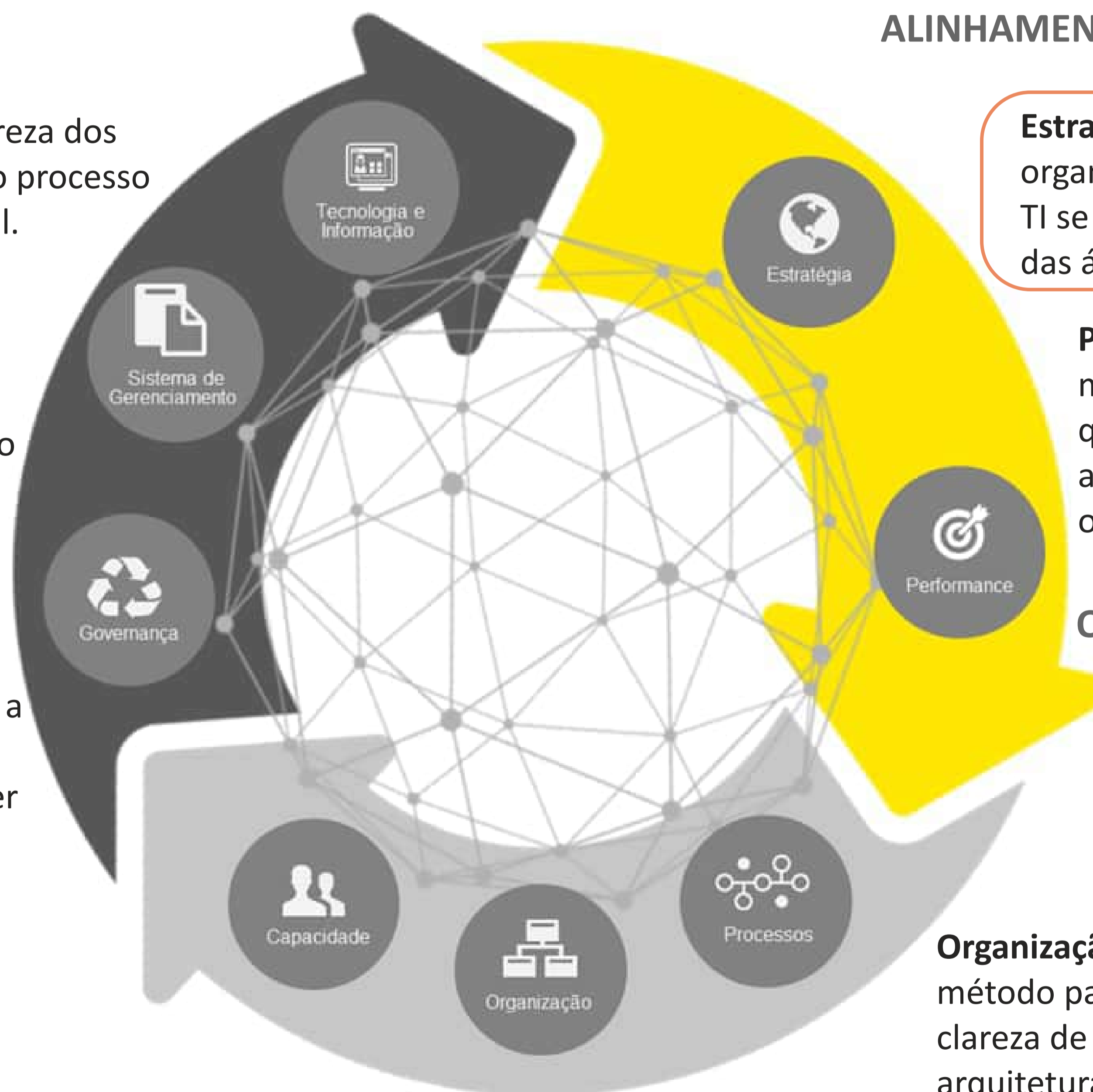
Performance deve ser considerada para modelagem da organização de TI, de modo que os objetivos e expectativas relacionadas a performance não encontrem obstáculos organizacionais na TI.

ORGANIZAÇÃO

Processos efetivados, incluindo formalização, atualização, eficiência, conhecimento e tem impacto transversal na estrutura organizacional.

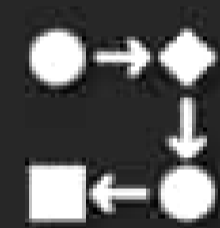
Organização com otimização de span of control, método para dimensionamento de força de trabalho, clareza de papéis e responsabilidades e princípios de arquitetura.

Capacidade é a gestão da força de trabalho envolvendo competitividade de remuneração, definição e clareza das competências requeridas, planos de desenvolvimento e sucessão.



Legenda:

Escopo da análise



Painel

Estratégia

Pessoas

Processos

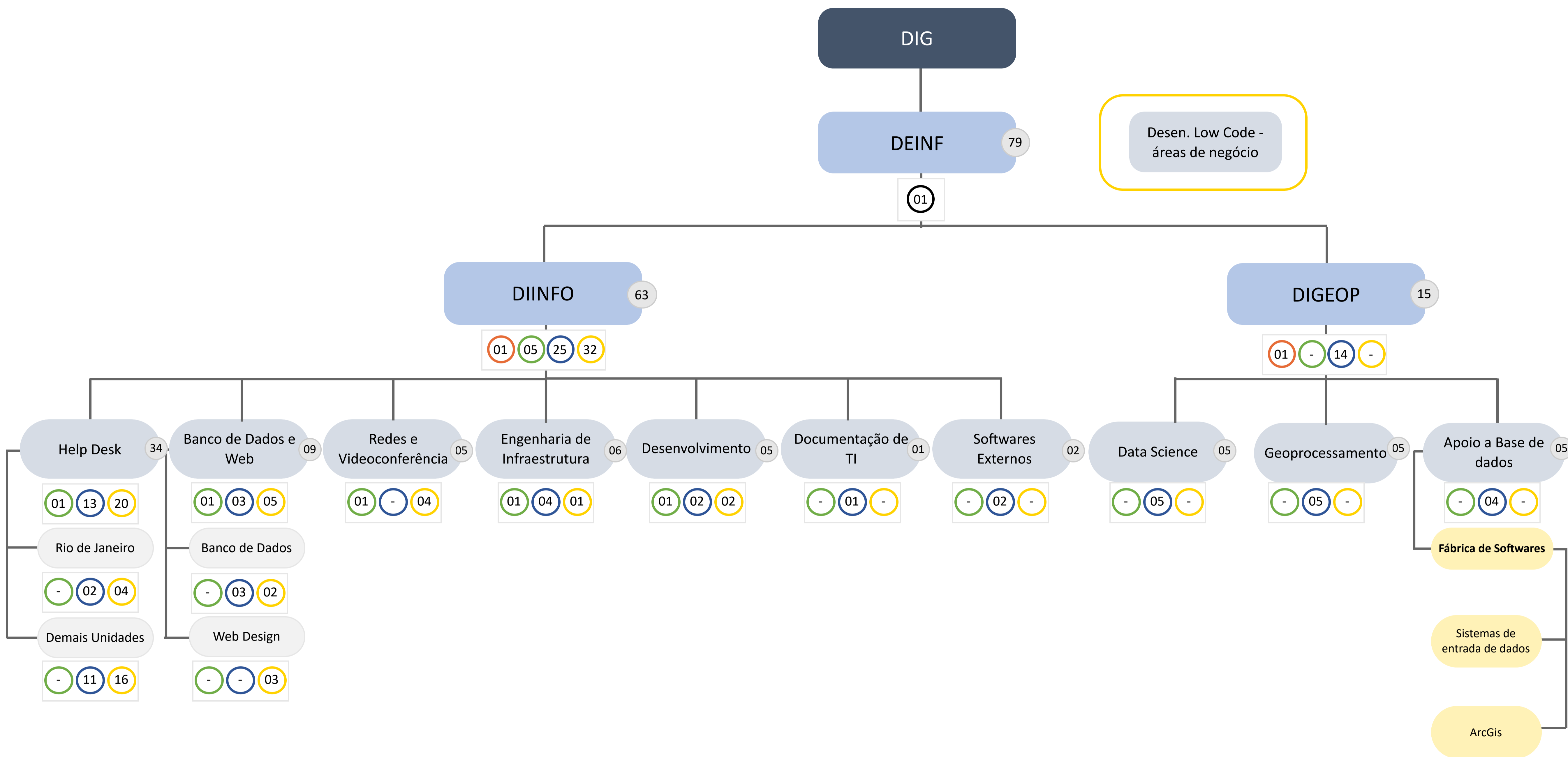
Tecnologia

Orçamento

Roadmap

MAPEAMENTO DA ESTRUTURA ORGANIZACIONAL ATUAL DA TI

- Painel
- Estratégia
- Pessoas**
- Processos
- Tecnologia
- Orçamento
- Roadmap



Legenda:

Diretoria	79 Total de FTEs
Divisões	01 Chefes de Departamento
Coordenações	02 Chefes de Divisão
Macro Responsabilidades	05 Coordenadores
Outsourcing	39 Colaboradores
	32 Terceiros

47 Próprios = 01 (Chefe de Departamento) + 02 (Chefes de Divisão) + 05 (Coordenadores) + 39 (Colaboradores)

Foram considerados como FTE os colaboradores próprios e terceiros. Os terceiros são profissionais cujo modelo de trabalho é bodyshop.

O escopo da análise engloba apenas colaboradores da área de TI.

A fábrica de software é constituída por duas entidades externas, que prestam serviço terceirizado sob demanda. O FTE da fábrica de software não foi adicionado ao quantitativo da área de TI.

Também está representado, núcleo que desenvolve soluções Low Code e que não possui governança por TI.

MAPEAMENTO DA ESTRUTURA ORGANIZACIONAL ATUAL DA TI



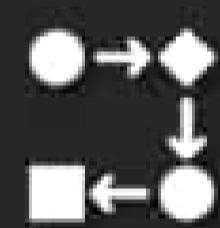
Painel



Estratégia



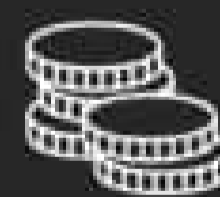
Pessoas



Processos



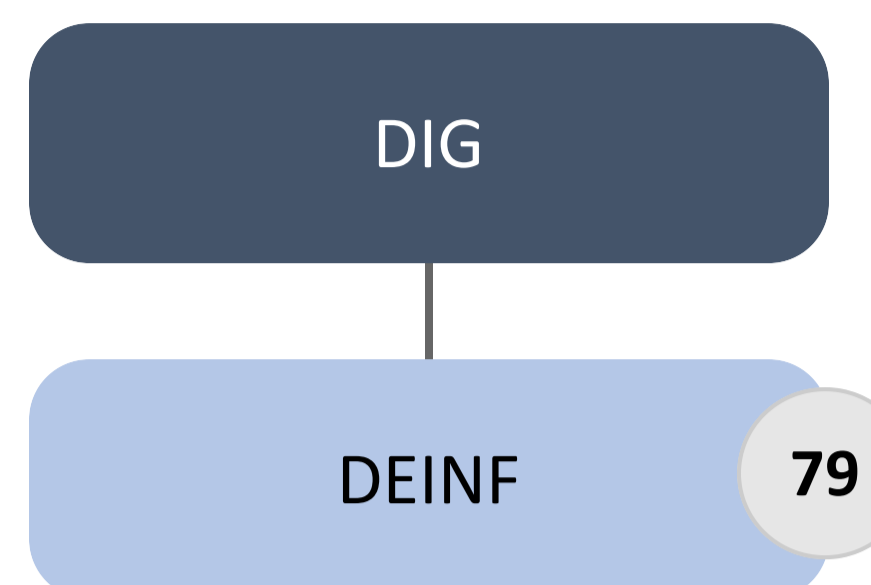
Tecnologia



Orçamento



Roadmap



Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista PI	Analista Jr	Terceiros
79	01	02	05	27	10	02	32

Responsabilidades

A DEINF (Departamento de Informações Institucionais) é um departamento que está subordinado à DIG (Diretoria de Infraestrutura Geocientífica), que tem por objetivo o estudo, planejamento, controle, coordenação e implantação de técnicas voltadas para a captura, armazenamento, tratamento, análise e a disseminação de informações do SGB. Que por sua vez, tem diversas atribuições sob a sua responsabilidade, sendo elas as seguintes:

- Promover a infraestrutura de Tecnologia da Informação e Rede de Comunicações (TIC) adequadas ao desenvolvimento das atividades;
- Promover e coordenar a adoção de padrões para a captura, armazenamento, tratamento, análise e disseminação de informações institucionais;
- Promover, coordenar, desenvolver e manter sistemas e plataformas de informações e documentação;
- Promover e coordenar a alimentação e a manutenção das Bases de Dados;
- Promover e coordenar o desenvolvimento e a disseminação do uso de metodologias e procedimentos de tratamento digital, de análise espacial de dados geocientíficos e de construção de modelos, envolvendo todas as áreas da Geomática como a cartografia, banco de dados, desenvolvimento, geoprocessamento e sensoriamento remoto;
- Analisar e propor alternativas adequadas de informatização, inclusive a padronização de hardwares, softwares e periféricos;
- Emitir documentos normativos, definindo as metodologias e procedimentos relativos à sua área de atuação;
- Cumprir e fazer cumprir as determinações e diretrizes previstas no Plano Diretor de Tecnologia da Informação – PDTI;
- Promover a integração dos órgãos administrativos internos com as áreas técnicas por meio de sistemas e plataformas corporativas de gestão (Enterprise Resource Planning – ERP).

MAPEAMENTO DA ESTRUTURA ORGANIZACIONAL ATUAL DA TI



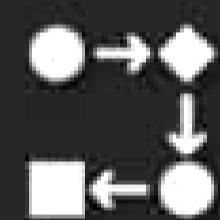
Painel



Estratégia



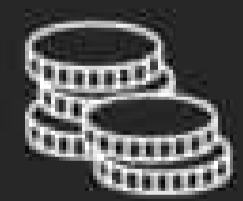
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

DIINFO

63

Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
63	-	01	05	13	10	02	32

Responsabilidades

A DIINFO (Divisão de Informática) é uma das divisões que estão subordinadas à DEINF, em que são atribuídas as seguintes responsabilidades:

- Definir a instalação de equipamentos locais e remotos, voltada para redes de teleprocessamento, coordenando a execução dos trabalhos;
- Operar os equipamentos de Processamento Eletrônico de Dados de grande porte, executando as rotinas normais de produção e garantindo a disponibilidade dos recursos computacionais para a comunidade de usuários;
- Administrar a rede corporativa de teleprocessamento do SGB;
- Avaliar e controlar o desempenho dos equipamentos de grande porte, adotando as medidas adequadas para a sua melhoria;
- Manter contatos com representantes e fornecedores de hardwares, visando a atualização tecnológica e sugerindo a sua implantação no SGB;
- Desenvolver e efetuar a manutenção dos sistemas do SGB, realizando os treinamentos de usuários para a sua utilização;
- Definir padrões e procedimentos para a documentação de aplicações e sistemas, bem como proceder a sua elaboração e atualização;
- Definir padrões de instalação e de utilização de recursos em redes de teleprocessamento;
- Prestar consultoria e assistência técnica aos usuários para desenvolverem, em computador, as soluções adequadas aos seus problemas;
- Treinar usuários para a utilização dos recursos computacionais e de teleprocessamento;
- Coordenar, com a participação das áreas de usuários, a realização de planos globais de informática, segundo as diretrizes do Plano Diretor de Informática.

MAPEAMENTO DA ESTRUTURA ORGANIZACIONAL ATUAL DA TI



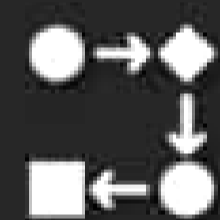
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

DIGEOP 15

Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
15	-	01	-	14	-	-	-

Responsabilidades

A DIGEOP (Divisão de Geoprocessamento) é uma das divisões que estão subordinadas à DEINF, em que são atribuídas as seguintes responsabilidades:

- Efetuar o desenvolvimento, a implantação, a documentação e a manutenção de sistemas e aplicativos geocientíficos, inclusive utilizando tecnologia de GIS (Sistemas de Informações Geográficas);
- Supervisionar e coordenar a aplicação de tratamento digital e de análise espacial de dados nas Unidades Regionais do SGB;
- Supervisionar e coordenar os trabalhos de captura e crítica de dados geocientíficos, visando o armazenamento dos dados e informações nas bases de dados institucionais do SGB;
- Modelar, implantar, manter e administrar as bases de dados geocientíficos do SGB;
- Definir e implantar procedimentos para a captura e para a alimentação das bases de dados, inclusive de dados obtidos por meio de cartografia digital;
- Desenvolver e propor metodologias e técnicas de integração e análise multitemática de dados digitais, inclusive com dados de sensores remotos, para serem adotados nas atividades do SGB;
- Estudar e propor metodologias de construção de modelos, utilizando o tratamento digital e a análise espacial de dados;
- Desenvolver metodologias de uso, conversão e utilização de dados geocientíficos provenientes das bases de dados do SGB, para aplicação em atividades da Companhia;
- Estudar e propor metodologias para a consistência e a documentação de dados e informações existentes nas bases de dados do SGB;
- Estabelecer padrões para a captura, armazenamento e intercâmbio de dados e informações geocientíficas digitais;
- Estabelecer padrões para o tratamento digital de dados e informações geocientíficas básicas, visando a sua integração e/ou a geração de produtos;
- Estudar e definir padrões de softwares para a utilização na área de geoprocessamento, inclusive de captura de dados.

MAPEAMENTO DA ESTRUTURA ORGANIZACIONAL ATUAL DA TI



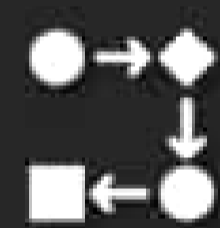
Painel



Estratégia



Pessoas



Processos



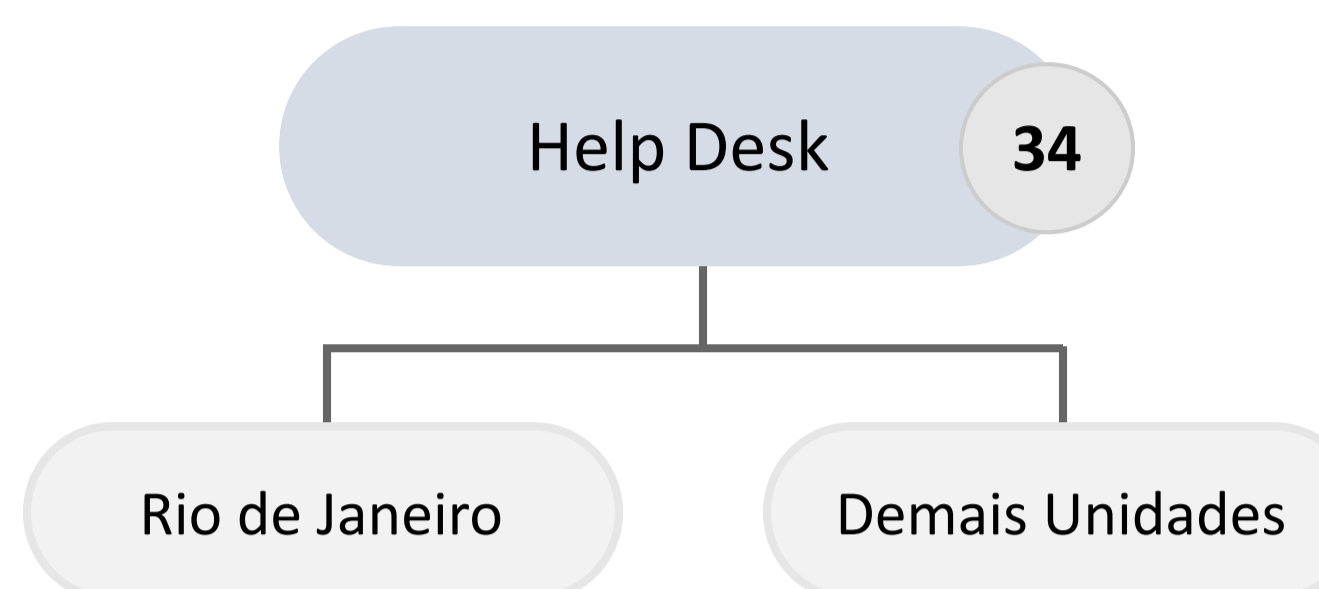
Tecnologia



Orçamento



Roadmap



Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
34	-	-	01	01	10	02	20

Detalhamento FTEs

- Belém - PA: 01 Analista Pleno e 01 Terceirizado;
- Belo Horizonte - MG: 02 Analista Pleno e 01 Terceirizado;
- Brasília - DF: 02 Analista Pleno e 01 Terceirizado;
- Fortaleza - CE: 01 - Analista Pleno e 01 - Terceirizado;
- Goiânia - GO: 02 Terceirizados;
- Manaus - AM: 01 Analista Pleno e 01 Terceirizado;
- Porto Alegre - RS: 01 Analista Pleno e 02 Terceirizados;
- Porto Velho - RO: 01 Terceirizado;
- Recife - PE: 01 Analista Pleno e 01 Terceirizado;
- Rio de Janeiro - RJ: 01 Coordenador, 02 Analista Junior e 04 Terceirizados;
- Salvador - BA: 01 Analista Sênior e 02 Terceirizados;
- São Paulo - SP: 01 Analista Pleno e 02 Terceirizados;
- Teresina - PI: 01 Terceirizado.

Reponsabilidades

O Help Desk possui infraestrutura operacional instalada em 13 unidades espalhadas pelo Brasil, tendo sua sede no Escritório Central da administração localizado no Rio de Janeiro. O quantitativo operacional de cada unidade é definido com base no volume de demandas por unidade. O Help Desk é uma das áreas da DIINFO, em que são atribuídas as seguintes responsabilidades:

- Suportes N1 e N2 ao usuário final;
- Gestão de incidentes e requisições;
- *Facilities* de TI nas localidades;
- Manutenção do parque tecnológico.

MAPEAMENTO DA ESTRUTURA ORGANIZACIONAL ATUAL DA TI



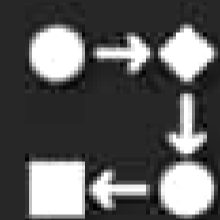
Painel



Estratégia



Pessoas



Processos



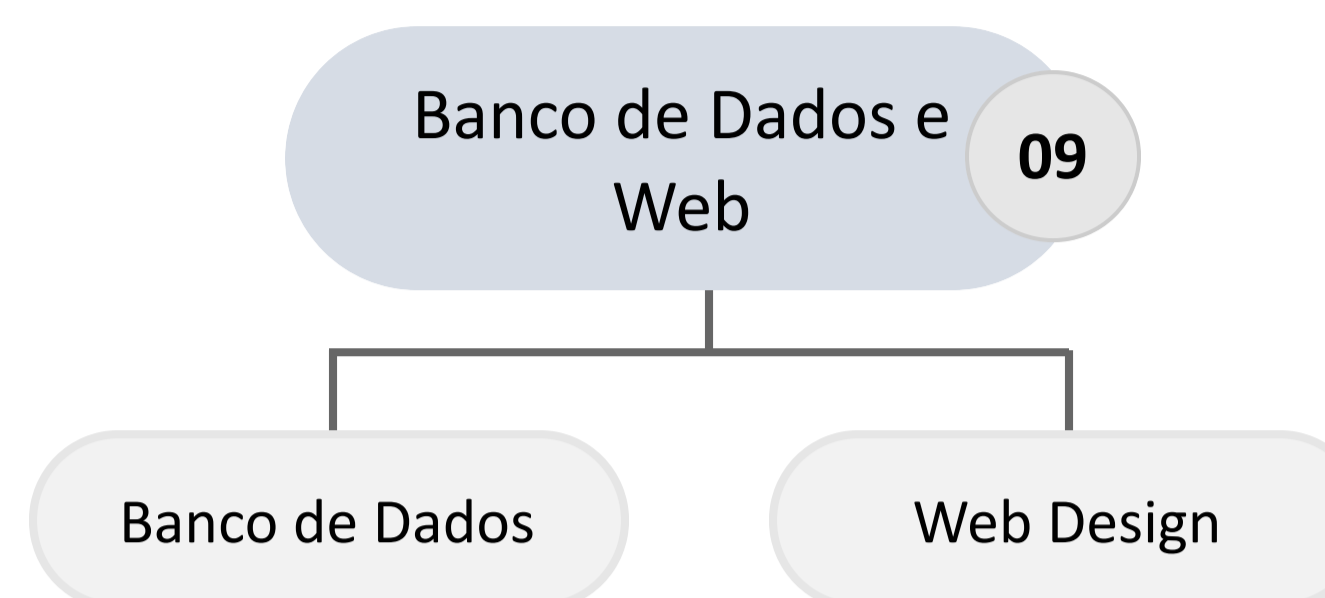
Tecnologia



Orçamento



Roadmap



Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
09	-	-	01	03	-	-	05

Responsabilidades

A coordenação Banco de Dados e Web é segmentada em Banco de Dados e Web Design que se reportam ao mesmo coordenador. É uma das áreas da DIINFO e possui as seguintes responsabilidades:

- **Banco de Dados:**
 - Gerenciar o Banco de Dados da empresa (SQLServer, PostgreSQL e Oracle);
 - Realizar alterações e customizações no Banco de Dados.
- **Web Design:**
 - Modificação e customização dos sites, portais e intranet do SGB, conforme a demanda das áreas de negócio e administrativa.

MAPEAMENTO DA ESTRUTURA ORGANIZACIONAL ATUAL DA TI ←



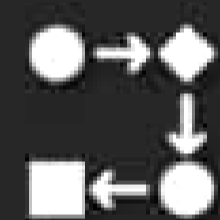
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Redes e Videoconferência **05**

Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
05	-	-	01	-	-	-	04

Responsabilidades

Redes e Videoconferência é uma das áreas da DIINFO, em que são atribuídas as seguintes responsabilidades:

- Gerenciamento da rede cabeada, distribuição geral de rede, conectorização, organização de racks;
- Configurações de switch e roteadores;
- Transmissão de videoconferência e operação dos equipamentos de vídeo;
- Apoio em eventos que necessitam de transmissão de vídeo.

MAPEAMENTO DA ESTRUTURA ORGANIZACIONAL ATUAL DA TI



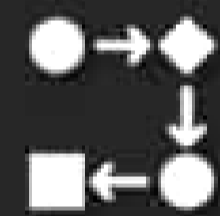
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Engenharia de Infraestrutura **06**

Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
06	-	-	01	04	-	-	01

Responsabilidades

Engenharia de Infraestrutura é uma das áreas da DIINFO, em que são atribuídas as seguintes responsabilidades:

- Gestão da infraestrutura de TI;
- Gestão do Datacenter;
- Gestão de acesso;
- Gestão da Segurança da Informação;
- Atendimento de chamados N3;
- Definição de políticas e padrões.

MAPEAMENTO DA ESTRUTURA ORGANIZACIONAL ATUAL DA TI



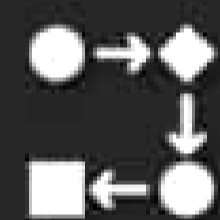
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Desenvolvimento **05**

Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
05	-	-	01	02	-	-	02

Responsabilidades

Desenvolvimento é uma das áreas da DIINFO, em que são atribuídas as seguintes responsabilidades:

- Desenvolvimento de aplicações administrativos;
- Manutenção de sistemas administrativos;
- Apoio a DIGEOP na fábrica de softwares para aplicações de negócio.

MAPEAMENTO DA ESTRUTURA ORGANIZACIONAL ATUAL DA TI



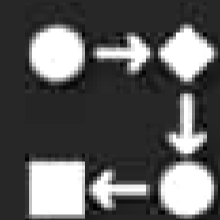
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Documentação de TI **01**

Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
01	-	-	-	01	-	-	-

Responsabilidades

Documentação de TI é uma das áreas da DIINFO, em que são atribuídas as seguintes responsabilidades:

- Elaboração dos normativos da TI.

MAPEAMENTO DA ESTRUTURA ORGANIZACIONAL ATUAL DA TI



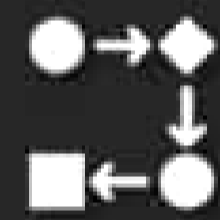
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Softwares Externos

02

Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
02	-	-	-	02	-	-	-

Responsabilidades

Softwares Externos é uma das áreas da DIINFO, em que são atribuídas as seguintes responsabilidades:

- Customização de softwares externos governamentais de uso obrigatório;
- Manutenção de softwares externos governamentais de uso obrigatório;
- Suporte aos usuários de softwares externos governamentais de uso obrigatório.

MAPEAMENTO DA ESTRUTURA ORGANIZACIONAL ATUAL DA TI

Data Science **05**

Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
05	-	-	-	05	-	-	-

Responsabilidades

Data Science é uma das áreas da DIGEOP, em que são atribuídas as seguintes responsabilidades:

- Estudar e definir padrões de softwares para a utilização na área de geoprocessamento, inclusive de captura de dados;
- Efetuar o desenvolvimento, a implantação, a documentação e a manutenção de sistemas e aplicativos geocientíficos, inclusive utilizando tecnologia de GIS (Sistemas de Informações Geográficas);
- Relacionamento com as áreas de negócio.



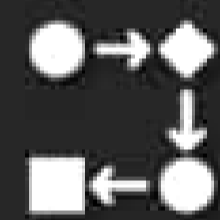
Painel



Estratégia



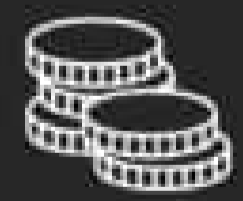
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

MAPEAMENTO DA ESTRUTURA ORGANIZACIONAL ATUAL DA TI



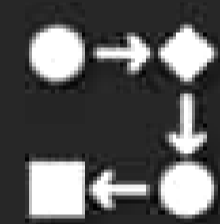
Painel



Estratégia



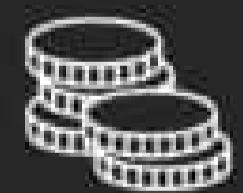
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Geoprocessamento **05**

Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
05	-	-	-	05	-	-	-

Responsabilidades

Geoprocessamento é uma das áreas da DIGEOP, em que são atribuídas as seguintes responsabilidades:

- Coordenar e supervisionar a aplicação de tratamento digital e de análise espacial de dados nas Unidades Regionais do SGB;
- Coordenar e supervisionar os trabalhos de captura e crítica de dados geocientíficos, visando o armazenamento dos dados e informações nas bases de dados institucionais do SGB;
- Apoio a área de negócio na transformação de dados (geoprocessamento) ou na utilização de softwares específicos (QGIS, ArcGIS Pro ou ArcMap);
- Responsável por treinamentos de geoprocessamento.

MAPEAMENTO DA ESTRUTURA ORGANIZACIONAL ATUAL DA TI



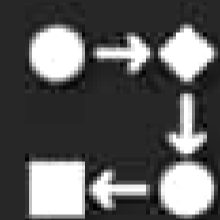
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Apoio à Base de Dados **04**

Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
04	-	-	-	04	-	-	-

Responsabilidades

Apoio à Base de Dados é uma das áreas da DIGEOP, em que são atribuídas as seguintes responsabilidades:

- Manutenção dos Bancos de Dados Geocientíficos;
- Gestão da fábrica de softwares externa;
- Estruturação de novas bases de dados, modelagem (modelo lógico e físico);
- Desenvolver metodologias de uso, conversão e utilização de dados geocientíficos provenientes das bases de dados, para aplicação em atividades;
- Estudar e propor metodologias para a consistência, documentação dos dados e informações existentes nas bases de dados;
- Estabelecer padrões para a captura, armazenamento e intercâmbio de dados e informações geocientíficas digitais;
- Estabelecer padrões para o tratamento digital de dados e informações geocientíficas básicas, visando a sua integração e/ou a geração de produtos.

MAPEAMENTO DA ESTRUTURA ORGANIZACIONAL ATUAL DA TI



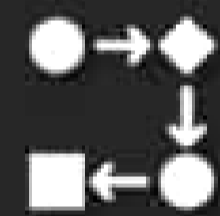
Painel



Estratégia



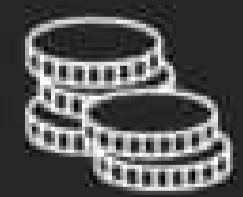
Pessoas



Processos



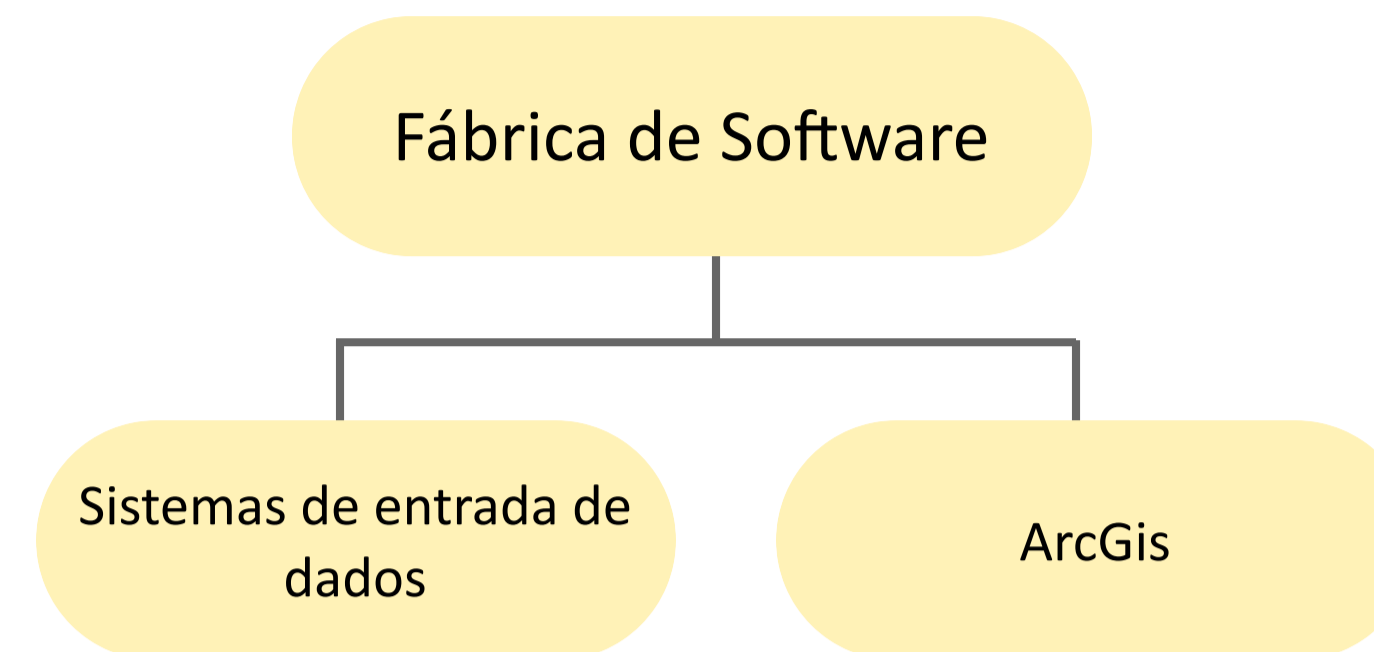
Tecnologia



Orçamento



Roadmap



Responsabilidades

A fábrica de software é composta por duas organizações distintas, sendo segregada pelos serviços ofertados, sendo eles: Sistemas de entrada de dados e o representante da plataforma ArcGis no Brasil. A fábrica está subordinada a área Apoio à Base de Dados, em que são atribuídas as seguintes responsabilidades:

Sistemas de entrada de dados:

- Construção de sistemas de entrada de dados e apresentação de dados;
- Jornada da descoberta (Levantamento da demanda e prototipação, após a aprovação eles procedem para construção e documentação);

Representante da plataforma ArcGis:

- Customização de funcionalidades na plataforma ArcGIS;
- Desenvolvimento de produtos que são extensões da plataforma ArcGIS.



DESIGNS PRATICADOS NO MERCADO ↩

Diante dos desafios existentes para a TI do SGB e oportunidade de alinhamento com as necessidades e expectativas das áreas de negócio, entende-se que a Estrutura Organizacional Futura deve ser híbrida, operando no modelo organizacional Bimodal.



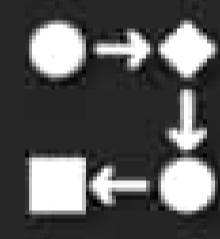
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



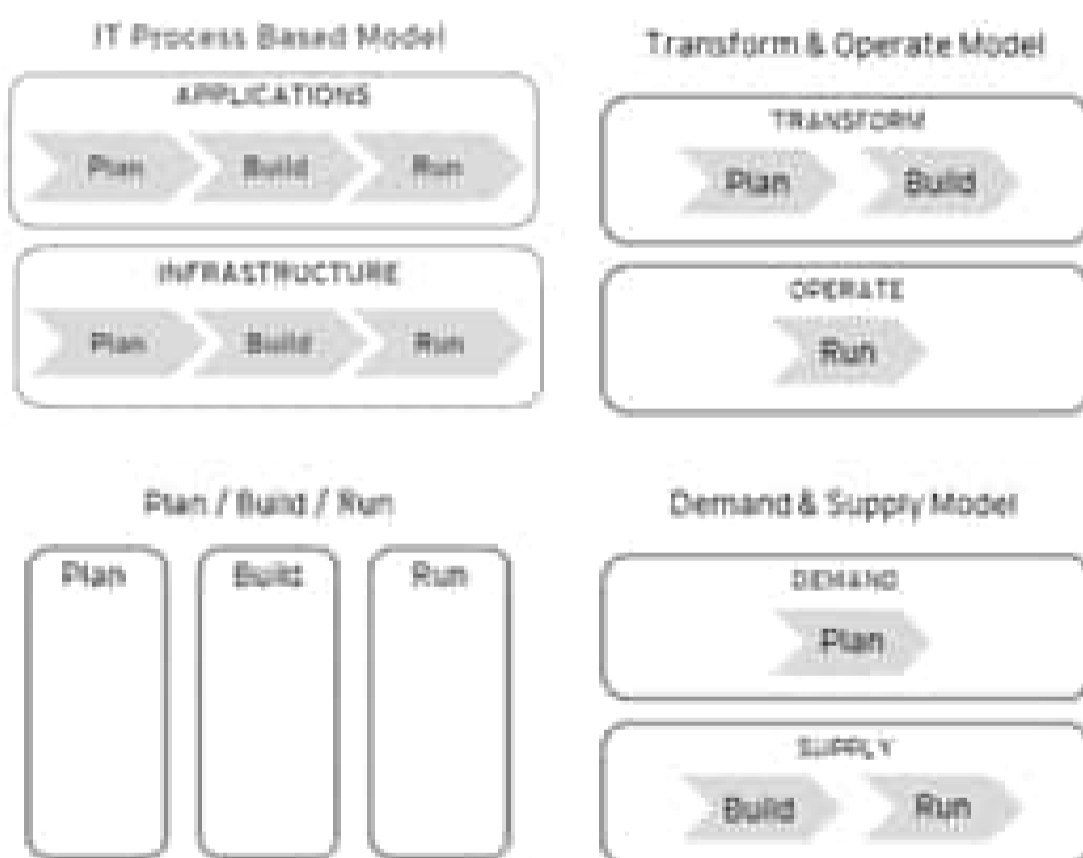
Roadmap

ORGANIZAÇÃO TRADICIONAL

Estrutura organizacional clássica, com hierarquia clara e equipes orientadas para o funcionamento em silos, projetadas para previsibilidade e eficiência.



Exemplos

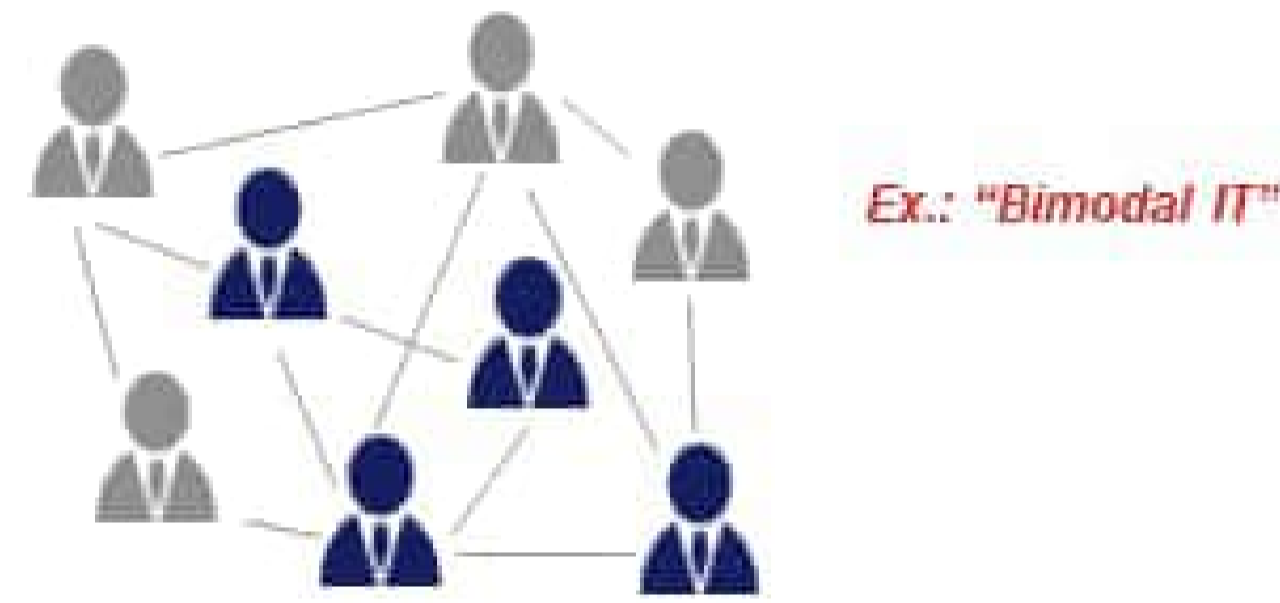


Ex.: "Service Broker"
Ex.: "Source Make Deliver"

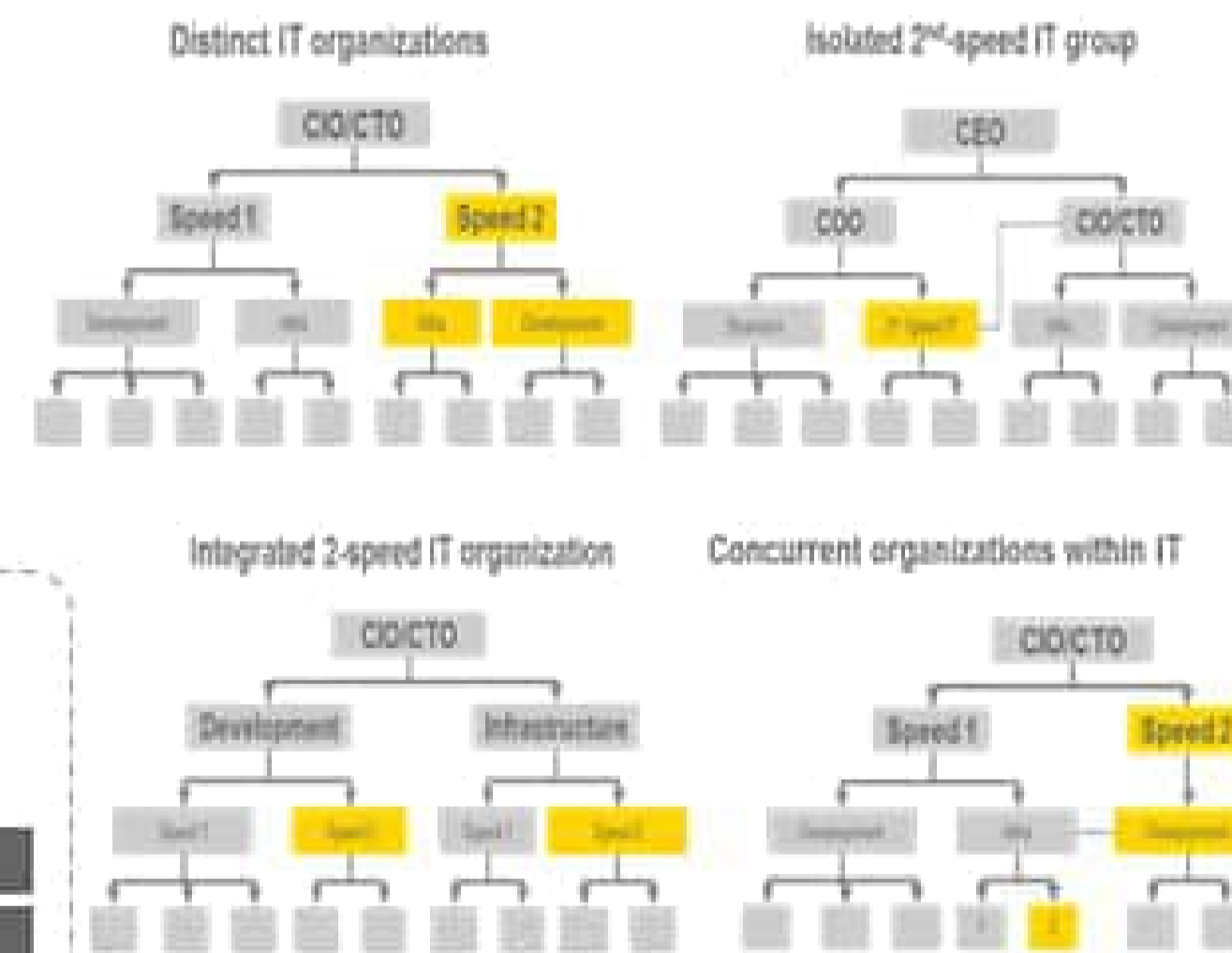
Serviço
Integração &
Gestão

ORGANIZAÇÃO HÍBRIDA

Organização clássica, tradicional, com elementos ágeis e estruturas de relacionamento.

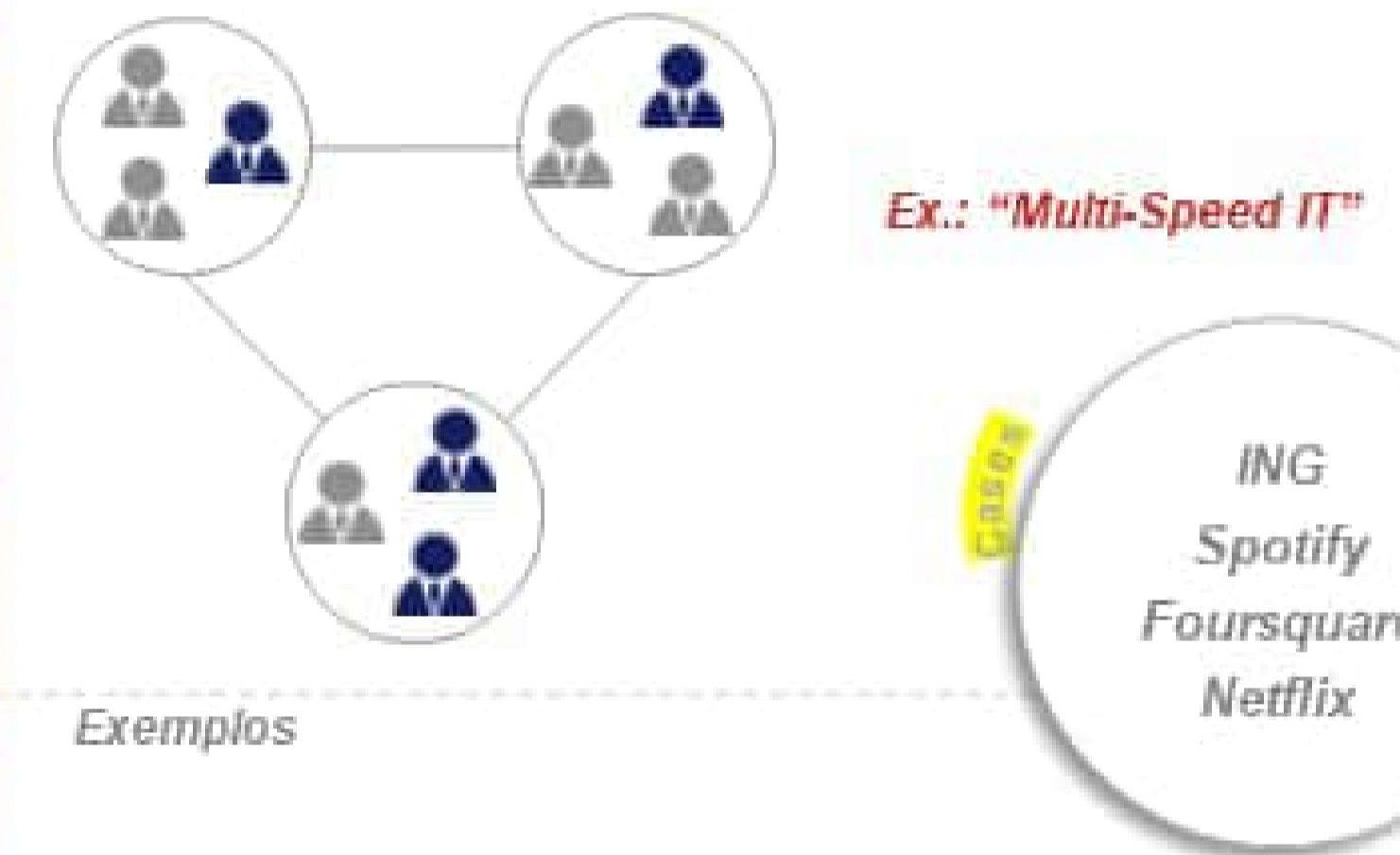


Exemplos

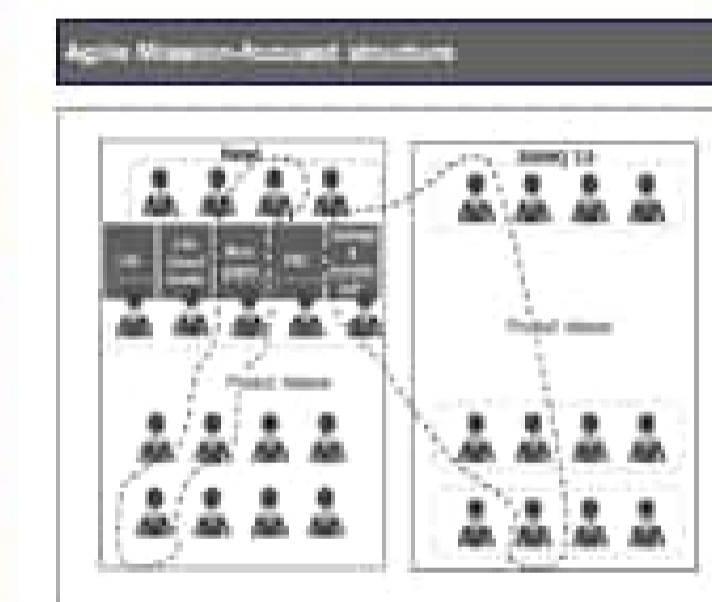


ORGANIZAÇÃO ÁGIL

"Organismo" ágil, multifuncional, auto organizável, equipes E2E, sistemas autônomos.



Exemplos



Equipes temporárias formadas para liberar produtos. A estrutura típica permanece a mesma.

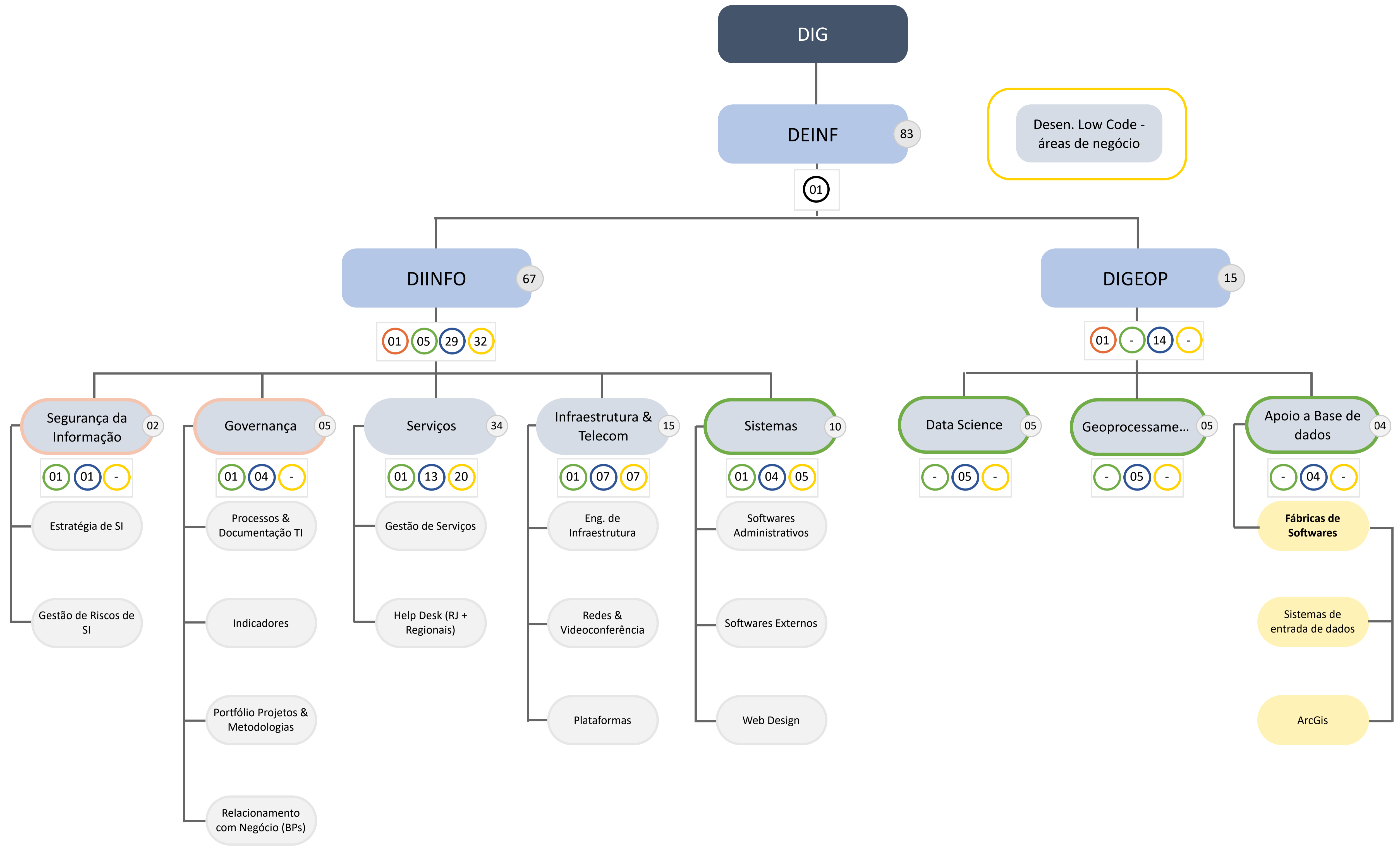


Permanentemente em estado Ágil: existe uma variedade de formações para desenvolver, melhorar e liberar produtos, incluindo foco nas áreas de interesse dos funcionários.



PROPOSTA FUTURA DA ESTRUTURA ORGANIZACIONAL DA TI ⏪

- Painel
- Estratégia
- Pessoas**
- Processos
- Tecnologia
- Orçamento
- Roadmap



Desen. Low Code - áreas de negócio

Legenda:

51 Próprios = 01 (Chefe de Departamento) + 02 (Chefes de Divisão) + 05 (Coordenadores) + 43 (Colaboradores)

83 Total de FTEs
01 Chefes de Departamento
02 Chefes de Divisão
05 Coordenadores
43 Colaboradores
32 Terceiros

Diretoria

Divisões

Coordenações

Macro Responsabilidades

Outsourcing

Áreas novas de suporte p/ demais

Modal Ágil

PROPOSTA FUTURA DA ESTRUTURA ORGANIZACIONAL DA TI

DEINF **83**

Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
84	01	02	05	27	14	02	32

Responsabilidades Atuais

- Promover a infraestrutura de Tecnologia da Informação e Rede de Comunicações (TIC) adequadas ao desenvolvimento das atividades;
- Promover e coordenar a adoção de padrões para a captura, armazenamento, tratamento, análise e disseminação de informações institucionais;
- Promover, coordenar, desenvolver e manter sistemas e plataformas de informações e documentação;
- Promover e coordenar a alimentação e a manutenção das Bases de Dados;
- Promover e coordenar o desenvolvimento e a disseminação do uso de metodologias e procedimentos de tratamento digital, de análise espacial de dados geocientíficos e de construção de modelos, envolvendo todas as áreas da Geomática como a cartografia, banco de dados, desenvolvimento, geoprocessamento e sensoriamento remoto;
- Analisar e propor alternativas adequadas de informatização, inclusive a padronização de hardwares, softwares e periféricos;
- Emitir documentos normativos, definindo as metodologias e procedimentos relativos à sua área de atuação;
- Cumprir e fazer cumprir as determinações e diretrizes previstas no Plano Diretor de Tecnologia da Informação – PDTI;
- Promover a integração dos órgãos administrativos internos com as áreas técnicas por meio de sistemas e plataformas corporativas de gestão (Enterprise Resource Planning – ERP).



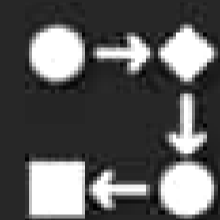
Painel



Estratégia



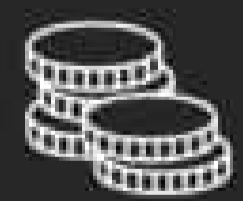
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

PROPOSTA FUTURA DA ESTRUTURA ORGANIZACIONAL DA TI



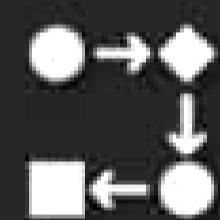
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

DIINFO

67

Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
67	-	01	05	13	14	02	32

Responsabilidades Atuais

- Definir a instalação de equipamentos locais e remotos, voltada para redes de teleprocessamento, coordenando a execução dos trabalhos;
- Operar os equipamentos de Processamento Eletrônico de Dados de grande porte, executando as rotinas normais de produção e garantindo a disponibilidade dos recursos computacionais para a comunidade de usuários;
- Administrar a rede corporativa de teleprocessamento do SGB;
- Avaliar e controlar o desempenho dos equipamentos de grande porte, adotando as medidas adequadas para a sua melhoria;
- Manter contatos com representantes e fornecedores de hardwares, visando a atualização tecnológica e sugerindo a sua implantação no SGB;
- Desenvolver e efetuar a manutenção dos sistemas do SGB, realizando os treinamentos de usuários para a sua utilização;
- Definir padrões e procedimentos para a documentação de aplicações e sistemas, bem como proceder a sua elaboração e atualização;
- Definir padrões de instalação e de utilização de recursos em redes de teleprocessamento;
- Prestar consultoria e assistência técnica aos usuários para desenvolverem, em computador, as soluções adequadas aos seus problemas;
- Treinar usuários para a utilização dos recursos computacionais e de teleprocessamento;
- Coordenar, com a participação das áreas de usuários, a realização de planos globais de informática, segundo as diretrizes do Plano Diretor de Informática.

Responsabilidades Adicionais

Equipe e Desenvolvimento de Liderança

- Conduzir a integração das equipes de TI, compartilhando uma visão clara da estratégia de sinergia e novos papéis e responsabilidades nas camadas de gestão.
- Supervisionar o desenvolvimento e a implementação de um plano de força de trabalho estratégico para maximizar a eficácia da força de trabalho atual e futura, à luz das prioridades estratégicas da firma.
- Formar a próxima geração de líderes e supervisionar os programas de desenvolvimento de habilidades dos funcionários.
- Atuar na retenção de talentos críticos.

Definição de Direção Estratégica

- Manter-se a par das tendências digitais e empresariais emergentes e colaborar com outros líderes empresariais para incorporar oportunidades digitais na estratégia de negócio.
- Desenvolver e executar uma estratégia de TI que aproveita as tecnologias emergentes para contribuir com a estratégia de negócio.
- Compartilhar informações estratégicas com os pares e o negócio sobre as mudanças corporativas que sustentam o sucesso na digitalização.
- Trabalhar com as partes interessadas para otimizar continuamente os processos de governança e tomada de decisão de TI, à medida que o contexto de negócio e o cenário de tecnologia mudam.

Serviço e Entrega de Produtos

- Fornecer as necessidades de conexões internas e externas para implementar mudanças necessárias para o sucesso na digitalização.
- Usar expertise em gerenciamento de mudanças e um entendimento completo da cadeia de valor digital para orientar os líderes de negócio.

Orçamento

- Realizar a gestão orçamentária.
- Realizar a modelagem financeira e gerenciamento do showback / chargeback dos custos de tecnologia.

PROPOSTA FUTURA DA ESTRUTURA ORGANIZACIONAL DA TI



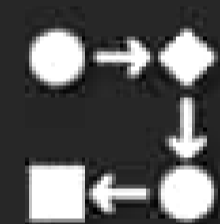
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

DIGEOP

15

Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
15	-	01	-	14	-	-	-

Responsabilidades Atuais

- Efetuar o desenvolvimento, a implantação, a documentação e a manutenção de sistemas e aplicativos geocientíficos, inclusive utilizando tecnologia de GIS (Sistemas de Informações Geográficas);
- Supervisionar e coordenar a aplicação de tratamento digital e de análise espacial de dados nas Unidades Regionais do SGB;
- Supervisionar e coordenar os trabalhos de captura e crítica de dados geocientíficos, visando o armazenamento dos dados e informações nas bases de dados institucionais do SGB;
- Modelar, implantar, manter e administrar as bases de dados geocientíficos do SGB;
- Definir e implantar procedimentos para a captura e para a alimentação das bases de dados, inclusive de dados obtidos por meio de cartografia digital;
- Desenvolver e propor metodologias e técnicas de integração e análise multitemática de dados digitais, inclusive com dados de sensores remotos, para serem adotados nas atividades do SGB;
- Estudar e propor metodologias de construção de modelos, utilizando o tratamento digital e a análise espacial de dados;
- Desenvolver metodologias de uso, conversão e utilização de dados geocientíficos provenientes das bases de dados do SGB, para aplicação em atividades da Companhia;
- Estudar e propor metodologias para a consistência e a documentação de dados e informações existentes nas bases de dados do SGB;
- Estabelecer padrões para a captura, armazenamento e intercâmbio de dados e informações geocientíficas digitais;
- Estabelecer padrões para o tratamento digital de dados e informações geocientíficas básicas, visando a sua integração e/ou a geração de produtos;
- Estudar e definir padrões de softwares para a utilização na área de geoprocessamento, inclusive de captura de dados.

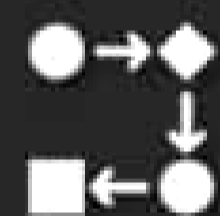
PROPOSTA FUTURA DA ESTRUTURA ORGANIZACIONAL DA TI



Estratégia



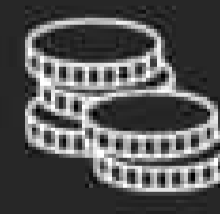
Pessoas



Processos



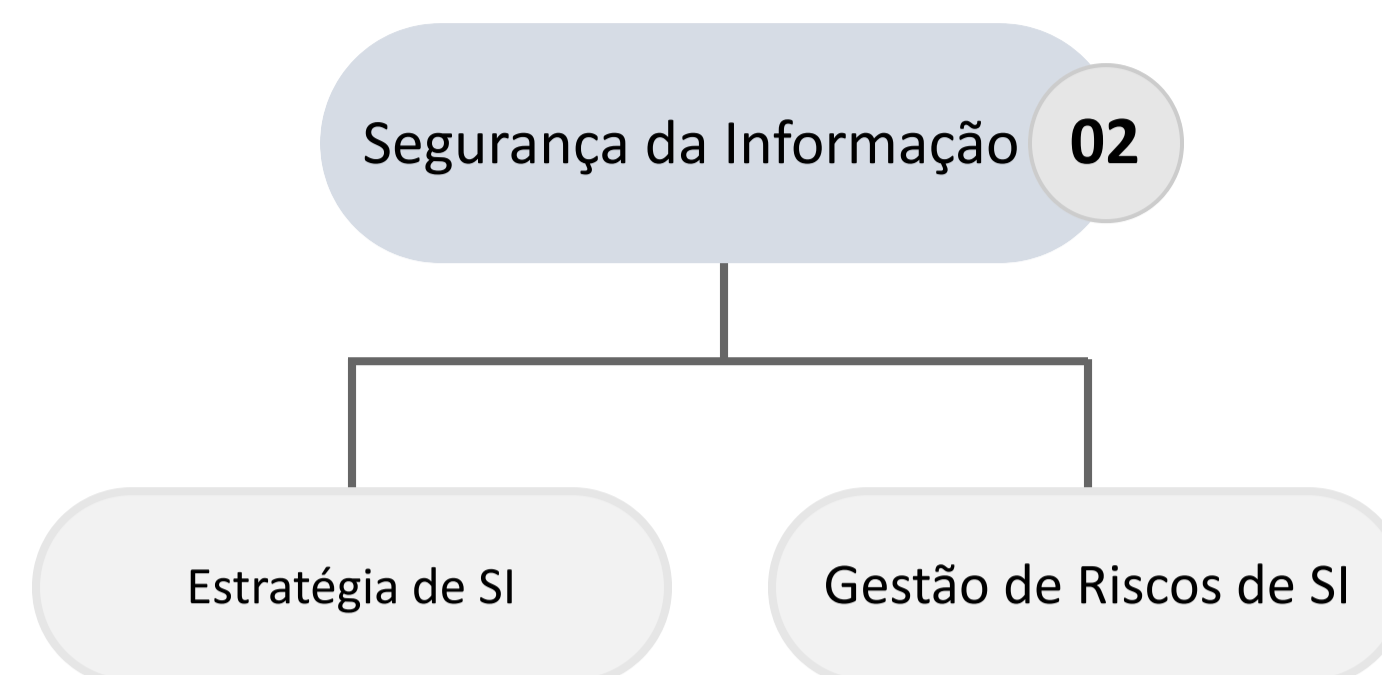
Tecnologia



Orçamento



Roadmap



Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
02	-	-	01	-	01	-	-

Responsabilidades Atuais

Atualmente a TI do SGB não possui uma área estruturada para Segurança da Informação (SI). Em sua estrutura atual, as atividades relacionadas à SI estão inseridas na área de Engenharia de Infraestrutura.

Reponsabilidades Adicionais

A Coordenação de Segurança da Informação (SI) estabelece a estratégia de SI para a organização, direciona a implementação e o monitoramento de padrões e políticas, recomenda investimentos e práticas apropriados em toda companhia e é responsável pelo gerenciamento de riscos relacionados à SI, planejamento de continuidade de negócio, gerenciamento de crises, privacidade e conformidade. Suas principais responsabilidades são:

- Definir a política de segurança e risco da empresa e supervisionar o desenvolvimento da arquitetura de tecnologia para suportar essa política.
- Alinhar as estratégias de segurança e risco da empresa com as prioridades do negócio, coordenando este assunto com as partes interessadas.
- Monitorar a conformidade com as políticas de segurança corporativa e instruir os líderes das unidades de negócio e os gerentes de serviços sobre os esforços de conformidade.
- Supervisionar o desenvolvimento de um programa de conscientização de segurança da informação com ferramentas e campanhas de comunicação personalizadas para cada unidade de negócio junto à área de Comunicação.
- Coordenar os esforços de planejamento de continuidade de negócio nas unidades de negócio.
- Identificar investimentos de risco equilibrado, entendendo o *trade-off* necessário para gerenciar diferentes níveis de tolerância ao risco e exposição ao risco em toda a organização.
- Acompanhar as ameaças / riscos, as tendências do setor e trabalhar para implementar as práticas recomendadas na organização.
- Coordenar consultas de auditoria e atividades de fornecedores externos para representar a empresa de uma perspectiva de segurança da informação, recuperação e risco de tecnologia.
- Supervisionar os relacionamentos com fornecedores relacionados à segurança, a seleção de produtos e a negociação de contratos de alto nível para fornecer serviços e recursos para a proteção dos ativos da organização.
- Gerenciar parceiros de segurança da informação para prestação de serviços que objetivam a operação da proteção dos ativos da organização dentro do apetite de risco alinhado com o negócio, preferencialmente em modelo *as a service*.
- Realizar a gestão de acesso e identidades em sistemas e plataformas de tecnologia.
- Co-gerenciar a gestão de privacidade e proteção de dados junto com as áreas de negócio e a área de conformidade.
- Realizar o monitoramento e gerenciamento de vulnerabilidades tecnológicas.
- Gerenciar o SOC as service.

PROPOSTA FUTURA DA ESTRUTURA ORGANIZACIONAL DA TI



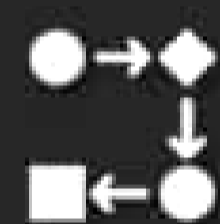
Painel



Estratégia



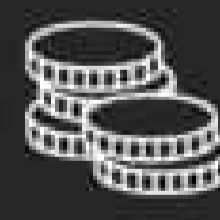
Pessoas



Processos



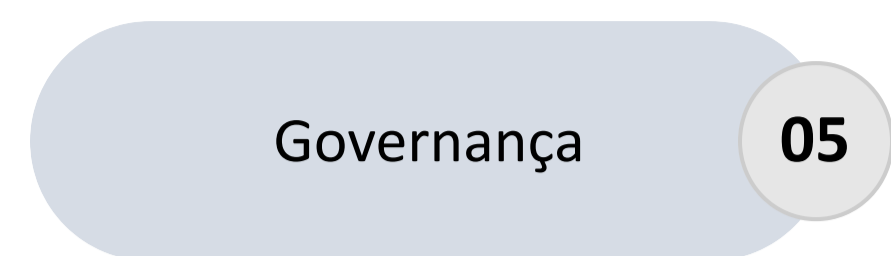
Tecnologia



Orçamento



Roadmap



Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
05	-	-	01	-	04	-	-

Responsabilidades Atuais

Atualmente a TI do SGB não possui uma área estruturada para Governança.

Responsabilidades Adicionais

A Coordenação de Governança de TI é responsável pela definição, monitoramento e controle de indicadores, processos e metodologias que apoiam o funcionamento da TI de acordo com as melhores práticas de mercado e alinhada as expectativas estratégicas de negócio. Com a finalidade de suprir as demandas de projetos e relacionamento com o negócio, a coordenação de Governança de TI também tem responsabilidade para gerenciamento e coordenação serviços, gerenciar projetos em toda TI, interagindo com a liderança para criar uma estratégia que se alinhe aos objetivos e prioridades de negócio. Também é responsável pelo desenvolvimento de uma metodologia de projeto robusta e flexível para uso em toda TI. Suas principais responsabilidades são:

- Analisar o negócio e o ambiente de TI atuais para detectar deficiências críticas e recomendar soluções para melhoria.
- Liderar e facilitar a criação de princípios de governança para orientar a tomada de decisão.
- Assegurar a estrutura de governança ideal e que as atividades de conformidade estejam associadas às práticas de tecnologia.
- Realizar a gestão contratual dos fornecedores.
- Documentar e manter políticas e normas de TI atualizadas e em linguagem de fácil compreensão.
- Monitorar fornecedores e serviços e aplicar cláusulas contratuais vigentes relacionadas a não conformidade na prestação de serviços.
- Realizar gestão dos pontos de controles internos e auditoria interna, bem como os riscos de TI.
- Acompanhar a gestão de requisitos de continuidade de negócio e suas implementações nos serviços de tecnologia.
- Estabelecer normas e padrões para utilização de soluções via democratização (Low/No code) que consiste no desenvolvimento de soluções pelo próprio time de negócio e não são suportados e/ou sustentados pela TI.
- Gerenciar um portfólio de projetos na TI.
- Facilitar mudanças no modelo operacional de TI para suportar a transformação digital.
- Apoiar a estratégia digital da empresa e da TI, liderando projetos digitais;
- Assegurar que investimentos e iniciativas em serviços de gerenciamento de projetos se alinhem com a estratégia e prioridades organizacionais.
- Desenvolver e gerenciar orçamento e custo de projetos, alocação de recursos e realocações.
- Priorizar o portfólio de projetos com base em critérios definidos pelo SGB.
- Monitorar as métricas de valor de projetos para tomar decisões informadas que maximizam o retorno nos projetos da empresa.
- Monitorar a entrega do objetivo de negócio do projeto e a experiência de serviço da área.
- Gerenciar e desenvolver habilidades e recursos da equipe de gerenciamento de projetos na TI.
- Realizar e supervisionar o coaching das metodologias de gerenciamento de projetos.
- Promover adoção de novas práticas de entrega, como Agile e DevOps.
- Comunicar o status do projeto para as partes interessadas relevantes.
- Definir princípios e padrões para harmonizar as metodologias de gerenciamento de projetos de terceiros ou provedores de serviços externos.
- Os analistas de negócio trabalham com o time de projetos de TI e clientes de negócio para coletar, esclarecer e traduzir os requisitos de negócio em documentação e projeto conceitual a partir dos quais os produtos e as soluções são desenvolvidas.
- Trabalhar com parceiros de negócio para extrair, analisar e documentar requisitos de negócio.
- Estabelecer ligação com as equipes de projetos de TI para comunicar as prioridades de negócio, converter requisitos de negócio em requisitos técnicos e identificar soluções apropriadas.
- Facilitar a coleta regular de requisitos, projetar sessões com a comunidade de usuários e comunicar as expectativas para a equipe de desenvolvimento.
- Negociar soluções de negócio inovadoras que satisfaçam as necessidades do cliente e que estejam em conformidade com os padrões de tecnologia.
- Trabalhar com vários stakeholders para avaliar o impacto das soluções propostas, facilitar implantações e minimizar a interrupção dos serviços.
- Influenciar os clientes internos a entenderem sobre suas prioridades e modos de resolver seus problemas.
- Validar que os produtos desenvolvidos estão de acordo com os requisitos de negócio.

PROPOSTA FUTURA DA ESTRUTURA ORGANIZACIONAL DA TI



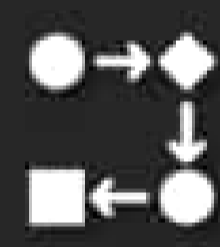
Painel



Estratégia



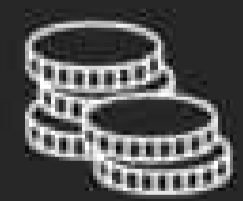
Pessoas



Processos



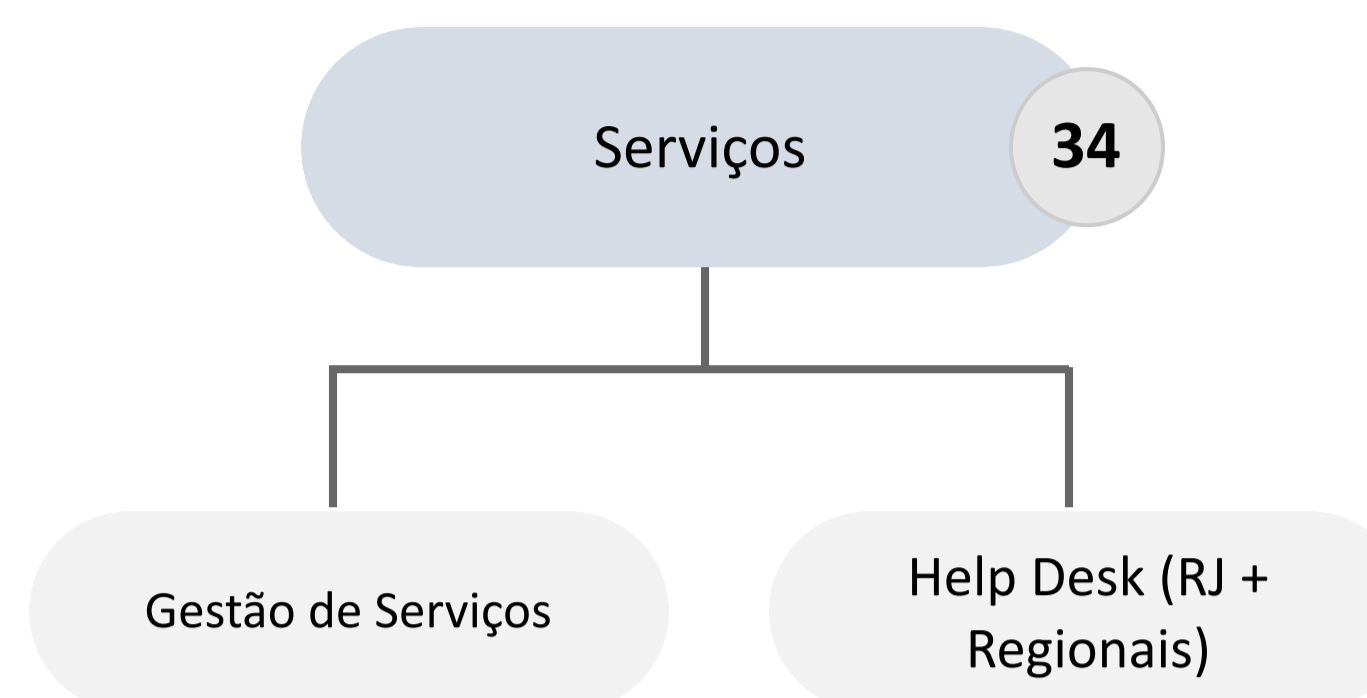
Tecnologia



Orçamento



Roadmap



Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
34	-	-	01	01	10	02	20

Detalhamento FTEs

O detalhamento do quantitativo de FTEs do Help Desk permanece com a mesma estrutura.

Responsabilidades Atuais

O Help Desk possui infraestrutura operacional instalada em 13 unidades espalhadas pelo Brasil, tendo sua sede no Escritório Central da administração localizado no Rio de Janeiro. O quantitativo operacional de cada unidade é definido com base no volume de demandas por unidade. O Help Desk é uma das áreas da DIINFO, em que são atribuídas as seguintes responsabilidades:

- Suportes N1 e N2 ao usuário final;
- Gestão de incidentes e requisições;
- *Facilities* de TI nas localidades;
- Manutenção do parque tecnológico.

Responsabilidades Adicionais

A Coordenação de Serviços é responsável pelo gerenciamento dos processos e ferramenta de ITSM (*Information Technology Service Management*), pela abordagem de TI como uma área prestadoras de serviços. Estabelece e aprimora os processos, técnicas e métodos usados pelos times técnicos, entregando orientação técnica e suporte às atividades diárias da equipe. Suas principais responsabilidades são:

- Avaliar e aprovar solicitação de mudanças para produção.
- Gerenciar configuração e ativos de TI.
- Negociar e acompanhar SLA's com as áreas de negócio.
- Elaborar e acompanhar indicadores de desempenho que sustentam os SLA's estabelecidos.
- Gerenciar fornecedores que suportam as aplicações e interface com os fabricantes dos produtos.
- Gerenciar contratos de microinformática e seus serviços relacionados.
- Gerenciar fornecedor e serviços da central de serviços e *field services*.
- Identificar e gerenciar a implementação de autosserviço para os usuários do SGB.
- Comunicar melhorias na prestação de serviços de TI e sobre paradas programadas.
- Definir padrões de atendimento para entrega de serviços aos usuários.
- Contribuir para melhoria do suporte ao cliente, aprimorando o tempo de resposta a consultas e reclamações.
- Fornecer orientação, apoio e treinamento para supervisores e equipe.
- Motivar a equipe a atender aos níveis de serviço e metas estabelecidas pelo departamento.
- Estabelecer e manter sólidas relações de trabalho com departamentos e fornecedores para viabilizar que a central de serviços atenda aos SLA's.
- Desenvolver e implementar metas anuais para atender às necessidades da TI.
- Comunicar interrupções de serviços para clientes e usuários.
- Reportar procedimentos de atendimento desatualizados.
- Realizar atendimentos de campo nas localidades onde houver usuários de TI do SGB.

PROPOSTA FUTURA DA ESTRUTURA ORGANIZACIONAL DA TI



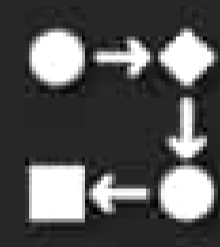
Painel



Estratégia



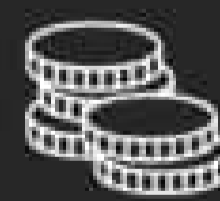
Pessoas



Processos



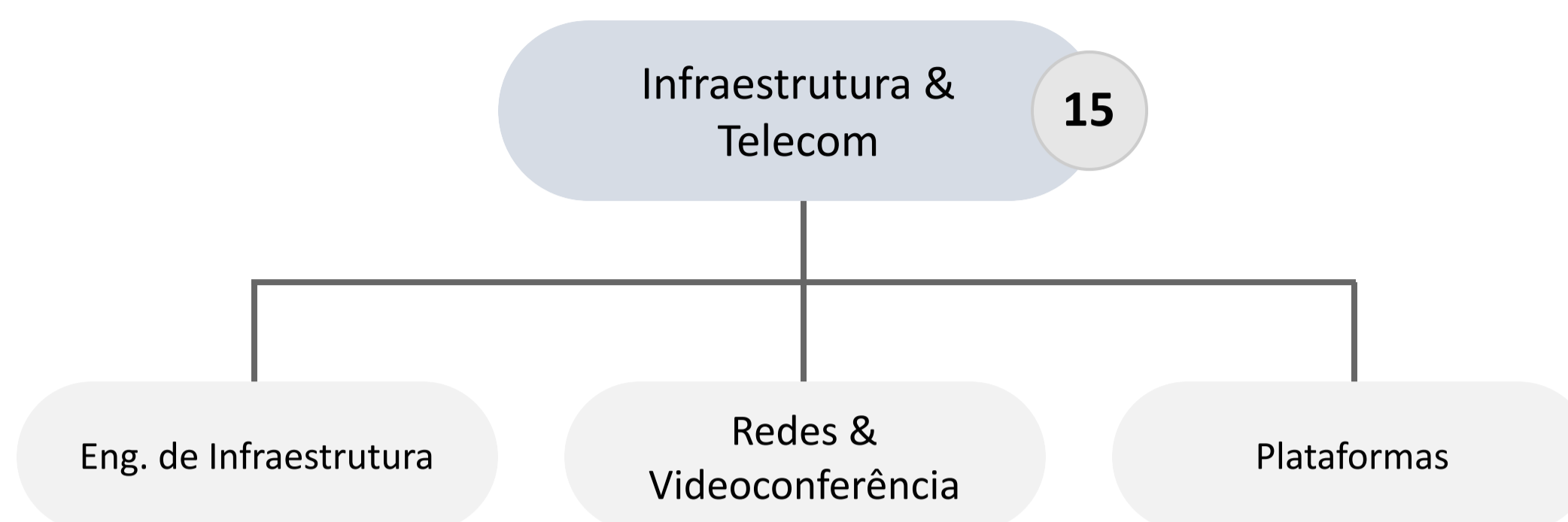
Tecnologia



Orçamento



Roadmap



Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
15	-	-	01	07	-	-	07

Responsabilidades Atuais

Banco de Dados:

- Gerenciar o Banco de Dados da empresa (SQLServer, PostgreSQL e Oracle);
- Realizar alterações e customizações no Banco de Dados.

Redes & Videoconferência:

- Gerenciamento da rede cabeada, distribuição geral de rede, conectorização, organização de racks;
- Configurações de switch e roteadores;
- Transmissão de videoconferência e operação dos equipamentos de vídeo;
- Apoio em eventos que necessitam de transmissão de vídeo.

Engenharia de Infraestrutura:

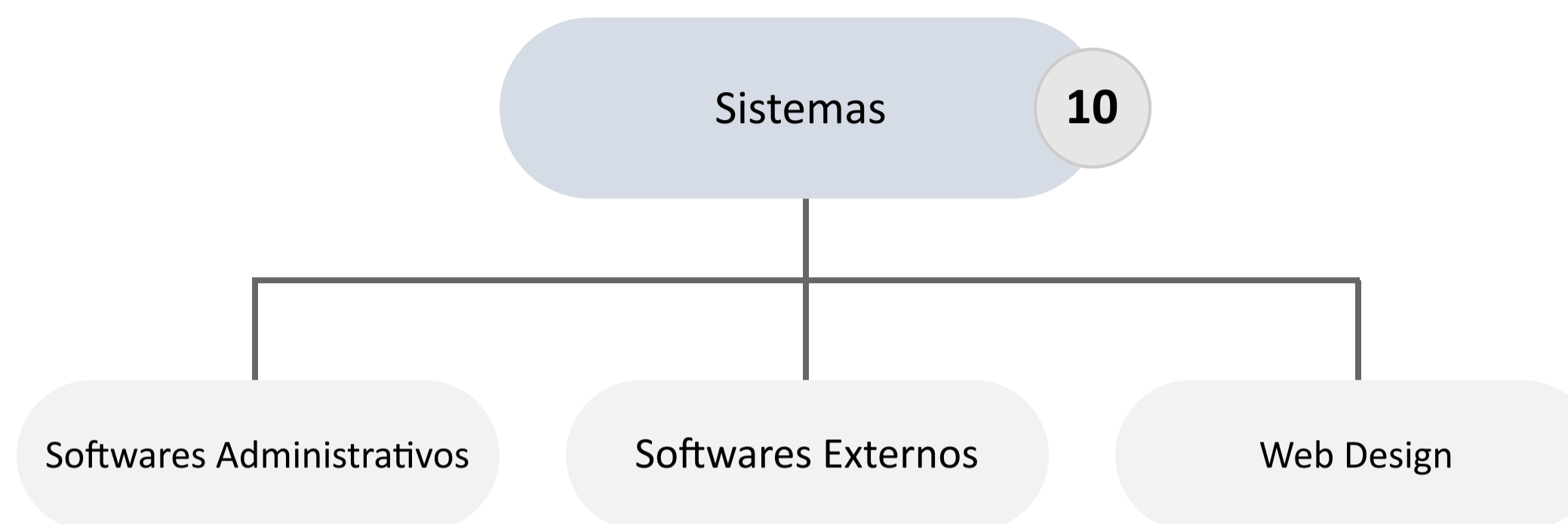
- Gestão da infraestrutura de TI;
- Gestão do Datacenter;
- Gestão de acesso;
- Gestão da Segurança da Informação;
- Atendimento de chamados N3;
- Definição de políticas e padrões.

Responsabilidades Adicionais

A coordenação de infraestrutura & Telecom oferece suporte aos negócios da empresa, provendo confiabilidade nos componentes de Infraestrutura e Conectividade para viabilizar sustentabilidade e eficiência aos recursos de TI. Suas principais responsabilidades são:

- Gerenciar a disponibilidade e capacidade de recursos para oferecer suporte contínuo e desempenho ideal aos negócios.
- Recomendar soluções de infraestrutura de tecnologia adequadas e atualizações para equipes de TI, a fim de desenvolver planejamento de longo e curto prazo.
- Recomendar alternativas para a arquitetura de infraestrutura de TI, a fim de garantir a sustentabilidade dos negócios.
- Gerenciar os fornecedores de infraestrutura física (data centers, redes, storages, telecomunicações) e lógica (middlewares, banco de dados, sistemas operacionais etc).
- Gerenciar níveis de serviços dos fornecedores relacionados à infraestrutura e telecomunicações.
- Suportar a criação e gestão de rotinas de operações.
- Gerenciar a liberação de pacotes em produção junto aos fornecedores.
- Responder pela manutenção da infraestrutura de redes e servidores.
- Atender a chamados no seu escopo de atuação ou encaminhá-los ao fornecedor correto.
- Identificar rotinas que possam ser atendidas pelo primeiro nível de atendimento, designando que as documentem em procedimentos.
- Elaborar estratégias e procedimentos de contingências em alinhamento com os requisitos definidos pela Segurança da Informação.
- Criar e manter procedimentos para a Central de Serviços lidar com chamados mais simples que são repassados aos especialistas.
- Liderar todos os aspectos da equipe de rede de dados, incluindo design, engenharia, segurança, implementação e operações para a rede da empresa.
- Trabalhar com a Coordenação de Governança e de Segurança da Informação para o alinhamento de regras e padrões a seguir.
- Garantir o monitoramento de serviços em todas as plataformas para viabilizar alta disponibilidade e capacidade de recuperação de desastres de sistemas críticos.
- Monitorar e analisar a rede para recomendar atualizações e alterações, conforme necessário.
- Direcionar iniciativas complexas de redes de TI.
- Direcionar equipes para gerenciamento de fornecedores e suporte à resolução de problemas.

PROPOSTA FUTURA DA ESTRUTURA ORGANIZACIONAL DA TI



Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
10	-	-	01	04	-	-	05

Responsabilidades Atuais

Desenvolvimento:

- Desenvolvimento de aplicações administrativos;
- Manutenção de sistemas administrativos;
- Apoio a DIGEOP na fábrica de softwares para aplicações de negócio.

Softwares Externos:

- Customização de softwares externos governamentais de uso obrigatório;
- Manutenção de softwares externos governamentais de uso obrigatório;
- Suporte aos usuários de softwares externos governamentais de uso obrigatório.

Web Design:

- Modificação e customização dos sites, portais e intranet do SGB, conforme a demanda das áreas de negócio e administrativa.

Responsabilidades Adicionais

A coordenação de Sistemas é responsável pelos sistemas administrativos, sistemas externos e Web Design de sites, portais e intranet. Seu time de especialistas atua com foco na evolução contínua dos sistemas, atendimento a demandas do negócio e suporte especializado em conjunto com a Central de Serviços. Suas principais responsabilidades são:

- Colaborar com analistas de negócios e proprietários de produtos para garantir a compreensão das prioridades de negócios.
- Auxiliar no suporte de aplicações existentes.
- Criar e executar os cenários/planos de teste necessários para garantir testes completos nos componentes novos e alterados.
- Realizar a transferência de conhecimento para outras equipes de TI e de negócios;
- Gerenciar a disponibilidade e capacidade de recursos para oferecer suporte contínuo e desempenho ideal aos negócios.
- Recomendar alternativas para a arquitetura de sistemas, a fim de garantir a sustentabilidade dos negócios.
- Gerenciar os fornecedores de aplicações e componentes.
- Gerenciar níveis de serviços dos fornecedores relacionados as aplicações.
- Suportar a criação e gestão de rotinas de operações.
- Atender a chamados no seu escopo de atuação ou encaminhá-los ao fornecedor correto.
- Identificar rotinas que possam ser atendidas pelo primeiro nível de atendimento, designando que as documentem em procedimentos.
- Elaborar estratégias e procedimentos de contingências em alinhamento com os requisitos definidos pela Segurança da Informação.
- Criar e manter procedimentos para a Central de Serviços lidar com chamados mais simples que são repassados aos especialistas.
- Trabalhar com a Coordenação de Governança e Segurança da Informação para o alinhamento de regras e padrões a seguir.
- Monitorar e analisar as aplicações para recomendar atualizações e alterações, conforme necessário.
- Direcionar equipes para gerenciamento de fornecedores e suporte a resolução de problemas.



