

POLÍTICAS E QUALIDADE EM T.I

(Gestão do Conhecimento)

Unidade 03

Prof. Daniel Caixeta



Auditoria em T.I: Processos, técnicas e metodologias.

8.1. Conceitos de auditoria em T.I.

8.2. Quem realiza a auditoria?

8.3. Modelos para a auditoria.

8.3.1. COBIT - *Control Objectives for Information and related Technology.*

8.3.2. ITIL - *Information Technology Infrastructure Library.*

8.3.3. CMMI - *Capability Maturity Model Integration.*

8.3.4. MPS.br - Melhoria do Processo de Software Brasileiro.

8.3.5. Val IT – *Enterprise Value: Governance of IT Investments.*

8.3.6. Risk IT – *Enterprise Risk: Identify, Govern and Manage IT Risk.*

8.3.7. SCRUM - Metodologia Ágil.

8.3.8. OPM3 - *Organizational Project Management Maturity Model.*

8.3.9. Seis Sigma / *Six Sigma.*

8.3.10. BSC - *Balanced Scorecard.*

8.3.11. Modelos ISO - *International Organisation for Standardisation.*

8.4. Das técnicas para a realização de auditorias.



08

[Continuação]

8.5. Processos de auditoria de *software*.

8.5.1. O planejamento [...].

8.5.2. A execução [...].

8.5.3. Os relatórios [...].

8.5.4. Fique atento!

09

Compliance em T.I: Leis vigentes e melhores práticas [...].

9.1. Introdução.

9.2. As legislações vigentes.

9.2.1. Lei da Propriedade Intelectual (Lei 9.279/1996).

9.2.2. Lei dos Direitos Autorais (Lei 9.609/1998).

9.2.3. Lei do *Software* (Lei 9.610/1998).

9.2.4. Lei das Provas Eletrônicas (Lei 12.850/2013).

9.2.5. Marco Civil da Internet (Lei 12.965/2014).

9.2.6. Lei do *Home Office* (Lei 13.467/2017).

9.2.7. Lei Geral de Proteção de Dados Pessoais - LGPD (Lei 13.709/2018).

REFERÊNCIAS



8. AUDITORIA EM T.I

Processos, técnicas e metodologias.

8.1. CONCEITOS DE AUDITORIA EM T.I.

- De acordo com Gonçalves (2018), auditoria em sistemas de T.I., é:

[...] uma atividade independente que objetiva gerenciar o risco operacional existente e avaliar a adequação das tecnologias e dos S.I utilizados na empresa. Esse processo revisa e avalia os controles, o desenvolvimento de *softwares*, os procedimentos de T.I, a infraestrutura, a operação, o desempenho e a segurança da informação.
- Em se tratando de *software* e seus processos de desenvolvimento, o conceito de auditoria se modifica um pouco. Digamos, que sejam quase similares:

É uma atividade que também gerencia riscos operacionais e avalia se as tecnologias utilizadas na organização são adequadas. Para isso, ela revisa e avalia os controles, os processos de desenvolvimento, a infraestrutura de T.I, a operação, o desempenho e a segurança da informação. (GONÇALVES, 2018 modificado CAIXETA 2022).

- Portanto, estão em jogo informações críticas que auxiliam nas tomadas de decisões.
- Por sua vez, o processo de desenvolvimento tem como objetivos e responsabilidades, medir e constatar a eficácia do sistema, atestar a segurança física e lógica e aferir se essas providências atendem às normas. (*ibidem*).



8.2. QUEM REALIZA A AUDITORIA?

- É função de um auditor com formação em auditoria computacional:
 - ✓ Compreender e analisar o ambiente;
 - ✓ Determinar quais são as situações mais sensíveis;
 - ✓ Elaborar e aplicar o *checklists*;
 - ✓ Analisar as simulações;
 - ✓ Opinar sobre o ambiente auditado.
- Além disso, o auditor alocado na área de desenvolvimento deve conhecer as metodologias de desenvolvimento de sistemas, suas etapas, técnicas, formulários e conceitos, além de conhecer os profissionais da área: o líder de projeto, o analista de sistemas e o próprio desenvolvedor. (GONÇALVES, 2018).



8.3. MODELOS PARA AUDITORIAS

- Em se tratando de *software* e S.I., com o aumento de problemas resultantes da relação de qualidade e segurança, e.g., o aumento do número de fraudes, perdas e/ou roubos de informações, etc., as corporações passaram por regulamentações que colocaram em cena leis rigorosas tais como:

ALGUMAS LEIS	
✓ <i>Sarbanes-Oxley Act (SOxA)</i> .	✓ Marco Civil da Internet.
✓ Acordo da Basiléia.	✓ LGPD (Lei Geral de Proteção de Dados), etc.

- Assim, as empresas passaram a adotar melhores práticas de gestão de risco e gestão operacional afim de alinhar seus modelos de negócios para garantia de melhorias nos processos empresariais. (GONÇALVES, 2018).

- A governança de T.I utiliza de ferramentas e aplicações cuja finalidade é aumentar a vantagem competitiva das organizações. Para isso foram criados vários institutos internacionais e modelos de gestão que, quando aplicados, asseguram a conformidade com as melhores práticas de processos, de segurança da informação e de gerenciamento dos riscos corporativos. (GONÇALVES, 2018).
- Esses modelos formam a base do desenvolvimento de controles internos para as instituições, sendo que cada um possui uma metodologia própria, desenvolvida pelo instituto responsável.
- Escolher um modelo de gestão depende dos objetivos da organização.
- A seguir, apresentaremos alguns modelos importantes:

8.3.1. COBIT - *Control Objectives for Information and related Technology*

- É um modelo abrangente aplicável para a auditoria e o controle de processos de T.I, desde o planejamento da tecnologia até a monitoração e auditoria de todos os processos.

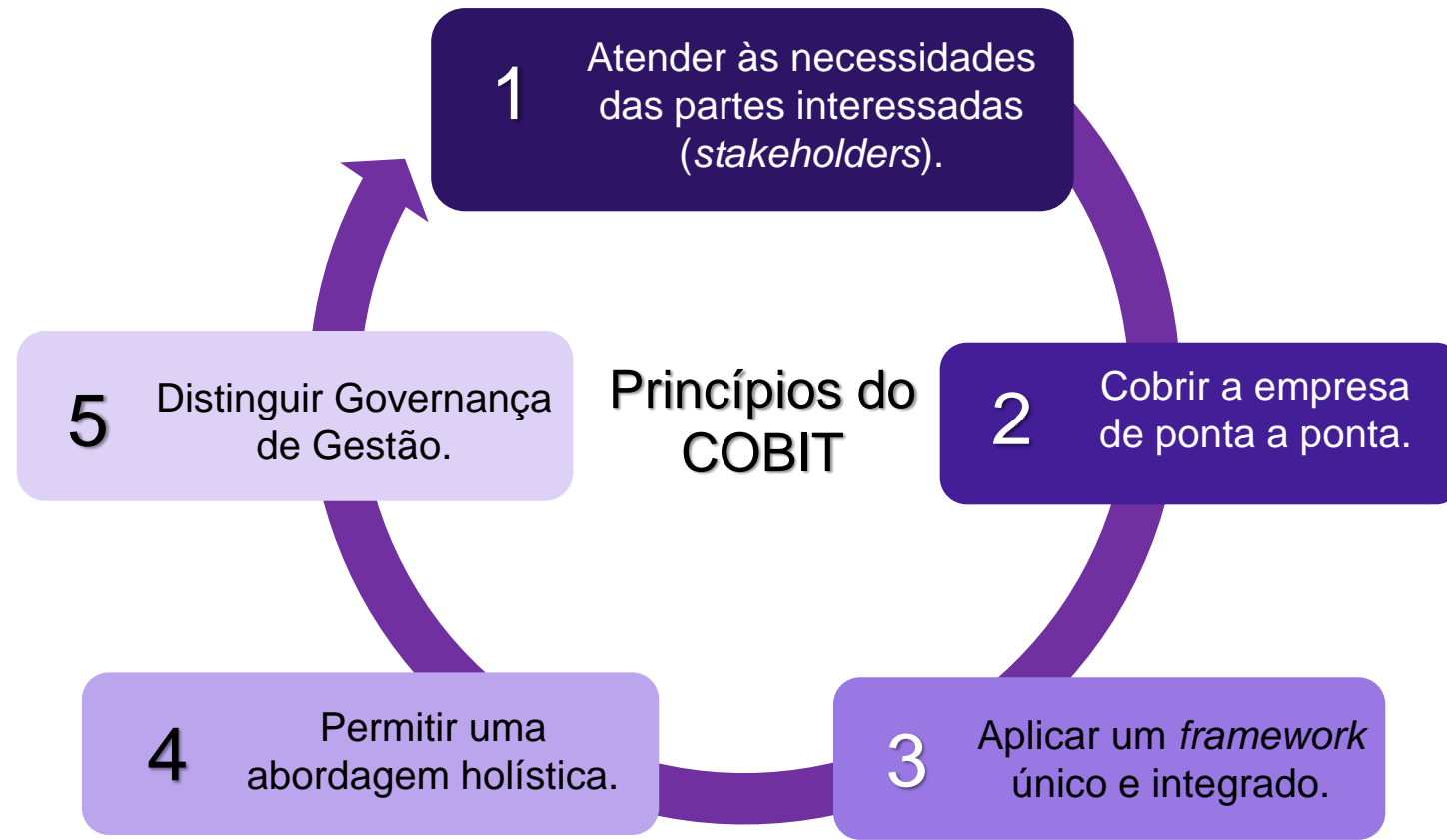


Figura 1. Princípios do COBIT 5. (Adaptado CAIXETA, 2021).

