COMPLIANCE

Autor: Leonardo Costa Passos

Data: junho 2023

Resumo com o que há de mais importante da disciplina de COMPLIANCE para provas de Concursos Públicos com foco em questões reais de bancas variadas.

Se o conteúdo for útil na sua jornada de estudos, você pode me agradecer fazendo um PIX de um valor que considere justo para a seguinte chave:

leonardx@gmail.com

Table of Contents

1) GESTÃO DE RISCOS

- refere-se ao processo de aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, avaliação, tratamento, monitoramento e análise crítica dos riscos.

- contínua avaliação da eficácia dos controles internos implantados na organização para mitigar os riscos relevantes.

2) COMPLIANCE

- O Compliance executa suas atividades de forma rotineira e permanente, sendo responsável por monitorar e assegurar de maneira corporativa e tempestiva que as diversas unidades da Instituição estejam respeitando as regras aplicáveis a cada negócio, por meio do cumprimento das normas, dos processos internos, da prevenção e do controle de riscos envolvidos em cada atividade.

- Os benefícios decorrentes da implantação de controles antifraude e anticorrupção devem ser maiores que os seus custos.

- Para uma relação custo-benefício mais vantajosa na aplicação de controles, a organização deve focalizar a sua atuação nas áreas de maior risco e naquelas em que os esforços tenham os maiores impactos.

- Toda organização é suscetível à ocorrência de fraude e corrupção e deve avaliar a abrangência e a profundidade da implementação de controles considerando os seus riscos, o seu tamanho, a sua natureza e a sua complexidade.

- É sempre possível ter controles para combater a fraude e a corrupção, mas esses controles devem permitir que as organizações entreguem seus resultados aos cidadãos honestos no menor tempo e custo possíveis.

- significa estar em conformidade com as leis, os regulamentos internos e externos e os princípios corporativos que garantem as melhores práticas do mercado.

- atuação conforme as normas e regras fixadas, tendo como escopo evitar fraudes, ilícitos e desvios de conduta.

- A auditoria que tem como foco a verificação do cumprimento das normas aplicáveis à entidade e os seus regulamentos

- Objetiva verificar o cumprimento das normas e procedimentos implantados pela companhia ou pelos órgãos reguladores de determinadas atividades.

- referem-se ao cumprimento de regras pré-estabelecidas (normas, leis, regras de controles internos e externos, além de todas as políticas e diretrizes estabelecidas para o seu negócio).

- monitorar, de maneira corporativa e tempestiva, as diversas unidades da instituição, assegurando-se de que respeitam as regras aplicáveis a cada negócio, por meio do cumprimento das normas, dos processos internos, da prevenção e do controle de riscos.

- função principal o monitoramento das unidades da instituição para garantir o cumprimento das normas e processos internos, além de trabalhar na prevenção e controle de riscos.

- A adoção pelas corporações de um código de ética para seus principais executivos, contendo formas de encaminhamento de questões relacionadas a conflitos de interesse, divulgação de informações e cumprimento das leis e regulamentos

3) Gerenciamento de Crises

O gerenciamento de crises é um processo estratégico que visa proteger a organização e seus stakeholders de eventos que possam ameaçar a reputação, a integridade operacional ou a viabilidade da organização. Envolve a identificação de potenciais crises, o desenvolvimento de planos de resposta, a coordenação de comunicações durante a crise e a implementação de medidas para mitigar os danos e facilitar a recuperação. As crises podem incluir eventos de origem natural, como desastres naturais, ou eventos causados pelo homem, como erros de gestão, falhas de tecnologia, ou escândalos financeiros ou de ética.

O gerenciamento eficaz de crises pode ser dividido em três fases principais:

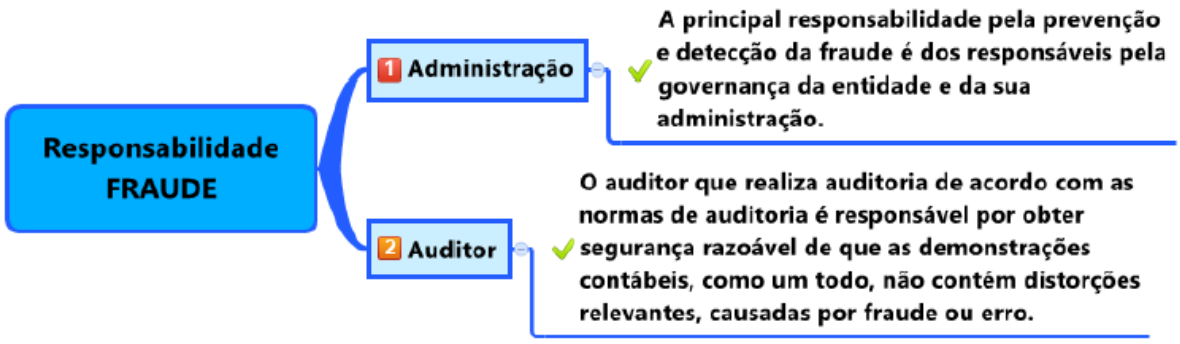
- Preparação: Isso inclui a identificação de riscos e ameaças potenciais, a preparação de planos de contingência, a formação de uma equipe de gerenciamento de crises e a realização de exercícios de treinamento.

- Resposta: Isso envolve a ativação do plano de gerenciamento de crises, a comunicação eficaz com todos os stakeholders e a coordenação das ações necessárias para mitigar os impactos da crise.

- Recuperação: Isso envolve a avaliação dos danos, a implementação de medidas de recuperação e a revisão e atualização do plano de gerenciamento de crises com base nas lições aprendidas.