Painel



Estratégia



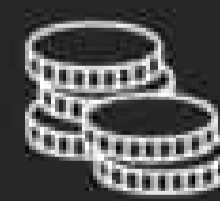
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

PROPOSTA FUTURA DA ESTRUTURA ORGANIZACIONAL DA TI

Data Science

05

Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
05	-	-	-	05	-	-	-

Responsabilidades Atuais

Data Science é uma das áreas da DIGEOP, em que são atribuídas as seguintes responsabilidades:

- Estudar e definir padrões de softwares para a utilização na área de geoprocessamento, inclusive de captura de dados;
- Efetuar o desenvolvimento, a implantação, a documentação e a manutenção de sistemas e aplicativos geocientíficos, inclusive utilizando tecnologia de GIS (Sistemas de Informações Geográficas);
- Relacionamento com as áreas de negócio.

Reponsabilidades Adicionais

A coordenação de Data Science é responsável pela evolução dos Sistemas Geocientíficos e aplicações que sejam colaborativas com Fábrica de Software. Seu time de especialistas atua com foco na evolução contínua dos sistemas, atendimento a demandas do negócio e suporte especializado em conjunto com a Central de Serviços. Suas principais responsabilidades são:

- Colaborar com analistas de negócios e proprietários de produtos para garantir a compreensão das prioridades de negócios.
- Auxiliar no suporte de aplicações existentes.
- Criar e executar os cenários/planos de teste necessários para garantir testes completos nos componentes novos e alterados.
- Realizar a transferência de conhecimento para outras equipes de TI e de negócios;
- Gerenciar a disponibilidade e capacidade de recursos para oferecer suporte contínuo e desempenho ideal aos negócios.
- Recomendar alternativas para a arquitetura de sistemas, a fim de garantir a sustentabilidade dos negócios.
- Gerenciar os fornecedores de aplicações e componentes.
- Gerenciar níveis de serviços dos fornecedores relacionados as aplicações.
- Suportar a criação e gestão de rotinas de operações.
- Atender a chamados no seu escopo de atuação ou encaminhá-los ao fornecedor correto.
- Identificar rotinas que possam ser atendidas pelo primeiro nível de atendimento, designando que as documentem em procedimentos.
- Elaborar estratégias e procedimentos de contingências em alinhamento com os requisitos definidos pela Segurança da Informação.
- Criar e manter procedimentos para a Central de Serviços lidar com chamados mais simples que são repassados aos especialistas.
- Trabalhar com a Coordenação de Governança e Segurança da Informação para o alinhamento de regras e padrões a seguir.
- Monitorar e analisar as aplicações para recomendar atualizações e alterações, conforme necessário.
- Direcionar equipes para gerenciamento de fornecedores e suporte a resolução de problemas.



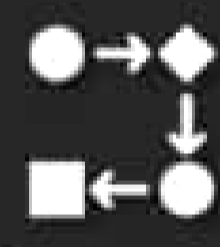
Painel



Estratégia



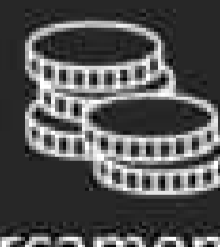
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

PROPOSTA FUTURA DA ESTRUTURA ORGANIZACIONAL DA TI

Geoprocessamento **05**

Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
05	-	-	-	05	-	-	-

Responsabilidades Atuais

- Coordenar e supervisionar a aplicação de tratamento digital e de análise espacial de dados nas Unidades Regionais do SGB;
- Coordenar e supervisionar os trabalhos de captura e crítica de dados geocientíficos, visando o armazenamento dos dados e informações nas bases de dados institucionais do SGB;
- Apoio a área de negócio na transformação de dados (geoprocessamento) ou na utilização de softwares específicos (QGIS, ArcGIS Pro ou ArcMap);
- Responsável por treinamentos de geoprocessamento.

Reponsabilidades Adicionais

- Desenvolver e aderir aos padrões e melhores práticas de modelagem de dados.
- Identificar oportunidades de alinhamento, normalização e reutilização de dados.
- Implementar princípios, políticas, padrões e diretrizes para gerenciamento de dados em parceria com a Coordenação de Governança.



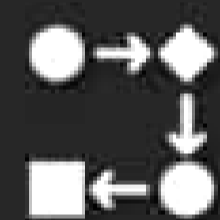
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

PROPOSTA FUTURA DA ESTRUTURA ORGANIZACIONAL DA TI

Apoio a Base de Dados **04**



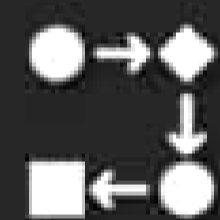
Painel



Estratégia



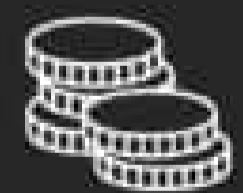
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Total de FTEs	Chefe de Depto.	Chefe de Divisão	Coordenador	Analista Sr	Analista Pl	Analista Jr	Terceiros
04	-	-	-	04	-	-	-

Responsabilidades Atuais

- Manutenção dos Bancos de Dados Geocientíficos;
- Gestão da fábrica de softwares externa;
- Estruturação de novas bases de dados, modelagem (modelo lógico e físico);
- Desenvolver metodologias de uso, conversão e utilização de dados geocientíficos provenientes das bases de dados, para aplicação em atividades;
- Estudar e propor metodologias para a consistência, documentação dos dados e informações existentes nas bases de dados;
- Estabelecer padrões para a captura, armazenamento e intercâmbio de dados e informações geocientíficas digitais;
- Estabelecer padrões para o tratamento digital de dados e informações geocientíficas básicas, visando a sua integração e/ou a geração de produtos.

Reponsabilidades Adicionais

- Viabilizar que os dados corporativos sejam estruturados para facilidade de uso.
- Manter a arquitetura de repositórios estruturados para armazenamento assertivo dos dados dos sistemas do SGB.
- Desenvolver e aderir aos padrões e melhores práticas de modelagem de dados.
- Identificar oportunidades de alinhamento, normalização e reutilização de dados.
- Implementar princípios, políticas, padrões e diretrizes para gerenciamento de dados em parceria com a Coordenação de Governança.

- Painel 
- Estratégia 
- Pessoas 
- Processos** 
- Tecnologia 
- Orçamento 
- Roadmap 
- Anexos 

APO06

APO09

APO12

BAI06

BAI09

BAI10

BAI11

DSS01

DSS02

DSS05

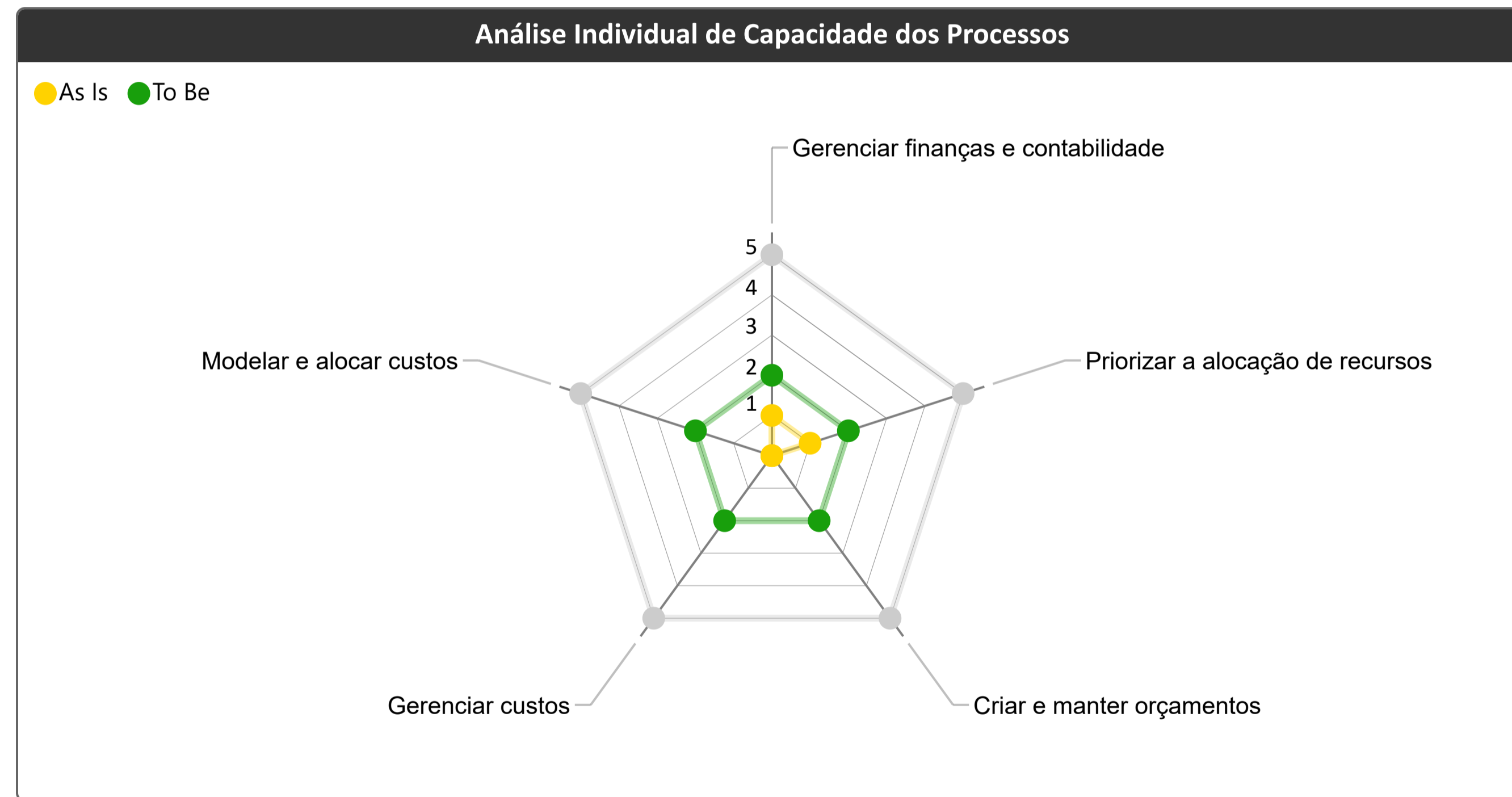
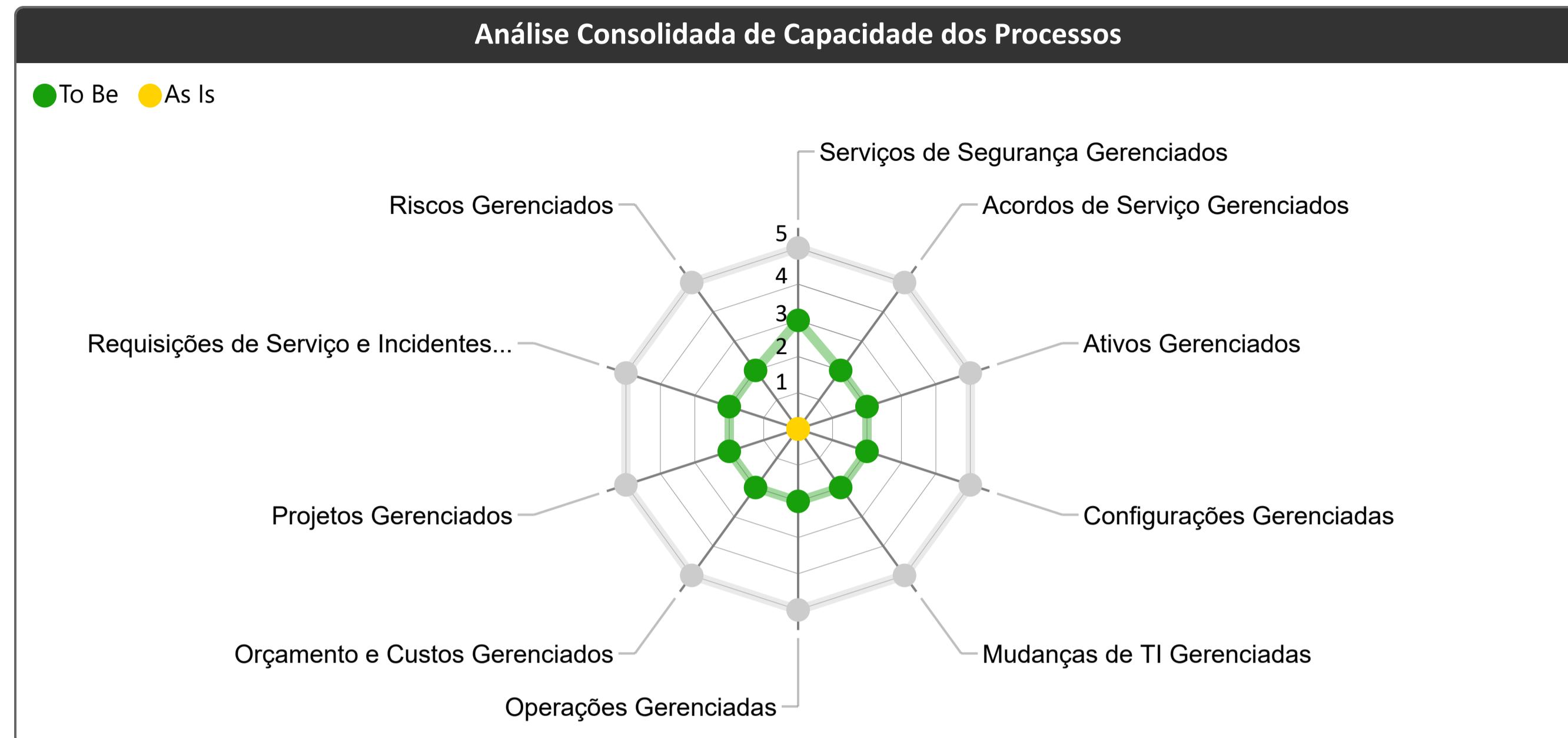


Nível	Processo	Descrição
0	Processo Incompleto	Processo não implementado ou não cumpre seu propósito.
1	Processo Executado	O processo implementado atinge o objetivo proposto.
2	Processo Gerenciado	O desempenho do processo agora é implementado de forma gerenciada e seus produtos de trabalho são apropriadamente estabelecidos, controlados e mantidos.
3	Processo Estabelecido	O processo gerenciado é agora implementado usando um processo definido que é capaz de alcançar seus resultados de processo
4	Processo Previsível	O processo estabelecido é agora operado dentro de limites definidos, apresentando atributos como a gestão e o controle do processo.
5	Processo Otimizado	O processo previsível do nível 4 é continuamente aprimorado para atingir as metas atuais e futuras de negócio.

Processo Orçamento e Custos Gerenciados

Descrição do Processo
Gerenciar as atividades financeiras relacionadas a TI nas funções de negócios e TI, abrangendo orçamento, gestão de custos e benefícios e priorização de gastos por meio do uso de práticas orçamentárias formais e um sistema justo e equitativo de alocação de custos para a empresa. Consultar as partes interessadas para identificar e controlar os custos e benefícios totais no contexto dos planos estratégicos e táticos de TI. Iniciar ação corretiva quando necessário.

Propósito
Promover uma parceria entre as partes interessadas de TI e da empresa para permitir o uso eficaz e eficiente dos recursos relacionados a TI e fornecer transparência e responsabilidade do custo e valor comercial de soluções e serviços. Permite que a empresa tome decisões municiada de informações sobre o uso de soluções e serviços de TI.



Pilar	Oportunidade	Recomendação To Be	Recomendação	Artefato
APO06.01 Gerenciar finanças e contabilidade	As classificações orçamentárias são realizadas de forma empírica, sem um processo documentado.	Recomendações To Be	Criar e documentar um esquema de classificação orçamentária.	Esquema de Classificação de Custos de TI.
APO06.01 Gerenciar finanças e contabilidade	Ausência de um processo definido e documentado para controle de entrada, saída e controle orçamentário. Não há uma definição clara sobre os papéis e responsabilidades acerca da análise e reporte da gestão financeira.	Recomendações To Be	Mapear e documentar o processo de controle orçamentário, incluindo periodicidade de reportes (incluindo, se possível, uma matriz RACI).	Documento do Processo de Controle Orçamentário.
APO06.02 Priorizar a alocação de recursos	Falta de um procedimento documentado para verificação de opções entre comprar ativos/serviços ou contratação de uso de ativos/serviços.	Recomendações To Be	Elaborar um processo para que se verifique entre a opção de compra ou locação do ativo, assim como desenvolver internamente um serviço ou contratá-lo externamente, a cada solicitação de compra de ativo ou serviço.	Documentação do Processo de Requisição de Compra/Serviço.
APO06.02 Priorizar a alocação de recursos	Inexistência de um processo documentado para priorização orçamentária.	Recomendações To Be	Estabelecer um processo para priorização orçamentária, assim como para estabelecer comunicações de decisões orçamentárias.	Priorização de Iniciativas Orçamentárias
APO06.03 Criar e manter orçamentos	Na criação do orçamento, não há uma documentação de quais componentes considerar. Estes são elencados de forma empírica.	Recomendações To Be	Criar uma documentação contendo os componentes a considerar na elaboração do orçamento.	Documentação do Processo de Criação de Orçamento
APO06.03 Criar e manter orçamentos	Não é elaborada uma documentação acerca da lógica considerada para criação do orçamento, o que dificulta a justificativa de continuação	Recomendações To Be	Criar um procedimento para elaborar um documento que registre a lógica realizada para criação do orçamento.	Documentação do Processo de Criação de Orçamento

APO06

APO09

APO12

BAI06

BAI09

BAI10

BAI11

DSS01

DSS02

DSS05

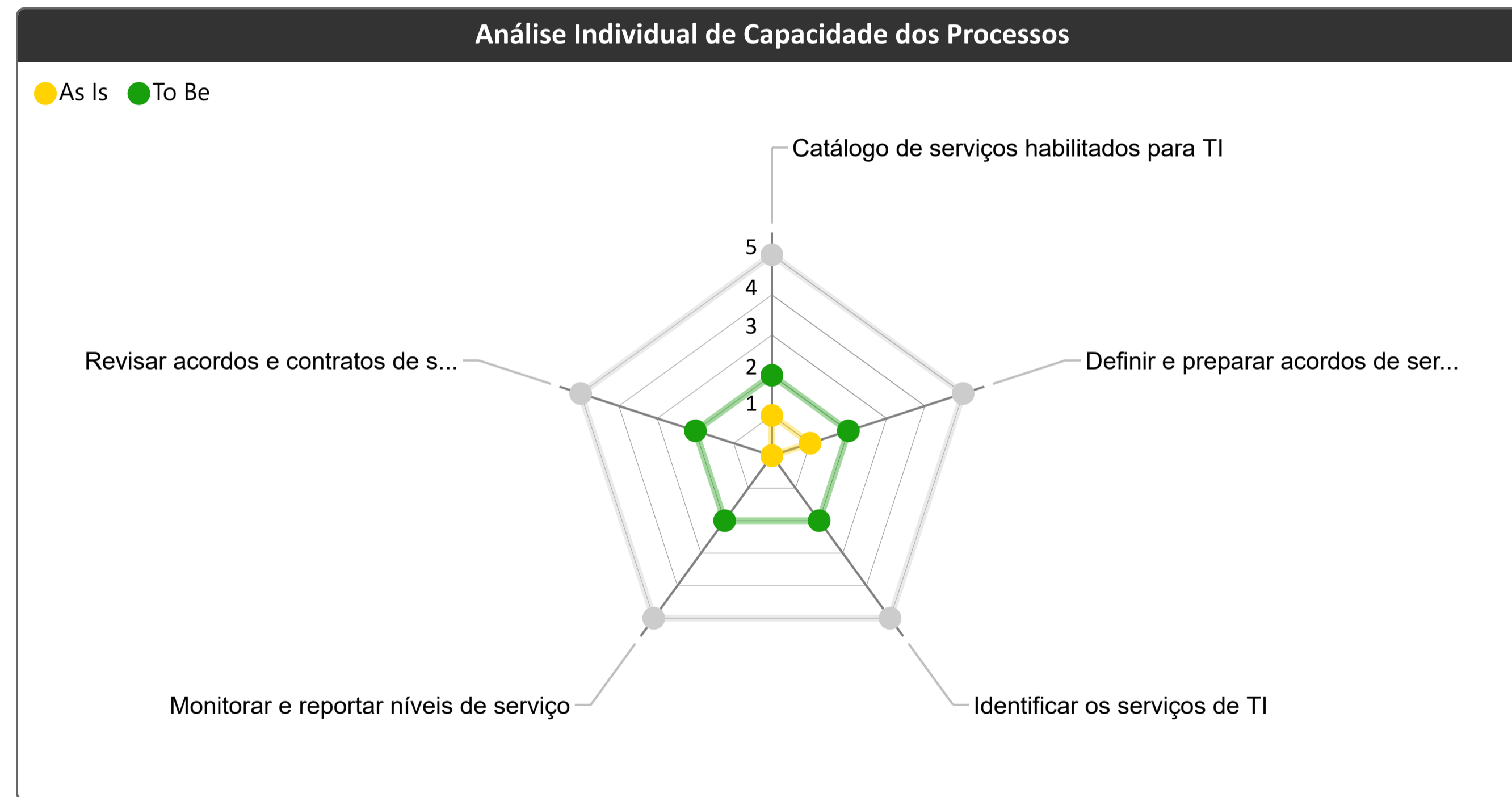
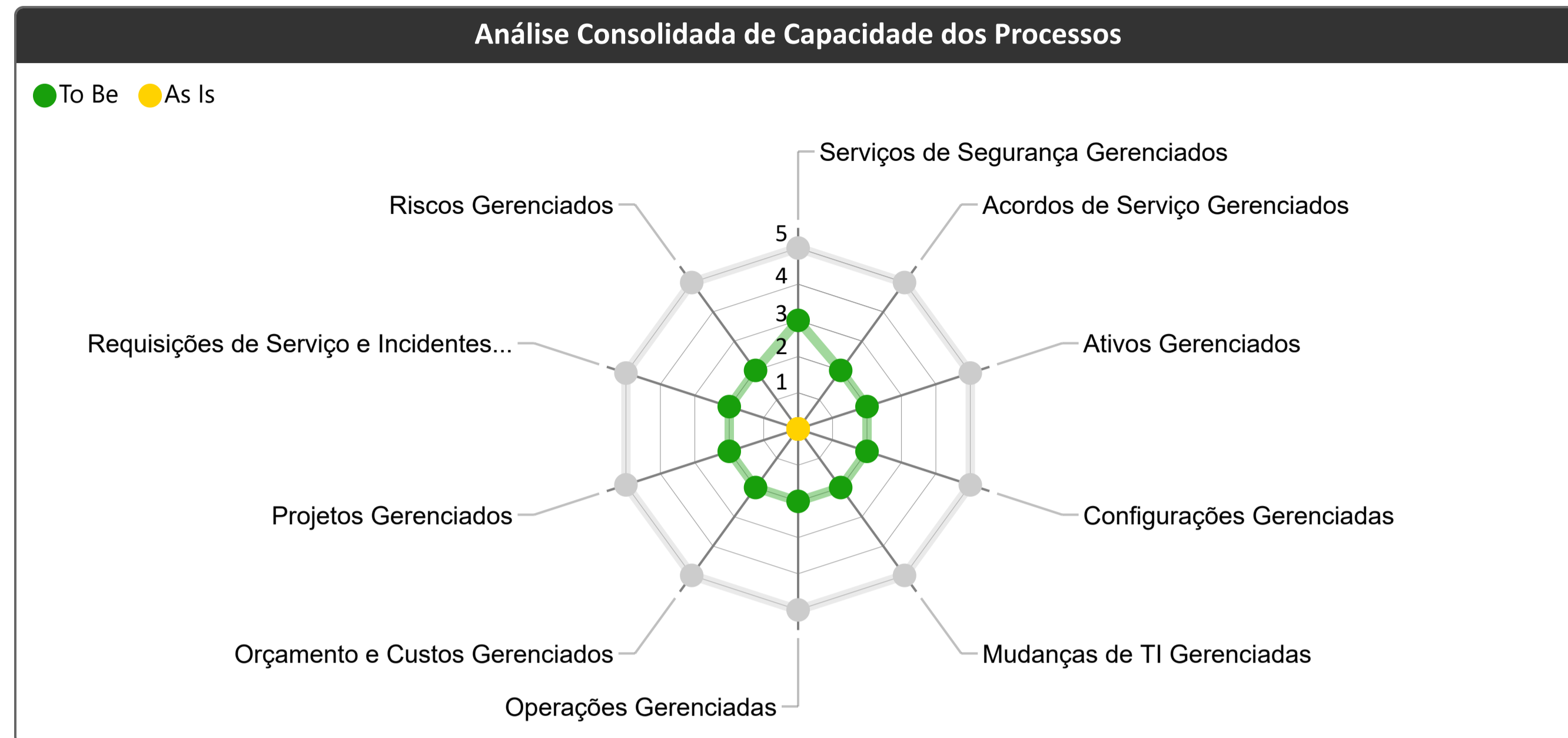


Nível	Processo	Descrição
0	Processo Incompleto	Processo não implementado ou não cumpre seu propósito.
1	Processo Executado	O processo implementado atinge o objetivo proposto.
2	Processo Gerenciado	O desempenho do processo agora é implementado de forma gerenciada e seus produtos de trabalho são apropriadamente estabelecidos, controlados e mantidos.
3	Processo Estabelecido	O processo gerenciado é agora implementado usando um processo definido que é capaz de alcançar seus resultados de processo
4	Processo Previsível	O processo estabelecido é agora operado dentro de limites definidos, apresentando atributos como a gestão e o controle do processo.
5	Processo Otimizado	O processo previsível do nível 4 é continuamente aprimorado para atingir as metas atuais e futuras de negócio.

Processo Acordos de Serviço Gerenciados

Descrição do Processo
Alinhar produtos e serviços habilitados para TI e níveis de serviço com as necessidades e expectativas da empresa, incluindo identificação, especificação, design, publicação, contratação e monitoramento de produtos e serviços de TI, níveis de serviço e indicadores de desempenho.

Propósito
Garantir que os produtos, serviços e níveis de serviço de TI atendam às necessidades atuais e futuras da empresa.



Recomendações To Be				
Pilar	Oportunidade	Recomendação	Artefato	
APO09.01 Identificar os serviços de TI	Não é realizado um estudo para estimar a demanda futura e tendência para confirmar a capacidade dos serviços.	Mapear, documentar e implementar um processo para realização de um estudo que possibilite estimar a demanda futura de serviços de TI para poder confirmar a capacidade dos serviços oferecidos.	Análise de Tendência da demanda de serviços de TI.	
APO09.01 Identificar os serviços de TI	Não há um processo definido para análise, em uma linha de tempo, dos serviços atuais de TI e seus SLAs, para identificar lacunas entre o esperado pelo negócio e o realizado.	Mapear e documentar um processo para análise dos serviços atuais de TI e seus SLAs, verificando se está alinhado com a necessidade do negócio. Este processo deverá ser realizado em uma rotina definida.	Documentação do Processo de Análise dos Serviços e SLA. Lacunas identificadas entre a necessidade do negócio e os serviços de TI e SLAs ofertados.	
APO09.02 Catálogo de serviços habilitados para TI	A publicação dos serviços e seus SLAs no catálogo de serviços é realizado esporadicamente, de forma empírica.	Criar uma recorrência para atualização do catálogo de serviços e SLAs, documentada em forma de processo.	Documentação do Processo de Atualização do Catálogo de Serviços	
APO09.03 Definir e preparar acordos de serviço	A definição do SLA necessário para o serviço realizado e/ou contratado é realizada de forma empírica, sem um processo definido e documentado.	Mapear e documentar um processo para definição dos SLAs necessários para os serviços a serem realizados e/ou contratados.	Documentação do Processo de definição do Nível de Acordo de Serviço.	

APO06

APO09

APO12

BAI06

BAI09

BAI10

BAI11

DSS01

DSS02

DSS05

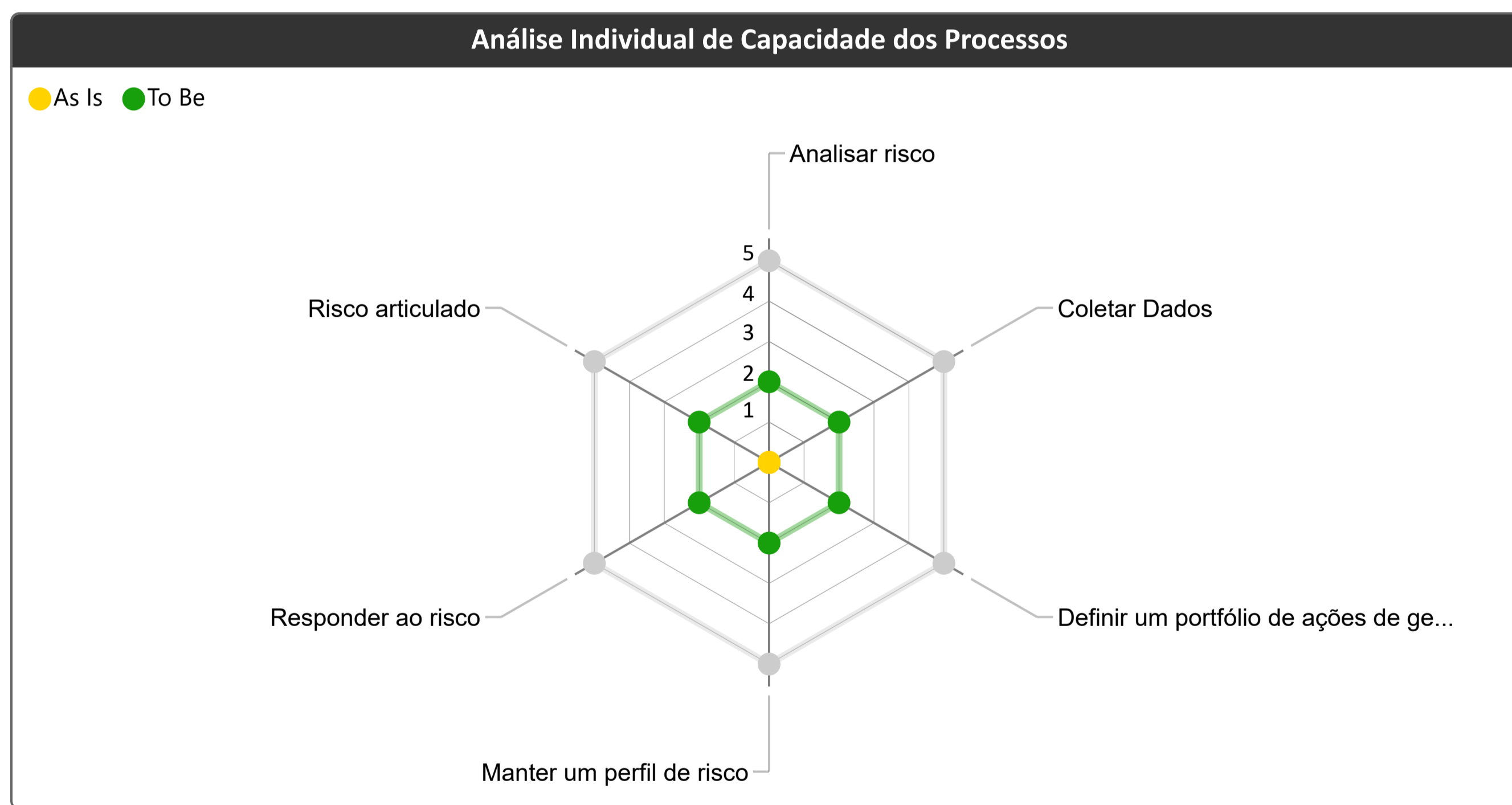
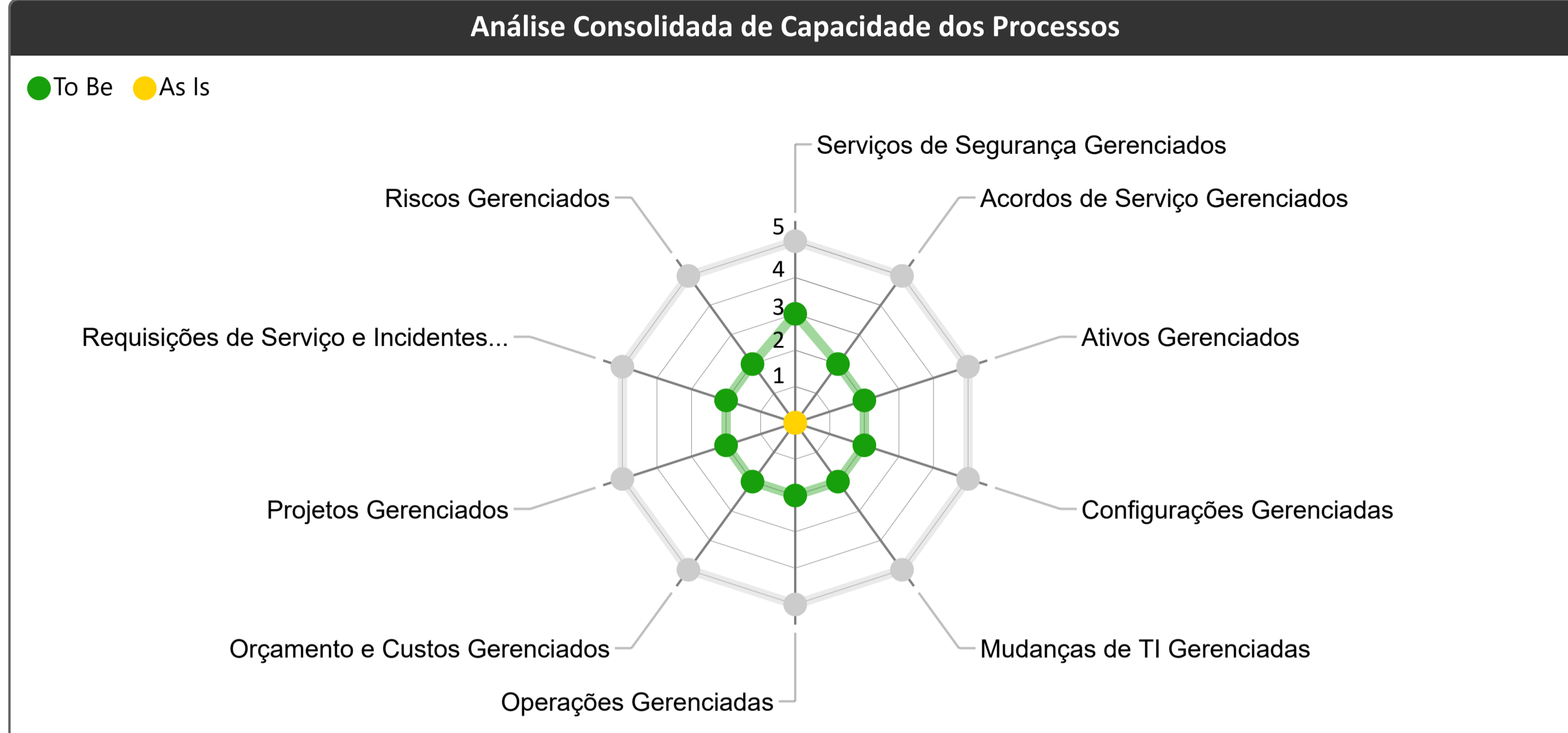


Nível	Processo	Descrição
0	Processo Incompleto	Processo não implementado ou não cumpre seu propósito.
1	Processo Executado	O processo implementado atinge o objetivo proposto.
2	Processo Gerenciado	O desempenho do processo agora é implementado de forma gerenciada e seus produtos de trabalho são apropriadamente estabelecidos, controlados e mantidos.
3	Processo Estabelecido	O processo gerenciado é agora implementado usando um processo definido que é capaz de alcançar seus resultados de processo
4	Processo Previsível	O processo estabelecido é agora operado dentro de limites definidos, apresentando atributos como a gestão e o controle do processo.
5	Processo Otimizado	O processo previsível do nível 4 é continuamente aprimorado para atingir as metas atuais e futuras de negócio.

Processo **Riscos Gerenciados**

Descrição do Processo
 Identificar, avaliar e reduzir continuamente os riscos relacionados a TI dentro dos níveis de tolerância definidos pela gerência executiva da empresa.

Propósito
 Integrar o gerenciamento de riscos corporativos relacionados a TI com o gerenciamento geral de riscos corporativos (ERM) e equilibrar os custos e benefícios de gerenciamento de riscos corporativos relacionados a TI.



Pilar	Oportunidade	Recomendações To Be	Recomendação	Artefato
APO12.01 Coletar Dados	Não existe um método documentado para coleta, classificação e análise de risco.	Estabelecer, documentar e manter um método para coleta, classificação e análise de dados relacionados a riscos de TI.		Documento do Processo de Gestão de Riscos
APO12.01 Coletar Dados	Não existe um método documentado para coleta, classificação e análise de risco.	Registrar dados relevantes e significativos relacionados a riscos de TI no ambiente operacional interno e externo da empresa.		Documento do Processo de Gestão de Riscos
APO12.03 Manter um perfil de risco	Não há documentação dos riscos, segregados por categoria, linha de negócio e área funcional.	Agregar e documentar cenários de risco atuais por categoria, linha de negócio e área funcional		Risco documentado. Cenários por linha de negócios e função.
APO12.03 Manter um perfil de risco	Não há uma documentação acerca de quais serviços de TI e infraestrutura são críticos para operação do negócio e riscos relacionados.	Determinar e concordar sobre quais serviços de TI e recursos de infraestrutura de TI são essenciais para sustentar a operação de negócio e processos. Analisar as dependências e identificar os elos fracos. Documentar em um catálogo de serviços críticos.		Serviços críticos de TI para sustentação do negócio.
APO12.05 Definir um portfólio de ações de gerenciamento de riscos.	Não há documentação sobre as atividades de controle de riscos.	Manter uma documentação das atividades de controle que estão em vigor para mitigar o risco e que permitam que o risco seja assumido de acordo com apetite do risco e tolerância. Classifique as atividades de controle e mapeie-as para cenários de risco de TI específicos.		Documentação das atividades de controle do risco.

APO06

APO09

APO12

BAI06

BAI09

BAI10

BAI11

DSS01

DSS02

DSS05



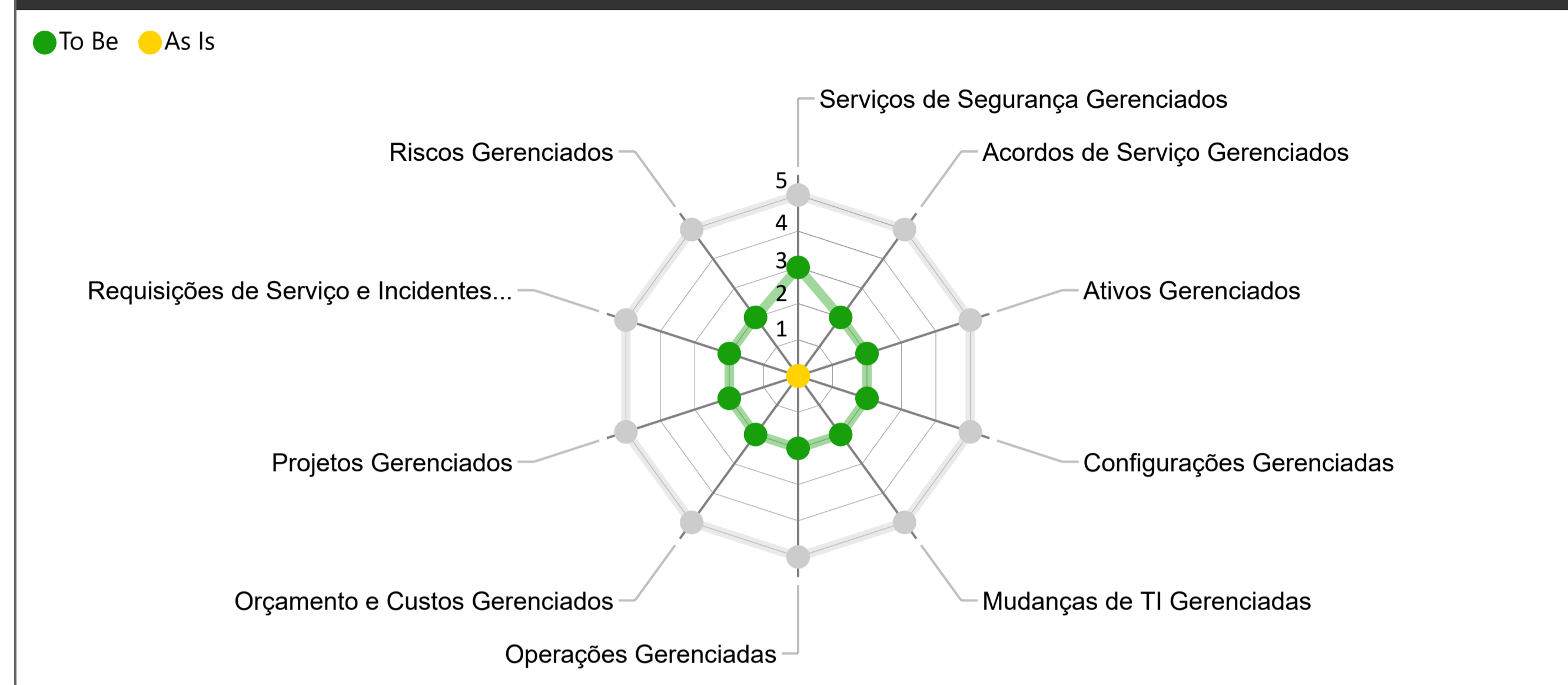
Nível	Processo	Descrição
0	Processo Incompleto	Processo não implementado ou não cumpre seu propósito.
1	Processo Executado	O processo implementado atinge o objetivo proposto.
2	Processo Gerenciado	O desempenho do processo agora é implementado de forma gerenciada e seus produtos de trabalho são apropriadamente estabelecidos, controlados e mantidos.
3	Processo Estabelecido	O processo gerenciado é agora implementado usando um processo definido que é capaz de alcançar seus resultados de processo
4	Processo Previsível	O processo estabelecido é agora operado dentro de limites definidos, apresentando atributos como a gestão e o controle do processo.
5	Processo Otimizado	O processo previsível do nível 4 é continuamente aprimorado para atingir as metas atuais e futuras de negócio.

Processo Mudanças de TI Gerenciadas

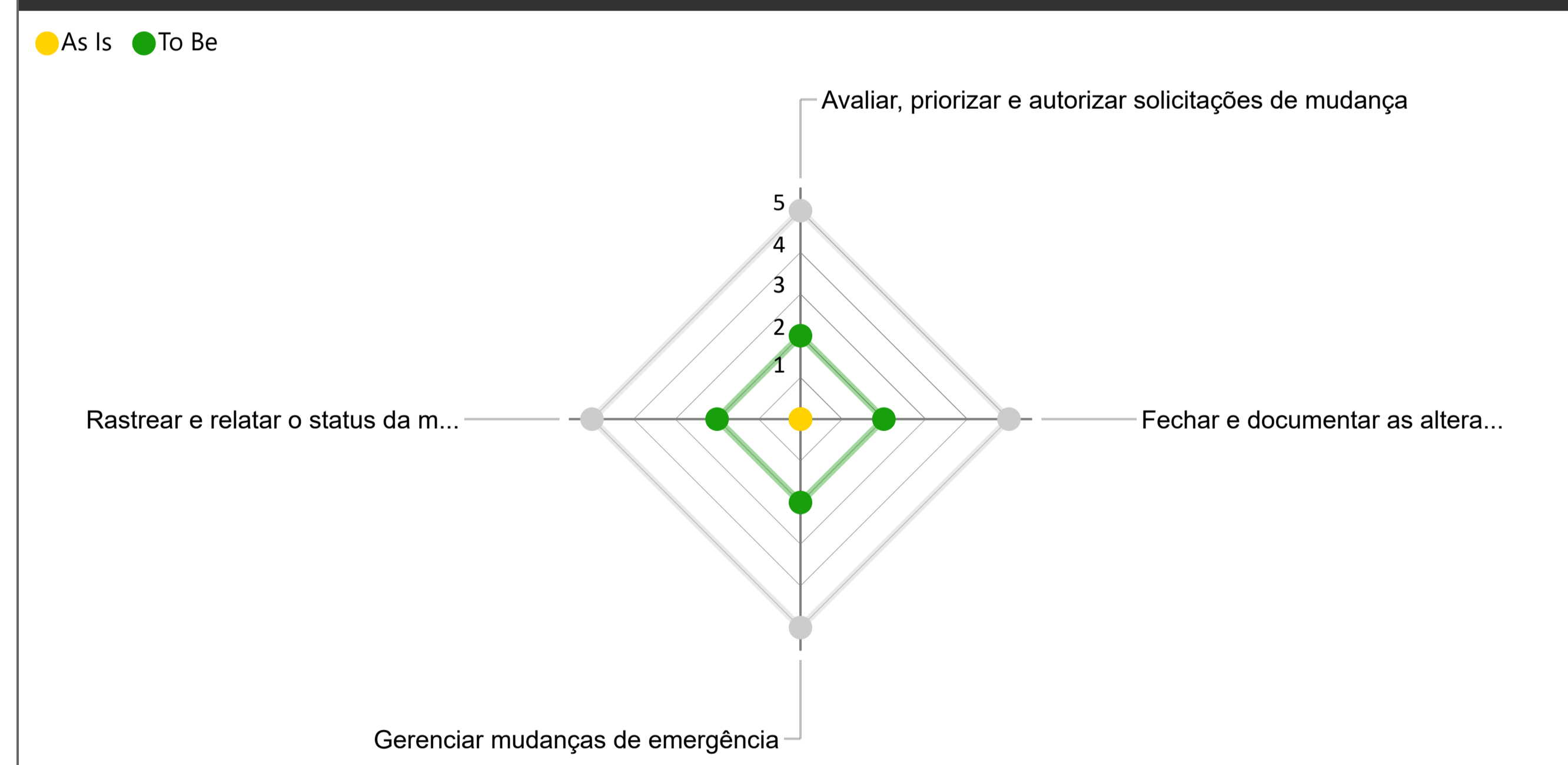
Descrição do Processo
Gerenciar todas as alterações de maneira controlada, incluindo alterações padrão e manutenção de emergência relacionadas a processos de negócios, aplicativos e infraestrutura. Isso inclui padrões e procedimentos de mudança, avaliação de impacto, priorização e autorização, mudanças de emergência, rastreamento, relatórios, encerramento e documentação.

Propósito
Permitir a entrega rápida e confiável de mudanças para o negócio. Mitigar o risco de impactar negativamente a estabilidade ou integridade do ambiente alterado.

Análise Consolidada de Capacidade dos Processos



Análise Individual de Capacidade dos Processos



Pilar	Oportunidade	Recomendação	Artefato
BAI06.01 Avaliar, priorizar e autorizar solicitações de mudança	Não há um processo de gestão de mudança definido e implementado na CPRM. Todas as mudanças são realizadas de forma empírica e pontual.	Aprovar formalmente as requisições de mudança pelos proprietários do processo de negócio afetado. Para as mudanças priorizadas como baixo risco deverão ser pré-aprovadas como mudança padrão.	Documento de Requisição de Mudança.
BAI06.01 Avaliar, priorizar e autorizar solicitações de mudança	Não há um processo de gestão de mudança definido e implementado na CPRM. Todas as mudanças são realizadas de forma empírica e pontual.	Criar uma categorização padrão para as mudanças. Ex: Infraestrutura, Sistema Operacional, Sistemas Aplicativos, etc.	Lista de Categorias de Mudança.
BAI06.01 Avaliar, priorizar e autorizar solicitações de mudança	Não há um processo de gestão de mudança definido e implementado na CPRM. Todas as mudanças são realizadas de forma empírica e pontual.	Definir uma formalização padrão para o requerimento de mudança, incluindo o solicitante e o aprovador.	Documento de Requisição de Mudança.
BAI06.01 Avaliar, priorizar e autorizar solicitações de mudança	Não há um processo de gestão de mudança definido e implementado na CPRM. Todas as mudanças são realizadas de forma empírica e pontual.	Mapear, definir e implementar um processo para gestão de mudança. Certificar que toda e qualquer mudança seja realizada através do processo de gestão de mudança.	Documento do Processo de Gestão de Mudança.
BAI06.01 Avaliar, priorizar e autorizar solicitações de mudança	Não há um processo de gestão de mudança definido e implementado na CPRM. Todas as mudanças são realizadas de forma empírica e pontual.	Planejar e comunicar a execução da mudança.	Comunicado da Mudança.
BAI06.01 Avaliar, priorizar e autorizar solicitações de mudança	Não há um processo de gestão de mudança definido e implementado na CPRM. Todas as mudanças são realizadas de forma empírica e pontual.	Priorizar toda e qualquer mudança, identificando também aquelas que são	N/A

APO06

APO09

APO12

BAI06

BAI09

BAI10

BAI11

DSS01

DSS02

DSS05



Nível	Processo	Descrição
0	Processo Incompleto	Processo não implementado ou não cumpre seu propósito.
1	Processo Executado	O processo implementado atinge o objetivo proposto.
2	Processo Gerenciado	O desempenho do processo agora é implementado de forma gerenciada e seus produtos de trabalho são apropriadamente estabelecidos, controlados e mantidos.
3	Processo Estabelecido	O processo gerenciado é agora implementado usando um processo definido que é capaz de alcançar seus resultados de processo
4	Processo Previsível	O processo estabelecido é agora operado dentro de limites definidos, apresentando atributos como a gestão e o controle do processo.
5	Processo Otimizado	O processo previsível do nível 4 é continuamente aprimorado para atingir as metas atuais e futuras de negócio.

Processo

Ativos Gerenciados

Descrição do Processo

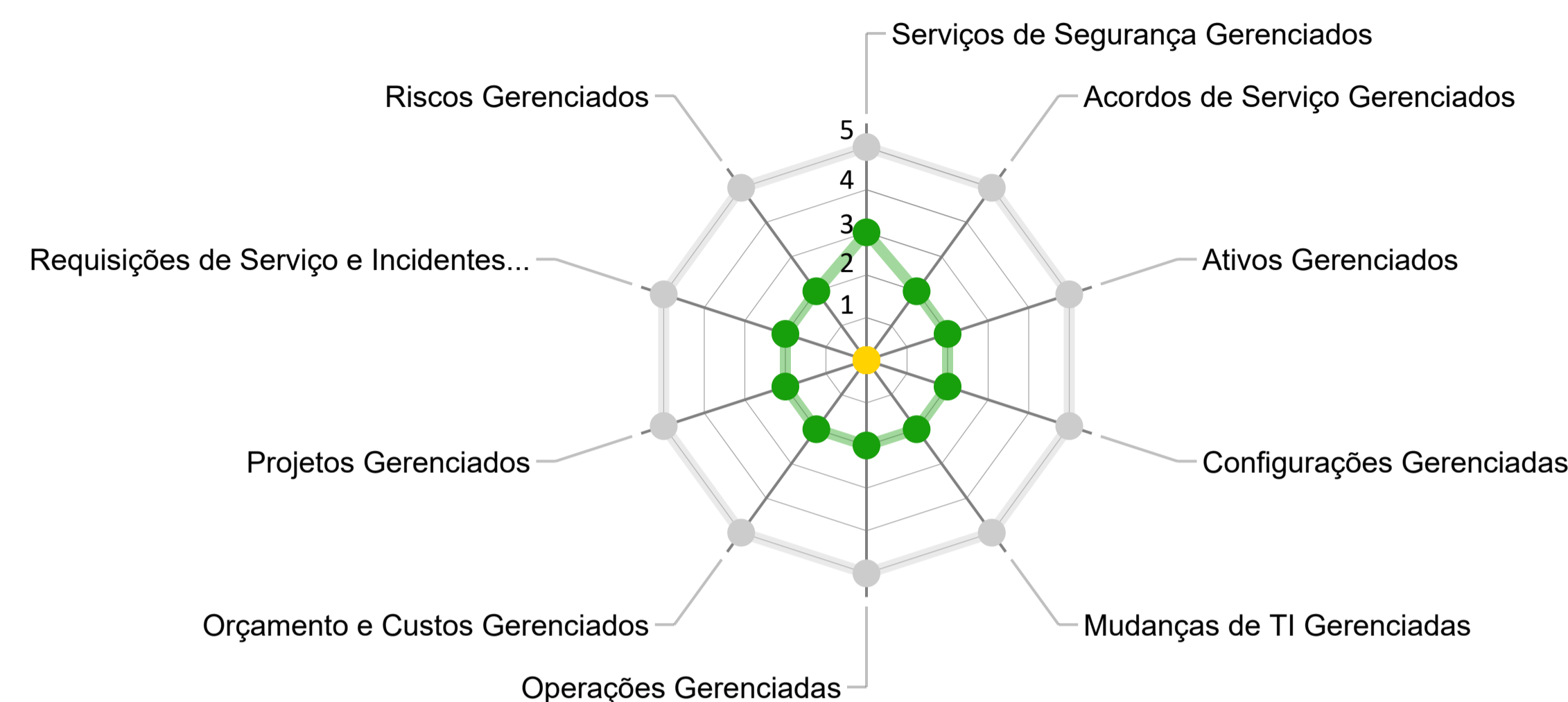
Gerencie os ativos de TI durante seu ciclo de vida para garantir que seu uso agregue valor ao custo ideal, permaneçam operacionais (adequados à finalidade) e eles são contabilizados e fisicamente protegidos. Certifique-se de que os ativos que são críticos para dar suporte à capacidade do serviço sejam confiáveis e estejam disponíveis. Gerenciar licenças de software para garantir que o número ideal seja adquirido, retido e implantado em relação ao uso comercial necessário e o software instalado está em conformidade com os contratos de licença.

Propósito

Contabilize todos os ativos de TI e otimize o valor fornecido pelo seu uso.

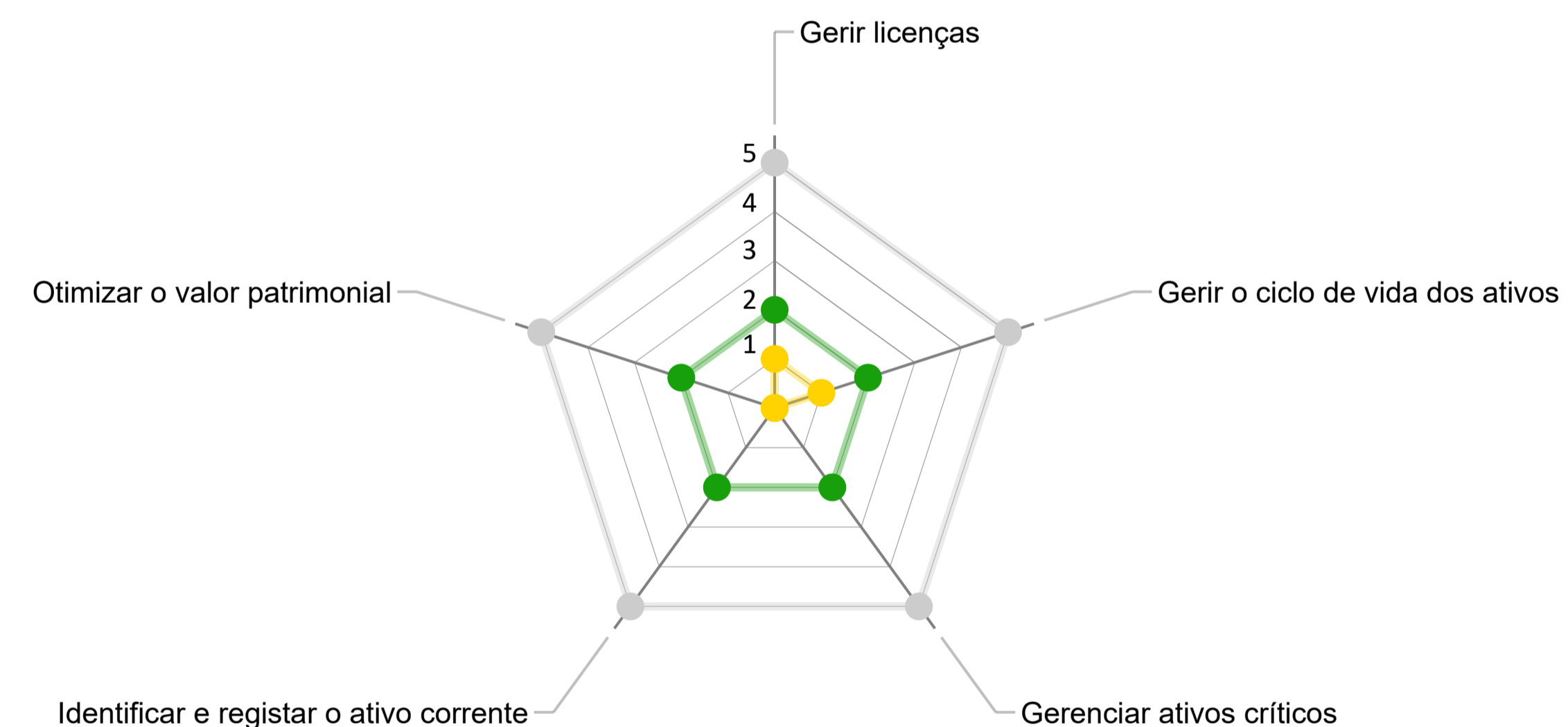
Análise Consolidada de Capacidade dos Processos

● To Be ● As Is



Análise Individual de Capacidade dos Processos

● As Is ● To Be



Recomendações To Be

Pilar	Oportunidade	Recomendação	Artefato
BAI09.01 Identificar e registrar o ativo corrente	Não existe um processo documentado para gestão de Ativos. O inventário não é completo e não é realizado de forma automática ou semi-automática.	Criar, documentar e implementar um processo para gestão dos ativos.	Documento do Processo de Gestão de Ativos
BAI09.01 Identificar e registrar o ativo corrente	Não existe um processo documentado para gestão de Ativos. O inventário não é completo e não é realizado de forma automática ou semi-automática.	Inventariar todos os ativos de Hardware e Software através de ferramentas autônomas ou semi-autônomas.	Inventário de Ativos
BAI09.01 Identificar e registrar o ativo corrente	Não existe um processo documentado para gestão de Ativos. O inventário não é completo e não é realizado de forma automática ou semi-automática.	Verificar e documentar periodicamente os requisitos legais, regulatórios ou contratuais para a aquisição/uso do ativo.	Resultado de Adequação de Ativos
BAI09.01 Identificar e registrar o ativo corrente	Não existe um processo documentado para gestão de Ativos. O inventário não é completo e não é realizado de forma automática ou semi-automática.	Verificar e documentar periodicamente se os ativos estão adequados ao propósito e em boas condições de uso.	Resultado de Adequação de Ativos
BAI09.02 Gerenciar ativos críticos	A identificação dos ativos críticos é realizada apenas de forma empírica, sem documentação.	Criar, documentar e implementar um processo para identificação e classificação dos ativos críticos.	Documento do Processo de Gestão de Ativos
BAI09.02 Gerenciar ativos críticos	Não há um procedimento documentado para comunicação aos usuários acerca de inatividade ou degradação de desempenho dos ativos em caso de manutenção preventiva.	Criar, documentar e implementar um processo formal para comunicação aos usuários acerca de manutenções preventivas e seus impactos nos serviços.	Comunicação de manutenção planejada e tempo de inatividade.

APO06

APO09

APO12

BAI06

BAI09

BAI10

BAI11

DSS01

DSS02

DSS05



Nível	Processo	Descrição
0	Processo Incompleto	Processo não implementado ou não cumpre seu propósito.
1	Processo Executado	O processo implementado atinge o objetivo proposto.
2	Processo Gerenciado	O desempenho do processo agora é implementado de forma gerenciada e seus produtos de trabalho são apropriadamente estabelecidos, controlados e mantidos.
3	Processo Estabelecido	O processo gerenciado é agora implementado usando um processo definido que é capaz de alcançar seus resultados de processo
4	Processo Previsível	O processo estabelecido é agora operado dentro de limites definidos, apresentando atributos como a gestão e o controle do processo.
5	Processo Otimizado	O processo previsível do nível 4 é continuamente aprimorado para atingir as metas atuais e futuras de negócio.

Processo **Configurações Gerenciadas**

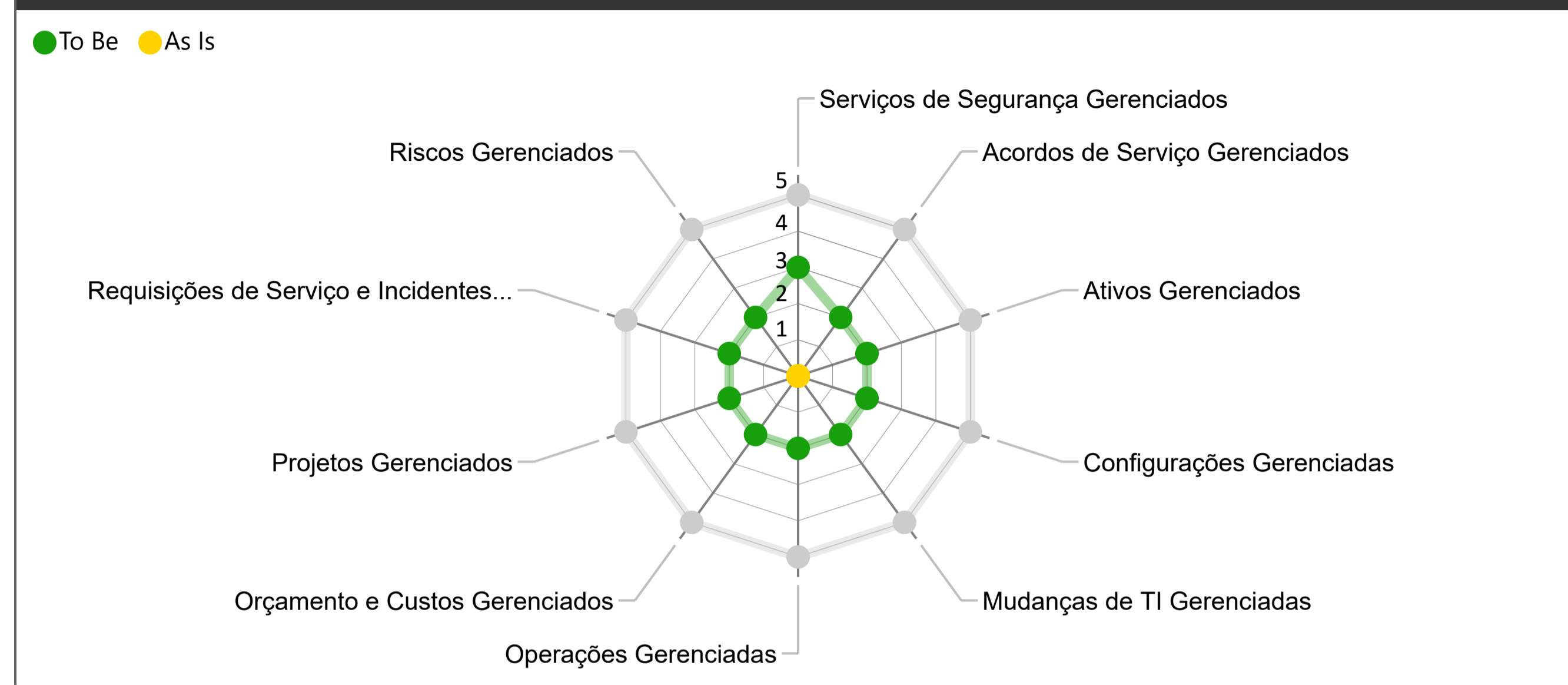
Descrição do Processo

Definir e manter descrições e relacionamentos entre os principais recursos e capacidades necessários para entregar serviços habilitados para TI. Inclua a coleta de informações de configuração, estabelecimento de linhas de base, verificação e auditoria de informações de configuração e atualização do repositório de configuração.

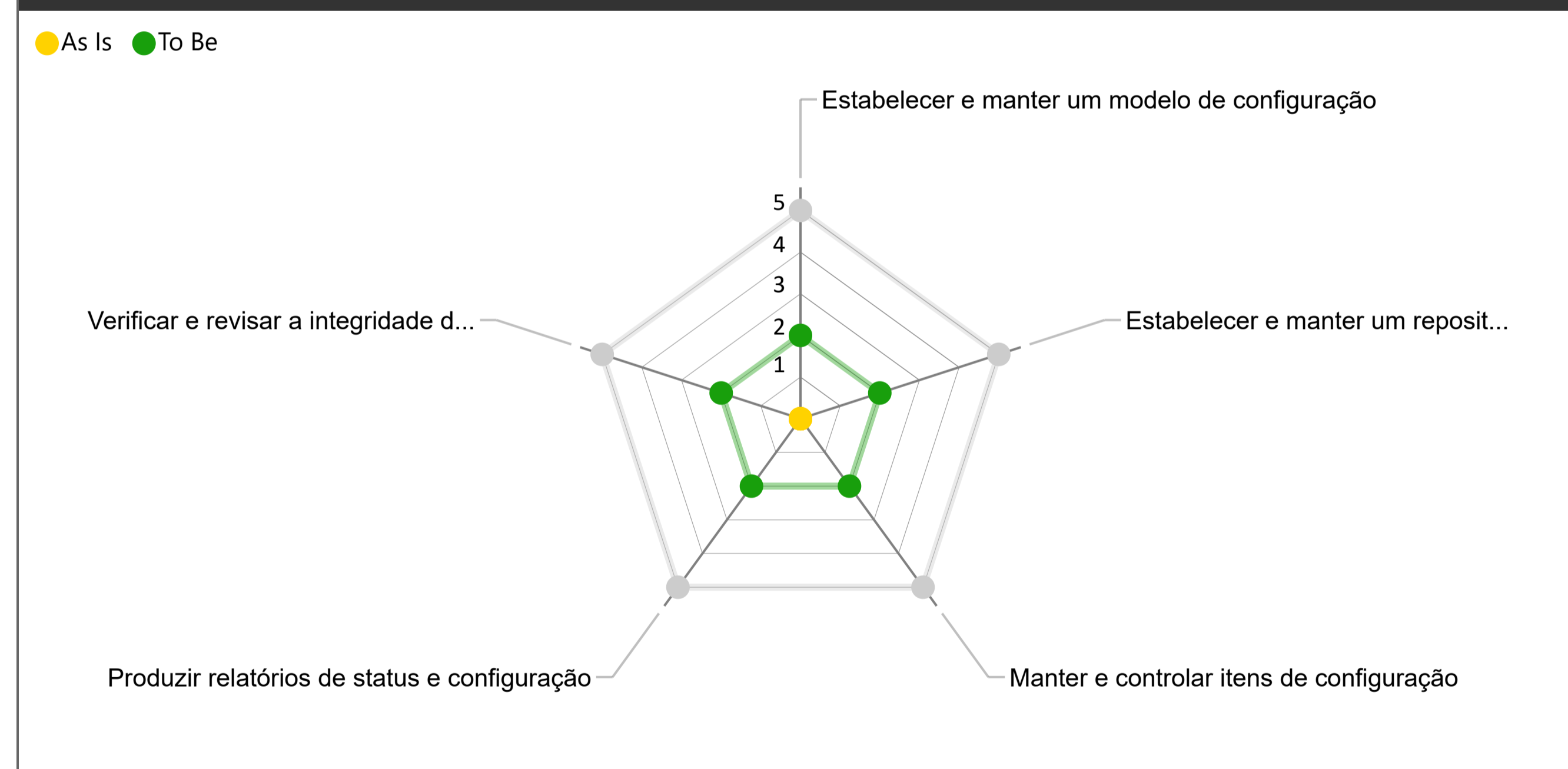
Propósito

Fornecer informações suficientes sobre os ativos de serviço para permitir que o serviço seja gerenciado com eficiência. Avaliar o impacto das mudanças e lidar com os incidentes de serviço.

Análise Consolidada de Capacidade dos Processos



Análise Individual de Capacidade dos Processos



Pilar	Oportunidade	Recomendação	Artefato
BAI10.02 Estabelecer e manter um repositório de configuração e linha de base	Não há um processo definido e documentado para gestão da configuração.	Criar, documentar e implementar um processo para gestão da configuração.	Documento do Processo de Gestão da Configuração.
BAI10.02 Estabelecer e manter um repositório de configuração e linha de base	Só existe o repositório de itens de configuração para equipamentos de rede (Switch, Firewall)	Identificar e registrar os itens de configuração de todos os ativos e suas respectivas linhas base.	Repositório de Configuração e Linhas Base.
BAI10.03 Manter e controlar itens de configuração	Não há registro das modificações realizadas nos itens de configuração.	Identificar regularmente todas as alterações nos Itens de Configuração e atualizar o repositório.	Repositório de Configuração e Linhas Base atualizado.
BAI10.04 Produzir relatórios de status e configuração	Não há registro das modificações realizadas nos itens de configuração.	Identificar a mudança de status dos Itens de Configuração e atualizar a Linha Base.	Repositório de Configuração e Linhas Base atualizado.

- APO06
- APO09
- APO12
- BAI06
- BAI09
- BAI10
- BAI11
- DSS01
- DSS02
- DSS05



Nível	Processo	Descrição
0	Processo Incompleto	Processo não implementado ou não cumpre seu propósito.
1	Processo Executado	O processo implementado atinge o objetivo proposto.
2	Processo Gerenciado	O desempenho do processo agora é implementado de forma gerenciada e seus produtos de trabalho são apropriadamente estabelecidos, controlados e mantidos.
3	Processo Estabelecido	O processo gerenciado é agora implementado usando um processo definido que é capaz de alcançar seus resultados de processo
4	Processo Previsível	O processo estabelecido é agora operado dentro de limites definidos, apresentando atributos como a gestão e o controle do processo.
5	Processo Otimizado	O processo previsível do nível 4 é continuamente aprimorado para atingir as metas atuais e futuras de negócio.

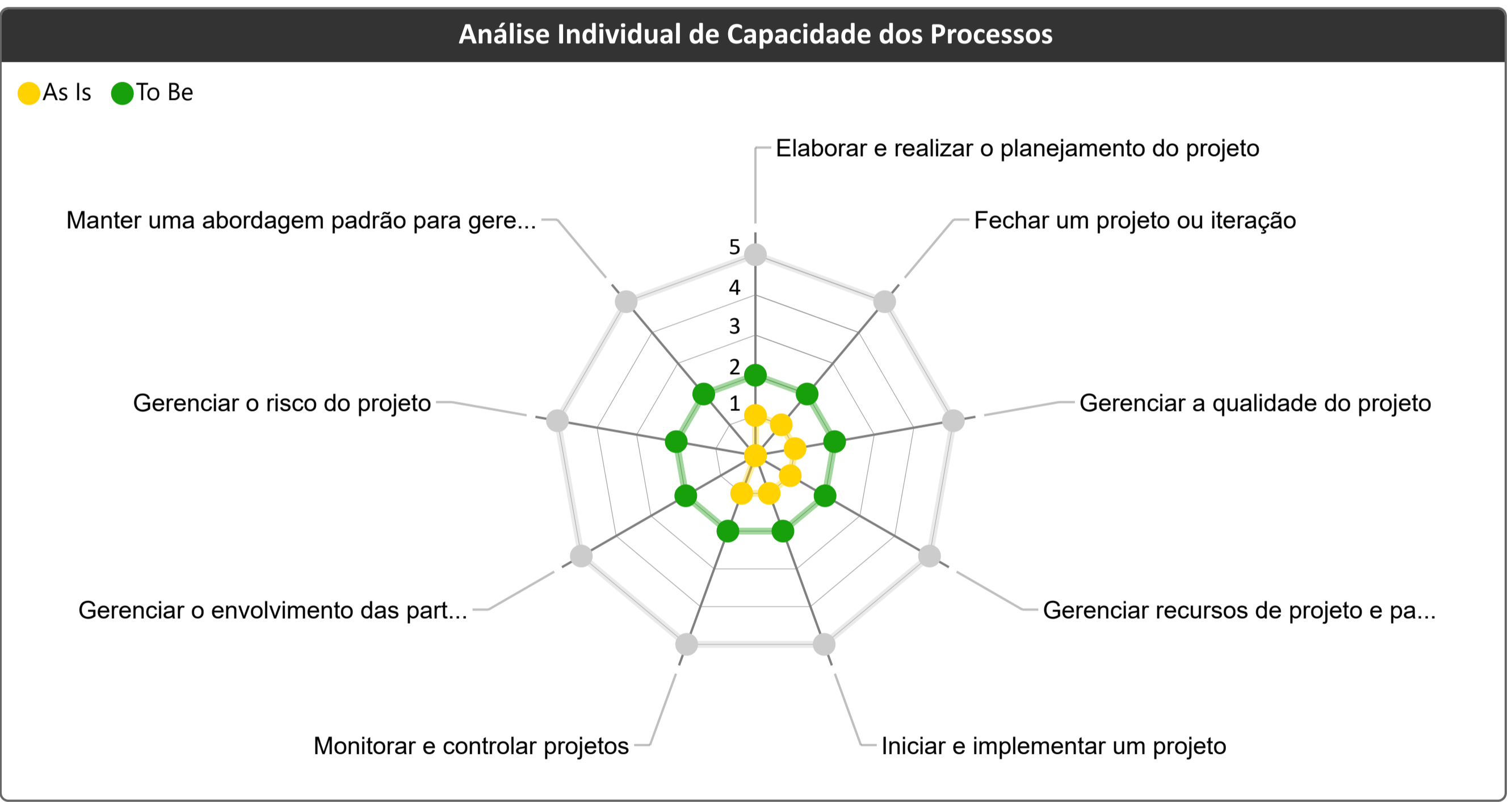
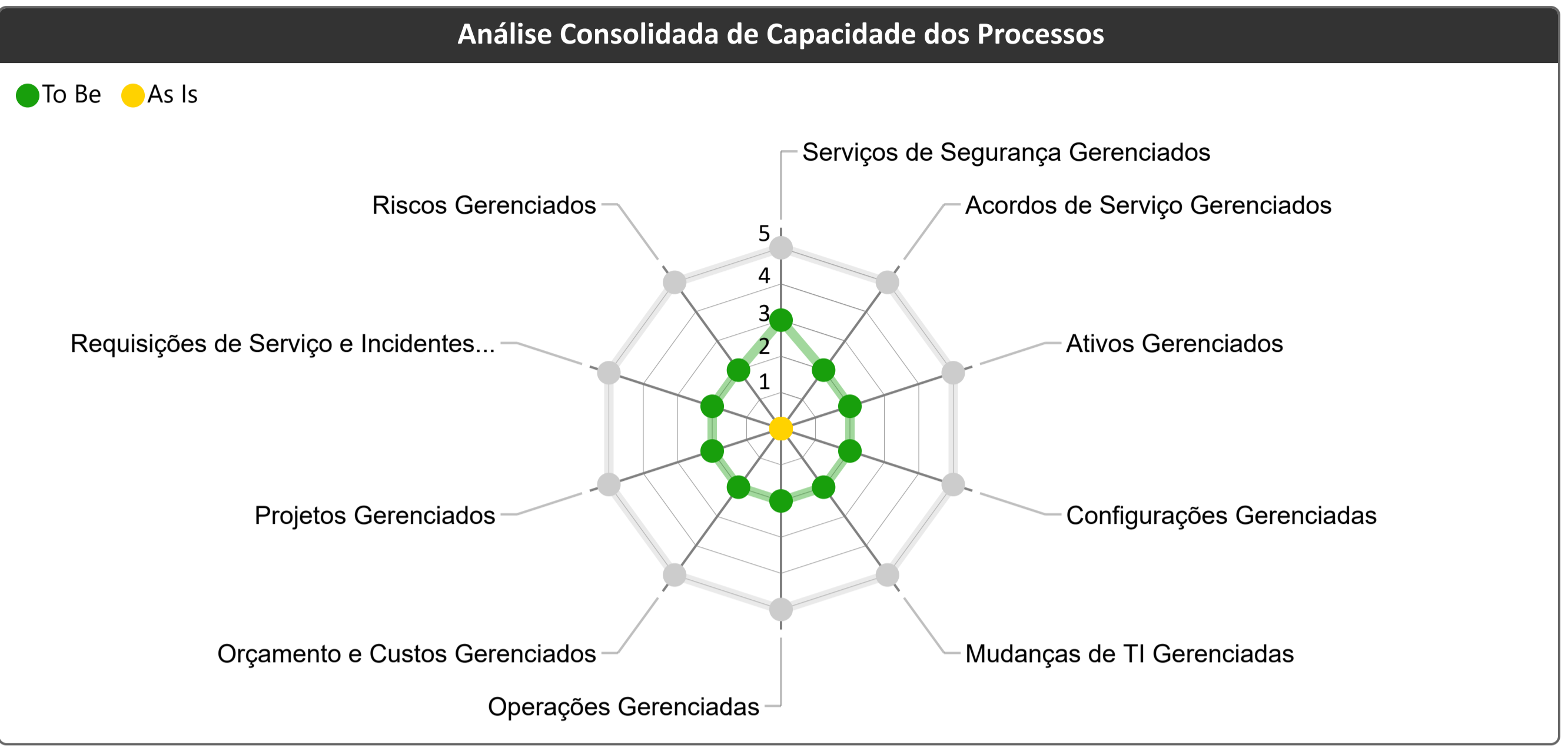
Processo Projetos Gerenciados

Descrição do Processo

Gerenciar todos os projetos que são iniciados dentro da empresa em alinhamento com a estratégia da empresa e de forma coordenada com base na abordagem padrão de gerenciamento de projetos. Iniciar, planejar, controlar e executar projetos e encerrar com uma revisão pós-implementação.

Propósito

Obter resultados de projeto definidos e reduzir o risco de atrasos inesperados, custos e reduções de valor, melhorando as comunicações e o envolvimento de negócios e usuários finais. Garantir o valor e a qualidade dos entregáveis do projeto e maximizar sua contribuição para os programas definidos e portfólio de investimentos.



Recomendações To Be				
Pilar	Oportunidade	Recomendação	Artefato	
BAI11.01	Manter uma abordagem padrão para gerenciamento de projetos.	Não existe programa de treinamento para gerenciamento de projetos.	Fornecer treinamento adequado em gerenciamento de projetos e considerar a certificação para gerentes de projeto.	Programa de Treinamento em Gestão de Projetos.
BAI11.02	Iniciar e implementar um projeto.	Quando um projeto é iniciado, não é assegurado que as partes interessadas e/ou patrocinadores (negócio) concordem e aceitem os requisitos do projeto, incluindo a definição dos critérios de sucesso (aceitação) do projeto e indicadores-chave de desempenho (KPIs).	Assegurar que as partes interessadas e patrocinadores concordem e aceitem os requisitos do projeto, definição do critério de aceitação e indicadores chave de desempenho.	Documentos de Iniciação do Projeto.
BAI11.06	Gerenciar o risco do projeto.	Não há um processo de gestão de riscos nos projetos.	Atribuir a pessoa devidamente qualificada a responsabilidade pela execução do processo de gerenciamento de riscos do projeto e garantir que isso seja incorporado às práticas de desenvolvimento da solução. Considere alocar essa função para uma equipe independente, especialmente se for necessário um ponto de vista objetivo ou se um projeto for considerado crítico.	Processo de gestão de riscos.

APO06

APO09

APO12

BAI06

BAI09

BAI10

BAI11

DSS01

DSS02

DSS05



Nível	Processo	Descrição
0	Processo Incompleto	Processo não implementado ou não cumpre seu propósito.
1	Processo Executado	O processo implementado atinge o objetivo proposto.
2	Processo Gerenciado	O desempenho do processo agora é implementado de forma gerenciada e seus produtos de trabalho são apropriadamente estabelecidos, controlados e mantidos.
3	Processo Estabelecido	O processo gerenciado é agora implementado usando um processo definido que é capaz de alcançar seus resultados de processo
4	Processo Previsível	O processo estabelecido é agora operado dentro de limites definidos, apresentando atributos como a gestão e o controle do processo.
5	Processo Otimizado	O processo previsível do nível 4 é continuamente aprimorado para atingir as metas atuais e futuras de negócio.

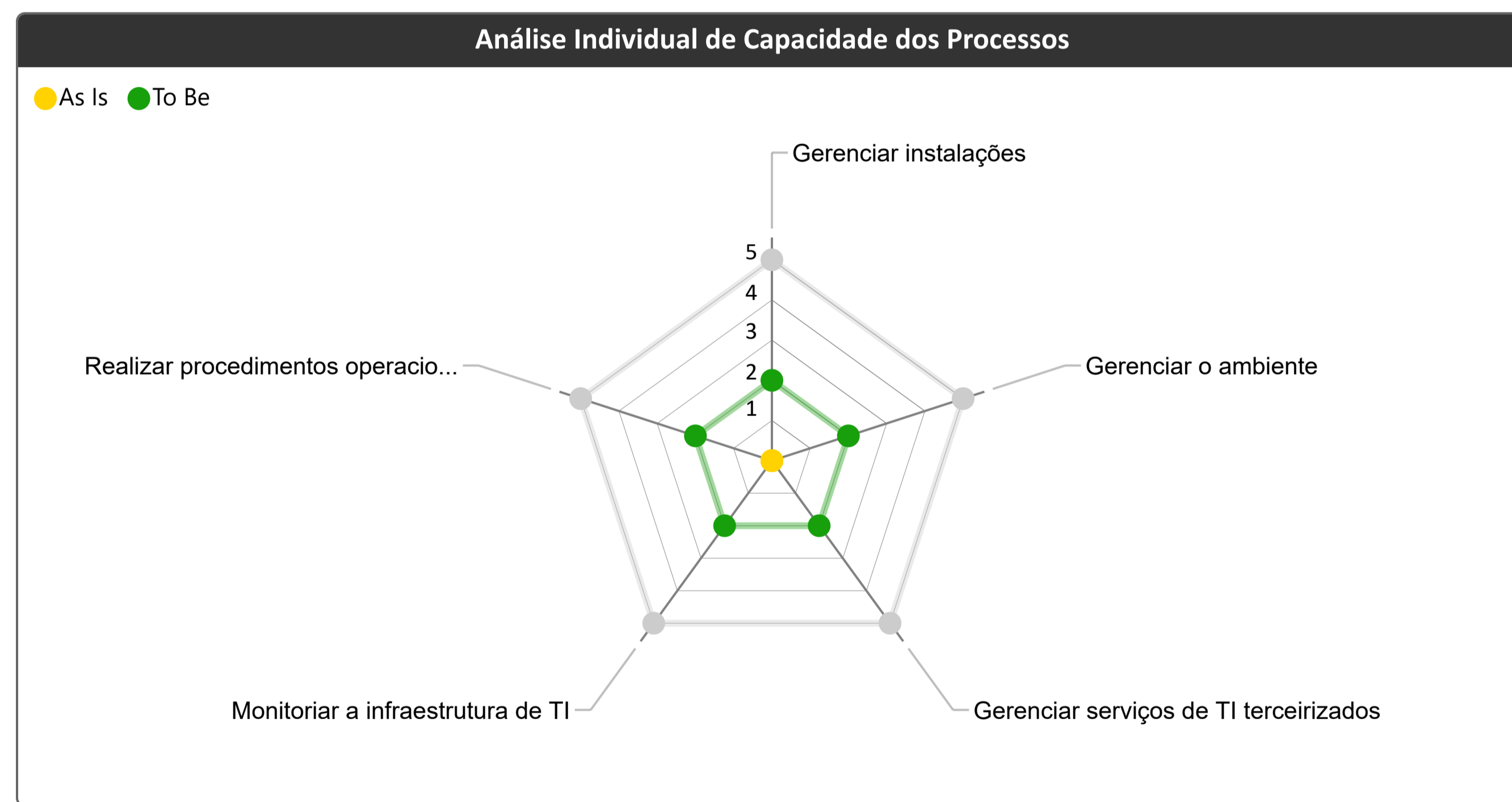
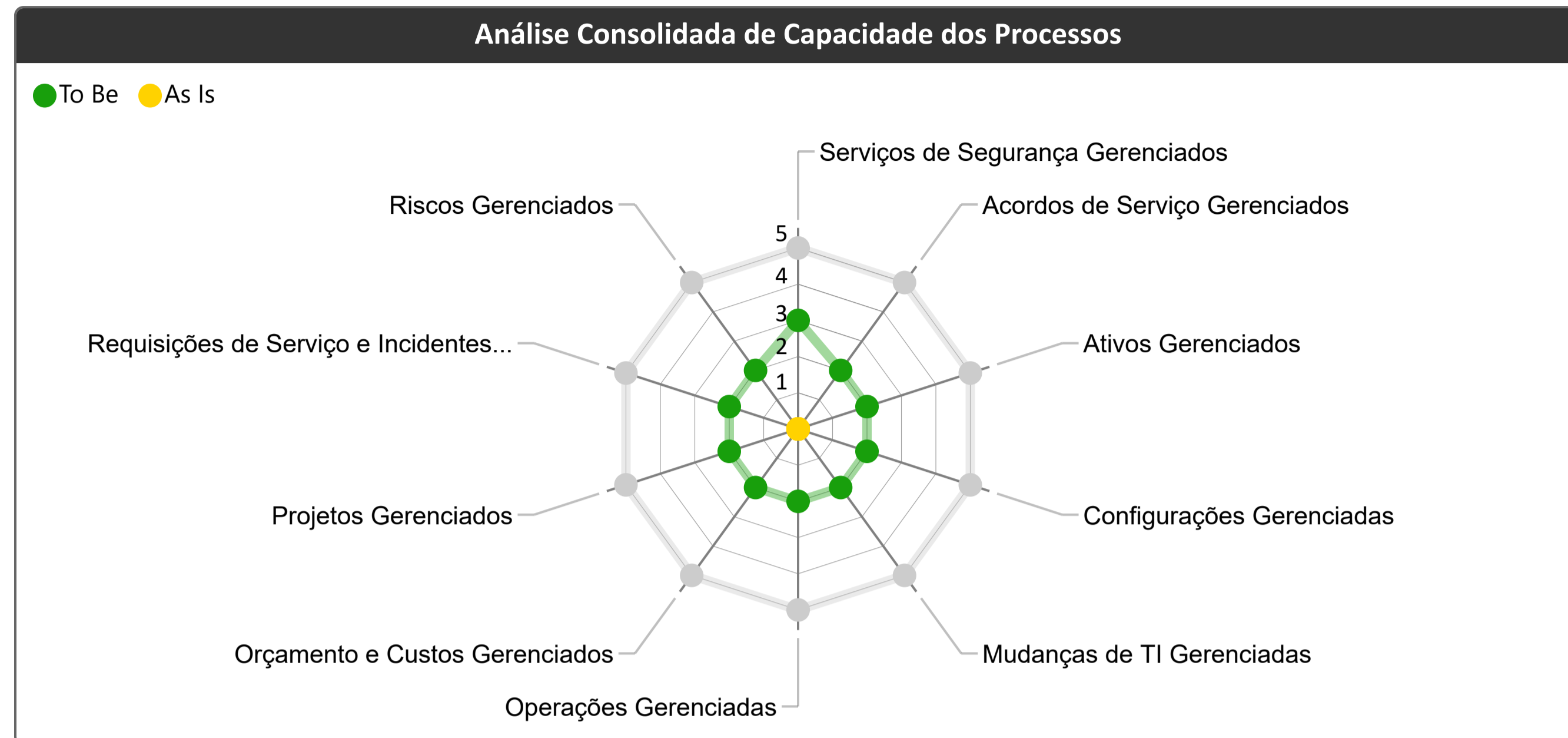
Processo **Operações Gerenciadas**

Descrição do Processo

Coordenar e executar as atividades e procedimentos operacionais necessários à prestação de serviços de TI internos e terceirizados. Inclui a execução de procedimentos operacionais padrão pré-definidos e as atividades de controle necessárias.

Propósito

Fornecer produtos e serviços operacionais de TI, conforme planejado.



Pilar	Oportunidade	Recomendação	Artefato
DSS01.01 Realizar procedimentos operacionais	Não há documentação acerca dos procedimentos operacionais da TI.	Criar uma documentação dos procedimentos operacionais da TI.	Procedimentos Operacionais.
DSS01.01 Realizar procedimentos operacionais	Não há planejamento das atividades operacionais.	Elaborar um planejamento de todas as atividades operacionais e sua execução.	Planejamento de Atividades
DSS01.03 Monitoriar a infraestrutura de TI	Não há registros de eventos ocorridos na infraestrutura de TI.	Registrar todos os eventos ocorridos na infraestrutura de TI, considerando os riscos associados ao evento.	Registro de Eventos
DSS01.04 Gerenciar o ambiente	Não há uma política de utilização dos equipamentos ou ambientes de TI com objetivo de prevenir danos aos equipamentos e/ou instalações.	Criar uma política com o objetivo de prevenir danos aos equipamentos e ambientes de TI, por exemplo: proibir o armazenamento de artigos de papelaria ou quaisquer outros objetos que representem risco de incêndio nas salas de informática, proibir o consumo de bebidas durante a utilização de equipamentos, etc.	Política de Utilização de Equipamentos e Ambientes de TI.
DSS01.05 Gerenciar instalações	Inexistência de um padrão do uso de cabeamento de rede lógica de dados e telefonia, sendo a rede não estruturada.	Estruturar a rede lógica de dados e telefonia conforme preconiza a NBR 14565.	Rede Lógica de Dados e Telefonia estruturada.