- É uma metodologia indicada para governança de T.I.
- O COBIT traz um conjunto de melhores práticas relacionadas ao controle de objetivos, à otimização de investimentos, aos mapas de auditoria e às técnicas de gerenciamento.
- É voltada para todas as empresas, independentemente das plataformas tecnológicas adotadas, e busca alinhar as práticas de T.I ao modelo de negócio cuja finalidade é regulamentar o processo.



COBIT5 FOUNDATION

COBIT2 FOUNDATION

8.3.2. ITIL - *Information Technology Infrastructure Library*

- Refere-se aos serviços de T.I, segurança da informação, gerenciamento da infraestrutura, gestão de ativos e aplicativos, etc.
- É indicado para a Gestão de serviços em T.I.

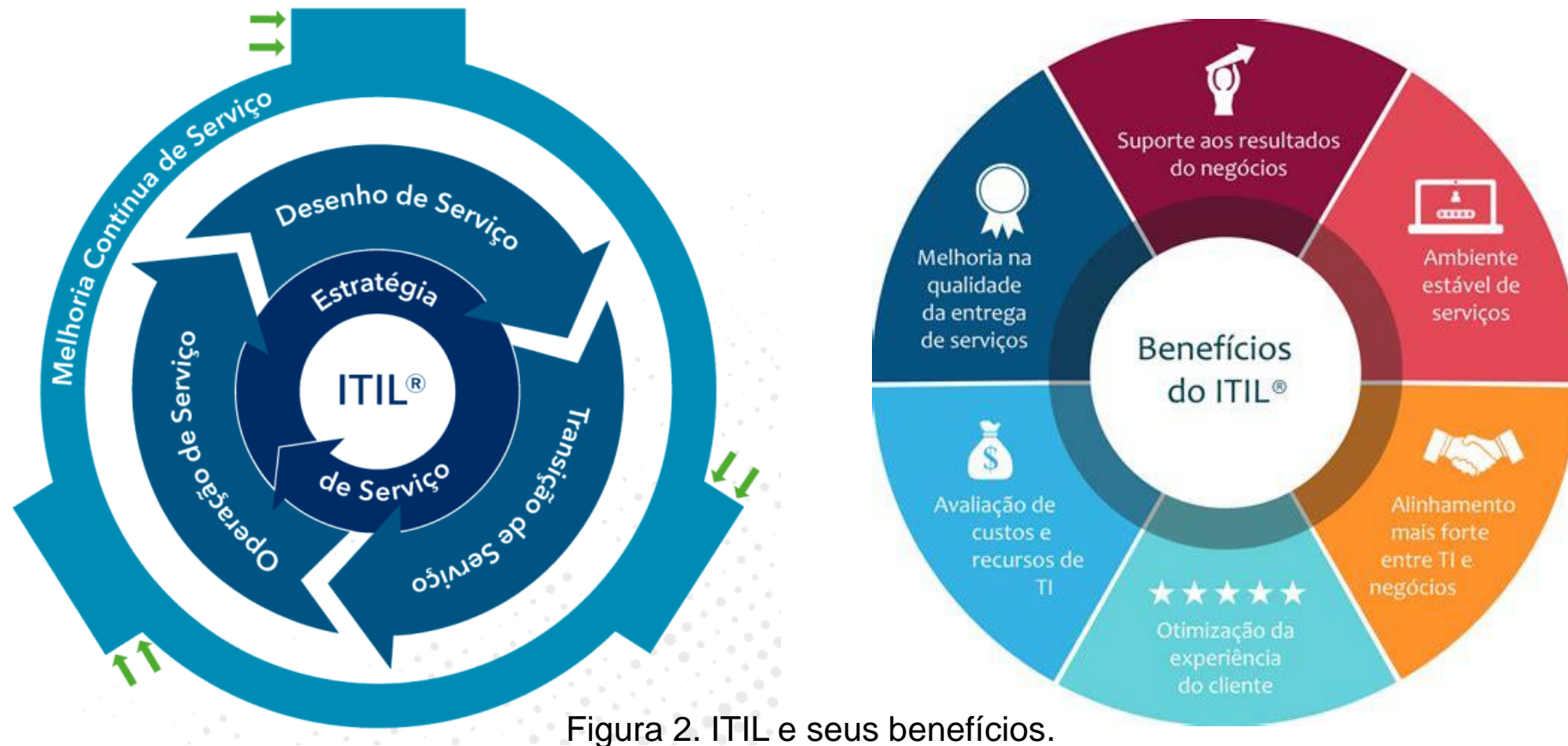


Figura 2. ITIL e seus benefícios.

8.3.3. CMMI - *Capability Maturity Model Integration*

- Tem o propósito de ser um guia para a implantação das melhores práticas para as organizações provedoras de serviços, sendo que essas melhores práticas estão focadas nas atividades para fornecer serviços com qualidade para os clientes e usuários finais. Foco no desenvolvimento de produtos e projetos de sistemas e software.

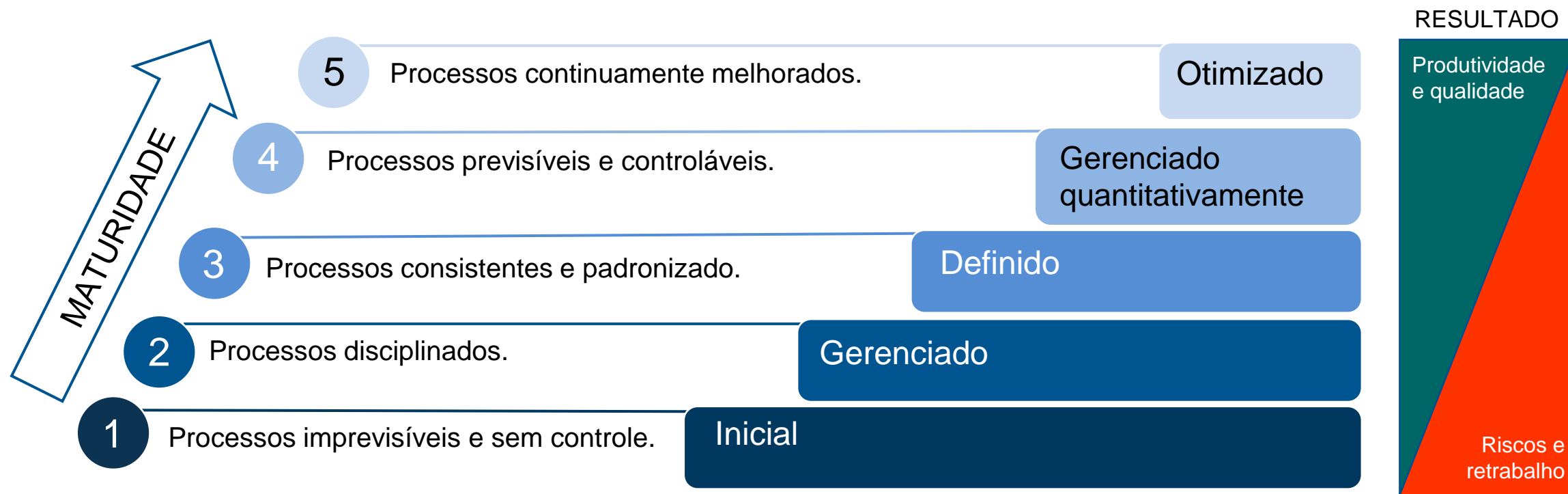


Figura 3. Níveis de maturidade CMMI.