4) Agentes de Governança

Os agentes de governança são indivíduos ou grupos que têm um papel na governança de uma organização. Eles podem ser internos ou externos à organização e têm responsabilidades que contribuem para o funcionamento eficaz do sistema de governança. Os agentes de governança podem incluir:



- Conselho de Administração: O conselho de administração tem a responsabilidade geral pela governança da organização. Eles estabelecem a direção estratégica, supervisionam a gestão e garantem a prestação de contas.

- A principal responsabilidade pela prevenção e detecção da fraude é dos responsáveis pela governança da entidade e da sua administração. Não do auditor.

- Alta Administração: A alta administração, geralmente liderada pelo CEO, é responsável pela implementação da estratégia estabelecida pelo conselho e pela gestão diária da organização.

- Auditores: Os auditores, tanto internos quanto externos, fornecem uma verificação independente da conformidade da organização com as leis, regulamentos e práticas de governança.

    - O auditor é responsável por obter segurança razoável de que as demonstrações contábeis, como um todo, não contêm distorções relevantes, causadas por fraude ou erro.

    - O auditor está preocupado com a fraude que causa distorção relevante nas demonstrações contábeis.

    - Dois tipos de distorções intencionais são pertinentes para o auditor – distorções decorrentes de informações contábeis fraudulentas e da apropriação indébita de ativos.

- Stakeholders: Os stakeholders, incluindo funcionários, clientes, fornecedores, a comunidade e os acionistas, têm um interesse na governança da organização e podem influenciar suas práticas de governança.

- Órgãos Reguladores: Os órgãos reguladores têm a responsabilidade de estabelecer e aplicar as regras e regulamentos que governam a conduta das organizações.

Cada um desses agentes desempenha um papel importante na criação de um sistema de governança eficaz, que promove a transparência, a responsabilidade e a integridade.

5) LEI SARBANES-OXLEY (SOX)

promulgada em 30 de julho de 2002 nos Estados Unidos, é uma legislação que visa melhorar a governança corporativa e a transparência nas empresas de capital aberto. Essa lei surgiu como resposta aos escândalos financeiros envolvendo grandes corporações, como Enron e WorldCom, que impactaram a confiança do mercado e dos investidores.

A SOX estabelece um conjunto de regras e regulamentações que abordam questões como auditoria, responsabilidade de executivos, conflitos de interesses e relatórios financeiros. As principais disposições da lei incluem:

- Compliance (Conformidade Legal): A SOX estabelece padrões rigorosos para garantir que as empresas de capital aberto sigam as leis e regulamentações aplicáveis. Isso inclui a implementação de controles internos efetivos e políticas de conformidade para assegurar a adesão às normas legais e regulatórias.

- Accountability (Prestação Responsável de Contas): A lei responsabiliza os executivos de alto escalão pela exatidão dos relatórios financeiros e pelo

cumprimento das normas estabelecidas. Isso incentiva uma cultura de responsabilidade e transparência nas organizações.

- Disclosure (Transparência): A SOX visa promover a transparência nas informações financeiras e operacionais das empresas, garantindo que sejam divulgadas de forma clara, precisa e tempestiva. Isso permite que os investidores, reguladores e outras partes interessadas tenham acesso a informações relevantes e precisas para tomar decisões informadas.

- Fairness (Senso de Justiça): A SOX busca garantir um tratamento justo a todos os acionistas e partes interessadas, fortalecendo a confiança na governança corporativa e na integridade das empresas. Isso inclui a independência dos auditores externos, a responsabilidade dos executivos e a garantia de que as práticas comerciais sejam éticas e justas.

6) CONTROLE INTERNO CORPORATIVO

conjunto de políticas, procedimentos e práticas implementadas para garantir a eficiência operacional, a precisão das informações financeiras e a conformidade com leis e regulamentos aplicáveis. Ele ajuda a prevenir fraudes, reduzir erros e proteger os ativos da empresa. Os controles internos são fundamentais para a governança corporativa e a gestão de riscos.

- PRESENÇA:
  - A presença se refere à determinação da existência dos componentes e princípios relacionados no desenho e na implementação do sistema de controle interno
  - se refere à existência e à implementação de políticas, procedimentos e estruturas de controle que estão em vigor para garantir o alcance dos objetivos da corporação. Isso envolve a definição clara de responsabilidades, a segregação de funções e a implementação de medidas de segurança física e lógica.

- FUNCIONAMENTO:
  - O funcionamento refere-se à determinação de que os componentes e princípios relacionados continuem a existir na operação e na condução do sistema de controle interno para atingir objetivos especificados
  - diz respeito à eficácia e eficiência dos processos e práticas implementadas. Os controles devem funcionar conforme o esperado, reduzindo riscos e garantindo que os objetivos da corporação sejam alcançados. A avaliação do funcionamento dos controles pode envolver auditorias internas e testes para verificar se os controles estão funcionando corretamente e conforme o planejado.