APO06

APO09

APO12

BAI06

BAI09

BAI10

BAI11

DSS01

DSS02

DSS05

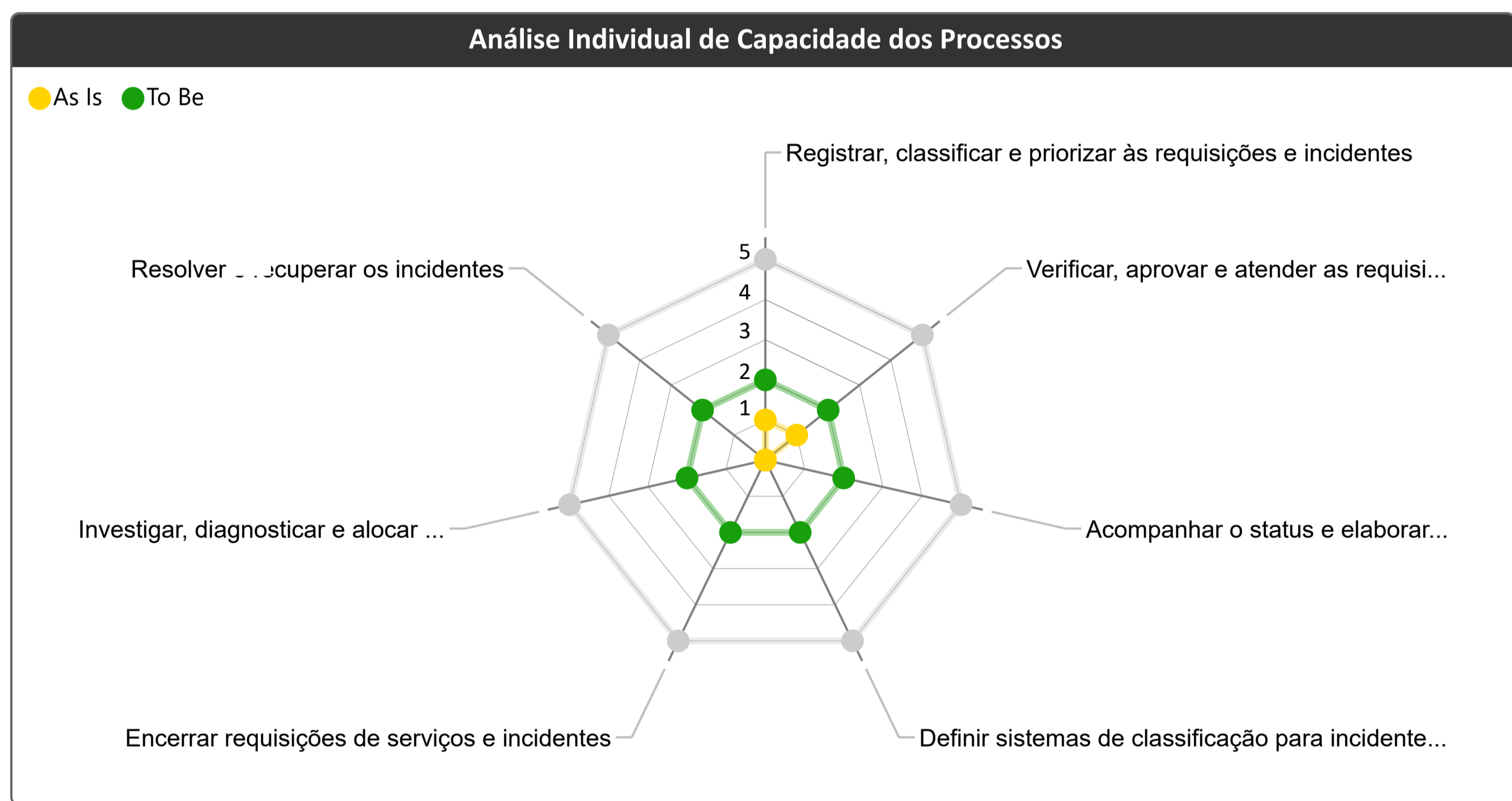
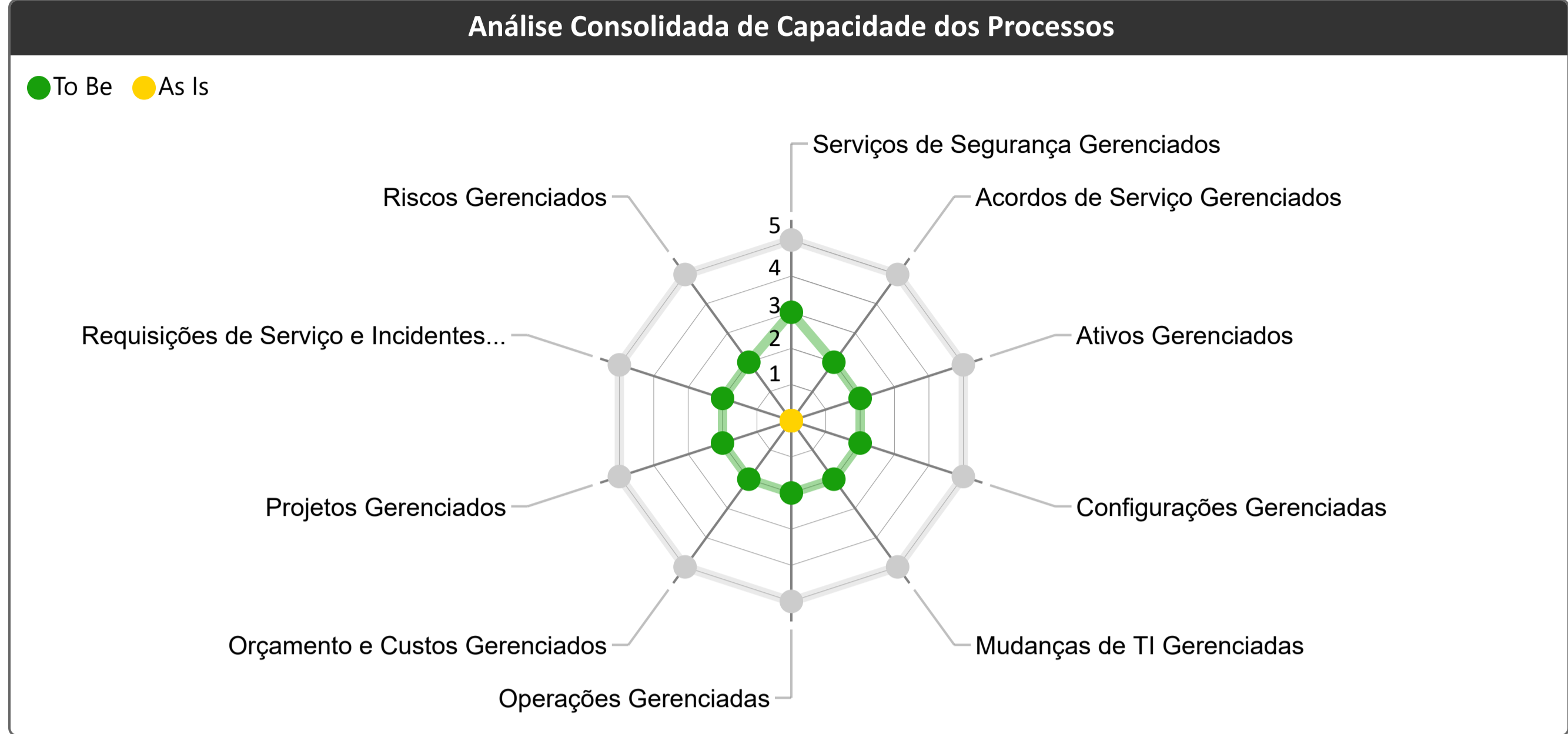


Nível	Processo	Descrição
0	Processo Incompleto	Processo não implementado ou não cumpre seu propósito.
1	Processo Executado	O processo implementado atinge o objetivo proposto.
2	Processo Gerenciado	O desempenho do processo agora é implementado de forma gerenciada e seus produtos de trabalho são apropriadamente estabelecidos, controlados e mantidos.
3	Processo Estabelecido	O processo gerenciado é agora implementado usando um processo definido que é capaz de alcançar seus resultados de processo
4	Processo Previsível	O processo estabelecido é agora operado dentro de limites definidos, apresentando atributos como a gestão e o controle do processo.
5	Processo Otimizado	O processo previsível do nível 4 é continuamente aprimorado para atingir as metas atuais e futuras de negócio.

Processo Requisições de Serviço e Incidentes Gerenciados

Descrição do Processo
Fornecer uma resposta rápida e eficaz as requisições dos usuários e a resolução de todos os tipos de incidentes. Restaurar o serviço normal; registrar e atender as requisições dos usuários; e registrar, investigar, diagnosticar, escalar e resolver incidentes.

Propósito
Alcançar uma maior produtividade e minimizar interrupções através da rápida resolução de consultas e incidentes dos usuários. Avaliar o impacto das mudanças e lidar com o serviço de incidentes. Resolver requisições de usuários e restaurar o serviço em resposta a incidentes.



Pilar	Oportunidade	Recomendações To Be	Recomendação	Artefato
DSS02.02 Registrar, classificar e priorizar as requisições e incidentes	Não existe um processo definido para atendimento as requisições de serviços e incidentes.	Criar, definir e implementar um processo de atendimento as requisições de serviços e incidentes, com classificação do serviço/incidente.	Documento do Processo de Atendimento as Requisições de Serviço e incidentes.	
DSS02.04 Investigar, diagnosticar e alocar incidentes	As requisições de serviço não são registradas em uma base de conhecimento para que soluções já implementadas possam ser consultadas.	Implementar uma base de conhecimento, registrando as requisições de serviços/incidentes para otimizar a solução de problemas/incidentes já conhecidos.	Base de Conhecimento de Requisições de Serviço/incidentes.	
DSS02.05 Resolver e recuperar os incidentes	Quando é dada uma solução temporária a uma requisição, esta informação não é registrada.	Registrar a informação de soluções temporárias às requisições de serviço/incidente.	Registro da informação de soluções temporárias.	
DSS02.06 Encerrar requisições de serviços e incidentes	Após a resolução da requisição, o usuário não é consultado para saber se a solução foi satisfatória.	Definir e implementar um procedimento para que, no fechamento da requisição de serviço/incidente, o usuário solicitante seja contactado para informar se a solução foi satisfatória.	Documento do Processo de Atendimento as Requisições de Serviço e incidentes.	
DSS02.07 Acompanhar o status e elaborar relatórios	Não há um processo definido para acompanhamento das requisições de serviço/incidentes.	Monitorar toda e qualquer requisição de serviço/incidente aberto, acompanhando suas variações e solicitar procedimentos para avançar para resolução.	Documento do Processo de Atendimento as Requisições de Serviço e incidentes.	

APO06

APO09

APO12

BAI06

BAI09

BAI10

BAI11

DSS01

DSS02

DSS05



Nível	Processo	Descrição
0	Processo Incompleto	Processo não implementado ou não cumpre seu propósito.
1	Processo Executado	O processo implementado atinge o objetivo proposto.
2	Processo Gerenciado	O desempenho do processo agora é implementado de forma gerenciada e seus produtos de trabalho são apropriadamente estabelecidos, controlados e mantidos.
3	Processo Estabelecido	O processo gerenciado é agora implementado usando um processo definido que é capaz de alcançar seus resultados de processo
4	Processo Previsível	O processo estabelecido é agora operado dentro de limites definidos, apresentando atributos como a gestão e o controle do processo.
5	Processo Otimizado	O processo previsível do nível 4 é continuamente aprimorado para atingir as metas atuais e futuras de negócio.

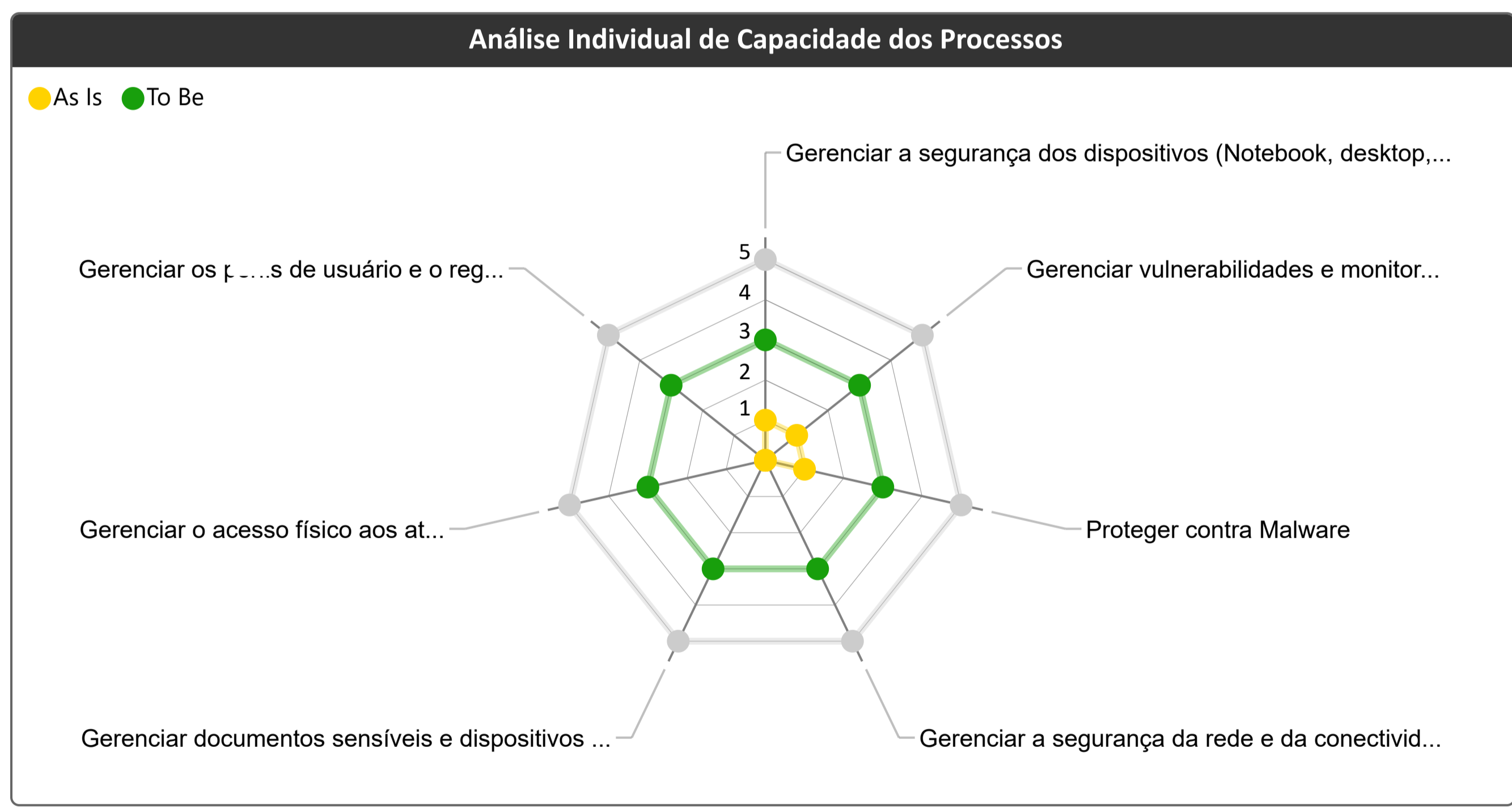
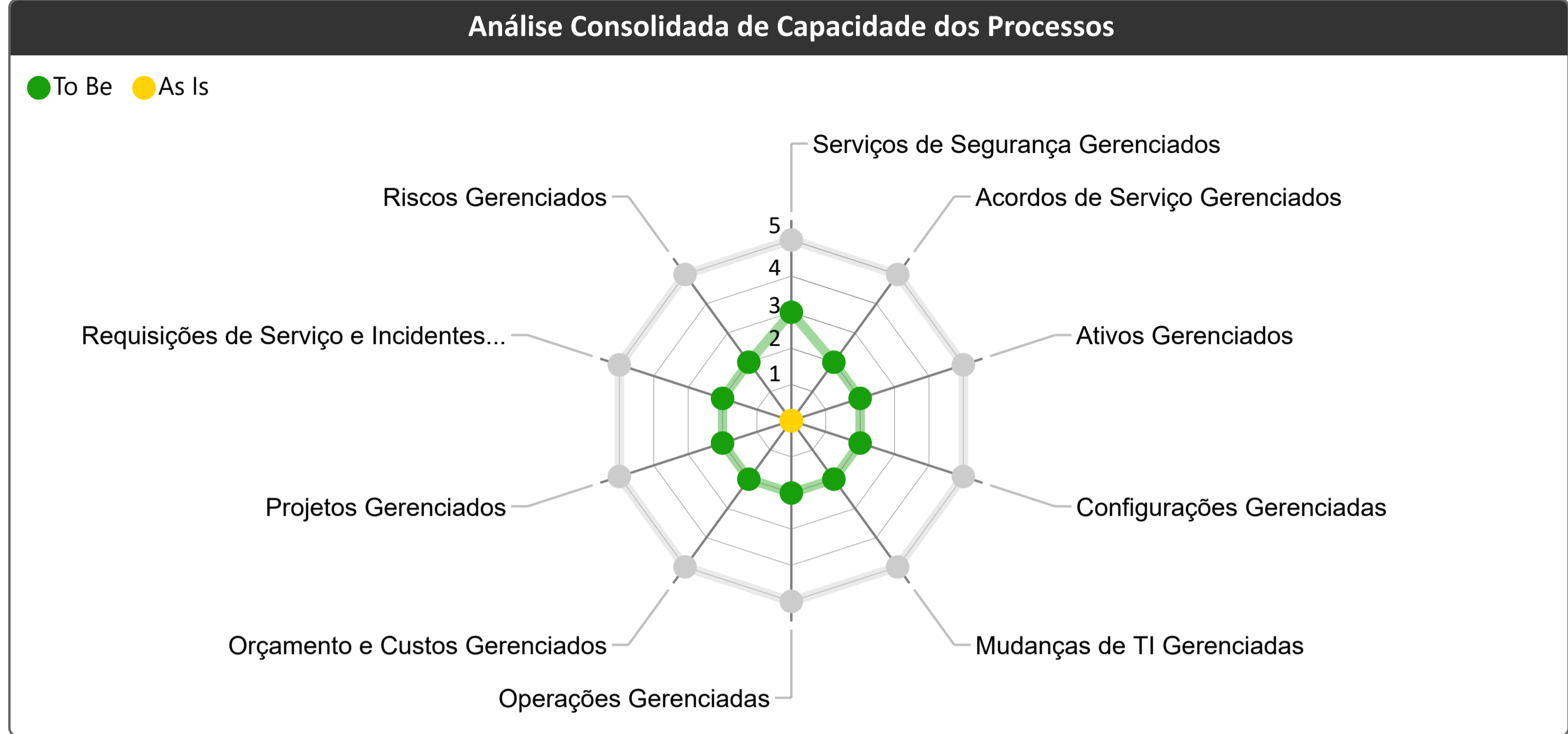
Processo Serviços de Segurança Gerenciados

Descrição do Processo

Proteger a informação da empresa para manter o nível de risco de segurança da informação aceitável para a empresa, de acordo com a política de segurança. Estabelecer e manter funções de segurança da informação e privilégios de acesso. Efetuar o controle de segurança.

Propósito

Minimizar o impacto comercial das vulnerabilidades e incidentes operacionais de segurança da informação.



Pilar	Oportunidade	Recomendação	Artefato
DSS05.01 Proteger contra Malware	A política de proteção contra Malware, incluindo o software endpoint, não possui documentação indicando os procedimentos e configurações.	Documentar a política de utilização de softwares de proteção contra Malware, incluindo sua versão, forma de configuração e atualização.	Política de Prevenção contra Malware.
DSS05.01 Proteger contra Malware	Não há filtragem de tráfego de internet e e-mails.	Implementar um filtro de conteúdo na borda que proteja contra links maliciosos e sites conhecidamente inseguros.	Implementação de Filtro de Conteúdo/anti-spam.
DSS05.01 Proteger contra Malware	Não há filtragem de tráfego de internet e e-mails.	Implementar um filtro na borda que proteja a navegação, downloads e e-mails contra Malwares, Spywares, Phishing e demais códigos maliciosos.	Implementação de Filtro de Conteúdo/anti-spam.
DSS05.02 Gerenciar a segurança da rede e da conectividade	Apenas a rede Wi-Fi possui proteção contra acesso de dispositivos não autorizados. Esta proteção baseia-se em autenticação. Para a rede cabeada, não possui nenhuma proteção contra acesso não autorizado.	Implementar uma proteção contra acesso de dispositivos não autorizados tanto para rede Wi-fi quanto para a rede cabeada, como por exemplo: filtragem por MAC-Address. Certifique-se que esta implementação seja documentada em uma política.	Implementação de uma política contra acesso de dispositivos não autorizados na rede.
DSS05.02 Gerenciar a segurança da rede e da conectividade	Não há documentação para configuração segura dos equipamentos de rede.	Documentar todas as configurações de segurança dos dispositivos de rede.	Documento de configuração de dispositivos de rede.
DSS05.03 Gerenciar a segurança dos	Não existe documentação que registre as configurações de instalação de	Criar uma documentação que registre todas as configurações e procedimentos	Documentação de Instalação e

- Painel 
- Estratégia 
- Pessoas 
- Processos 
- Tecnologia** 
- Orçamento 
- Roadmap 
- Anexos 



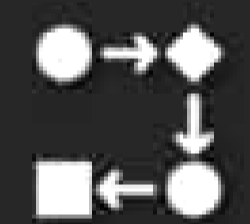
Painel



Estratégia



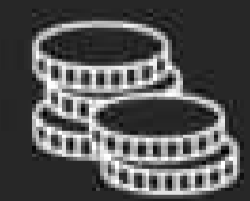
Pessoas



Processos



Tecnologia



Orçamento



Roadmap



CATÁLOGO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - CSTI

Introdução

CSTI

O **Catálogo de Serviços de Tecnologia da Informação – CSTI**, é um instrumento que fornece uma fonte única e organizada de todos os serviços prestados pela área de TI para responder às necessidades de negócio do SGB. Este catálogo deve atender a objetivos específicos, conforme apresentado abaixo.

Para que ter Portfólio e Catálogo de Serviços de TI ?

- 1 Fator crítico de sucesso para o PDTI
- 2 Promove a posição estratégica de TI para o Negócio
- 3 Melhora a comunicação e transparência entre TI e Negócio
- 4 Auxilia a justificar a criação de novos serviços



Objetivos Específicos do CSTI:

- Comunicar como TI provê Serviços
- Padronizar entregas de serviços
- Definir e atingir expectativas do negócio
- Gerenciar solicitações de serviços
- Padronizar solicitações de Serviços
- Incrementar qualidade aos serviços.

- Painel
- Estratégia
- Pessoas
- Processos
- Tecnologia
- Orçamento
- Roadmap

CATÁLOGO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO - CSTI



Introdução

CSTI

Nível	Processo	Descrição
0	Processo Incompleto	Processo não implementado ou não cumpre seu propósito.
1	Processo Executado	O processo implementado atinge o objetivo proposto.
2	Processo Gerenciado	O desempenho do processo agora é implementado de forma gerenciada e seus produtos de trabalho são apropriadamente estabelecidos, controlados e mantidos.
3	Processo Estabelecido	O processo gerenciado é agora implementado usando um processo definido que é capaz de alcançar seus resultados de processo
4	Processo Previsível	O processo estabelecido é agora operado dentro de limites definidos, apresentando atributos como a gestão e o controle do processo.
5	Processo Otimizado	O processo previsível do nível 4 é continuamente aprimorado para atingir as metas atuais e futuras de negócio.

Processo

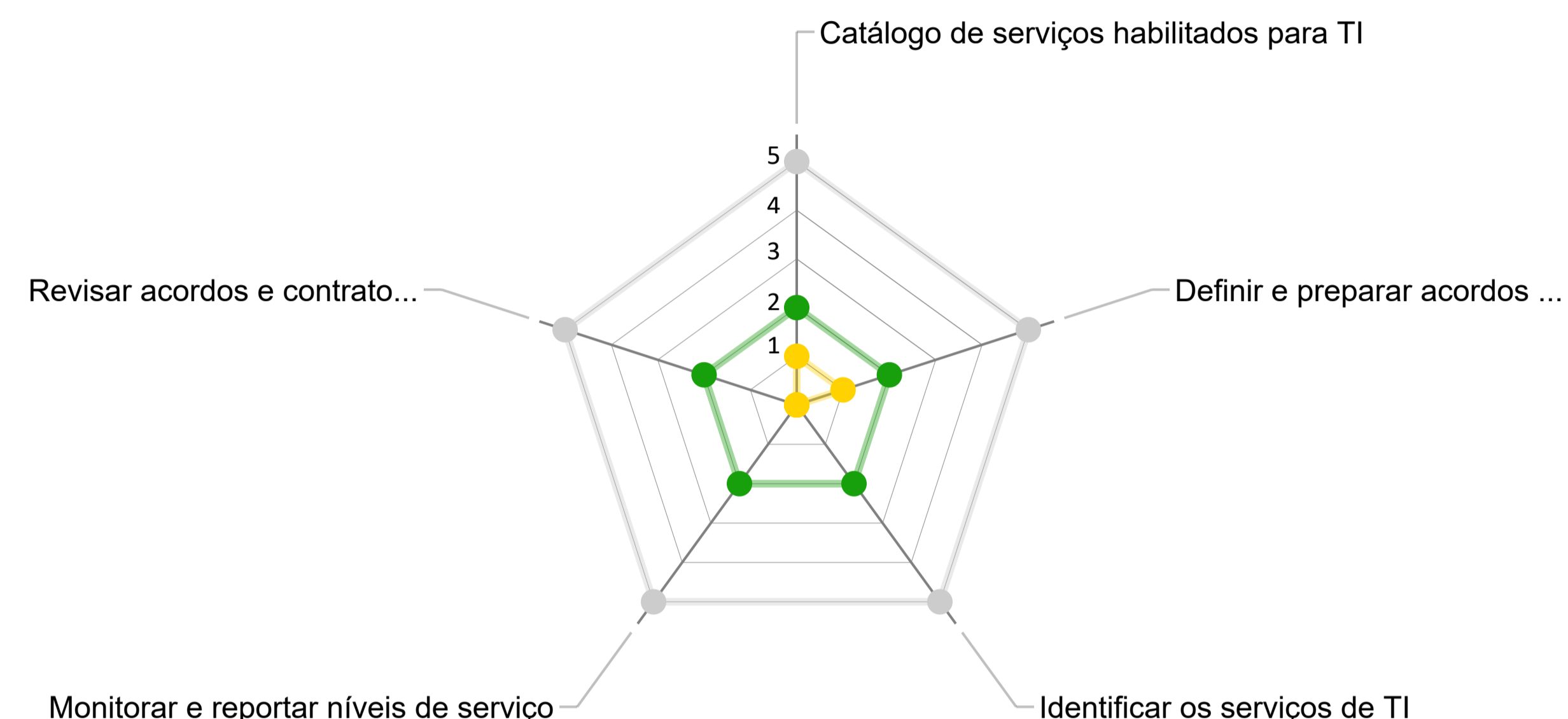
Acordos de Serviço Gerenciados

Descrição do Processo

Alinhar produtos e serviços habilitados para TI e níveis de serviço com as necessidades e expectativas da empresa, incluindo identificação, especificação, design, publicação, contratação e monitoramento de produtos e serviços de TI, níveis de serviço e indicadores de desempenho.

Análise Individual de Capacidade dos Processos

● As Is ● To Be



Propósito

Garantir que os produtos, serviços e níveis de serviço de TI atendam às necessidades atuais e futuras da empresa.

Pilar	Oportunidade	Recomendação	Artefato
APO09.01 Identificar os serviços de TI	Não é realizado um estudo para estimar a demanda futura e tendência para confirmar a capacidade dos serviços.	Mapear, documentar e implementar um processo para realização de um estudo que possibilite estimar a demanda futura de serviços de TI para poder confirmar a capacidade dos serviços oferecidos.	Análise de Tendência da demanda de serviços de TI.
APO09.01 Identificar os serviços de TI	Não há um processo definido para análise, em uma linha de tempo, dos serviços atuais de TI e seus SLAs, para identificar lacunas entre o esperado pelo negócio e o realizado.	Mapear e documentar um processo para análise dos serviços atuais de TI e seus SLAs, verificando se está alinhado com a necessidade do negócio. Este processo deverá ser realizado em uma rotina definida.	Documentação do Processo de Análise dos Serviços e SLA. Lacunas identificadas entre a necessidade do negócio e os serviços de TI e SLAs ofertados.
APO09.02 Catálogo de serviços habilitados para TI	A publicação dos serviços e seus SLAs no catálogo de serviços é realizado esporadicamente, de forma empírica.	Criar uma recorrência para atualização do catálogo de serviços e SLAs, documentada em forma de processo.	Documentação do Processo de Atualização do Catálogo de Serviços
APO09.03 Definir e preparar acordos de serviço	A definição do SLA necessário para o serviço realizado e/ou contratado é realizada de forma empírica, sem um processo definido e documentado.	Mapear e documentar um processo para definição dos SLAs necessários para os serviços a serem realizados e/ou contratados.	Documentação do Processo de definição do Nível de Acordo de Serviço.



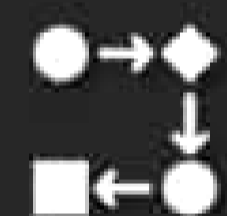
Painel



Estratégia



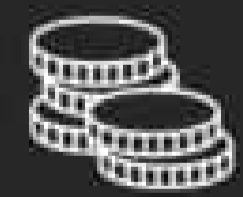
Pessoas



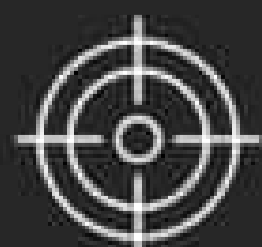
Processos



Tecnologia



Orçamento



Roadmap



SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

Segurança da Informação é um conjunto de processos e metodologias com o objetivo de proteger dados e informações relacionadas ao negócio, evitando que pessoas mal-intencionadas tenham acesso as informações não-públicas da empresa, seja por meio do acesso a dispositivos físicos como: computadores, sistemas, redes como a internet, ou qualquer outro meio em que a informação esteja armazenada (cartas, papéis, etc).

Este trabalho consistiu na análise, em alto nível, de alguns dos principais componentes (pilares) de um Sistema de Gestão da Segurança da Informação (SGSI), baseado nas normas ISO/IEC 27001 e 27002.

O Sistema de Gestão de Segurança da Informação (SGSI) é um sistema de gerenciamento documentado que consiste em um conjunto de controles de segurança que protegem a confidencialidade, disponibilidade e integridade da informação contra ameaças e vulnerabilidades.

A ISO/IEC 27001 é o padrão internacional que estabelece os detalhes e as melhores práticas para o SGSI de uma organização, enquanto a ISO/IEC 27002 traz um código de práticas com um conjunto completo de controles que auxiliam na aplicação do SGSI.



Painel



Estratégia



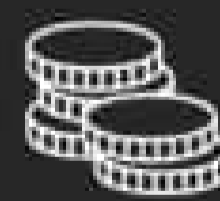
Pessoas



Processos



Tecnologia



Orçamento



Roadmap



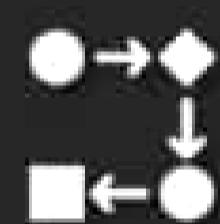
Painel



Estratégia



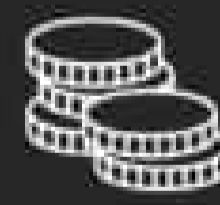
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

SEGURANÇA LÓGICA

Classificação da Informação

Criptografia de Dados

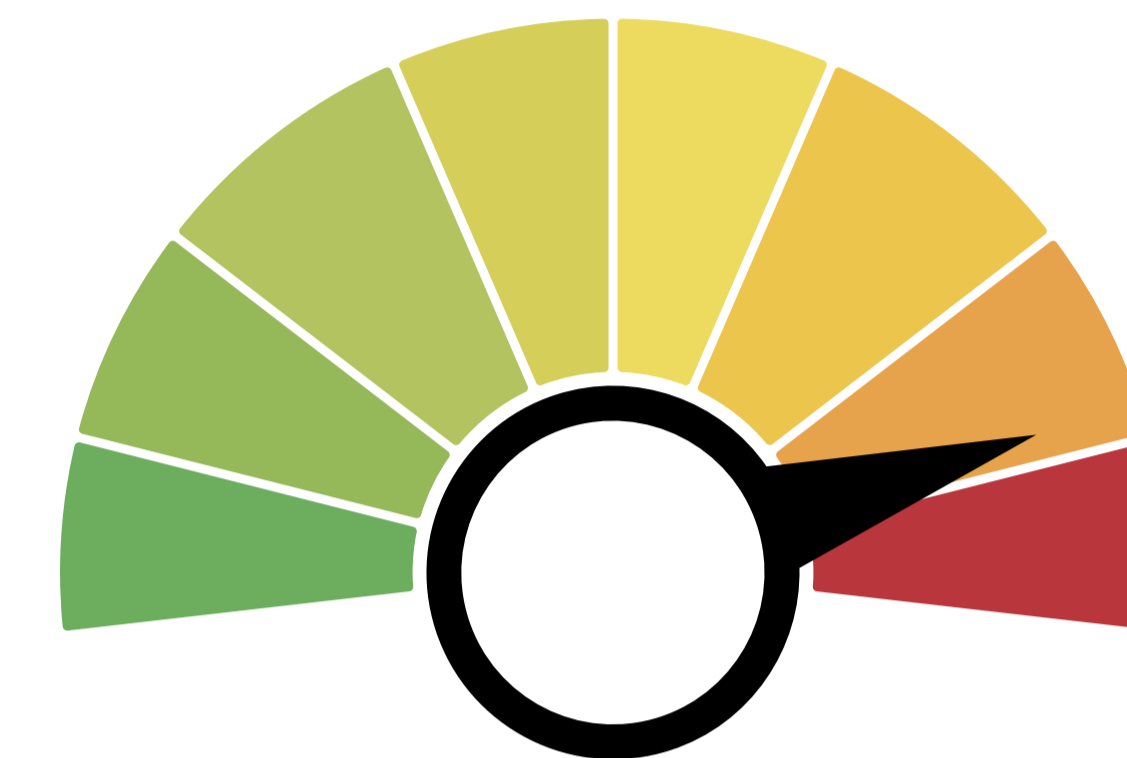
Gestão de Acesso pela Rede Cabeada

Licença de uso das soluções Anti-Malware do Firewall

Política de Backup

Servidor de Arquivos

Exposição ao Risco



Risco

Acesso indevido a informações que deveriam ser confidenciais ou restritas, por não estarem classificadas devidamente.

Análise As Is

Não foi identificado nenhum processo definido para classificação da informação do SGB.

Recomendação

Estabelecer, implementar e monitorar um processo para classificação da informação, a ser executado pelo(s) dono(s) da mesma.



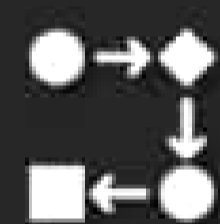
Painel



Estratégia



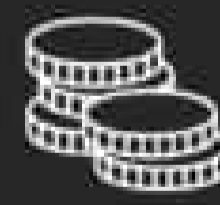
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

SEGURANÇA LÓGICA

Classificação da Informação

Criptografia de Dados

Gestão de Acesso pela Rede Cabeada

Licença de uso das soluções Anti-Malware do Firewall

Política de Backup

Servidor de Arquivos

Exposição ao Risco



Risco

Apesar do domínio exigir autenticação de usuário e senha para acesso às informações corporativas, há um elevado risco de roubo de informações e ataques maliciosos, vindo da rede interna, pela concessão de IP para dispositivos não autorizados. A partir do momento em que estão na rede interna, poderão realizar ataques direcionados, utilizando-se, por exemplo, da engenharia social para burlar outras camadas de proteção.

Análise As Is

Não há gestão de acesso/concessão de IP para os ativos que utilizam a rede cabeada. Ao conectar qualquer dispositivo à rede cabeada, o mesmo receberá um IP válido, independente do ativo ser ou não autorizado.

Recomendação

Estabelecer, implementar e monitorar um processo de gestão de ativos, impedindo que dispositivos não autorizados conectem-se à rede SGB.



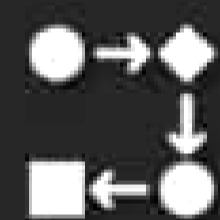
Painel



Estratégia



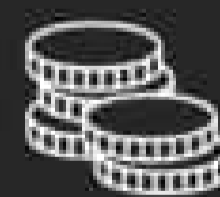
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

SEGURANÇA LÓGICA

Classificação da Informação

Criptografia de Dados

Gestão de Acesso pela Rede Cabeada

Licença de uso das soluções Anti-Malware do Firewall

Política de Backup

Servidor de Arquivos

Exposição ao Risco



Risco

Realizar rotinas de backup de forma empírica compromete sua eficiência, pois será necessário alocar mais espaço de armazenamento do que o realmente necessário para as cópias de dados.

Análise As Is

Não há uma política de backup definida. Apesar de existirem rotinas de backup com armazenamentos online e offline, não há uma política definindo premissas e responsabilidades, recorrência e como será armazenada a cópia de segurança.

Recomendação

Estabelecer, implementar e monitorar uma política de backup de dados.



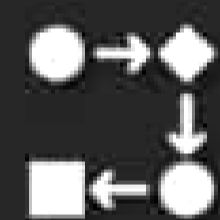
Painel



Estratégia



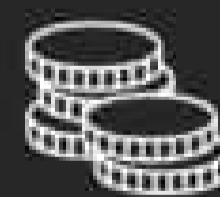
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

SEGURANÇA LÓGICA

Classificação da Informação

Criptografia de Dados

Gestão de Acesso pela Rede Cabeada

Licença de uso das soluções Anti-Malware do Firewall

Política de Backup

Servidor de Arquivos

Exposição ao Risco



Risco

Ao não se utilizar da criptografia de dados nos ativos, principalmente aqueles que são móveis (HDs externos, Laptops, Pendrives, etc), aumenta-se a exposição ao risco de roubo de informações confidenciais da organização, pois qualquer um que tenha acesso ao dispositivo, terá acesso à informação nele contida.

Análise As Is

A atual solução anti-malware utilizada pelo SGB não contempla a criptografia dos dados armazenados nos ativos. (Computadores, Pendrives, HDs externos, etc)

Recomendação

Utilizar solução anti-malware que contemple a criptografia das unidades de armazenamento ou solução específica de criptografia de dados.



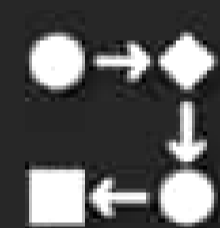
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

SEGURANÇA LÓGICA

Classificação da Informação

Criptografia de Dados

Gestão de Acesso pela Rede Cabeada

Licença de uso das soluções Anti-Malware do Firewall

Política de Backup

Servidor de Arquivos

Exposição ao Risco



Risco

Perda imediata das soluções de proteção contra malware na borda do perímetro, aumentando exponencialmente o risco de ataques cibernéticos.

Análise As Is

A licença de uso das soluções anti-malware do Firewall estão com data próxima de expiração e ainda não foram renovadas.

Recomendação

Renovar a licença das soluções anti-malware do firewall antes do seu vencimento.



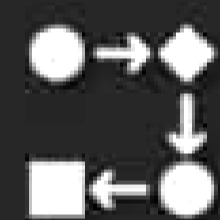
Painel



Estratégia



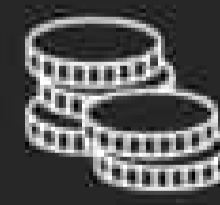
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

SEGURANÇA LÓGICA

Classificação da Informação

Criptografia de Dados

Gestão de Acesso pela Rede Cabeada

Licença de uso das soluções Anti-Malware do Firewall

Política de Backup

Servidor de Arquivos

Exposição ao Risco



Risco

Perda de arquivos por não haver backup e vulnerabilidade para ataques malwares.

Análise As Is

Existem servidores de arquivos instalados nas áreas sem o conhecimento da TI e fora dos padrões de segurança e backup.

Recomendação

Identificar, através de protocolo de compartilhamento de arquivos, máquinas instaladas como servidores de arquivos sem o conhecimento da TI e adequar aos padrões existentes.



Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

SEGURANÇA FÍSICA

Acesso à sala de CFTV

Acesso Físico nas Unidades Regionais

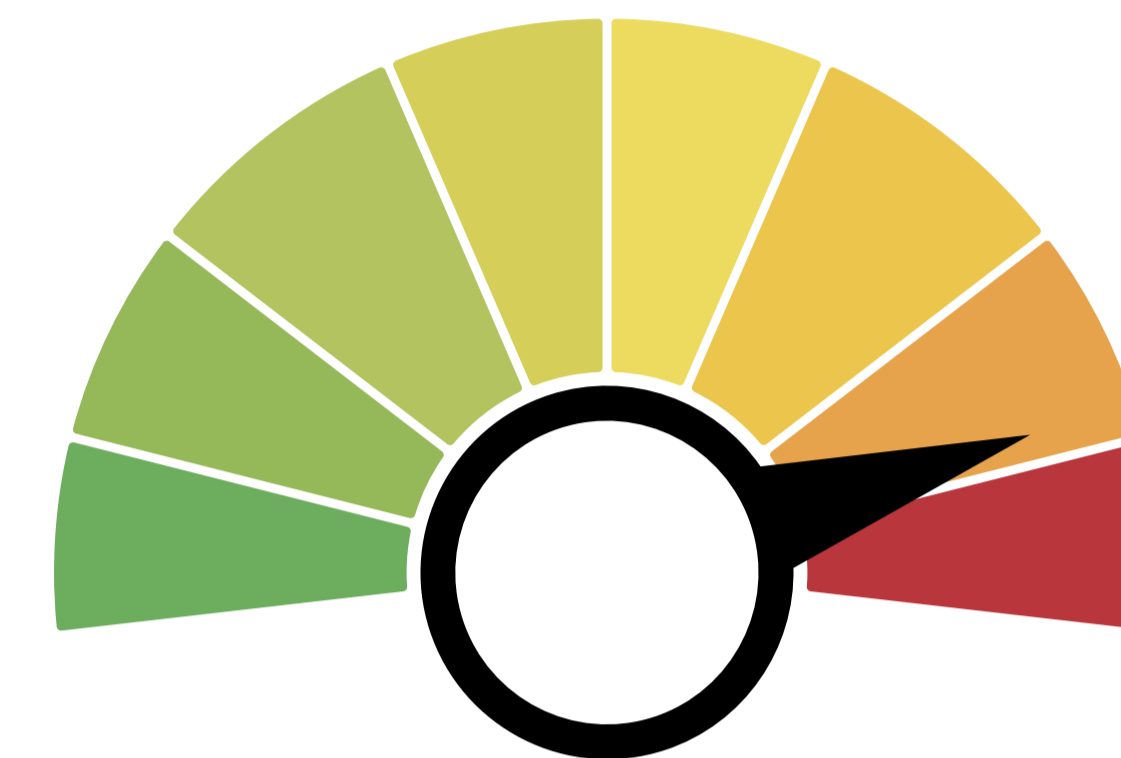
Ausência de Câmeras em salas restritas

Catracas de Acesso

Chave do Datacenter de Backup

Datacenter de Backup

Exposição ao Risco



Risco

Entrada de qualquer pessoa na sala de controle CFTV, podendo ocasionar perda de informações de registro das imagens acidentalmente ou intencionalmente.

Análise As Is

Não há controle de acesso físico na sala de CFTV.

Recomendação

Solicitar ao departamento responsável pela administração de controle de acesso a implementação de um controle de acesso físico na sala onde ficam armazenados os equipamentos/gravações das imagens do circuito interno de TV (CFTV).



Painel



Estratégia



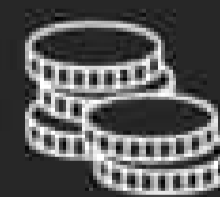
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

SEGURANÇA FÍSICA

Acesso à sala de CFTV

Acesso Físico nas Unidades Regionais

Ausência de Câmeras em salas restritas

Catracas de Acesso

Chave do Datacenter de Backup

Datacenter de Backup

Exposição ao Risco



Risco

Ações realizadas dentro das salas não poderão ser auditadas.

Análise As Is

As salas restritas da TI (Datacenter de produção e Datacenter de Backup) não possuem câmeras de monitoramento na parte interna.

Recomendação

Solicitar ao departamento responsável pela administração do circuito interno de TV (CFTV) a instalação de câmeras de segurança no interior das salas de equipamentos da TI com acesso restrito.



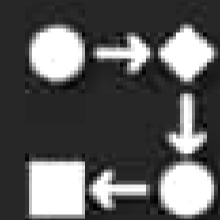
Painel



Estratégia



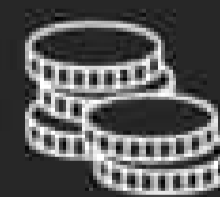
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

SEGURANÇA FÍSICA

Acesso à sala de CFTV

Acesso Físico nas Unidades Regionais

Ausência de Câmeras em salas restritas

Catracas de Acesso

Chave do Datacenter de Backup

Datacenter de Backup

Exposição ao Risco



Risco

Acesso indevido à sala do Datacenter de Backup por pessoas não autorizadas. Mesmo a entrega da chave sendo realizada apenas para uma lista de pessoas, há o risco de, através da engenharia social, esta chave ser entregue para alguém fora dessa lista.

Análise As Is

Apesar de possuir controle de acesso biométrico, a sala pode ser aberta por uma chave que fica armazenada na portaria e pode ser entregue para uma lista de pessoas.

Recomendação

Solicitar ao departamento responsável pelo controle de acesso ao prédio, a regularização do funcionamento do acesso biométrico ao datacenter de backup e inutilizar o acesso via chave.



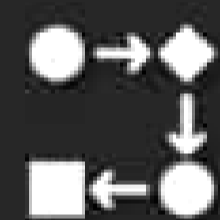
Painel



Estratégia



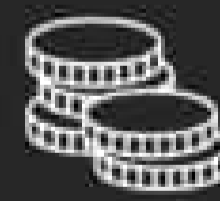
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

SEGURANÇA FÍSICA

Acesso à sala de CFTV

Acesso Físico nas Unidades Regionais

Ausência de Câmeras em salas restritas

Catracas de Acesso

Chave do Datacenter de Backup

Datacenter de Backup

Exposição ao Risco



Risco

Acesso de pessoas não autorizadas às dependências das unidades regionais, assim como às salas de acesso restrito à TI, podendo ocasionar roubo de informações e/ou ataques maliciosos.

Análise As Is

Não há controle de acesso físico nas unidades regionais.

Recomendação

Solicitar ao departamento responsável pelo acesso de pessoas em cada unidade regional a implementação de um controle de acesso físico, dando ênfase em salas que possuam equipamentos de TI.



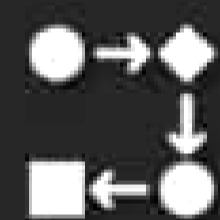
Painel



Estratégia



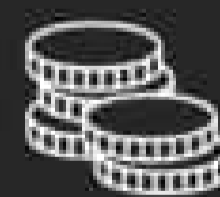
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

SEGURANÇA FÍSICA

Acesso à sala de CFTV

Acesso Físico nas Unidades Regionais

Ausência de Câmeras em salas restritas

Catracas de Acesso

Chave do Datacenter de Backup

Datacenter de Backup

Exposição ao Risco



Risco

Perda da eficiência do controle de acesso, não registrando acesso de pessoas ao local com horário de entrada e/ou saída, além da possibilidade de acesso de pessoas não autorizadas na ausência temporária de um funcionário no local.

Análise As Is

As catracas de acesso ao prédio não estão ativas, possibilitando o acesso e saída sem crítica sistêmica.

Recomendação

Solicitar ao departamento responsável pelo controle de acesso ao prédio a ativação da catraca de acesso para permitir a entrada/saída da unidade apenas para pessoas autorizadas, registrando data e hora dos eventos.



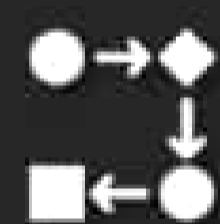
Painel



Estratégia



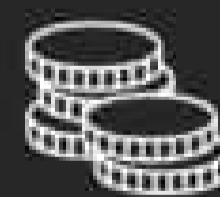
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

SEGURANÇA FÍSICA

Acesso à sala de CFTV

Acesso Físico nas Unidades Regionais

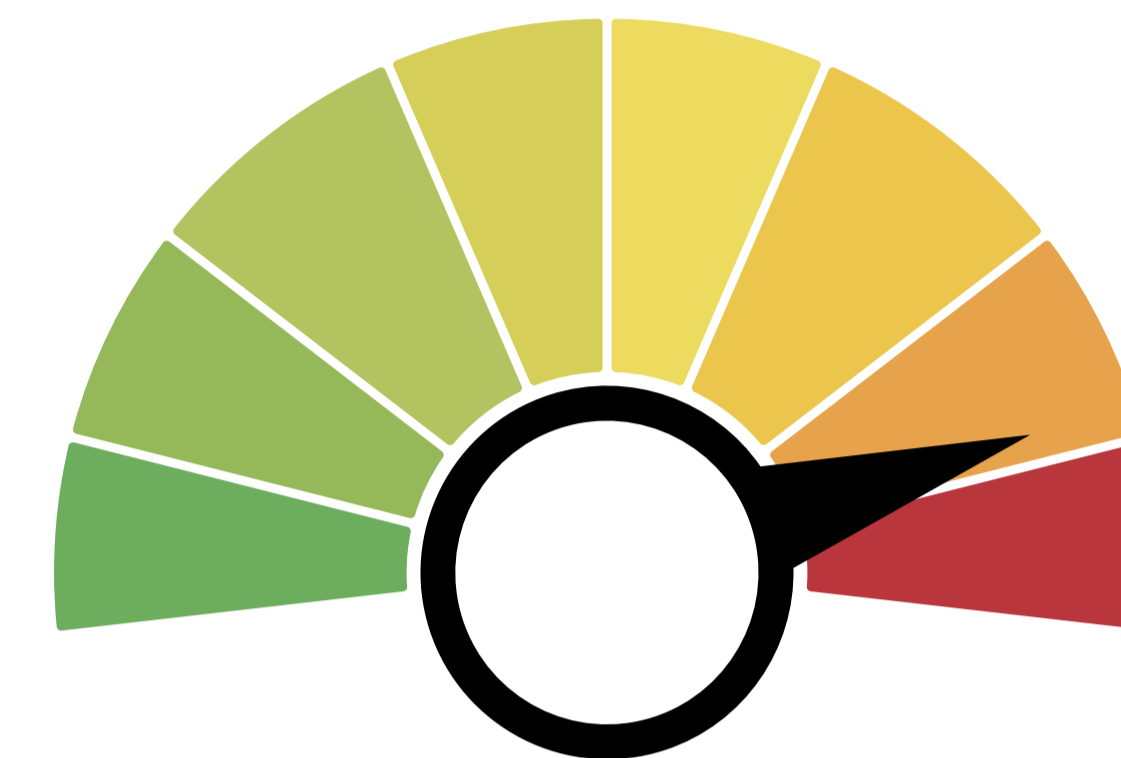
Ausência de Câmeras em salas restritas

Catracas de Acesso

Chave do Datacenter de Backup

Datacenter de Backup

Exposição ao Risco



Risco

Atos de vandalismo, com facilidade de quebrar o vidro e lançar substâncias que podem causar incêndios dentro da sala.

Análise As Is

A sala do Datacenter de Backup possui uma janela de vidro para a via pública.

Recomendação

Solicitar ao departamento responsável pela infraestrutura predial vedar a janela com madeira, metal ou alvenaria para mitigar o risco de atos de vandalismo na sala do datacenter de backup.



Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

SEGURANÇA ORGANIZACIONAL

Plano de Continuidade de Negócio

Plano de Recuperação de Desastres

Treinamentos em SI

Exposição ao Risco



Risco

A ausência de um Plano de Continuidade de Negócio corporativo expõe a organização à riscos de interrupção de seus serviços em caso de desastres ou falha crítica.

Análise As Is

Não há Plano de Continuidade de Negócio corporativo definido.

Recomendação

Solicitar à área de Governança Corporativa a elaboração de um Plano de Continuidade do Negócio, apontando processos críticos e tempo de resposta da TI necessário para restabelecimento destes processos em caso de incidentes.



Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

SEGURANÇA ORGANIZACIONAL

Plano de Continuidade de Negócio

Plano de Recuperação de Desastres

Treinamentos em SI

Exposição ao Risco



Risco

Pessoas mais vulneráveis a ataques através da engenharia social.

Análise As Is

Há treinamentos anuais, em parceria com a RNP, que abordam temas relacionados à Segurança da Informação, porém possuem baixa adesão.

Recomendação

Buscar patrocínio da alta gestão e maior adesão do público aos treinamentos relacionados à Segurança da Informação.



Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

SEGURANÇA ORGANIZACIONAL

Plano de Continuidade de Negócio

Plano de Recuperação de Desastres

Treinamentos em SI

Exposição ao Risco



Risco

Incapacidade de restaurar os serviços comprometidos de forma priorizada, organizada e de acordo com os direcionadores das áreas de negócio.

Análise As Is

Não há Plano de Recuperação de Desastres definido.

Recomendação

Solicitar à área de Governança Corporativa a elaboração de um Plano de Recuperação de Desastres, apontando processos críticos e tempo de resposta da TI necessário para restabelecimento destes processos em caso de incidentes.



Painel



Estratégia



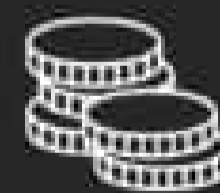
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

POLÍTICAS

Penalidades Previstas

Senhas de Administração

Validação da Política de SI

Exposição ao Risco



Risco

Baixa adesão às normas da Política pela indefinição de quais penalidades serão aplicadas em caso de descumprimento.

Análise As Is

O capítulo VI da Política de Segurança da Informação, que versa sobre as penalidades previstas para o descumprimento da política, está redigido de forma genérica, não especificando quais as reais penalidades serão aplicadas para os casos de descumprimento.

Recomendação

Especificar detalhadamente quais as penalidades serão aplicadas para cada tipo de descumprimento.



Painel



Estratégia



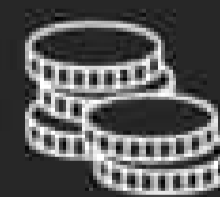
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

POLÍTICAS

Penalidades Previstas

Senhas de Administração

Validação da Política de SI

Exposição ao Risco



Risco

Não ter uma Política de SI em vigor expõe a organização à riscos relacionadoa a falta de padronização/comportamento de seus usuários.

Análise As Is

A Política de Segurança da Informação criada para o SGB está aguardando aprovação pela área de Governança Corporativa e ainda não foi implementada.

Recomendação

Solicitar à Governança Corporativa a aprovação, divulgação e implementação da Política de Segurança da Informação, que deverá ser revisada na periodicidade definida pelo SGB.



Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SEGURANÇA DA INFORMAÇÃO

Segurança Lógica

Segurança Física

Segurança Organizacional

Políticas

POLÍTICAS

Penalidades Previstas

Senhas de Administração

Validação da Política de SI

Exposição ao Risco



Risco

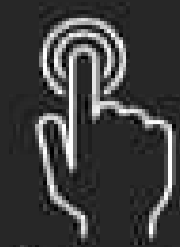
Risco de comprometimento da confidencialidade da senha com privilégios de Administrador, podendo acarretar em acessos indevidos à ativos da organização.

Análise As Is

O artigo 37 da Política de Segurança da Informação versa que a senha de administração deverá ser compartilhada com o corpo técnico e com terceiros que realizam suporte técnico.

Recomendação

Não compartilhar senhas. Definir senhas individuais de administrador para os usuários necessários.



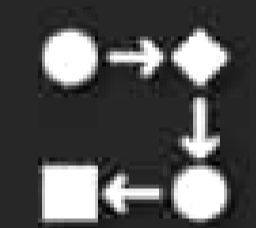
Painel



Estratégia



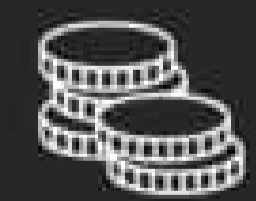
Pessoas



Processos



Tecnologia



Orçamento



Roadmap





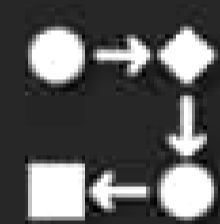
Painel



Estratégia



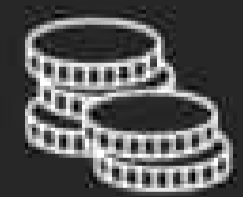
Pessoas



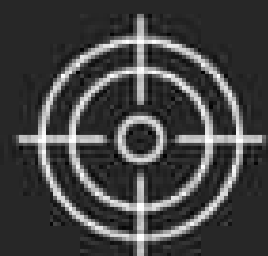
Processos



Tecnologia



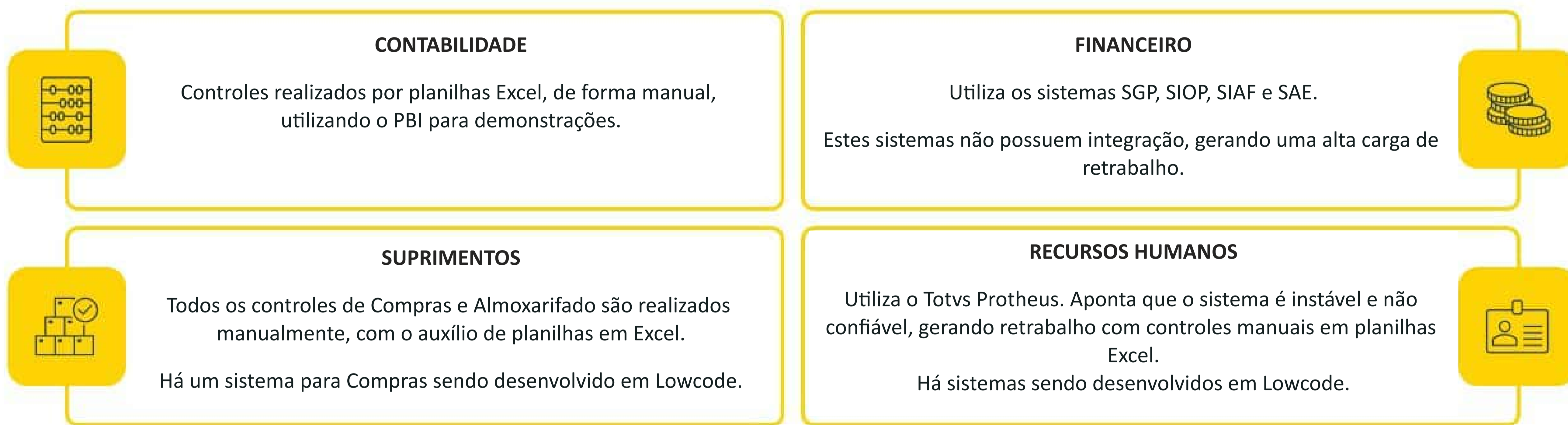
Orçamento



Roadmap

ERP - COMO ALGUMAS FUNCIONALIDADES DE BACKOFFICE SÃO EXECUTADAS NO SGB

No cenário atual do SGB, as funcionalidades comuns de um ERP são executadas com o auxílio de diferentes sistemas não integrados e manualmente através de planilhas em Excel e outras ferramentas. O quadro abaixo relaciona os processos e sua operacionalização.



Principais desvantagens da utilização do modelo atual:



INEFICIÊNCIA OPERACIONAL



RISCO ELEVADO DE FALHAS CAUSADAS POR INTERAÇÃO HUMANA



MAIOR VULNERABILIDADE A ATAQUES CIBERNÉTICOS



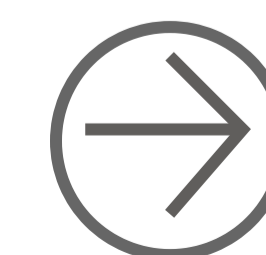
ALTO ÍNDICE DE CONTROLES DE APOIO MANUAIS



GRANDE QUANTIDADE DE SISTEMAS NÃO INTEGRADOS E BASES DE DADOS DESCENTRALIZADAS



ALTA COMPLEXIDADE PARA SUSTENTAÇÃO DOS SISTEMAS





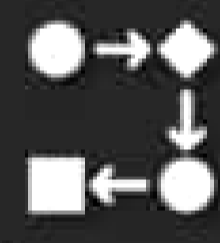
Painel



Estratégia



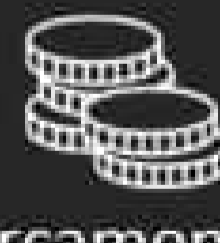
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ERP - PLANEJAMENTO DE RECURSOS EMPRESARIAIS



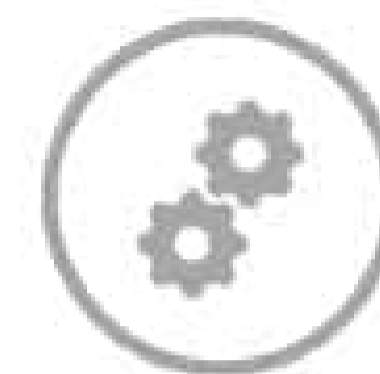
A maneira mais simples de definir ERP é relacioná-lo aos processos empresariais necessários na administração das empresas (finanças, RH, produção, cadeia de suprimentos, serviços, procurement e etc).

Em seu nível mais básico, o ERP ajuda a gerenciar eficientemente todos esses processos em um **sistema integrado**.



Oferece automação, integração e inteligência essenciais para a execução eficiente das operações comerciais diárias.

Como sistema centralizador das informações mais importantes das companhias e única fonte de dados, promove confiabilidade aos dados e mitiga erros causados por falha humana.



O sistema é composto por módulos integrados ou aplicativos empresariais que se comunicam entre si e compartilham um banco de dados comum.

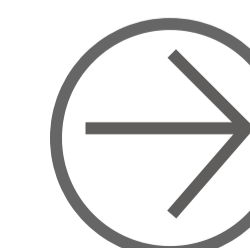
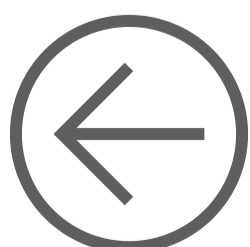
Usualmente, cada módulo ERP se concentra em uma área empresarial, mas eles trabalham juntos usando os mesmos dados para atender às necessidades da empresa.

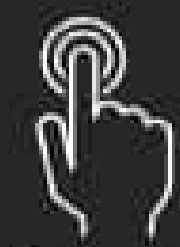


Um ERP oferece diversas vantagens, como por exemplo: Maior produtividade, rapidez na emissão de relatórios, menos riscos, TI simplificada e agilidade aumentada.

FATORES CRÍTICOS DE SUCESSO

- ▶ Patrocínio da Alta Gestão;
- ▶ Gestão da Mudança Cultural;
- ▶ Alta Disponibilidades dos usuários chave durante a execução do projeto;
- ▶ Treinamento adequado aos usuários;
- ▶ Mapeamento da cadeia de valor dos processos de negócio;
- ▶ Escopo adequado às necessidades do Negócio.





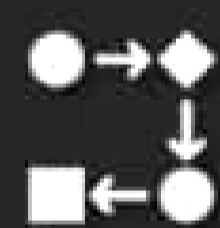
Painel



Estratégia



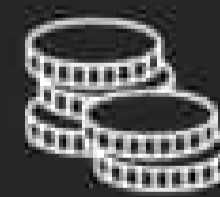
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ERP - HABILITA A EMPRESA PARA UM ROADMAP DE CRESCIMENTO E TRANSFORMAÇÃO DIGITAL

A implementação de um ERP não é uma necessidade apenas para suportar uma operação e assegurar o compliance dos processos, o **ERP habilita o crescimento** organizado de uma empresa, dá **visibilidade e consistência as informações** para a alta gestão, **facilita e aumenta a segurança** em processos de M&A, melhora a **experiência dos colaboradores e clientes**.



- ▶ Integridade e padronização das informações
- ▶ Transparência das informações para toda a organização
- ▶ Segregação de acessos e monitoramento de transações
- ▶ Melhora na tomada de decisões e Aumento de Compliance



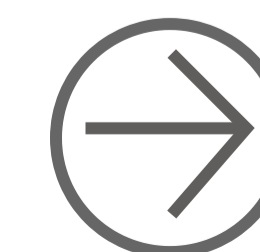
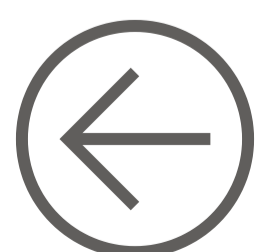
- ▶ Melhor interface com o usuário
- ▶ Redução de problemas sistêmicos
- ▶ Engajamento colaborativo
- ▶ Melhora na Experiência dos funcionários e dos clientes



- ▶ Padronização de Processos
- ▶ Alavancagem de melhores práticas de mercado
- ▶ Relatórios operacionais em tempo real
- ▶ Análises preditivas
- ▶ Aumento de Produtividade

- ▶ Integridade e visibilidade dos dados
- ▶ Jornada de funcionários, clientes e ecossistema
- ▶ Solução robusta e escalável

- ▶ Decisões melhores e mais rápidas
- ▶ Melhor experiência aos clientes
- ▶ Crescimento orgânico e M&A





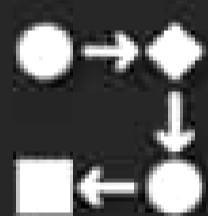
Painel



Estratégia



Pessoas



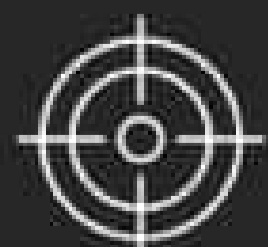
Processos



Tecnologia



Orçamento



Roadmap

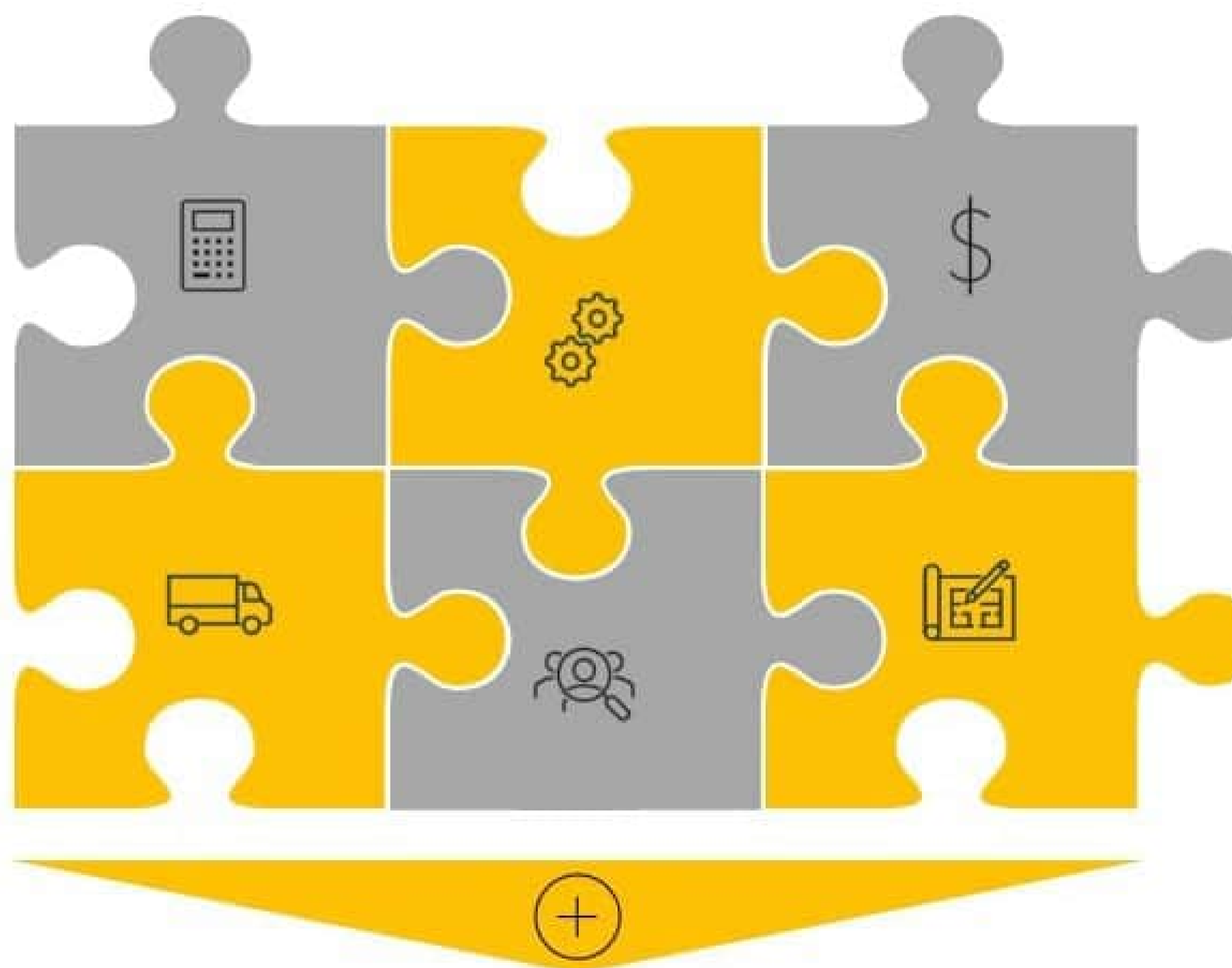
ERP - MÓDULOS COMUNS

O sistema ERP possui diferentes módulos integrados para atender as diferentes necessidades das áreas de negócio. Cada módulo suporta processos específicos, como finanças, procurement ou produção, e fornece aos usuários dos departamentos as transações necessárias para execução de suas atividades. Cada módulo se conecta ao **ERP**, o que gera uma única fonte de dados precisos e compartilhados entre os departamentos.

Finanças: O módulo de finanças e contabilidade é o núcleo de um sistema ERP. Gerencia o Razão, automatiza as principais tarefas financeiras, ajuda no rastreamento de contas a pagar e a receber, no fechamento eficiente dos livros, na geração de relatórios financeiros, no cumprimento de padrões de reconhecimento de receitas, na mitigação de riscos financeiros e etc.

Gestão de recursos humanos: Grande parte dos sistemas ERP inclui um módulo de RH que fornece recursos essenciais, como pontualidade, presença e folha de pagamento.

Sourcing e procurement: Centraliza e automatiza o processo de compras, incluindo solicitações de cotações, criação de contratos e aprovações.

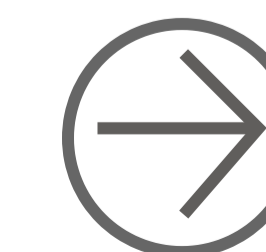
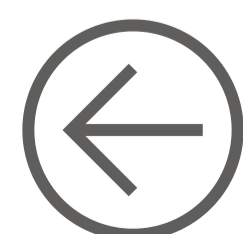


Logística e gestão da cadeia de suprimentos: Rastreia a movimentação de mercadorias e suprimentos em toda a cadeia de suprimentos da organização. O módulo fornece ferramentas para gestão de estoques em tempo real, operações de armazenamento, transporte e logística e pode aumentar a visibilidade e a resiliência da cadeia de suprimentos.

Serviço: Ajuda empresas a fornecer serviço confiável e personalizado. Pode incluir ferramentas para consertos internos, peças de reposição, gestão de serviços externos e fluxos de receita baseados em serviços.

P&D e engenharia: Fornece ferramentas para design e desenvolvimento de produtos, gestão do ciclo de vida do produto (PLM), compliance do produto e etc.

Os módulos do ERP destacados acima possuem suas funções realizadas por sistemas ou processos manuais no SGB. Vale ressaltar que o ERP é modular e a definição dos componentes necessários deverá ser alinhada às necessidades das áreas de negócio.





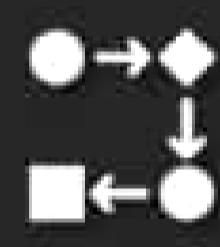
Painel



Estratégia



Pessoas



Processos



Tecnologia



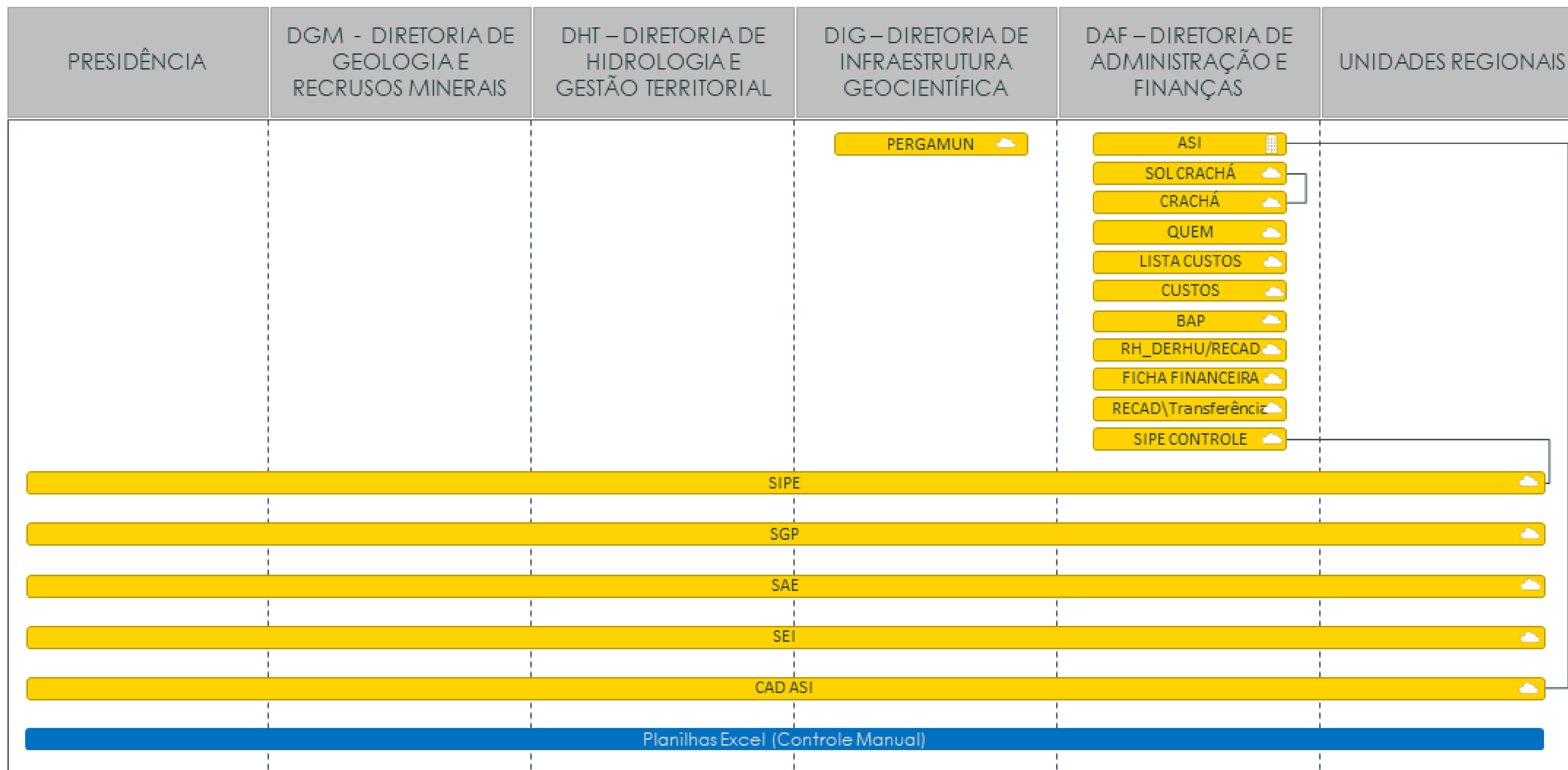
Orçamento



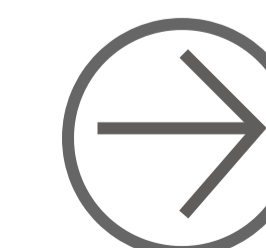
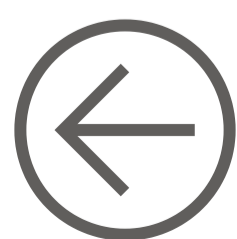
Roadmap

ERP - COMO AS FUNCIONALIDADES COMUNS SÃO EXECUTADAS NO SGB

O mapa abaixo apresenta os sistemas que poderão ser descontinuados após a implementação do ERP, pois suas funcionalidades estarão contidas, de forma integrada, dentro da nova solução.



LEGENDA: Sistemas em utilização Controles Manuais 🏢 On Premise (DC Interno) 📄 Colocation 🗣 SaaS ☁ Cloud





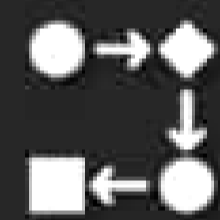
Painel



Estratégia



Pessoas



Processos



Tecnologia



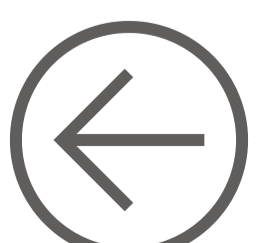
Orçamento



Roadmap

ERP - VANTAGENS

A utilização de um bom sistema ERP proporciona uma série de vantagens, que podem variar de acordo com o modelo de implantação da solução. Diante disso, a relação abaixo contempla os benefícios principais e comuns das soluções ERP modernas.





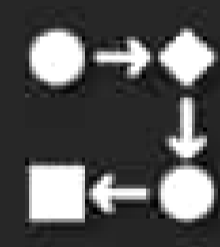
Painel



Estratégia



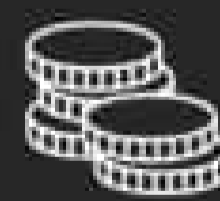
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

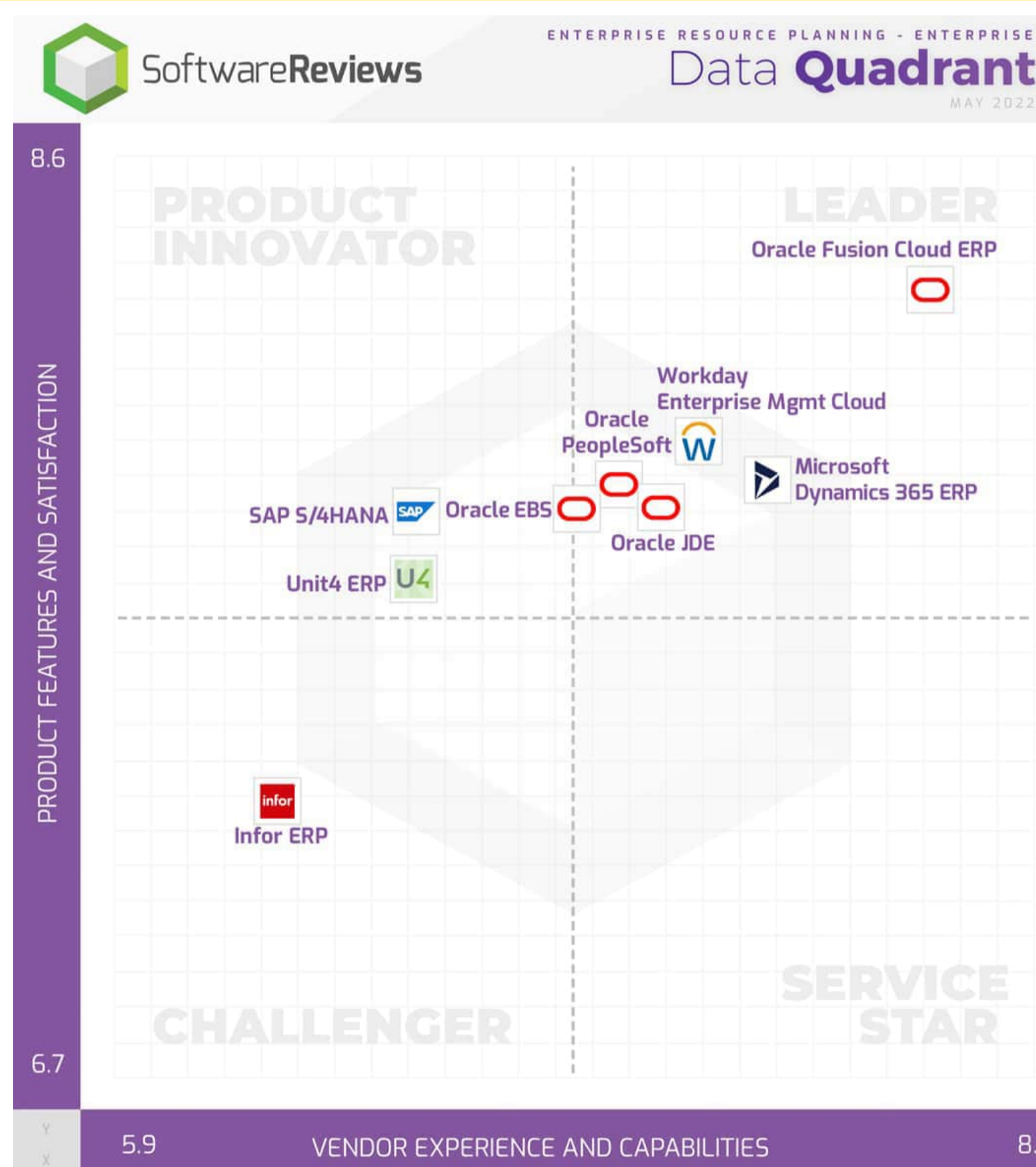
ERP - MELHORES FERRAMENTAS ERP NA VISÃO DO MERCADO EM 2022

Sob a ótica de boas práticas, consultamos relatórios de mercado que avaliam as soluções mais utilizadas pelas empresas em relação a sua posição competitiva. Abaixo são demonstrados os quadrantes: **Gartner**, **SoftwareReviews** e **IDC**. Estes indicam o resultado da avaliação, em 2022, das melhores ferramentas de mercado para ERP e suas posições no ranking. Entretanto, no âmbito federal a ferramenta de ERP SUAP (desenvolvida pela Universidade Federal do Rio Grande do Norte) é amplamente utilizada pelas instituições e sugere-se que seja avaliada a aderência técnica e funcional do mesmo de acordo com as necessidades do SGB.

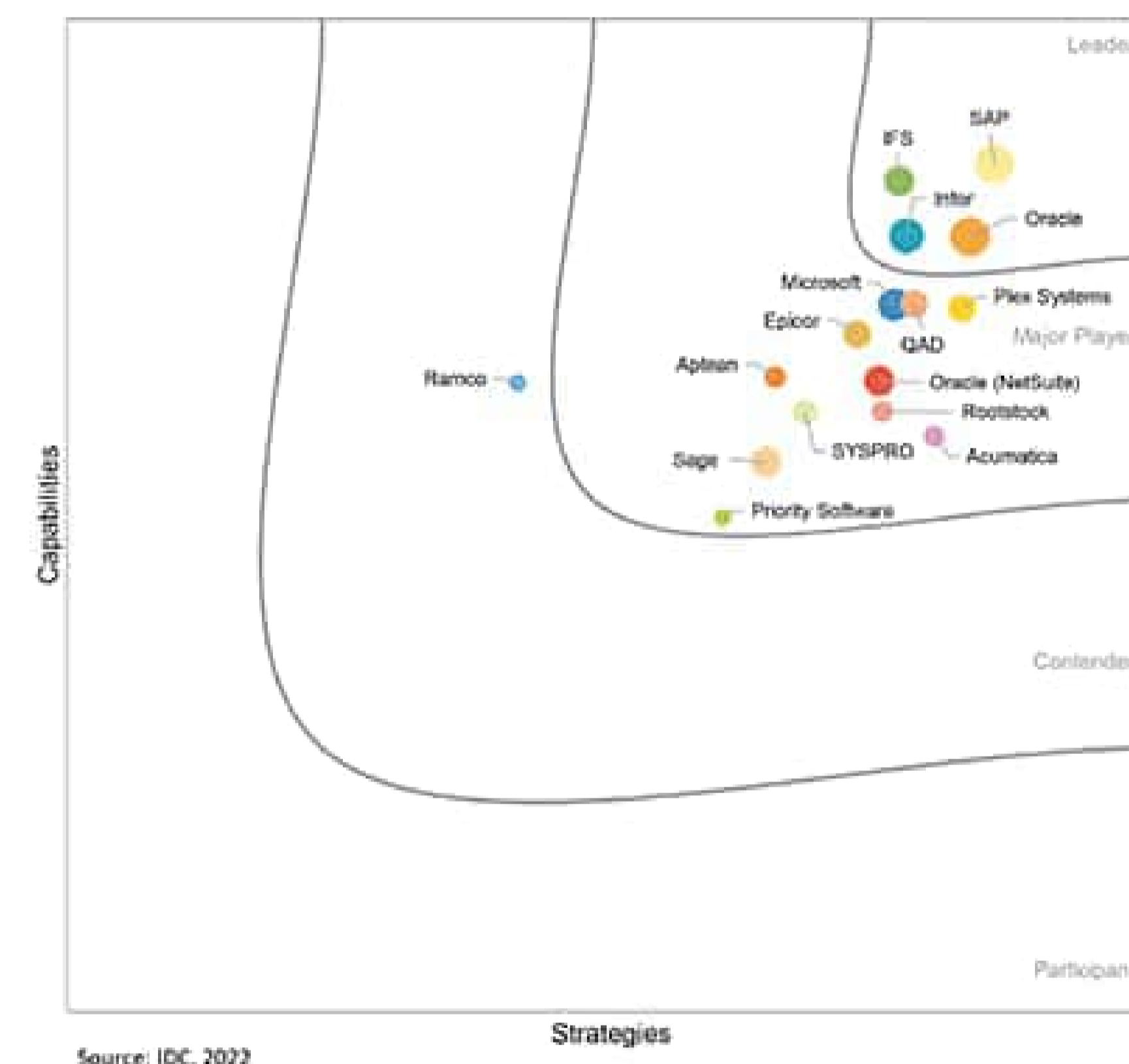
GARTNER



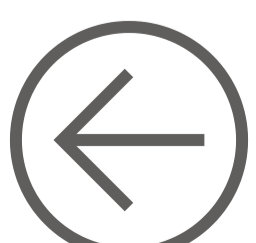
SOFTWARE REVIEWS



IDC



Com isso, recomenda-se a realização de estudo para escolha de ERP adequado às necessidades do SGB, de acordo com os requisitos de negócio, levando-se em conta a regulamentação para compra/desenvolvimento de softwares para uso em organizações vinculadas ao governo federal.





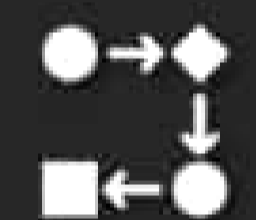
Painel



Estratégia



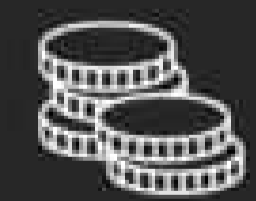
Pessoas



Processos



Tecnologia



Orçamento



Roadmap





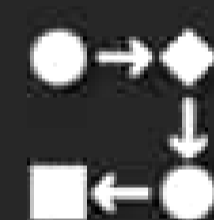
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

SISTEMAS - UNIVERSO DE ANÁLISE

Status das Aplicações



Sistemas que não estão em produção

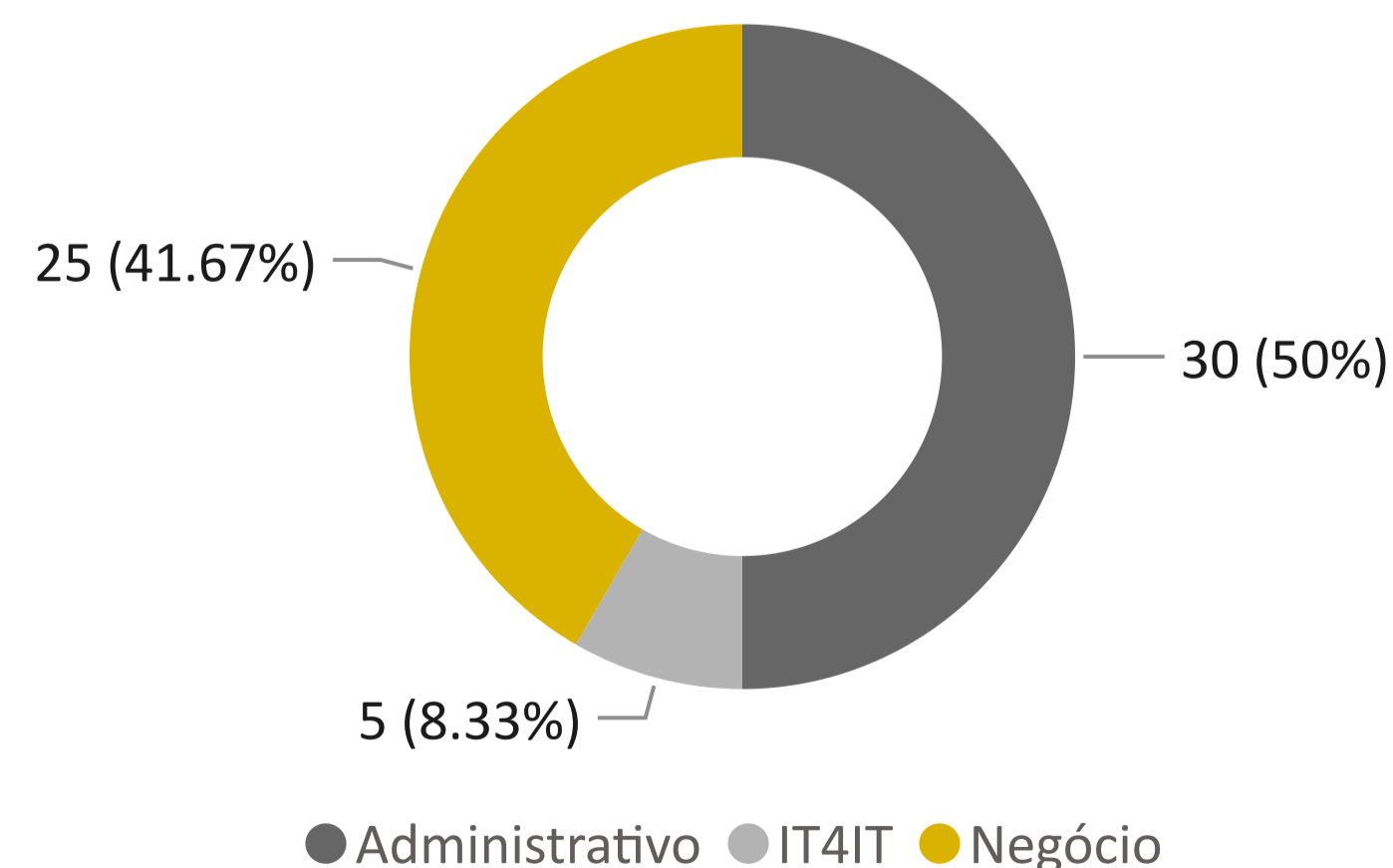
Sigla	Nome	Status
AGERENCIAL	Acompanhamento Gerencial	Consulta
Integrador de Mapas e Projetos	Fluxo de entrada de dados (Rigeo/GeoSGB/integrador)	Descontinuado
SCDI	Sistema de Controle de Incidentes Naturais	Descontinuado
AGUAMIN	Sistema de Análise de Águas Minerais	Descontinuado
PALEO	Sistema de Bases de Dados Paleontológicos	Descontinuado
SISMOLOGIA	Sismologia - DGM - SEISCOMP	Homologação
LIFERAY	Sistema de gerenciamento de conteúdo web	Homologação

O gráfico provê a visão geral das aplicações existentes no SGB quanto a sua utilização. O universo desta análise abrange as aplicações que estão sendo utilizadas, as que estão sendo homologadas e aquelas que são utilizadas como consulta.