8.3.4. MPS.br - Melhoria do Processo de Software Brasileiro

- Modelo brasileiro proposto para a melhoria do processo e desenvolvimento de *softwares* no Brasil.

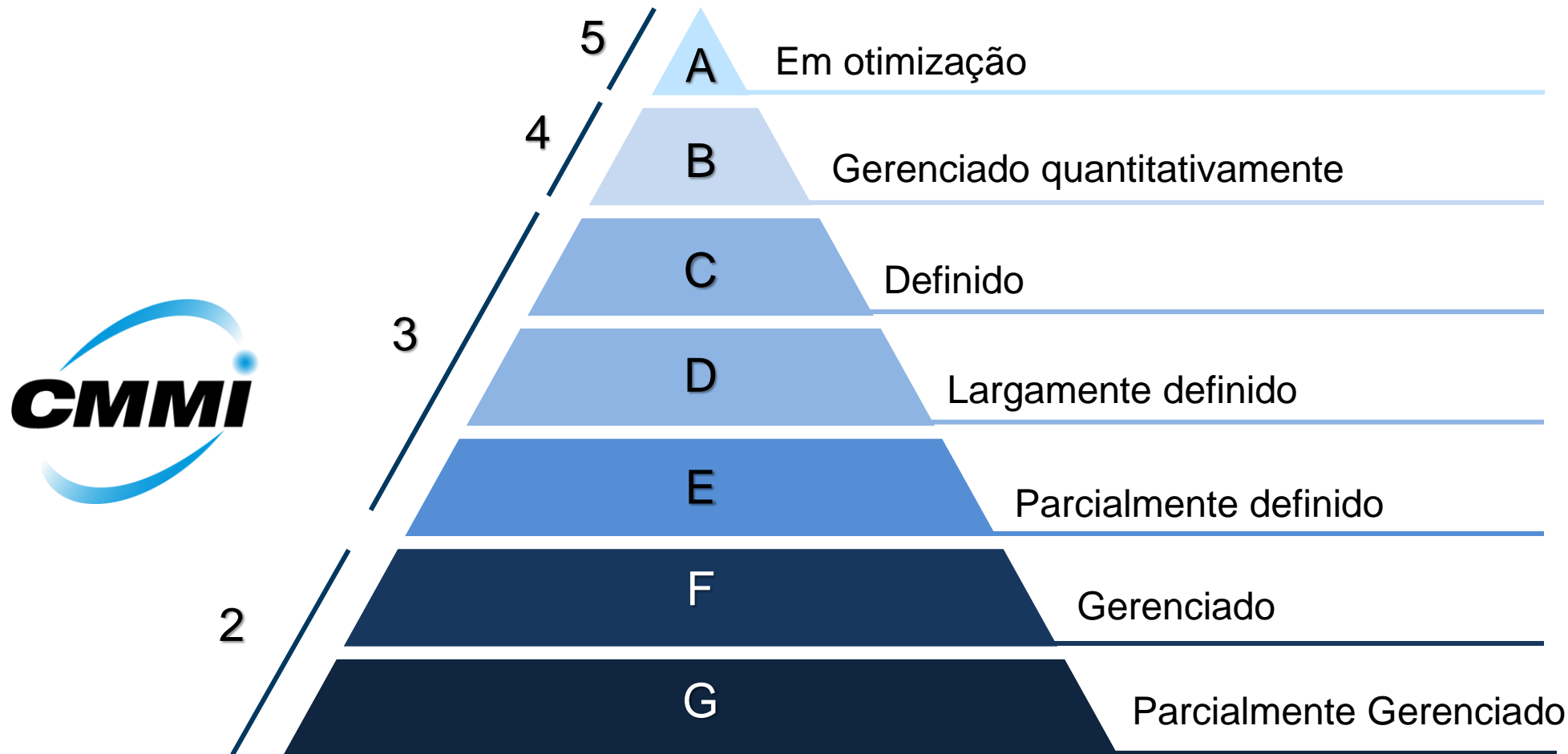


Figura 4. CMMI e MPS.BR. (Adaptado CAIXETA, 2021).

8.3.5. Val IT – *Enterprise Value: Governance of IT Investments*

- Modelo que trata da governança dos investimentos de T.I e gerenciamento do portfólio desses investimentos.