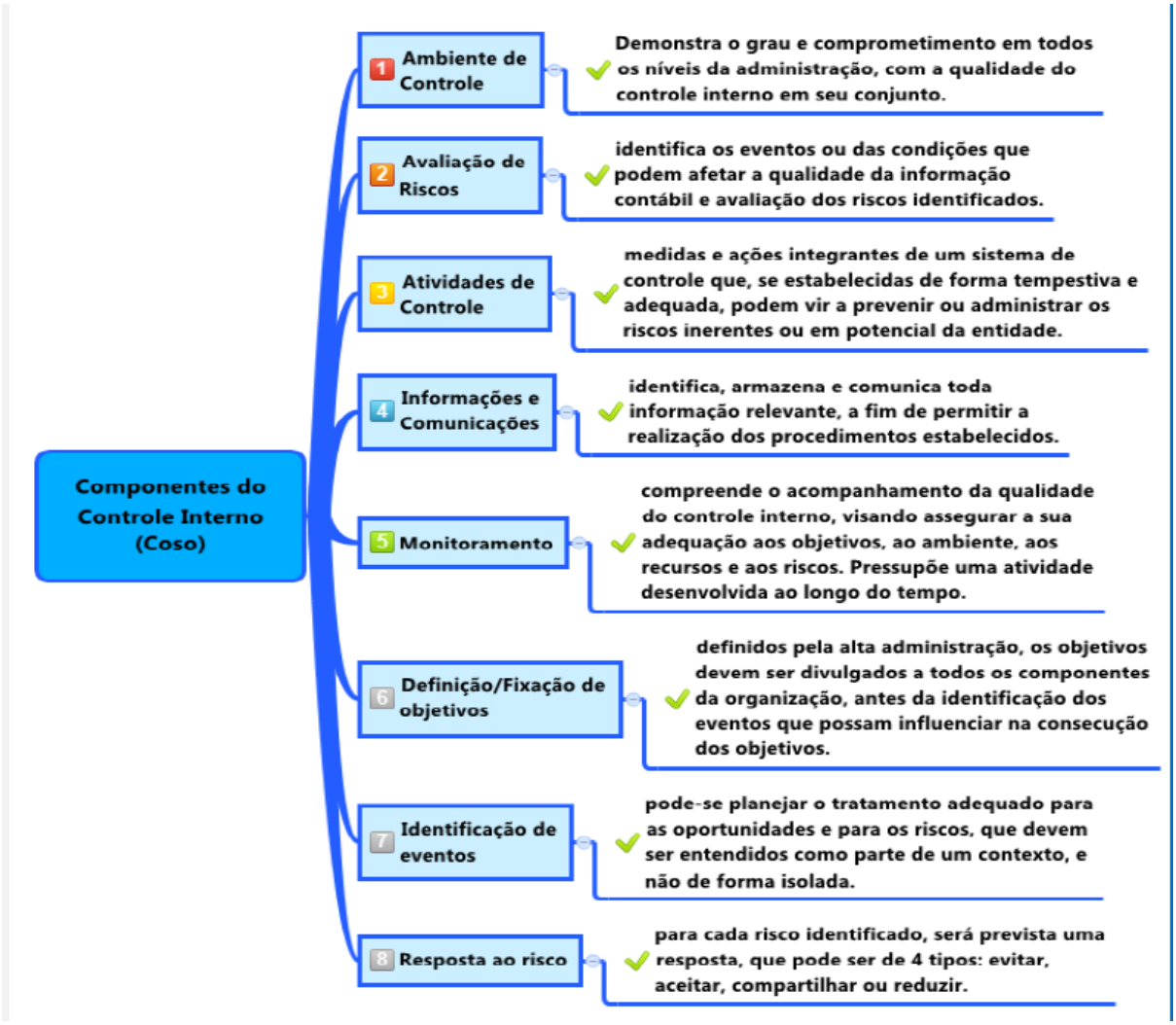
- MONITORAMENTO:
  - O monitoramento é o processo que avalia a eficácia dos componentes do sistema de controle interno
  - componente essencial do controle interno, que garante a continuidade e a eficácia dos controles implementados. Envolve a revisão contínua dos controles internos, a identificação de deficiências e a implementação de correções necessárias. O

monitoramento pode incluir a análise de indicadores de desempenho, a realização de auditorias internas e externas e a revisão de relatórios gerenciais.

- ABRANGÊNCIA:
    - A abrangência se refere à extensão e alcance do sistema de controle interno em relação aos objetivos da entidade
    - se refere ao alcance e à extensão dos controles implementados na corporação. Os controles internos devem ser aplicados a todas as áreas, processos e atividades relevantes para garantir a eficácia e a eficiência operacional, a precisão das informações financeiras e a conformidade com leis e regulamentos aplicáveis.
- ESTRUTURA:
    - A estrutura se refere à organização e disposição dos componentes e princípios relacionados ao sistema de controle interno,
    - engloba o conjunto de políticas, procedimentos e práticas estabelecidas para garantir o controle efetivo da corporação. Isso inclui a definição de responsabilidades, a segregação de funções, a implementação de medidas de segurança, a documentação de processos e a comunicação clara das expectativas e responsabilidades dos funcionários. A estrutura do controle interno deve ser adaptada às necessidades e características específicas da corporação e deve ser continuamente revisada e atualizada para garantir sua eficácia e relevância.

7) COSO (Committee of Sponsoring Organizations of the Treadway Commission)

é uma iniciativa conjunta de cinco organizações profissionais voltadas para a promoção da governança corporativa, controle interno e gerenciamento de riscos. Criado em 1985 nos Estados Unidos, o COSO tem como objetivo desenvolver e disseminar diretrizes e estruturas que ajudem as empresas a melhorar o gerenciamento de riscos e a governança corporativa.



7.1. COSO 2013

Essa estrutura é composta por cinco componentes e 17 PRINCÍPIOS inter-relacionados e visam fornecer uma base sólida para a implementação de um sistema eficaz de controle interno nas organizações.

1) AMBIENTE DE CONTROLE: O ambiente de controle é o componente que estabelece a base para o sistema de controle interno, incluindo aspectos como a integridade e valores éticos, a filosofia de gestão e estilo operacional, e a atribuição de responsabilidades e autoridade dentro da organização.

1. A organização demonstra ter comprometimento com a integridade e os valores éticos.

2.A estrutura de governança demonstra independência em relação aos seus executivos e supervisiona o desenvolvimento e o desempenho do controle interno.

3. A administração estabelece, com a suspensão da estrutura de governança, as estruturas, os níveis de subordinação e as autoridades e responsabilidades adequadas na busca dos objetivos.

4. A organização demonstra comprometimento para atrair, desenvolver e reter talentos competentes, em linha com seus objetivos.

5. A organização faz com que as pessoas assumam responsabilidade por suas funções de controle interno na busca pelos objetivos.

2) AVALIAÇÃO DE RISCOS:

6. A organização especifica os objetivos com clareza suficiente, a fim de permitir a identificação e a avaliação dos riscos associados aos objetivos.