Não faz parte desta análise as aplicações descontinuadas.

CLASSIFICAÇÃO DOS SISTEMAS

Classificação dos Sistemas



Negócio

Aplicações core, diretamente relacionadas ao negócio praticado pela CPRM

Administrativo

Aplicações utilizadas pelas áreas de negócio para realização das atividades administrativas

IT4IT

Aplicações da TI, diretamente relacionadas aos processos da TI

O gráfico acima exibe a quantidade de sistemas existentes no SGB, de acordo com a classificação adotada, assim como seus respectivos percentuais. Seu resultado é aritmético onde cada aplicação possui o mesmo peso nessa análise.



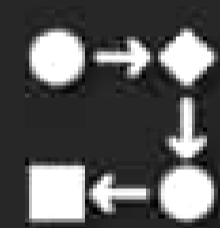
Painel



Estratégia



Pessoas



Processos



Tecnologia

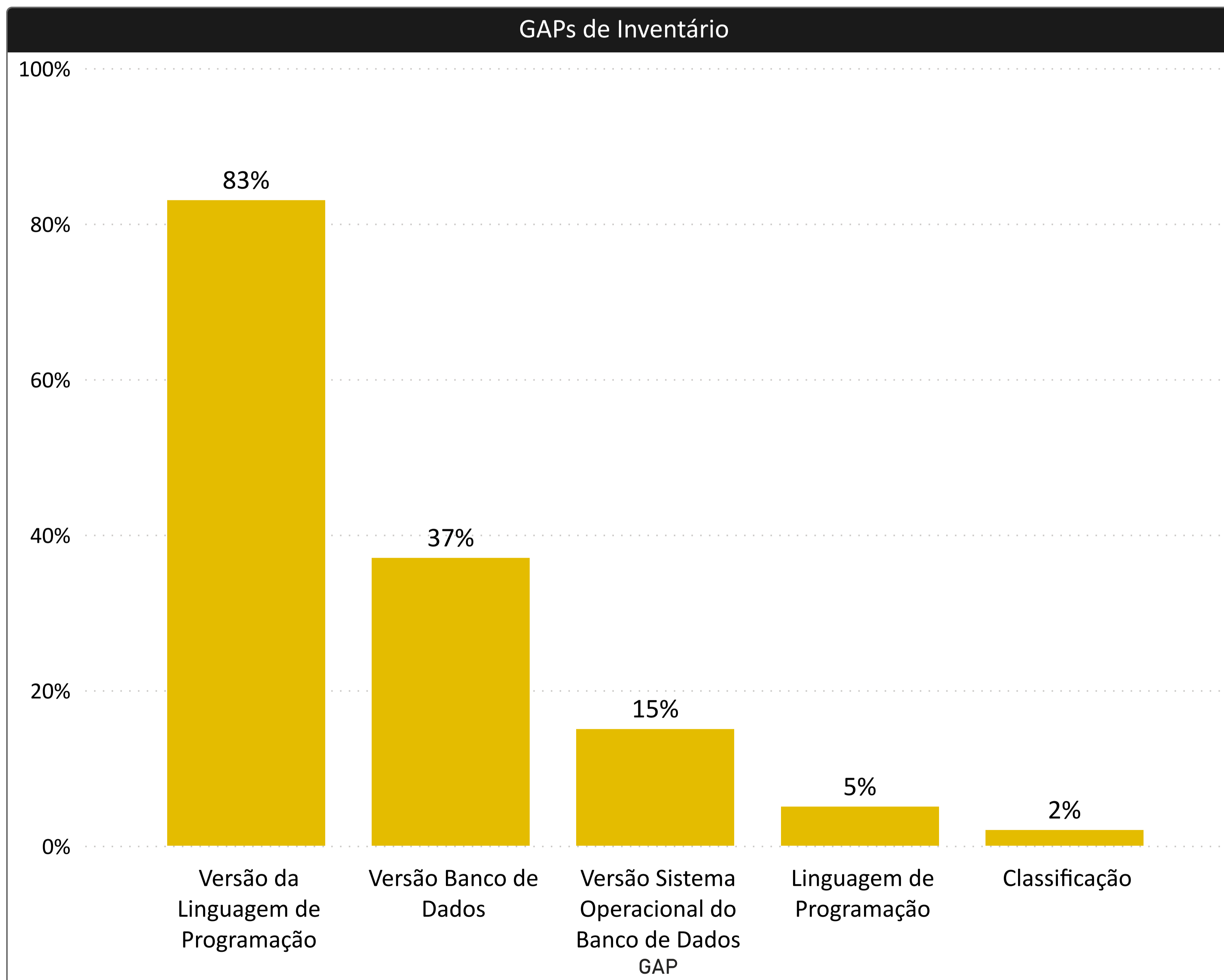


Orçamento



Roadmap

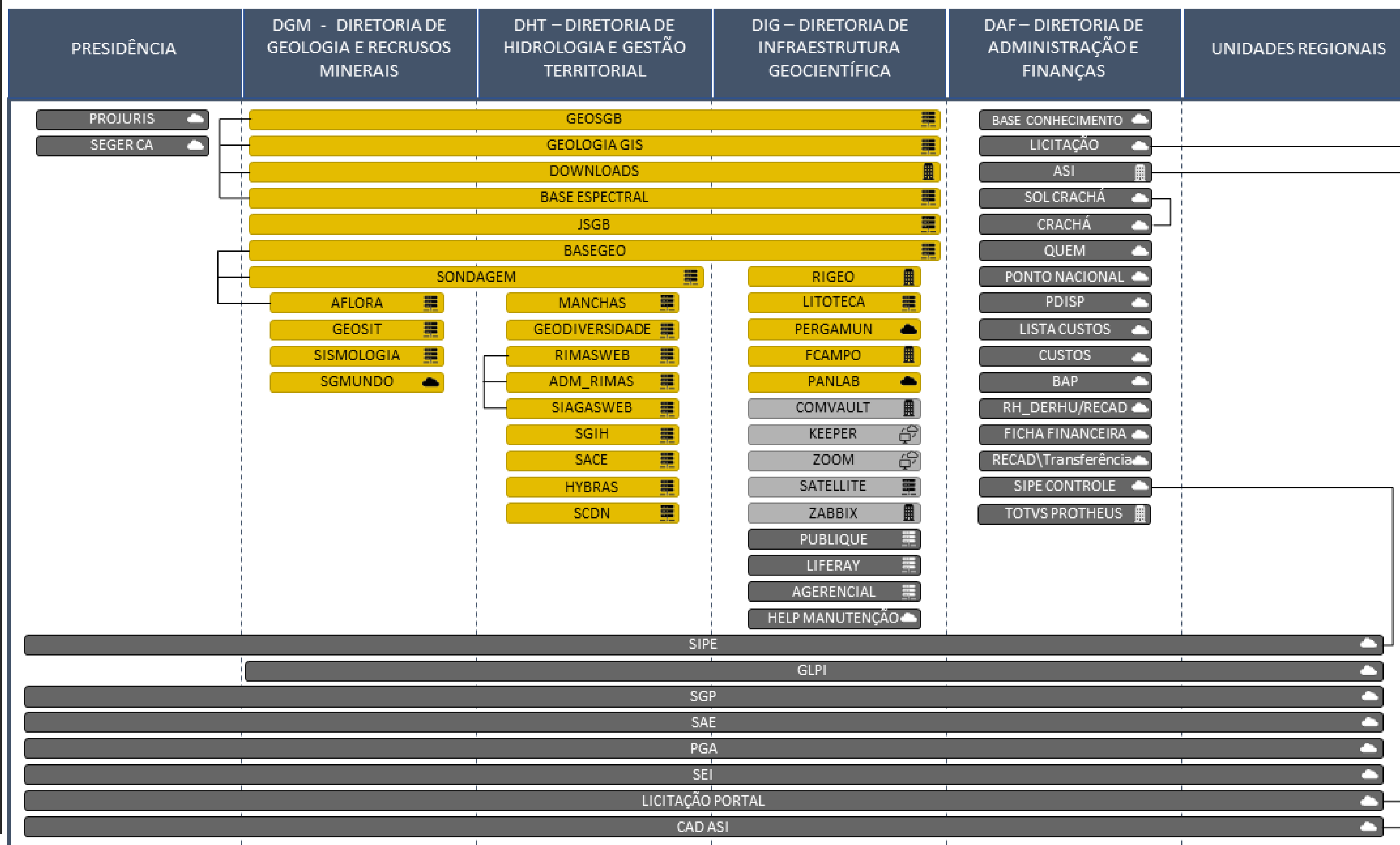
GAPS DE INVENTÁRIO



O inventário de aplicações não foi integralmente preenchido, pois o SGB não possui documentos atualizados e estruturados que relacionem as informações para elaboração correta do mesmo. Desta forma, as análises foram realizadas com base nos dados disponíveis e foi apontado o percentual de itens **Não Informados** por categoria do estudo.

O gráfico ao lado exibe o percentual de dados não informados em cada uma das categorias analisadas, assim como a relação dos sistemas que tiveram seus dados não informados ou incompletos.

MAPA DE SISTEMAS ATUAL



Os sistemas utilizados no SGB são exibidos na figura ao lado e agrupados em:

- 1) Negócio
- 2) Administrativo
- 3) IT4IT

Os sistemas da categoria Negócio estão organizados de acordo com as diretorias existentes atualmente no SGB.

LEGENDA

Negócio
 Administrativo
 IT4IT
 ☁ On.Primise (DC Interno)
 ☁ Colocation
 ☁ SaaS
 ☁ Cloud
 — Integração Sistêmica

Visão Geral dos Sistemas

GAPS de Inventário

Mapa de Sistemas Atual

Aderência Funcional



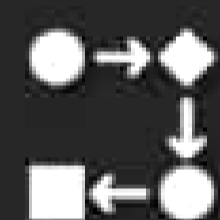
Painel



Estratégia



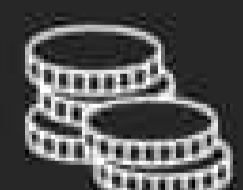
Pessoas



Processos



Tecnologia

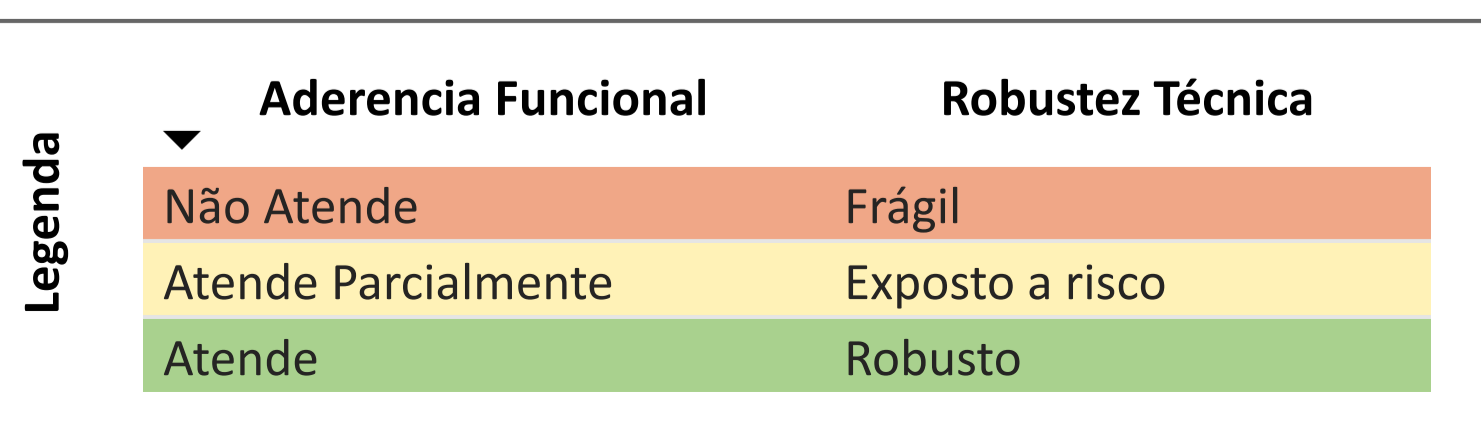
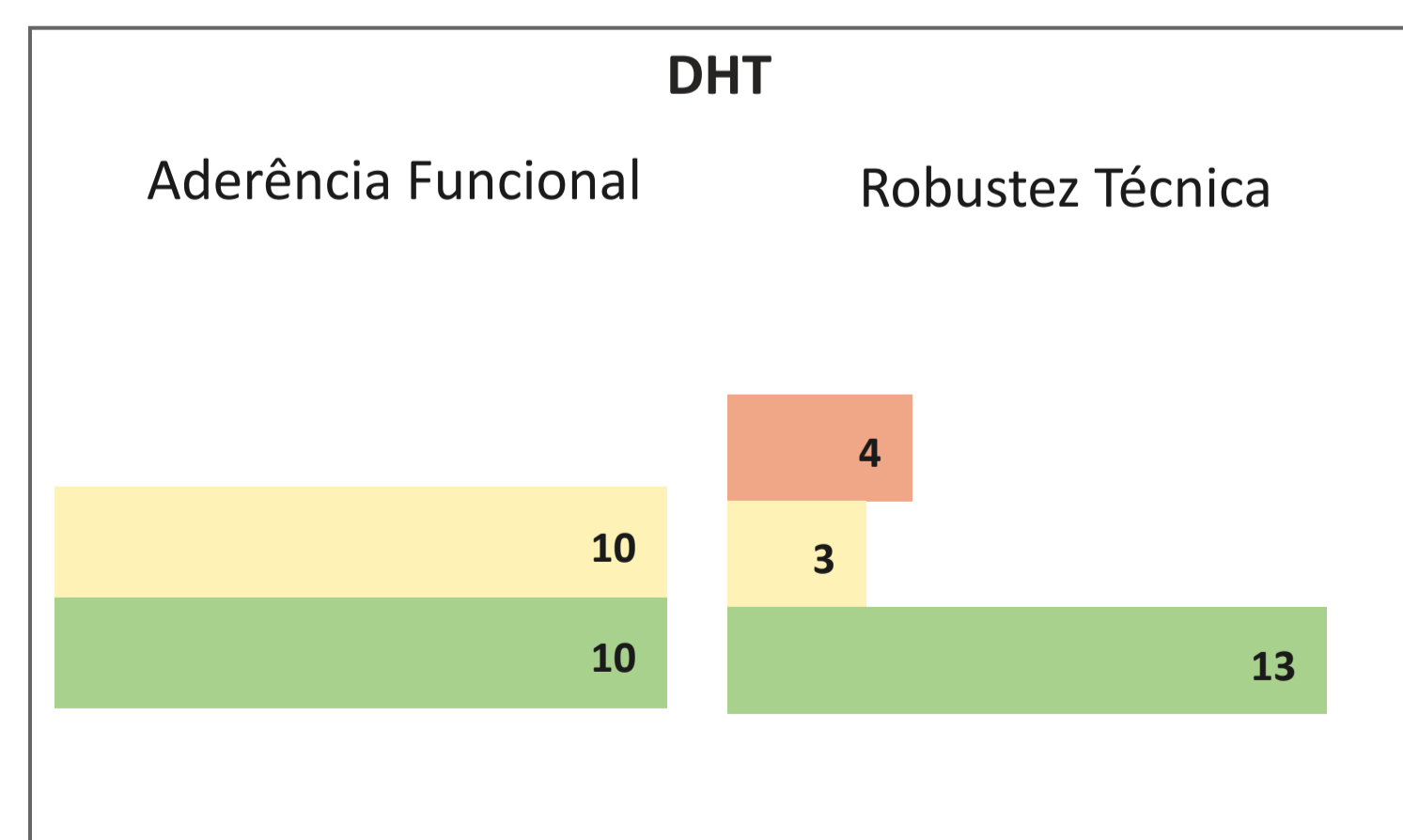
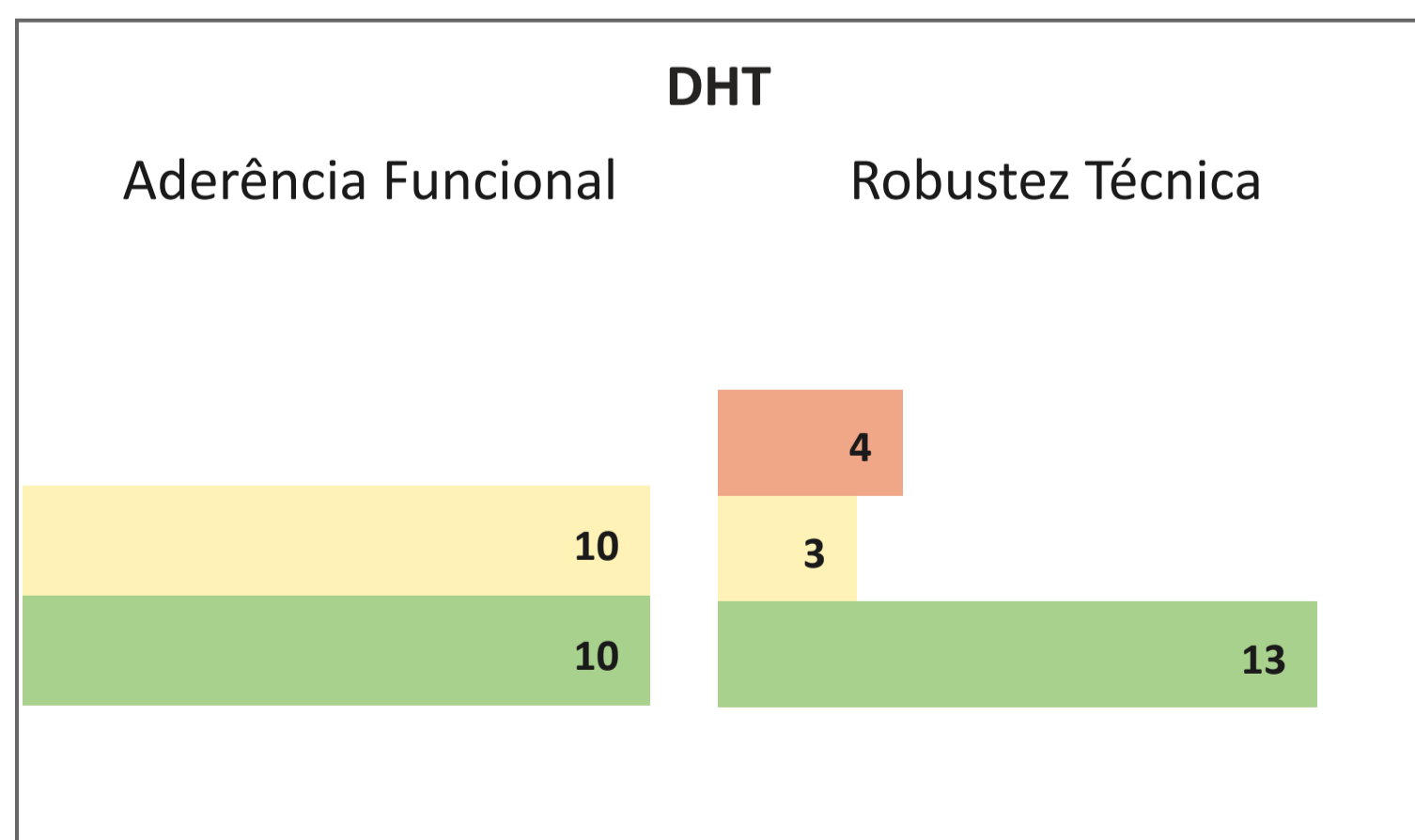
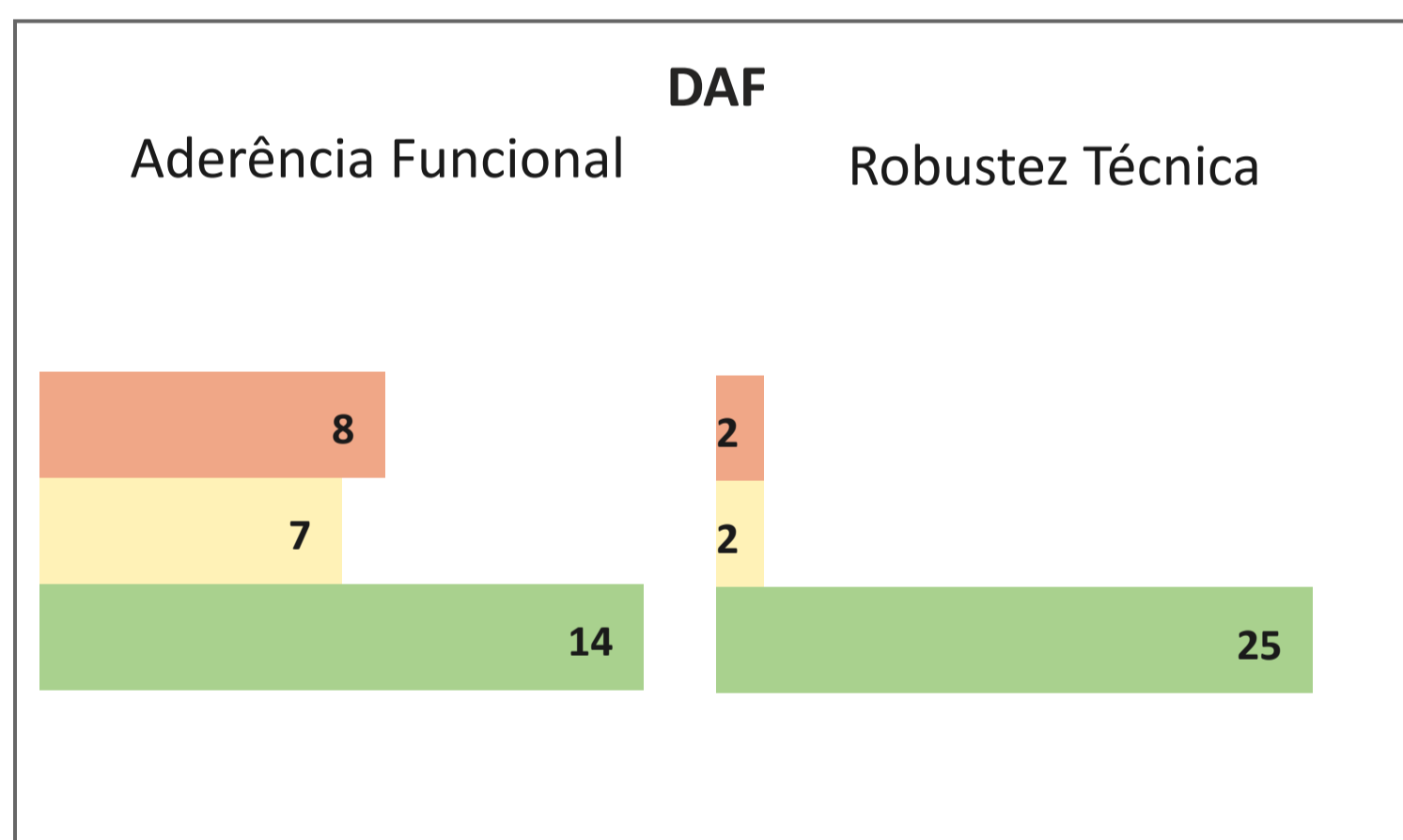
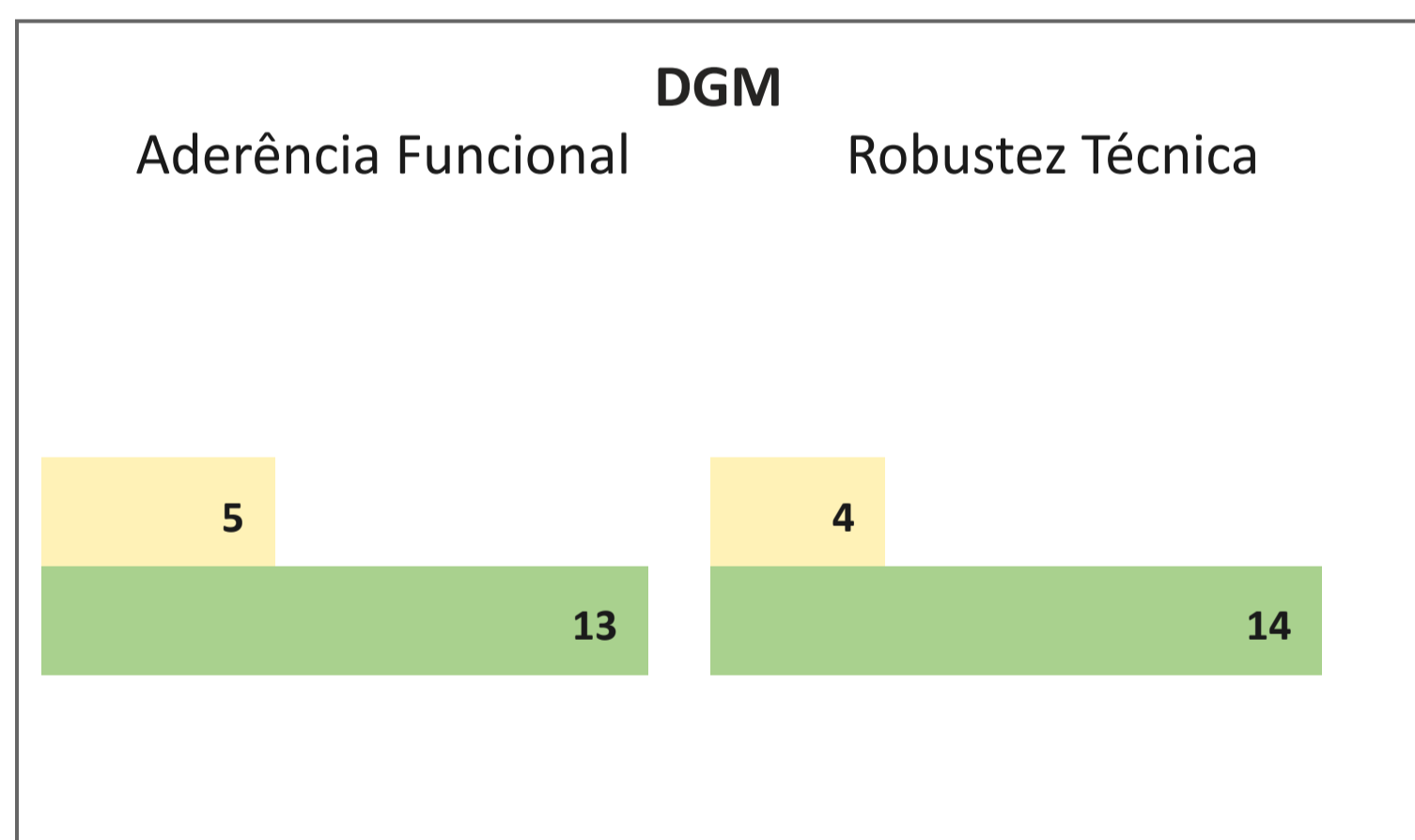
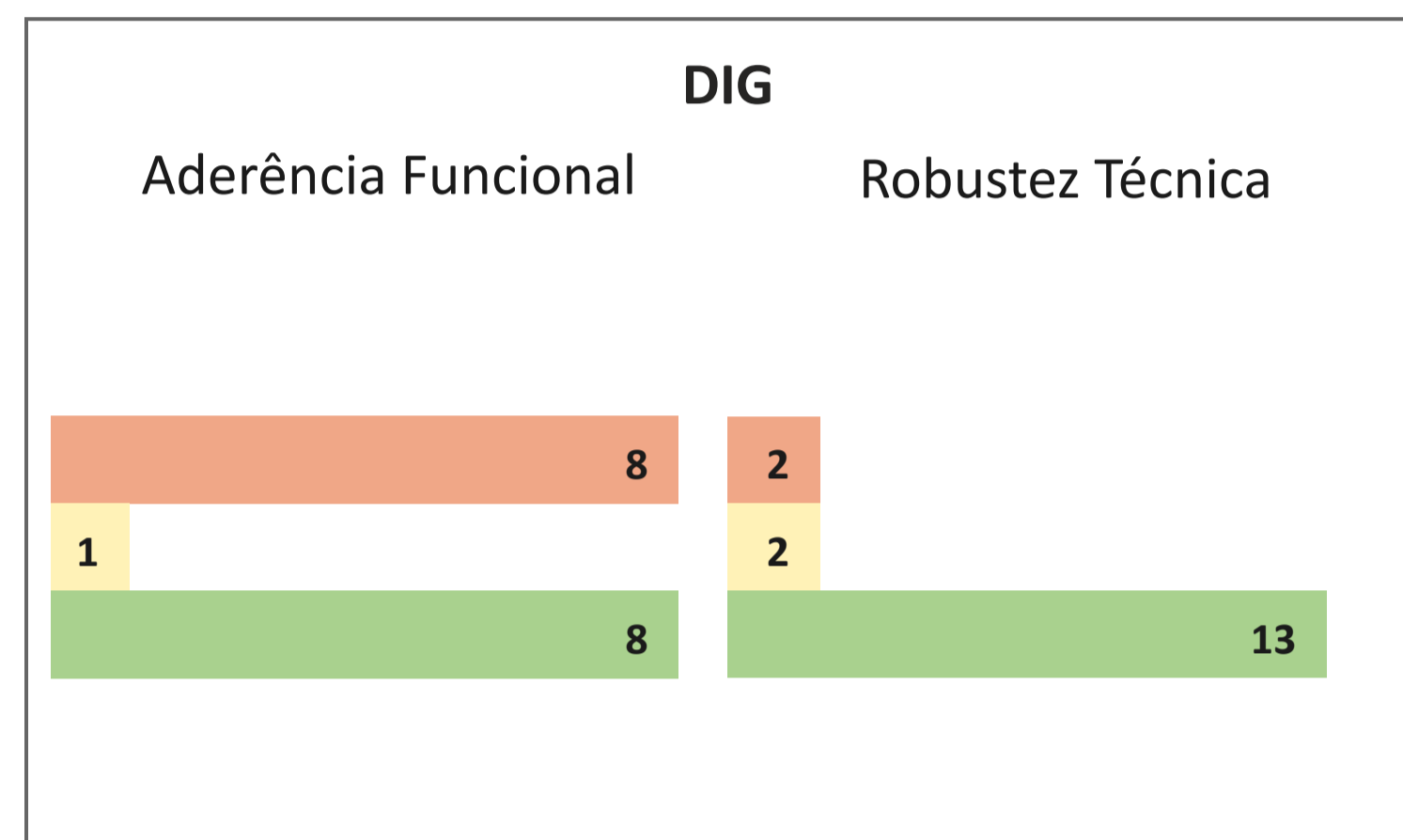
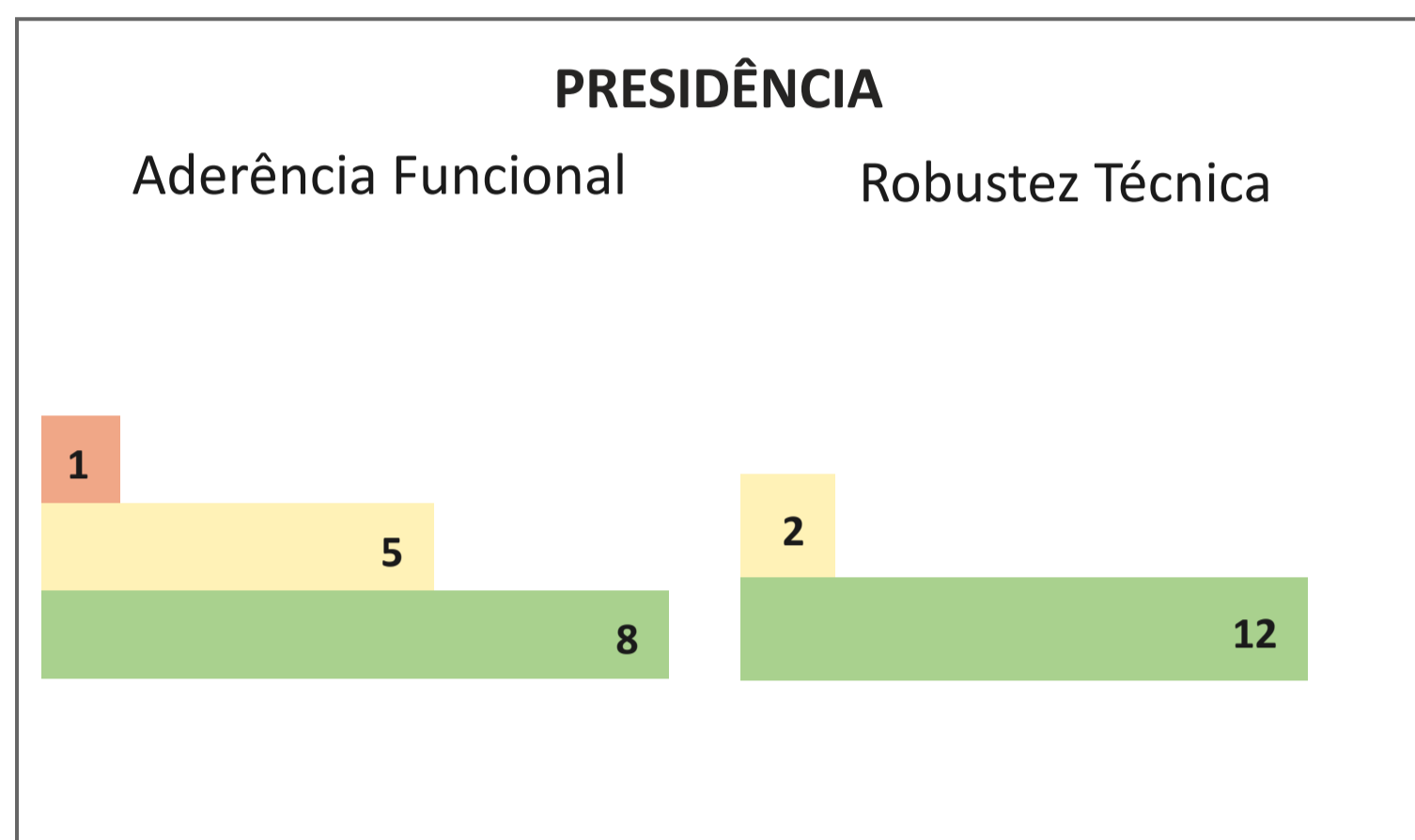


Orçamento



Roadmap

VISÃO SISTÊMICA POR ÁREA



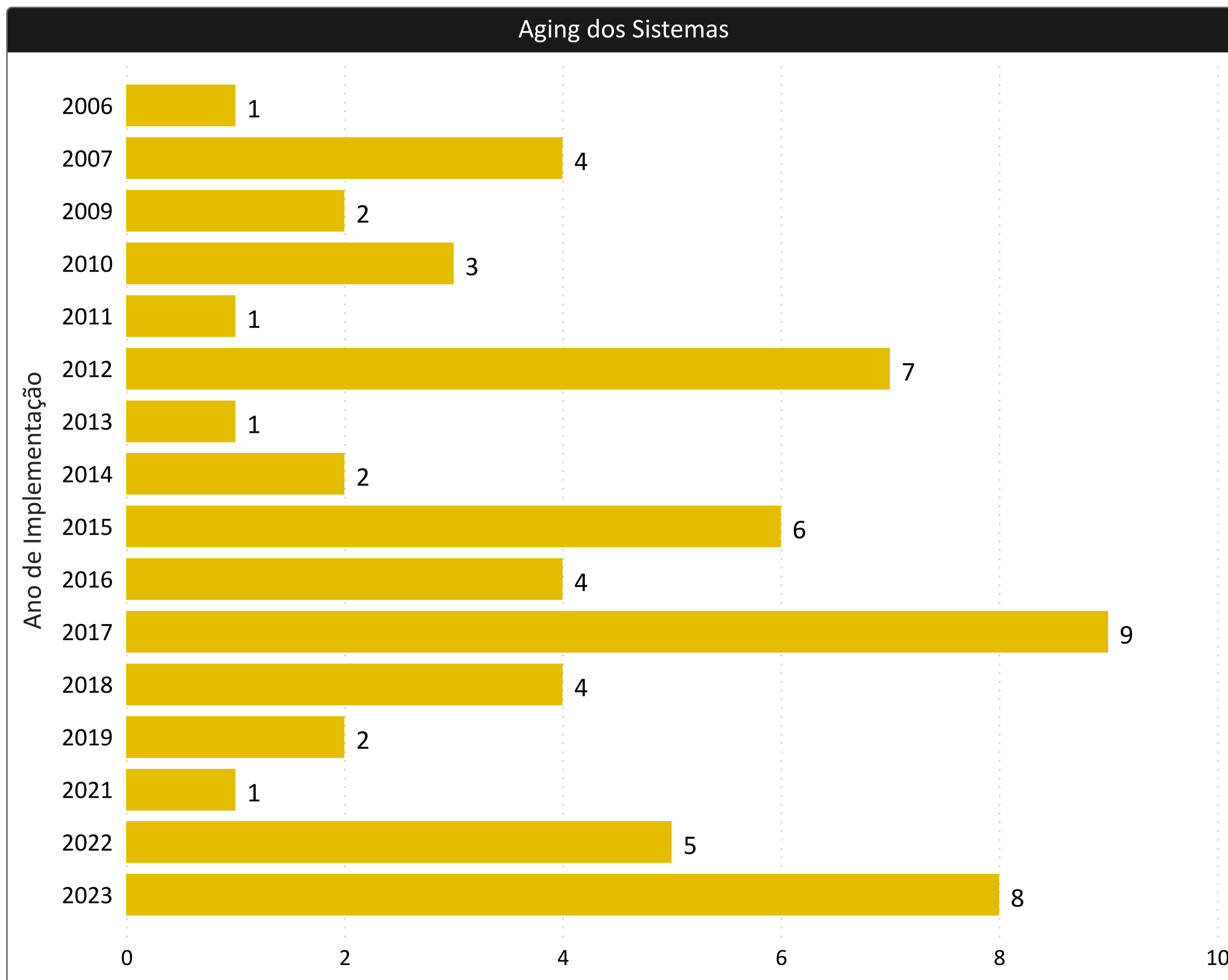
Os quadros ao lado apresentam a visão por áreas em relação ao atendimento dos seus sistemas. Eles apresentam a visão sob 2 pilares que serão usados para direcionar o tratamento do portfólio de sistemas como um todo:

Aderência Funcional*: a aderência funcional representa, de forma resumida, o quanto o processo de negócio da área é suportado pelos seus sistemas.

Robustez Técnica: mostra o quão sólido estão os sistemas sob a ótica das tecnologias que os suportam. Este pilar é mensurado de acordo com a arquitetura técnica do sistemas, seu banco de dados, sistema operacional e linguagens de programação.

* É importante enfatizar que a aderência funcional foi identificada por meio de indagação e não se utilizou de metodologias de cruzamento das necessidade das atividades das áreas de negócio com os requisitos dos sistemas, mantendo o nível de detalhe próprio de um Plano Diretor.

AGING DOS SISTEMAS



A partir do gráfico *Aging* dos sistemas é possível identificar o período de maior investimento na implantação de soluções tecnológicas no SGB, assim como a idade dos sistemas utilizados.

Esses dados apoiam a verificação da adequação funcional das soluções existentes, assim como a robustez técnica das suas arquiteturas.

DESENVOLVIMENTO DE SISTEMAS

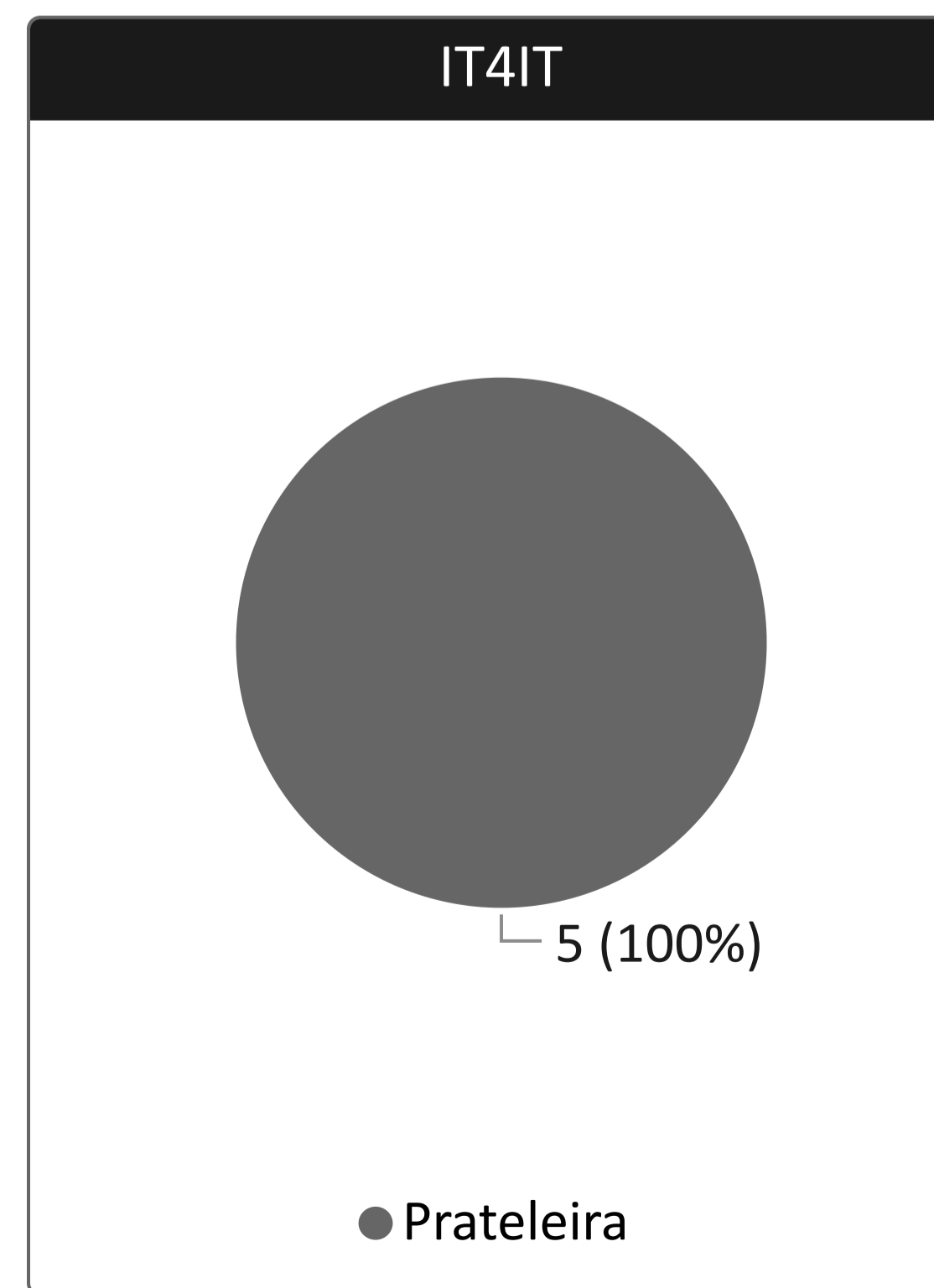
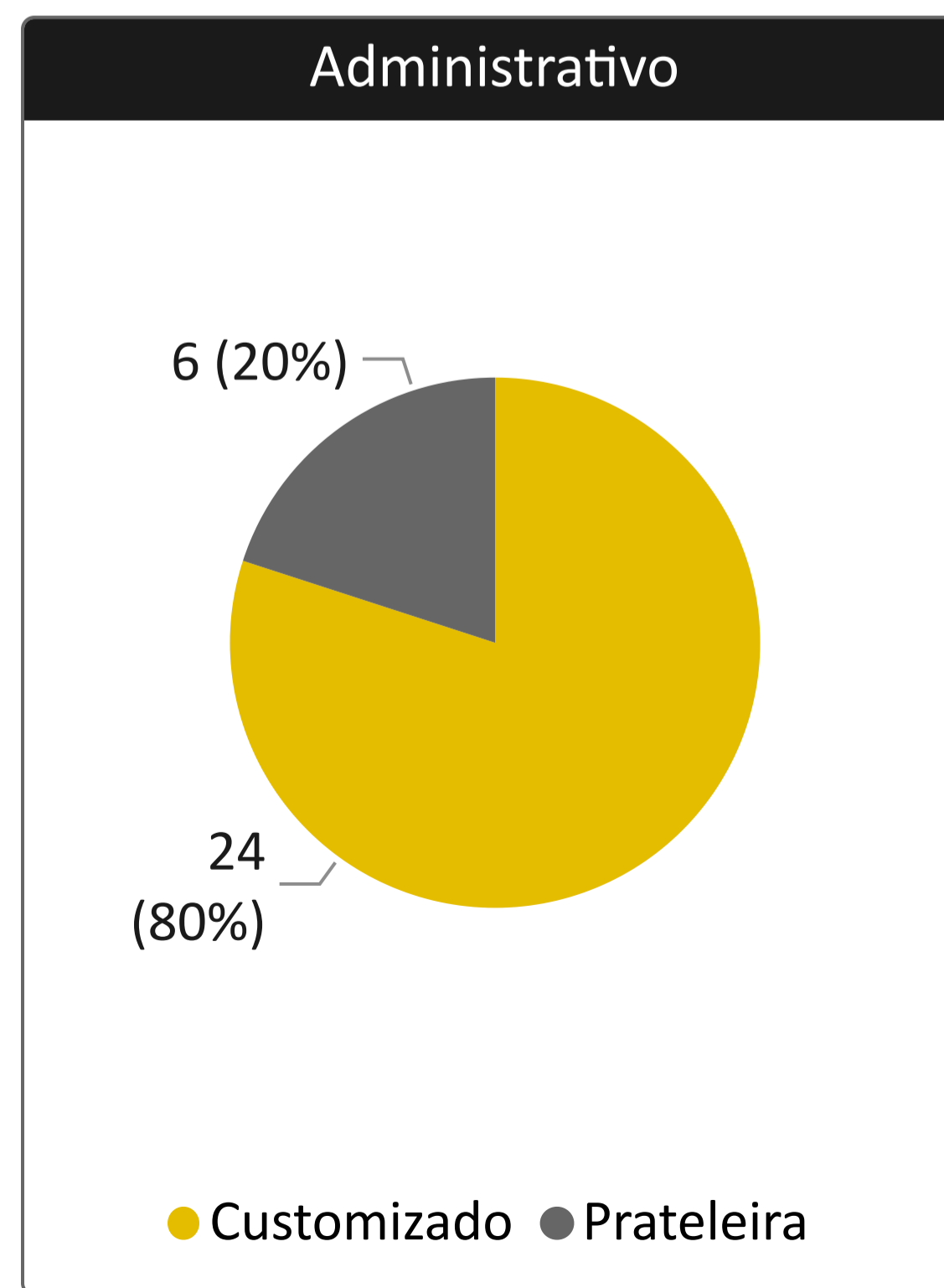
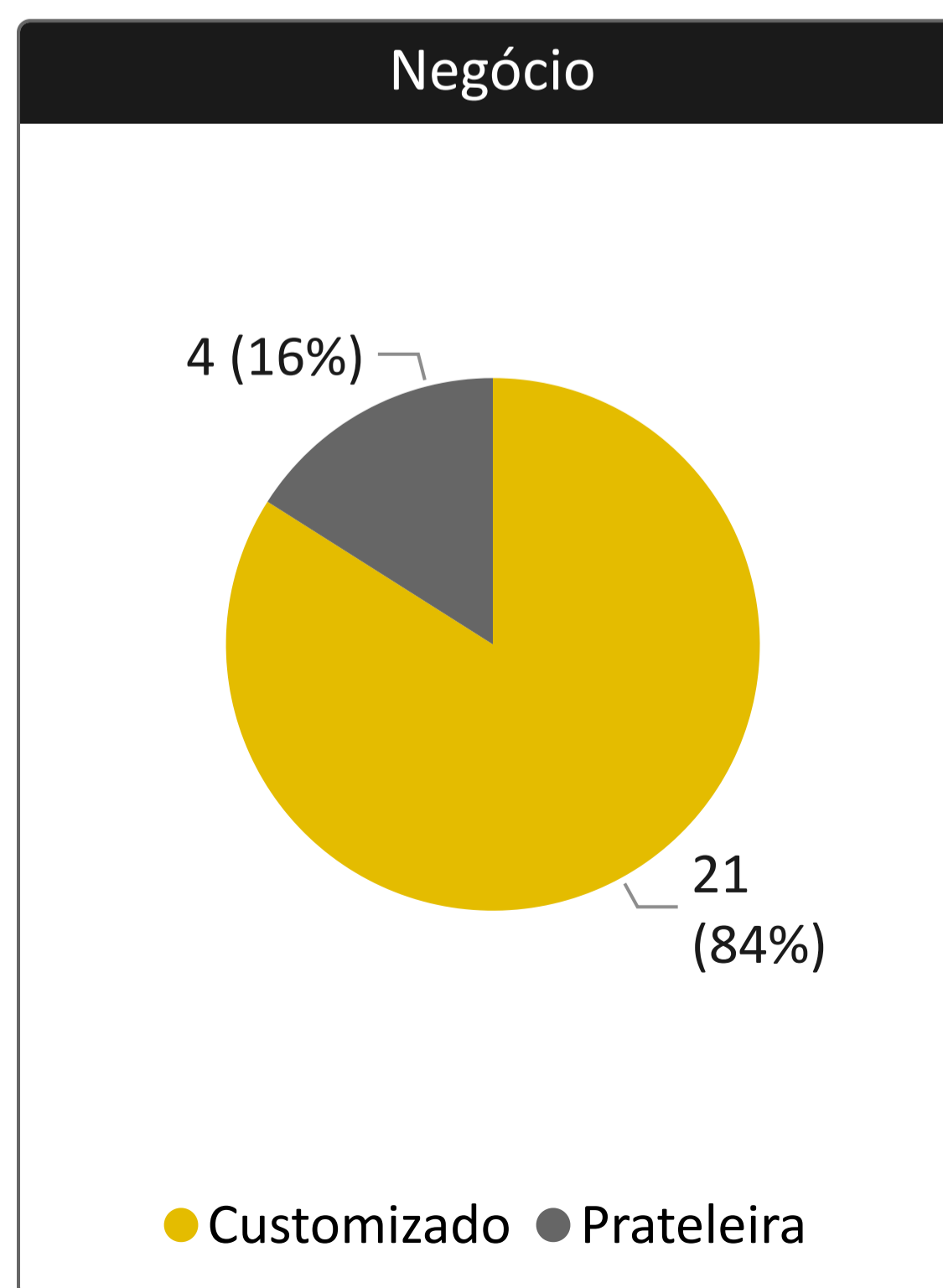
Origem dos sistemas



De um total de 60 aplicações, 33% são compradas de algum fornecedor e 67% são desenvolvidas internamente. O desenvolvimento interno implica expertise e maturidade em práticas de desenvolvimento e manutenção de sistemas.

72% das aplicações no SGB são customizadas. A alta incidência de aplicações customizadas impacta diretamente a sustentação do ambiente mantido pela TI.

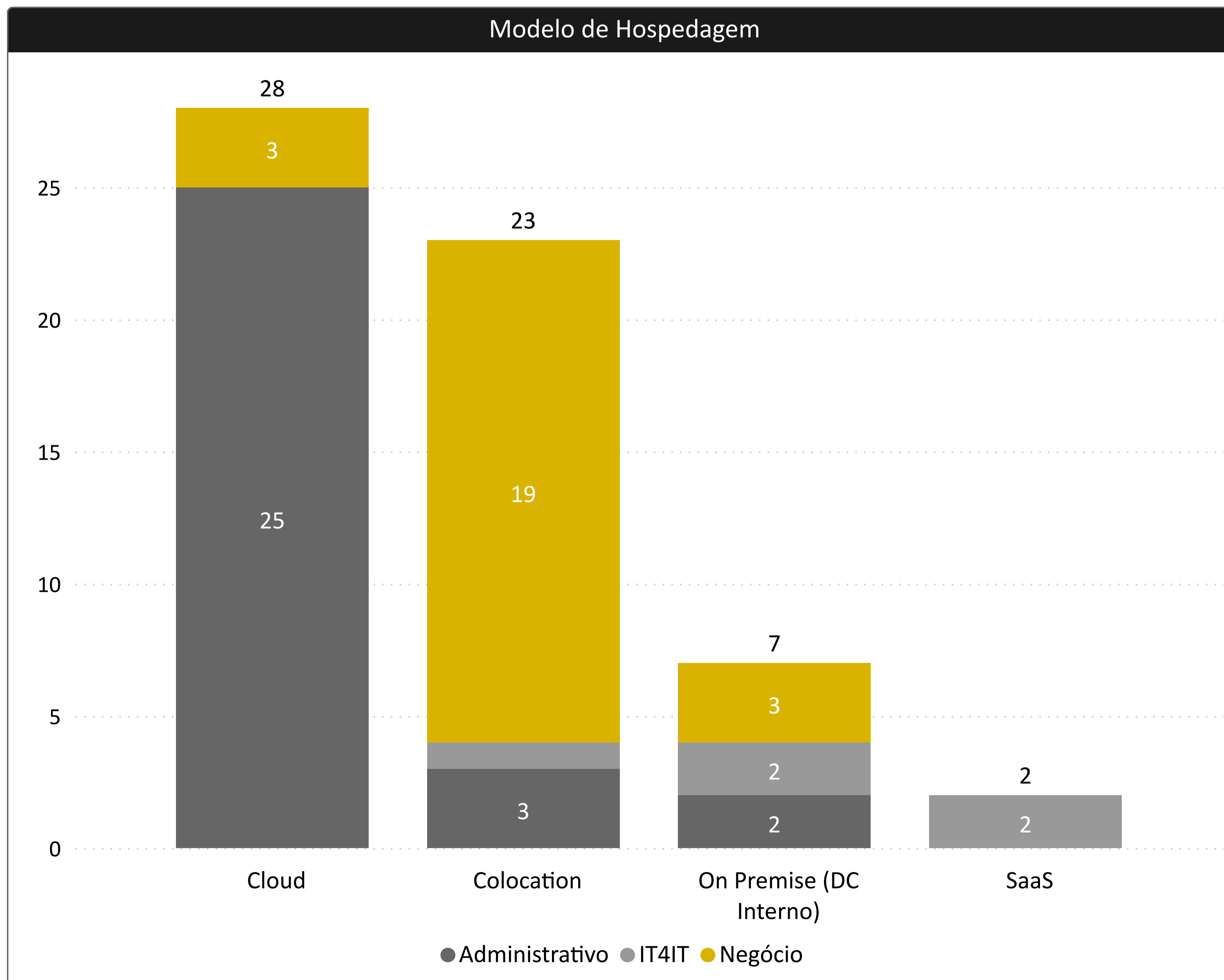
TIPO DE DESENVOLVIMENTO POR CLASSIFICAÇÃO DE SISTEMAS



Apesar do negócio solicitar frequentemente a customização de soluções, para que elas se adequem aos processos da empresa, é imprescindível mensurar sua viabilidade a longo prazo, pois envolvem maior esforço de manutenção, maior maturidade nas práticas de desenvolvimento, comparadas com aquelas que são *commodities* e mantidas por fornecedores robustos.

A alta incidência de soluções desenvolvidas internamente/customizadas implica riscos à continuidade do negócio, em função de fatores, como: perda de conhecimento, obsolescência de tecnologia, mudanças regulatórias e etc.

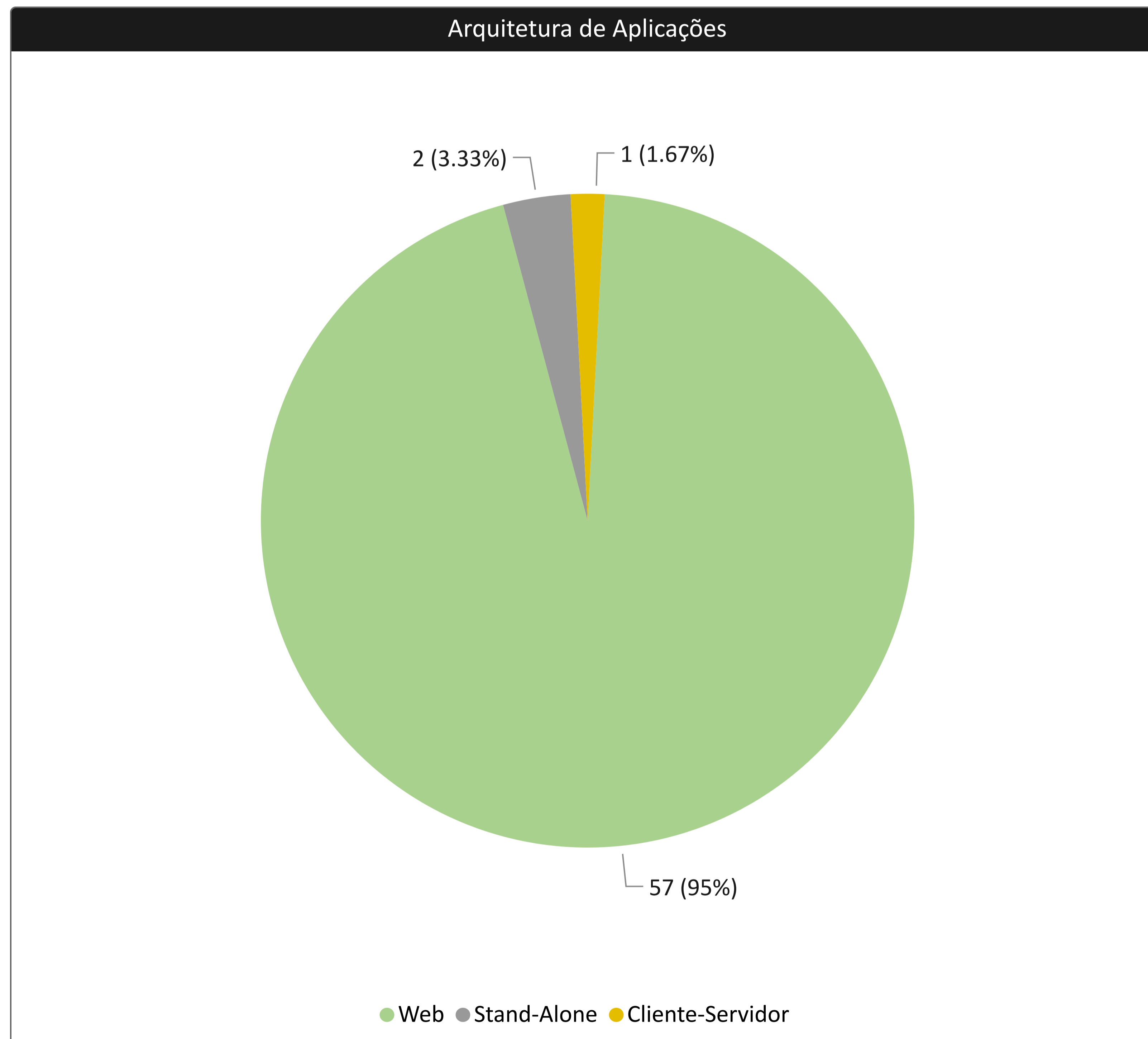
HOSPEDAGEM



A hospedagem *on premise* demanda maturidade para ser operacionalizada, pois em um ambiente de maturidade baixa há maior risco de instabilidade, indisponibilidade e eventuais impactos na integridade dos dados.

No caso do SGB, 07 aplicações estão hospedadas no data center interno. Dentre as quais 03 estão classificadas como "Negócio".

ARQUITETURA DE APLICAÇÕES



Existe apenas 1 aplicação no SGB que utiliza a arquitetura cliente-servidor de 3 camadas. Aplicações com arquitetura cliente-servidor de 3 camadas possuem uma camada "Cliente", que é a apresentação da aplicação; a camada "Aplicação", onde armazena a aplicação em si, com suas regras de negócio, em um servidor onde ocorre todo o processamento e a camada "Banco de Dados", esta última onde os dados ficam armazenados, também em um servidor distinto. Esta arquitetura, assim como a Web, é considerada segura.

95% dos aplicações utilizados possuem arquitetura Web.

Arquitetura Stand-Alone são aplicações que são executadas localmente. Podem ou não possuir banco de dados, mas caso possuam, estes são locais.



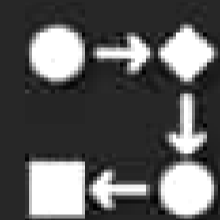
Painel



Estratégia



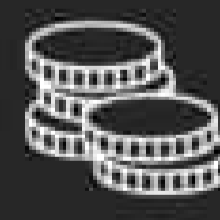
Pessoas



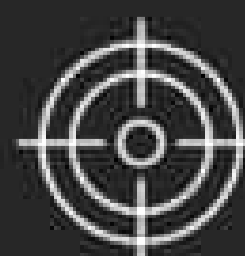
Processos



Tecnologia



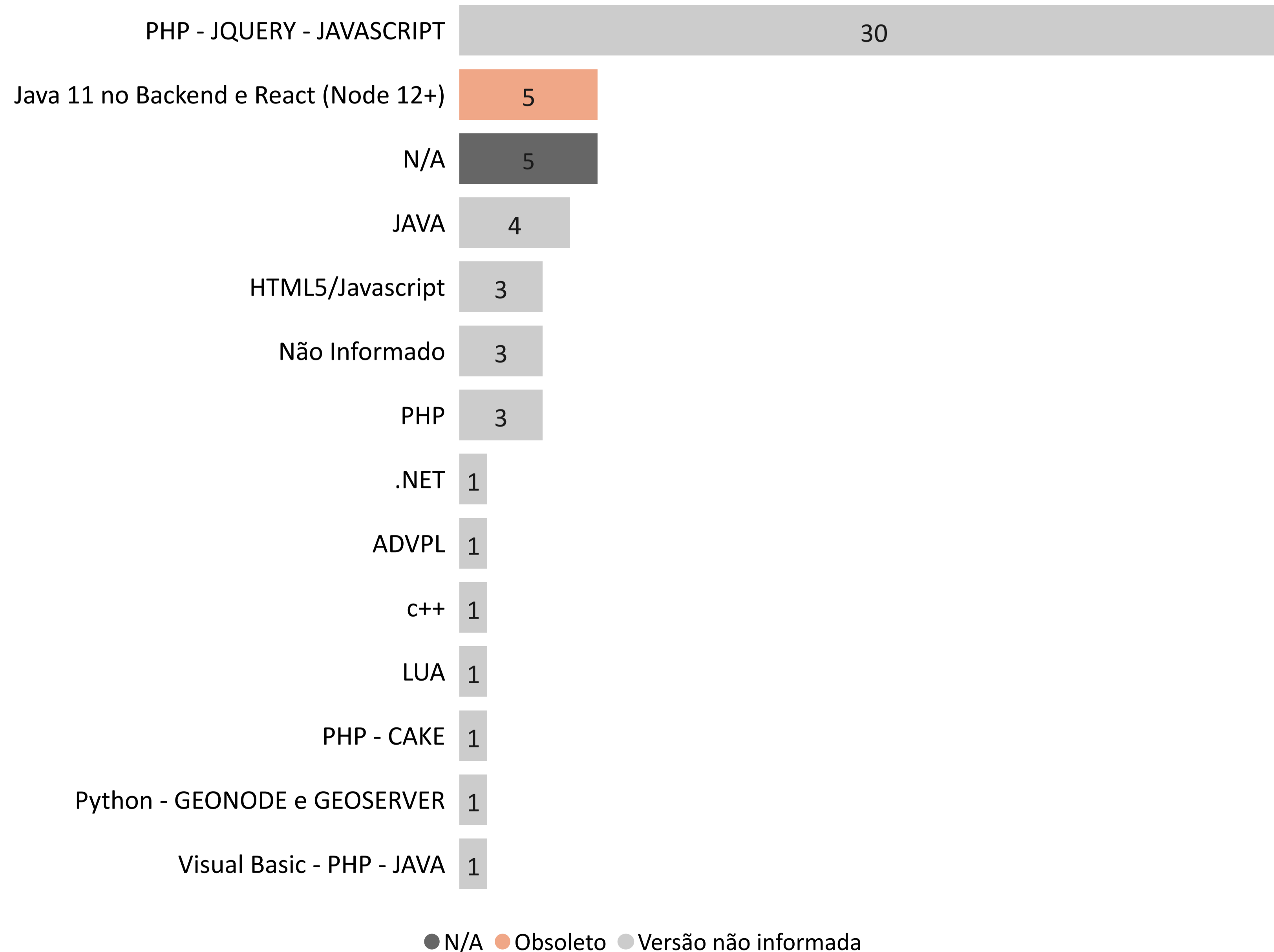
Orçamento



Roadmap

LINGUAGEM DE PROGRAMAÇÃO

Obsolescência - Linguagem de Programação



A utilização de linguagens obsoletas acarreta em vulnerabilidades e aumento dos riscos operacionais, uma vez que os fabricantes não disponibilizam *patches* de correção.

***Nas aplicações sinalizadas como N/A, não foi possível identificar a linguagem de programação e não será objeto de análise.*



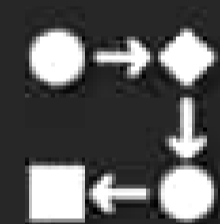
Painel



Estratégia



Pessoas



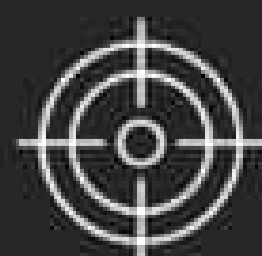
Processos



Tecnologia



Orçamento



Roadmap

Linguagem de Programação

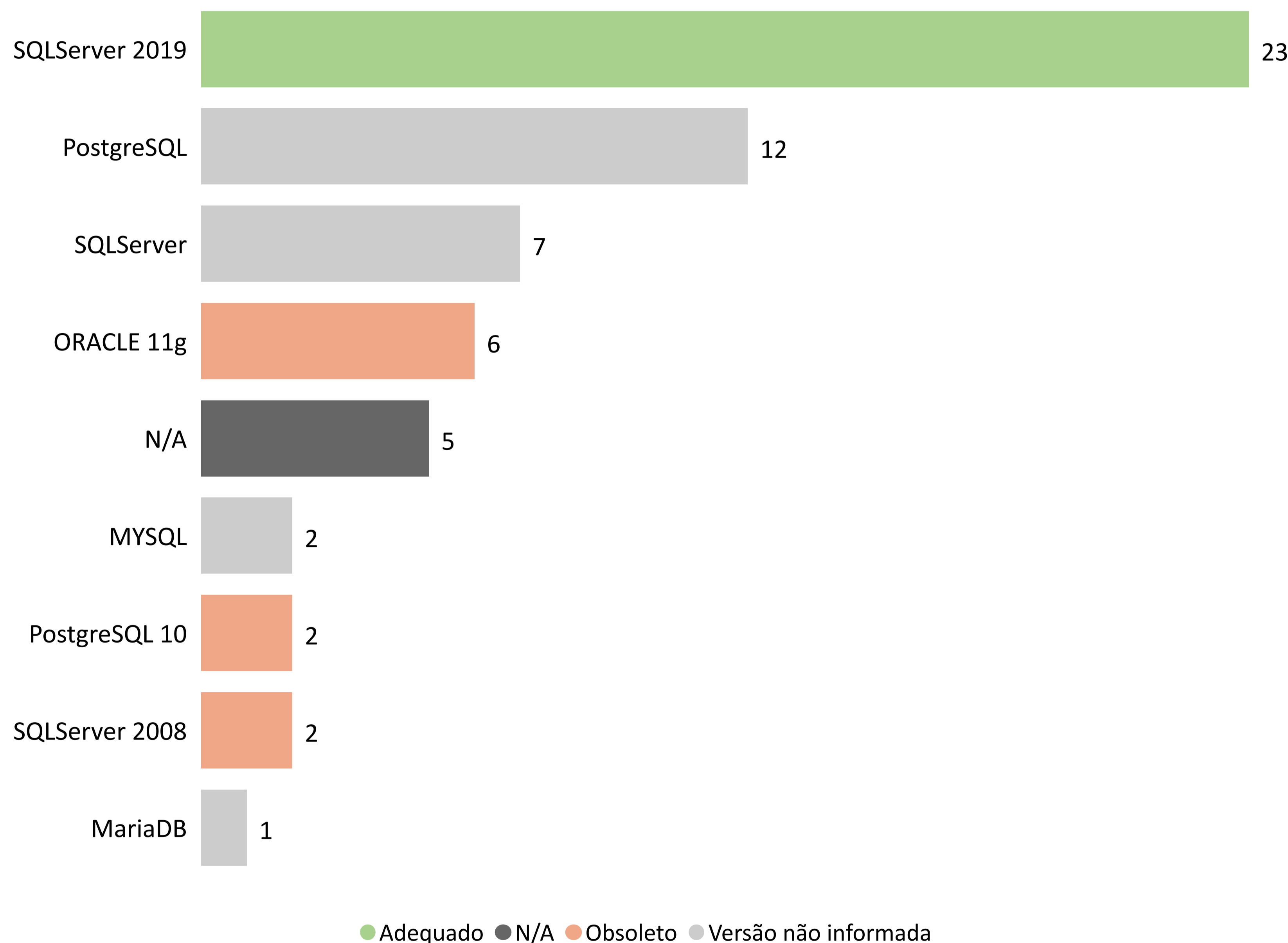
Banco de Dados

SO do Banco de Dados

SO das Aplicações

BANCO DE DADOS

Obsolescência - Banco de Dados

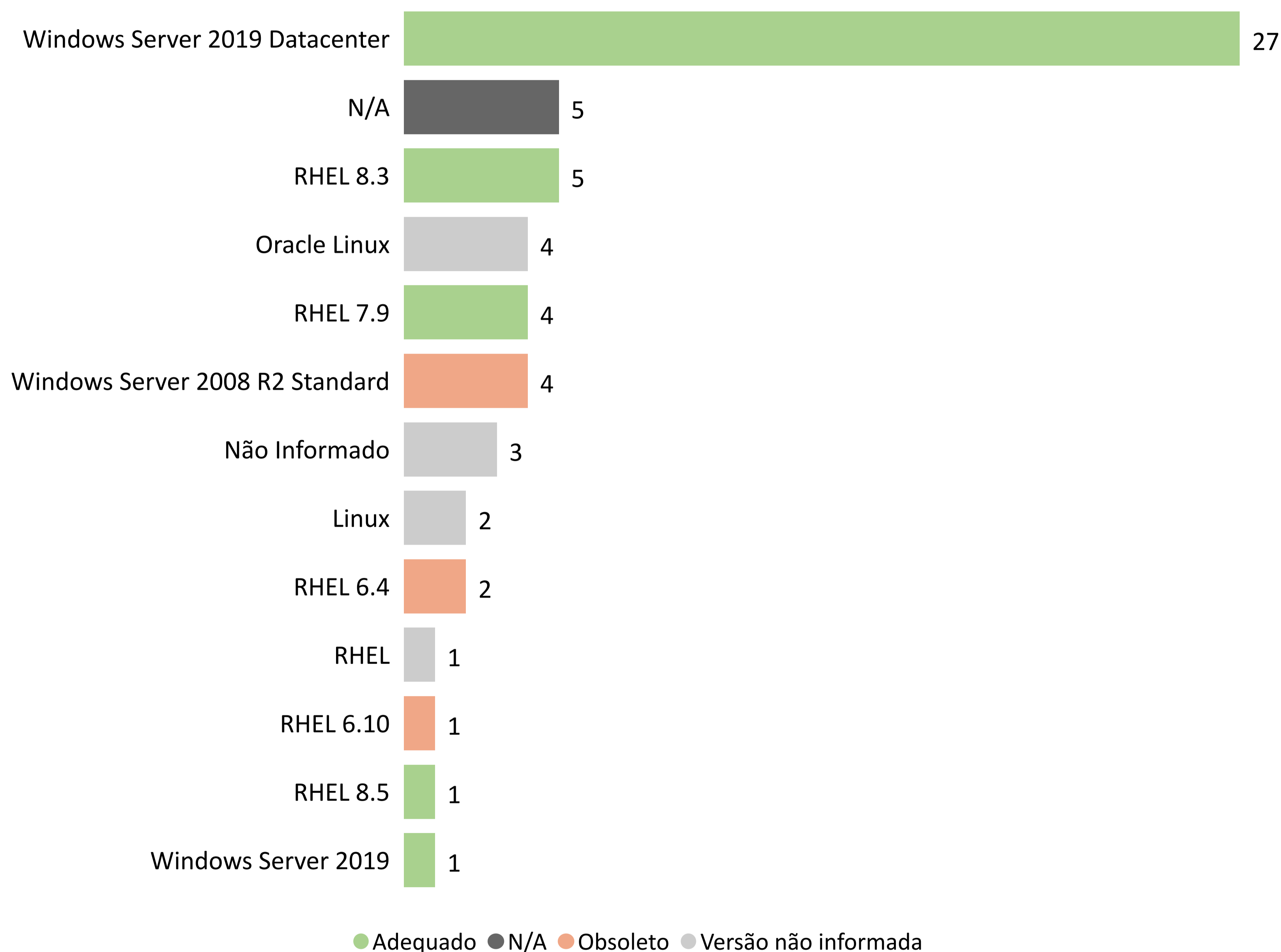


O SGB possui em sua infraestrutura aplicações que utilizam tecnologias de Banco de Dados obsoletas, sem suporte do fabricante ou próximo de perdê-lo. A adequação técnica desses itens se faz necessária para minimizar riscos operacionais e aumentar o nível de segurança das soluções. Dos sistemas core, 10 encontram-se inadequados tecnicamente.

***As aplicações sinalizadas como N/A possuem seus bancos de dados embarcados na própria solução ou são SaaS (Software as a Service).*

SO DO BANCO DE DADOS

Obsolescência - Sistema Operacional do Banco de Dados



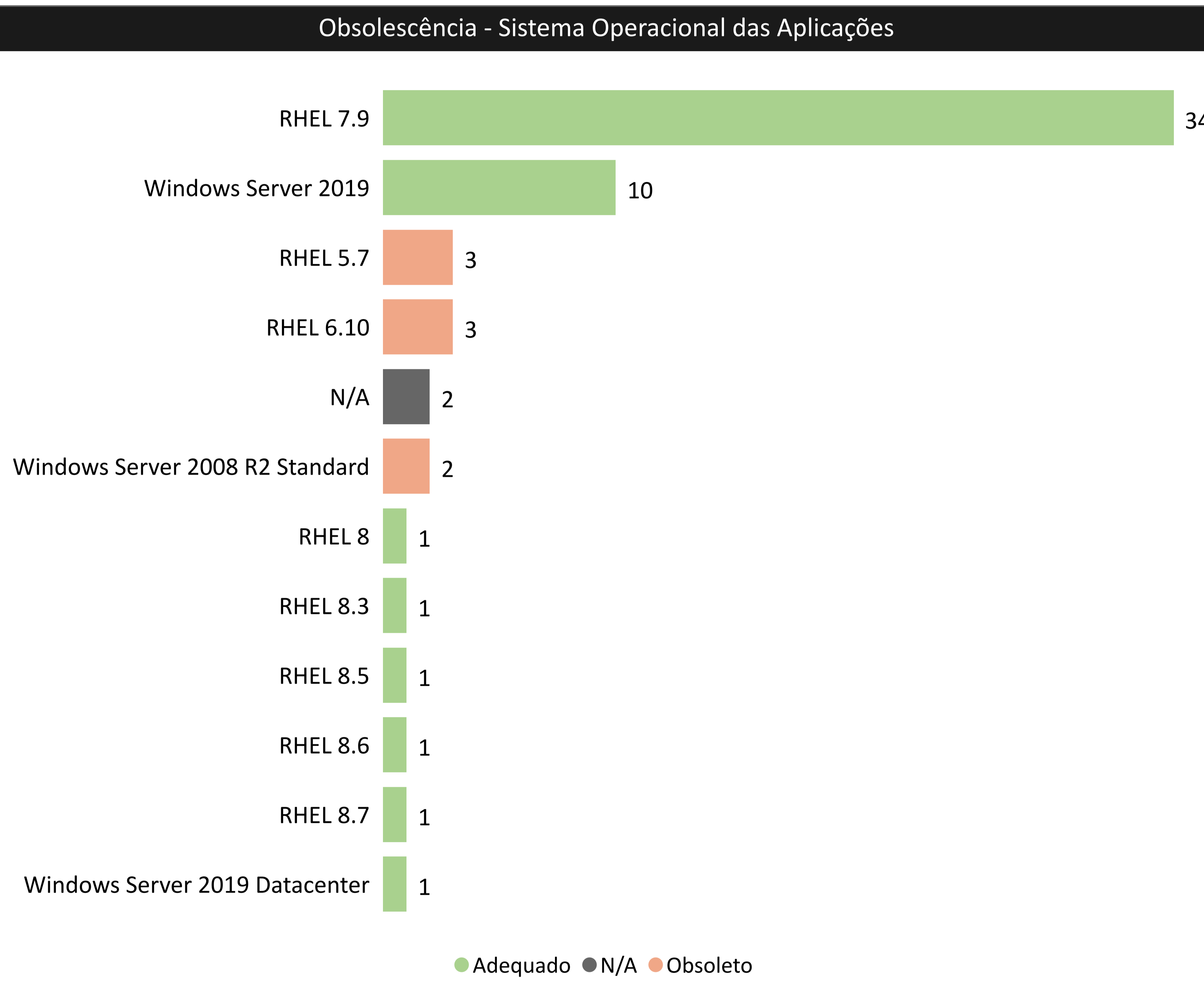
Assim como o apontado com as tecnologias de Banco de Dados obsoletas utilizadas no SGB, o mesmo acontece com sistemas operacionais utilizados para os bancos de dados, ou seja, existem bancos de dados instalados em servidores com sistemas operacionais sem suporte do fabricante ou próximo de perdê-lo.

***As aplicações sinalizadas como N/A não possuem servidor apartado para o Banco de Dados.*



SO DAS APLICAÇÕES

Obsolescência - Sistema Operacional das Aplicações



Existem sistemas operacionais instalados em servidores de aplicações que são obsoletos, sem suporte do fabricante ou próximo de perdê-lo.

A adequação se faz necessária para minimizar riscos operacionais e de segurança da informação.

***As aplicações sinalizadas como N/A são aplicações SaaS (Software as a Service), não possuindo servidor local de aplicação.*



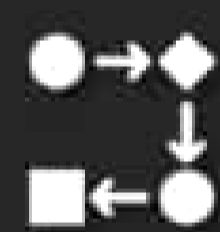
Painel



Estratégia



Pessoas



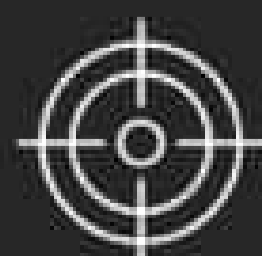
Processos



Tecnologia

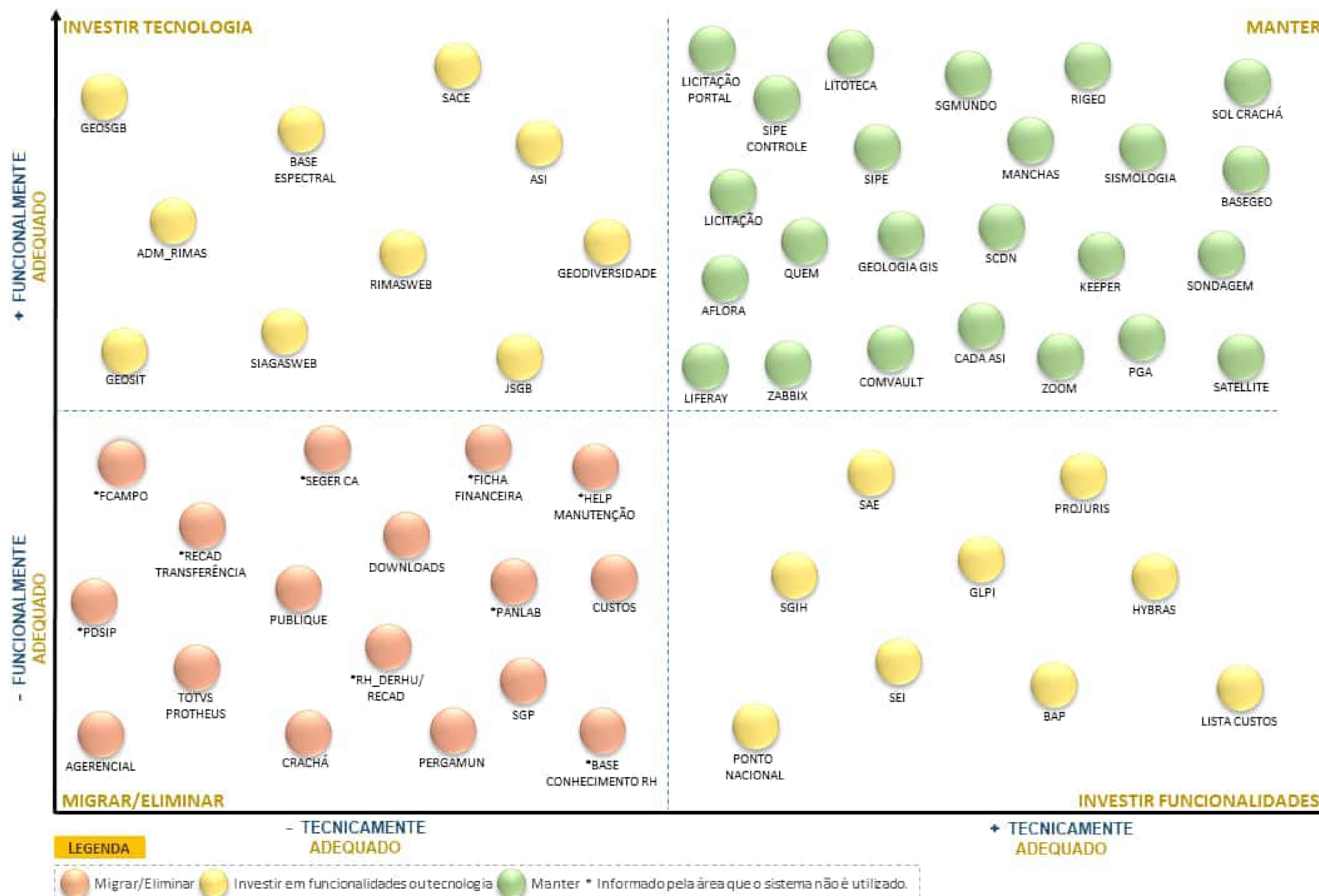


Orçamento



Roadmap

PORTFÓLIO DE SISTEMAS ATUAL

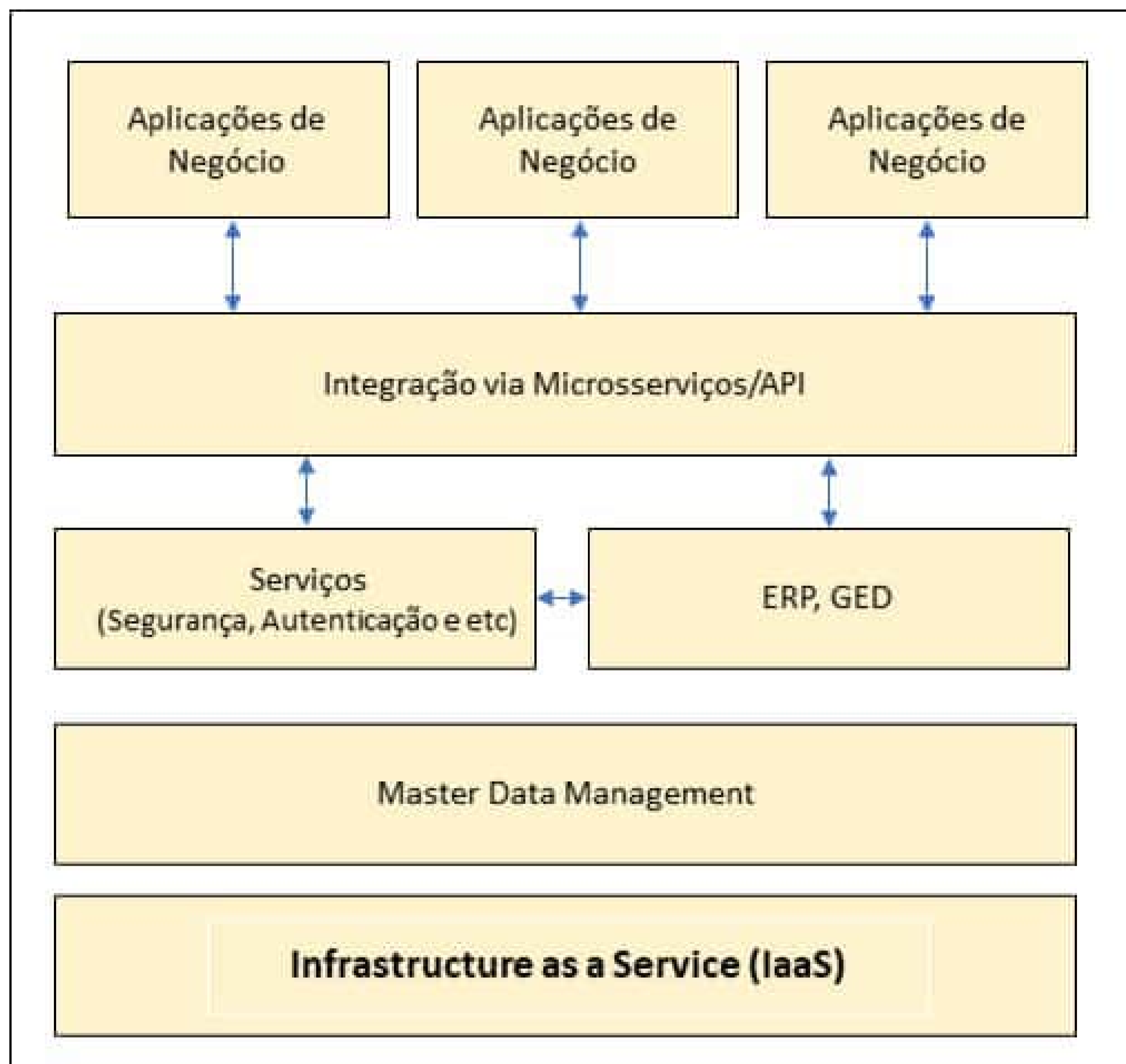


A visão consolidada das análises realizadas dos sistemas do SGB estão agrupadas nos quadrantes apresentados na imagem ao lado.

O eixo vertical representa o grau de aderência funcional (segundo as áreas de negócio) dos sistemas. O eixo horizontal representa a robustez dos sistemas sob o ponto de vista técnico, de TI.

Ressalta-se que a posição dos sistemas no quadrante, não representa uma análise de priorização. Está priorização deve ser tratada pela TI em conjunto com negócio.

ARQUITETURA DE SISTEMAS



No Direcionamento para o Portfólio de Sistemas são apresentadas as ações necessárias para adequação funcional e técnica dos sistemas do SGB.

Aliado a essas recomendações e baseado no alto volume de sistemas customizados, sugere-se a utilização de uma arquitetura sistêmica baseada em uma abordagem de microserviços.

Também deve ser considerada a implantação de um ERP para suportar todo o backoffice, uma solução GED como fonte única de documentos e a estruturação de dados através do conceito de MDM.