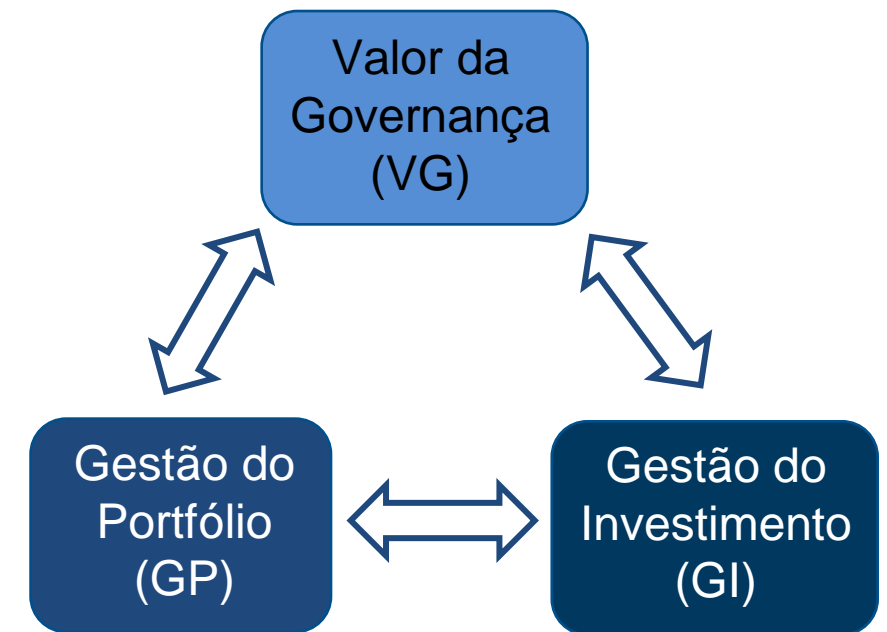
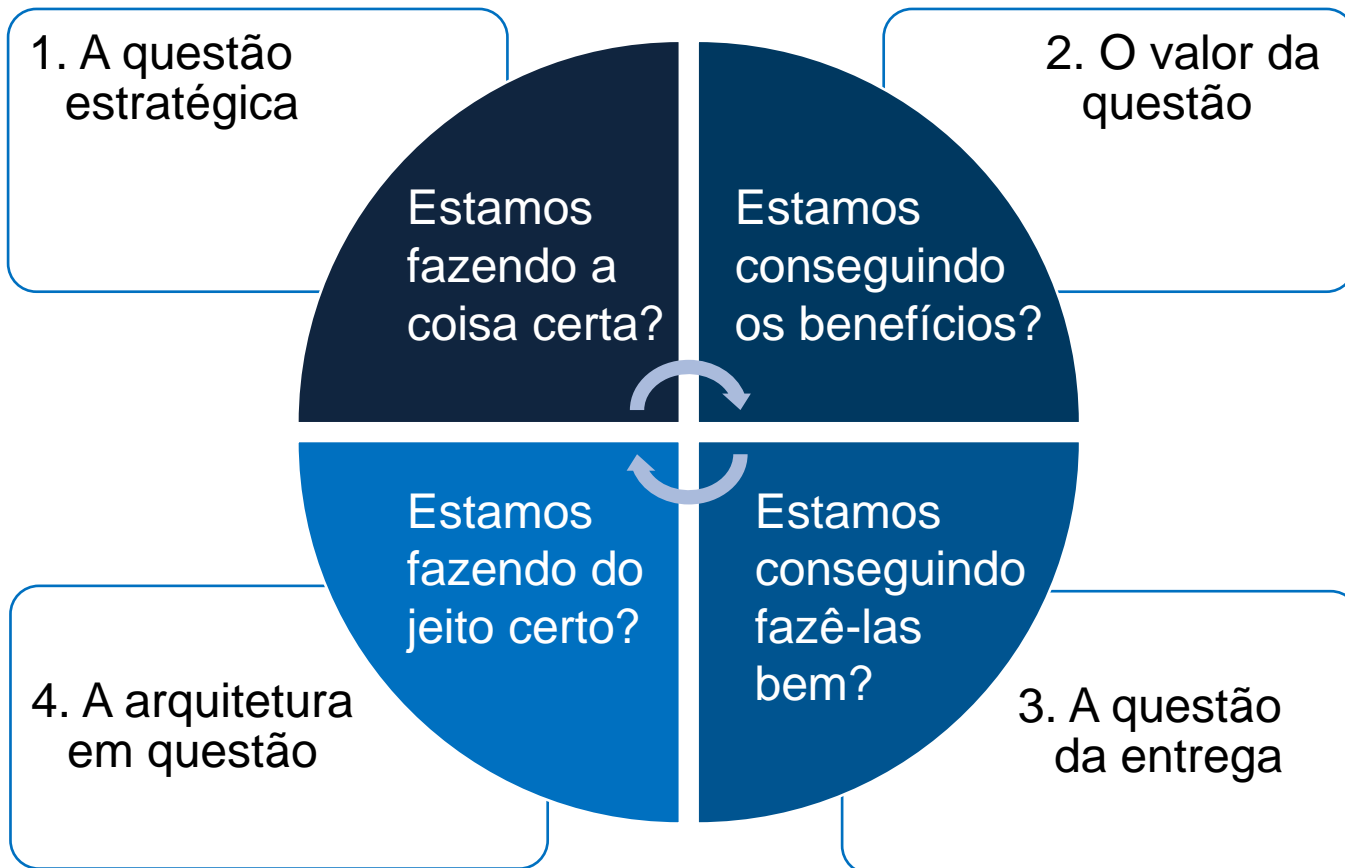
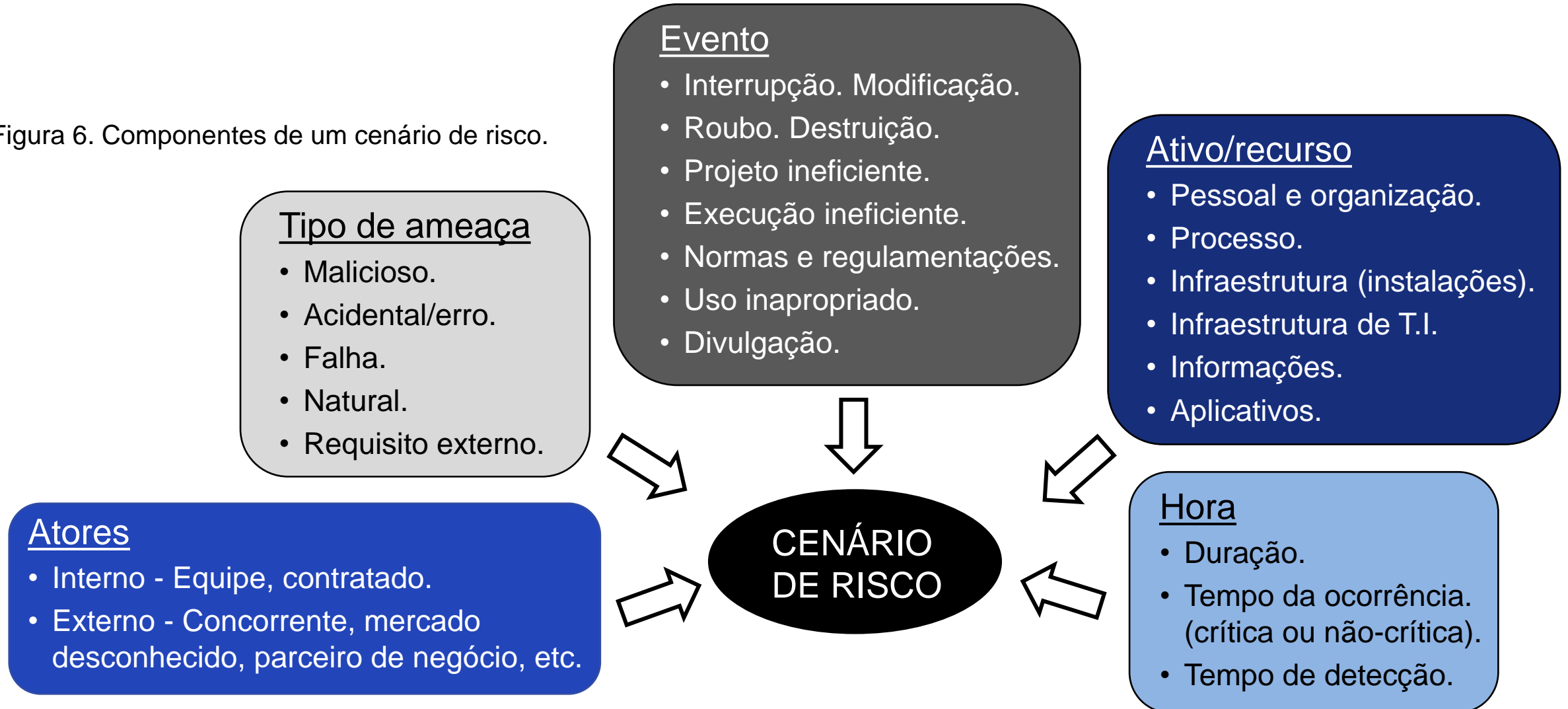


Figura 5. Questionamentos do *framework* Val IT e suas relações. (Adaptado CAIXETA, 2021).

8.3.6. Risk IT – *Enterprise Risk: Identify, Govern and Manage IT Risk*

- Modelo que trata do gerenciamento de riscos na TI.

Figura 6. Componentes de um cenário de risco.



8.3.7. SCRUM - Metodologia Ágil

- Metodologia para gerenciamento de projetos de *softwares*, *hardwares*, etc., de forma ágil.



Figura 7. Valores e princípios do SCRUM.

8.3.8. OPM3 - *Organizational Project Management Maturity Model*

- Modelo de maturidade para gerenciamento de projetos.