7. A organização identifica os riscos à realização de seus objetivos por toda a entidade e analisa os riscos como uma base para determinar a forma como devem ser gerenciados.

8. A organização considera o potencial para fraude na avaliação dos riscos à realização dos objetivos.

9. A organização identifica e avalia as mudanças que poderiam afetar, de forma significativa, o sistema de controle interno.

3) ATIVIDADE DE CONTROLE: Atividades de controle são ações que ajudam a garantir que as ações gerenciais necessárias sejam tomadas para lidar com os riscos identificados

10. A organização seleciona e desenvolve atividades de controle que contribuem para a redução, a níveis aceitáveis, dos riscos à realização dos objetivos.

11. A organização seleciona e desenvolve atividades gerais de controle sobre a tecnologia para apoiar a realização dos objetivos.

12. A organização estabelece atividades de controle por meio de políticas que estabelecem o que é esperado e os procedimentos que colocam em prática essas políticas.

4) INFORMAÇÃO e COMUNICAÇÃO: Informação e comunicação é o componente que trata da identificação, captura e comunicação de informações relevantes

13. A organização obtém ou gera e utiliza informações significativas e de qualidade para apoiar o funcionamento do controle interno.

14. A organização transmite internamente as informações necessárias para apoiar o funcionamento do controle interno, inclusive os objetivos e responsabilidades pelo controle.

15. A organização comunica-se com os públicos externos sobre assuntos que afetam o funcionamento do controle interno.

5) ATIVIDADES de MONITORAMENTO: processo de avaliação contínua e/ou independente do funcionamento dos componentes do controle interno

16. A organização seleciona, desenvolve e realiza avaliações contínuas e/ou independentes para se certificar da presença e do funcionamento dos componentes do controle interno.

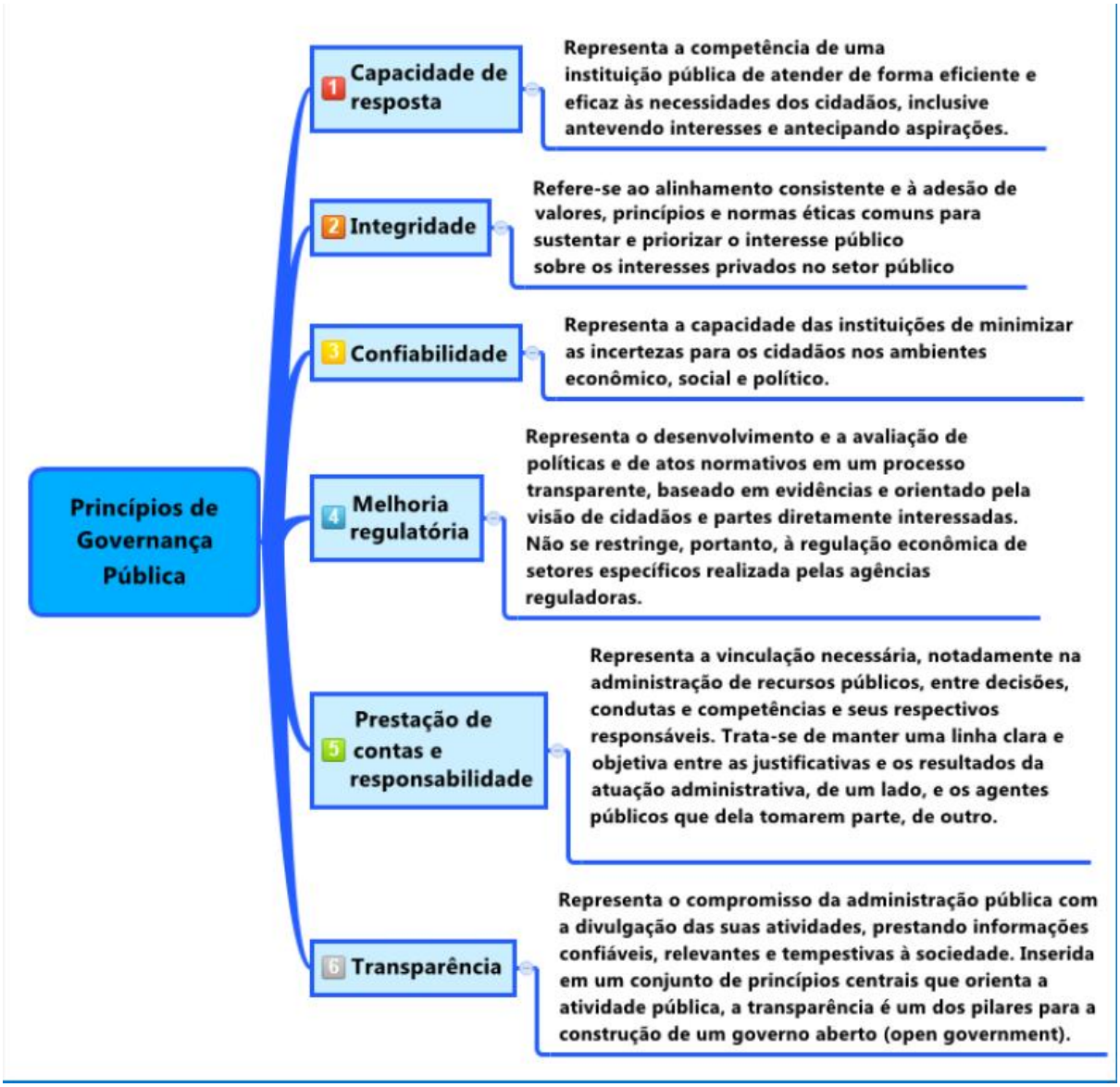
17. A organização avalia e comunica deficiências no controle interno em tempo hábil aos responsáveis por tomar ações corretivas, inclusive a estrutura de governança e alta administração, conforme aplicável. [grifo nosso]

A governança no setor público pode ser analisada sob quatro perspectivas de observação:

- Sociedade e Estado
- Entes federativos, esferas de poder e políticas públicas
- Órgãos e entidades
- Atividades intraorganizacionais.