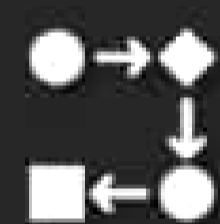
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

Portfólio de Sistemas

Arquitetura de Sistemas

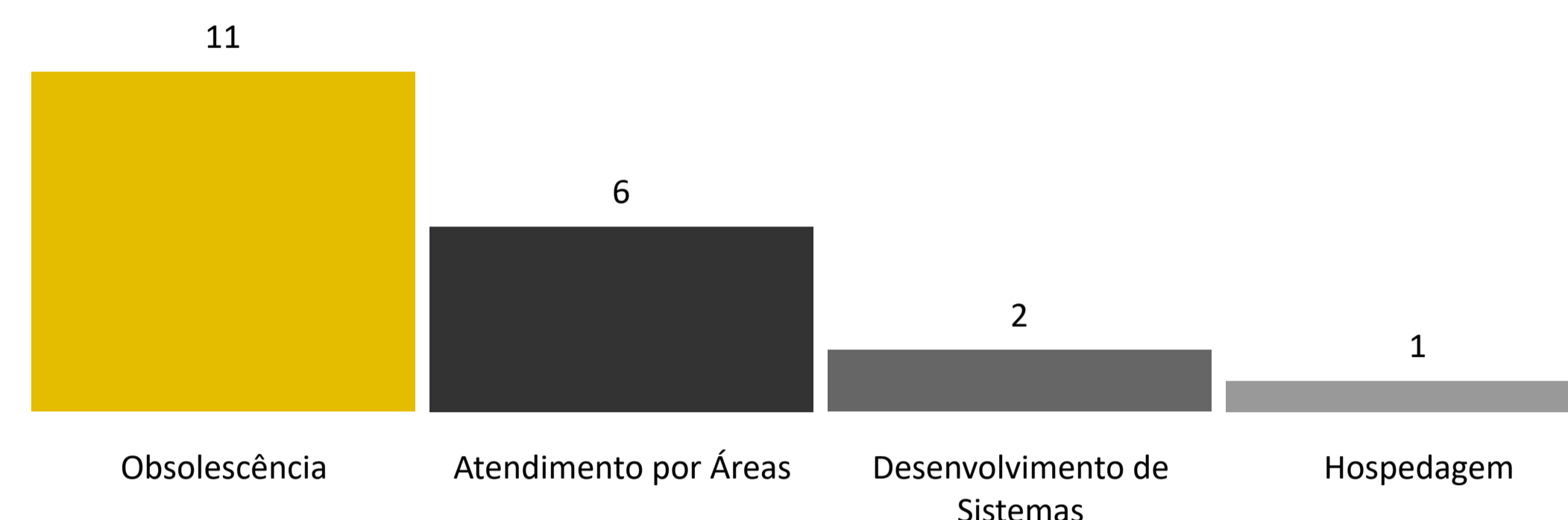
Oportunidades e Recomendações

OPORTUNIDADES E RECOMENDAÇÕES

Oportunidades x Recomendações



Detalhamento Oportunidades



Tema	Oportunidade	Recomendação
Desenvolvimento de Sistemas	Quando há uma demanda por sistemas de tecnologia, não há um processo definido de "make or buy" para decisão entre comprar um software/funcionalidade de mercado que atenda as necessidades ou desenvolvê-lo internamente.	Definir e implementar um processo de "make or buy" para analisar a viabilidade de compra ou desenvolvimento interno de software/funcionalidade e suportar a tomada de decisão.
Desenvolvimento de Sistemas	Existe uma célula de desenvolvimento interna no SGB, atendendo as demandas do negócio para sistemas de tecnologia, sem a vinculação/supervisão da Tecnologia da Informação, sendo esta célula financiada pela área de negócio.	Em alguns casos, soluções via democratização (Low/No Code) que consistem no desenvolvimento de soluções pelo próprio time de negócio e não são suportados e/ou sustentados pela TI, apresentam resultados extremamente positivos. A TI deverá estabelecer normas e padrões para utilização desta metodologia adotada pelas áreas de negócio.
Hospedagem	50% das aplicações analisadas possuem sua hospedagem On Premise (tanto em data center interno quanto colocation). Este tipo de hospedagem pode gerar riscos de indisponibilidade sistêmica caso o ambiente ou a gestão não possuam a maturidade adequada.	Migrar as aplicações On Premise para Cloud, conforme os equipamentos cheguem ao final do ciclo de vida. (EoL)
Obsolescência de Tecnologia - Linguagem de Programação	Houve um GAP de inventário de 83% referente as informações de versionamento das linguagens de programação utilizadas. Das informações recebidas (5 aplicações), 100% estão obsoletas. São elas: Java 11 + React 12+. (EoL atingido em abril/2022)	Verificar a possibilidade de substituir as aplicações customizadas/desenvolvidas internamente por soluções existentes no mercado.
Obsolescência de Tecnologia - Linguagem de Programação	Houve um GAP de inventário de 83% referente as informações de versionamento das linguagens de programação utilizadas. Das informações recebidas (5 aplicações), 100% estão obsoletas. São elas: Java 11 + React 12+. (EoL atingido em abril/2022)	Caso não seja possível substituir as aplicações customizadas, atualiza-las com as versões mais recentes das linguagens de programação.
Obsolescência de Tecnologia - Banco de Dados	Existem 6 (seis) aplicações que utilizam o banco de dados Oracle 11g, que já está considerado obsoleto e teve seu EoL em dezembro/2020.	Atualizar a versão do banco de dados Oracle 11g para a mais recente (Oracle 19c).
Obsolescência de Tecnologia - Banco de Dados	Existem 2 (duas) aplicações que utilizam o banco de dados PostgreSQL10, que já está considerado obsoleto e teve seu EoL em novembro/2022.	Atualizar a versão do banco de dados PostgreSQL10 para a mais recente (PostgreSQL 15.2).
Obsolescência de Tecnologia - Banco de Dados	Existem 2 (duas) aplicações que utilizam o banco de dados SQL Server 2008, que já está considerado obsoleto e teve seu EoL em julho/2022.	Atualizar a versão do banco de dados SQL Server 2008 para a mais recente (SQL Server 2019).
Obsolescência de Tecnologia - Sistema Operacional Banco de	Existem 4 (quatro) aplicações que utilizam banco de dados que são hospedadas em servidor(es) com Sistema Operacional Windows Server 2008 R2 Standard	Atualizar o sistema operacional do(s) servidor(es) que utiliza(m) o Windows 2008 R2 Standard e hospedam banco de dados de aplicações (Windows Server 2022)



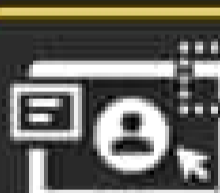
Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap



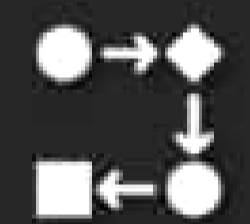
Painel



Estratégia



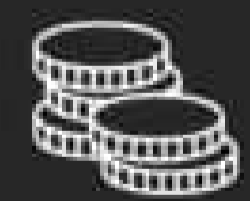
Pessoas



Processos



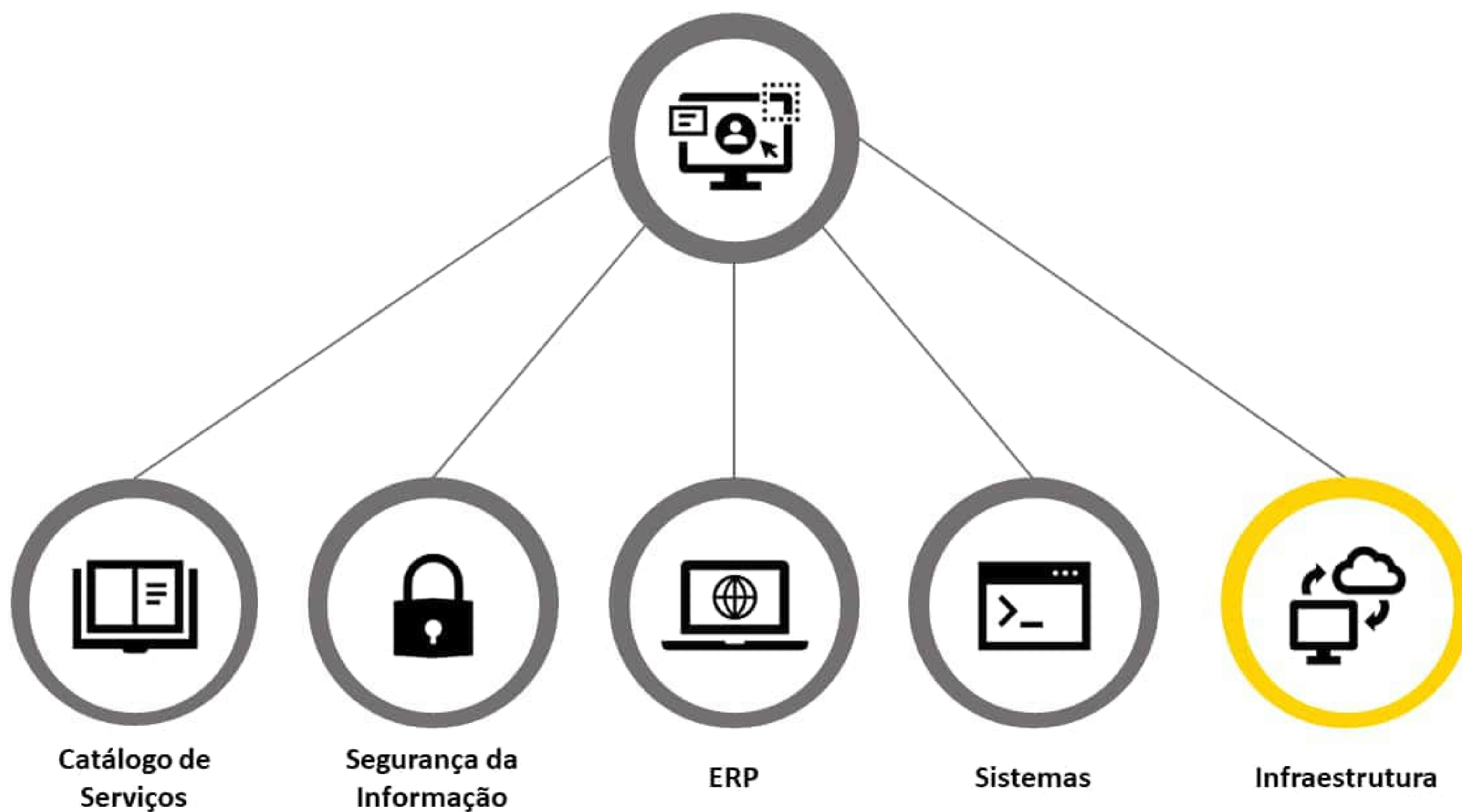
Tecnologia



Orçamento

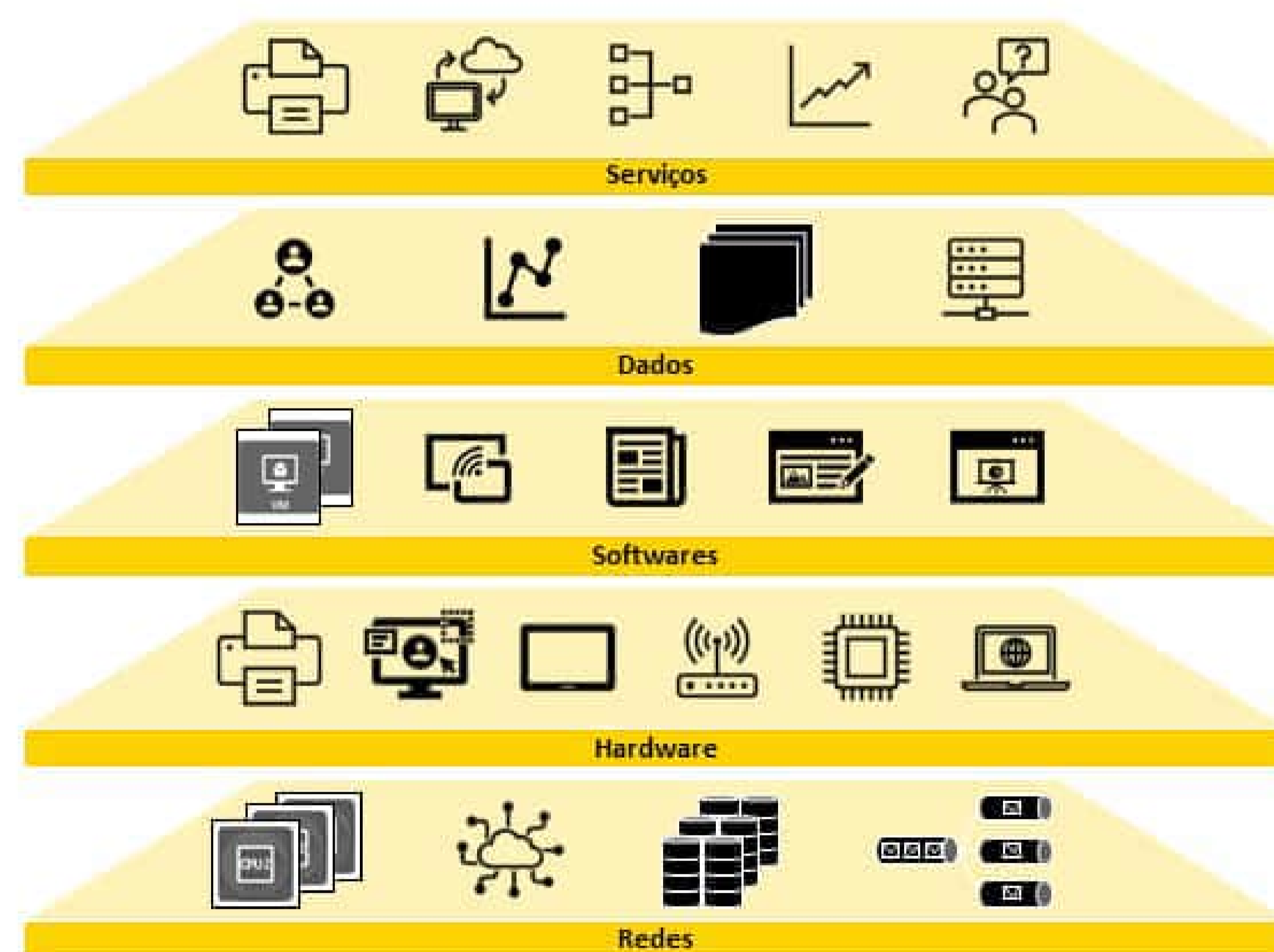
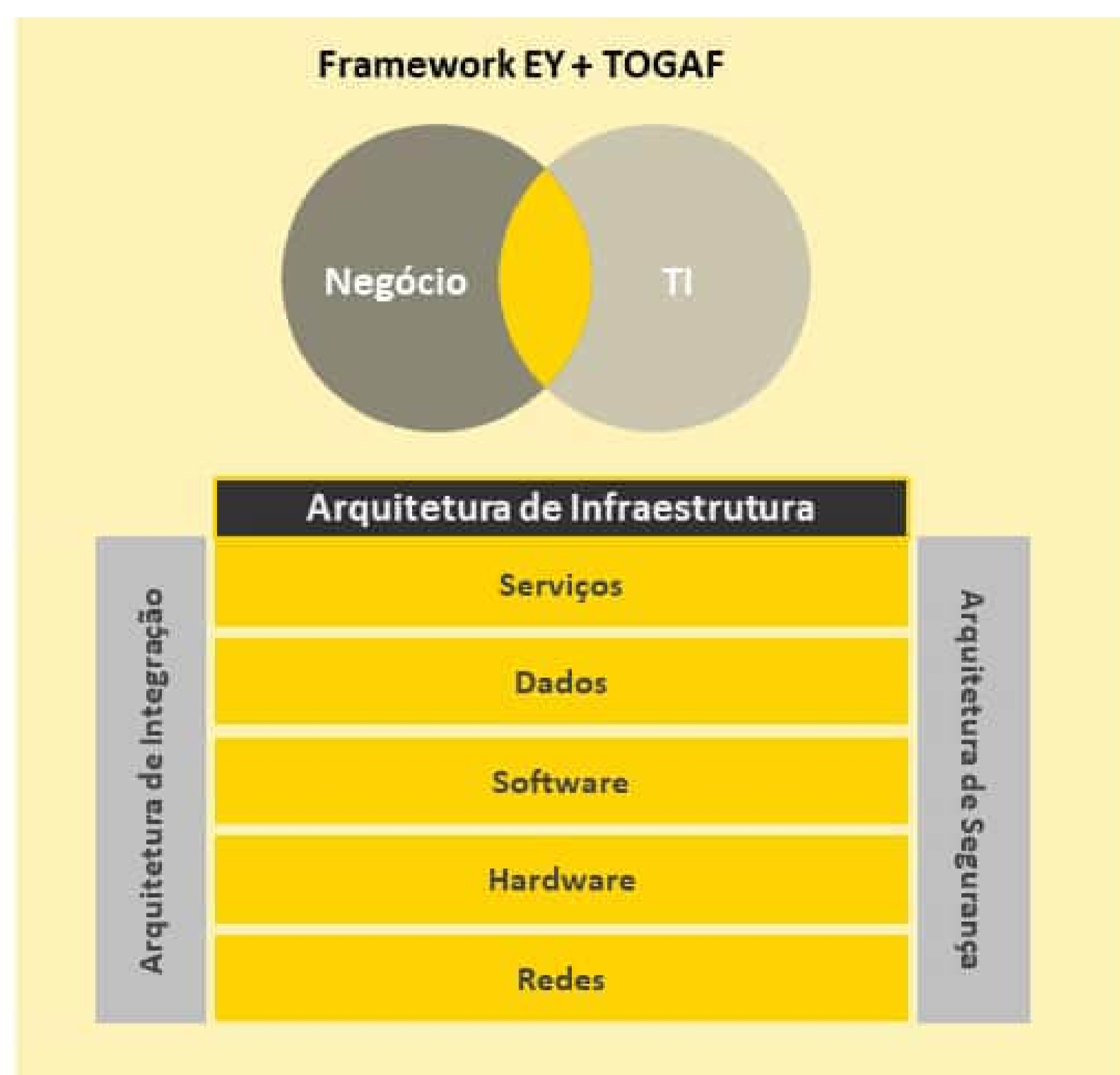


Roadmap



INFRAESTRUTURA

A análise da infraestrutura de TI é realizada utilizando-se metodologia própria EY em conjunto com o TOGAF (The Open Group Architecture Framework). A metodologia consiste na organização da arquitetura corporativa em camadas para que o estado atual do modelo de infraestrutura do SGB seja retratado.



OBJETIVOS

Gerar valor ao Negócio

Alinhamento com as mudanças de Negócio

Racionalização e otimização dos investimentos em tecnologia

Transformação das capacidades em Tecnologia



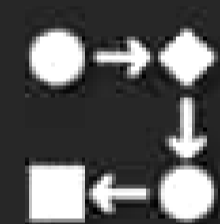
Painel



Estratégia



Pessoas



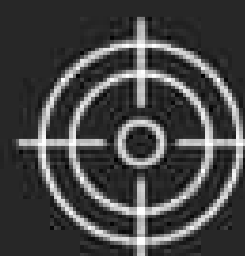
Processos



Tecnologia



Orçamento



Roadmap

INFRAESTRUTURA

Serviços

Dados

Softwares

Hardware

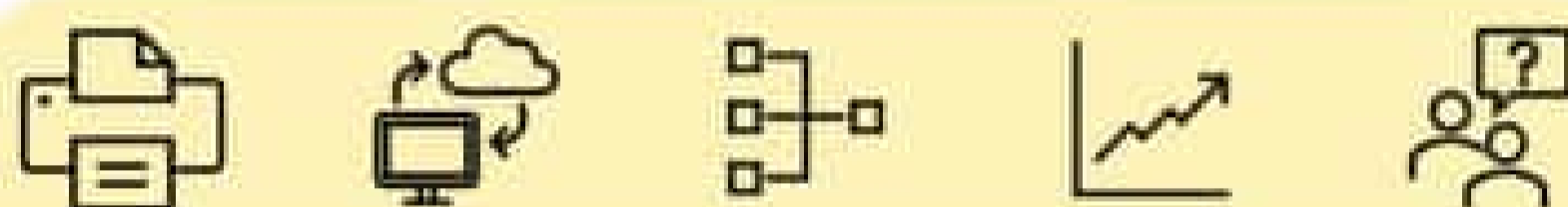
Redes

Resumo

SERVIÇOS

Situação Atual

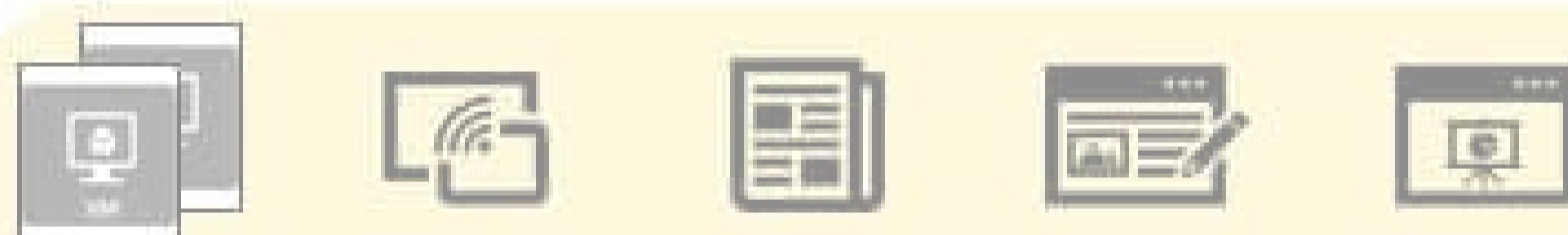
Mapa dos Serviços



Serviços



Dados



Softwares



Hardware



Redes

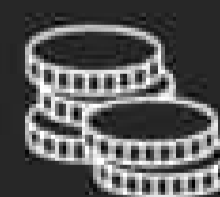
Pontos Identificados

Incidentes: A Central de Atendimento (*service desk*) é terceirizada com a empresa **G&P**. A ferramenta utilizada para a gestão de *tickets* é o **GLPI 4.1.9**.

Monitoramento: Todos os ativos de infraestrutura de TI na Matriz e Filiais são monitorados através da ferramenta **Zabbix**.

Acesso à recursos: Os recursos disponíveis para uso dos colaboradores são: Impressão, links de comunicação, cloud, armazenamento, PC's, laptops, rede interna e telefonia.

Localidades: 01 Sede (Brasília) + 12 regionais



Painel

Estratégia

Pessoas

Processos

Tecnologia

Orçamento

Roadmap

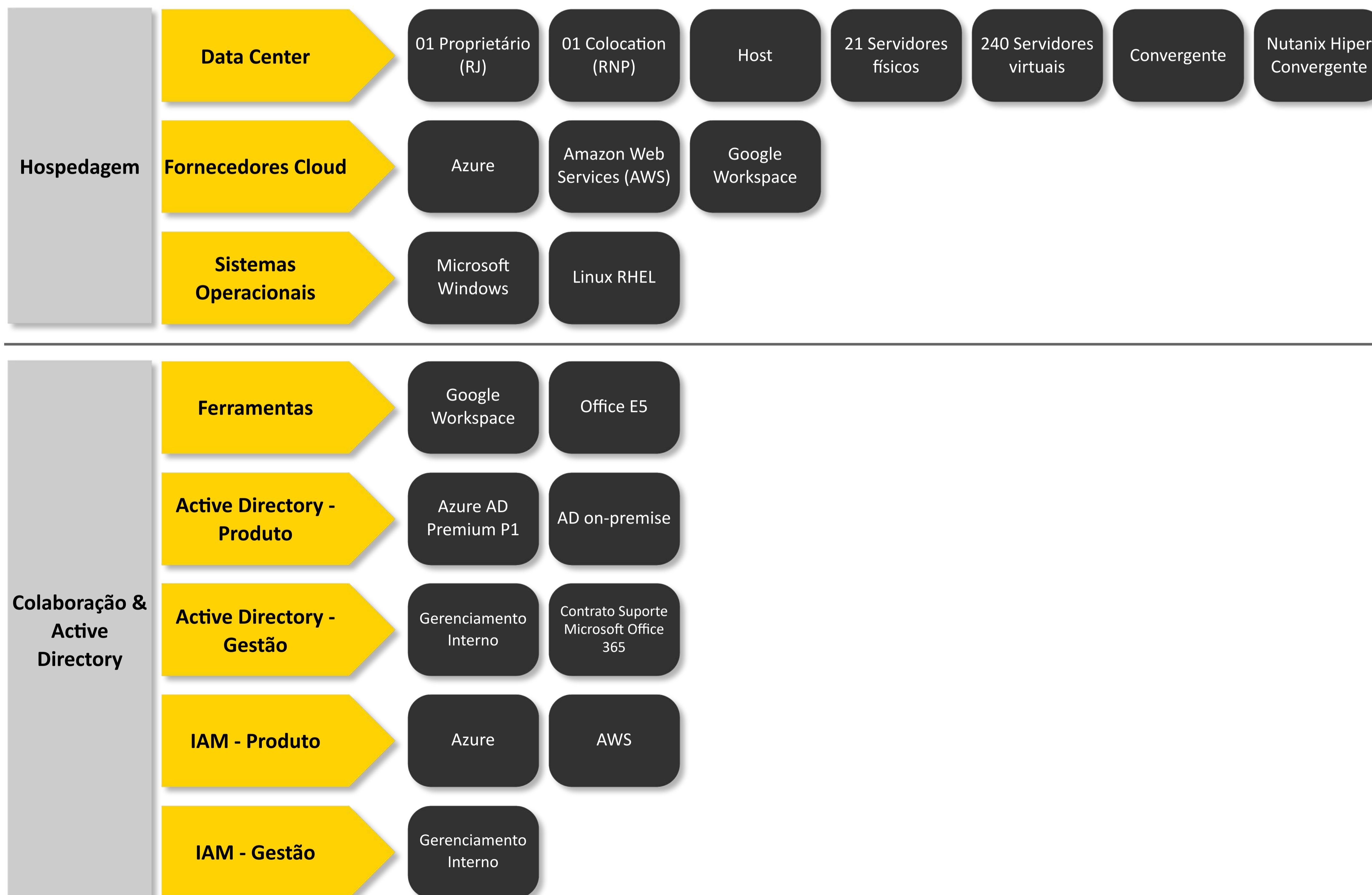
INFRAESTRUTURA

[Serviços](#)
[Dados](#)
[Softwares](#)
[Hardware](#)
[Redes](#)
[Resumo](#)

SERVIÇOS

[Situação Atual](#)
[Mapa dos Serviços](#)

O quadro abaixo exhibe os serviços prestados pela TI atualmente e suas principais características técnicas, classificados de acordo com o framework EY + TOGAF utilizados para análise.





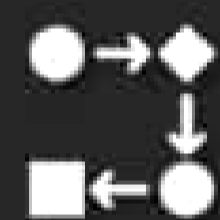
Painel



Estratégia



Pessoas



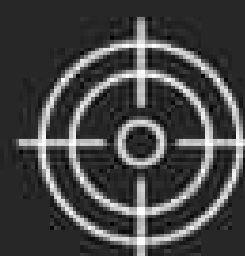
Processos



Tecnologia



Orçamento



Roadmap

INFRAESTRUTURA

Serviços

Dados

Softwares

Hardware

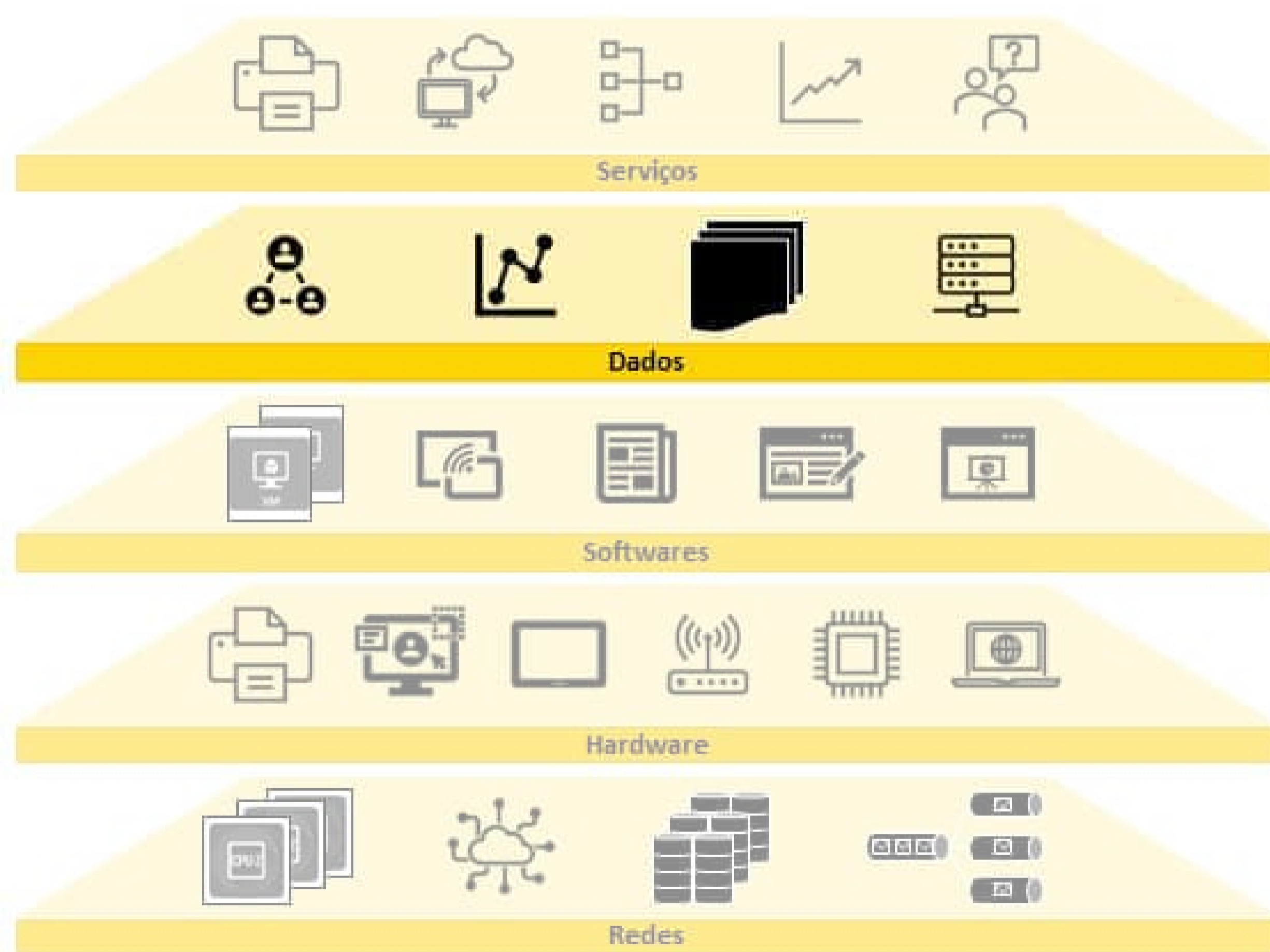
Redes

Resumo

DADOS

Situação Atual

Mapa dos Serviços de Dados



Pontos Identificados

Backup: Política de backup não identificada, assim como a quantidade limite de dados que o **SGB tolera perder em caso de pane ou paralisação** (RPO - *Recovery Point Objective*) e o tempo de recuperação (RTO - *Recovery Time Objective*) dos processos definidos como críticos pela companhia. O Backup é realizado em 2 cópias, sem o uso de fitas, e a infraestrutura possui isolamento (bolha).

Segurança: Solução com foco na prevenção a perdas de dados (DLP - *Data Loss Prevention*) não identificada. Nome padrão do usuário para conta de administrador do Windows não é utilizada.

Planos de Continuidade e Recuperação da TI: Planos de continuidade de negócio e recuperação da TI não identificados.

INFRAESTRUTURA

[Serviços](#)
[Dados](#)
[Softwares](#)
[Hardware](#)
[Redes](#)
[Resumo](#)

DADOS

[Situação Atual](#)
[Mapa dos Serviços de Dados](#)

O quadro abaixo exhibe os serviços de dados prestados pela TI atualmente e suas principais características técnicas, classificados de acordo com o framework EY + TOGAF utilizados para análise.

Plataformas	Backup	Commvault	2 cópias	Backup com infra em bolha	Não há política de backup				
	Armazenamento	14 File Servers On Premise 390TB	Storage EMC e SAN	File Server Windows	Object Storage AWS S3				
Segurança	DLP	Não implementado no ambiente Microsoft							
	Políticas ou filtro	DKIM	DMARC	CASB	Anti-Spoof	Não monitora arquivos com senha e compactados	Inbound e outbound e-mails	SPF	Não há WAF
	Autenticação	Azure MFA	Politica de senha	Administrator padrão Microsoft não usado	Root padrão Linux não usado				
	Anti-vírus e endpoint	SEP							
Infraestrutura	Banco de dados	MongoDB	Oracle	MS SQLServer	Postgre SQL	MariaDB			



Roadmap



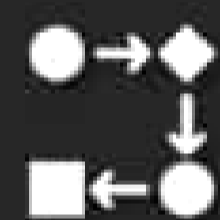
Painel



Estratégia



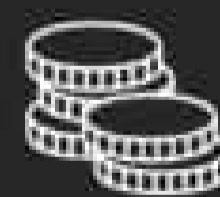
Pessoas



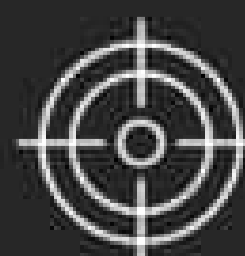
Processos



Tecnologia



Orçamento



Roadmap

INFRAESTRUTURA

Serviços

Dados

Softwares

Hardware

Redes

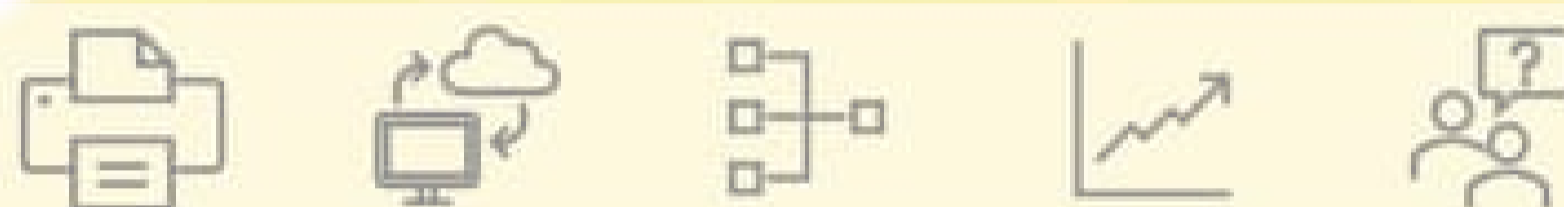
Resumo

SOFTWARES

Situação Atual

Mapa dos Softwares

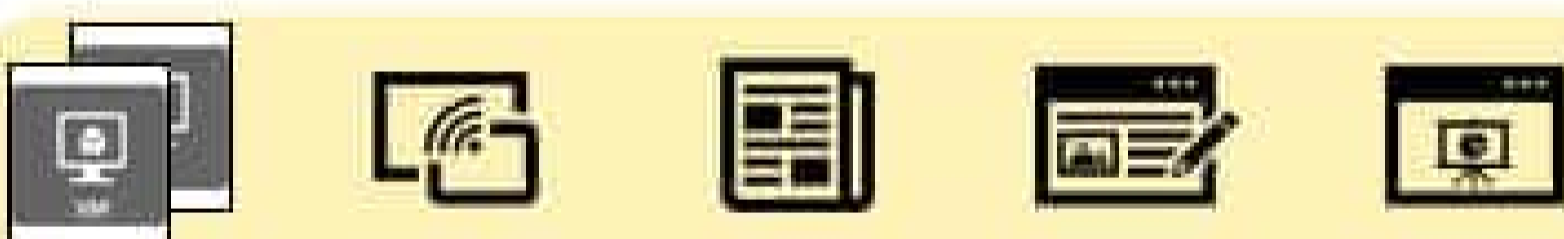
Servidores por SO



Serviços



Dados



Softwares



Hardware



Redes

Pontos Identificados

Licença Office: E3: 10 unidades | PowerBI Pro: 30 unidades.

Azure: O modelo de subscrição adotado é o Office 365 em decorrência da pouca utilização de recursos da cloud. Aplicações específicas utilizam o SSO (*single sign-on*) com o AD local.

Servidores Virtuais:

Ferramenta Virtualização: VMWare Center

Sistema Operacional:

- 130 Servidores Linux
- 110 Servidores Windows

Servidores Físicos:

Sistema Operacional:

- 15 Servidores Linux
- 06 Servidores Windows

Sistemas Operacionais: Servidores com versões Windows Server 2003, 2008, 2012, 2019 e 2022.



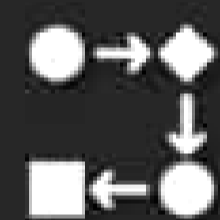
Painel



Estratégia



Pessoas



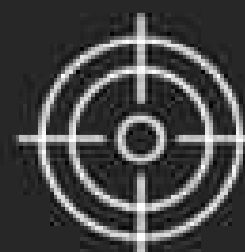
Processos



Tecnologia



Orçamento



Roadmap

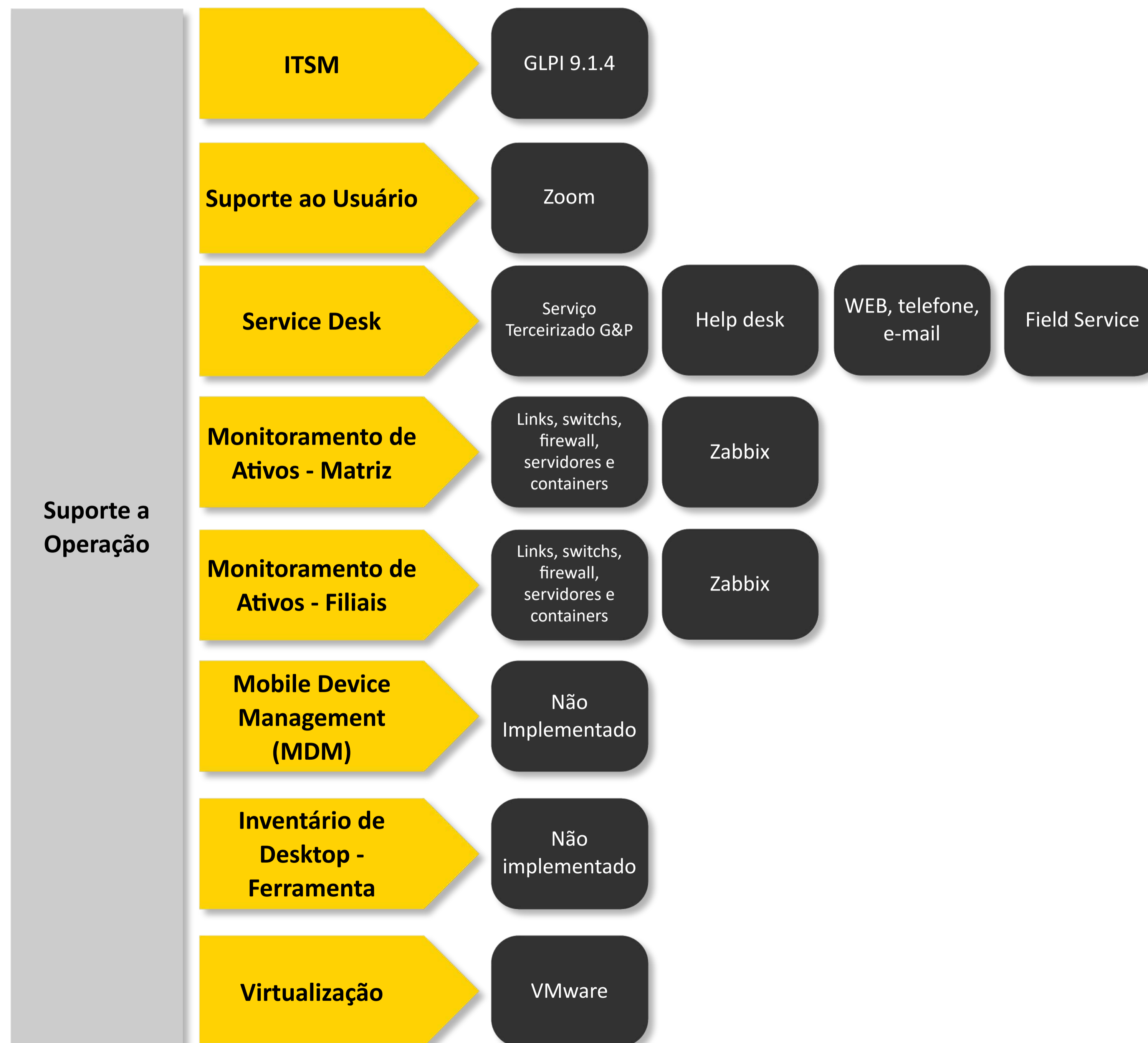
INFRAESTRUTURA

[Serviços](#)
[Dados](#)
[Softwares](#)
[Hardware](#)
[Redes](#)
[Resumo](#)

SOFTWARES

[Situação Atual](#)
[Mapa dos Softwares](#)
[Servidores por SO](#)

O quadro abaixo exibe os softwares utilizados pela TI atualmente e suas principais características técnicas, classificados de acordo com o framework EY + TOGAF utilizados para análise.





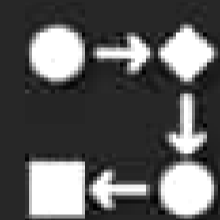
Painel



Estratégia



Pessoas



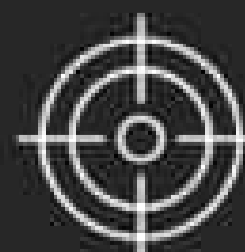
Processos



Tecnologia



Orçamento



Roadmap

INFRAESTRUTURA

Serviços

Dados

Softwares

Hardware

Redes

Resumo

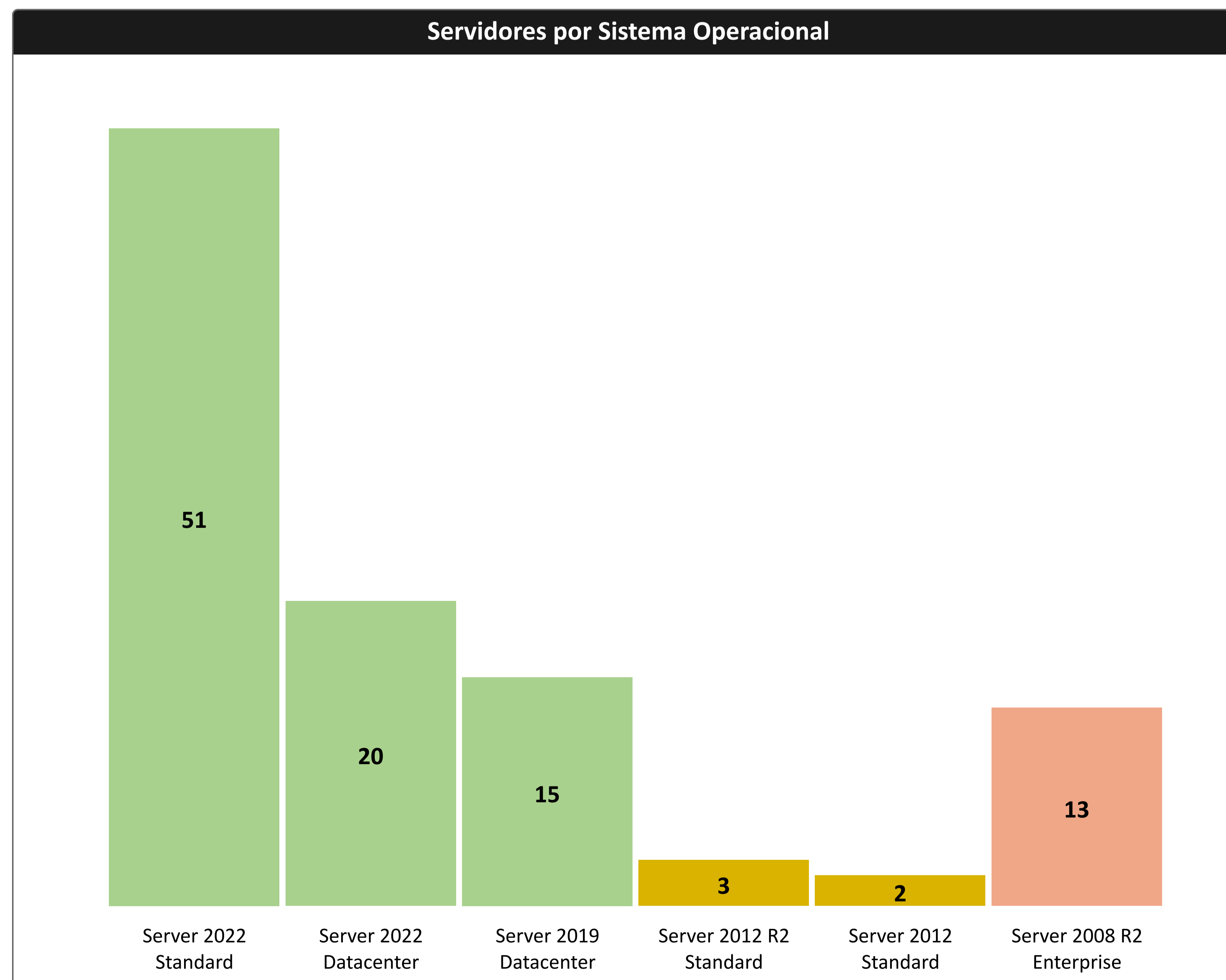
SOFTWARES

Situação Atual

Mapa dos Softwares

Servidores por SO

Servidores por Sistema Operacional



No gráfico ao lado destaca-se em amarelo os servidores que ficarão sem suporte a partir de out/2023. Isso representa, 5% do parque instalado.

O item em vermelho apresenta o Sistema Operacional que está sem suporte desde jan/2020. Isso representa, 12% do parque instalado.



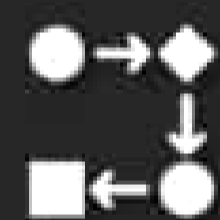
Painel



Estratégia



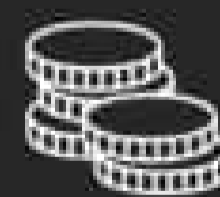
Pessoas



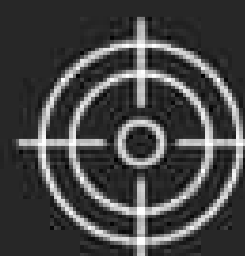
Processos



Tecnologia



Orçamento

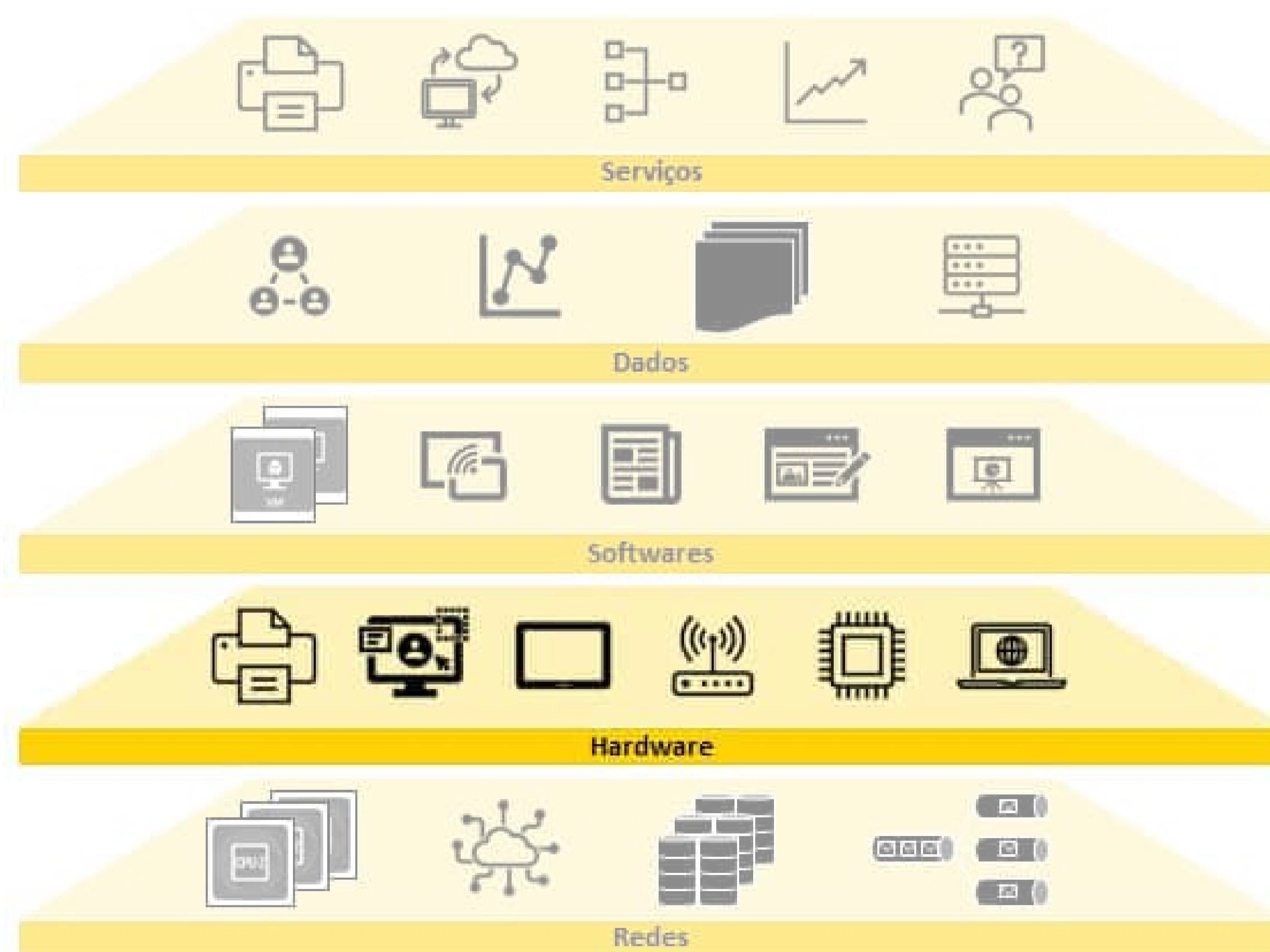


Roadmap

INFRAESTRUTURA

[Serviços](#)
[Dados](#)
[Softwares](#)
[Hardware](#)
[Redes](#)
[Resumo](#)

HARDWARE

[Situação Atual](#)
[Mapa dos Contratos](#)


Pontos Identificados

PC's e Laptops: Predominância do parque de equipamentos com sistema operacional Windows 10 instalado.

Impressoras: A SGB utiliza o modelo de impressoras próprias e locadas em suas unidades.

Servidores de Arquivos:

- 14 servidores distribuídos entre o data center (RJ) e regionais.

Servidores, Switches e Roteadores: Equipamento adquiridos com capital da empresa (CAPEX).

Missão Crítica: Abaixo estão relacionados os ativos de TI classificados como críticos para a operação:

- Servidores: Nutanix (hiperconvergência)
- Switches: Equipamentos Core de rede
- Firewall: Fortinet



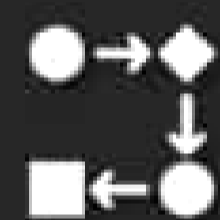
Painel



Estratégia



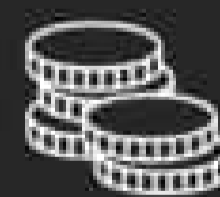
Pessoas



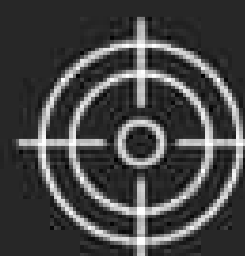
Processos



Tecnologia



Orçamento



Roadmap

INFRAESTRUTURA

Serviços

Dados

Softwares

Hardware

Redes

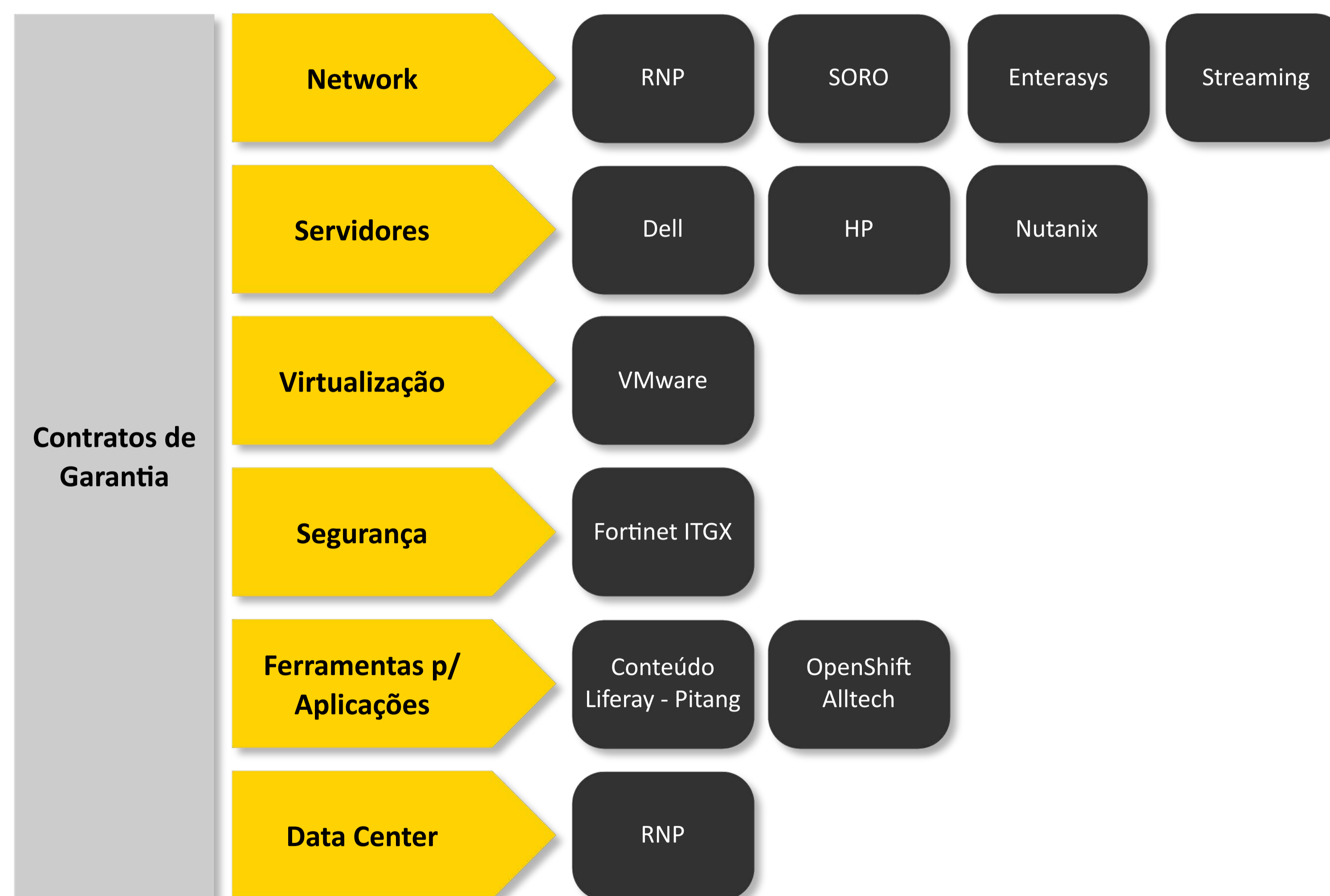
Resumo

HARDWARE

Situação Atual

Mapa dos Contratos

O quadro abaixo exibe os contratos de Hardware utilizados pela TI atualmente e suas principais características técnicas, classificados de acordo com o framework EY + TOGAF utilizados para análise.





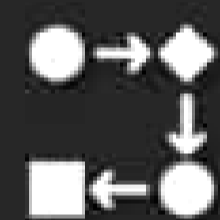
Painel



Estratégia



Pessoas



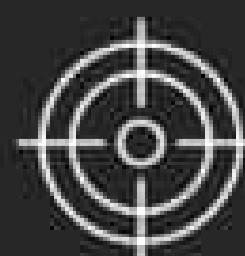
Processos



Tecnologia



Orçamento



Roadmap

INFRAESTRUTURA

Serviços

Dados

Softwares

Hardware

Redes

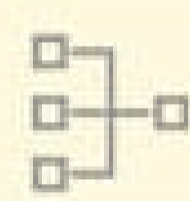
Resumo

REDES

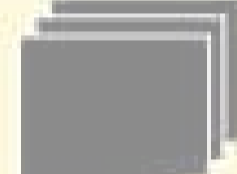
Situação Atual

Mapa de Rede

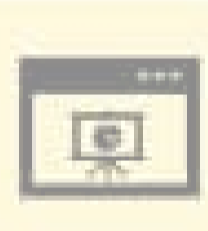
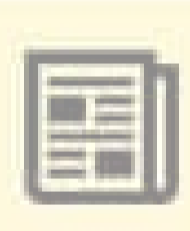
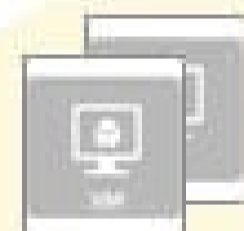
Topologia de Redes



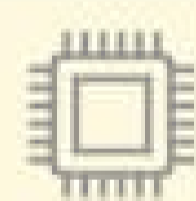
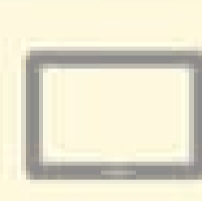
Serviços



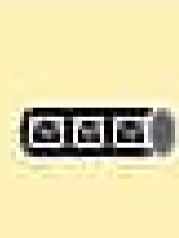
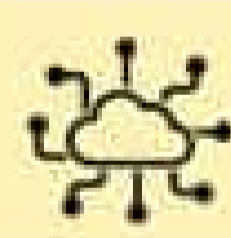
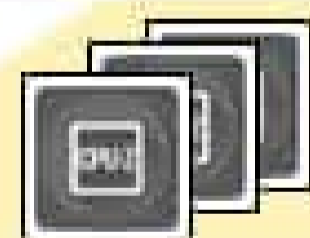
Dados



Softwares



Hardware



Redes

Pontos Identificados

Topologia: A Rede Corporativa utiliza o backbone da RNP e links internet de diferentes provedores para conexão de suas principais unidades. As regionais se conectam a rede RNP através de VPN.

Roteamento: O Datacenter e regionais trocam informações de roteamento através do protocolo BGP.

- Projeto para conexão de cada regional com a cloud, via internet, em andamento. Previsão: 12/2023.

Rede e cloud:

- **AWS/GCP:** A arquitetura atual para acesso aos ambientes **cloud é constituída por VPNs site-to-site** entre o Datacenter e a cloud. Esse trânsito via Datacenter adiciona latência para acesso das regionais, já que não possuem VPN direta.
- **Azure:** Usado apenas para O365. Replicação do AD usando pass-through authentication.

Links: Cada unidade possui apenas 1 link de comunicação. Com isso, não apresenta redundância e/ou balanceamento de carga.

VPN Hub/Spoke: A rede MAN é projetada para centralizar o acesso da seguinte forma:

Data center:

- Caminho Primário: RJ
- Caminho Secundário: Colocation (Brasília)

Regionais:

- Caminho Primário: RJ
- Caminho Secundário: RNP

INFRAESTRUTURA

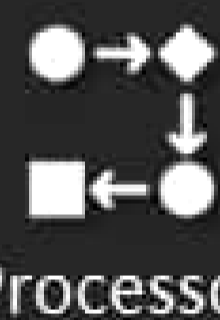
[Serviços](#)
[Dados](#)
[Softwares](#)
[Hardware](#)
[Redes](#)
[Resumo](#)

REDES

[Situação Atual](#)
[Mapa de Rede](#)
[Topologia de Redes](#)

O quadro abaixo exhibe os componentes da rede de dados suportada pela TI atualmente e suas principais características técnicas, classificados de acordo com o framework EY + TOGAF utilizados para análise.

Links de Comunicação	MAN	Não há links MAN	Local -> Provedor Internet -> RNP				
	Intranet	13 links	Não há redundância	Monitoramento ativo			
	Centro de Operações de Rede - NOC	NOC RNP	Não há NOC para infraestrutura	Internet - time interno	Não há SOC e SIEM		
	Monitoramento de Links - Ferramenta	Zabbix					
	Roteamento	Não há SD-WAN	Não há VRF	RNP	BGP	Não apresenta controle de IPs	Não suporta Segment Route
	Operadoras	Local -> RNP					
Wi-Fi	Access Point	Ruckus					
	Controladora	Ruckus (On-premises)	Ruckus (On-premises por região)				
	Analytics	Flexmaster					
Rede	Segurança	Fortigate					
	Data Center	DC (Convergente)	Hiper Convergente				
Plataformas	Telefônica	Avaya	Huawei				
	Vídeo Conferência	Avaya CU360	Avaya XT5000	Google Meet	Avaya Scopia	ConferênciaWeb RNP	Teams



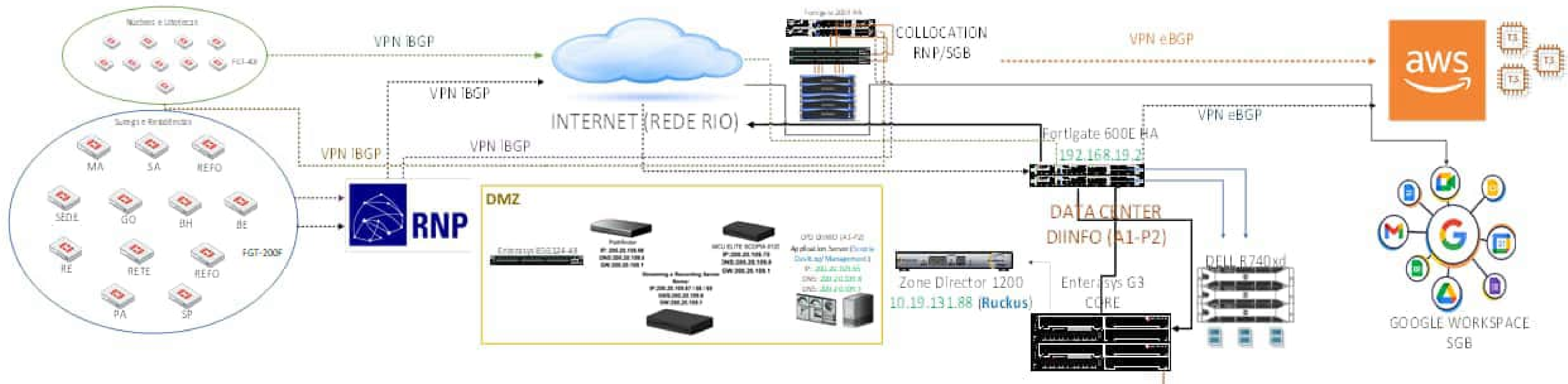
INFRAESTRUTURA

[Serviços](#)
[Dados](#)
[Softwares](#)
[Hardware](#)
[Redes](#)
[Resumo](#)

REDES

[Situação Atual](#)
[Mapa de Rede](#)
[Topologia de Redes](#)

Visão macro da topologia de Rede



Data Center Rio de Janeiro:

Não é permitida a movimentação lateral L2 Isolation/Protected na camada de acesso e L3 ACL entre as Vlans de Usuários na camada Core.

A Rede Wi-Fi também não permite por default a movimentação lateral entre dispositivos por AP.

As Vlans de Servidores (LAN Servers) são segmentadas diretamente no Fortigate 600E, permitindo a aplicação de camadas de segurança mais avançadas no fluxo Cliente/Servidor.

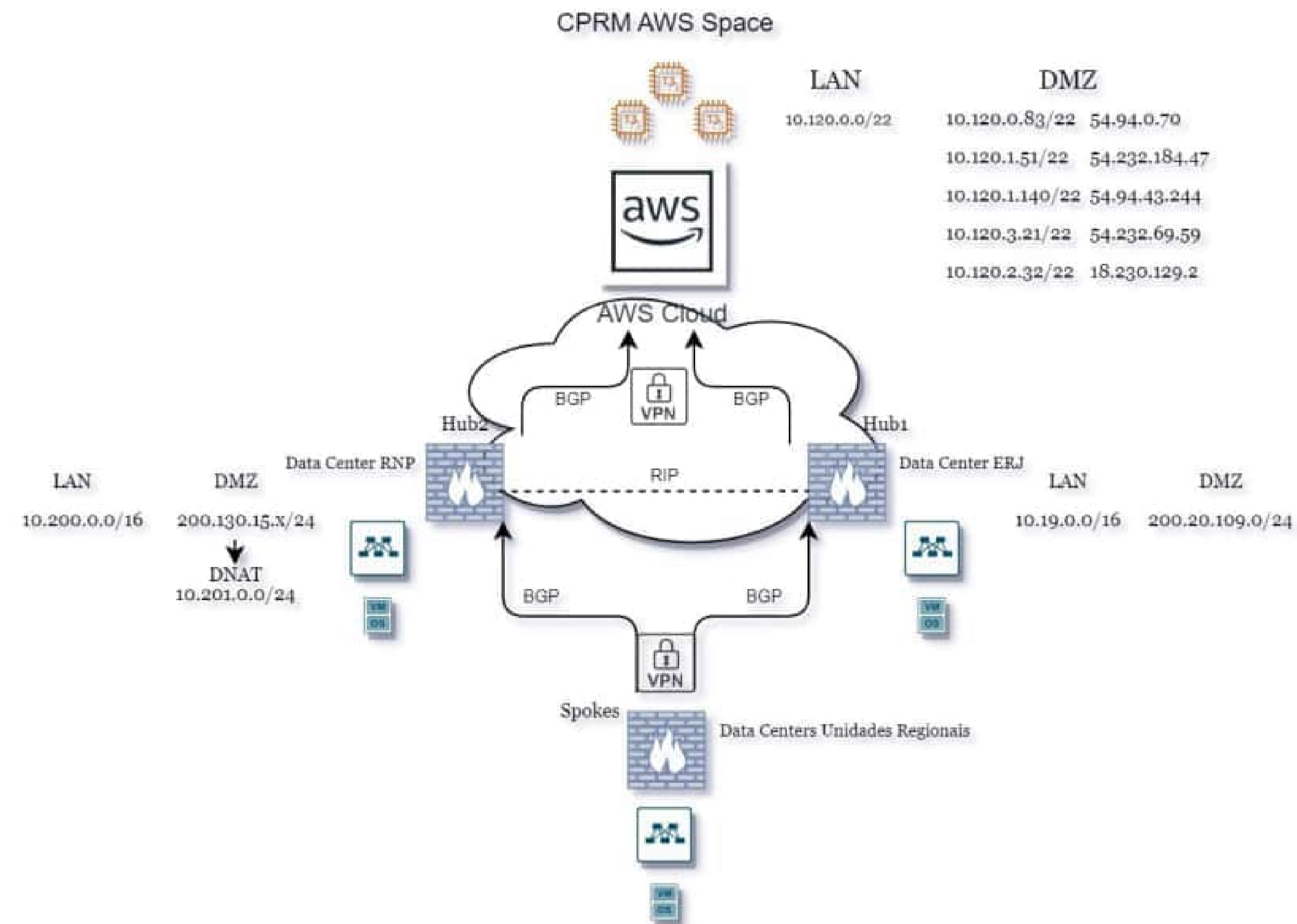
INFRAESTRUTURA

[Serviços](#)
[Dados](#)
[Softwares](#)
[Hardware](#)
[Redes](#)
[Resumo](#)

REDES

[Situação Atual](#)
[Mapa de Rede](#)
[Topologia de Redes](#)

Visão macro da topologia de Rede para acesso a cloud



A topologia atualmente implementada no SGB, conforme figura acima, apresenta 1 conexão internet com 1 fornecedor em cada localidade conectada à rede RNP via VPN.

O acesso a cloud é realizado de forma centralizada, esse trânsito via Datacenter adiciona latência para acesso das regionais já que não possuem VPN direta.

INFRAESTRUTURA

[Serviços](#)
[Dados](#)
[Softwares](#)
[Hardware](#)
[Redes](#)
[Resumo](#)

RESUMO

[Mandala Tecnológica](#)
[Stack Tecnológica](#)

Camada de Redes:

- Não tem Ponto a ponto 13 links MAN VPN;
- 13 links Internet;
- 13 Redes Privadas Virtuais (VPN);
- 13 operadores de telecom;
- Nutanix;
- Wifi Ruckus;
- DC Hiper Convergente.

Camada de Hardware:

- Servidores (HP, Dell, Nutanix);
- Armazenamento em Disco (EMC, SAN);
- Dispositivos de Rede (Juniper, Huawei);
- Dispositivos de Segurança (Fortinet, Akamai);
- Dispositivos de Acesso (Dell, HP, Smartphones).

Camada de Serviços:

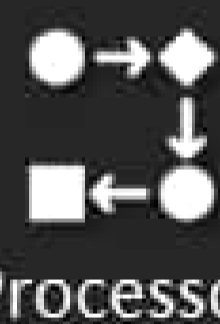
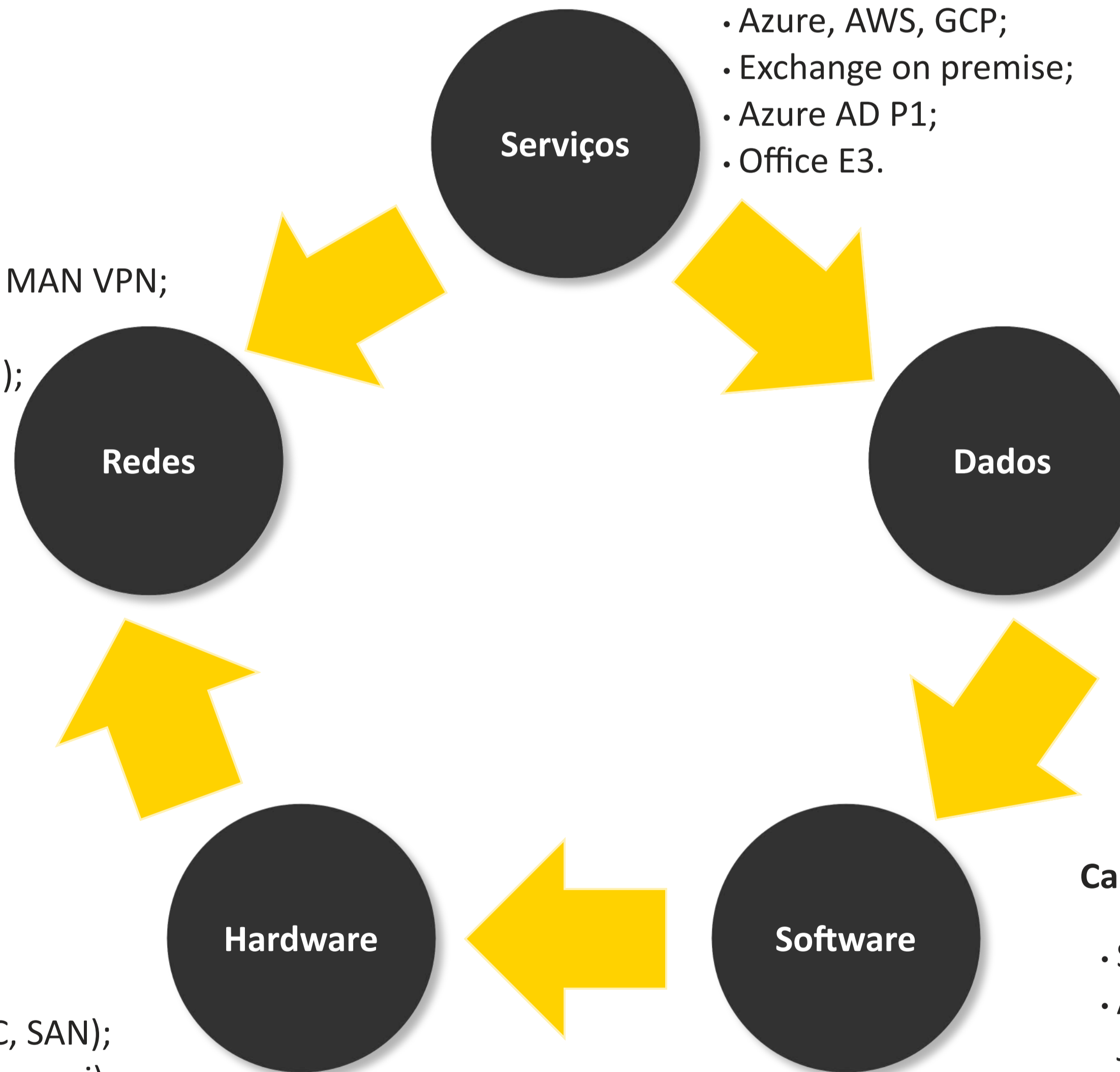
- 1 Data Center -> RNP;
- Cloud;
- Azure, AWS, GCP;
- Exchange on premise;
- Azure AD P1;
- Office E3.

Camada de Dados:

- Bancos de Dados Relacionais (Oracle, SQL Server, Postgre, MariaDB);
- Bancos de Dados NoSQL (MongoDB);
- 14 file servers, GCP file server, Objetos Storages AWS e IBM;
- AWS S3 backup, 2 cópias, Nutanix VM's, Commvault.
- SEP, MFA, Anti-Spoof

Camada de Software:

- Sistemas Operacionais (Windows, RHEL);
- Aplicações de Produtividade (Microsoft Office, Jira);
- GLPI 9.1.4, Zoom, Zabbix;
- Vmware.



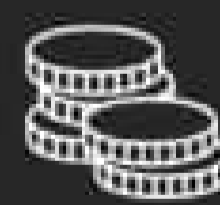
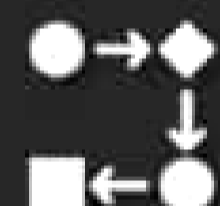
INFRAESTRUTURA

[Serviços](#)
[Dados](#)
[Softwares](#)
[Hardware](#)
[Redes](#)
[Resumo](#)

RESUMO

[Mandala Tecnológica](#)
[Stack Tecnológica](#)

Camada	Componentes										
Serviços	2 Data Centers	Azure Office	Amazon Web Services (AWS)	Google Workspace	AD on-premise	Azure AD Premium P1	Office E5				
Dados	14 File Servers On Premise	Storage EMC	File Server Windows	Banco de dados	AWS S3	Commvault	Data Protector				
Softwares	GLPI	Zoom	Zabbix	VMware							
Hardware	Dell	Nutanix	SORO	Enterasys	HP	Fortinet					
Redes	Não há links MAN	13 Links Internet	Operadoras de telecom regionais	Não há SD-WAN	Não há VRF	VPN	BGP	Wifi Rukus	DC (Hiper Convergente)	Avaya	Não há balanceador



Painel

Estratégia

Pessoas

Processos

Tecnologia

Orçamento

Roadmap

DIRECIONADORES PARA INFRAESTRUTURA FUTURA

Serviços

Dados

Softwares

Hardware

Redes

Oportunidades

As diretrizes de arquitetura de Infraestrutura foram elaboradas com base no diagnóstico da sua situação atual e nas informações coletadas com a TI durante a fase de entrevistas, onde foram identificados importantes pontos de melhorias e mudanças. As diretrizes que balizam a visão futura de arquitetura da infraestrutura foram elaboradas para impulsionar que a estratégia de TI seja alcançada.

AGILIDADE



Usar recursos e processos que possibilitam agilidade nas atividades de manutenção e suporte de infraestrutura.

CUSTO



Eficiência no uso dos recursos de infraestrutura e na forma como a área de TI se organiza para suportar esses recursos.

DESEMPENHO



Utilização de tecnologias que viabilizam alta performance da infraestrutura, em aderência aos requisitos da empresa.

AUTOMAÇÃO



Simplificação da operação de TI, por meio de recursos que consigam automatizar as atividades de rotina no suporte de infraestrutura por meio configurações e orquestração.

ESCALABILIDADE



Possibilidade de adequar a capacidade de infraestrutura à escala necessária com facilidade.

RESILIÊNCIA



Disponibilidade e continuidade dos recursos de infraestrutura aderentes aos requisitos de risco da empresa.



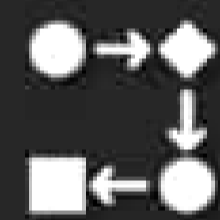
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

DIRECIONADORES PARA INFRAESTRUTURA FUTURA

Serviços

Dados

Softwares

Hardware

Redes

Oportunidades

CLOUD

Cloud

Landing Zone

Hub/Spoke

FinOps

DevOps

A Jornada *cloud* na empresa deve ser iniciada e continua, transferindo serviços e aplicações ainda instalados em servidores próprios, serviços de *hosting*, *colocation*, centralizando em provedor único, objetivando a simplificação da sustentação, maior resiliência e eficiência tecnológica. A consolidação deve ser orientada pelas aplicações e serviços, movendo ou reinstalando em um novo Tenant/Conta/Assinatura. Em caso de incompatibilidade com as tecnologias, a aplicação ou serviço deve ter a sua viabilidade de substituição testada por um estudo de caso. Requisitos da rede WAN devem ser considerados nesta consolidação, de modo a dimensionar a capacidade dos *links* necessária para performance dos usuários nos ambientes *cloud*.

Principais componentes de uma jornada bem-sucedida para a nuvem:



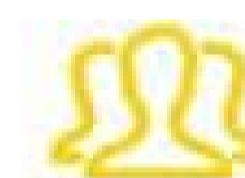
Alinhamento Estratégico / Criação de Valor

- Desenvolver estratégia de nuvem adaptável, incluindo plataformas, dados, engenharia de software, risco.
- Alinhar com as prioridades de negócios e o resultado esperado (experiência do cliente, melhorias de receita, ganhos de produtividade e economia de custos)
- Documentar o caso de negócios para mudança
- Realizar modelagem de valor (TCC/TCO/ROI)



Prontidão do Aplicativo

- Desenvolver uma estrutura subjacente para a seleção estratégica de aplicativos para maximizar o ROI
- Padronizar padrões de design para adequação à nuvem
- Implementar ferramentas de CI/CD
- Otimizar aplicativos para dimensionamento horizontal
- Analisar modelos de dados comuns



Pessoas, Cultura e Mudança

- Definir as habilidades necessárias para habilitar o ambiente de nuvem
- Empregar os princípios do espaço de trabalho digital
- Capacitar os funcionários por meio da autonomia
- Construir uma cultura de aprendizagem contínua e orientada por propósitos
- Injetar valores inovadores compartilhados
- Definir mecanismos de feedback de fluidos



Abordagem robusta

- Abordar de forma simples a migração rápida para a nuvem
- Desenvolver manuais, padrões e práticas recomendadas da fábrica de migração
- Realizar lançamento em pequena escala para prova de conceito
- Garantir o patrocínio executivo e o alinhamento para a eficácia da adoção e a realização dos benefícios



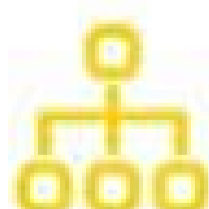
Estrutura de padrões de design

- Definir padrões para infraestrutura como código
- Definir padrões de gerenciamento de capacidade
- Desenvolver o processo de colocation e abstração de dados
- Aproveitar os padrões de arquitetura de data lake/hub
- Conectividade do arquiteto entre ambientes de nuvem



Automação / DevSecOps

- Otimizar a adoção da nuvem com automação avançada e DevOps
- os processos de lançamento e implantação
- Segmentar um estado final NoOps com PaaS



Modelo operacional de nuvem

- Desenvolver funções, responsabilidades e capacitação claras
- Reconhecer o valor do gerenciamento de fornecedores, coordenação de engajamento de nuvem
- Reconhecer o valor crítico da arquitetura



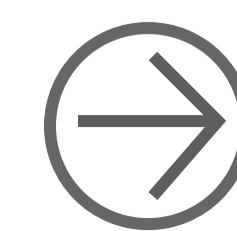
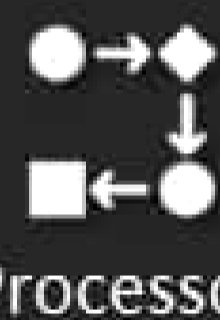
Nuvem Viável Mínima e Cargas de Trabalho Iniciais

- Desenvolver padrões de design personalizados e modelos associados de Infraestrutura como Código (IAC)
- Desenvolver listas de verificação pré e pós-migração
- Realizar shakeout, validação de dados, desempenho, garantia de qualidade, failover e testes de integração



Segurança, Risco, Conformidade

- Adotar os padrões de segurança do setor
- Definir princípios de risco distribuído
- Dados seguros por meio de protocolos de proteção de dados
- Implementar estrutura de governança de nuvem
- Revise os padrões de regulamentação e conformidade



DIRECIONADORES PARA INFRAESTRUTURA FUTURA

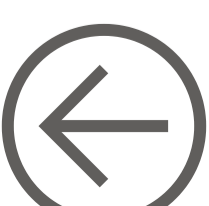
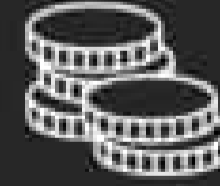
[Serviços](#)
[Dados](#)
[Softwares](#)
[Hardware](#)
[Redes](#)
[Oportunidades](#)

SERVIÇOS CLOUD x FORNECEORES

[Cloud](#)
[Landing Zone](#)
[Hub/Spoke](#)
[FinOps](#)
[DevOps](#)

A tabela abaixo apresenta os serviços padrões de 3 fornecedores de cloud com maior aderência do mercado.

Serviço	Azure	AWS	GCP
Administration	Azure Active Directory	AWS Identity and Access Management	Cloud Identity
AI and Machine Learning	Azure Machine Learning	Amazon SageMaker	AI Platform
Analytics	Stream Analytics	Kinesis	Dataflow
API Management	Azure API Management	Amazon API Gateway	Apigee
App Hosting	App Service	Elastic Beanstalk	App Engine
Automation	Azure Automation	AWS Systems Manager	Cloud Scheduler
Backup and Recovery	Azure Backup	AWS Backup	Cloud Backup
Big Data	HDInsight	Elastic MapReduce	Dataproc
Block Storage	Azure Disk Storage	Amazon EBS	Compute Engine Persistent Disks
Blockchain	Azure Blockchain Workbench	Amazon Managed Blockchain	Blockchain
Cloud Management	Azure Resource Manager	AWS CloudFormation	Cloud Deployment Manager
Compute Services	Virtual Machines	Elastic Compute Cloud	Compute Engine
Container Support	Azure Kubernetes Service	Amazon ECS, EKS, Fargate	Google Kubernetes Engine (GKE)
Content Delivery	Azure CDN	Amazon CloudFront	Cloud CDN
Database	Azure SQL Database	Amazon RDS	Cloud SQL
Desktop and App Streaming	Azure Virtual Desktop	Amazon WorkSpaces	AppStream 2.0
DevOps	Azure DevOps Services	AWS CodePipeline	Cloud Build
DNS Services	Azure DNS	Amazon Route 53	Cloud DNS
HPC and High Performance	Azure HPC Cache	Amazon Elastic Fabric Adapter	
IoT	IoT Hub	AWS IoT Core	IoT Core
Load Balance	Azure Load Balancer	Elastic Load Balancing	Cloud Load Balancing
Log Monitoring	Azure Log Analytics	Amazon CloudWatch	Stackdriver Logging
Management Services	Azure Monitor	AWS Management Console	Cloud Console
Messaging	Azure Service Bus	Amazon Simple Notification Service	Cloud Pub/Sub
Mobile	Azure Mobile Apps	AWS Mobile	Firebase
Monitoring	Azure Application Insights	Amazon CloudWatch	Cloud Monitoring
NoSQL Database Options	Azure Cosmos DB	Amazon DynamoDB	Cloud Firestore, Cloud Bigtable
Object Storage	Azure Blob Storage	Amazon S3	Google Cloud Storage
Private Connectivity	Azure ExpressRoute	AWS Direct Connect	Cloud Interconnect
Regions	60+ regions	24 regions	26 regions
Scaling Options	Autoscale	Auto Scaling	Autoscaling
Security	Azure Security Center	Amazon GuardDuty	Cloud Security Command
Serverless Computing	Azure Functions	AWS Lambda	Cloud Functions
Virtual Network	Virtual Network	Virtual Private Cloud	Virtual Private Cloud (VPC)



DIRECIONADORES PARA INFRAESTRUTURA FUTURA

Serviços

Dados

Softwares

Hardware

Redes

Oportunidades

LANDING ZONE

Cloud

Landing Zone

Hub/Spoke

FinOps

DevOps

Uma landing zone é a saída de um ambiente com várias assinaturas que leva em conta a escala, a governança de segurança, a rede e a identidade. A landing zone permite a migração, modernização e a inovação de aplicativos em escala empresarial. Essa abordagem considera todos os recursos da plataforma necessários para dar suporte ao portfólio de aplicativos e não diferencia entre infraestrutura como serviço (IaaS) ou plataforma como serviço (PaaS). Uma landing zone é um ambiente para hospedar suas cargas de trabalho, pré-provisionadas por meio de código. Existem dois tipos de landing zone:

Landing Zone da plataforma: Assinaturas implantadas para fornecer serviços centralizados, geralmente operados por uma equipe central, ou várias equipes centrais divididas por função (por exemplo, rede, identidade), que serão usadas por várias cargas de trabalho e aplicativos. As zonas de aterrissagem da plataforma representam serviços-chave que geralmente se beneficiam da consolidação para eficiência e facilidade de operações.

Landing Zone do aplicativo: uma ou mais assinaturas implantadas como um ambiente para um aplicativo ou carga de trabalho. Os aplicativos são colocados em grupos de gerenciamento como "corp" ou "online" abaixo do grupo de gerenciamento de "landing zone" para garantir que os controles de política sejam aplicados corretamente.

05 princípios de design para migração ou novas implantações de aplicativos:

- 1- Democratização da assinatura
- 2- Governança orientada por políticas
- 3- Plano único de controle e gerenciamento
- 4- Centrado na aplicação e arquétipo neutro
- 5- Alinhe o design e o roteiro nativos do Azure

Além disso, o Enterprise-Scale lista diretrizes de design e recomendações. Essas 8 áreas de design ajudarão a companhia a lidar com a incompatibilidade entre o data center local e a infraestrutura de design em nuvem. Não se faz necessário a implementação de todas as recomendações de design, desde que o modelo definido esteja alinhado aos 05 princípios de design listados acima. As 8 áreas de design são:

- 1- Registro do Enterprise Agreement (EA) e Tenant do Azure Active Directory
- 2- Gerenciamento de identidade e acesso
- 3- Grupo de gerenciamento e organização de assinaturas
- 4- Topologia de rede e conectividade
- 5- Gerenciamento e monitoramento
- 6- Continuidade de negócios e recuperação de desastres
- 7- Segurança, governança e conformidade
- 8- Automação de plataforma e DevOps



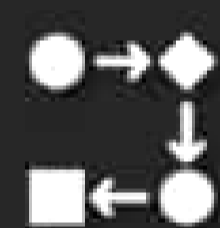
Painel



Estratégia



Pessoas



Processos



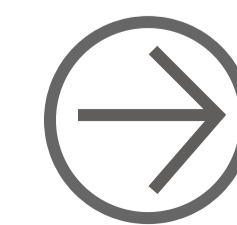
Tecnologia



Orçamento



Roadmap



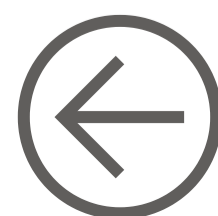
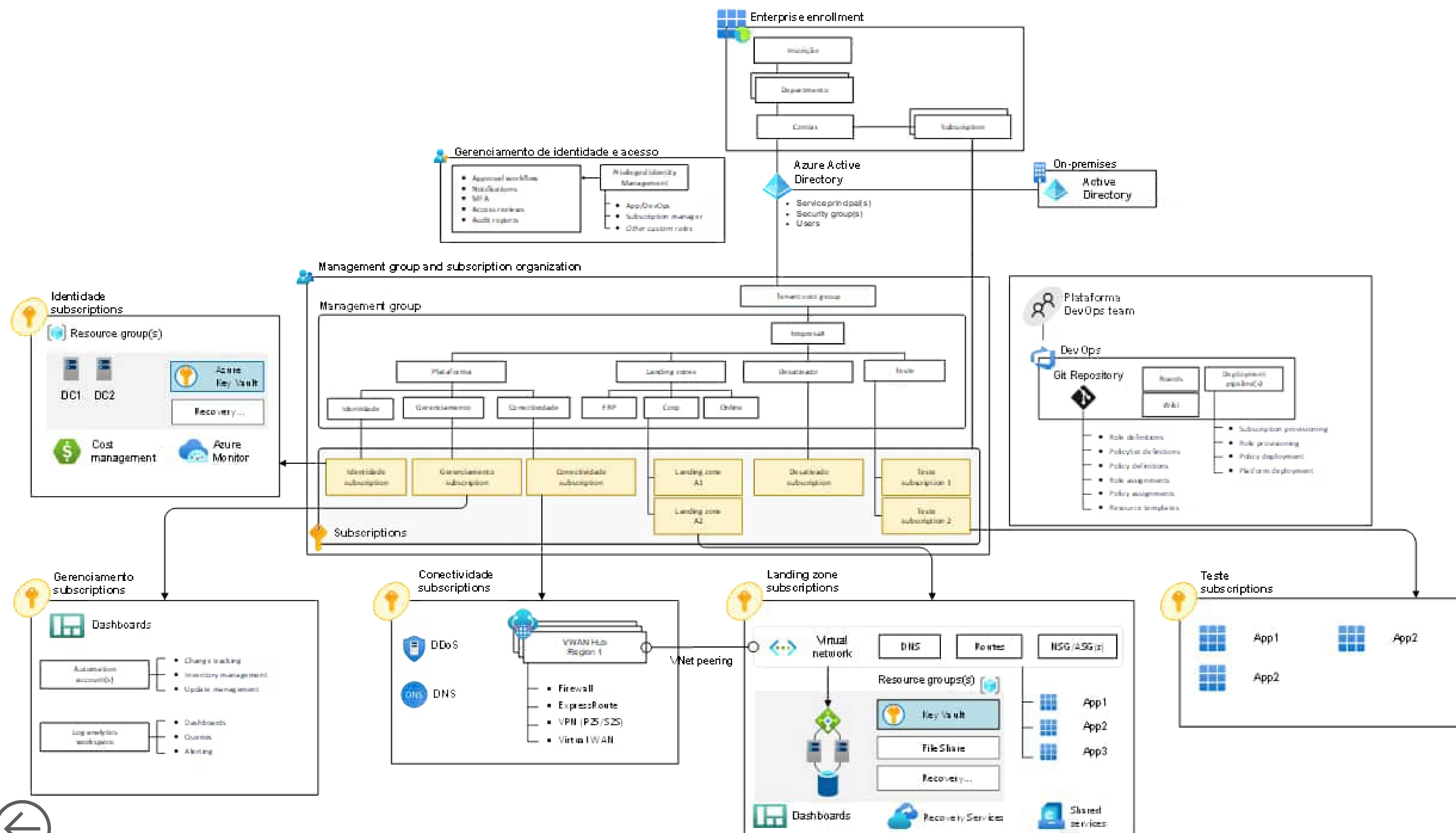
DIRECIONADORES PARA INFRAESTRUTURA FUTURA

[Serviços](#)[Dados](#)[Softwares](#)[Hardware](#)[Redes](#)[Oportunidades](#)

LANDING ZONE

[Cloud](#)[Landing Zone](#)[Hub/Spoke](#)[FinOps](#)[DevOps](#)

Abaixo é apresentado um framework para adoção de operação em cloud chamado de landing zone.