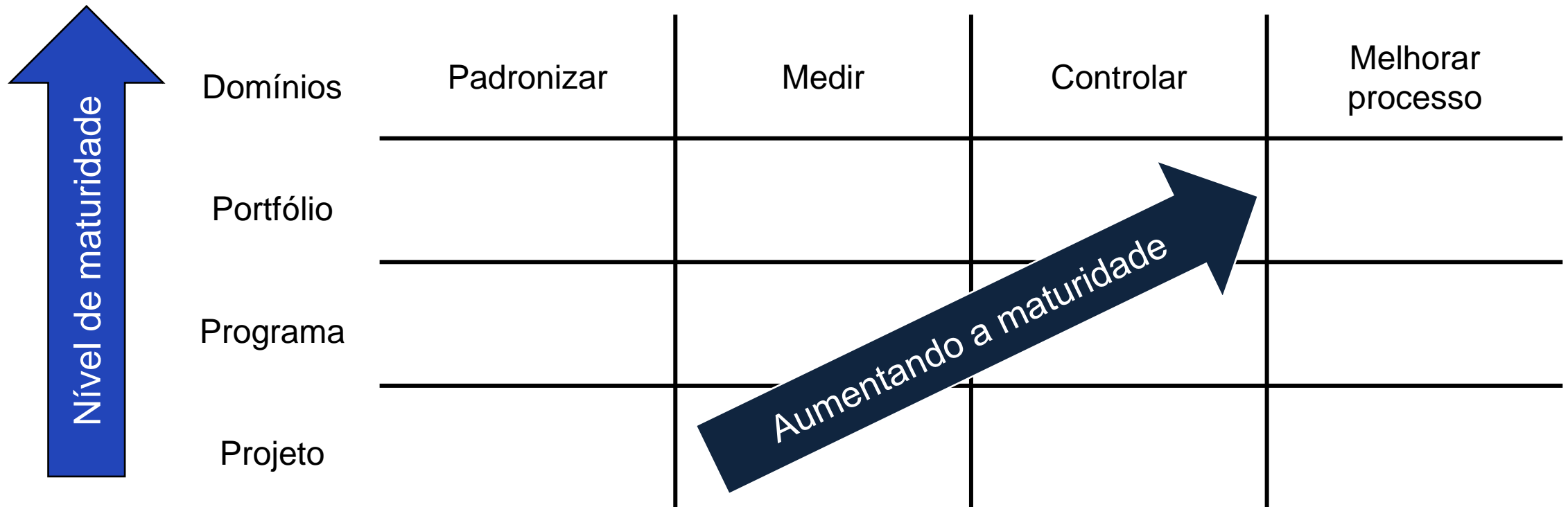


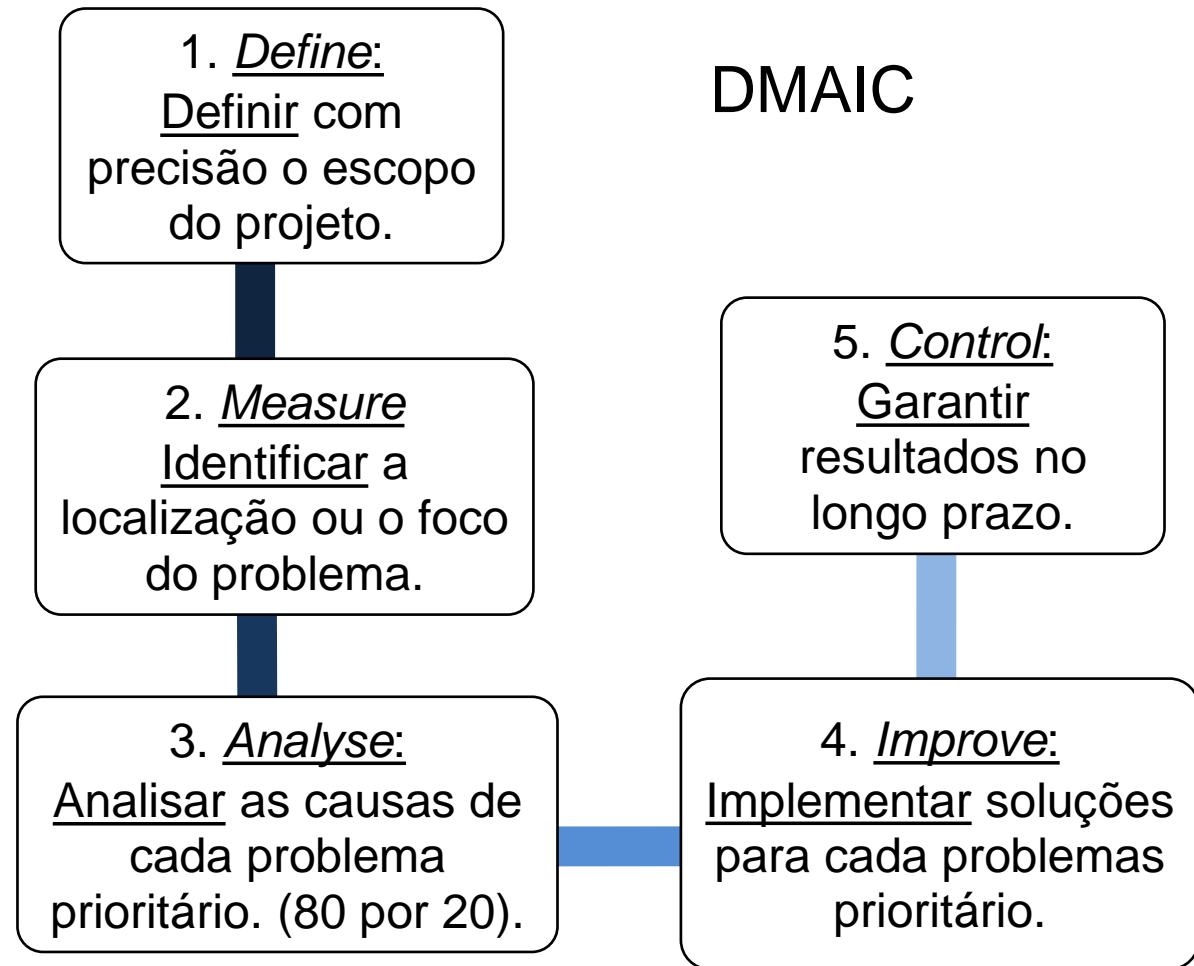
Figura 8. Matriz OPM3.

8.3.9. Seis Sigma / Six Sigma

- Metodologia para melhoria da qualidade do processo.



Figura 9. Ciclo Seis Sigma/Six Sigma.

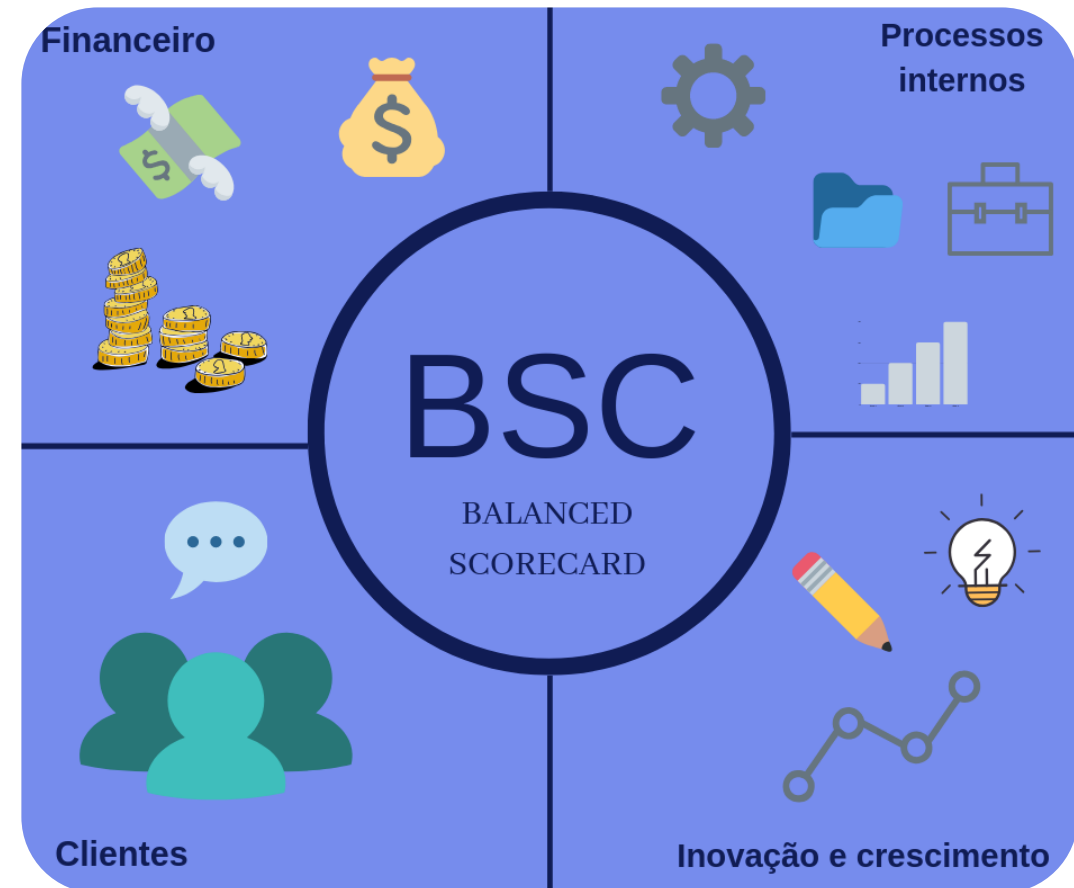


8.3.10. BSC - *Balanced Scorecard*

- Metodologia de planejamento e gestão da estratégia.



Figura 10. Processos BSC.



8.3.11. Modelos ISO - *International Organisation for Standardisation*

- Trata-se de sistemas de qualidade, ciclo de vida de *software*, teste de qualidade, etc., além das normas descritas na tabela abaixo:



NORMA	DO QUE SE TRATA
ISO 31.000	<ul style="list-style-type: none">• Trata-se dos princípios e guias para o gerenciamento de riscos.
ISO/IEC 20.000	<ul style="list-style-type: none">• Norma que aborda requisitos e melhores práticas para o gerenciamento de serviços de T.I.
ISO/IEC 27.001/ ISO/IEC 27.002	<ul style="list-style-type: none">• Requisitos e código de prática para a gestão de segurança da informação.
ISO 21.500	<ul style="list-style-type: none">• Normas que recomenda às organizações um modo profissional de gerenciar os projetos com base nas melhores práticas do mercado global.

(FERNANDES & ABREU (2012, p.200-201) & CAIXETA (2021)).

Figure 5.1: Risk Management Components



Figura 11. Controles internos (COSO 2013) e Gestão de Risco (ISO 31.000).

Disponível em: https://iso31000.net/wp-content/uploads/2018/01/COSO-ERM-2017_overview.png.