Instâncias do Sistema de Governança do Setor Público:

- Instâncias externas de governança: fiscalização, controle e regulação. Ex: Congresso Nacional e Tribunais de Contas.
- Instâncias externas de opoio à governança: avaliação, auditoria e monitoramento independente. Ex: auditorias independentes e o controle social organizado.
- Instâncias internas de governança: avaliar a estratégia e as políticas, bem como monitorar a conformidade e o desempenho destas. Ex: conselhos de administração ou equivalentes e, na falta desses, a alta administração.
- Instâncias internas de opoio à governança: realizam a comunicação entre partes interessadas internas e externas à administração, bem como auditorias internas . Ex: a ouvidoria, a auditoria interna, o conselho fiscal, as comissões e os comitês.



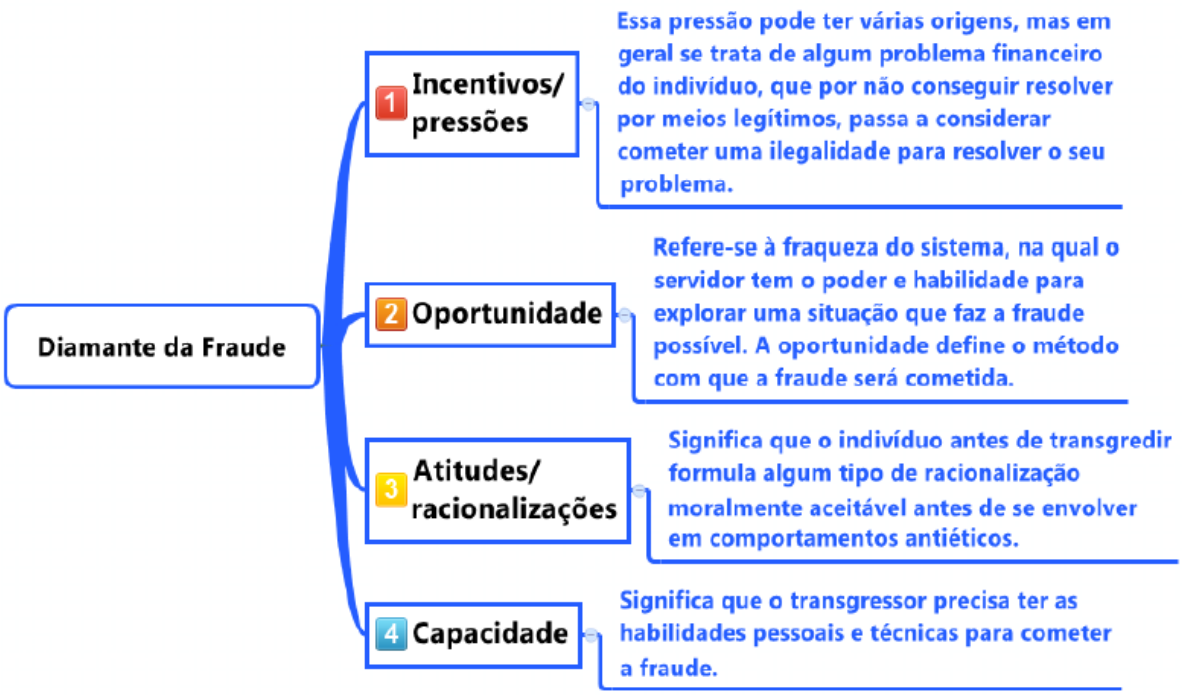
8) GESTÃO DE RISCOS NO SETOR PÚBLICO.

- FRAUDE: ato intencional praticado por um ou mais indivíduos entre gestores, responsáveis pela governança, empregados ou terceiros, envolvendo o uso de falsidade para obter uma vantagem injusta ou ilegal; A intenção é um elemento importante para diferenciar a fraude do erro.

- CORRUPÇÃO: se apresenta de duas formas: corrupção ativa e corrupção passiva, que respectivamente e suscintamente significam oferecer ou solicitar alguma vantagem indevida.

- TEORIA DO TRIÂNGULO DA FRAUDE: para uma fraude ocorrer, é necessária a ocorrência de três fatores: pressão, oportunidade e racionalização.

- DIAMANTE DA FRAUDE: Nesse modelo a nova aresta é a capacidade. Isso significa que para a fraude ocorrer, além dos fatores do triângulo da fraude, o transgressor precisa ter as habilidades pessoais e técnicas para cometer a fraude.



- CUSTO BENEFÍCIO NA APLICAÇÃO DE CONTROLES PARA COMBATER A FRAUDE E CORRUPÇÃO: investir em um controle preventivo e detectivo para suas áreas de alto risco inerente e onde os esforços tenham os maiores impactos.

    - Toda organização é suscetível à ocorrência de fraude e corrupção e deve avaliar a abrangência e a profundidade da implementação de controles considerando os seus riscos, o seu tamanho, a sua natureza e a sua complexidade.

    - O benefício decorrente da implementação de controles antifraude e anticorrupção deve ser maior que o seu custo.

    - É sempre possível ter controles para combater a fraude e a corrupção, mas esses
    - controles devem permitir que as organizações entreguem seus resultados aos cidadãos honestos no menor tempo e custo possíveis.