DIRECIONADORES PARA INFRAESTRUTURA FUTURA

Serviços

Dados

Softwares

Hardware

Redes

Oportunidades

HUB/SPOKE

Cloud

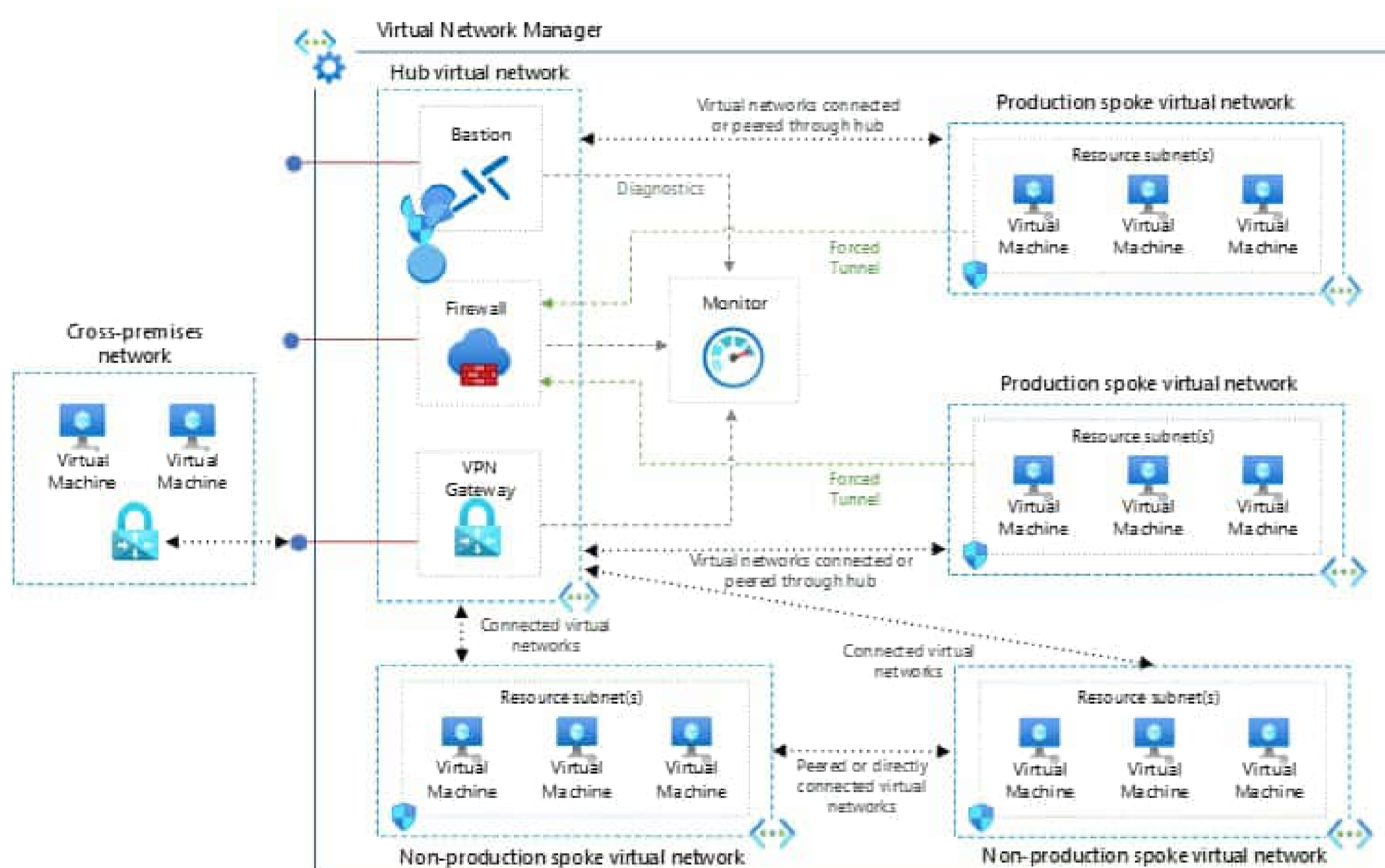
Landing Zone

Hub/Spoke

FinOps

DevOps

Usar uma arquitetura de rede hub/spoke no ambiente cloud é importante para segurança, pois permite uma gestão centralizada do tráfego de rede e acesso aos recursos da cloud, além de garantir a separação lógica entre ambientes. Com a rede hub/spoke, é possível definir políticas de segurança, monitorar e auditar o tráfego de rede e implementar recursos de proteção contra ameaças de forma mais eficiente. Isso ajuda a mitigar riscos e proteger os dados e recursos da empresa na cloud. Além disso, a arquitetura hub/spoke também facilita a escalabilidade e o gerenciamento da infraestrutura de rede na cloud.



Rede virtual hub: A rede virtual do hub hospeda serviços compartilhados. As cargas de trabalho hospedadas nas redes virtuais spoke podem usar esses serviços. A rede virtual do hub é o ponto central de conectividade para redes entre locais.

Redes virtuais spoke: As redes virtuais spoke isolam e gerenciam cargas de trabalho separadamente em cada spoke. Cada carga de trabalho pode incluir várias camadas, com várias sub-redes conectadas por meio de balanceadores de carga. Os spokes podem existir em assinaturas diferentes e representar ambientes diferentes, como Produção e Não produção.

Conectividade da rede virtual: Essa arquitetura conecta redes virtuais usando conexões de emparelhamento ou grupos conectados. Conexões de emparelhamento e grupos conectados são conexões não transitivas e de baixa latência entre redes virtuais. Redes virtuais emparelhadas ou conectadas podem trocar o tráfego pelo backbone do Azure sem precisar de um roteador.

Host do Bastion: fornece conectividade segura do portal para VMs. Um host do Bastion implantado dentro de uma rede virtual pode acessar VMs nessa rede virtual ou em redes virtuais conectadas.

Firewall: Existe uma instância de firewall gerenciada em sua própria sub-rede.

Gateway de VPN ou ExpressRoute: Um gateway de rede virtual permite que uma rede virtual se conecte a um dispositivo VPN (rede virtual privada) ou a um circuito do ExpressRoute. O gateway fornece conectividade de rede entre locais.

Dispositivo VPN: pode ser um dispositivo de hardware ou uma solução de software, como o RRAS no Windows Server.

DIRECIONADORES PARA INFRAESTRUTURA FUTURA

[Serviços](#)
[Dados](#)
[Softwares](#)
[Hardware](#)
[Redes](#)
[Oportunidades](#)

SERVIÇOS - FinOps

[Cloud](#)
[Landing Zone](#)
[Hub/Spoke](#)
[FinOps](#)
[DevOps](#)

Cloud FinOps é a prática de gerenciamento financeiro na nuvem. Requer trabalho em equipe multifuncional para identificar a compensação ideal entre custo, velocidade e agilidade, que é um equilíbrio guiado pelas necessidades estratégicas e táticas do negócio. Existem três principais impulsionadores de negócios para a adoção de FinOps, a saber, redução de gastos com nuvem, gerenciamento de custos em várias nuvens e forte demanda dos clientes para remover o desperdício de nuvem. Cloud FinOps também chamado de Cloud Financial Engineering, Cloud Optimization, Cloud Cost Management, Cloud Cost Optimization e Cloud Financial Optimization.

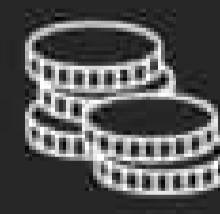
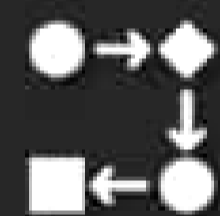
Domínios & Capacidades

Compreender o custo e a utilização de cloud	Acompanhamento do desempenho e Benchmarking	Tomada de decisão em tempo real	Otimização da taxa de cloud	Otimização da utilização de cloud	Alinhamento Organizacional
Alocação de custo	Avaliação de custos unitários	Gestão de crise	Gestão de descontos baseados em comprometimento	Cargas de trabalho integradas	Implementação da cultura FinOps
Análise de dados e showback	Projeção	Estabelecer uma estrutura de decisão e responsabilização de FinOps		Utilização de recursos e eficiência	Integração financeira & Chargeback
Gestão de custos compartilhados	Gestão do orçamento			Gestão do volume de trabalho e automação	Formação e capacitação em FinOps
Inclusão e normalização de dados					Política e governança cloud
					FinOps e colaboração com outros frameworks

Copyright 2019-2023 FinOps Foundation - All rights reserved.

O Cloud FinOps é definido em três fases e cinco blocos de construção, conforme apresentado na tabela abaixo:

INFORMAR		OTIMIZAR		OPERAR
Entender totalmente o custo empregado	Avaliação comparativa de desempenho	Tomada de decisão em tempo real	Estimar, planejar e adquirir capacidade	Colaboração entre TI, finanças e LoB
Visibilidade das despesas de TI	Análise de tendências e desvios	Localizar e eliminar serviços subutilizados	Redimensionar instâncias e serviços	As finanças avançam na velocidade da TI
Alocação detalhada de custos	Avaliação comparativa da equipe interna	Compreender se os recursos estão sub ou superprovisionados	Processo de compra de Reserva de instância centralizado	Melhoria contínua para eficiência e inovação
Orçamentos e acompanhamento ao nível de pessoal	Avaliação comparativa entre pares da mesma área	Automatizar recursos	Comparar preços	Definir governança e controles para a utilização da nuvem



Roadmap

DIRECIONADORES PARA INFRAESTRUTURA FUTURA

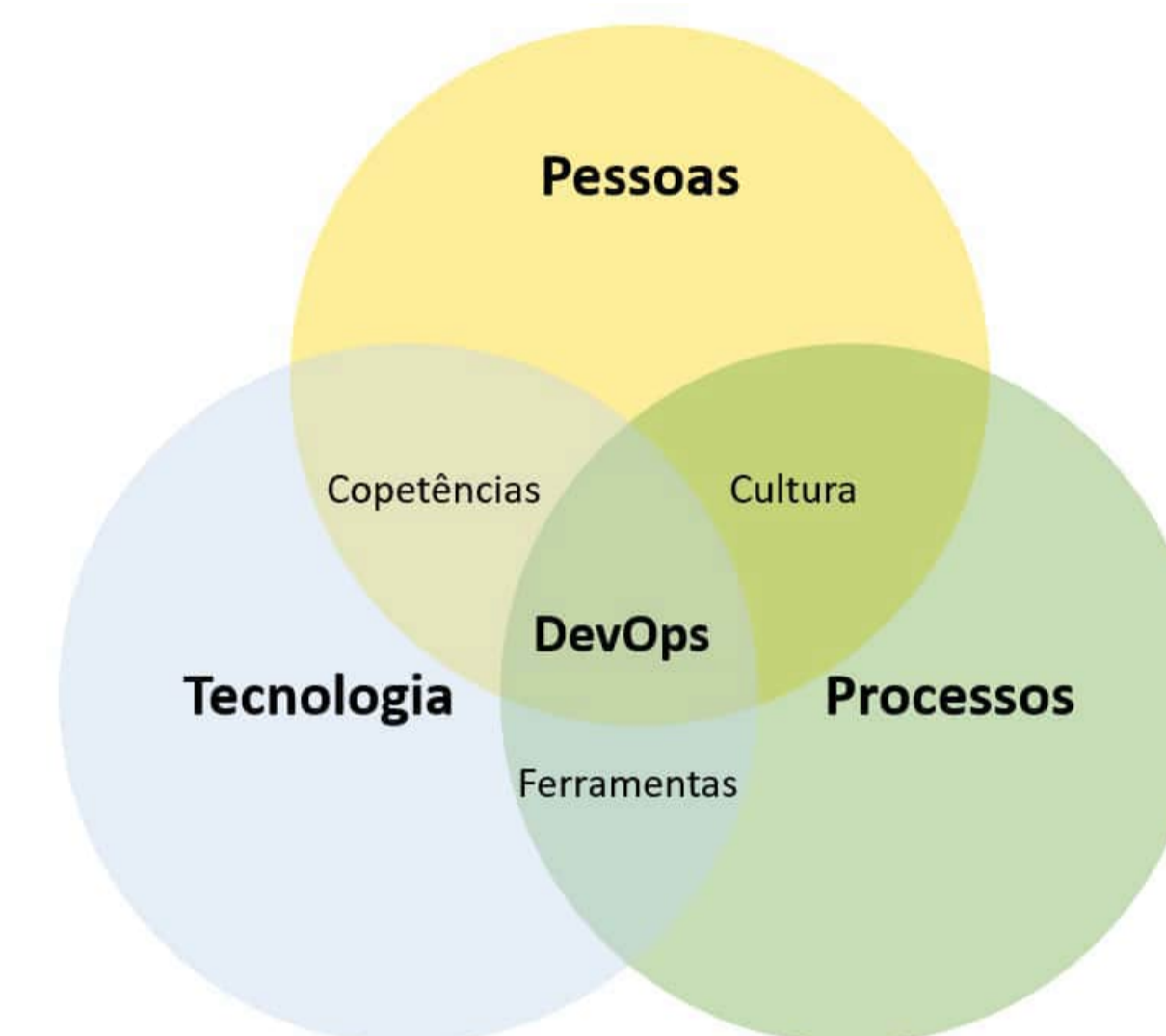
[Serviços](#)
[Dados](#)
[Softwares](#)
[Hardware](#)
[Redes](#)
[Oportunidades](#)

SERVIÇOS - DevOps

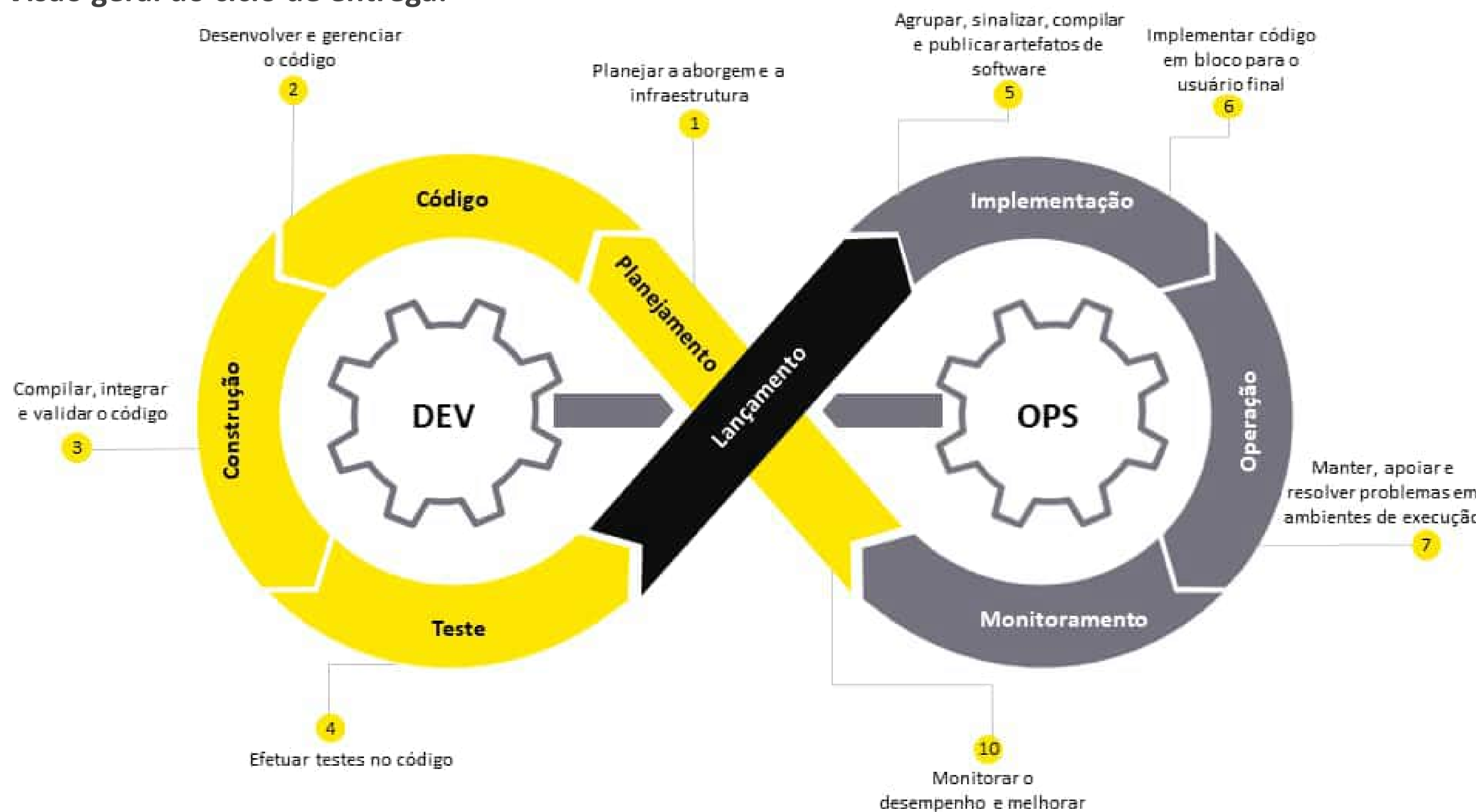
[Cloud](#)
[Landing Zone](#)
[Hub/Spoke](#)
[FinOps](#)
[DevOps](#)

DevOps é uma cultura que promove a colaboração entre os times de desenvolvimento e operações de uma empresa. Essa cultura busca a automação de processos, a integração e entrega contínua (CI/CD) de software, o monitoramento e a resolução de incidentes de forma rápida e eficiente.

Além disso, a cultura DevOps permite que as equipes de desenvolvimento e operações trabalhem de forma mais colaborativa, eliminando silos e aumentando a transparência. O DevOps também ajuda a melhorar a qualidade do software entregue, uma vez que as ferramentas de automação e integração contínua permitem a detecção de problemas mais cedo no ciclo de vida do desenvolvimento. O monitoramento contínuo também permite que a empresa detecte e corrija problemas de forma mais rápida, minimizando impactos no negócio.



Visão geral do ciclo de entrega:



A implementação do DevOps é importante para empresas porque permite a criação de um ambiente de desenvolvimento mais ágil e eficiente, reduzindo o tempo de lançamento de novas funcionalidades e correções de bugs.

Por fim, o DevOps ajuda as empresas a serem mais competitivas no mercado, já que a velocidade de lançamento de novas funcionalidades e correções é um fator crítico de sucesso no mundo dos negócios atual. Em resumo, a implementação de uma cultura DevOps pode trazer muitos benefícios para a empresa, desde a melhoria da eficiência até a vantagem competitiva no mercado.

DIRECIONADORES PARA INFRAESTRUTURA FUTURA

Serviços

Dados

Softwares

Hardware

Redes

Oportunidades

ESTRATÉGIA DE SEGURANÇA CLOUD

Estratégia de Segurança

Endpoints

Gestão de Acessos

Redundância de Armazenamento

Na era da transformação digital, proteger ambientes de nuvem nunca foi tão importante. Como arquitetos corporativos, devemos navegar pelas responsabilidades compartilhadas entre nossas organizações e fornecedores de cloud para garantir uma infraestrutura de nuvem segura, compatível e resiliente. Os princípios de Nuvem Confiável destacam-se a importância de uma abordagem colaborativa para a segurança na nuvem. Embora os fornecedores de cloud forneçam controles e recursos de segurança robustos, os clientes são proprietários de seus dados, identidades e da segurança de seus recursos locais e componentes de nuvem. Entender os domínios e subdomínios que englobam a segurança na infraestrutura é necessário para implementá-la.

VRM	Risco do Fornecedor / Terceiros	GRC	Governança, Riscos e Compliance
	Gerenciamento de Riscos de Fornecedores	Políticas, baseline de segurança operacional	Gestão de Riscos de TI
	Controles de Segurança para aplicações SaaS	Conscientização e Treinamento	Compliance e Auditoria
			Monitoramento e Relatórios (Métricas, Painel de Riscos)
IAM	Gerenciamento de identidades e acesso	DPP	Proteção de Dados
	Gestão de Identidades	Governança de dados	TC
	Gerenciamento de Senhas	Proteção IP	Controles Técnicos
	Serviços de autenticação	Gerenciamento do ciclo de vida dos dados	DevSecOps (SDLC seguro e codificação segura)
	Autorização e funções	Privacidade	Infraestrutura (Servidor/Rede/Configuração.)
	Gerenciamento de acesso privilegiado	Prevenção de perda de dados	Gerenciamento de dispositivos/conteúdo móvel
SO	Operações de Segurança	ER	Resiliência Empresarial
	Inteligência de ameaças	Serviços de criptografia	Recuperação de Desastres
	Gerenciamento de Vulnerabilidades e Incidentes		Gestão de Crises
	Monitoramento de segurança		
PRM	Gestão de Riscos de Portfólio		
	Gestão da Qualidade		



A partir dessa definição, **controles de segurança** devem ser implementados, visando a manutenção de uma **infraestrutura segura** e reforçada contra ameaças e vulnerabilidades.



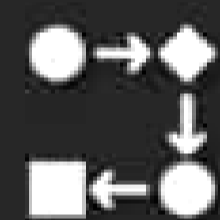
Painel



Estratégia



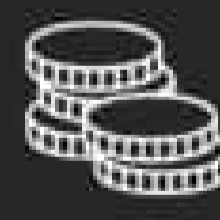
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

DIRECIONADORES PARA INFRAESTRUTURA FUTURA

Serviços

Dados

Softwares

Hardware

Redes

Oportunidades

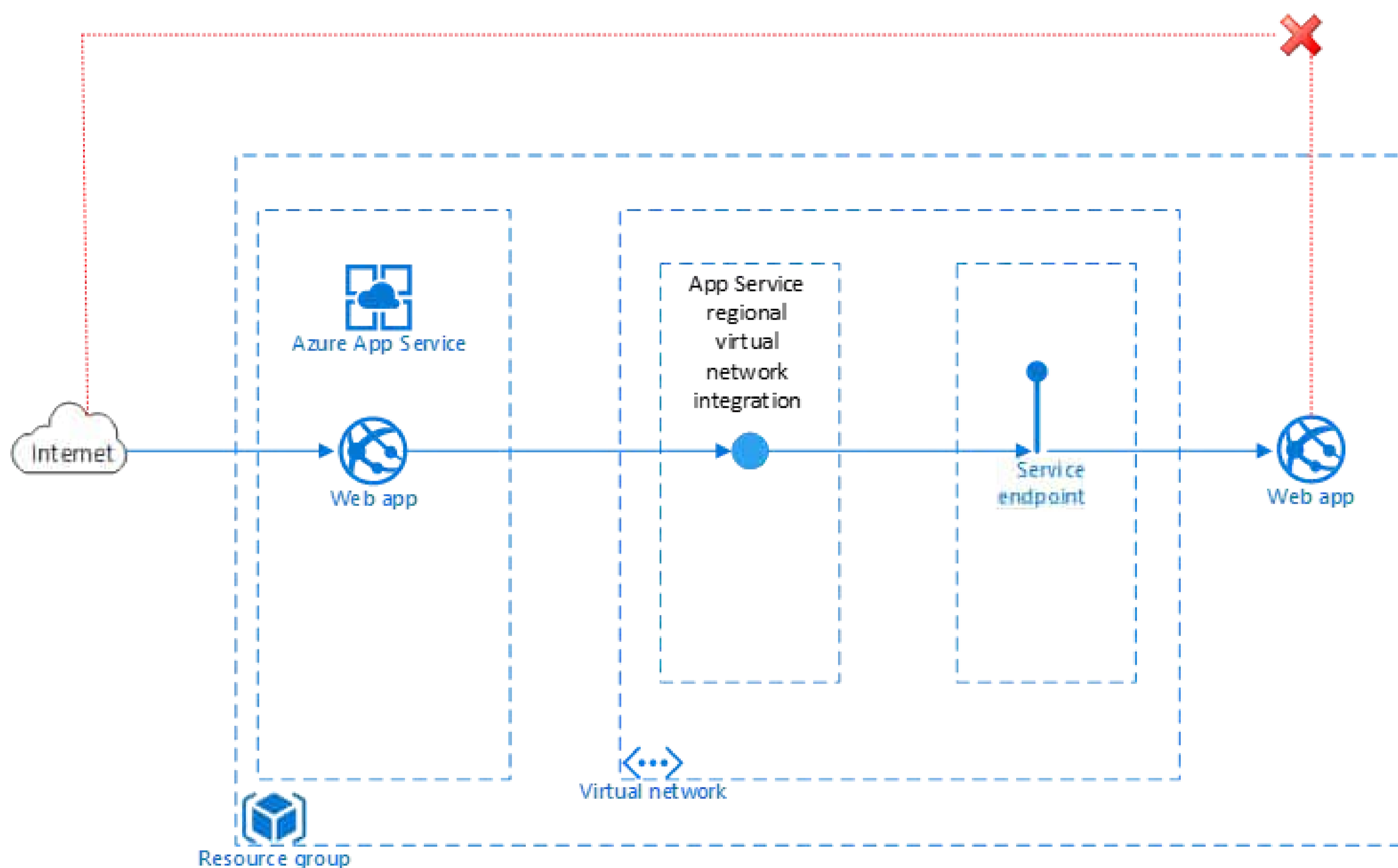
CLOUD SERVICE ENDPOINT

Estratégia de Segurança

Endpoints

Gestão de Acessos

Redundância de Armazenamento



Utilizar a configuração Service Endpoints para que o tráfego seja restrito no backbone do provedor de cloud, e não via internet, na troca de informações entre objetos para serviços não críticos ou sensíveis para segurança de dados. Pode restringir o acesso por serviços, como: SQL, Storage, vNet etc.

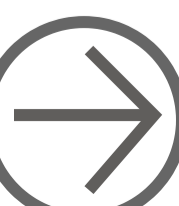
Usar o Service Endpoint em ambientes de nuvem é importante por várias razões:

Segurança: Quando o tráfego é roteado por meio de um Service Endpoint, o acesso aos recursos em nuvem é restrito apenas a usuários e recursos autorizados. Isso ajuda a garantir que apenas aqueles que têm permissão possam acessar e manipular dados e aplicativos em nuvem, reduzindo o risco de ataques externos.

Controle de Acesso: O uso exclusivo de Service Endpoint permite que o acesso aos recursos em nuvem seja restrito apenas a usuários e recursos autorizados. Isso ajuda a garantir que apenas aqueles que têm permissão possam acessar e manipular dados e aplicativos em nuvem, reduzindo o risco de acesso não autorizado aos recursos.

Conformidade: Para empresas que precisam cumprir regulamentações de segurança e privacidade, o uso exclusivo de Service Endpoint pode ser essencial para garantir a conformidade. Isso porque o uso de conexões públicas pode aumentar o risco de vazamento de dados e, portanto, violar as regulamentações.

Desempenho: O uso exclusivo de Service Endpoint pode melhorar o desempenho da rede, pois reduz a latência e a largura de banda necessárias para a transmissão de dados. Isso pode resultar em tempos de resposta mais rápidos e menos atrasos na transmissão de informações. Recomendado para ambiente sem informações sensíveis e baixo grau de exposição.



DIRECIONADORES PARA INFRAESTRUTURA FUTURA

Serviços

Dados

Softwares

Hardware

Redes

Oportunidades

CLOUD PRIVATE ENDPOINT

Estratégia de Segurança

Endpoints

Gestão de Acessos

Redundância de Armazenamento

Utilizar a configuração Private Service Endpoints para que o tráfego seja via rede interna do provedor de cloud, não via backbone ou internet, na troca de informações entre objetos para serviços críticos ou sensíveis para segurança de dados.

O uso de Private Endpoint em ambientes de nuvem é importante por várias razões:

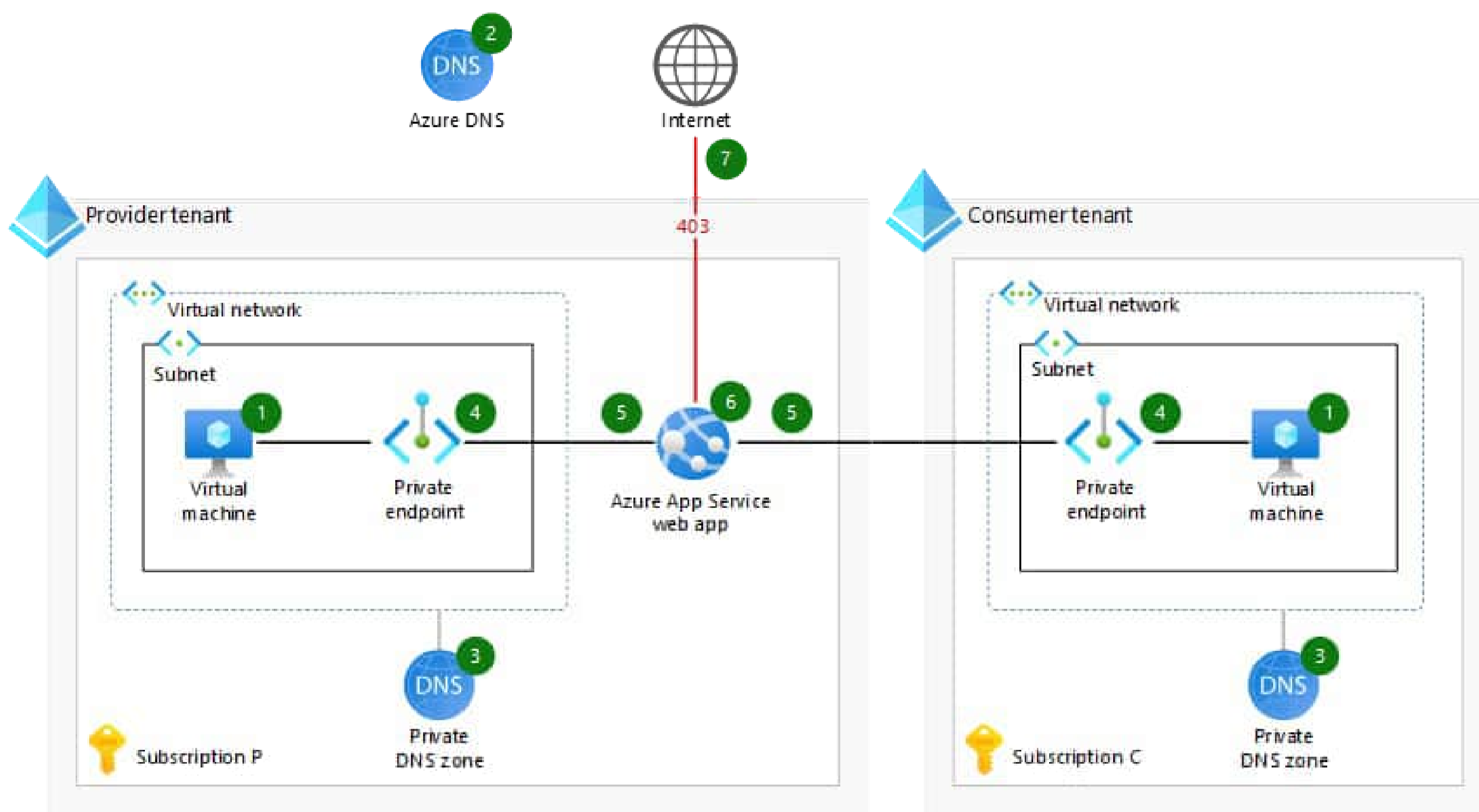
Segurança: Quando o tráfego é roteado por meio de uma conexão privada, como um Private Endpoint, os dados são protegidos contra possíveis ataques externos. Isso é especialmente importante em ambientes de nuvem onde a exposição a ameaças é maior.

Controle de Acesso: O uso exclusivo de Private Endpoint permite que o acesso aos recursos em nuvem seja restrito apenas a usuários e recursos autorizados. Isso ajuda a garantir que apenas aqueles que têm permissão possam acessar e manipular dados e aplicativos em nuvem.

Conformidade: Para empresas que precisam cumprir regulamentações de segurança e privacidade, o uso exclusivo de Private Endpoint pode ser essencial para garantir a conformidade. Isso porque o uso de conexões públicas pode aumentar o risco de vazamento de dados e, portanto, violar as regulamentações.

Desempenho: O uso exclusivo de Private Endpoint pode melhorar o desempenho da rede, pois reduz a latência e a largura de banda necessárias para a transmissão de dados. Isso pode resultar em tempos de resposta mais rápidos e menos atrasos na transmissão de informações.

Recomendado para ambiente com informações sensíveis e alto grau de exposição.



DIRECIONADORES PARA INFRAESTRUTURA FUTURA

Serviços

Dados

Softwares

Hardware

Redes

Oportunidades

GESTÃO DE ACESSO

Estratégia de Segurança

Endpoints

Gestão de Acessos

Redundância de Armazenamento



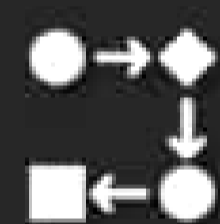
Painel



Estratégia



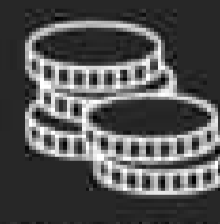
Pessoas



Processos



Tecnologia



Orçamento



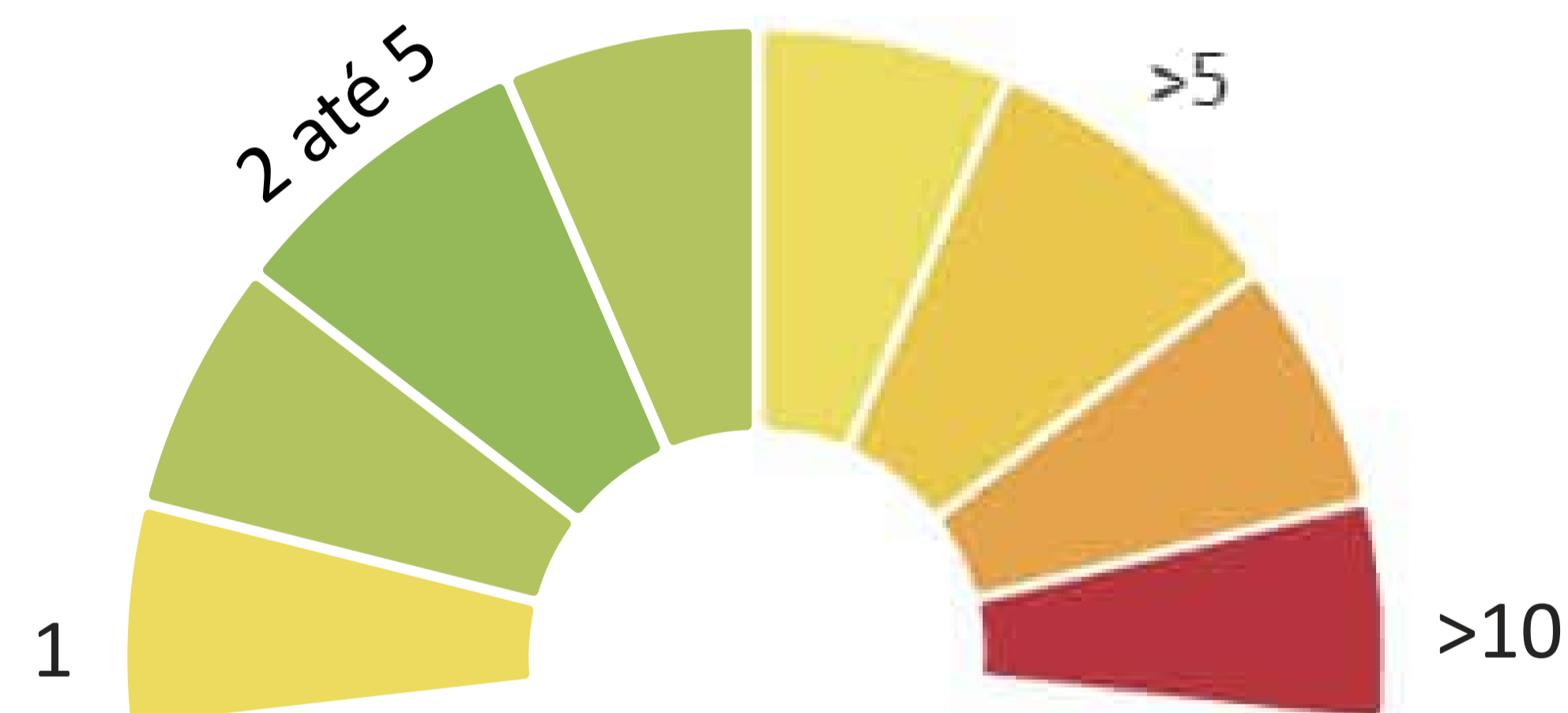
Roadmap

Como uma melhor prática, recomenda-se que seja atribuído a função de Administrador global a menos de cinco pessoas em sua organização. Os administradores globais têm acesso a todos os recursos administrativos e é de seu interesse manter a superfície de ataque baixa. Todas essas contas devem ser protegidas com a autenticação multifator.

Por padrão, quando um usuário se inscreve em um serviço de nuvem da Microsoft, um locatário do Azure AD ou qualquer outro provedor de cloud é criado e o usuário se torna membro da função de administradores globais. Os usuários atribuídos à função de Administrador global podem ler e modificar todas as configurações administrativa em sua organização do Azure AD. Com algumas exceções, os administradores globais também podem ler e modificar todas as definições de configuração em sua organização do Microsoft 365. Os administradores globais também têm a capacidade de elevar o acesso para ler dados.

É recomendado manter duas contas de emergência atribuídas permanentemente à função de Administrador global. Verifique se essas contas não exigem o mesmo mecanismo de autenticação multifator que suas contas administrativas normais para entrar.

Quantas contas de Global Admins no Azure AD / Microsoft 365 tem na sua organização?



DIRECIONADORES PARA INFRAESTRUTURA FUTURA

Serviços

Dados

Softwares

Hardware

Redes

Oportunidades

REDUNDÂNCIA DE ARMAZENAMENTO NA CLOUD

Estratégia de Segurança

Endpoints

Gestão de Acessos

Redundância de Armazenamento

A redundância do Armazenamento do Azure sempre armazena várias cópias dos seus dados para que eles sejam protegidos contra eventos planejados e não planejados, incluindo falhas de hardware transitórias, interrupções de energia ou rede e desastres naturais de grandes proporções. A redundância garante que sua conta de armazenamento atenda às suas metas de disponibilidade e durabilidade mesmo diante de falhas.

O LRS é a opção mais econômica de redundância, mas possui baixa durabilidade, já que o armazenamento é replicado três vezes em um único datacenter. O ZRS é mais durável do que o LRS, replicando os dados em três datacenters diferentes em uma mesma região, porém é mais caro do que o LRS. O GZRS é mais caro do que o ZRS, mas oferece proteção contra falhas em um datacenter inteiro em uma região. O RA-GRS, por sua vez, permite a leitura de dados em um segundo datacenter, mas é mais caro do que o GZRS. Por fim, o ZRS Premium é a opção mais cara, mas oferece maior durabilidade e desempenho do que o ZRS padrão.

Redundância	Descrição	Vantagens	Desvantagens
GZRS	Geo-Redundant Storage (Armazenamento com Redundância Geográfica)	Cópias dos dados são mantidas em duas regiões diferentes	Mais caro que o LRS e o ZRS, e a replicação pode causar latência
LRS	Locally Redundant Storage (Armazenamento com Redundância Local)	Cópias dos dados são mantidas em um único data center	Proteção limitada contra falhas em um data center inteiro
RA-GRS	Read Access-Geo Redundant Storage (Armazenamento com Redundância Geográfica com Acesso de Leitura)	Cópias dos dados são mantidas em duas regiões diferentes e podem ser lidos em qualquer uma delas	Mais caro que o LRS, o ZRS e o GZRS, e a replicação pode causar latência
ZRS	Zone Redundant Storage (Armazenamento com Redundância de Zona)	Cópias dos dados são mantidas em três zonas diferentes em uma região	Mais caro que o LRS e menos durável que o GZRS e o RA-GRS
ZRS Premium	Zone Redundant Storage Premium	Cópias dos dados são mantidas em três zonas diferentes em uma região, com mais recursos de armazenamento e rede	Mais caro que o ZRS padrão e só está disponível em algumas regiões do Azure.



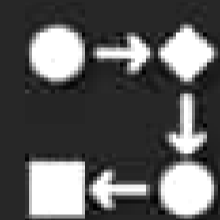
Painel



Estratégia



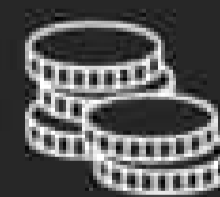
Pessoas



Processos



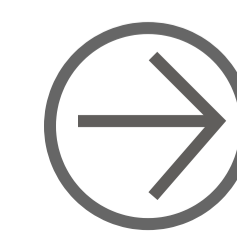
Tecnologia



Orçamento



Roadmap



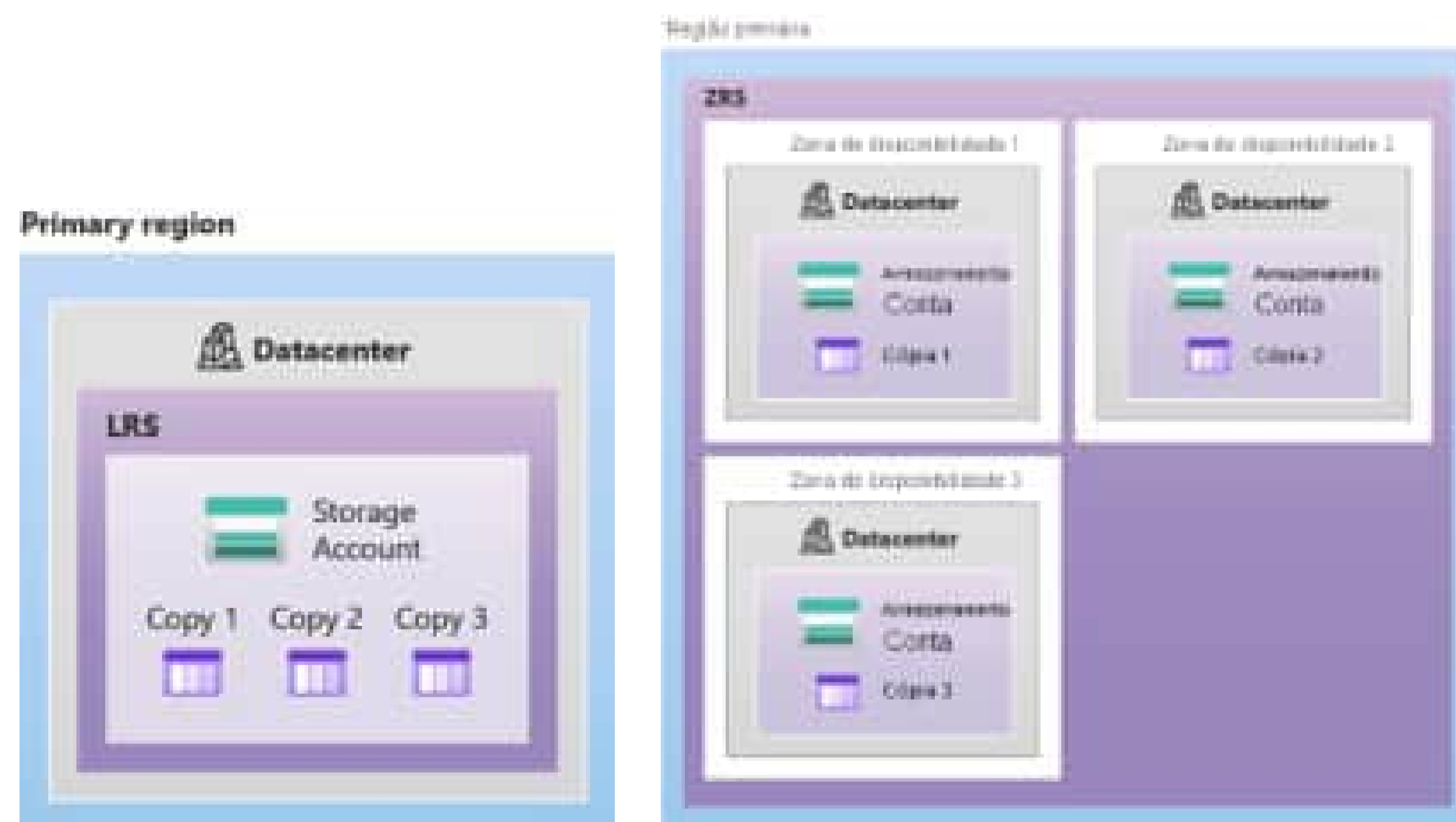
DIRECIONADORES PARA INFRAESTRUTURA FUTURA

REDUNDÂNCIA DE ARMAZENAMENTO NA CLOUD

A redundância do Armazenamento do Azure sempre armazena várias cópias dos seus dados para que eles sejam protegidos contra eventos planejados e não planejados, incluindo falhas de hardware transitórias, interrupções de energia ou rede e desastres naturais de grandes proporções. A redundância garante que sua conta de armazenamento atenda às suas metas de disponibilidade e durabilidade mesmo diante de falhas.



Dados são replicados com o GRS ou com o RA-GRS.

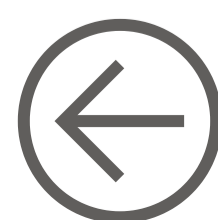


Dados são replicados em um único data center com o LRS.

Dados são replicados entre as zonas de disponibilidade na região primária com o ZRS.



Dados são replicados com o GZRS ou com o RA-GZRS.



DIRECIONADORES PARA INFRAESTRUTURA FUTURA

Serviços

Dados

Softwares

Hardware

Redes

Oportunidades

INFRAESTRUTURA COMO CÓDIGO

IaC

A Infraestrutura como Código (IaC – *Infrastructure as Code*) usa a metodologia DevOps e o controle de versão com um modelo descritivo para definir e implantar infraestrutura, como redes, máquinas virtuais, banco de dados, balanceadores de carga e topologias de conexão meio do uso script, e não por meio de processos manuais. Basicamente infraestrutura como *software*, e os códigos e *scripts* ajudam a configurar e implantar os componentes de maneira rápida e consistente sem necessidade de intervenção humana e automatizando o processo de implantação de infraestrutura de maneira repetitiva e consistente, gerando ganhos de produtividade, consistência de configuração e reduzindo riscos humanos. Os 4 itens abaixo mostram diretrizes para o uso e adoção da prática de IaC.

1

Infraestrutura Imutável

Se forem necessárias alterações na arquitetura de infraestrutura ou em sua configuração, é possível que a pilha de códigos IaC possa se tornar descartável.

2

Menos documentação

O código IaC é a sua documentação, portanto, no que tange a operação de infraestrutura, os scripts funcionam como documentação de como procedimentos, mas não se deve abandonar diagramas, gestão de configuração, etc.

3

Controle de Versão

Qualquer alteração no *script* deve ser rastreada, gerenciada e reconciliada, fornecendo uma trilha de auditoria sobre o que acontece nos *scripts* que alteram os ambientes produtivos. Deve existir um controle robusto nas mudanças.

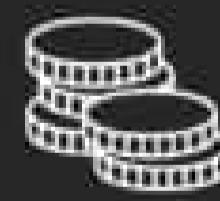
4

IaC Modular

O IaC deve ser construído de forma modular para ser executado independentemente do resto dos componentes (como microsserviços), podendo ser combinados de maneira automatizada.



Uma ferramenta deve prover a capacidade de gerir orquestrar e configurar a infraestrutura de forma automática e as plataformas a serem automatizadas precisam ser compatíveis. Quando se trata de *cloud*, a maioria das plataformas e serviços existentes já possuem esses recursos ou são compatíveis.



DIRECIONADORES PARA INFRAESTRUTURA FUTURA

Serviços

Dados

Softwares

Hardware

Redes

Oportunidades

HARDWARE

Não foi possível estabelecer as recomendações futuras para o capítulo de Hardware, pois o inventário de equipamentos de TI não foi entregue para realização das análises pertinentes.



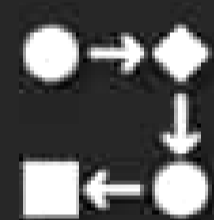
Painel



Estratégia



Pessoas



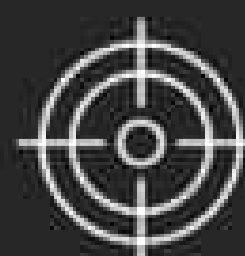
Processos



Tecnologia



Orçamento



Roadmap

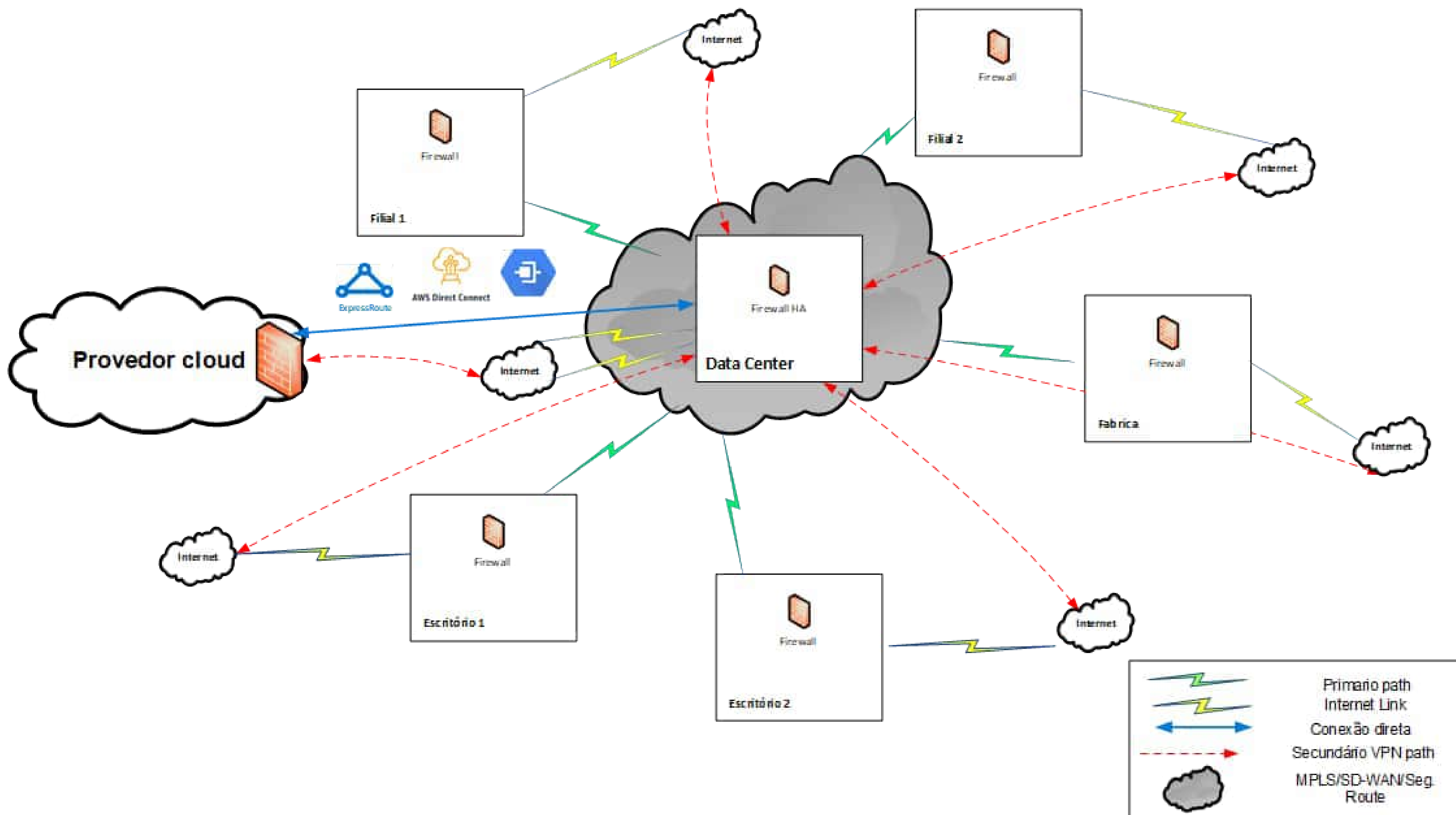
DIRECIONADORES PARA INFRAESTRUTURA FUTURA

[Serviços](#)
[Dados](#)
[Softwares](#)
[Hardware](#)
[Redes](#)
[Oportunidades](#)

DATA CENTERS

[Data Centers](#)
[Conexão Out-of-Band](#)
[Latência Cloud](#)

Abaixo é apresentada uma proposta de topologia de referência para a rede de dados futura. Sugere-se a substituição de Links ponto a ponto em conjunto com a utilização dos conceitos de SD-WAN, objetivando a melhora de performance e eficiência dos múltiplos serviços de rede, reduzindo o tempo de gerenciamento, transporte, processamento e custo. Também é recomendado a adoção do modelo de roteamento, SD-WAN, Segment Route ou correlatos, objetivando a melhora de performance e eficiência dos múltiplos serviços de rede, reduzindo o tempo de gerenciamento, transporte, processamento e custo.



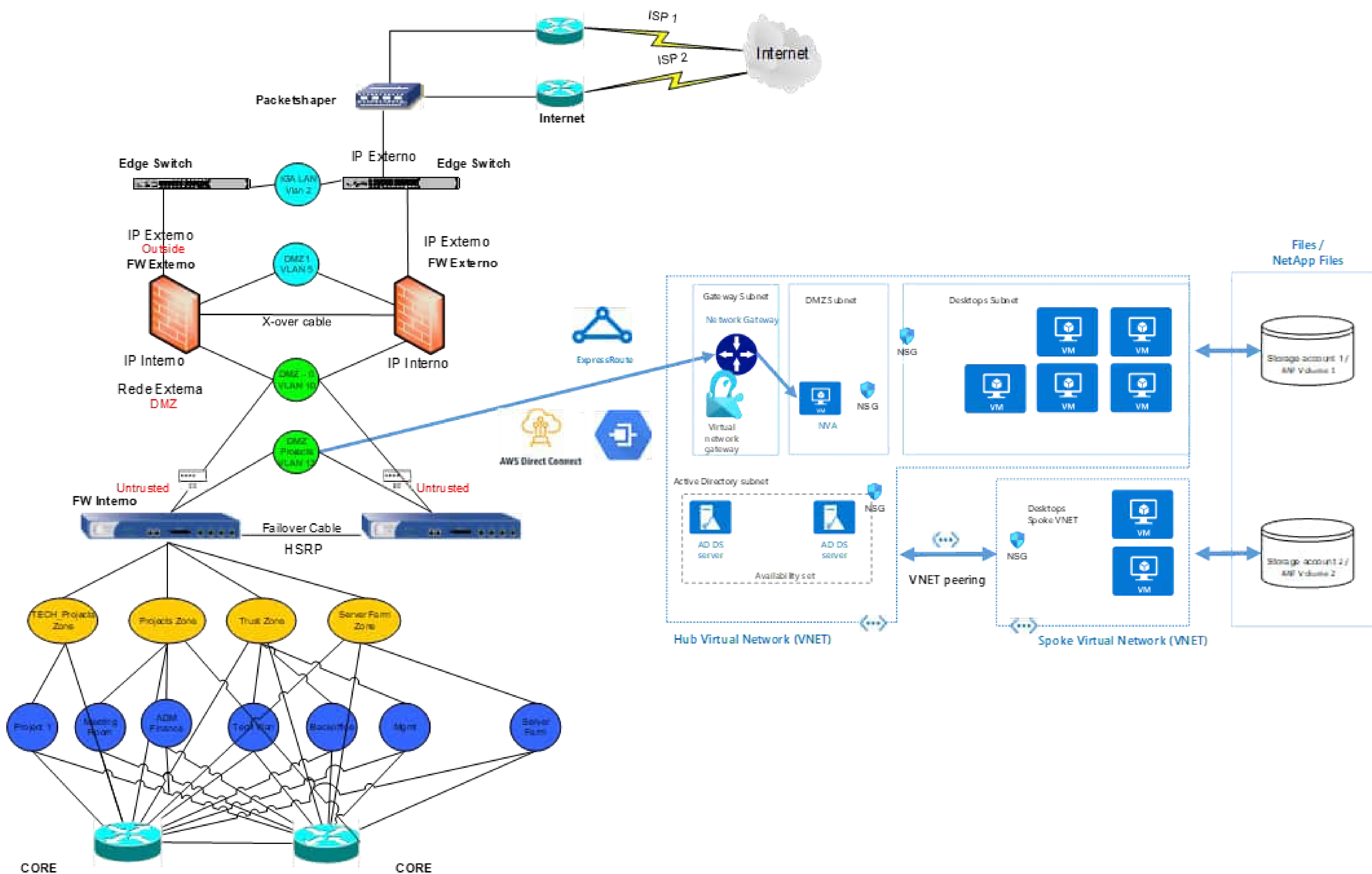
DIRECIONADORES PARA INFRAESTRUTURA FUTURA

[Serviços](#)
[Dados](#)
[Softwares](#)
[Hardware](#)
[Redes](#)
[Oportunidades](#)

DATA CENTERS

[Data Centers](#)
[Conexão Out-of-Band](#)
[Latência Cloud](#)

Abaixo é apresentada uma proposta de arquitetura futura para o data center central, consolidando os acessos a partir de um ponto único.



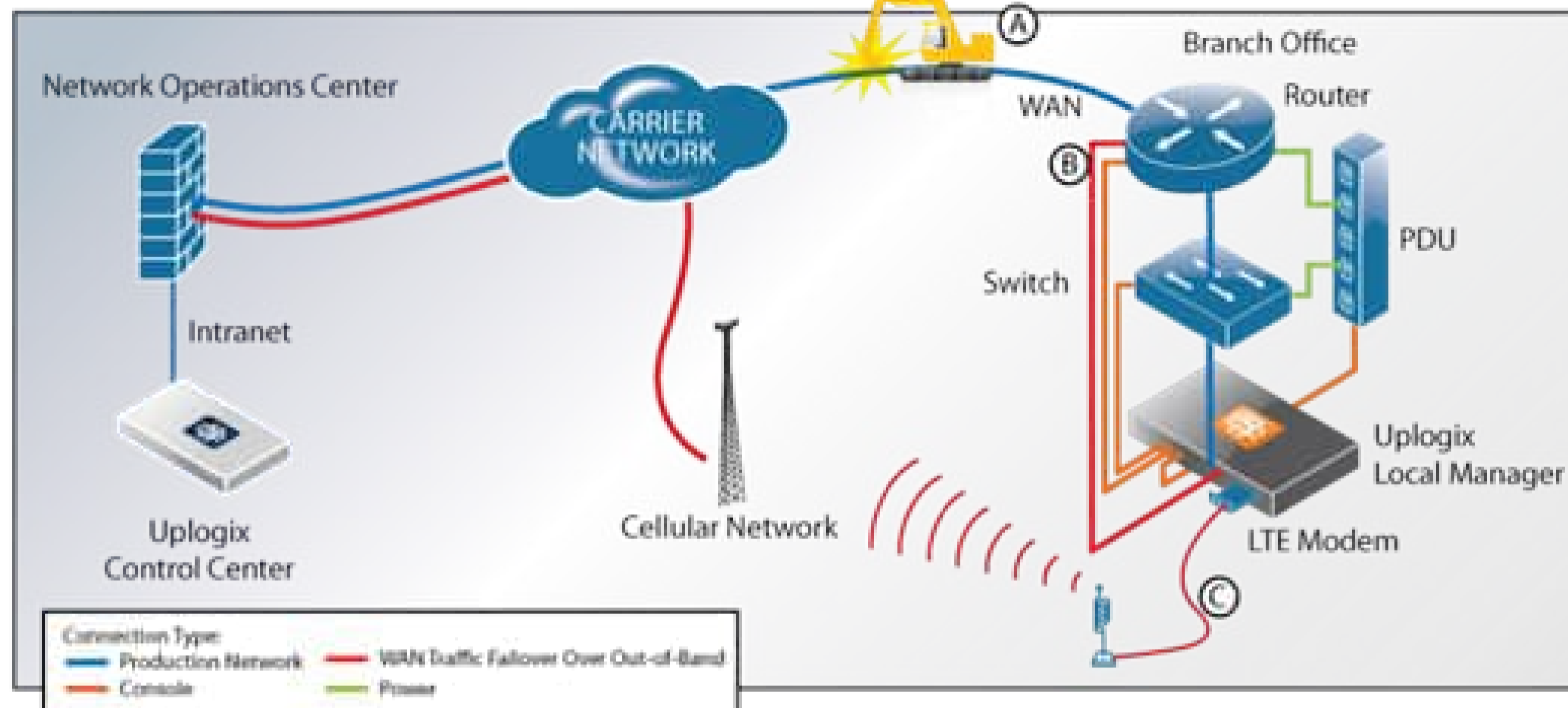
DIRECIONADORES PARA INFRAESTRUTURA FUTURA

[Serviços](#)
[Dados](#)
[Softwares](#)
[Hardware](#)
[Redes](#)
[Oportunidades](#)

CONEXÃO OUT-OF-BAND

[Data Centers](#)
[Conexão Out-of-Band](#)
[Latência Cloud](#)

Uplogix WAN Traffic Failover



A conexão Out-of-Band é um método de comunicação que permite o acesso separado e independente do ambiente principal de uma rede ou sistema. Em outras palavras, é uma conexão que ocorre por meio de uma interface diferente daquela usada para o tráfego de dados normais, o que garante que a gestão do sistema seja realizada de forma segura e isolada.

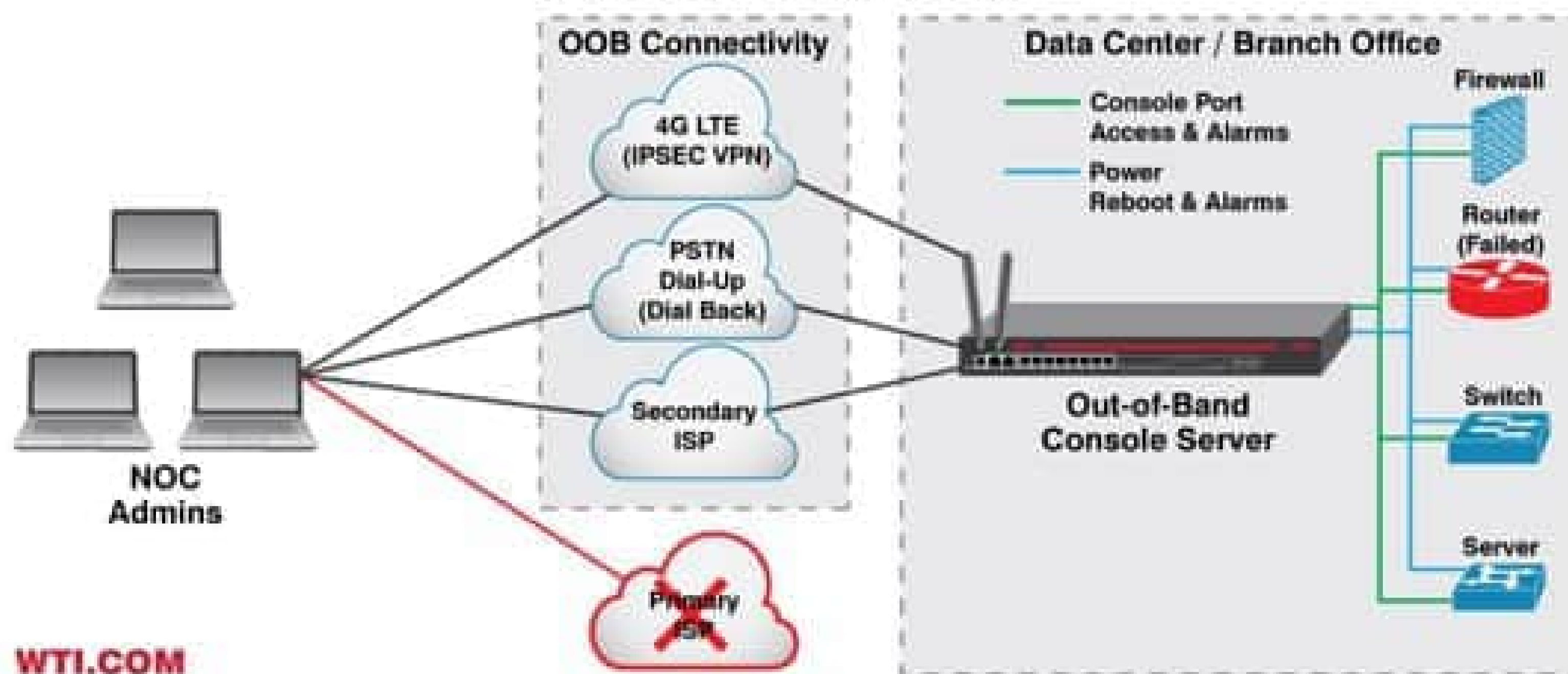
A principal vantagem da conexão Out-of-Band é que ela fornece um canal de gerenciamento de rede que é completamente separado da rede principal. Isso significa que o acesso a recursos críticos de gerenciamento, como consoles de gerenciamento, sistemas de backup e recuperação, e dispositivos de monitoramento de rede, podem ser feitos de forma segura, mesmo que a rede principal esteja comprometida por um ataque cibernético.

Outra vantagem é que a conexão Out-of-Band pode ajudar a solucionar problemas de rede de forma mais rápida e eficiente. Por exemplo, um administrador de rede pode acessar remotamente um servidor de gerenciamento usando uma conexão Out-of-Band, mesmo que o servidor esteja inacessível por meio da rede principal. Isso pode economizar tempo valioso e evitar que problemas se agravem.

No entanto, há também algumas desvantagens na conexão Out-of-Band. Uma delas é que ela requer equipamentos adicionais e configurações complexas para estabelecer e manter a conexão separada. Isso pode aumentar o custo e a complexidade da rede.

Além disso, a conexão Out-of-Band não é infalível e pode ser vulnerável a ataques cibernéticos, especialmente se os protocolos de segurança não forem adequadamente implementados. Portanto, é importante que os administradores de rede implementem medidas de segurança rigorosas para garantir a integridade da conexão Out-of-Band.

Out-of-Band Management



WTI.COM

DIRECIONADORES PARA INFRAESTRUTURA FUTURA

Serviços

Dados

Softwares

Hardware

Redes

Oportunidades

LATÊNCIA CLOUD

Data Centers

Conexão Out-of-Band

Latência Cloud

Ao implantar workloads em outras regiões, é importante entender como isso pode afetar a latência de rede e, conseqüentemente, a experiência do usuário final. Por exemplo, se sua solução está sendo executada na região do Brazil East (São Paulo sa-saopaulo-1) e você precisa fazer uma apresentação para um cliente na Austrália, duplicar seu workload na região da Australia East (Sydney ap-sydney-1) pode ser uma estratégia eficaz para melhorar a experiência do cliente. No entanto, é importante lembrar que, se o seu novo workload ainda precisa se comunicar com a região principal ou base, você precisará garantir que a latência entre as regiões não seja um problema.

Outro cenário em que a latência de rede é um fator crítico é quando você deseja implementar um Disaster Recovery Site ou um Site Backup. Para calcular o RPO (Recovery Point Objective) e o RTO (Recovery Time Objective) precisamente, é essencial ter visibilidade da latência de rede entre as duas regiões que estão sendo utilizadas. Isso ajudará a garantir que a cópia de backup seja mantida atualizada e que a recuperação do site seja realizada dentro do tempo previsto. Portanto, antes de implementar um plano de recuperação de desastres, é fundamental avaliar cuidadosamente as latências de rede entre as regiões envolvidas para garantir a eficácia e a rapidez do processo de recuperação.

É importante lembrar que, ao falar sobre a latência de rede entre as regiões de um CSP (Cloud Service Provider), estamos nos referindo aos backbones de comunicação nativos que já existem entre todas as regiões da nuvem. Esses backbones de comunicação foram projetados para fornecer uma conectividade confiável e segura entre as diferentes regiões, minimizando a latência de rede e garantindo um desempenho consistente para os workloads em execução em toda a infraestrutura de nuvem. É por isso que é crucial entender as latências de rede entre as regiões ao planejar o dimensionamento e a configuração dos seus workloads na nuvem, para garantir que você obtenha a melhor experiência possível para seus usuários finais.

Latência é o tempo que leva para um pacote de dados viajar de um ponto a outro em uma rede. É uma medida da velocidade e da eficiência de uma conexão de rede e pode ser afetada por vários fatores, como a distância geográfica entre os pontos de origem e destino, o congestionamento da rede e a qualidade do equipamento de rede usado.

A importância da latência é que ela pode afetar significativamente a experiência do usuário ao usar aplicativos ou outros serviços em cloud. Por exemplo, acesso a VMs, banco de dados, web sites, uma latência alta pode causar atrasos na resposta.

Portanto, a latência é uma medida importante da qualidade da rede e pode ser crucial para garantir a satisfação do usuário em muitas aplicações e serviços online. As empresas que dependem de conexões de rede de alta qualidade podem precisar monitorar e otimizar a latência para garantir que seus serviços sejam entregues com a melhor qualidade possível.

Recomenda-se usar soluções em cloud o mais próximo do usuário para fazer seu deploy reduzindo a latência aumentando a satisfação do usuário ao realizar seu trabalho.

Geografia	Região	Localização Física	Latência média (ms)
South America	Brazil South	Sao Paulo State	42 ms
US	Central US	Iowa	186 ms
US	East US	Virginia	162 ms
US	East US 2	Virginia	156 ms
US	North Central US	Illinois	174 ms
US	South Central US	Texas	178 ms
US	West Central US	Wyoming	196 ms
US	West US	California	206 ms
US	West US 2	Washington	212 ms
US	West US 3	Phoenix	193 ms



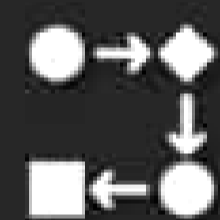
Painel



Estratégia



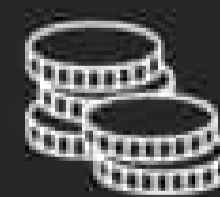
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

DIRECIONADORES PARA INFRAESTRUTURA FUTURA

Serviços

Dados

Softwares

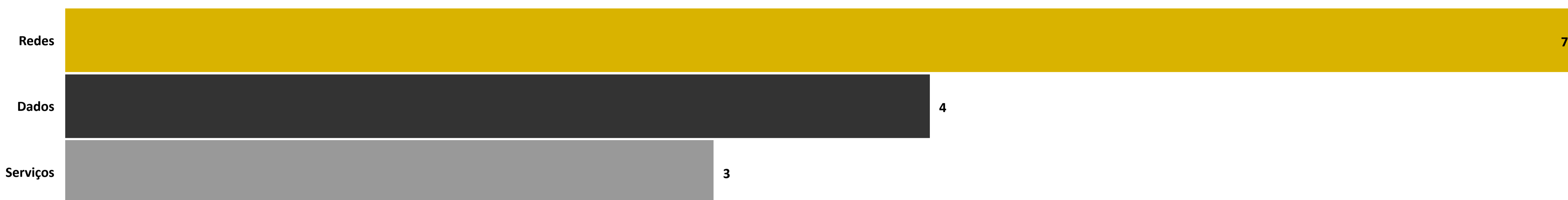
Hardware

Redes

Oportunidades

OPORTUNIDADES

Detalhamento Oportunidades



Tema

Oportunidades

Dados	Ausência de gerenciamento de dispositivos móveis.
Dados	Gerenciamento descentralizado de conta do administrador local do sistema operacional Windows.
Dados	Impossibilidade de utilização do SSO (single sign-on) para as aplicações, através do Azure AD.
Dados	Serviço de armazenamento descentralizado e sem consolidação.
Redes	Ausência de contratos de extensão de garantia para equipamentos de infraestrutura de rede críticos para a sustentação do Negócio.
Redes	Ausência de informações sobre o compartilhamento de infraestrutura dos provedores de internet.
Redes	Ausência de links redundantes nas unidades.
Redes	Custos elevados com links, gerenciamento de rotas não otimizado, autenticação para acesso aos ativos de rede descentralizados e ausência de acesso alternativo ao ambiente.
Redes	Gerenciamento de rotas, políticas, QoS e backbone interno descentralizados.
Redes	Performance da Rede de Dados abaixo dos padrões e necessidades das aplicações.
Redes	Rede de dados não segmentada.
Serviços	Ausência de conexão ponto a ponto com fornecedor de cloud.
Serviços	Gestão financeira realizada sem a adoção das melhores práticas de mercado.
Serviços	Serviços e atividades de TI descentralizados, Estrutura de clouds despadronizadas e vulnerabilidade em ambiente cloud.



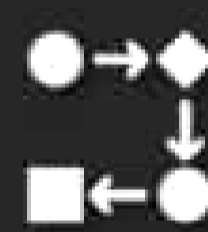
Painel



Estratégia



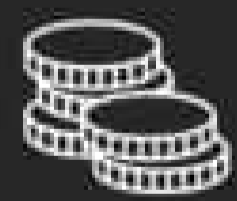
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

- Painel 
- Estratégia 
- Pessoas 
- Processos 
- Tecnologia 
- Orçamento** 
- Roadmap 
- Anexos 

ORÇAMENTO - VISÃO GERAL

Visão Geral

Situação Atual

Detalhamento



Painel

Estratégia

Pessoas

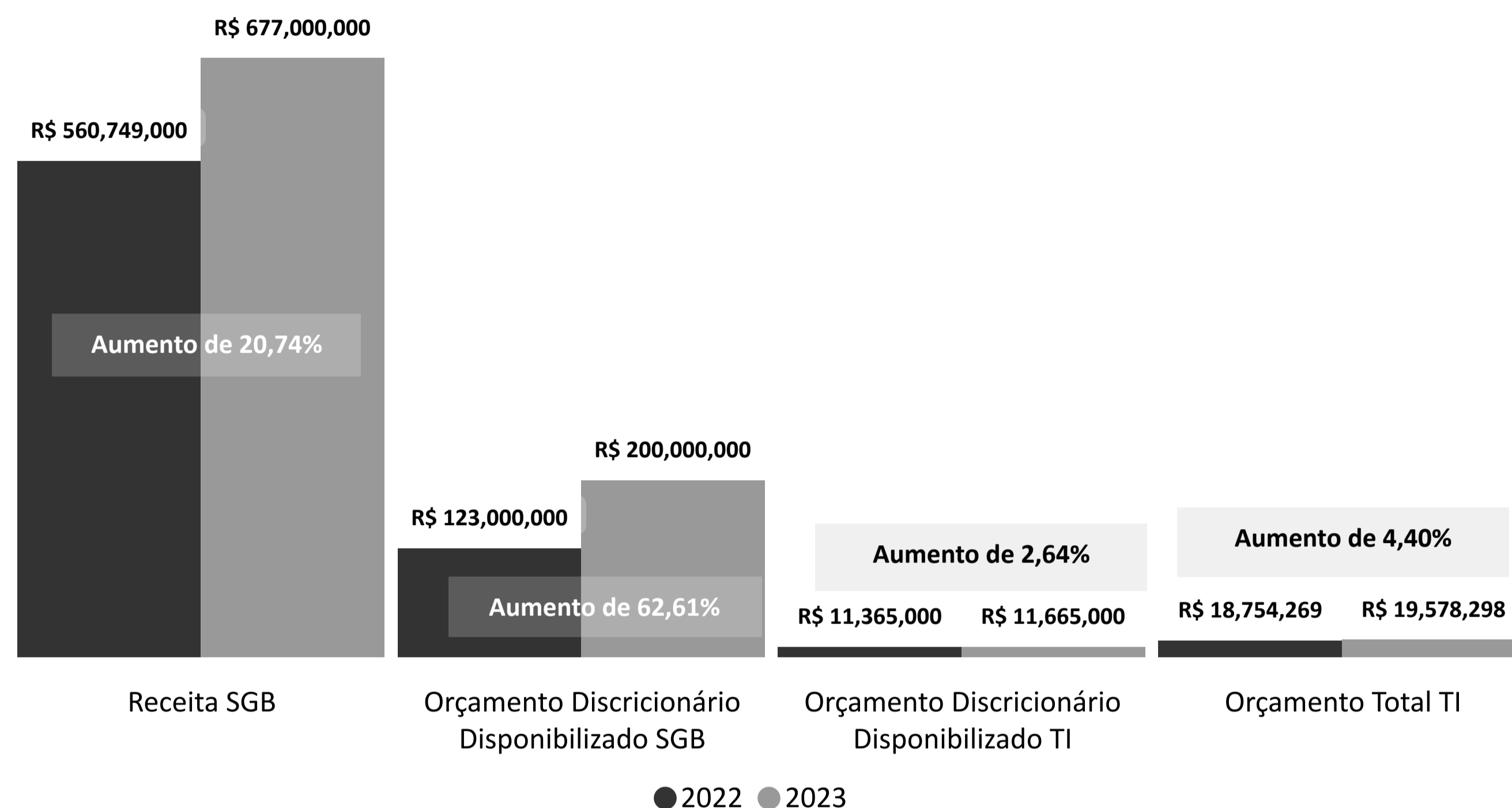
Processos

Tecnologia

Orçamento

Roadmap

Orçamento 2022 x 2023



Foram analisados os orçamentos da TI referentes aos anos de 2022 e 2023, identificando o percentual correspondente à **receita do SGB** e do **orçamento discricionário** disponibilizado para o SGB.

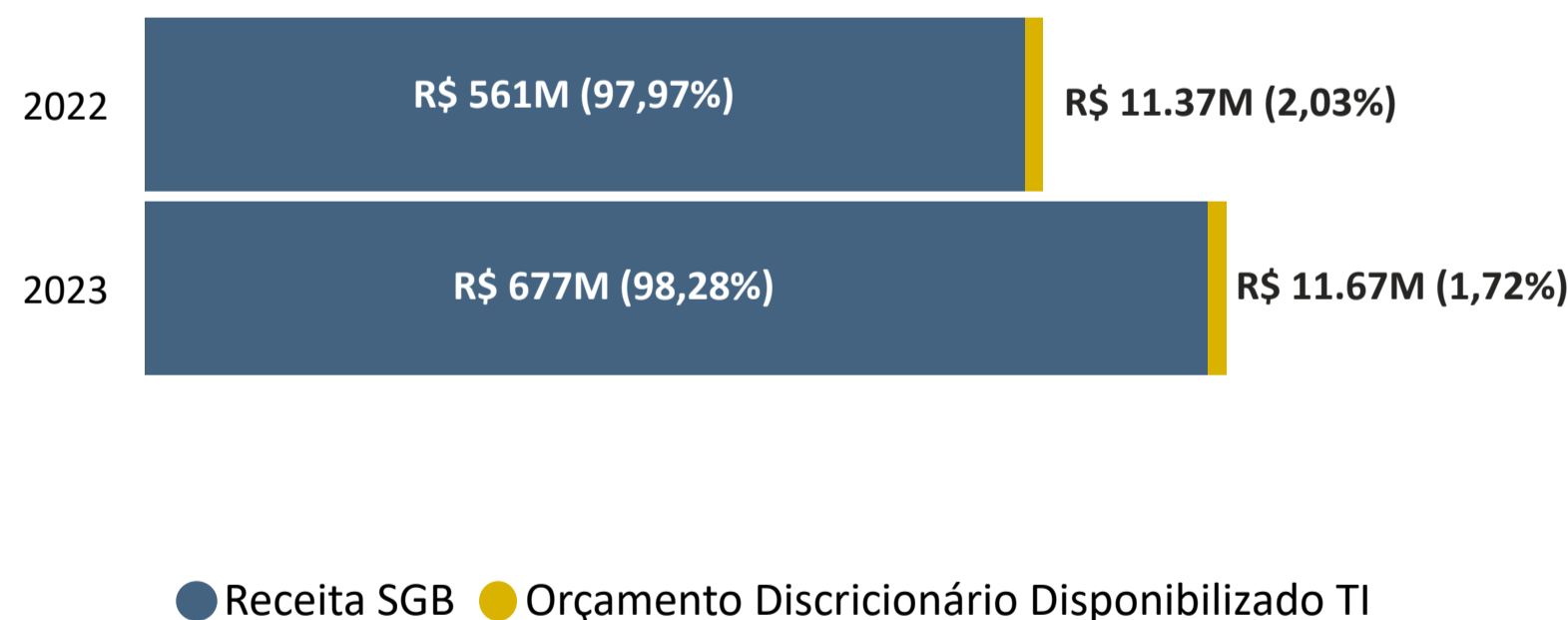
Há um **crescimento** previsto de **20,74%** na **receita do SGB** para o ano de 2023, comparado à 2022. Para o **orçamento discricionário disponibilizado para a TI** em 2023, apesar de ocorrer um aumento de **2,64%** em valores **absolutos**, sofreu uma **redução de 18%** frente à receita prevista.

O **orçamento discricionário disponibilizado ao SGB*** teve um **aumento de 62,61%** em 2023, comparado à 2022, enquanto o **disponibilizado à TI** sofreu uma **redução de 60%** frente ao total disponibilizado para companhia.

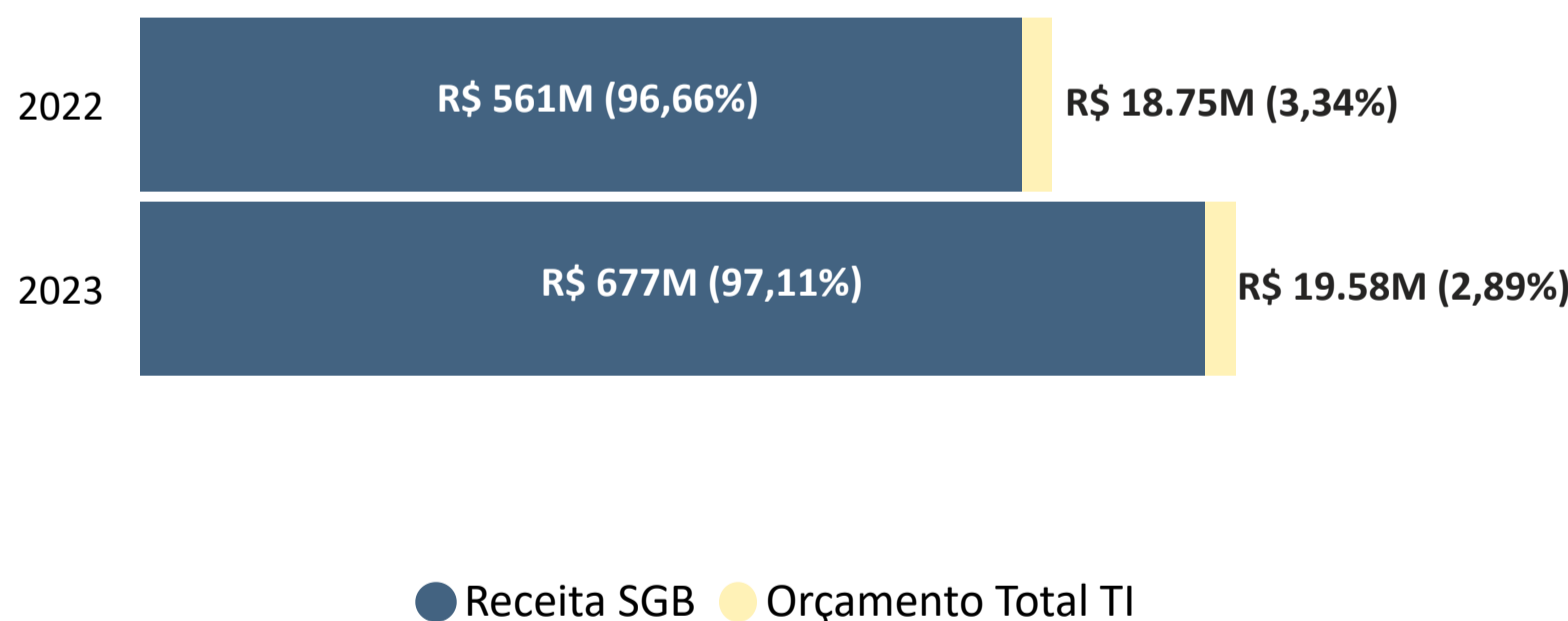
A **diferença** de valores entre o orçamento discricionário e o orçamento da TI corresponde à **R\$ 7,91M**, que se refere ao pagamento do pessoal próprio da TI, que é custeado pela **folha de pagamento** e não incide no **orçamento discricionário da TI**.

*Orçamento discricionário é destinado a execução dos projetos e ao custeio das atividades de infraestrutura técnica e administrativa.

Receita SGB x Orçamento Discricionário Disponibilizado TI



Receita SGB x Orçamento Total TI

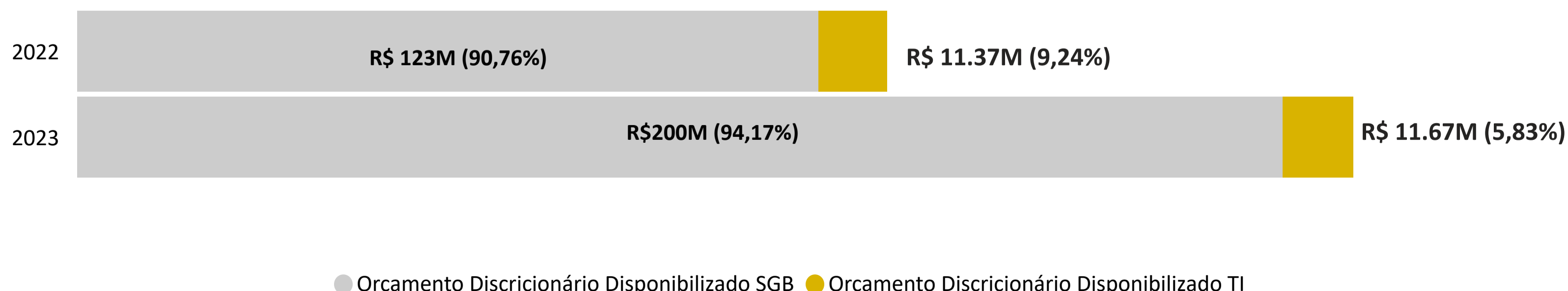


O **orçamento discricionário disponibilizado para TI**, em 2022, foi de **R\$ 11.37M** e a **receita do SGB** de **R\$ 561M**. Isto significa que o orçamento discricionário disponibilizado para TI **corresponde à 2,03%** da receita do SGB.

Em relação à 2023, o **orçamento discricionário disponibilizado para TI** foi de **R\$ 11.67M** e a receita do SGB de **R\$ 677M**. Isto significa que o orçamento discricionário disponibilizado para TI **corresponde à 1,72%** da receita do SGB.

O gráfico **Orçamento Total TI** contempla os valores de folha de pagamento, que é destinado ao pagamento de pessoal próprio da TI.

Orçamento Discricionário Disponibilizado SGB x Orçamento Discricionário Disponibilizado TI



O **orçamento discricionário disponibilizado para o SGB**, em 2022, foi de **R\$ 123M**. O orçamento discricionário disponibilizado para a TI corresponde à **9,24%** deste valor.

Em relação à 2023, o **orçamento discricionário disponibilizado para a TI** corresponde à **5,83%** do orçamento discricionário disponibilizado para o SGB. Uma redução de **3,41%** em relação ao ano anterior.

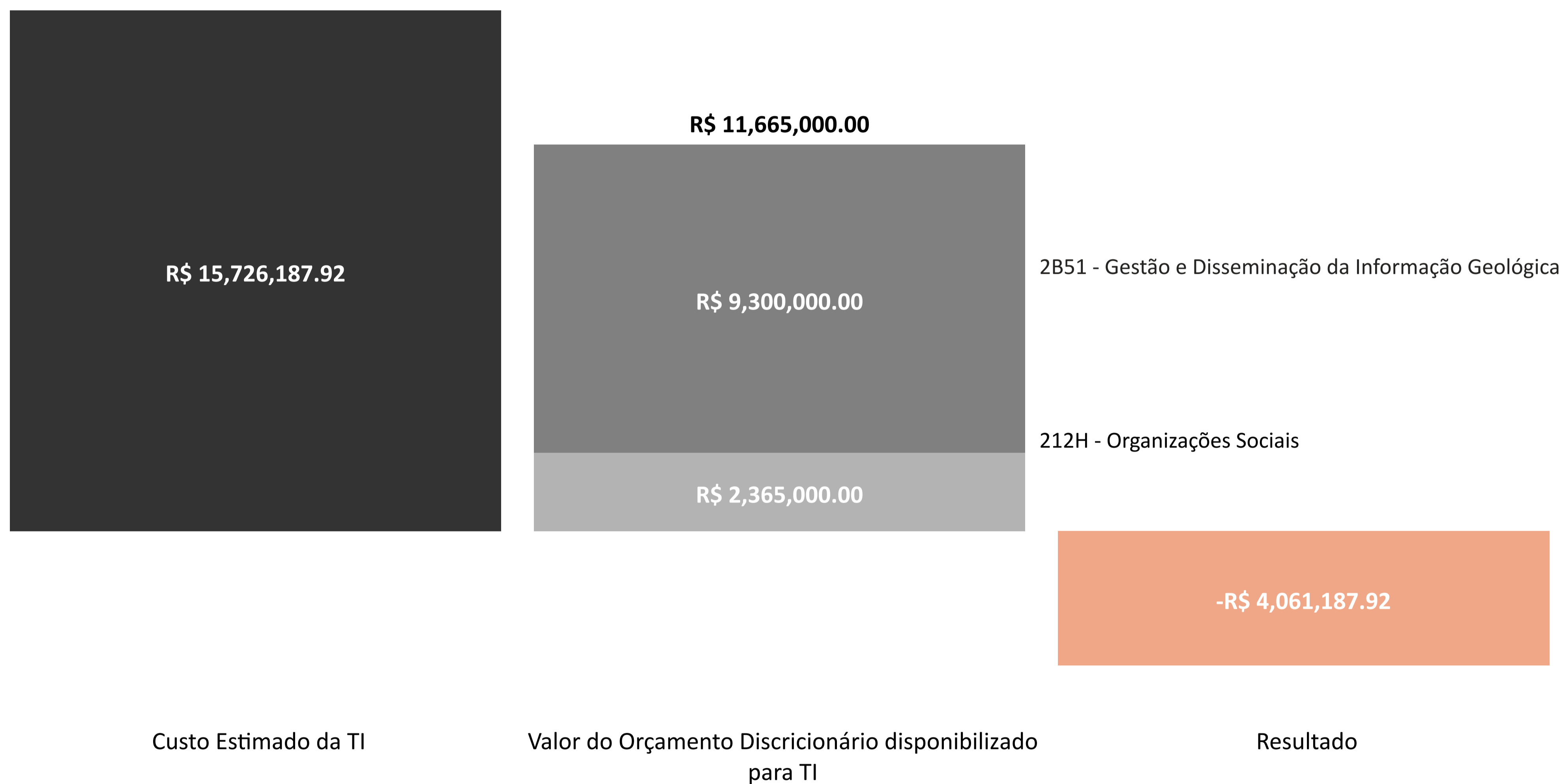
ORÇAMENTO - SITUAÇÃO ATUAL

Visão Geral

Situação Atual

Detalhamento

Receita x Despesa 2023



O orçamento discricionário da TI para 2023 está segregado em duas rubricas:

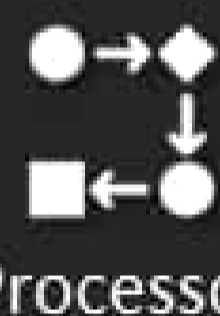
2B51 - Gestão e Disseminação da Informação Geológica - **R\$ 9.3M**

212H - Organizações Sociais - **R\$ 2.3M**

Total do orçamento discricionário disponibilizado para TI: **R\$ 11.6M**

O orçamento discricionário disponibilizado para a TI corresponde à **74,18% do custo total projetado*** para 2023, que é de **R\$ 15.7M**. Isto demonstra que a TI possui, para 2023, um **GAP orçamentário de aproximadamente R\$ 4M**, o que corresponde à **25,82% do custo projetado**.