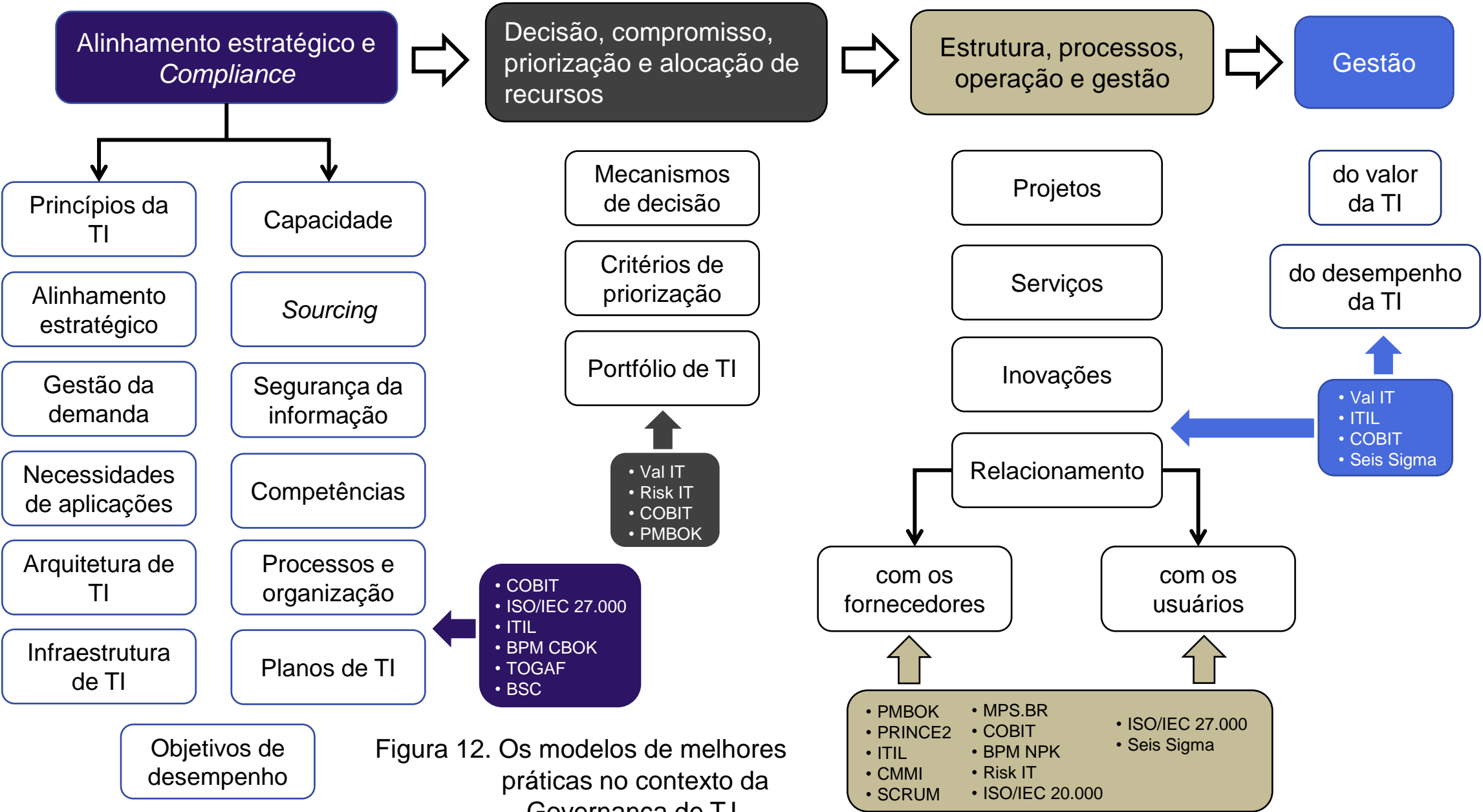


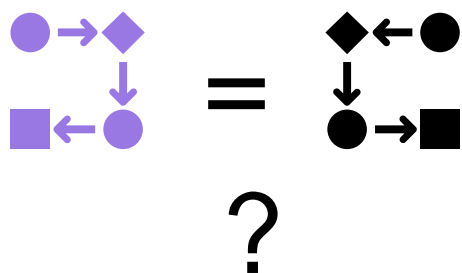
Figura 12. Os modelos de melhores práticas no contexto da Governança de T.I.

8.4. DAS TÉCNICAS PARA A REALIZAÇÃO DE AUDITORIAS

- A realização de auditorias é feita por meio de técnicas. Entre elas, considere as apresentadas a seguir segundo Gonçalves (2018):

1. Questionários

- ✓ Por meio dessa técnica, é possível adequar o ponto de controle em relação aos parâmetros de controle interno, como segurança física, lógica, eficiência, entre outros.



2. Simulação de dados

- ✓ O auditor afere se a aplicação está dentro das normas, verificando se os dados inseridos no sistema são incompatíveis ou estão em duplicidade.

3. Visita *in loco*

- ✓ Trata-se da atuação dos auditores junto às pessoas da organização relacionadas ao sistema e às instalações. A partir dessa técnica, pode-se anotar procedimentos, nomes de pessoas, analisar a documentação e emitir opinião em relatórios.



4. Entrevista

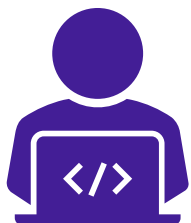
- ✓ São reuniões entre os auditores e os auditados.
- ✓ Depois de realizar a entrevista, o auditor pode analisar os resultados e emitir o seu relatório.

5. Análise de logs

- ✓ Aqui verifica-se a utilização de dispositivos componentes de uma configuração ou rede de computadores e do *software* aplicativo. Assim, pode-se verificar a ineficiência da utilização do computador, bem como identificar erros de programa e/ou operação, utilização de programas que geram fraudes, tentativas de acesso indevidas e problemas na configuração do computador (análise de dispositivos com folga ou sobrecarregados).



6. Análise de programa-fonte (código-fonte)



- ✓ Essa técnica consiste na análise visual do programa. Compara-se também a versão do objeto que está sendo executado com o objeto resultante da última versão compilada. Essa técnica analisa se o desenvolvedor cumpriu as normas de padronização do código e a qualidade de estruturação do código-fonte.

- De acordo com Gonçalves (2018), a realização de auditorias é feita por meio de técnicas que podem ser conduzidas de três maneiras, sendo elas:
 - 1ª - Realizada pela própria organização.
 - 2ª - Conduzida por uma organização sobre outra.
 - 3ª - Realizada por uma terceira organização independente, sem que haja interesse nos possíveis resultados da auditoria.
- Na figura a seguir, observa-se como a auditoria se insere no ciclo de vida de produtos da T.I.