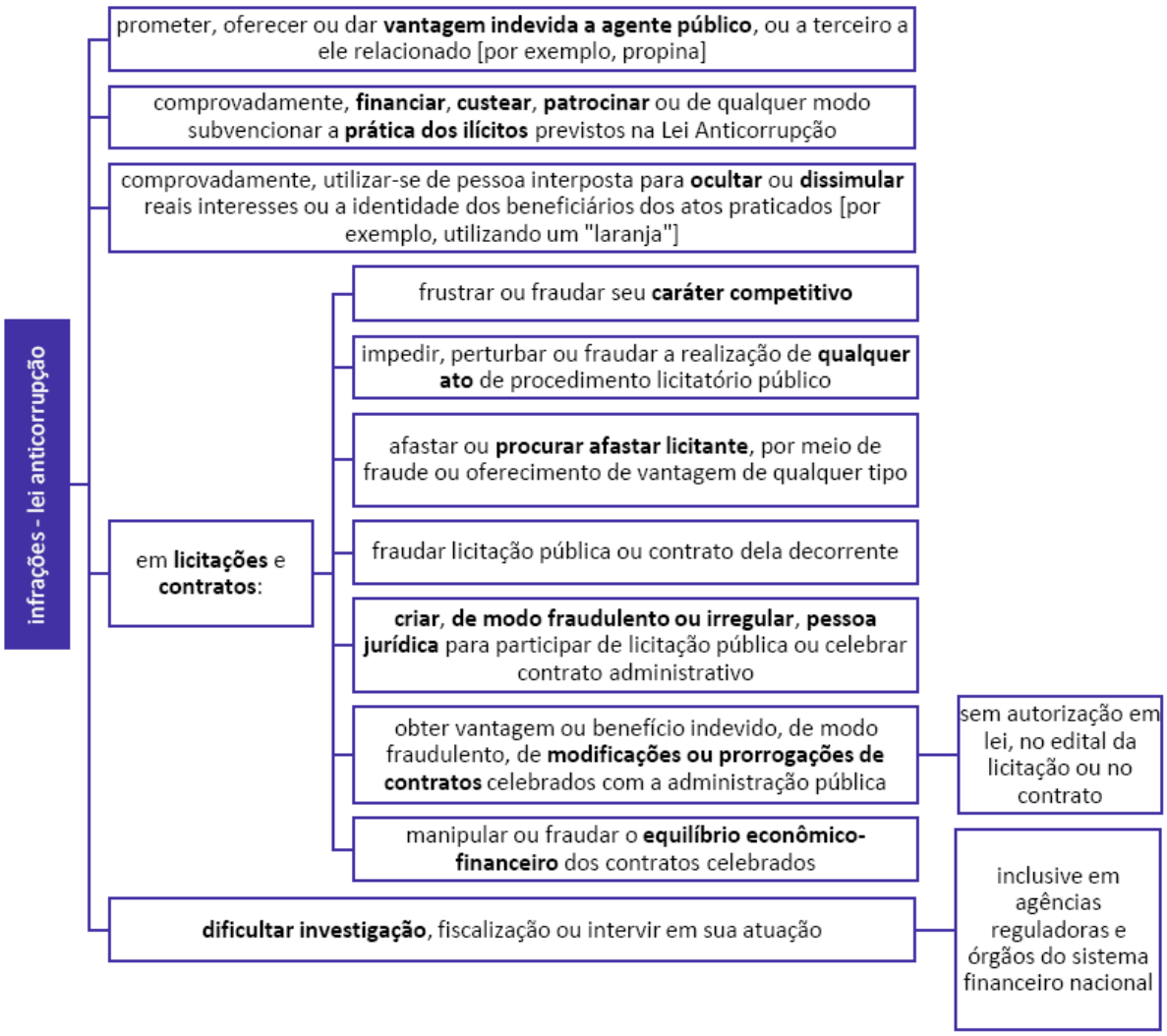
8.1 Três Linhas de Defesa

9) LEI ANTICORRUPÇÃO (12.846/2013)

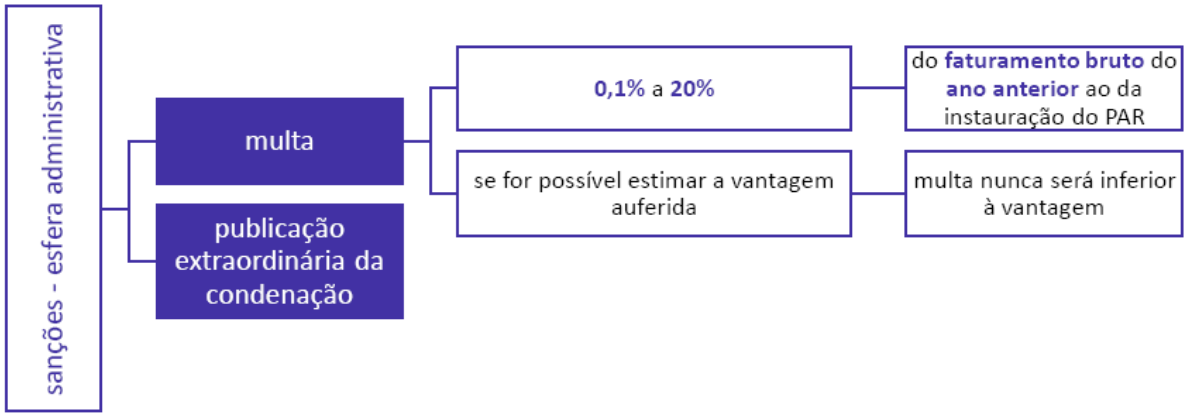
- a grande inovação da Lei Anticorrupção foi prever a responsabilidade objetiva de pessoas jurídicas, viabilizando a aplicação de sanções a pessoas jurídicas sem comprovação de culpa e a pessoas físicas quando houver dolo ou culpa.

- se uma empresa estrangeira com filial no Brasil, por exemplo, pratica um ato de corrupção previsto na Lei contra um órgão público brasileiro, tal empresa estará sujeita às sanções da Lei Anticorrupção.