*O Custo total projetado para TI em 2023 é baseado em contratos já existentes.



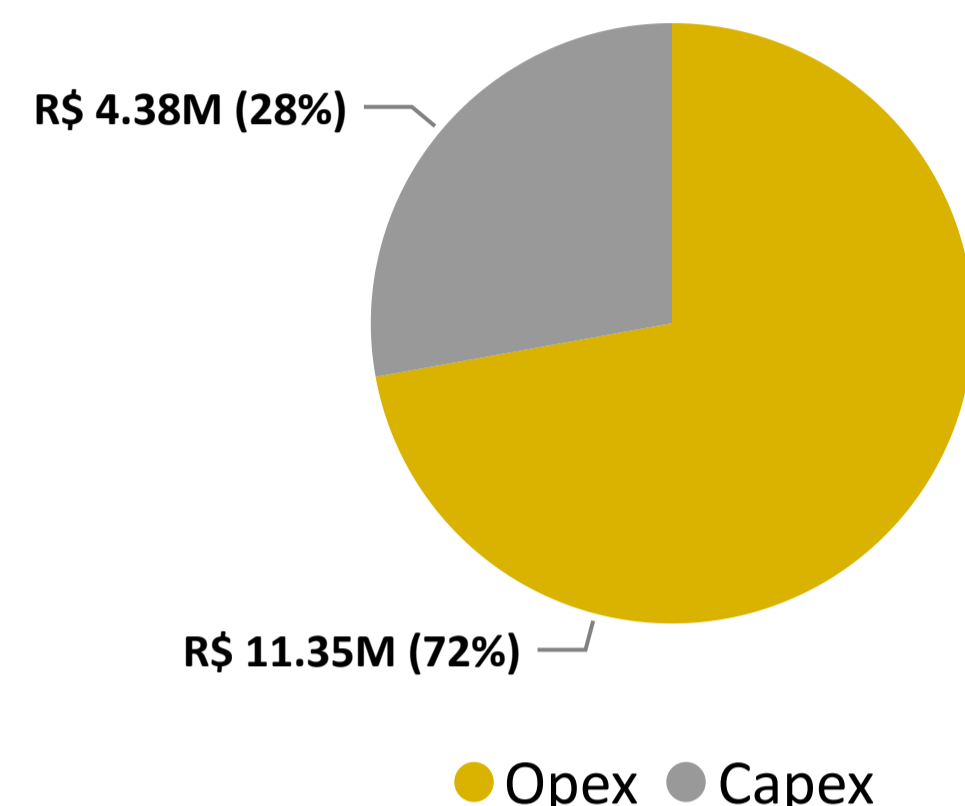
ORÇAMENTO - DETALHAMENTO

Visão Geral

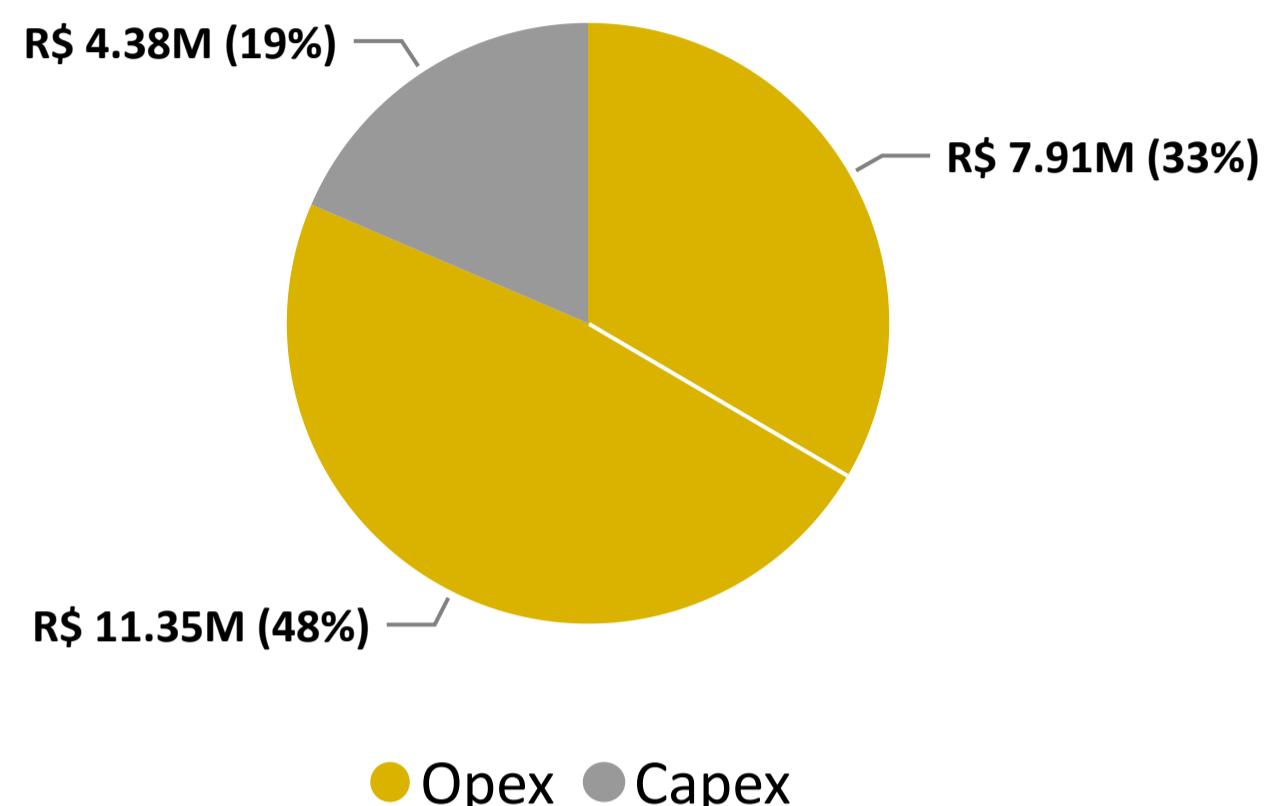
Situação Atual

Detalhamento

Classificação CAPEX x OPEX - Orçamento Discricionário



Classificação CAPEX x OPEX - Orçamento TI



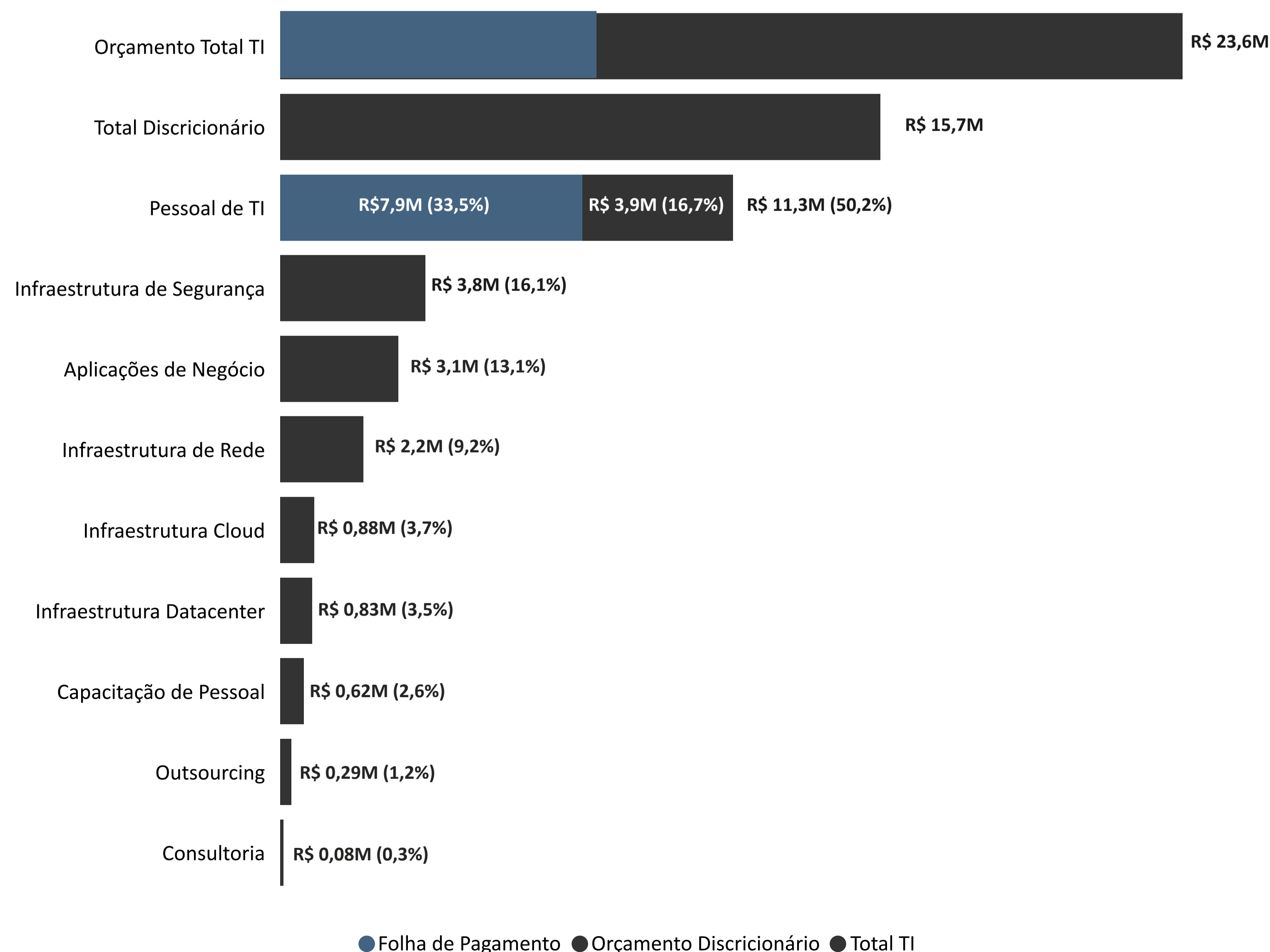
Segregamos o orçamento previsto da TI para 2023 em despesas operacionais (OPEX) e despesas de capital (CAPEX).

Do orçamento total previsto para a TI em 2023, **81%** corresponde a **despesas operacionais (OPEX)** e **19%** **despesas de capital (CAPEX)**.

Do orçamento discricionário previsto para TI em 2023, **72%** corresponde a despesas operacionais (OPEX) e **28%** despesas de capital (CAPEX).

A **diferença** de valores entre o orçamento discricionário e o orçamento da TI corresponde à **R\$ 7,91M**, que se refere ao pagamento do pessoal próprio da TI, que é custeado pela **folha de pagamento** e não incide no **orçamento discricionário da TI**.

Custo Estimado da TI por Categoria 2023



O Orçamento da TI previsto para 2023 foi segregado em 9 categorias:

Pessoal de TI – Inclui todos os custos de pessoal terceirizado e interno. Apenas o custo referente ao pessoal terceirizado incide no orçamento discricionário da TI.

Aplicações de Negócio - Inclui taxas de licença e manutenção de software, custos de aquisição e desenvolvimento para aplicativos externos e custos de assinatura para aplicativos hospedados ou software-como-serviço (SaaS).

Infraestrutura de Rede - Inclui todo o hardware e software de rede e sistemas de comunicação.

Infraestrutura de Segurança - Inclui os custos de aquisição e manutenção de hardware, software e serviços de segurança, como auditorias de segurança, avaliações, testes e serviços de segurança gerenciados.

Infraestrutura Data Center - (hardware/software) - Inclui servidores, armazenamento e software do sistema operacional associado. Também inclui utilitários de data center, sistemas de automação, aplicativos de gerenciamento de armazenamento e aplicativos de gerenciamento de sistemas.

Infraestrutura Cloud - Inclui os custos referentes aos serviços contratados na nuvem.

Outsourcing - Inclui os custos de leasing e manutenção de todas as impressoras, copiadoras, scanners, plotters e consumíveis relacionados. Inclui serviços de impressão gerenciados.

Consultoria - Inclui custos relacionados a consultoria especializada para softwares e banco de dados.

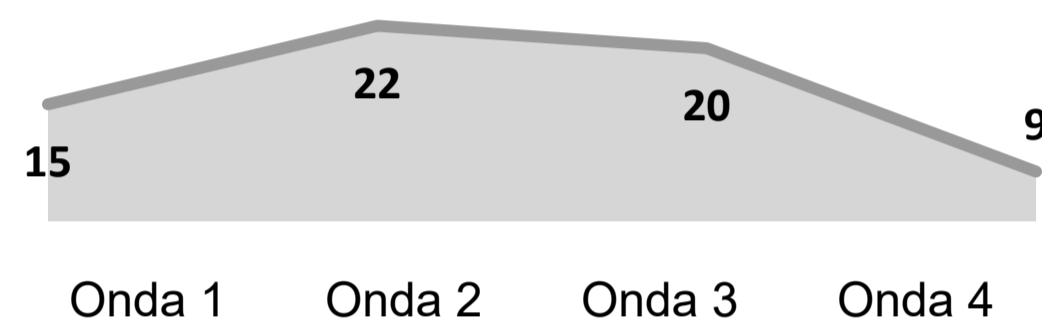
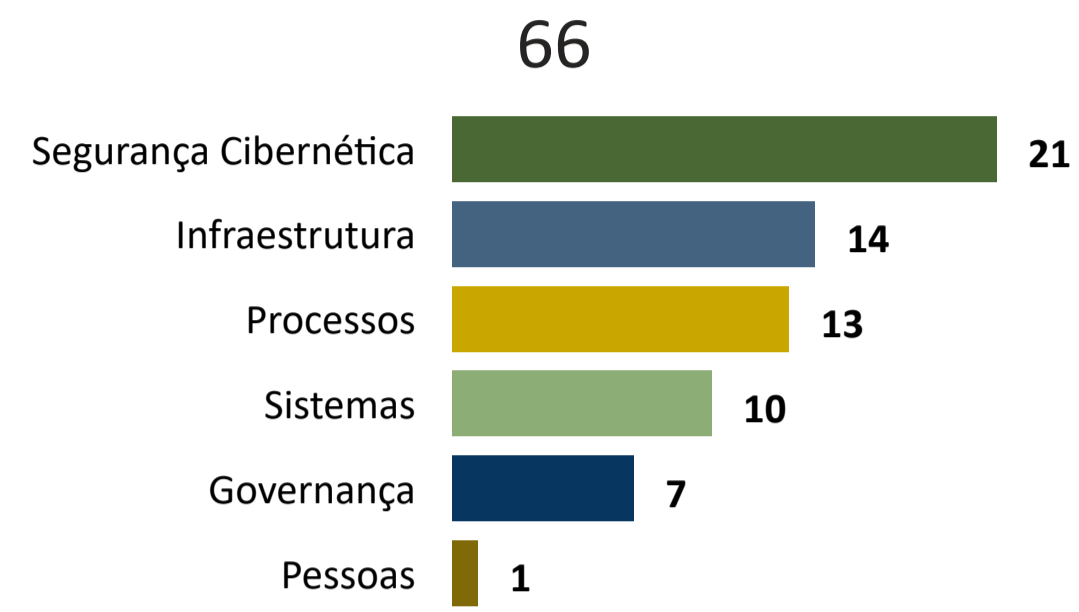
Capacitação de Pessoal - Inclui custos relacionados a treinamentos do pessoal de TI.

- Painel 
- Estratégia 
- Pessoas 
- Processos 
- Tecnologia 
- Orçamento 
- Roadmap** 
- Anexos 

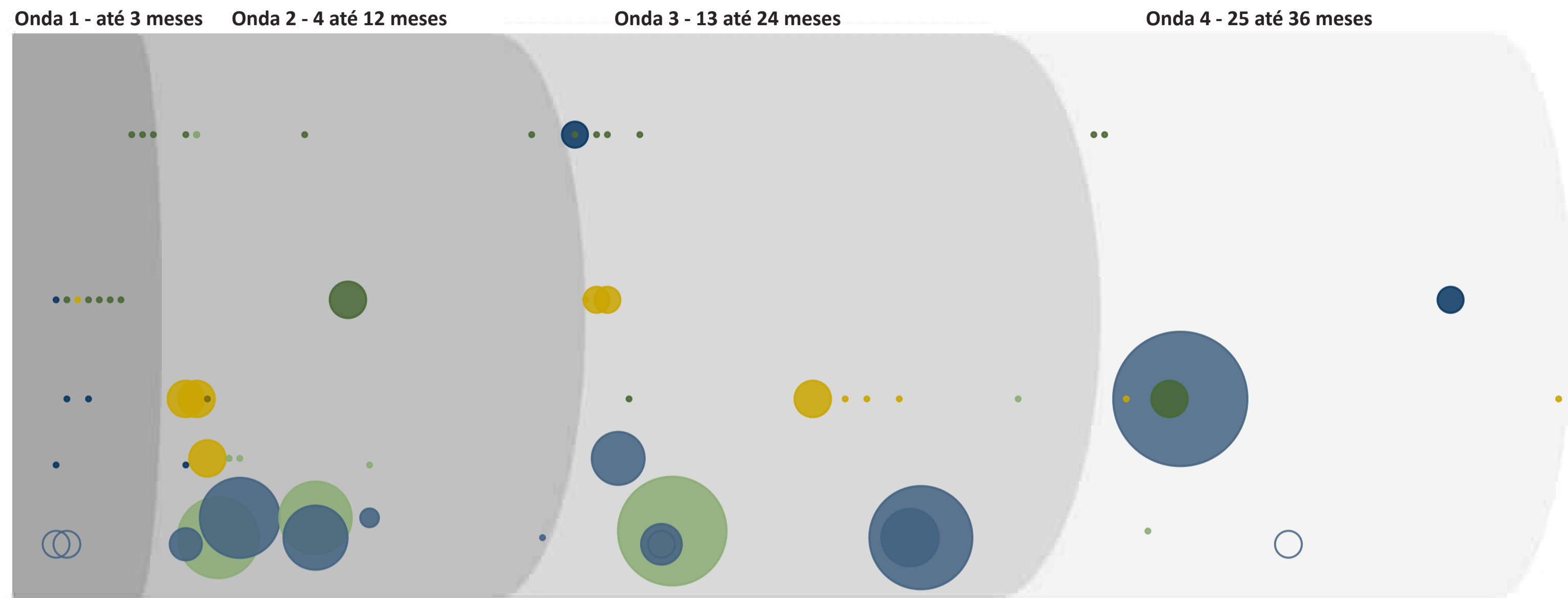
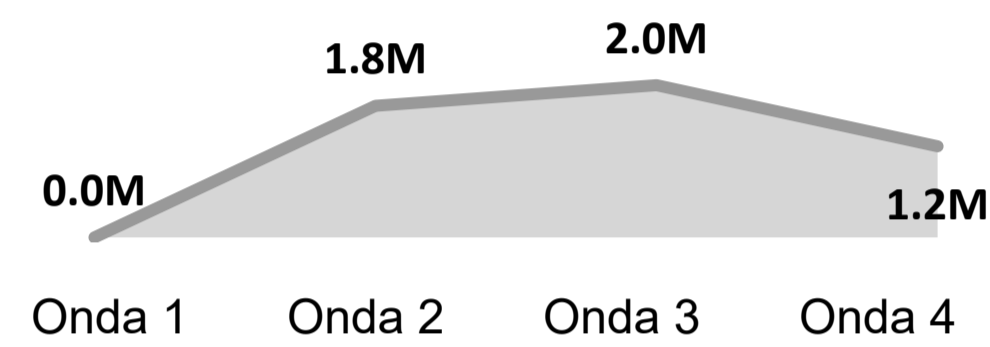
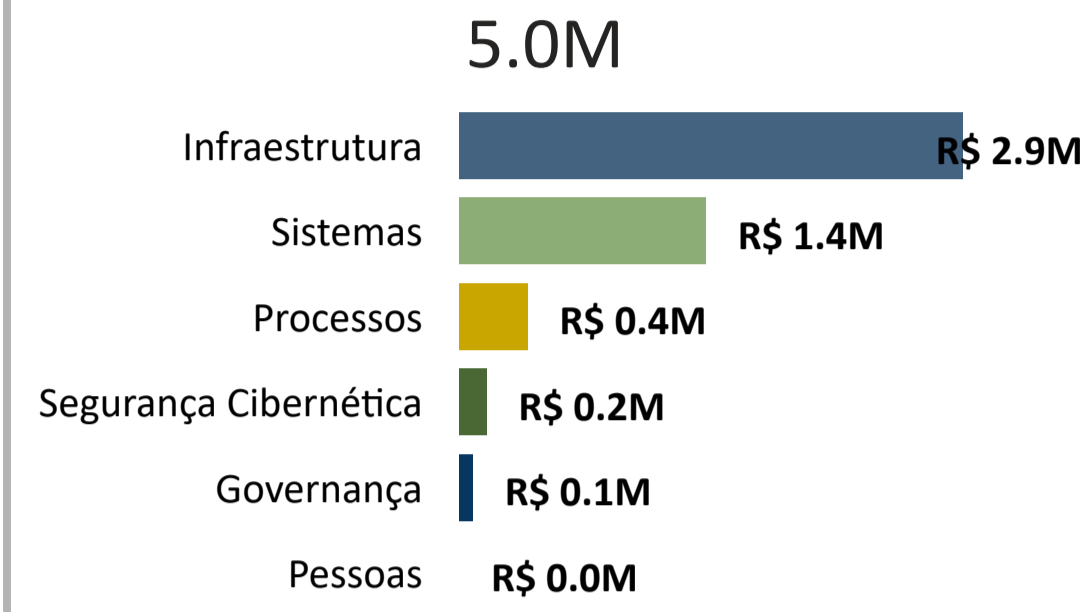
ROADMAP DE INICIATIVAS DE TI ↩



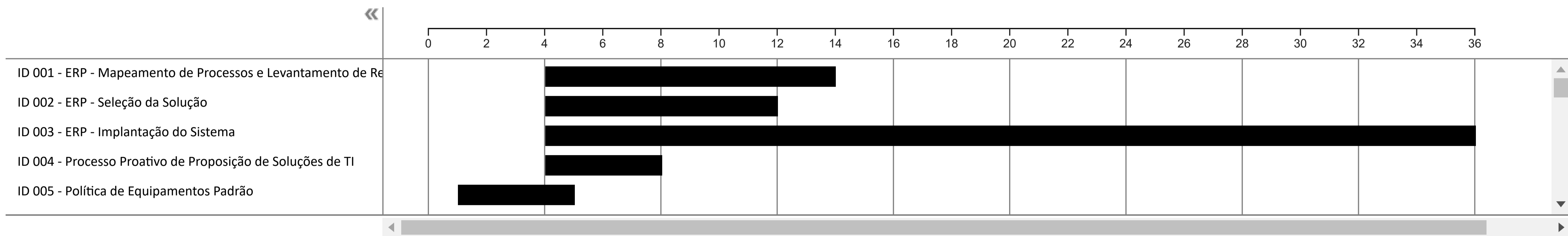
Quantidade de Recomendações



Estimativa de Investimento



Linha do Tempo



Tema	Issue	Risco de TI	Risco de Negócio
Duração em Semanas	Predecessora		
Estimativa de Investimento	Recomendação		
Critério de Priorização			
Sinergia Financeira			
Exequibilidade			
Sinergia na Operação			



ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética

Sistemas
1

Quantidade de Recomendações

1

Estimativa de Investimento

400.0K

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Sistemas



1

Sistemas



R\$ 0.40M

Prioridade

1

0.40M

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4



Linha do Tempo



4 5 6 7 8 9 10 11 12 13 14

ID 001 - ERP - Mapeamento de Processos e Levantamento de Re



Sistemas

ID 001 - ERP - Mapeamento de Processos e Levantamento de Requisitos

Tema
ERP

Duração em Semanas
10

Estimativa de Investimento
R\$ 400K

Critério de Priorização
Sinergia Financeira
Baixa

Exequibilidade
Média

Sinergia na Operação
Baixa

Issue
Utilização de sistemas departamentais sem integração e alto volume de controles manuais.

Predecessora
N/A

Recomendação
Apoiar as áreas Administrativas na contratação de consultoria técnica especializada para mapeamento de processos e levantamento de requisitos funcionais e não funcionais para implantação de sistema ERP.

Risco de TI
N/A

Risco de Negócio
N/A



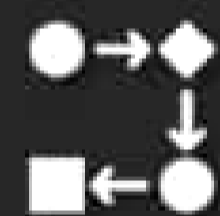
Painel



Estratégia



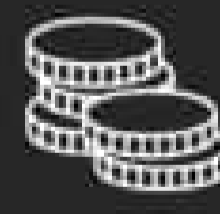
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI

Painel

Estratégia

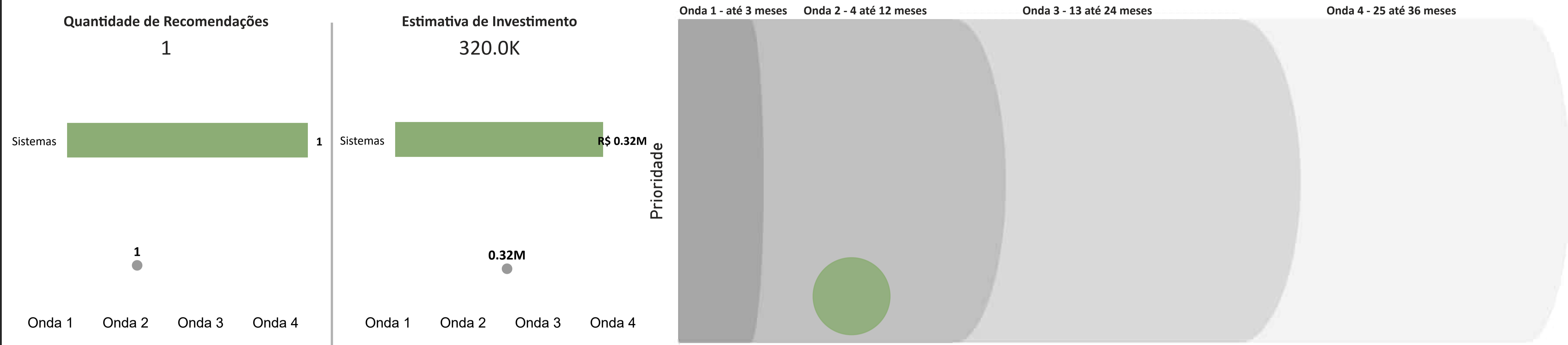
Pessoas

Processos

Tecnologia

Orçamento

Roadmap



Sistemas	ID 002 - ERP - Seleção da Solução		
Tema ERP	Issue Utilização de sistemas departamentais sem integração e alto volume de controles manuais.	Risco de TI N/A	Risco de Negócio N/A
Duração em Semanas 8	Predecessora ID 001 - ERP - Mapeamento de Processos e Levantamento de Requisitos		
Estimativa de Investimento R\$ 320K	Recomendação Apoiar as áreas Administrativas na contratação de consultoria técnica especializada na seleção da solução ERP mais adequada às necessidades do SGB, escrita de RFP e "Business Case" para seleção de fornecedor e implantação sistêmica.		
Critério de Priorização			
Sinergia Financeira Baixa			
Exequibilidade Média			
Sinergia na Operação Média			

ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética

Sistemas
1

Quantidade de Recomendações

1

Estimativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Sistemas



1

Sistemas R\$ 0

1

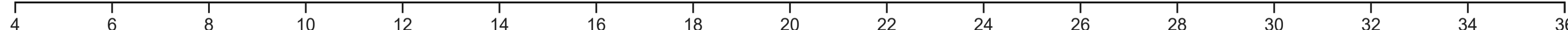
0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade

Linha do Tempo



ID 003 - ERP - Implantação do Sistema



Sistemas

ID 003 - ERP - Implantação do Sistema

Tema
ERP

Duração em Semanas
48

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Baixa

Exequibilidade
Alta

Sinergia na Operação
Alta

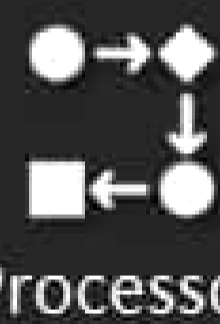
Issue
Utilização de sistemas departamentais sem integração e alto volume de controles manuais.

Predecessora
ID 002 - ERP - Seleção da Solução

Recomendação
Apoiar as áreas Administrativas na contratação de consultoria técnica especializada para implantação de sistema ERP selecionado, gestão da mudança cultural e organizacional, gerenciamento do programa e controle de qualidade das entregas.

Risco de TI
Maior vulnerabilidade a ataques cibernéticos;
Alta complexidade para sustentação dos sistemas;

Risco de Negócio
Ineficiência operacional;
Falhas causadas por interações humanas;
Alto índice de controles manuais de apoio;
Informações sistêmicas descentralizadas.



ROADMAP DE INICIATIVAS DE TI ↩



Quantidade de Recomendações
1

Esmativa de Investimento
0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Governança 1

Governança R\$ 0

Prioridade

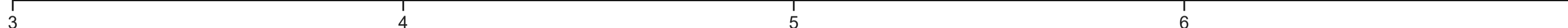
1

0

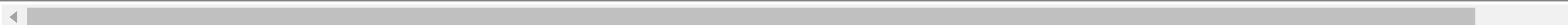
Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Linha do Tempo



ID 004 - Processo Proativo de Proposição de Soluções de TI



Governança

ID 004 - Processo Proativo de Proposição de Soluções de TI

Tema
Liderança

Issue
Gestão do relacionamento com o negócio ineficiente.

Risco de TI
Ineficácia das operações de TI

Risco de Negócio
Não atendimento das necessidades pela TI

Duração em Semanas
4

Predecessora
N/A

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Baixa

Recomendação
Estabelecer processo proativo de proposição de soluções de TI para atendimento às necessidades do negócio, mapeando os pontos focais de cada área da empresa, definindo suas responsabilidades, frequência e forma de atuação.

Exequibilidade
Alta

Sinergia na Operação
Alta



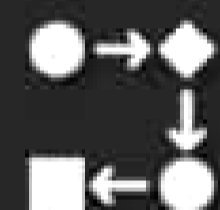
Painel



Estratégia



Pessoas



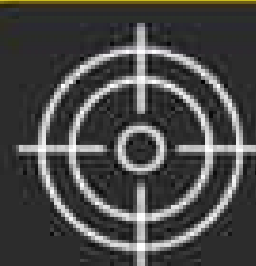
Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI ↩



Quantidade de Recomendações

1

Governança



1

1

Onda 1 Onda 2 Onda 3 Onda 4

Esmatima de Investimento

0.0

Governança R\$ 0

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Prioridade

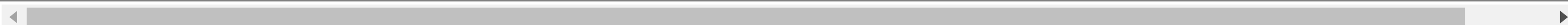


Linha do Tempo



1 2 3 4 5

ID 005 - Política de Equipamentos Padrão



Governança

Tema
Liderança

Duração em Semanas
4

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Média

Exequibilidade
Média

Sinergia na Operação
Alta

ID 005 - Política de Equipamentos Padrão

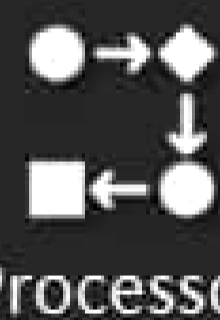
Issue
Inexistência de padronização dos equipamentos.

Predecessora
N/A

Recomendação
Estabelecer política padrão dos equipamentos de tecnologia e divulgar para toda companhia.

Risco de TI
Suporte à diversos modelos de equipamentos com contratos descentralizados.

Risco de Negócio
N/A



ROADMAP DE INICIATIVAS DE TI ↩



Quantidade de Recomendações

1

Governança



1

1

Onda 1 Onda 2 Onda 3 Onda 4

Esmativa de Investimento

0.0

Governança R\$ 0

0

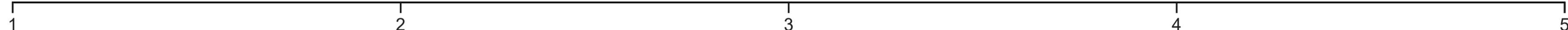
Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

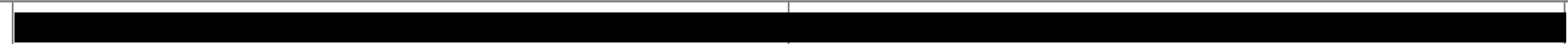
Prioridade



Linha do Tempo



ID 006 - Processo Make or Buy para aquisição de Softwares.



Governança

Tema
Liderança

Duração em Semanas
4

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Média

Exequibilidade
Alta

Sinergia na Operação
Alta

ID 006 - Processo Make or Buy para aquisição de Softwares.

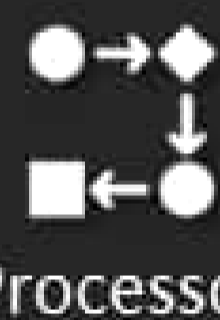
Issue
Processo decisório para aquisição de softwares ineficiente.

Predecessora
N/A

Recomendação
Estabelecer diretrizes e processo estruturado para aquisição de novos softwares e/ou desenvolvimento dos mesmos para atendimento às áreas de negócio; (Processo Make or Buy).

Risco de TI
Maior esforço na construção de ferramentas existentes no mercado.

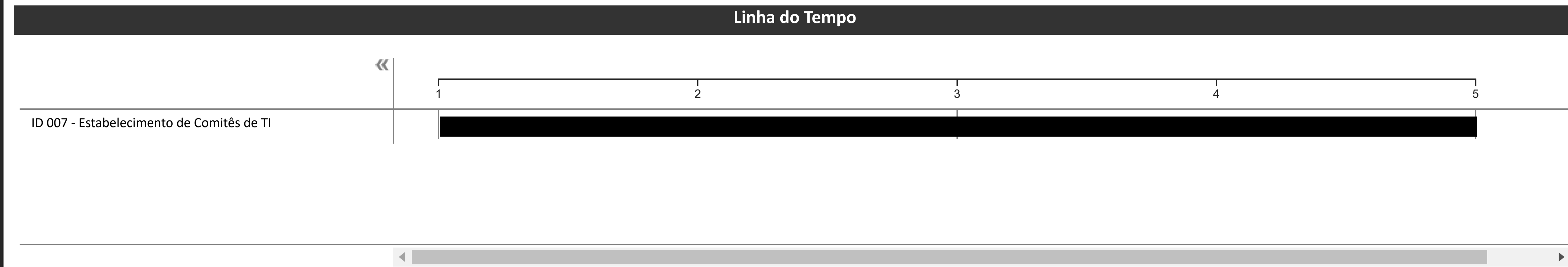
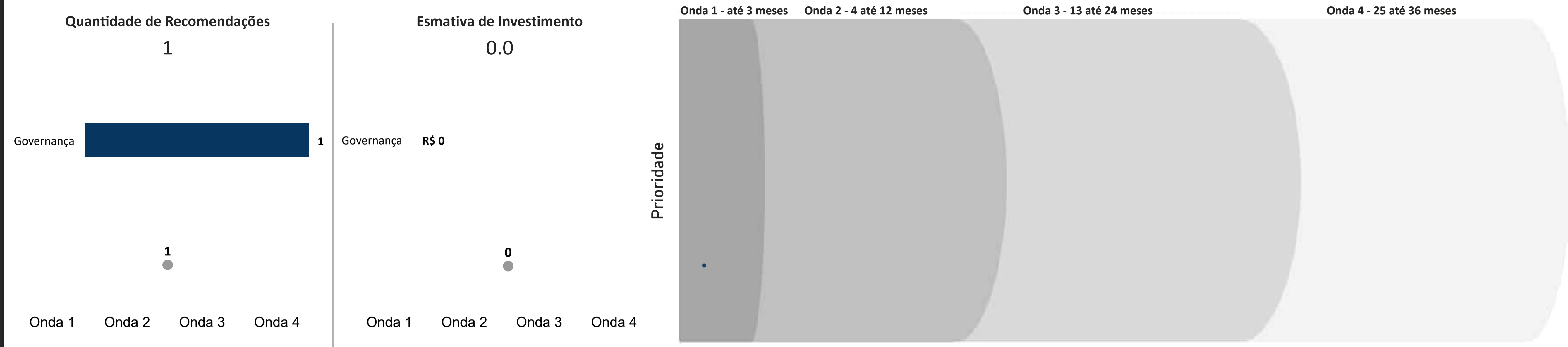
Risco de Negócio
Demora e custo excessivo no aporte de soluções sistêmicas.



ROADMAP DE INICIATIVAS DE TI

- Painel
- Estratégia
- Pessoas
- Processos
- Tecnologia
- Orçamento
- Roadmap

Governança 1	Infraestrutura	Pessoas	Processos	Segurança Cibernética	Sistemas
-----------------	----------------	---------	-----------	-----------------------	----------



Governança	ID 007 - Estabelecimento de Comitês de TI		
<p>Tema</p> <p style="text-align: center;">Comissões</p>	<p>Issue</p> <p style="text-align: center;">Ausência de comitês de TI.</p>	<p>Risco de TI</p> <p style="text-align: center;">Desalinhamento estratégico da TI com o negócio.</p>	<p>Risco de Negócio</p> <p style="text-align: center;">N/A</p>
<p>Duração em Semanas</p> <p style="text-align: center;">4</p>	<p>Predecessora</p> <p style="text-align: center;">N/A</p>		
<p>Estimativa de Investimento</p> <p style="text-align: center;">N/A</p>	<p>Recomendação</p> <p style="text-align: center;">Estabelecer Comitês que enderecem os assuntos de Governança de TI, Projetos e Inovação de TI, observando suas responsabilidades, periodicidade e público alvo, estabelecendo ponto focal de TI em cada unidade regional para participação nos comitês aplicáveis.</p>		
<p>Critério de Priorização</p> <p>Sinergia Financeira</p> <p style="text-align: center;">Baixa</p>			
<p>Exequibilidade</p> <p style="text-align: center;">Alta</p>			
<p>Sinergia na Operação</p> <p style="text-align: center;">Alta</p>			

ROADMAP DE INICIATIVAS DE TI ↶



Quantidade de Recomendações

1



1

Onda 1 Onda 2 Onda 3 Onda 4

Esmativa de Investimento

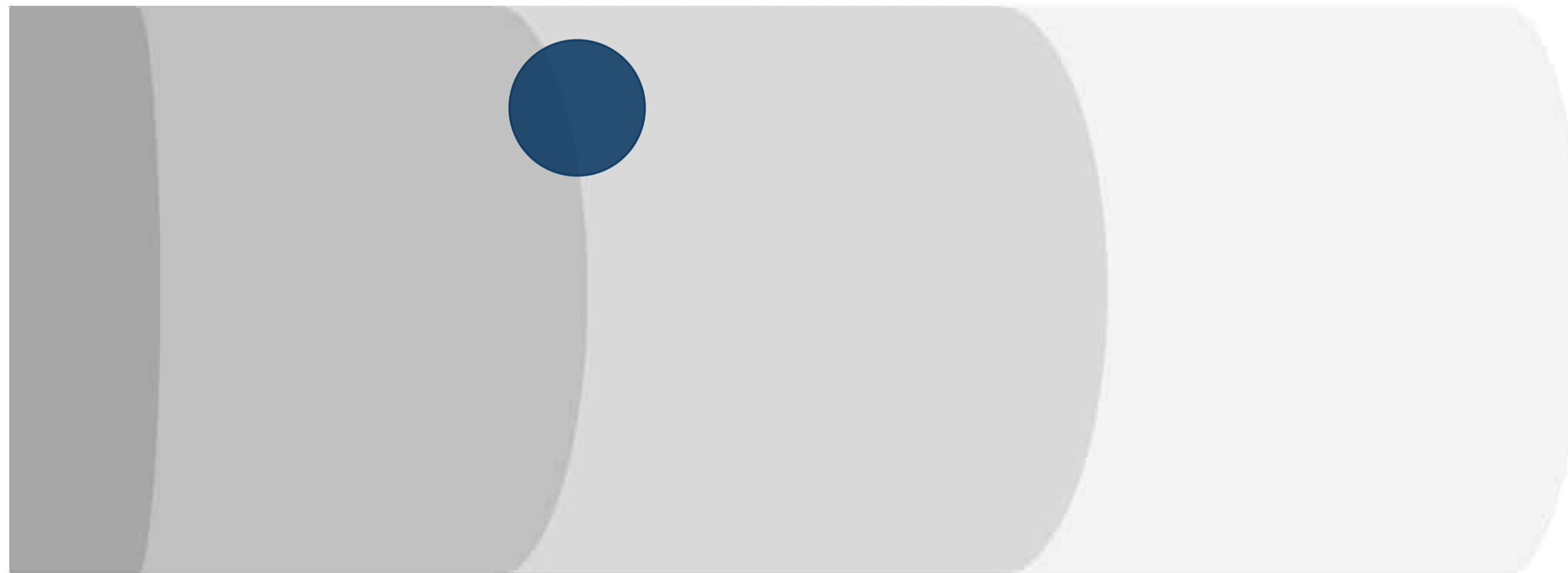
40.0K



40K

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses



Prioridade

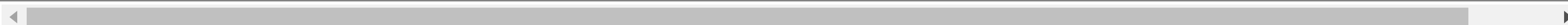
Linha do Tempo



6

8

ID 008 - Estratégia de Terceirização



Governança

Tema
Planejamento

Duração em Semanas
2

Estimativa de Investimento
R\$ 40K

Critério de Priorização
Sinergia Financeira
Alta

Exequibilidade
Alta

Sinergia na Operação
Alta

ID 008 - Estratégia de Terceirização

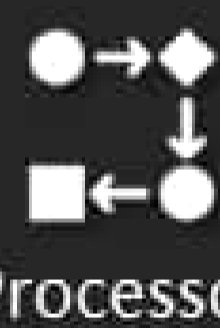
Issue
Ausência de estratégia para adoção de serviços de TI terceirizados.

Predecessora
N/A

Risco de TI
Contratações ad-hoc de terceiros.

Risco de Negócio
Ineficiência no atendimento de demandas pela TI

Recomendação
Definir estratégia de terceirização de fornecedores, considerando os tipos de serviços e as responsabilidades que devem ser mantidas com a equipe interna de TI ou repassadas a terceiros.

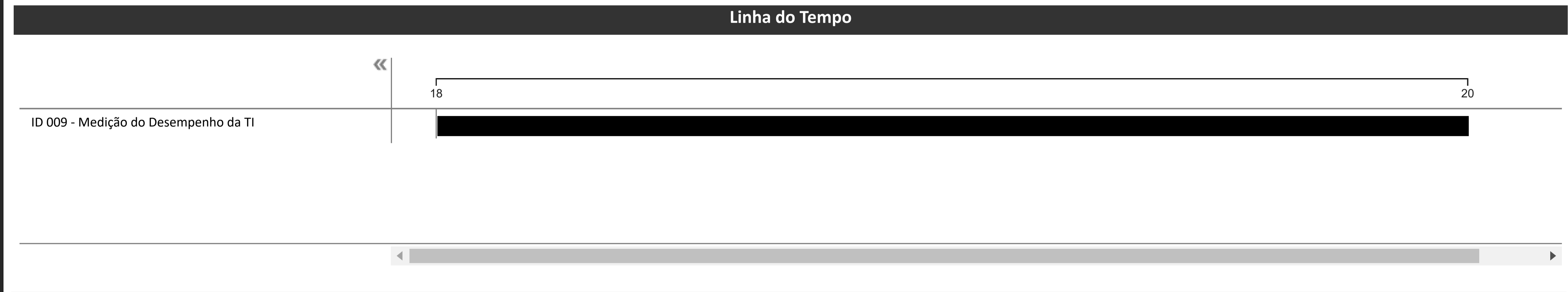
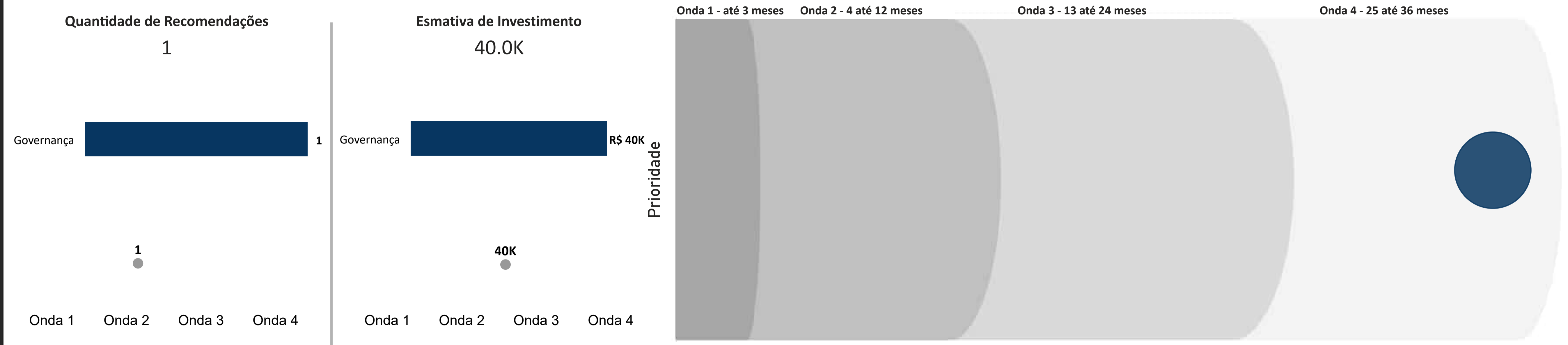


Roadmap

ROADMAP DE INICIATIVAS DE TI

- Painel
- Estratégia
- Pessoas
- Processos
- Tecnologia
- Orçamento
- Roadmap

Governança 1	Infraestrutura	Pessoas	Processos	Segurança Cibernética	Sistemas
-----------------	----------------	---------	-----------	-----------------------	----------



Governança	ID 009 - Medição do Desempenho da TI		
Tema Monitoramento e Controle	Issue Apenas 2 metas definidas para o acompanhamento operacional de TI, não suficientes para a visão geral do desempenho.	Risco de TI Incapacidade de monitorar o desempenho da TI	Risco de Negócio N/A
Duração em Semanas 2	Predecessora N/A		
Estimativa de Investimento R\$ 40K	Recomendação Estabelecer KPIs e OKRs que possibilitem medir e monitorar o desempenho e a evolução de TI.		
Critério de Priorização			
Sinergia Financeira Média			
Exequibilidade Alta			
Sinergia na Operação Alta			

ROADMAP DE INICIATIVAS DE TI ↩



Quantidade de Recomendações

1

Governança



1

1

Onda 1 Onda 2 Onda 3 Onda 4

Esmativa de Investimento

0.0

Governança R\$ 0

0

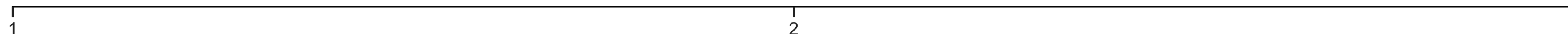
Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Prioridade



Linha do Tempo



ID 010 - Gestão de Penalidades



Governança

ID 010 - Gestão de Penalidades

Tema
Monitoramento e Controle

Duração em Semanas
2

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Média

Exequibilidade
Alta

Sinergia na Operação
Média

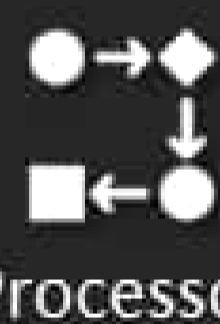
Issue
Contratos estabelecidos entre TI e fornecedores possuem penalidades previstas, porém não foram identificadas práticas nem processos formais para aplicação das penalidades previstas, quando aplicáveis.

Predecessora
N/A

Recomendação
Estabelecer processo de monitoramento dos serviços contratados e, na ocorrência de fatos geradores de penalidades previstas em contrato, acionar departamento jurídico e avaliar sua aplicabilidade.

Risco de TI
Degradação do serviço prestado pelos fornecedores pela falta de aplicação de penalidades previstas em contrato.

Risco de Negócio
N/A



ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

80.0K

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Processos



1

Processos



R\$ 80K

Prioridade



Onda 1

Onda 2

Onda 3

Onda 4

Onda 1

Onda 2

Onda 3

Onda 4

Linha do Tempo



3

4

5

6

7

ID 011 - Processo de Controle Orçamentário



Processos

ID 011 - Processo de Controle Orçamentário

Tema
Controle Orçamentário

Duração em Semanas
4

Estimativa de Investimento
R\$ 80K

Critério de Priorização
Sinergia Financeira
Alta

Exequibilidade
Média

Sinergia na Operação
Média

Issue
Ausência de processo definido e documentado para controle de entrada, saída e orçamentário. Não há definição clara sobre os papéis e responsabilidades acerca da análise e reporte da gestão financeira.

Predecessora
N/A

Recomendação
Mapear e documentar o processo de controle orçamentário, incluindo documentação do esquema de classificação orçamentária, matriz RACI e periodicidade de reportes.

Risco de TI
Gestão Orçamentária Ineficiente

Risco de Negócio
N/A



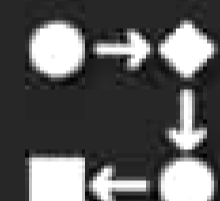
Painel



Estratégia



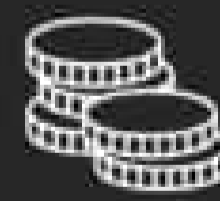
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura

Pessoas

Processos
1

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

40.0K

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Processos



1

Processos



R\$ 40K

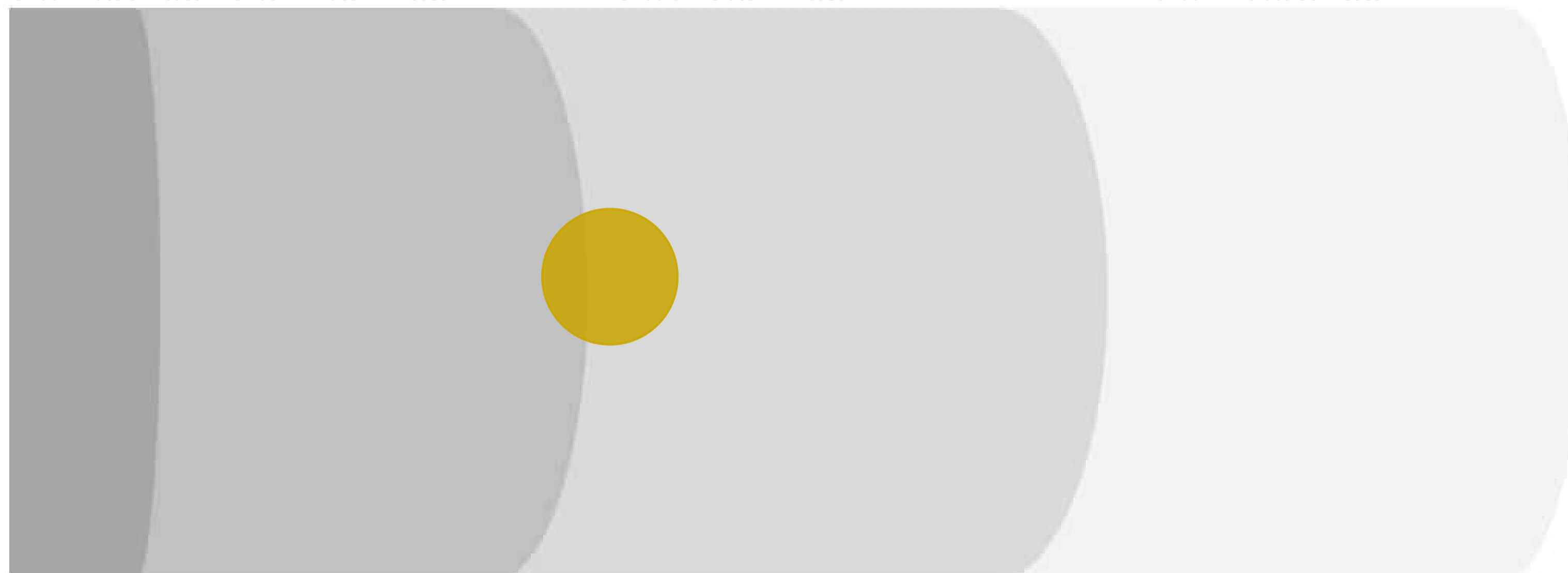
Prioridade

1

40K

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4



Linha do Tempo



6

8

ID 012 - Priorização Orçamentária



Processos

ID 012 - Priorização Orçamentária

Tema
Alocação de Recursos

Issue
Inexistência de um processo documentado para priorização orçamentária.

Risco de TI
Gestão Orçamentária Ineficiente

Risco de Negócio
N/A

Duração em Semanas
2

Predecessora
ID 009 - Medição do Desempenho da TI

Estimativa de Investimento
R\$ 40K

Critério de Priorização
Sinergia Financeira
Alta

Recomendação
Estabelecer um processo para priorização orçamentária, assim como para estabelecer comunicações de decisões orçamentárias.

Exequibilidade
Alta

Sinergia na Operação
Média



ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura

Pessoas

Processos
1

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

40.0K

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Processos



1

Processos



R\$ 40K

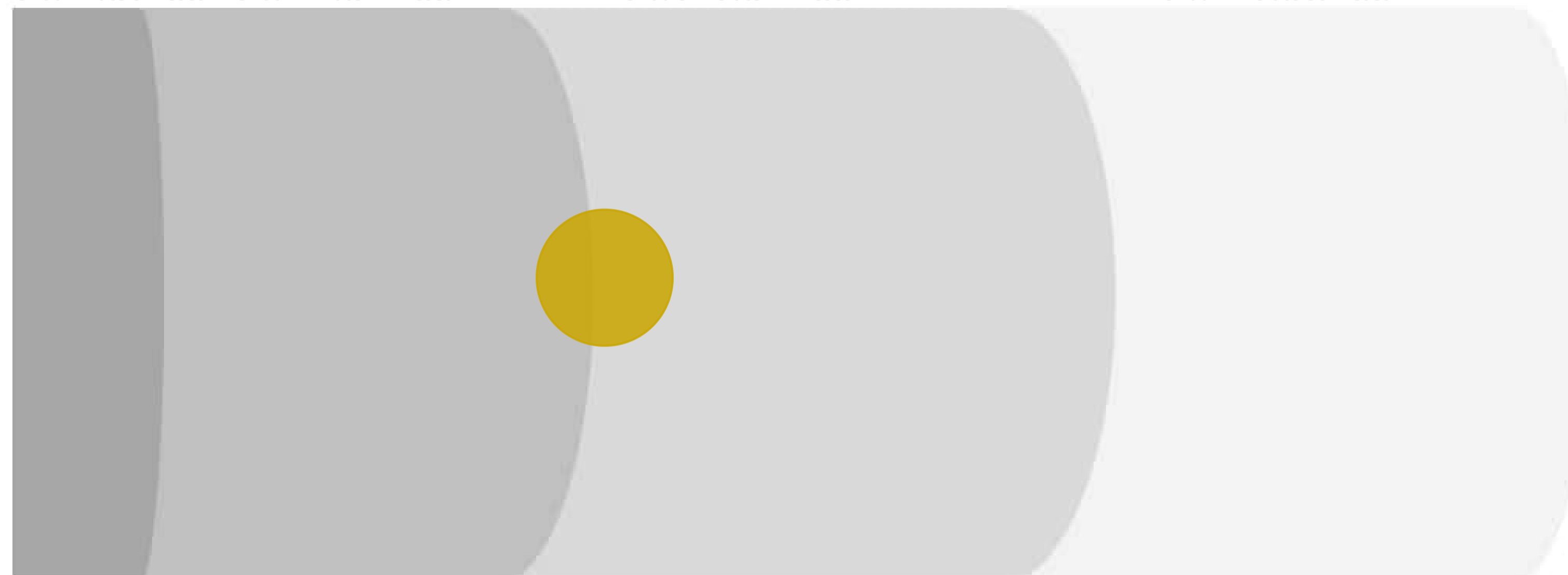
Prioridade

1

40K

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4



Linha do Tempo



6

8

ID 013 - Processo de Compra ou Locação de Ativos



Processos

ID 013 - Processo de Compra ou Locação de Ativos

Tema
Alocação de Recursos

Duração em Semanas
2

Estimativa de Investimento
R\$ 40K

Critério de Priorização
Sinergia Financeira
Alta

Exequibilidade
Alta

Sinergia na Operação
Média

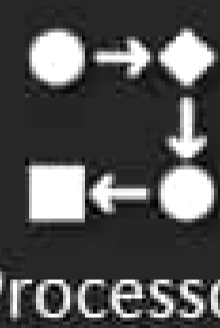
Issue
Falta de um procedimento documentado para verificação de opções entre comprar ativos/serviços ou contratação de uso de ativos/serviços.

Predecessora
ID 006 - Processo Make or Buy para aquisição de Softwares.

Recomendação
Elaborar um processo para que se verifique entre a opção de compra ou locação do ativo, assim como desenvolver internamente um serviço ou contratá-lo externamente, a cada solicitação de compra de ativo ou serviço.

Risco de TI
Gestão Orçamentária Ineficiente

Risco de Negócio
N/A



ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura

Pessoas

Processos
1

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Processos



1

Processos

R\$ 0

1

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade



Linha do Tempo



6

8

ID 014 - Elaboração Orçamentária



Processos

ID 014 - Elaboração Orçamentária

Tema
Elaboração Orçamentária

Issue
Na criação do orçamento, não há uma documentação de quais componentes considerar.

Risco de TI
Gestão Orçamentária Ineficiente

Risco de Negócio
N/A

Duração em Semanas
2

Predecessora
ID 009 - Medição do Desempenho da TI

Estimativa de Investimento
N/A

Recomendação
Criar uma documentação contendo os componentes a considerar na elaboração do orçamento, registrando a lógica realizada na elaboração.

Critério de Priorização
Sinergia Financeira
Alta

Exequibilidade
Alta

Sinergia na Operação
Média



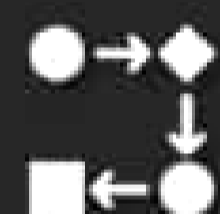
Painel



Estratégia



Pessoas



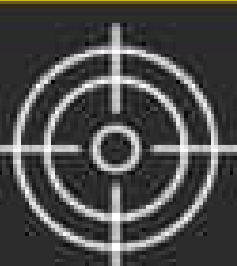
Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética

Sistemas

1

Quantidade de Recomendações

1



1

Onda 1 Onda 2 Onda 3 Onda 4

Esmativa de Investimento

0.0

Processos R\$ 0

0

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade



Linha do Tempo



18 19 20 21 22

ID 015 - Coleta de Dados Orçamentários



Processos

ID 015 - Coleta de Dados Orçamentários

Tema
Dados Orçamentários

Duração em Semanas
4

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Alta

Exequibilidade
Média

Sinergia na Operação
Média

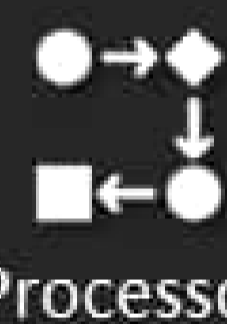
Issue
Não há um processo para coleta de dados relevantes para identificar desvios no orçamento quanto ao real praticado, tendências do custo de serviços e ROI do investimento, quando aplicável.

Predecessora
ID 009 - Medição do Desempenho da TI

Recomendação
Definir, documentar e implementar um processo para coleta e verificação de dados relevantes para mensurar possíveis desvios no orçamento quanto ao real praticado, tendências do custo de serviços e mensurar ROI do investimento, quando aplicável.

Risco de TI
Gestão Orçamentária Ineficiente

Risco de Negócio
N/A



ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Estima de Investimento

80.0K

Onda 1 - até 3 meses

Onda 2 - 4 até 12 meses

Onda 3 - 13 até 24 meses

Onda 4 - 25 até 36 meses

Processos



1

Processos



R\$ 80K

Prioridade

1

80K

Onda 1

Onda 2

Onda 3

Onda 4

Onda 1

Onda 2

Onda 3

Onda 4

Linha do Tempo



6

7

8

9

10

ID 016 - APO09 - Estabelecer processo Acordos de Serviços Gerenciados



Processos

ID 016 - APO09 - Estabelecer processo Acordos de Serviços Gerenciados

Tema
Acordos de Serviços Gerenciados

Duração em Semanas
4

Estimativa de Investimento
R\$ 80K

Critério de Priorização
Sinergia Financeira
Média

Exequibilidade
Média

Sinergia na Operação
Alta

Issue
Não há processo definido para análise, em uma linha de tempo, dos serviços atuais de TI e seus SLAs, para identificar lacunas entre o esperado pelo negócio e o realizado.

Predecessora
N/A

Recomendação
Estabelecer processo Acordos de Serviço Gerenciados para:
- Análise dos serviços atuais de TI e seus SLAs, verificando se está alinhado com as necessidades do negócio;
- Estudo que possibilite estimar a demanda futura de serviços de TI, para que se possa confirmar a capacidade dos serviços oferecidos;
- Definição dos SLAs necessários para os serviços a serem realizados e/ou contratados, assim como a definição dos ANOs para atendimento destes, quando aplicável.

Risco de TI
Ineficiência na prestação dos serviços ao negócio

Risco de Negócio
N/A



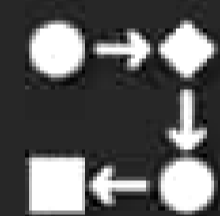
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura

Pessoas

Processos
1

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Processos



1

Processos

R\$ 0

1

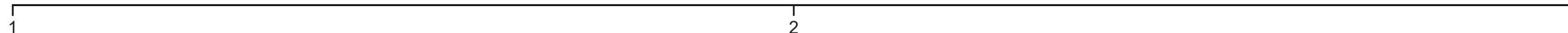
0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade

Linha do Tempo



ID 017 - APO09 - Atualização do Catálogo de Serviços de TI



Processos

ID 017 - APO09 - Atualização do Catálogo de Serviços de TI

Tema
Acordos de Serviços Gerenciados

Issue
Não há processo definido para atualização periódica do Catálogo de Serviços de TI

Risco de TI
N/A

Risco de Negócio
N/A

Duração em Semanas
2

Predecessora
N/A

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Média

Recomendação
Estabelecer processo para revisão periódica do Catálogo de Serviços de TI para atendimento às necessidades do negócio.

Exequibilidade
Alta

Sinergia na Operação
Alta



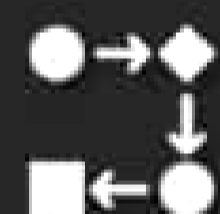
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI ↩



Quantidade de Recomendações

1

Processos



1

1

Onda 1 Onda 2 Onda 3 Onda 4

Esmatima de Investimento

80.0K

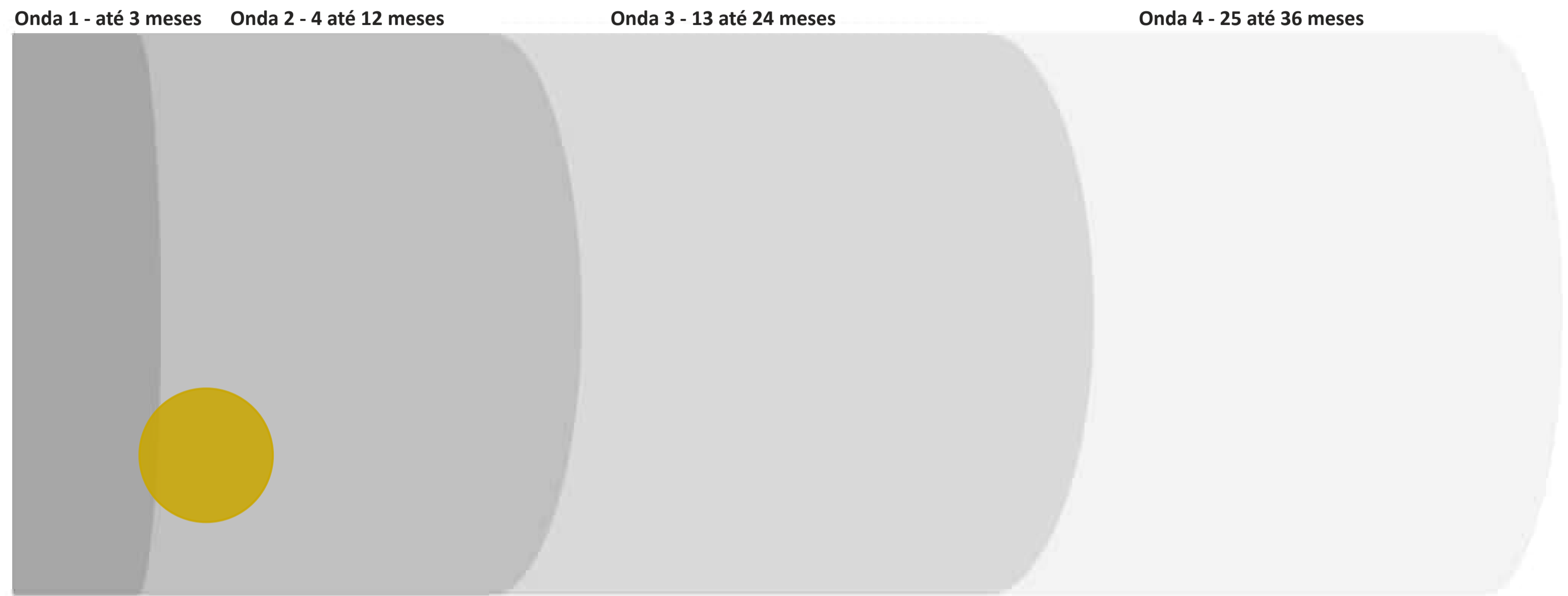
Processos



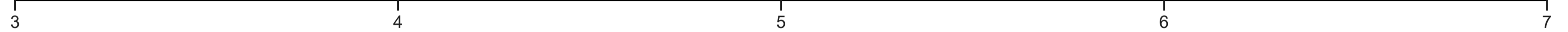
R\$ 80K

80K

Onda 1 Onda 2 Onda 3 Onda 4



Linha do Tempo



ID 018 - APO012 - Estabelecer processo Riscos Gerenciados



Processos

ID 018 - APO012 - Estabelecer processo Riscos Gerenciados

Tema
Riscos Gerenciados

Duração em Semanas
4

Estimativa de Investimento
R\$ 80K

Critério de Priorização
Sinergia Financeira
Média

Exequibilidade
Média

Sinergia na Operação
Média

Issue
Não há processo definido e implementado para gestão de riscos de TI.

Predecessora
N/A

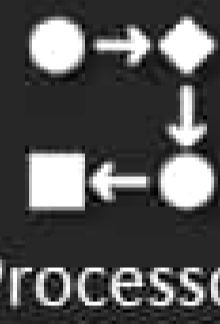
Risco de TI
Inexistência de identificação, documentação e classificação dos riscos de TI.

Risco de Negócio
N/A

Recomendação

Estabelecer processo de gestão de riscos de TI para:

- Documentar e manter um método para coleta, classificação e análise de dados relacionados a riscos de TI;
- Registrar dados relevantes e significativos no ambiente operacional interno e externo do SGB que possam estar relacionados à riscos;
- Criar o Mapa de Riscos de TI, agregando e documentando cenários de risco atuais por categoria, linha de negócio e área funcional.



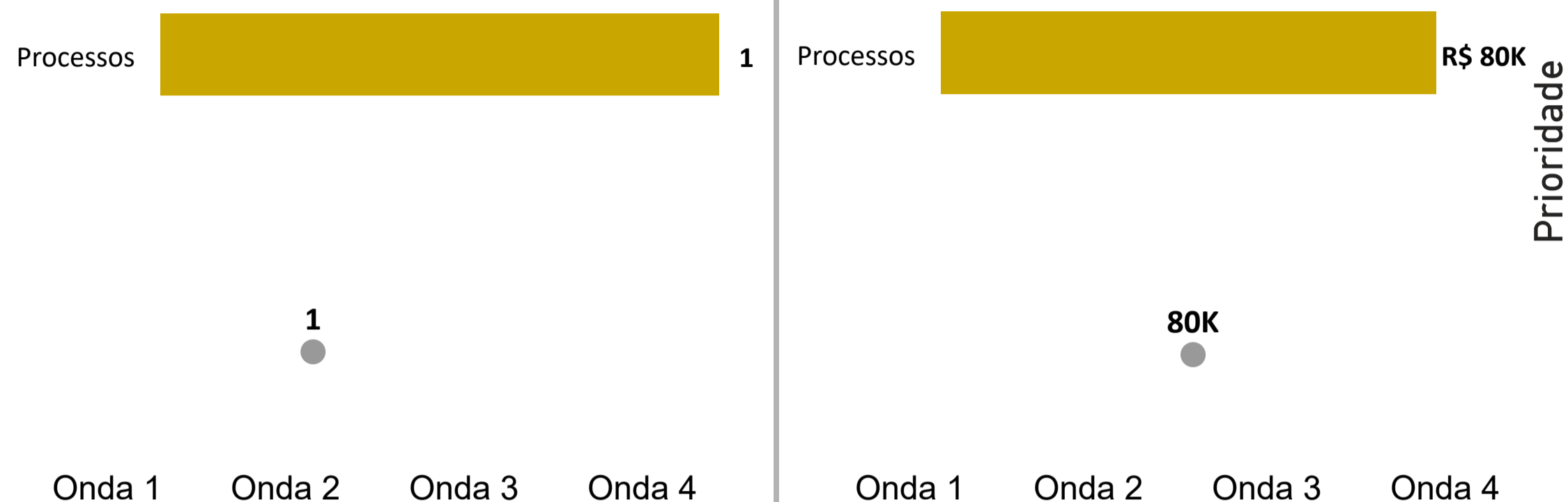
ROADMAP DE INICIATIVAS DE TI ↵



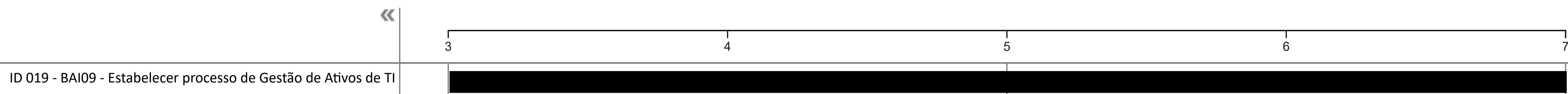
Quantidade de Recomendações
1

Esmativa de Investimento
80.0K

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

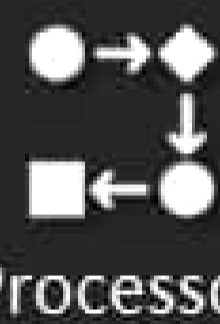


Linha do Tempo



Processos ID 019 - BAI09 - Estabelecer processo de Gestão de Ativos de TI

Tema Ativos Gerenciados	Issue Não existe um processo documentado e implementado para gestão de Ativos.	Risco de TI Ausência de controle dos ativos da empresa.	Risco de Negócio Fuga de Capital e multas por descumprimento de requisitos legais para licenciamento de softwares.
Duração em Semanas 4	Predecessora N/A		
Estimativa de Investimento R\$ 80K	Recomendação Estabelecer processo de Gestão de Ativos de TI para: - Identificar o inventário de ativos tecnológico, requisitos legais e regulatórios, ativos críticos, risco e impacto na falha de um ativo, adequação do ativo ao propósito; - Formalização do processo de compra de Ativo de TI; - Centralizar a gestão de licenças de software no departamento de TI; - Realizar estudo para escolha de ferramenta autônoma ou semi-autônoma de inventário de ativos tecnológicos na rede e realizar sua implementação.		
Critério de Priorização Sinergia Financeira Média			
Exequibilidade Média			
Sinergia na Operação Alta			



ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura

Pessoas

Processos
1

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Processos



1

Processos

R\$ 0

1

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade



Linha do Tempo



6 7 8 9 10

ID 020 - BAI06 - Estabelecer processo de Gestão de Mudança de



Processos

ID 020 - BAI06 - Estabelecer processo de Gestão de Mudança de TI

Tema
Mudanças de TI Gerenciadas

Duração em Semanas
4

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Média

Exequibilidade
Média

Sinergia na Operação
Alta

Issue
Não há processo de Gestão de Mudanças de TI

Predecessora
ID 017 - APO09 - Atualização do Catálogo de Serviços de TI

Recomendação

Estabelecer processo Gestão de Mudança para:

- Definir que toda mudança seja realizada através do processo de Gestão de Mudança, com requerimento e aprovação formal, categorização, priorização, planejamento e comunicação;
- Criar um registro de toda e qualquer mudança realizada, contendo informações do que foi realizado, quais configurações foram alteradas e etc. Manter este registro por um tempo determinado.

Risco de TI
Mudanças de TI não documentadas e/ou programadas.

Risco de Negócio
Instabilidade dos Serviços de TI



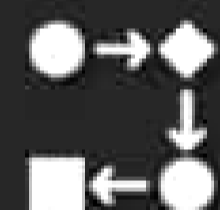
Painel



Estratégia



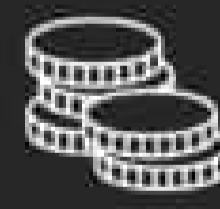
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura

Pessoas

Processos
1

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Processos



1

1

Onda 1 Onda 2 Onda 3 Onda 4

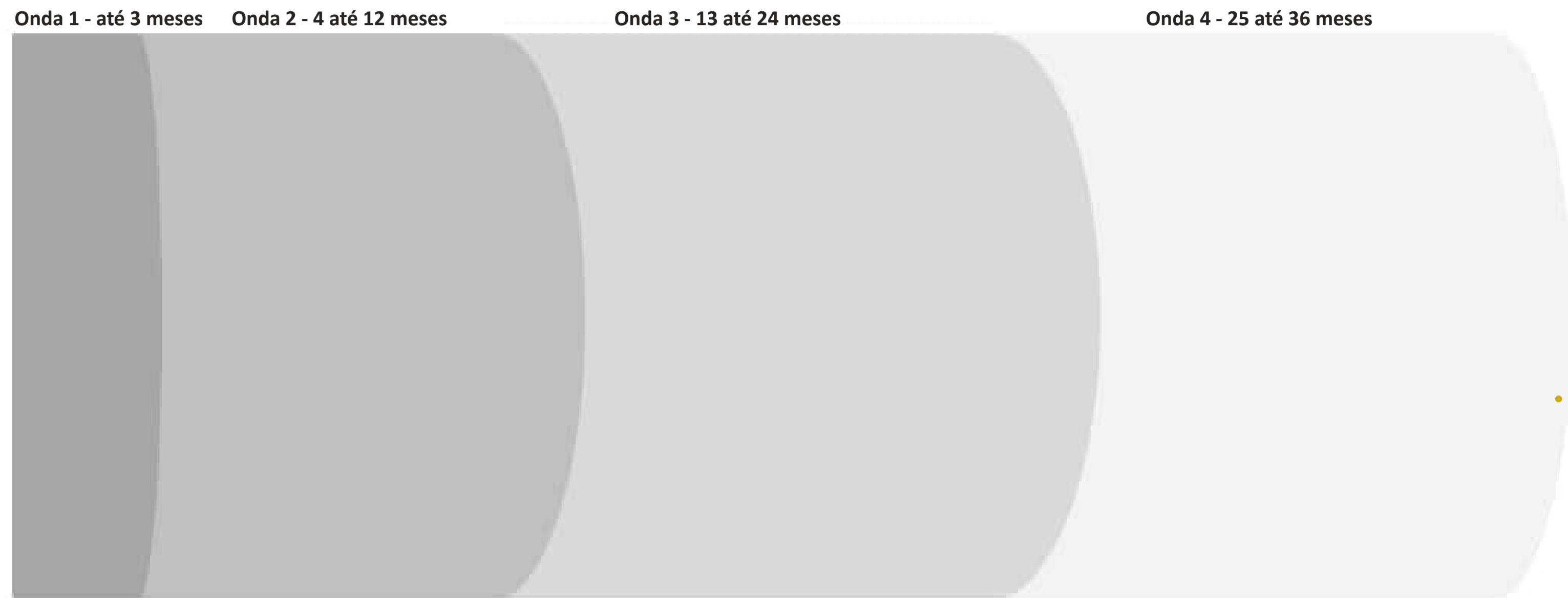
Estimativa de Investimento

0.0

Processos R\$ 0

0

Onda 1 Onda 2 Onda 3 Onda 4



Linha do Tempo



18 19 20 21 22

ID 021 - BAI10 - Estabelecer processo Gestão da Configuração



Processos

ID 021 - BAI10 - Estabelecer processo Gestão da Configuração

Tema
Configurações Gerenciadas

Duração em Semanas
4

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira Média

Exequibilidade
Média

Sinergia na Operação
Alta

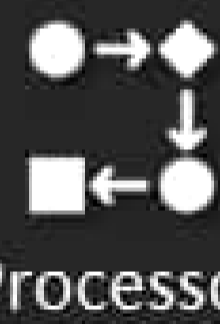
Issue
Não há processo definido para gestão da configuração.

Predecessora
ID 017 - APO09 - Atualização do Catálogo de Serviços de TI

Recomendação
Estabelecer processo para gestão da configuração de ativos, definindo e documentando as linhas-base necessárias.

Risco de TI
Falta de padrão na configuração dos ativos

Risco de Negócio
N/A



ROADMAP DE INICIATIVAS DE TI ↵



Quantidade de Recomendações

1

Processos



1

1

Onda 1 Onda 2 Onda 3 Onda 4

Esmativa de Investimento

0.0

Processos R\$ 0

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Prioridade

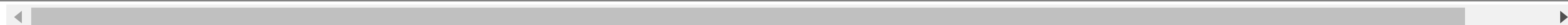


Linha do Tempo



6 7 8 9 10

ID 022 - DSS01 - Estabelecer Procedimento Operacional de TI



Processos

ID 022 - DSS01 - Estabelecer Procedimento Operacional de TI

Tema
Operações Gerenciadas

Duração em Semanas
4

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira Média

Exequibilidade
Média

Sinergia na Operação
Alta

Issue
Não há procedimento operacional de TI definido e documentado.

Predecessora
N/A

Recomendação
Estabelecer documentação referente aos procedimentos operacionais da TI, contendo planejamento de todas as atividades operacionais e sua execução, incluindo ações de testes e checagem de ativos, quando aplicável. Registrar todos os eventos ocorridos na infraestrutura de TI, considerando os riscos associados.

Risco de TI
Ausência de padronização operacional.

Risco de Negócio
N/A



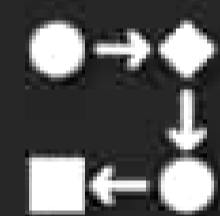
Painel



Estratégia



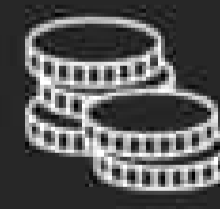
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Processos



1

Processos

R\$ 0

1

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade

Linha do Tempo



6 7 8 9 10

ID 023 - DSS02 - Estabelecer processo de gestão de Requisições



Processos

ID 023 - DSS02 - Estabelecer processo de gestão de Requisições de Serviço e Incidentes.

Tema
Requisições de Serviço e Incidentes Gerenciados

Issue
Não existe um processo definido para atendimento as requisições de serviços e incidentes.

Risco de TI
Ausência de histórico de incidentes e base de conhecimento.

Risco de Negócio
N/A

Duração em Semanas
4

Predecessora
ID 020 - BAI06 - Estabelecer processo de Gestão de Mudança de TI

Estimativa de Investimento
N/A

Critério de Priorização

Sinergia Financeira
Média

Recomendação
Estabelecer processo de atendimento as requisições de serviços e incidentes, classificando-os e implementando uma base de conhecimento para otimizar a solução de problemas/incidentes já conhecidos. Elaborar um documento FAQ para problemas/incidentes amplamente conhecidos e de suporte primário.

Exequibilidade
Média

Sinergia na Operação
Alta



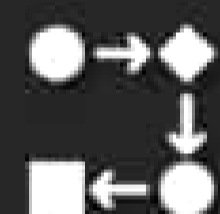
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI

Painel

Estratégia

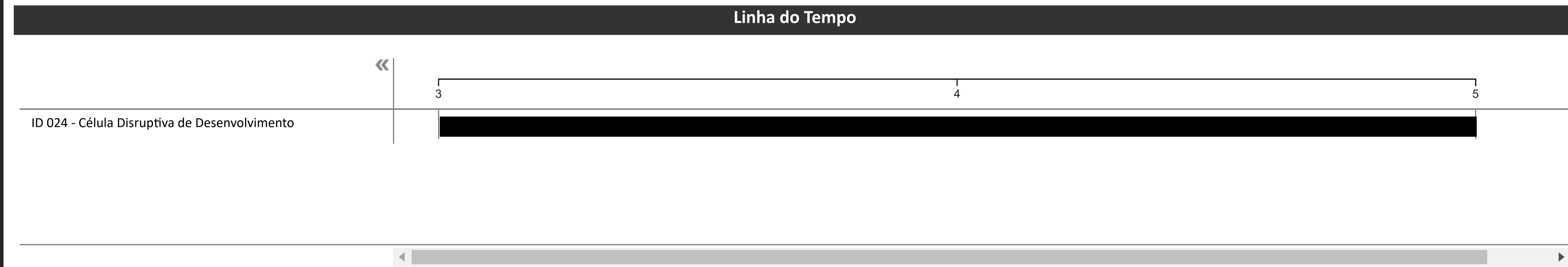
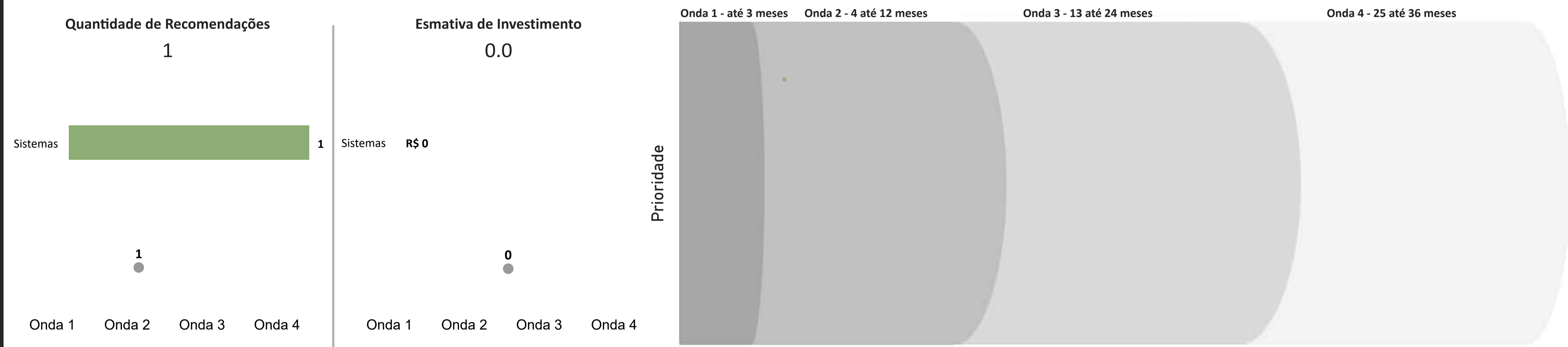
Pessoas

Processos

Tecnologia

Orçamento

Roadmap



Sistemas	ID 024 - Célula Disruptiva de Desenvolvimento		
Tema Desenvolvimento	Issue Existe uma célula de desenvolvimento interna no SGB atendendo as demandas do negócio para sistemas de tecnologia, sem a normatização/governança da TI.	Risco de TI Exposição à riscos tecnológicos e de segurança, devido ao desenvolvimento não normatizado pela TI.	Risco de Negócio N/A
Duração em Semanas 2	Predecessora N/A		
Estimativa de Investimento N/A	Recomendação Em alguns casos, soluções via democratização (Low/No Code) que consistem no desenvolvimento de soluções pelo próprio time de negócio e não são suportados e/ou sustentados pela TI, apresentam resultados extremamente positivos. A TI deverá estabelecer normas e padrões para utilização desta metodologia adotada pelas áreas de negócio.		
Critério de Priorização			
Sinergia Financeira Alta			
Exequibilidade Alta			
Sinergia na Operação Alta			

ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética

Sistemas

1

Quantidade de Recomendações

1

Esmativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Sistemas



1

Sistemas R\$ 0

1

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade



Linha do Tempo



18

19

ID 025 - Hospedagem de Sistemas On Premise



Sistemas

ID 025 - Hospedagem de Sistemas On Premise

Tema
Hospedagem

Duração em Semanas
N/A

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Baixa

Exequibilidade
Baixa

Sinergia na Operação
Alta

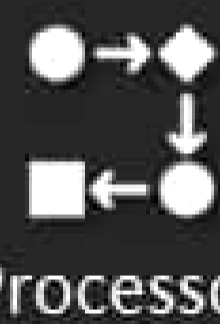
Issue
52% das aplicações analisadas possuem sua hospedagem On Premise (tanto em data center interno quanto colocation).

Predecessora
N/A

Recomendação
Migrar as aplicações On Premise para Cloud, conforme os equipamentos cheguem ao final do ciclo de vida. (EoL)

Risco de TI
Indisponibilidade sistêmica caso o ambiente ou a gestão não possuam a maturidade adequada.

Risco de Negócio
Indisponibilidade de sistemas/serviços tecnológicos



ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética

Sistemas
1

Quantidade de Recomendações

1

Esmativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Sistemas



1

Sistemas R\$ 0

1

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade

Linha do Tempo



3 4 5 6 7 8 9

ID 026 - Banco de Dados



Sistemas

ID 026 - Banco de Dados

Tema
Obsolescência de Tecnologia

Duração em Semanas
6

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Média

Exequibilidade
Média

Sinergia na Operação
Média

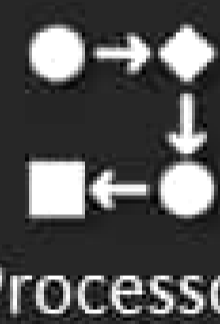
Issue
Existem 10 aplicações que utilizam bancos de dados já considerados obsoletos: Oracle 11g, PostgreSQL10 e SQL Server 2008, com término do ciclo de vida em dezembro/2020, novembro/2022 e julho/2022, respectivamente.

Predecessora
N/A

Recomendação
Atualizar a versão dos bancos de dados para a mais recente: Oracle 19c; PostgreSQL 15.2 e SQL Server 2019

Risco de TI
Vulnerabilidades e inexistência de suporte técnico em versões de Bancos de Dados consideradas obsoletas.

Risco de Negócio
Indisponibilidade em serviços e sistemas de TI que utilizam base de dados.



ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética

Sistemas

1

Quantidade de Recomendações

1

Estimativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Sistemas



1

Sistemas R\$ 0

1

0

Prioridade

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4



Linha do Tempo



3 4 5 6 7 8 9

ID 027 - Sistema Operacional dos servidores de Banco de Dados



Sistemas

ID 027 - Sistema Operacional dos servidores de Banco de Dados

Tema
Obsolescência de Tecnologia

Duração em Semanas
6

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Média

Exequibilidade
Media

Sinergia na Operação
Média

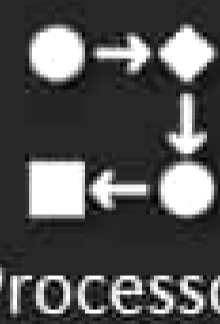
Issue
Existem 4 aplicações que utilizam banco de dados que são hospedados em servidor(es) com sistema operacional Windows Server 2008 R2, considerado obsoleto e teve seu ciclo de vida terminado em janeiro/2020. Ademais, existem 7 aplicações que utilizam banco de dados que são hospedados em servidores que possuem sistema operacional com término de seu ciclo de vida prorrogado para junho/2024: RHEL 6.x e RHEL 7.x.

Predecessora
N/A

Recomendação
Atualizar o sistema operacional dos servidores de banco de dados mencionados para as versões: Windows Server 2022 e RHEL 9.

Risco de TI
Vulnerabilidades e inexistência de suporte técnico em versões de Sistemas Operacionais obsoletas.

Risco de Negócio
Indisponibilidade em serviços e sistemas de TI que utilizam base de dados.



ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética

Sistemas

1

Quantidade de Recomendações

1

Esmatima de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Sistemas



1

Sistemas R\$ 0

1

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade

Linha do Tempo



3 4 5 6 7 8 9

ID 028 - Sistema Operacional dos servidores de Aplicação



Sistemas

ID 028 - Sistema Operacional dos servidores de Aplicação

Tema
Obsolescência de Tecnologia

Duração em Semanas
6

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Média

Exequibilidade
Media

Sinergia na Operação
Média

Issue
Existem 8 aplicações que são hospedadas em servidor(es) com sistema operacional considerado obsoleto: Windows Server 2008 R2; RHEL 6.10 e RHEL 5.7, que obtiveram seu ciclo de vida terminado em janeiro/2020; novembro/2020 e março/2017, respectivamente. Ademais, existem 34 aplicações que são hospedadas em servidor(es) com sistema operacional cujo ciclo de vida está próximo de sua finalização: RHEL 7.9 - junho/2024.