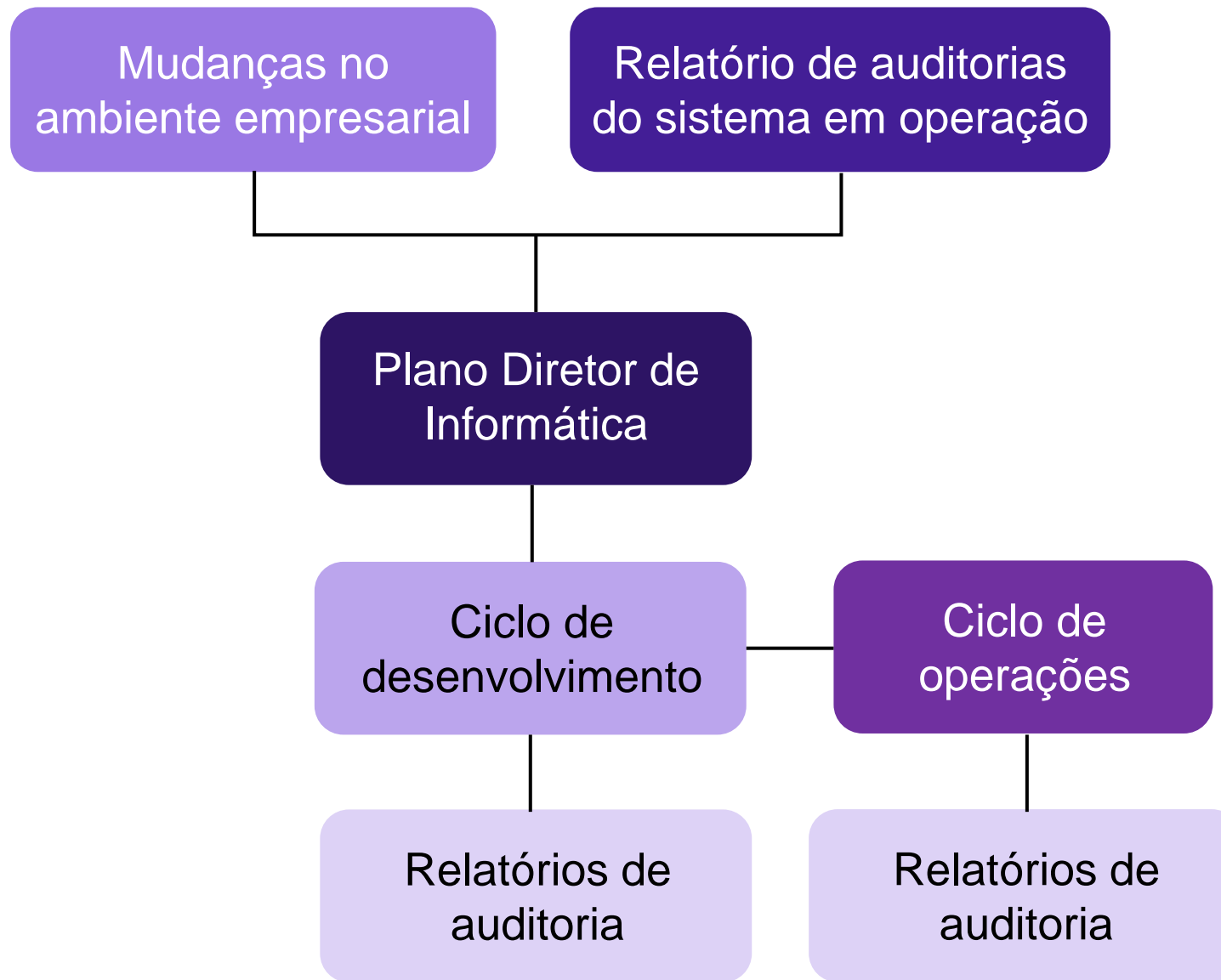
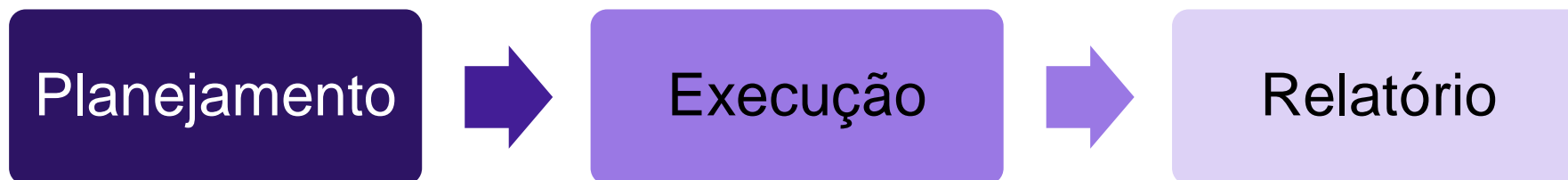


Figura 13. Auditoria no ciclo de vida de um produto de T.I. (GONÇALVES, 2018).

8.5. PROCESSOS DE AUDITORIA DE SOFTWARE

- A auditoria de *software* tem como objetivo:
 1. Verificar e constatar a eficácia do sistema;
 2. Atestar a sua segurança física e lógica;
 3. Garantir a sua qualidade;
 4. Ajudar a organização a avaliar e validar normas e padrões preestabelecidos.
- A auditoria de *software* é dividida em três etapas:

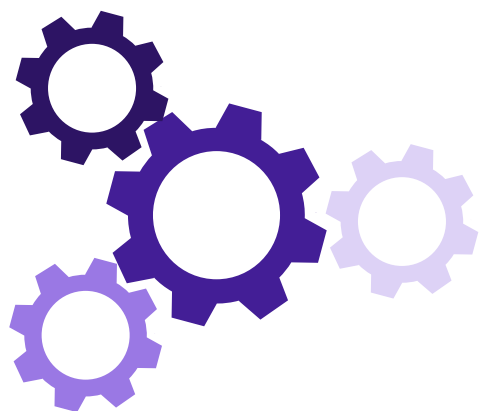


8.5.1. O PLANEJAMENTO [...]

- No planejamento, é definido o escopo prévio do trabalho, para que o auditado possa preparar-se de maneira adequada. (GONÇALVES, 2018).
- Em processos transparentes de auditoria, a validade e toda forma de licenciamento são explícitas. (*ibidem*).
- Nessa etapa, identifica-se o objetivo referente a cada auditoria, opta-se por auditar o processo ou o produto e define-se a estratégia, bem como o cronograma, que deve ser conhecido pelos membros do projeto. (*ibidem*).



8.5.2. A EXECUÇÃO [...]



- Na etapa da execução, os funcionários da área de T.I (possíveis auditados indicados pelo líder da equipe) são apresentados ao auditor (ou aos auditores).
- Aqui são identificados os critérios de auditoria, assim como as *checklists* que servirão de guia durante o processo.
- Nessa etapa, o desenvolvedor executa um aplicativo que coleta as informações e as configurações existentes no servidor. O sistema auditor faz uma análise de servidores, aplicações, *softwares*, homologações, licenças, seriais, etc.
- Além disso, o auditor questiona o auditado de acordo como a *checklist*, e todas as informações são anotadas e utilizadas para identificar possíveis não conformidades.

8.5.3. OS RELATÓRIOS [...]

- Aqui o auditor apresenta toda a descrição de produtos e usuários, a comprovação de utilização, as não conformidades e as ações recomendadas. (GONÇALVES, 2018).
- Todas as informações e evidências coletadas devem estar em conformidade afim de comprovar sua autenticidade. A ideia é que a adoção de modelos de maturidades dê origem a uma infraestrutura que garanta a entrega dos serviços e/ou produtos.
- Exemplos de *frameworks* (modelos): ISO¹, IEEE², COBIT e ITIL. (GONÇALVES, 2018).
- E para finalizar, o auditor afere, por meio de análise norteadas por *checklist*, a conformidade ou não do que foi realizado com o padrão devido.



1. *International Organization for Standardization.*

2. *Institute of Electrical and Electronics Engineers.*

8.5.4. FIQUE ATENTO!



- Para cada não conformidade, o auditor deve apresentar uma ação de correção, contendo data de conclusão e responsável. (GONÇALVES, 2018).
- Também tornar-se necessária a identificação de oportunidades de melhorias e boas práticas, e sugerir para as organizações auditadas. (*ibidem*).
- As não conformidades devem ser acompanhadas até o encerramento. Caso as datas não sejam cumpridas, deve-se utilizar um critério que escale os prazos de acordo com cada não conformidade, até que todas sejam finalizadas. (*ibidem*).
- E atenção: Lembre-se que o relatório deve estar em um repositório com controle de versão (e.g., Git, GitHub, GitLab, etc.) e deve ser de conhecimento de todos. (*ibidem*).



9. *COMPLIANCE* EM T.I

Leis vigentes e melhores práticas [...]

9.1. INTRODUÇÃO

- Segundo a Garbos (2020), a Governança de T.I e o *Compliance* possuem funções estratégica nas organizações. E diante do cenário atual, de incertezas sobre a manutenção das atividades empresariais, a gestão das políticas de *compliance* se torna um desafio.
- Podemos definir Políticas de *Compliance* em T.I como:

Um conjunto de estratégias utilizadas por empresas para alinhar os seus processos, produtos e serviços de Tecnologia da Informação às leis, normas e códigos organizacionais vigentes. (*ibidem*).
- É importante ressaltar que a ausência de boas práticas contribuem para o aumento dos riscos corporativos. Portanto, se manter atento às legislações vigentes é fundamental para a gestão desses riscos e também para a imagem empresarial. (GARBOS, 2020).

9.2. AS LEGISLAÇÕES VIGENTES

9.2.1. Lei da Propriedade Intelectual (Lei 9.279/1996)

- Regula o direito de propriedade de patentes, marcas, desenhos industriais, e demais bens imateriais que uma pessoa ou empresa possa vir a adquirir ou desenvolver. (GARBO, 2020).
- Essa lei também recomenda a proteção de sites e/ou aplicativos através da elaboração e publicação do Termo de responsabilidade pelo uso de recursos da T.I, conhecido como “Termo e Condições de Uso”. Por meio desse documento é possível esclarecer e explicitar aos usuários e terceiros os tipos de condutas permitidas na utilização do site e/ou aplicativos. Além disso, registra a quem pertencem os direitos autorais dos mesmos.