- se uma empresa brasileira pratica ato lesivo contra um órgão público americano, por exemplo, tal empresa estará sujeita às sanções da Lei Anticorrupção, ainda que o dano não tenha sido causado ao Brasil.



9.1. RESPONSABILIZAÇÃO ADMINISTRATIVA



- A aplicação da multa administrativa não dispensa a devolução dos recursos relacionados ao dano causado (em hipótese alguma) e, como veremos adiante, também não afasta a responsabilização judicial.

10) Código de Ética e Conduta - AGERIO

O Código de Ética e Conduta da AgeRio tem como objetivo direcionar e orientar os membros da Alta Administração, do Conselho Fiscal e do Comitê de Auditoria, os empregados, prepostos, estagiários, prestadores de serviço e demais colaboradores da Agência, pautando suas ações e comportamentos conforme os valores e normas da empresa.

O comprometimento com o respeito e a disseminação dos valores e normas descritos neste Código é responsabilidade de cada empregado e colaborador da Agência.

Todos os empregados e colaboradores devem, anualmente, renovar seu compromisso com o Código de Ética e Conduta da AgeRio, por meio da assinatura de Termo de Ciência.

Ocorrerá, anualmente, a disseminação dos valores da conduta ética e dos preceitos estabelecidos no Código de Ética e Conduta direcionada a todos os empregados, colaboradores e administradores da empresa.

O comprometimento com os valores e preceitos éticos da AgeRio é fundamental para a construção de reputação, imagem e valor para corpo funcional e empresa

10.1) Missão e valores:

A AgeRio tem como missão fomentar, por meio de soluções financeiras, o desenvolvimento sustentável do Estado do Rio de Janeiro, com excelência na prestação de serviços. A AgeRio tem como prática se pautar nos seguintes valores:

a) Aperfeiçoamento Contínuo;
b) Decisões apoiadas em Critérios Técnicos, Colegiadas e com Conformidade;
c) Foco no Cliente;

d) Integridade;
e) Respeito à Diversidade;
f) Responsabilidade Socioambiental.

10.2) Princípios de Ética e Normas de Conduta Profissional

- Legalidade, justiça, transparência:
- Prevalência do interesse público:
- Lealdade, dignidade, discrição, cooperação:
- Respeito, honestidade, probidade:
- Responsabilidade, eficiência, impessoalidade:
- Assiduidade, pontualidade:
- Cortesia, presteza e tempestividade:

10.3) Denúncias, Processo de Apuração de Responsabilidades e Penalidade

- A AgeRio possui Comitê de Ética instituído, que é o órgão responsável por examinar eventuais questões referentes a este Código, sua aplicação e atualizações com base nos procedimentos definidos em seu Regimento Interno;

- Os procedimentos de apuração de denúncia de falta de ética terão a chancela de "reservado", sendo preservada a identidade do denunciante durante todo o processo.

- Em caso de descumprimento do Código de Ética ou da legislação vigente, o denunciado estará sujeito a penalidades definidas nos normativos vigentes da AgeRio e poderá ser responsabilizado em esfera administrativa e judicial;

- Quando configurada falta de ética, considerando a gravidade da conduta, o denunciado poderá sofrer, alternada ou conjuntamente, as seguintes penalidades:

    - a) Aplicação da pena de censura ética;
    - b) Abertura de processo administrativo para apuração de fato irregular;
    - c) Devolução do empregado ao órgão ou empresa de origem;
    - d) Exoneração do cargo em comissão ou destituição da função de confiança, ou ainda, demissão do empregado;
    - e) Encaminhamento de cópia dos autos à autoridade competente para a respectiva apuração, quando configurada a ocorrência de infração administrativa, ilícitos penais ou civis, infração disciplinar ou improbidade administrativa.

- Os empregados da AgeRio também podem se valer do Canal de Denúncias "Disque Rio Contra a Corrupção", da Controladoria Geral do Estado (CGE).

11) A Resolução CMN nº 4.859/2020

emitida pelo Conselho Monetário Nacional do Brasil (CMN), estabelece regras para a implementação da governança de tecnologia da informação (TI) e segurança da informação nas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

As principais disposições dessa resolução incluem:

- Estrutura de governança de TI: As instituições devem implementar uma estrutura de governança de TI que seja compatível com a natureza, o porte, a complexidade, a estrutura e o modelo de negócio da instituição e com a complexidade dos serviços e produtos oferecidos. A estrutura de governança de TI deve estar alinhada à estratégia da instituição e incluir políticas e procedimentos claros para a gestão de TI.

- Gestão de riscos de TI: As instituições devem adotar práticas de gestão de riscos de TI, incluindo a identificação e avaliação dos riscos, a implementação de controles e a monitoração dos riscos. A gestão de riscos de TI deve ser integrada à gestão de riscos corporativos da instituição.

- Segurança da informação: As instituições devem implementar políticas e procedimentos de segurança da informação que visem garantir a confidencialidade, a integridade e a disponibilidade das informações. As políticas de segurança da informação devem incluir medidas para prevenir, detectar e responder a incidentes de segurança.

- Continuidade de negócios: As instituições devem ter um plano de continuidade de negócios que vise garantir a continuidade dos serviços de TI em caso de interrupções. O plano de continuidade de negócios deve ser testado regularmente.

- Outsourcing de TI: Quando os serviços de TI são terceirizados, as instituições devem garantir que os prestadores de serviços cumprem os requisitos de governança de TI e segurança da informação.

- Relatórios: As instituições devem fornecer relatórios periódicos à alta administração e ao conselho de administração sobre a implementação da governança de TI e a gestão de riscos de TI.

12)A Resolução CMN nº 4.595 de 28 de agosto de 2017

emitida pelo Conselho Monetário Nacional do Brasil (CMN), estabelece diretrizes para a implementação e aprimoramento da estrutura de gerenciamento do risco operacional pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

O risco operacional é definido como a possibilidade de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos. Isso inclui o risco legal associado à inadequação ou deficiência de contratos firmados pela instituição, bem como a sanções em razão de descumprimento de dispositivos legais e a indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela instituição.