Predecessora
N/A

Recomendação
Atualizar o sistema operacional dos servidores de banco de dados mencionados para as versões: Windows Server 2022 e RHEL 9.

Risco de TI
Vulnerabilidades e inexistência de suporte técnico em versões de Sistemas Operacionais obsoletas.

Risco de Negócio
Indisponibilidade em aplicações de TI.



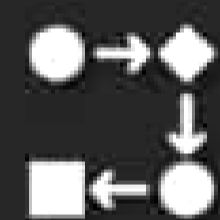
Painel



Estratégia



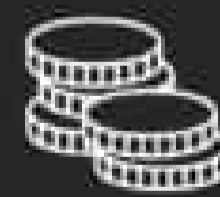
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI

Painel

Estratégia

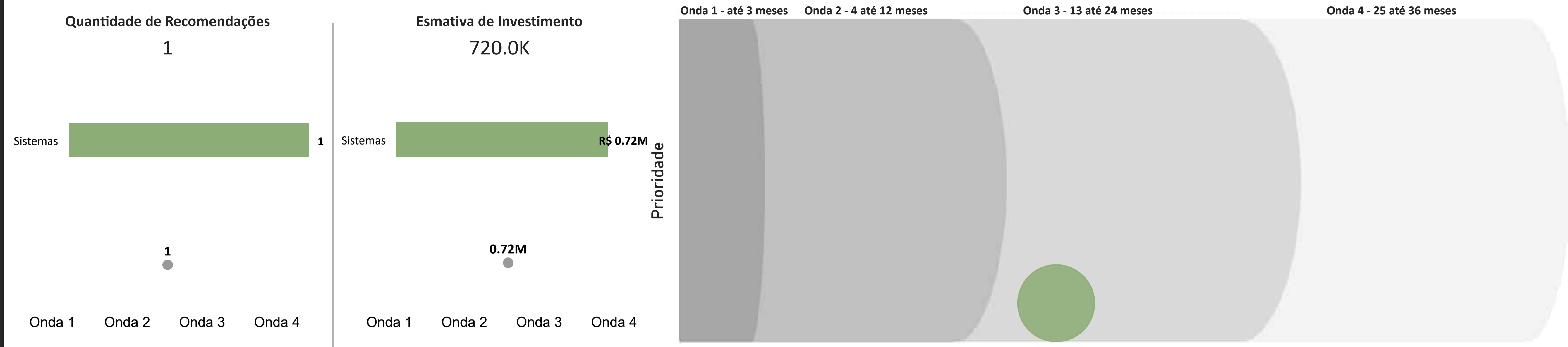
Pessoas

Processos

Tecnologia

Orçamento

Roadmap



Sistemas	ID 029 - Interpretação de Dados Técnicos/Geológicos armazenados		
Tema Dados	Issue Os dados técnicos/geológicos são armazenados em base de dados distintas, sem padrões específicos para os dados que representam as características das análises, o que dificulta a interpretação da informação pelos usuários finais.	Risco de TI Ineficiência no armazenamento de dados	Risco de Negócio Interpretação incorreta de dados técnicos.
Duração em Semanas 12	Predecessora N/A		
Estimativa de Investimento R\$ 720K	Recomendação Realizar Projeto de Estruturação de Dados, para que os dados possam ser classificados e organizados de maneira padrão, incluindo suas unidades de medida e nomenclaturas para descrição de suas características, de acordo com os conceitos de MDM (Master Data Management).		
Critério de Priorização			
Sinergia Financeira Baixa			
Exequibilidade Baixa			
Sinergia na Operação Alta			

ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética

Sistemas
1

Quantidade de Recomendações

1

Esmatima de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Sistemas



1

Sistemas R\$ 0

1

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade



Linha do Tempo



6 7 8 9 10

ID 030 - Software de Gestão para área MCTER (Museu)



Sistemas

ID 030 - Software de Gestão para área MCTER (Museu)

Tema
Aplicações

Duração em Semanas
4

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Média

Exequibilidade
Média

Sinergia na Operação
Alta

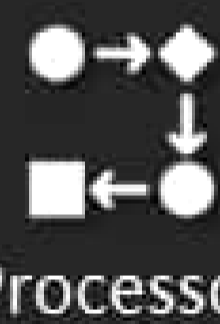
Issue
A área MCTER não possui um sistema que apoie na gestão do Museu. O sistema Pergamun utilizado (sistema de prateleira específico para operacionalização de bibliotecas) não é suficiente para apoiar todos os processos da área, segundo relatado pela mesma, gerando grande trabalho...

Predecessora
ID 001 - ERP - Mapeamento de Processos e Levantamento de Requisitos

Recomendação
Utilizar o módulo de Gestão de Suprimentos da solução ERP a ser implementada ou investir em uma solução de mercado que contenha todos os requisitos funcionais definidos pela área usuária em substituição as soluções atuais.

Risco de TI
N/A

Risco de Negócio
Ineficiência no catálogo de itens do Museu e alto volume de trabalho manual em planilhas Excel.



ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Esmatima de Investimento

170.0K

Infraestrutura



1

Infraestrutura



R\$ 0.17M

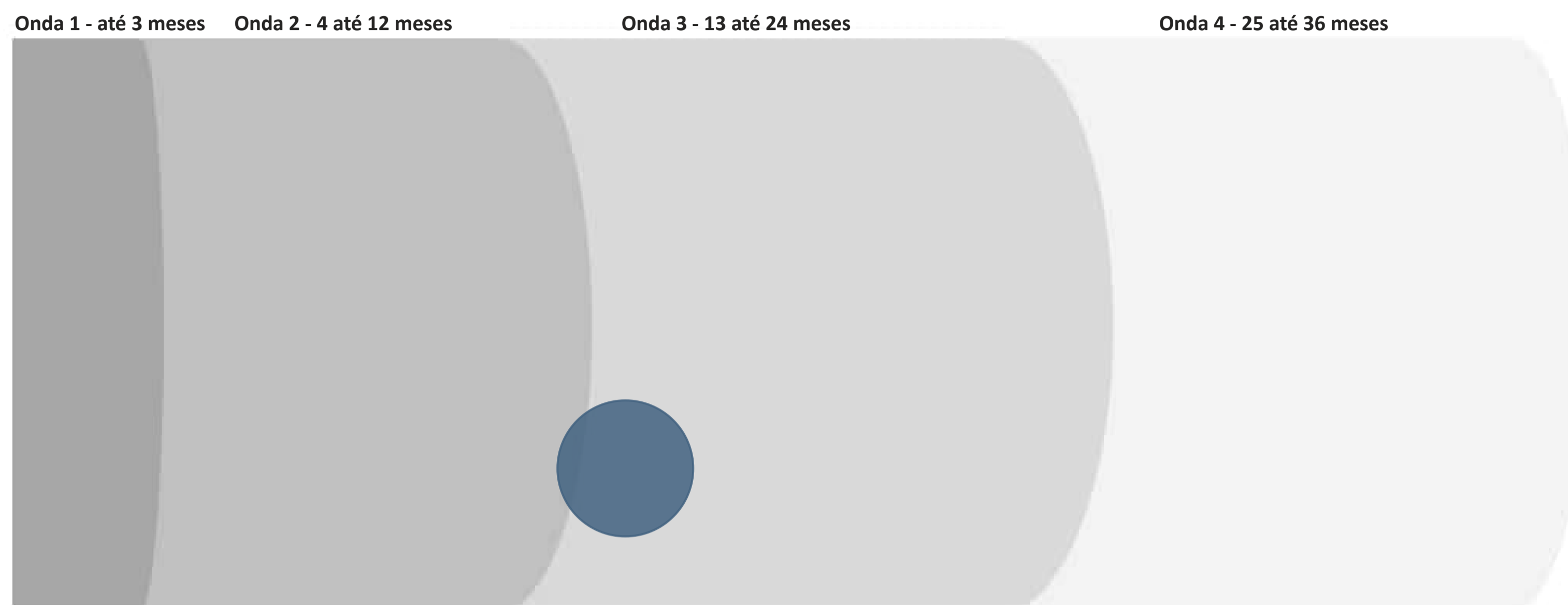
Prioridade

1

0.17M

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4



Linha do Tempo



6 7 8 9 10

ID 031 - Cloud - Fundação



Infraestrutura

ID 031 - Cloud - Fundação

Tema
Serviços

Duração em Semanas
4

Estimativa de Investimento
R\$ 170K

Critério de Priorização
Sinergia Financeira
Média

Exequibilidade
Média

Sinergia na Operação
Média

Issue
Serviços e atividades de TI descentralizados, Estrutura de clouds despadronizadas e vulnerabilidade em ambiente cloud.

Predecessora
N/A

Recomendação
Implementar o conceito de landing zone (detalhado em diagrama) em todos os serviços de cloud.
Implementar firewall no ambiente cloud e rede Hub/Spoke para aumento de segurança e velocidade na escalabilidade.
Utilizar a configuração Service Endpoints para que o tráfego seja via backbone, não via internet, na troca de informações entre objetos para serviços não críticos ou sensíveis para segurança de dados.
Utilizar a configuração Private Service Endpoints para que o tráfego seja via rede interna do Fornecedor, não via backbone ou internet, na troca de informações entre objetos para serviços críticos ou sensíveis para segurança de dados.

Risco de TI
Acesso indevido as aplicações ou ambiente;
Dados sendo trafegados pela internet em acessos mútuos de serviços da cloud.

Risco de Negócio
Exposição de informações sensíveis via internet



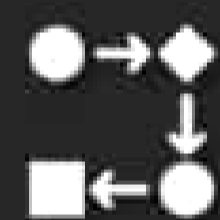
Painel



Estratégia



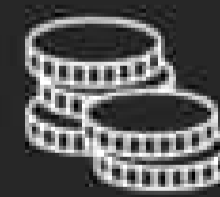
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura
1

Pessoas

Processos

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

20.0K

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Infraestrutura



1

Infraestrutura



R\$ 20K

Prioridade

1

20.0K

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4



Linha do Tempo



3 4 5 6 7 8 9 10 11 12 13 14 15

ID 032 - Cloud - Conexão Privada



Infraestrutura

ID 032 - Cloud - Conexão Privada

Tema
Serviços

Issue
Ausência de conexão ponto a ponto com fornecedor de cloud.

Risco de TI
Dados sendo trafegados pela internet ao acessar os recursos da cloud

Risco de Negócio
Exposição de informações sensíveis na internet

Duração em Semanas
12

Predecessora
N/A

Estimativa de Investimento
R\$ 20K

Critério de Priorização
Sinergia Financeira
Média

Recomendação
Estabelecer conexão dedicada e privada com fornecedor de cloud para acesso seguro aos seus serviços e produtos.

Exequibilidade
Média

Sinergia na Operação
Baixa



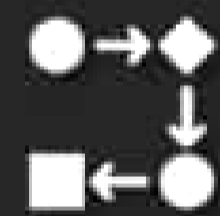
Painel



Estratégia



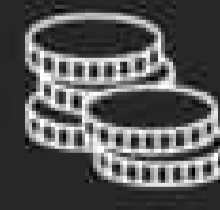
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI ↩



Quantidade de Recomendações

1

Infraestrutura



1

1

Onda 1 Onda 2 Onda 3 Onda 4

Estimativa de Investimento

0.0

Infraestrutura

R\$ 0

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Prioridade



Linha do Tempo



3 4 5 6 7 8 9 10 11 12 13 14 15

ID 033 - Cloud - Adoção de Cultura FinOps



Infraestrutura

ID 033 - Cloud - Adoção de Cultura FinOps

Tema
Serviços

Duração em Semanas
12

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Baixa

Exequibilidade
Média

Sinergia na Operação
Baixa

Issue
Gestão financeira realizada sem a adoção das melhores práticas de mercado.

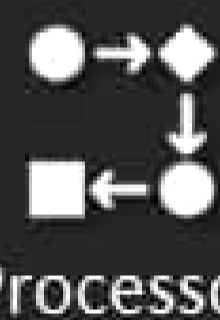
Predecessora
N/A

Risco de TI
Não manter o controle de custos de TI

Risco de Negócio
N/A

Recomendação

Implementar FinOps de acordo com seus conceitos e considerando os pontos listados abaixo:
 Realizar Capacitação/Treinamento para área responsável e equipes de TI sobre os conceitos de FinOps, custos operacionais da TI e sua estrutura;
 Efetuar mapa de capacitação com base nos perfis futuros da TI alinhados com a prática;
 Utilizar estratégias como microlearning, programas de reconhecimento, gamificação e divulgação em diversos canais para disseminar a cultura e adoção ao novo modo de trabalho;



ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

648.0K

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Infraestrutura



1

Infraestrutura



R\$ 0.65M

Prioridade

1

0.65M

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4



Linha do Tempo



6 7 8 9 10 11 12

ID 034 - Azure - Licença P1



Infraestrutura

ID 034 - Azure - Licença P1

Tema
Dados

Issue
Impossibilidade de utilização do SSO (single sign-on) para as aplicações, através do Azure AD.

Risco de TI
N/A

Risco de Negócio
N/A

Duração em Semanas
6

Predecessora
N/A

Estimativa de Investimento
R\$ 648K

Critério de Priorização
Sinergia Financeira
Média

Recomendação
Implementar funcionalidades da licença P1 da Azure tendo em vista o aumento da capacidade de monitoramento, revisão de acessos, proteção de vulnerabilidades, riscos e acesso privilegiado.
Implementar SSO
Implementar Acesso condicional baseado em risco.
Criar processo de Revisões de acesso.
Configurar Gerenciamento de direitos.

Exequibilidade
Baixa

Sinergia na Operação
Baixa



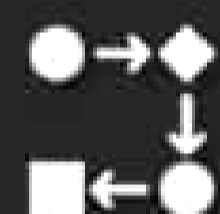
Painel



Estratégia



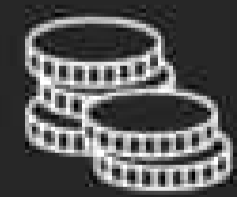
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI ↶



Quantidade de Recomendações

1

Infraestrutura



1

Onda 1 Onda 2 Onda 3 Onda 4

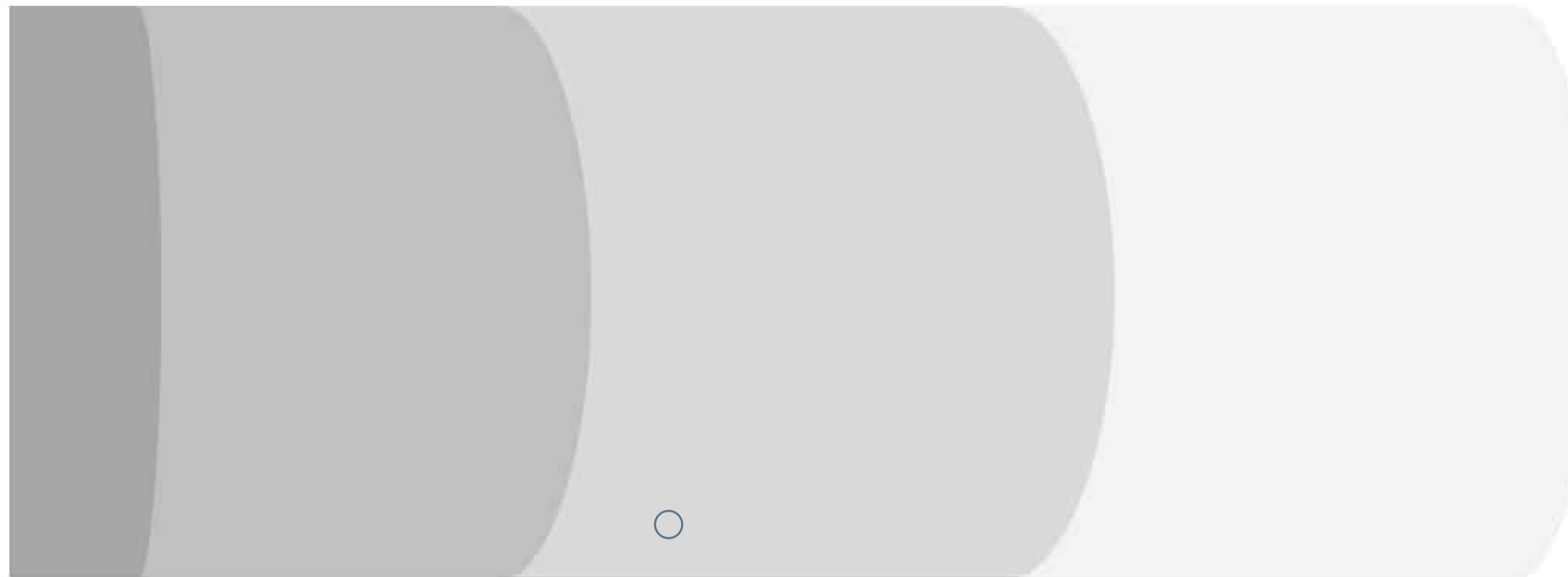
Esmativa de Investimento

0.0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

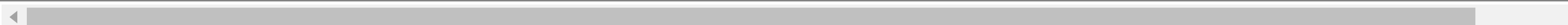
Prioridade



Linha do Tempo



ID 035 - Rede de Dados - Latência



Infraestrutura

ID 035 - Rede de Dados - Latência

Tema
Redes

Duração em Semanas
16

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Baixa

Exequibilidade
Baixa

Sinergia na Operação
Baixa

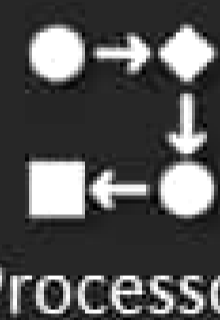
Issue
Performance da Rede de Dados abaixo dos padrões e necessidades das aplicações.

Predecessora
N/A

Risco de TI
N/A

Risco de Negócio
N/A

Recomendação
Verificar latência das regionais para o data center e cloud gerando documento de controle;
Realizar estudo de tempos e movimentos para analisar performance dos links e aplicações de negócio.



ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura
1

Pessoas

Processos

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

390.0K

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Infraestrutura



1

Infraestrutura



R\$ 0.39M

Prioridade

1

0.39M

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

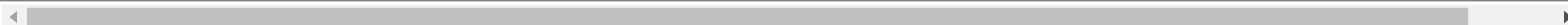


Linha do Tempo



3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19

ID 036 - Rede de Dados - Redundância de Links



Infraestrutura

ID 036 - Rede de Dados - Redundância de Links

Tema
Redes

Issue
Ausência de links redundantes nas unidades.

Risco de TI
Indisponibilidade de conectividade de rede

Risco de Negócio
Indisponibilidade de aplicações e serviços.

Duração em Semanas
16

Predecessora
N/A

Estimativa de Investimento
R\$ 390K

Critério de Priorização
Sinergia Financeira
Média

Recomendação
Realizar a contratação de link adicional para cada unidade, promovendo disponibilidade dos serviços de TI em casos de falha dos links principais. Configurar a utilização dos links de dados no modo "Ativo-Ativo" (failover, Balanceamento de carga).

Exequibilidade
Média

Sinergia na Operação
Baixa



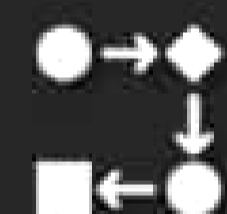
Painel



Estratégia



Pessoas



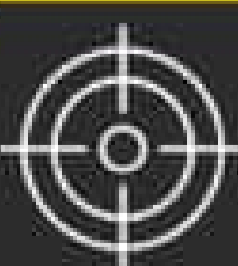
Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura
1

Pessoas

Processos

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Infraestrutura



1

1

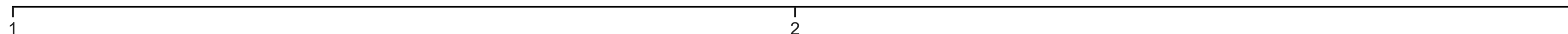
Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade



Linha do Tempo



ID 037 - Rede de Dados - Compartilhamento de Backbones Inter



Infraestrutura

ID 037 - Rede de Dados - Compartilhamento de Backbones Internet

Tema
Redes

Duração em Semanas
2

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Baixa

Exequibilidade
Baixa

Sinergia na Operação
Baixa

Issue
Ausência de informações sobre o compartilhamento de infraestrutura dos provedores de internet.

Predecessora
N/A

Recomendação

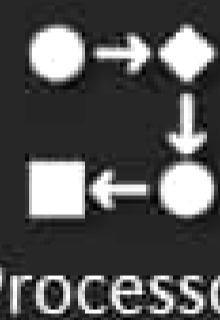
Obter a informação da seguinte forma:

- 1 - Solicitar para a operadora todos os saltos de inter-conexão, ou;
- 2 - Acessar o site apinfo.oi e pesquisar pelo nome do provedor ou na tela inicial aparecerá o ASN do provedor do qual você está acessando. Garantir que você está no ambiente ao qual você deseja obter o ASN.

Com o código ASXXXX, no site bgp.he.net, no campo search digitar o ASN do provedor, para rede IPv4, clicar na aba Graph v4 ou para IPv6 clicar na aba Graph v6, cada aba mostra todas as rotas BGP por qual o provedor inicial salta para acessar a internet.

Risco de TI
Indisponibilidade de conexão internet em decorrência de backbone compartilhado entre operadoras

Risco de Negócio
Indisponibilidade de ambiente, recursos e aplicações de negócio



ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura
1

Pessoas

Processos

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

62.0K

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Infraestrutura



1

Infraestrutura



R\$ 62K

Prioridade

1

62K

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Linha do Tempo



3 4 5 6 7 8 9 10 11 12 13 14 15

ID 038 - Rede de Dados - Fundação



Infraestrutura

ID 038 - Rede de Dados - Fundação

Tema
Redes

Duração em Semanas
12

Estimativa de Investimento
R\$ 62K

Critério de Priorização
Sinergia Financeira
Baixa

Exequibilidade
Baixa

Sinergia na Operação
Baixa

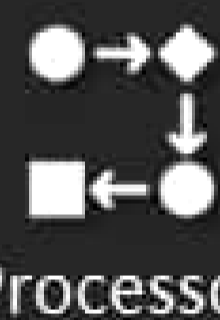
Issue
Custos elevados com links, gerenciamento de rotas não otimizado, autenticação para acesso aos ativos de rede descentralizados e ausência de acesso alternativo ao ambiente.

Predecessora
N/A

Recomendação
Realizar RFP com Operadoras de abrangência nacional para redução de custos e melhorias na prestação de serviços;
Implementar configuração usando técnica de VRF que tem como objetivo replicar rotas padrões para todos os equipamentos de rede de forma centralizada;
Implementar protocolo de segurança (RADIUS ou TACACS) para o gerenciamento da autorização e autenticação centralizada de acesso aos roteadores e switches;
Centralizar controladoras em ambiente com redundância em cloud ou on-premise;
Implementar controle de endereçamento de rede que contenha informações como: VLAN ID, rede/xx, departamento, usado para, gateway, status, PAT, NAT.

Risco de TI
Acesso indevido aos ativos de rede e indisponibilidade do ambiente.

Risco de Negócio
Indisponibilidade de ambiente, recursos e aplicações de negócio.



ROADMAP DE INICIATIVAS DE TI

Painel

Estratégia

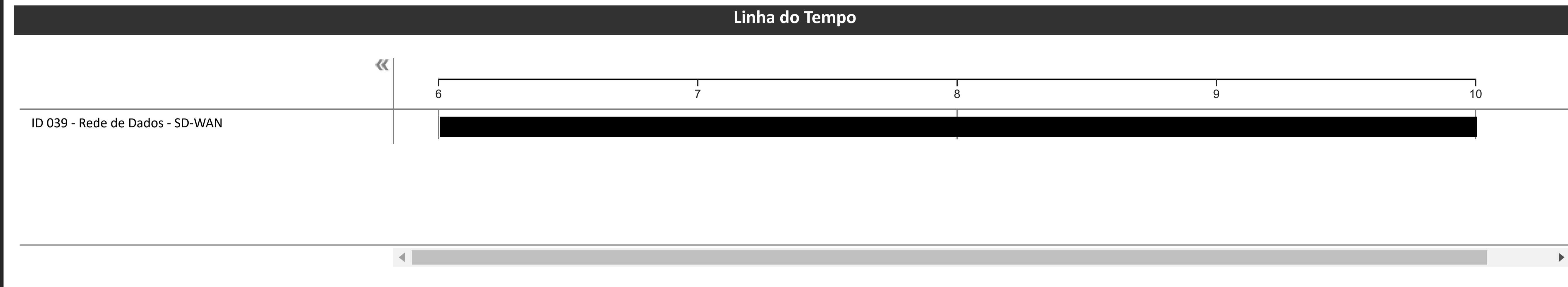
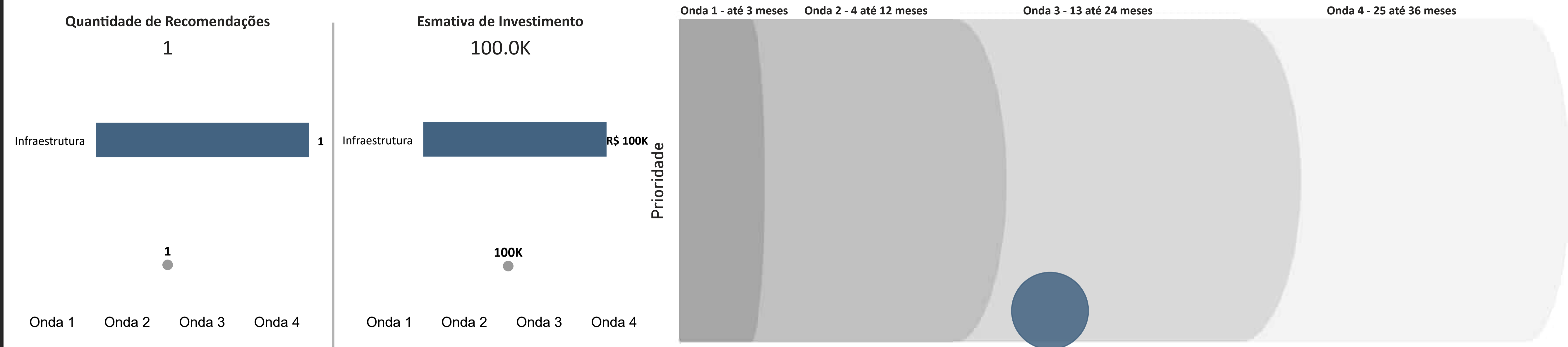
Pessoas

Processos

Tecnologia

Orçamento

Roadmap



Infraestrutura	ID 039 - Rede de Dados - SD-WAN		
Tema Redes	Issue Gerenciamento de rotas, políticas, QoS e backbone interno descentralizados.	Risco de TI Ineficiência no gerenciamento do ambiente	Risco de Negócio N/A
Duração em Semanas 4	Predecessora N/A		
Estimativa de Investimento R\$ 100K	Recomendação Implementar conceitos de SD-WAN para a rede de dados, centralizando o roteamento dinâmico para tráfego nos links via BPG, OSPF ou protocolos similares, criando um backbone próprio.		
Critério de Priorização	Sinergia Financeira Baixa		
Exequibilidade Baixa	Sinergia na Operação Baixa		

ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura
1

Pessoas

Processos

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Infraestrutura



1

1

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade



Linha do Tempo



18 19 20 21 22 23 24

ID 040 - Rede de Dados - VLAN



Infraestrutura

ID 040 - Rede de Dados - VLAN

Tema
Redes

Issue
Rede de dados não segmentada.

Risco de TI
Ataque lateral hacker no ambiente

Risco de Negócio
Exposição de informações sensíveis.

Duração em Semanas
12

Predecessora
N/A

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Baixa

Recomendação
Segmentar as VLANs por departamentos e demais separações necessárias;
Limitar escopo DHCP de acordo com a quantidade de dispositivos por departamento.

Exequibilidade
Baixa

Sinergia na Operação
Baixa



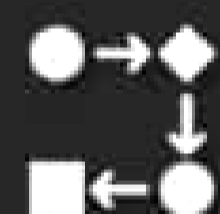
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura
1

Pessoas

Processos

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Esmatima de Investimento

250.0K

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Infraestrutura



1

Infraestrutura



R\$ 0.25M

Prioridade

1

250K

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4



Linha do Tempo



3 4 5 6 7 8 9 10 11

ID 041 - Rede de Dados - Contratos



Infraestrutura

ID 041 - Rede de Dados - Contratos

Tema
Redes

Duração em Semanas
8

Estimativa de Investimento
R\$ 250K

Critério de Priorização
Sinergia Financeira
Média

Exequibilidade
Baixa

Sinergia na Operação
Baixa

Issue
Ausência de contratos de extensão de garantia para equipamentos de infraestrutura de rede críticos para a sustentação do Negócio.

Predecessora
N/A

Recomendação
Contratar extensão de garantia para equipamentos de rede com suporte 4X24X365 para equipamentos críticos ou que sejam únicos. Suporte 8XNBD para equipamentos com baixa criticidade.

Risco de TI
Indisponibilidade de ambiente, recursos e aplicações de negócio

Risco de Negócio
Indisponibilidade de ambiente, recursos e aplicações de negócio



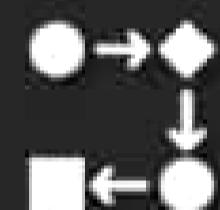
Painel



Estratégia



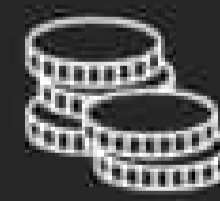
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura
1

Pessoas

Processos

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

1.1M

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Infraestrutura



1

Infraestrutura



R\$ 1.10M

Prioridade

1

1.10M

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4



Linha do Tempo



18 19 20 21 22 23 24

ID 042 - Serviço - Servidor de Arquivos



Infraestrutura

ID 042 - Serviço - Servidor de Arquivos

Tema

Dados

Issue

Serviço de armazenamento descentralizado e sem consolidação.

Risco de TI

Grupos ou usuários com permissões de acesso indevidas

Risco de Negócio

Acesso indevido a informações

Duração em Semanas

16

Predecessora

N/A

Estimativa de Investimento

R\$ 1M

Recomendação

Critério de Priorização

Sinergia Financeira

Alta

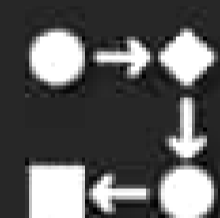
Exequibilidade

Média

Sinergia na Operação

Média

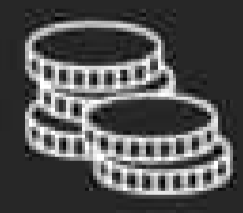
Implementar uma solução híbrida de servidor de arquivos on-premise e cloud;
 Revisar os arquivos que deverão ser movidos para cloud. Arquivos com tempo de vida maior que 3 anos deverão ser armazenados em archive;
 Realizar o mapeamento de grupos e pastas em cada dominio;
 Realizar a copia/mover os arquivos garantindo suas permissões através de snapshot ou backup/restore ou ferramenta robocopy;
 Validar os acessos para os grupos nas pastas préviamente mapeadas;
 Obs: Exemplo usando um cenário com Azure o valor estimado para 670TB -> Reserva 1 ano -> LRS -> Hot-> R\$ 1.1M Ano ou Reserva 3 anos -> LRS -> Blob Hot -> USD 54k Ano



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI

Painel

Estratégia

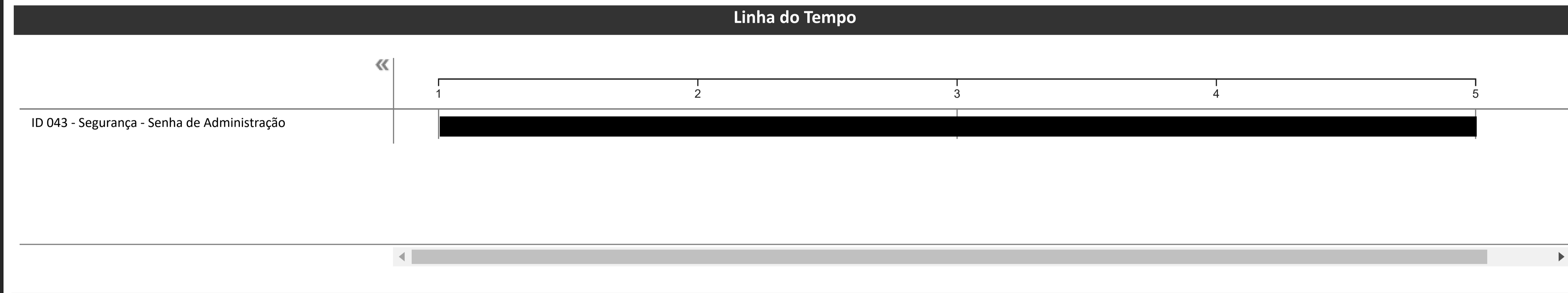
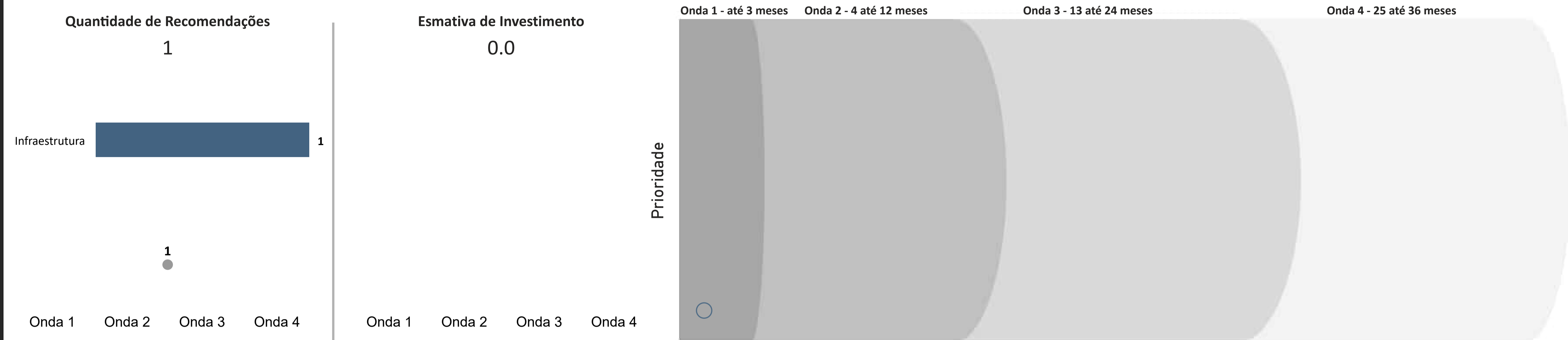
Pessoas

Processos

Tecnologia

Orçamento

Roadmap



Infraestrutura	ID 043 - Segurança - Senha de Administração		
Tema Dados	Issue Gerenciamento descentralizado de conta do administrador local do sistema operacional Windows.	Risco de TI Ataque lateral hacker no ambiente	Risco de Negócio Exposição de informações sensíveis.
Duração em Semanas 4	Predecessora N/A		
Estimativa de Investimento N/A	Recomendação		
Critério de Priorização	<p>Implementar Windows LAPS na empresa e limitar a quantidade de contas com privilégios elevados, oferecendo uma solução de centralização e gerenciamento de senhas para conta de administrador local das estações de trabalho</p> <p>Rever política referente ao tamanho da senha no ambiente e nome de conta do administrador (contas com privilégios de administrador deverão ter no mínimo 16 caracteres de tamanho); Para ambiente cloud habilitar MFA e/ou certificado e/ou cofre de senhas</p> <p>Tamanho de senhas para firewalls, switches, roteadores e demais equipamentos de infraestrutura: Definir através de política que contas com acesso a dispositivos de rede interno tenham no mínimo 12 caracteres de tamanho; Definir através de política que contas com acesso a dispositivos de rede na DMZ ou externo tenham no mínimo 16 caracteres de tamanho e cofre de senha e/ou certificado;</p> <p>Nome da conta do administradores: Realizar a alteração do nome de conta padrão de administradores, como: administrador, root, admin, etc, para um nome de conta diferente e sem correlações; Definir a troca periódica de senhas para contas de administradores locais e do domínio.</p>		
Sinergia Financeira Baixa			
Exequibilidade Baixa			
Sinergia na Operação Baixa			

ROADMAP DE INICIATIVAS DE TI

Painel

Estratégia

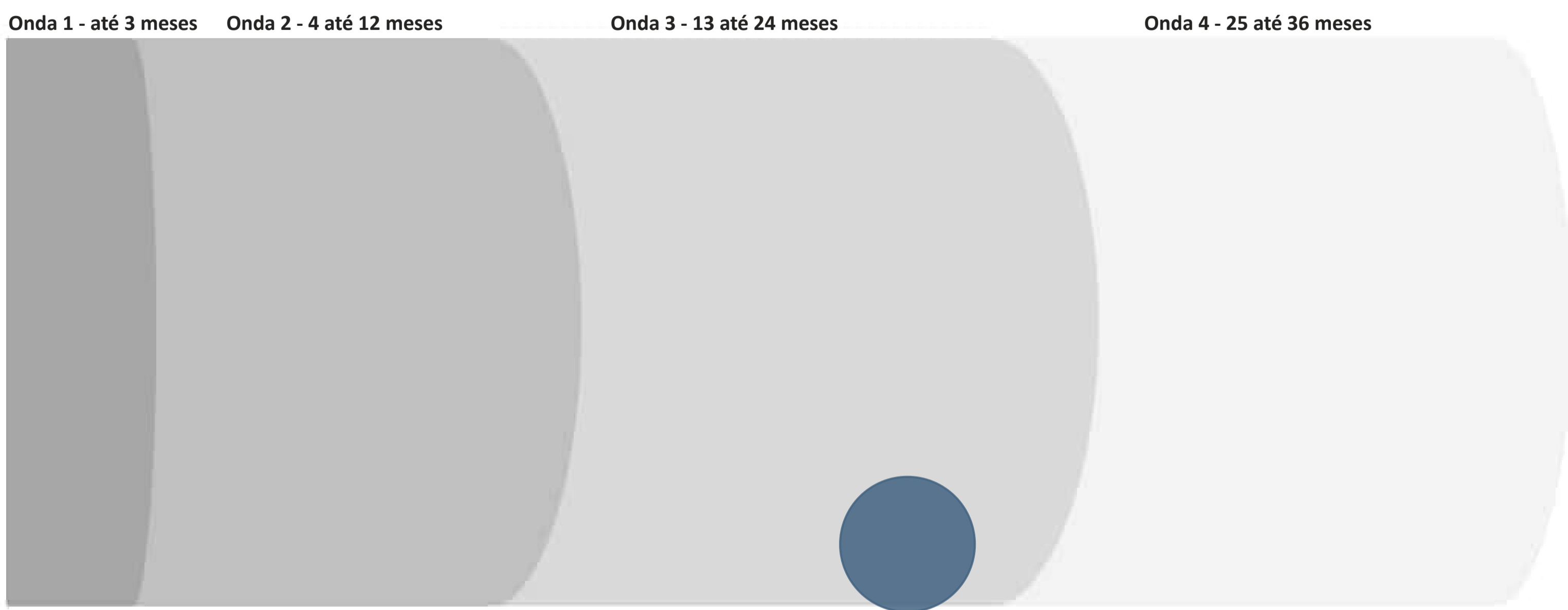
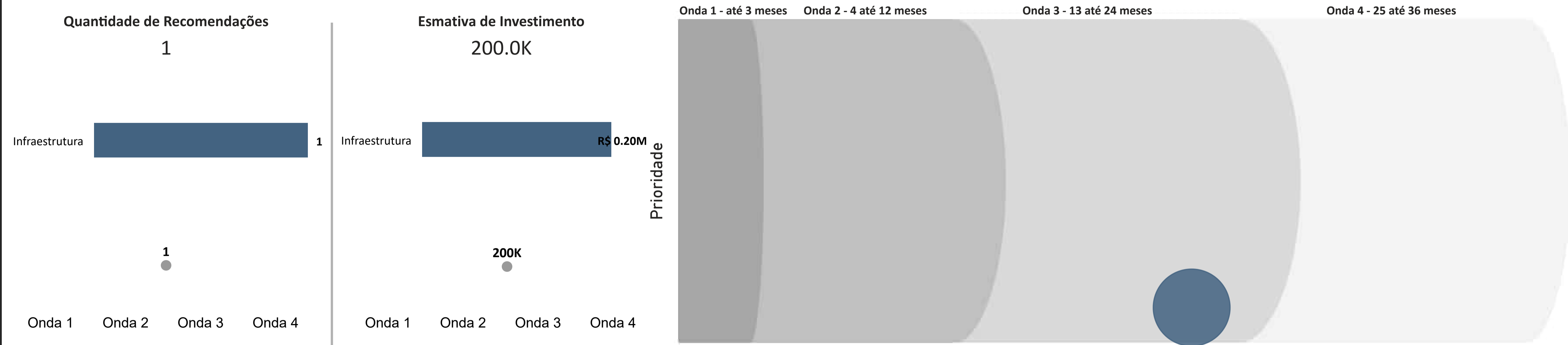
Pessoas

Processos

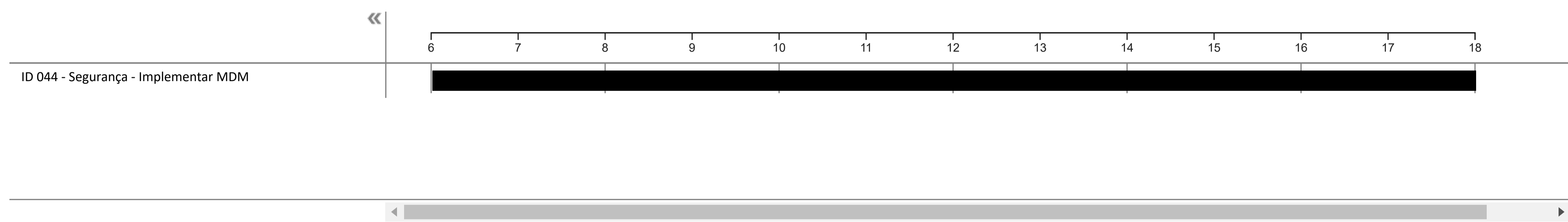
Tecnologia

Orçamento

Roadmap



Linha do Tempo



Infraestrutura ID 044 - Segurança - Implementar MDM

Tema Dados	Issue Ausência de gerenciamento de dispositivos móveis.	Risco de TI Acesso indevido as aplicações ou ambiente sem autorização, controle e monitoramento	Risco de Negócio Exposição de informações sensíveis.
Duração em Semanas 12	Predecessora N/A		
Estimativa de Investimento R\$ 200K	Recomendação Implementar solução de MDM (Mobile Device Management) para toda empresa, oferecendo maior segurança e produtividade para equipamentos e dispositivos móveis na organização.		
Critério de Priorização	Sinergia Financeira Média		
Exequibilidade Baixa	Sinergia na Operação Baixa		

ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética
1

Sistemas

Quantidade de Recomendações

1

Esmatima de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Segurança Cibernética



1

Segurança Cibernética

R\$ 0

1

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

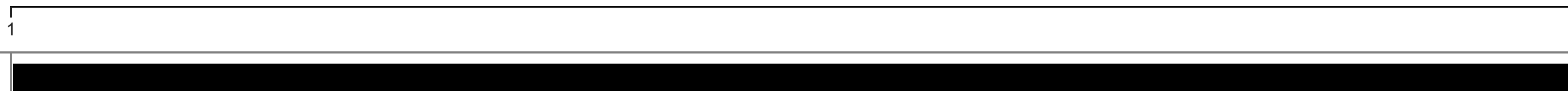
Prioridade



Linha do Tempo



ID 045 - Política de proteção contra malware



Segurança Cibernética

ID 045 - Política de proteção contra malware

Tema
Política

Issue
A política de proteção contra Malware, incluindo o software endpoint, não possui documentação indicando os procedimentos e configurações.

Risco de TI
Falta de padronização e perda de conhecimento técnico.

Risco de Negócio
N/A

Duração em Semanas
1

Predecessora
N/A

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Média

Recomendação
Documentar a política de utilização de softwares de proteção contra Malware, incluindo sua versão, forma de configuração e atualização.

Exequibilidade
Alta

Sinergia na Operação
Alta



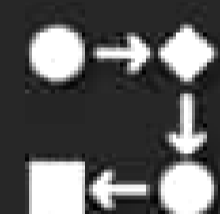
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI

Painel

Estratégia

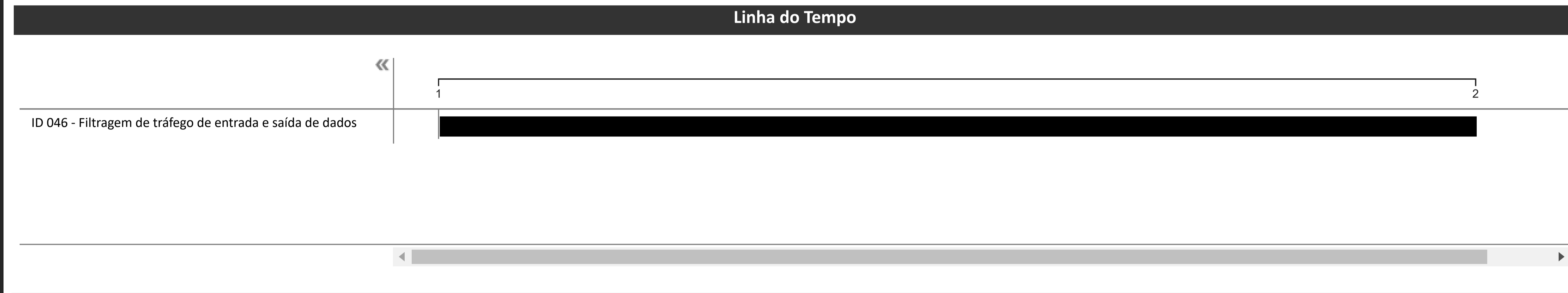
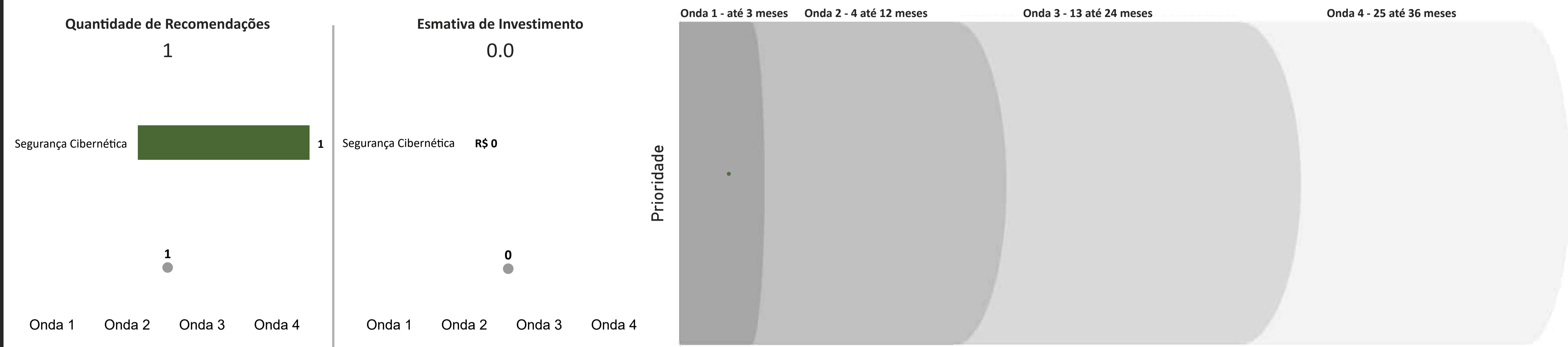
Pessoas

Processos

Tecnologia

Orçamento

Roadmap



Segurança Cibernética	ID 046 - Filtragem de tráfego de entrada e saída de dados		
Tema Segurança Lógica	Issue Não há filtragem de tráfego de internet e e-mails.	Risco de TI Exposição ao risco de ataques cibernéticos através de Phishing, SPAM e outros.	Risco de Negócio N/A
Duração em Semanas 1	Predecessora N/A		
Estimativa de Investimento N/A	Recomendação Implementar um filtro na borda que proteja a navegação, downloads e e-mails contra Malwares, Spywares e demais códigos maliciosos, além de filtro de conteúdo que impeça o acesso a links maliciosos e sites conhecidamente inseguros.		
Critério de Priorização			
Sinergia Financeira Média			
Exequibilidade Alta			
Sinergia na Operação Alta			

ROADMAP DE INICIATIVAS DE TI

Painel

Estratégia

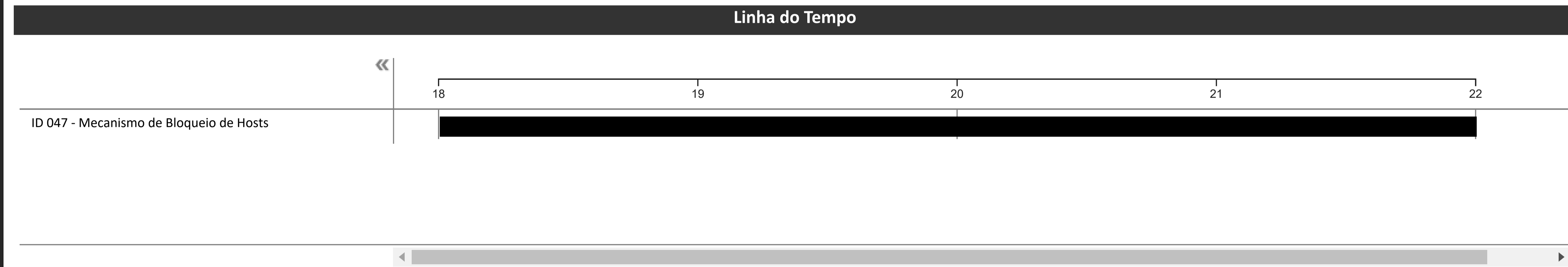
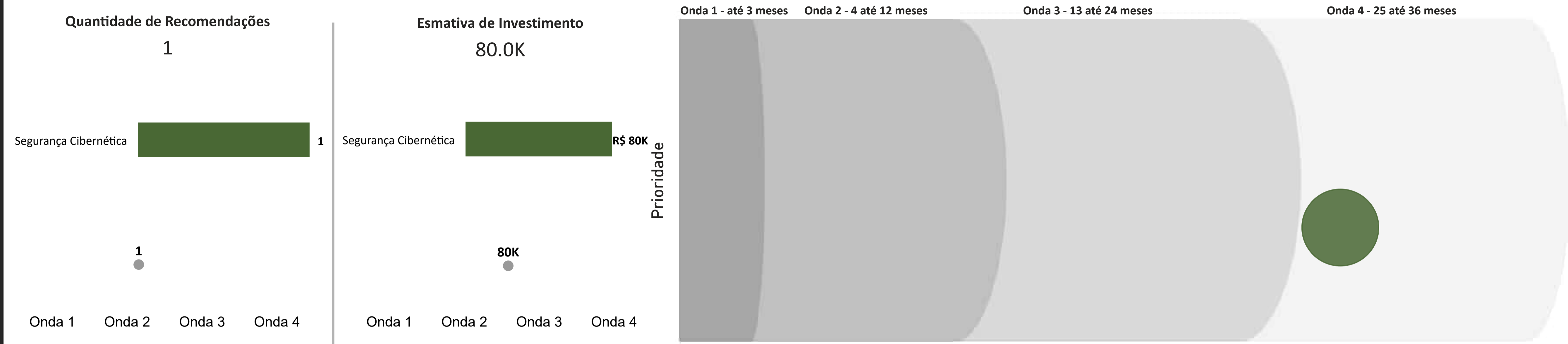
Pessoas

Processos

Tecnologia

Orçamento

Roadmap



Segurança Cibernética	ID 047 - Mecanismo de Bloqueio de Hosts		
Tema Segurança Lógica Duração em Semanas 4 Estimativa de Investimento R\$ 80K Critério de Priorização Sinergia Financeira Média Exequibilidade Média Sinergia na Operação Alta	Issue Não existe mecanismo de bloqueio de dispositivo. Predecessora N/A Recomendação Implementar um mecanismo que possibilite bloquear todo e qualquer dispositivo conectado à rede, a partir do momento em que o mesmo passe a não ser mais autorizado.	Risco de TI Impossibilidade de bloqueio de ativos conectados a rede corporativa.	Risco de Negócio N/A

ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética
1

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Segurança Cibernética



1

Segurança Cibernética

R\$ 0

1

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade



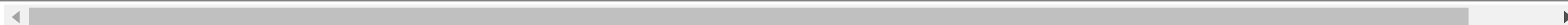
Linha do Tempo



ID 048 - Verificação de Perfil de Acesso

1

2



Segurança Cibernética

ID 048 - Verificação de Perfil de Acesso

Tema
Segurança Lógica

Duração em Semanas
N/A

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Alta

Exequibilidade
Média

Sinergia na Operação
Alta

Issue
Os acessos são concedidos baseados em perfis, mas estes não são confirmados periodicamente. Ou seja, quando um funcionário entra, ele possui uma permissão e as demais são adicionadas.

Predecessora
N/A

Recomendação
Verificar periodicamente as permissões ativas e necessárias para cada usuário.

Risco de TI
Quebra de confidencialidade da informação.

Risco de Negócio
Acesso indevido à informação.



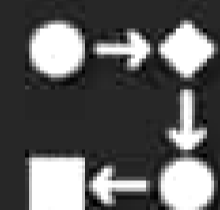
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética
1

Sistemas

Quantidade de Recomendações

1

Segurança Cibernética



1

1

Onda 1 Onda 2 Onda 3 Onda 4

Esmativa de Investimento

80.0K

Segurança Cibernética



R\$ 80K

80K

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses



Prioridade

Linha do Tempo



3 4 5 6 7

ID 049 - Classificação da Informação



Segurança Cibernética

ID 049 - Classificação da Informação

Tema
Segurança Lógica

Duração em Semanas
4

Estimativa de Investimento
R\$ 80K

Critério de Priorização
Sinergia Financeira
Alta

Exequibilidade
Média

Sinergia na Operação
Alta

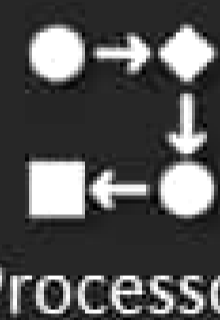
Issue
Não foi identificado nenhum processo definido para classificação da informação do SGB.

Predecessora
N/A

Recomendação
Estabelecer, implementar e monitorar um processo para classificação da informação, a ser executado pelo(s) dono(s) da mesma.

Risco de TI
Quebra de confidencialidade da informação.

Risco de Negócio
Acesso indevido a informações que deveriam ser confidenciais ou restritas, por não estarem classificadas devidamente.



ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética
1

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Segurança Cibernética



1

Segurança Cibernética

R\$ 0

1

0

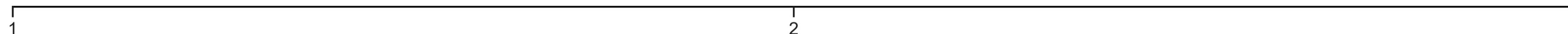
Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade



Linha do Tempo



ID 050 - Política de Backup



Segurança Cibernética

ID 050 - Política de Backup

Tema
Segurança Lógica

Duração em Semanas
2

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Alta

Exequibilidade
Alta

Sinergia na Operação
Média

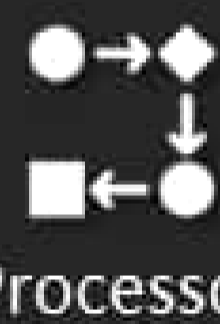
Issue
Não há uma política de backup definida. Apesar de existirem rotinas de backup com armazenamentos online e offline, não há uma política definindo premissas e responsabilidades, recorrência e como será armazenada a cópia de segurança.

Predecessora
N/A

Recomendação
Estabelecer, implementar e monitorar uma política de backup de dados.

Risco de TI
Realizar rotinas de backup de forma empírica compromete sua eficiência.

Risco de Negócio
N/A



ROADMAP DE INICIATIVAS DE TI

Painel

Estratégia

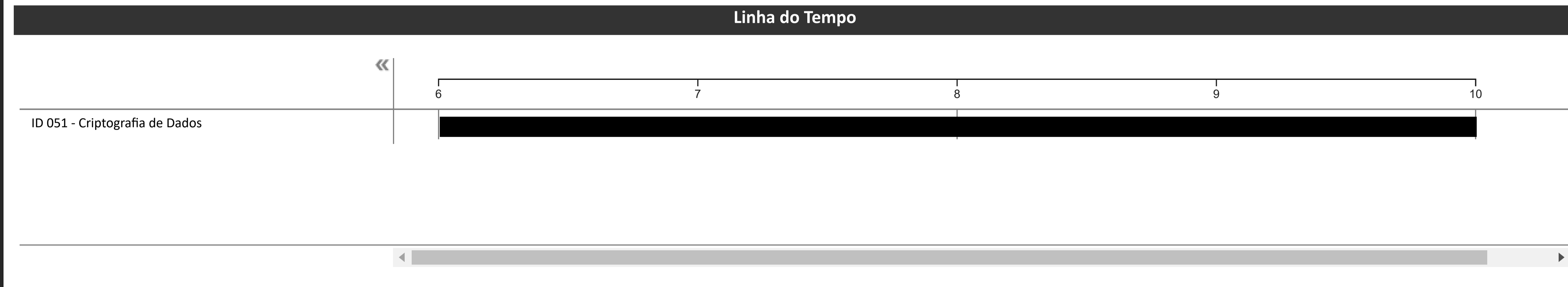
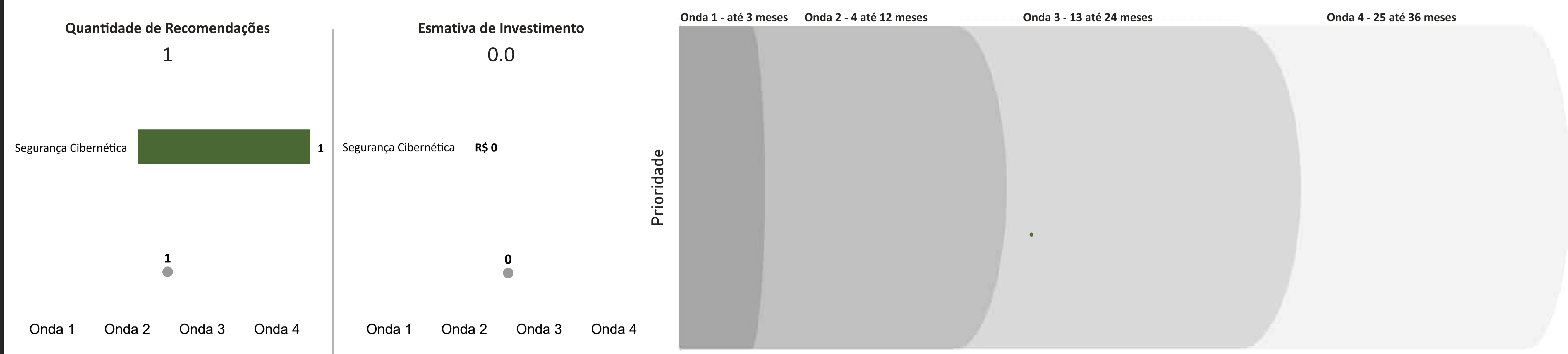
Pessoas

Processos

Tecnologia

Orçamento

Roadmap



Segurança Cibernética	ID 051 - Criptografia de Dados		
Tema Segurança Lógica	Issue A atual solução anti-malware utilizada pelo SGB não contempla a criptografia dos dados armazenados nos ativos. (Computadores, Pendrives, HDs externos, etc)	Risco de TI A não utilização da criptografia de dados nos ativos, principalmente aqueles que são móveis (HDs externos, Laptops, Pendrives, etc), aumenta-se a exposição ao risco de roubo de informações confidenciais da organização, pois qualquer um que tenha acesso ao dispositivo, terá acesso à informação.	Risco de Negócio N/A
Duração em Semanas 4	Predecessora N/A		
Estimativa de Investimento N/A	Recomendação Utilizar solução anti-malware que contemple a criptografia nas unidades de armazenamento ou solução específica de criptografia de dados.		
Critério de Priorização	Sinergia Financeira Média		
Exequibilidade Média	Sinergia na Operação Alta		

ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética
1

Sistemas

Quantidade de Recomendações

1

Esmatima de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Segurança Cibernética



1

Segurança Cibernética

R\$ 0

1

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade



Linha do Tempo



ID 052 - Licença de uso das soluções Anti-Malware do Firewall

1

2

Segurança Cibernética

ID 052 - Licença de uso das soluções Anti-Malware do Firewall

Tema
Segurança Lógica

Duração em Semanas
N/A

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Média

Exequibilidade
Alta

Sinergia na Operação
Alta

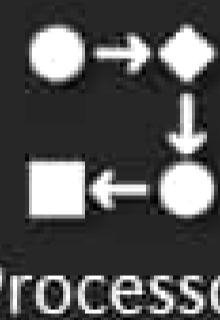
Issue
A licença de uso das soluções anti-malware do Firewall estão com data próxima de expiração e ainda não foram renovadas.

Predecessora
N/A

Recomendação
Renovar a licença das soluções anti-malware do firewall antes do seu vencimento.

Risco de TI
Perda imediata das soluções de proteção contra malware na borda do perímetro, aumentando exponencialmente o risco de ataques cibernéticos.

Risco de Negócio
Indisponibilidade dos serviços e possível perda de informação caso ocorra um ataque cibernético.



ROADMAP DE INICIATIVAS DE TI

Painel

Estratégia

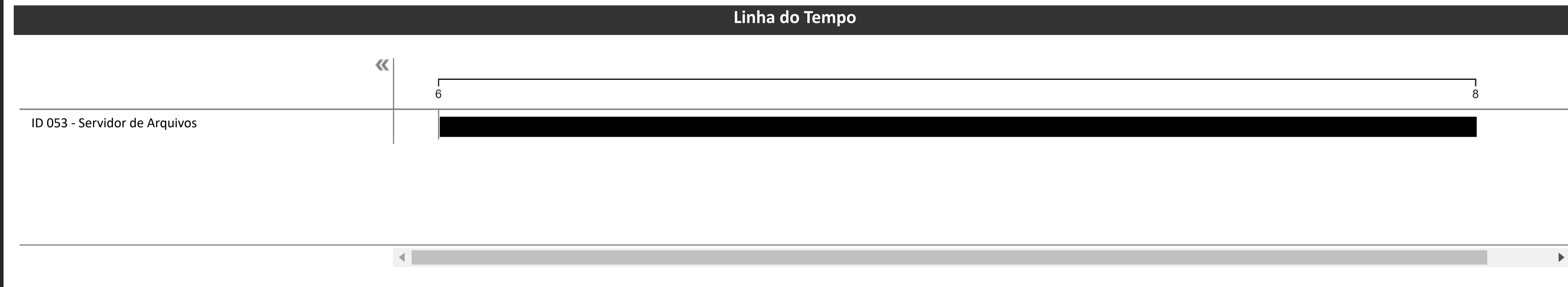
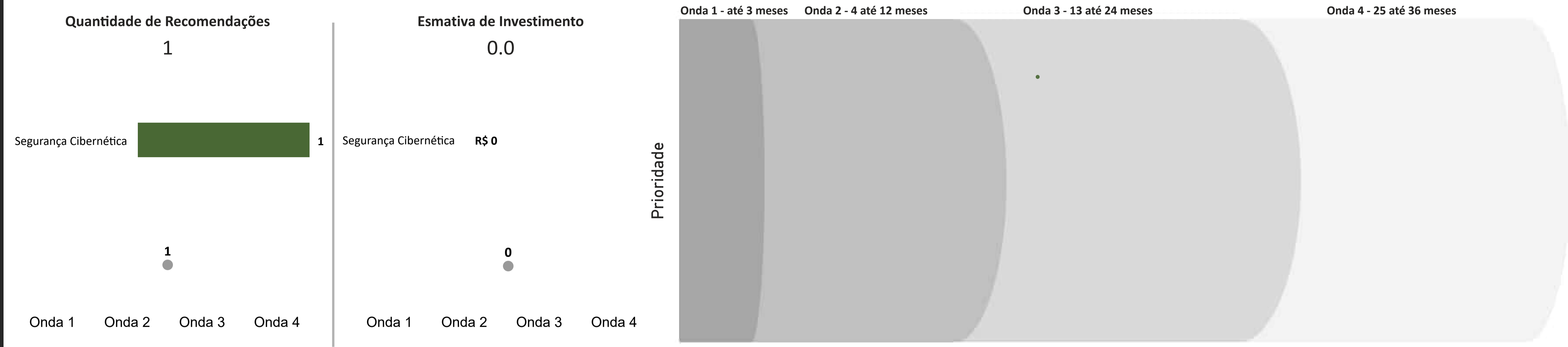
Pessoas

Processos

Tecnologia

Orçamento

Roadmap



Segurança Cibernética	ID 053 - Servidor de Arquivos		
Tema Segurança Lógica	Issue Existem servidores de arquivos instalados nas áreas sem o conhecimento da TI e fora dos padrões de segurança e backup.	Risco de TI Perda de arquivos por não haver backup e risco de ataques via códigos maliciosos.	Risco de Negócio N/A
Duração em Semanas 2	Predecessora ID 017 - APO09 - Atualização do Catálogo de Serviços de TI		
Estimativa de Investimento N/A	Recomendação Identificar, através de protocolo de compartilhamento de arquivos, máquinas instaladas como servidores de arquivos sem o conhecimento da TI e adequar aos padrões existentes.		
Critério de Priorização Sinergia Financeira: Alta			
Exequibilidade Alta			
Sinergia na Operação Alta			

ROADMAP DE INICIATIVAS DE TI ↶

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética
1

Sistemas

Quantidade de Recomendações

1

Segurança Cibernética



1

1

Onda 1 Onda 2 Onda 3 Onda 4

Esmativa de Investimento

0.0

Segurança Cibernética R\$ 0

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Prioridade



Linha do Tempo



3

4

ID 054 - Catracas de Acesso



Segurança Cibernética

ID 054 - Catracas de Acesso

Tema
Segurança Física

Duração em Semanas
N/A

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Alta

Exequibilidade
Alta

Sinergia na Operação
Alta

Issue
As catracas de acesso ao prédio não estão ativas, possibilitando o acesso e saída sem crítica sistêmica.

Predecessora
N/A

Recomendação
Solicitar ao departamento responsável pelo controle de acesso ao prédio a ativação da catraca de acesso para permitir a entrada/saída da unidade apenas para pessoas autorizadas, registrando data e hora dos eventos.

Risco de TI
N/A

Risco de Negócio
Perda da eficiência do controle de acesso, não registrando acesso de pessoas ao local com horário de entrada e/ou saída, além da possibilidade de acesso de pessoas não autorizadas na ausência temporária de um funcionário no local.



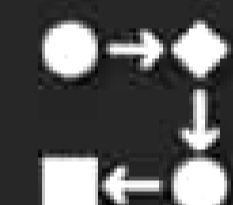
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI

Painel

Estratégia

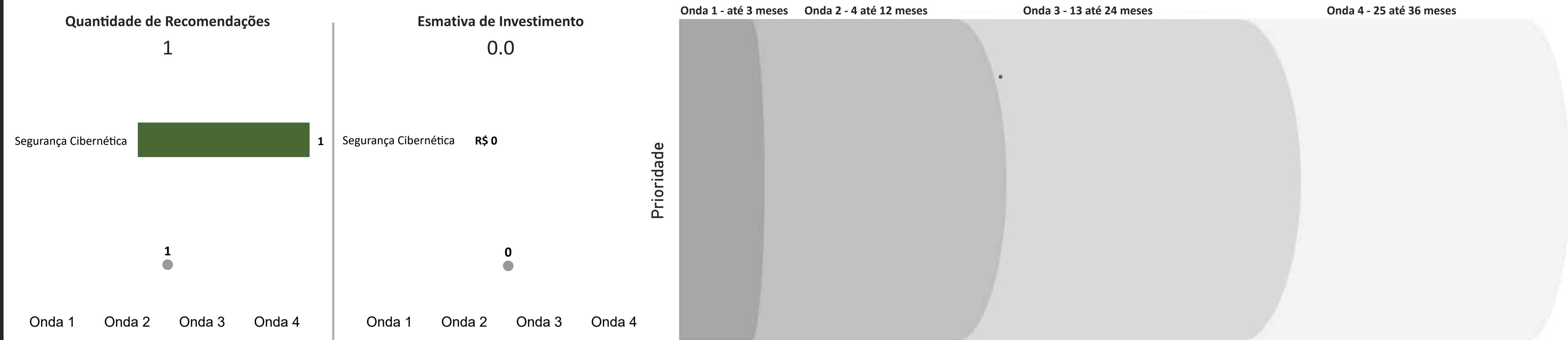
Pessoas

Processos

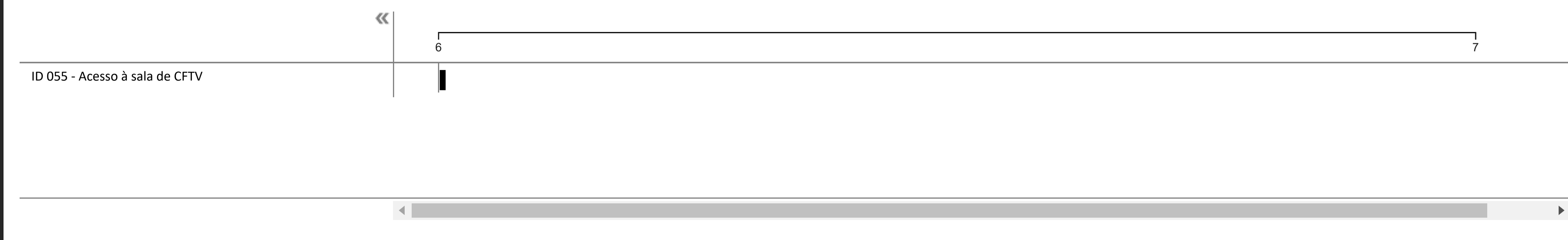
Tecnologia

Orçamento

Roadmap



Linha do Tempo



Segurança Cibernética ID 055 - Acesso à sala de CFTV

Tema Segurança Física	Issue Não há controle de acesso físico na sala de CFTV.	Risco de TI N/A	Risco de Negócio Entrada de qualquer pessoa na sala de controle CFTV, podendo ocasionar perda de informações de registro das imagens acidentalmente ou intencionalmente.
Duração em Semanas N/A	Predecessora N/A		
Estimativa de Investimento N/A	Recomendação Solicitar ao departamento responsável pela administração de controle de acesso a implementação de um controle de acesso físico na sala onde ficam armazenados os equipamentos/gravações das imagens do circuito interno de TV (CFTV).		
Critério de Priorização			
Sinergia Financeira Alta			
Exequibilidade Alta			
Sinergia na Operação Alta			

ROADMAP DE INICIATIVAS DE TI

Painel

Estratégia

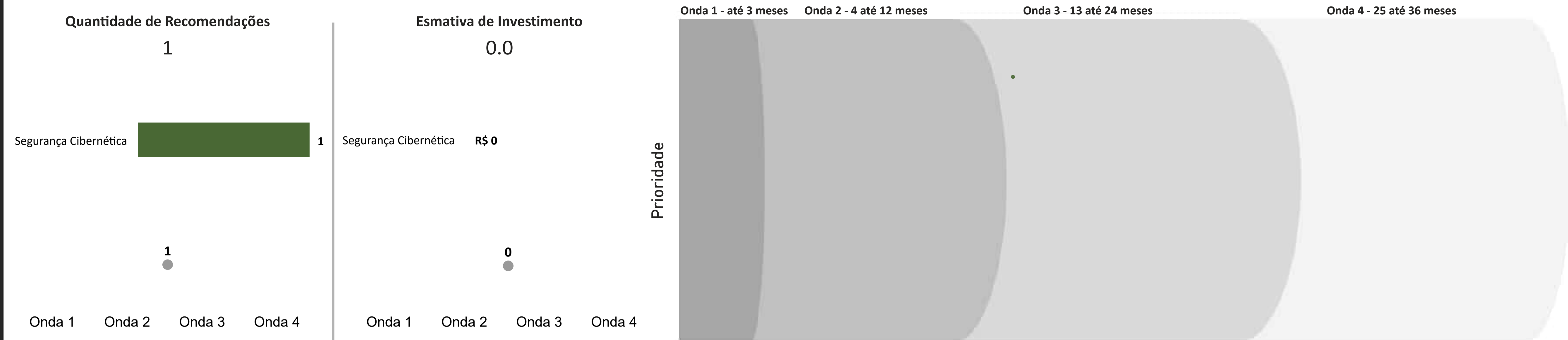
Pessoas

Processos

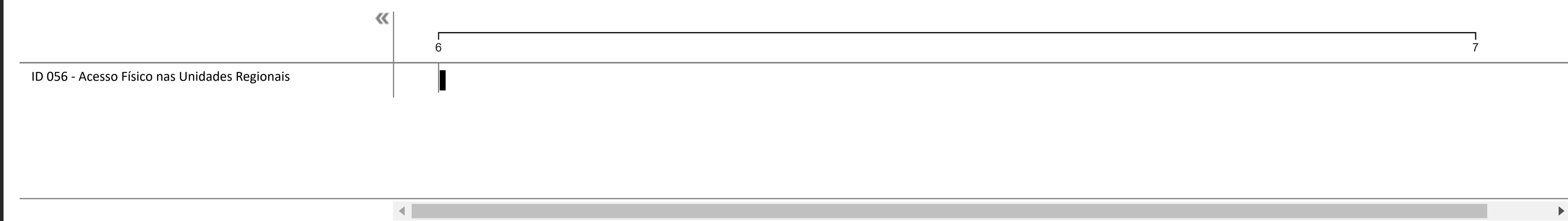
Tecnologia

Orçamento

Roadmap



Linha do Tempo



Segurança Cibernética	ID 056 - Acesso Físico nas Unidades Regionais		
Tema Segurança Física	Issue Não há controle de acesso físico nas unidades regionais.	Risco de TI Acesso de pessoas não autorizadas às salas de acesso restrito da TI, podendo ocasionar roubo de informações e/ou ataques maliciosos.	Risco de Negócio Acesso de pessoas não autorizadas às dependências das unidades regionais, comprometendo a confidencialidade das informações do negócio.
Duração em Semanas N/A	Predecessora N/A		
Estimativa de Investimento N/A	Recomendação Solicitar ao departamento responsável pelo acesso de pessoas em cada unidade regional a implementação de um controle de acesso físico, dando ênfase em salas que possuam equipamentos de TI.		
Critério de Priorização			
Sinergia Financeira Alta			
Exequibilidade Alta			
Sinergia na Operação Alta			

ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética
1

Sistemas

Quantidade de Recomendações

1

Segurança Cibernética



1

1

Onda 1 Onda 2 Onda 3 Onda 4

Esmatima de Investimento

0.0

Segurança Cibernética R\$ 0

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Prioridade



Linha do Tempo



6

7

ID 057 - Ausência de Câmeras em salas restritas



Segurança Cibernética

ID 057 - Ausência de Câmeras em salas restritas

Tema
Segurança Física

Issue
As salas restritas da TI (Datacenter de produção e Datacenter de Backup) não possuem câmeras de monitoramento na parte interna.

Risco de TI
Ações realizadas dentro das salas não poderão ser auditadas.

Risco de Negócio
N/A

Duração em Semanas
N/A

Predecessora
N/A

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Alta

Recomendação
Solicitar ao departamento responsável pela administração do circuito interno de TV (CFTV) a instalação de câmeras de segurança no interior das salas de equipamentos da TI com acesso restrito.

Exequibilidade
Alta

Sinergia na Operação
Alta



ROADMAP DE INICIATIVAS DE TI

Painel

Estratégia

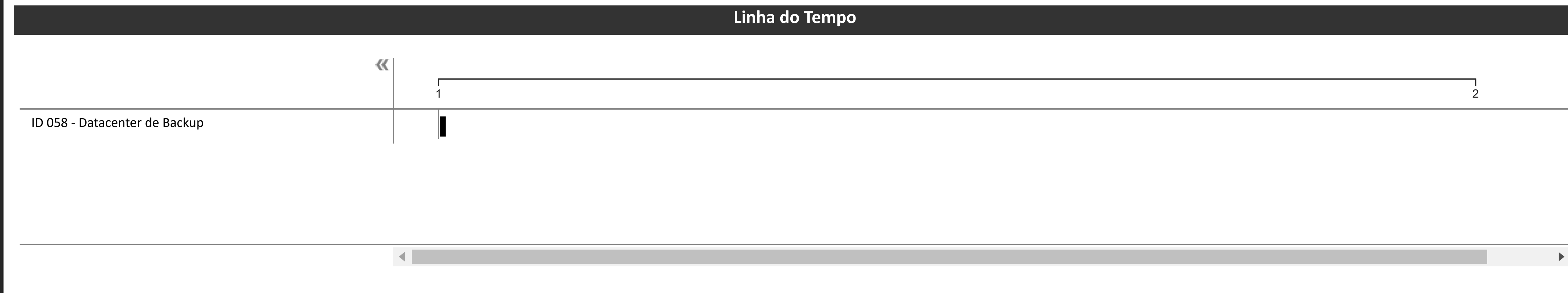
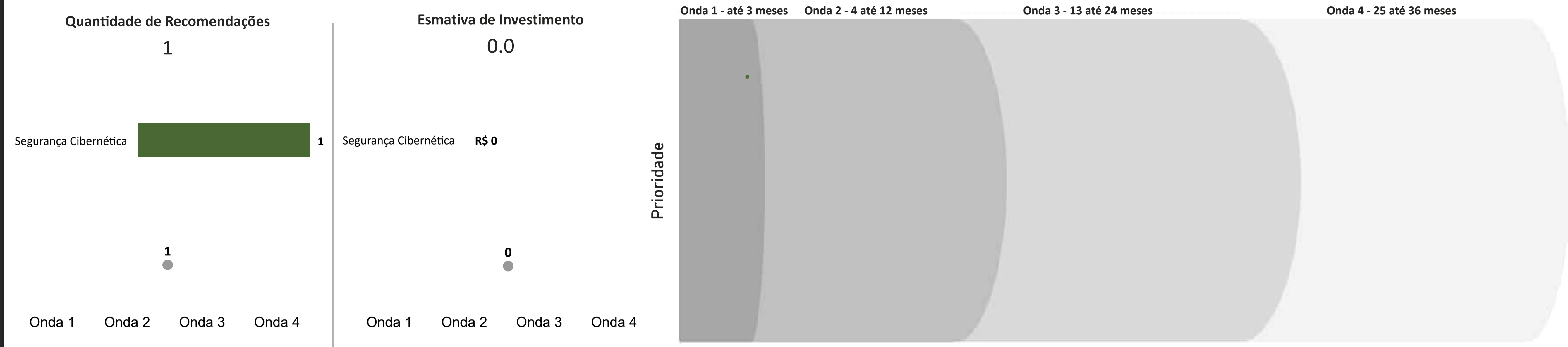
Pessoas

Processos

Tecnologia

Orçamento

Roadmap



Segurança Cibernética	ID 058 - Datacenter de Backup		
Tema Segurança Física	Issue A sala do Datacenter de Backup possui uma janela de vidro para a via pública.	Risco de TI Atos de vandalismo, com facilidade de quebrar o vidro e lançar substâncias que podem causar incêndios dentro da sala.	Risco de Negócio N/A
Duração em Semanas N/A	Predecessora N/A		
Estimativa de Investimento N/A	Recomendação Solicitar ao departamento responsável pela infraestrutura predial vedar a janela com madeira, metal ou alvenaria para mitigar o risco de atos de vandalismo na sala do datacenter de backup.		
Critério de Priorização			
Sinergia Financeira Alta			
Exequibilidade Alta			
Sinergia na Operação Alta			

ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética
1

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Segurança Cibernética



1

Segurança Cibernética

R\$ 0

1

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade



Linha do Tempo



3

4

ID 059 - Chave do Datacenter de Backup



Segurança Cibernética

ID 059 - Chave do Datacenter de Backup

Tema
Segurança Física

Issue
Apesar de possuir controle de acesso biométrico, a sala pode ser aberta por uma chave que fica armazenada na portaria e pode ser entregue para uma lista de pessoas.

Risco de TI
Acesso indevido à sala do Datacenter de Backup por pessoas não autorizadas.

Risco de Negócio
N/A

Duração em Semanas
N/A

Predecessora
N/A

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Alta

Recomendação
Solicitar ao departamento responsável pelo controle de acesso ao prédio, a regularização do funcionamento do acesso biométrico ao datacenter de backup e inutilizar o acesso via chave.

Exequibilidade
Alta

Sinergia na Operação
Alta



ROADMAP DE INICIATIVAS DE TI ↵

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Segurança Cibernética



1

1

Onda 1 Onda 2 Onda 3 Onda 4

Esmativa de Investimento

0.0

Segurança Cibernética R\$ 0

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Prioridade



Linha do Tempo



18

19

ID 060 - Plano de Continuidade de Negócio



Segurança Cibernética

ID 060 - Plano de Continuidade de Negócio

Tema
Segurança Organizacional

Duração em Semanas
N/A

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Alta

Exequibilidade
Alta

Sinergia na Operação
Alta

Issue
Não há Plano de Continuidade de Negócio corporativo definido.

Predecessora
N/A

Recomendação
Solicitar à área de Governança Corporativa a elaboração de um Plano de Continuidade do Negócio, apontando processos críticos e tempo de resposta da TI necessário para restabelecimento destes processos em caso de incidentes.

Risco de TI
N/A

Risco de Negócio
A ausência de um Plano de Continuidade de Negócio corporativo expõe a organização à riscos de interrupção de seus serviços em caso de desastres ou falha crítica.



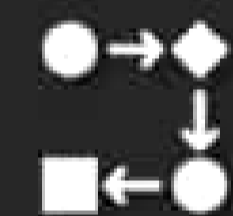
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética
1

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Segurança Cibernética



1

Segurança Cibernética

R\$ 0

1

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade



Linha do Tempo



18

19

ID 061 - Plano de Recuperação de Desastres



Segurança Cibernética

ID 061 - Plano de Recuperação de Desastres

Tema
Segurança Organizacional

Issue
Não há Plano de Recuperação de Desastres definido.

Risco de TI
Incapacidade de restaurar os serviços comprometidos de forma priorizada, organizada e de acordo com os direcionadores das áreas de negócio.

Risco de Negócio
Interrupção prolongada de seus serviços em caso de desastres ou falha crítica.

Duração em Semanas
N/A

Predecessora
N/A

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Alta

Recomendação
Solicitar à área de Governança Corporativa a elaboração de um Plano de Recuperação de Desastres, apontando processos críticos e tempo de resposta da TI necessário para restabelecimento destes processos em caso de incidentes.

Exequibilidade
Alta

Sinergia na Operação
Alta



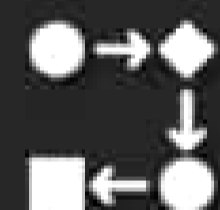
Painel



Estratégia



Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética
1

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Segurança Cibernética



1

Segurança Cibernética

R\$ 0

1

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade



Linha do Tempo



ID 062 - Treinamentos em SI

1

2

Segurança Cibernética

ID 062 - Treinamentos em SI

Tema
Segurança Organizacional

Issue
Baixa adesão aos treinamentos anuais, realizados em parceria com a RNP, que abordam temas relacionados à Segurança da Informação.

Risco de TI
Pessoas mais vulneráveis a ataques através da engenharia social.

Risco de Negócio
N/A

Duração em Semanas
N/A

Predecessora
N/A

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Alta

Recomendação
Buscar patrocínio da alta gestão e maior adesão do público aos treinamentos relacionados à Segurança da Informação.

Exequibilidade
Alta

Sinergia na Operação
Alta



Painel



Estratégia



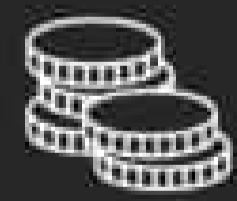
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética
1

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Segurança Cibernética



1

Segurança Cibernética R\$ 0

1

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade



Linha do Tempo



3

4

ID 063 - Validação da Política de SI



Segurança Cibernética

ID 063 - Validação da Política de SI

Tema
Política

Issue
A Política de Segurança da Informação criada para o SGB está aguardando aprovação pela área de Governança Corporativa e ainda não foi implementada.

Risco de TI
Não ter uma Política de SI em vigor expõe a organização à riscos de aumento da vulnerabilidade para ataques cibernéticos, pela falta de padronização/comportamento de seus usuários.

Risco de Negócio
N/A

Duração em Semanas
N/A

Predecessora
N/A

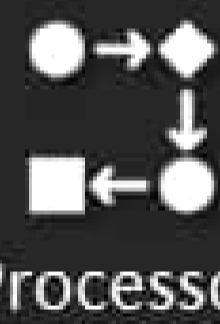
Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Alta

Recomendação
Solicitar à Governança Corporativa a aprovação, divulgação e implementação da Política de Segurança da Informação, que deverá ser revisada na periodicidade definida pelo SGB.

Exequibilidade
Alta

Sinergia na Operação
Alta



ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética
1

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Segurança Cibernética



1

Segurança Cibernética

R\$ 0

1

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade



Linha do Tempo



ID 064 - Senhas de Administração

1

2

Segurança Cibernética

ID 064 - Senhas de Administração

Tema
Política

Issue
O artigo 37 da Política de Segurança da Informação versa que a senha de administração deverá ser compartilhada com o corpo técnico e com terceiros que realizam suporte técnico.

Risco de TI
Risco de comprometimento da confidencialidade da senha com privilégios de Administrador, podendo acarretar em acessos indevidos à ativos da organização.

Risco de Negócio
N/A

Duração em Semanas
N/A

Predecessora
N/A

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Alta

Recomendação
Não compartilhar senhas. Definir senhas individuais de administrador para os usuários necessários.

Exequibilidade
Alta

Sinergia na Operação
Alta



Painel



Estratégia



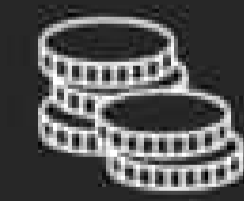
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI

Governança

Infraestrutura

Pessoas

Processos

Segurança Cibernética
1

Sistemas

Quantidade de Recomendações

1

Esmativa de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Segurança Cibernética



1

Segurança Cibernética

R\$ 0

1

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade



Linha do Tempo



3

4

ID 065 - Penalidades Previstas



Segurança Cibernética

ID 065 - Penalidades Previstas

Tema
Política

Issue
O capítulo VI da Política de Segurança da Informação, que versa sobre as penalidades previstas para o descumprimento da política, está redigido de forma genérica, não especificando quais as reais penalidades serão aplicadas para os casos de descumprimento.

Risco de TI
Baixa adesão às normas da Política pela indefinição de quais penalidades serão aplicadas em caso de descumprimento.

Risco de Negócio
N/A

Duração em Semanas
N/A

Predecessora
N/A

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Alta

Recomendação
Especificar detalhadamente quais as penalidades serão aplicadas para cada tipo de descumprimento.

Exequibilidade
Alta

Sinergia na Operação
Alta



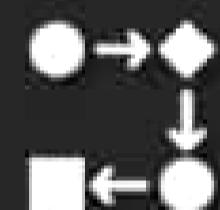
Painel



Estratégia



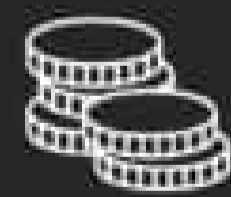
Pessoas



Processos



Tecnologia



Orçamento



Roadmap

ROADMAP DE INICIATIVAS DE TI ↩

Governança

Infraestrutura

Pessoas
1

Processos

Segurança Cibernética

Sistemas

Quantidade de Recomendações

1

Esmatima de Investimento

0.0

Onda 1 - até 3 meses Onda 2 - 4 até 12 meses Onda 3 - 13 até 24 meses Onda 4 - 25 até 36 meses

Pessoas



1

Pessoas R\$ 0

1

0

Onda 1 Onda 2 Onda 3 Onda 4

Onda 1 Onda 2 Onda 3 Onda 4

Prioridade



Linha do Tempo



3

4

ID 066 - Alteração na estrutura organizacional



Pessoas

ID 066 - Alteração na estrutura organizacional

Tema
Estrutura Organizacional

Issue
N/A

Risco de TI
N/A

Risco de Negócio
N/A

Duração em Semanas
N/A

Predecessora
N/A

Estimativa de Investimento
N/A

Critério de Priorização
Sinergia Financeira
Média

Recomendação
Implementar os ajustes na Estrutura Organizacional de acordo com o modelo da estrutura futura recomendada e detalhada no capítulo Pessoas do PDTI.

Exequibilidade
Média

Sinergia na Operação
Alta



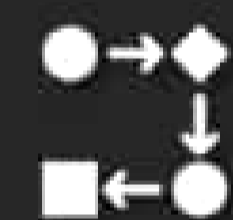
Painel



Estratégia



Pessoas



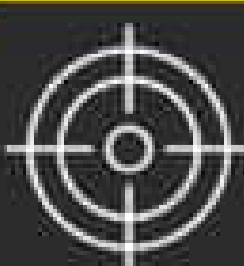
Processos



Tecnologia



Orçamento



Roadmap

- Painel 
- Estratégia 
- Pessoas 
- Processos 
- Tecnologia 
- Orçamento 
- Roadmap 
- Anexos** 

LISTA DE DOCUMENTOS ANEXOS AO PDTI

Anexo I - Make or Buy 

Anexo II - Modelo de Capacidade 

Anexo III - Gaps e Recomendações Processos 

Anexo IV - Inventário de Aplicações 

Anexo V - Gaps e Recomendações Sistemas 

Anexo VI - Ficha Iniciativas - PDTI 

Zip da lista de documentos anexos ao PDTI 



**SERVIÇO GEOLÓGICO
DO BRASIL - CPRM**



**Building a better
working world**