- De acordo com a Garbos (2020) a ausência dessas normas e demais esclarecimentos podem causar dúvidas e ferir os direitos de usuários ou de terceiros, além de dificultar a coleta de evidências relativas à utilização dos recursos de T.I, solicitadas pela auditoria.
- A adoção do Termo de Condições e Uso, portanto, além da segurança jurídica, contribui para o aprimoramento dos processos de governança ao buscar a conformidade com os guias e modelos de mercado. (*ibidem*).



9.2.2. Lei dos Direitos Autorais (Lei 9.609/1998)

- Segundo a Garbos (2020), essa lei regula os direitos autorais, que se trata da denominação dos direitos do autor e os que lhes são conexos.
- Protege, entre outras obras, as audiovisuais, sonORIZADAS ou não, fotográficas e ilustrações. Mas, apesar de se tratar de uma norma relativamente atual, não dispõe de regras específicas para o assunto das mídias, redes sociais ou proteção dos direitos autorais na *internet*. Dessa forma, é recomendável a adoção de algumas medidas protetivas. (*ibidem*).



9.2.3. Lei do Software (Lei 9.610/1998)

- De acordo com a Garbos (2020), essa lei garante os direitos autorais e de registro da produção de *softwares*, aplicando-se às obras sob encomenda ou assalariadas, produzidas em empresas privadas ou em órgão público.
- Destaca-se a nova Lei dos Direitos Autorais (nº 10.695/2003), também conhecida como Lei Anti-Pirataria, amplia a punição para quem violar os direitos autorais. (GARBOS, 2020).
- Portanto, em caso de ausência de licenciamento, e.g., a empresa terá como consequência não somente o pagamento de multas, mas também irá responder criminalmente pelo ato. As falhas no gerenciamento de licenças de *softwares* são bastante comuns e causam grandes prejuízos à organização. (*ibidem*).

- Dentre as recomendações de boas práticas, citamos:



Figura 14. Boas práticas sugeridas pela adoção da Lei do *Software*. (GARBOS, 2020 *adaptado* CAIXETA, 2021).

- Já sobre os benefícios, temos:

BENEFÍCIOS

- ✓ Minimização dos problemas com auditorias.
- ✓ Redução dos custos.
- ✓ Acompanhamento do uso.
- ✓ Minimização de problemas com segurança e desempenho.
- ✓ Aumento da produtividade do pessoal de T.I.

(GARBOS, 2020).

9.2.4. Lei das Provas Eletrônicas (Lei 12.850/2013)

- Dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal. E aborda algumas providências sobre o acesso a Registros, Dados cadastrais, Documentos e Informações. (GARBOS, 2020).
- É importante ressaltar que, com a popularização da *internet* e dos meios eletrônicos, tornou-se necessário estabelecer algumas premissas no que tange aos meios de comprovação dos fatos veiculados eletronicamente. (*ibidem*).
- Define-se Prova eletrônica como um ato de evidenciar determinado fato através de meios eletrônicos. [...]. Portanto, só terá validade de prova o documento eletrônico assinado digitalmente, com a criptografia adequada.

- Dessa forma, é recomendável a adoção da Certificação Digital como medida de boas práticas a fim de garantir a segurança e a idoneidade das provas a serem produzidas na empresa. (GARBOS, 2020).
- Os tipos de certificações podem ser:
 - ✓ Assinatura eletrônica simples.
 - ✓ Assinatura eletrônica qualificada.
 - ✓ Certificado qualificado para selos eletrônicos.
 - ✓ Biometria.



9.2.5. Marco Civil da Internet (Lei 12.965/2014)

- O Marco Civil da Internet trouxe novas regras para o uso da *internet* no Brasil, em relação aos princípios, normas, garantias, direitos e deveres de seus usuários. [...]. Trouxe também garantias gerais satisfatórias para a privacidade. (GARBOS, 2020).
- O Princípio da neutralidade da rede assegura a inviolabilidade e o sigilo da troca de informações entre os usuários. (*ibidem*).
- O artigo 7º merece destaque por assegurar, entre outros, o direito à “informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais”. (*ibidem*).



- A Lei, portanto, foi considerada o marco legal da proteção de dados pessoais no Brasil. E apesar de não garantir a sua proteção de forma abrangente, completa e estruturada, ela teve como uma de suas principais premissas a questão do direito à privacidade, baseada no consentimento e no uso legítimo dos dados pessoais. (GARBOS, 2020).
- Destacamos alguns pontos de atenção, passíveis de auditoria, que são suportados pelo ITIL – guia de boas práticas para infraestrutura, operação e gerenciamento de serviços de tecnologia da informação (ITSM). (*ibidem*).



9.2.6. Lei do Home Office (Lei 13.467/2017)

- Conhecida como Reforma Trabalhista, trouxe uma série de regras previstas na Consolidação das Leis do Trabalho (CLT). Porém, a Medida Provisória 927/2020 promoveu flexibilizações de algumas dessas regras devido à pandemia do novo coronavírus (Covid-19), como o fornecimento de equipamento e ferramentas para viabilizar o teletrabalho. (GARBOS, 2020).
- É importante ressaltar que, mesmo no *home office*, os funcionários permanecem sujeitos ao cumprimento de suas obrigações de confidencialidade em relação às informações obtidas durante o trabalho, responsabilizando-se por não permitir que terceiros tenham acesso a essas informações. (*ibidem*).
- Portanto, ao fornecer os equipamentos necessários para a execução do trabalho a empresa também deve reiterar as orientações relativas à proteção e privacidade de seus dados. (*ibidem*).

- Na família ISO/IEC 27.000, guia de boas práticas em Segurança da Informação, existe uma série de recomendações de controles, inclusive sobre a estrutura adequada de gerenciamento para iniciar e controlar a implementação da segurança da informação na organização. (GARBOS, 2020).

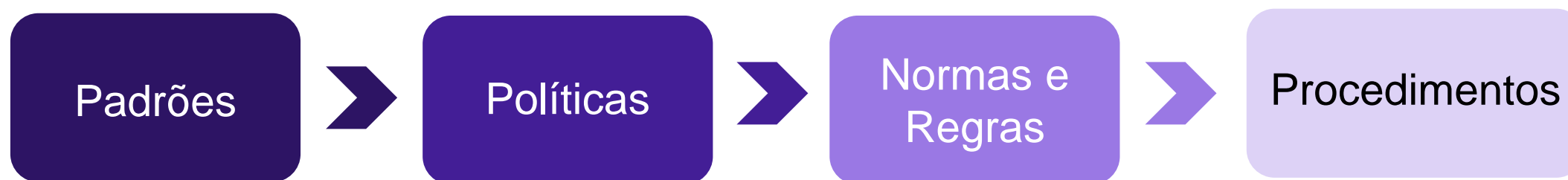


Figura 15. Boas práticas sugeridas pela ISO/IEC 27.000 para a Segurança da Informação. (GARBOS, 2020 modificado CAIXETA, 2021).



Figura 16. Dicas de proteção e privacidade em trabalho *home office*. (GARBOS, 2020).

9.2.7. Lei Geral de Proteção de Dados Pessoais - LGPD (Lei 13.709/2018)

- A LGPD trouxe um novo conjunto de regras com a intenção de garantir ao titular mais privacidade e maior controle sobre seus dados, afim de evitar o mal-uso por parte de terceiros.
- A área de T.I, em especial, completa o planejamento e a implementação das alterações necessárias relacionadas à Segurança da Informação a fim de que a empresa se mantenha em *compliance*.





Figura 17. O que muda com a LGPD. (Disponível em: <https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd>).



OBRIGADO!

Políticas e Qualidade em T.I & Gestão do Conhecimento

REFERÊNCIAS

FERNANDES, A. A., ABREU, V. F., Implantando a Governança de TI das Estratégias à Gestão de Processos e Serviços. 3ª edição. BRASPORT Livros e Multimídias Ltda. R.J., 2012.

LAUDON, Kenneth C., LAUDON, Jane P. Sistemas de Informações Gerenciais. 11ª ed. Pearson, 2014.

GARBOS8 – Governança, Riscos e Compliance. Compliance em T.I: Leis vigentes e melhores práticas. Disponível em: <https://www.garbos8.com.br/compliance-ti-leis/>. Acessado em: 14.mai.22.

SERPRO – O que muda com a LGPD. Disponível em: <https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd>. Acessado em: 15.mai.22.