As principais disposições dessa resolução incluem:

- Estrutura de Gerenciamento do Risco Operacional: As instituições devem implementar uma estrutura de gerenciamento do risco operacional que seja compatível com a natureza, porte, complexidade das operações e tipo de instituição.

- Política de Gerenciamento do Risco Operacional: A política deve estabelecer a estratégia para o gerenciamento do risco operacional, definindo claramente os papéis e responsabilidades das áreas envolvidas, os procedimentos e controles internos, a segregação de funções e a capacitação dos profissionais envolvidos.

- Identificação, Avaliação, Monitoração, Controle e Mitigação do Risco Operacional: A instituição deve dispor de processos robustos para identificar, avaliar, monitorar, controlar e mitigar o risco operacional, incluindo a realização de testes de estresse.

- Sistema de Informações: A instituição deve dispor de sistema de informações gerenciais que permita identificar, medir, controlar e monitorar o risco operacional.

- Plano de Contingência: A instituição deve dispor de plano de contingência contendo as estratégias a serem adotadas para assegurar a continuidade das atividades e a limitação de perdas no caso da concretização de riscos operacionais relevantes.

- Relatório de Avaliação do Gerenciamento do Risco Operacional: A instituição deve elaborar relatório de avaliação do gerenciamento do risco operacional, o qual deve ser encaminhado à alta administração e ao conselho de administração, se houver.

A Resolução CMN nº 4.595/2017 é uma peça crucial para garantir que as instituições financeiras no Brasil possuam uma estrutura sólida para gerenciar o risco operacional, promovendo a estabilidade e a confiabilidade do sistema financeiro.

13) CONTROLES INTERNOS

são processos implementados por uma organização para fornecer garantia razoável em relação à realização de objetivos nas seguintes categorias: efetividade e eficiência das operações, confiabilidade dos relatórios financeiros e conformidade com as leis e regulamentos aplicáveis.

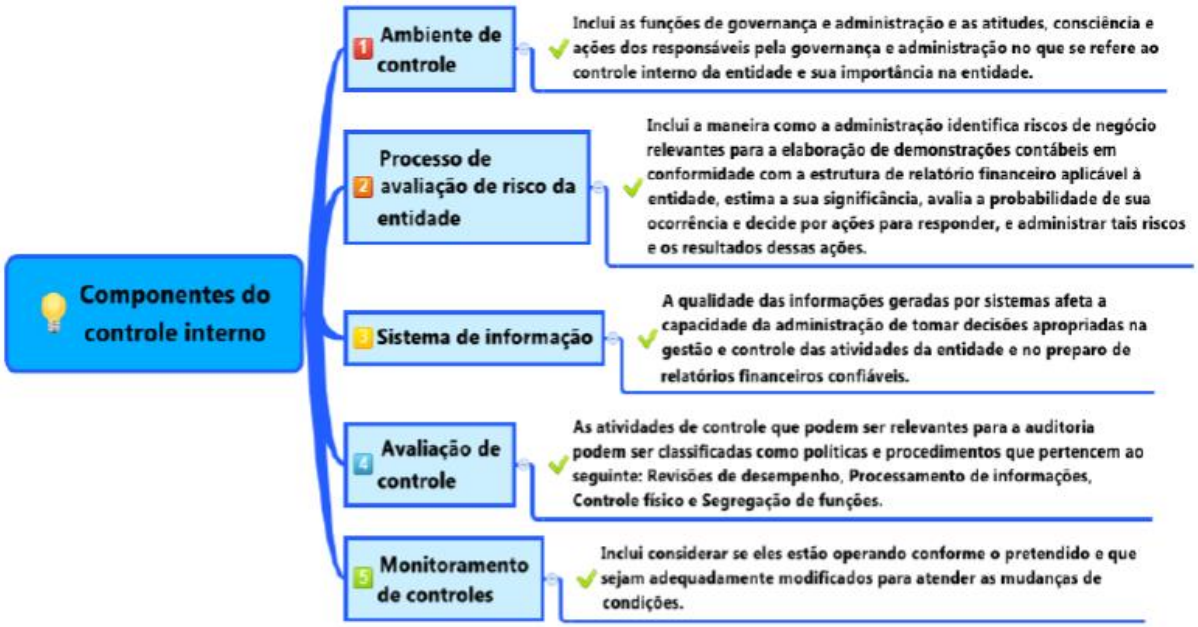
Controle interno é o processo planejado, implementado e mantido pelos responsáveis pela governança, administração e outros empregados para fornecer segurança razoável quanto à realização dos objetivos da entidade no que se refere à confiabilidade dos relatórios financeiros, efetividade e eficiência das operações e conformidade com leis e regulamentos aplicáveis...

Os controles internos são uma parte essencial da gestão de riscos e da governança corporativa, pois ajudam a evitar erros e fraudes, proteger os ativos da organização, garantir a precisão e a integridade dos dados financeiros e operacionais, promover a eficiência operacional e incentivar a adesão às políticas e procedimentos da organização.

Os controles internos podem ser divididos em duas categorias principais: controles preventivos e controles detectivos.

- Controles preventivos: São projetados para prevenir erros ou fraudes antes que eles ocorram. Exemplos incluem aprovações e autorizações (por exemplo, um gerente deve aprovar despesas acima de um determinado limite), segregação de funções (diferentes pessoas são responsáveis por diferentes partes de um processo para evitar abuso ou erros) e controles físicos sobre ativos (como cofres para dinheiro e fechaduras para equipamentos).

- Controles detectivos: São projetados para identificar erros ou fraudes que já ocorreram. Exemplos incluem reconciliações (comparando diferentes fontes de dados para identificar discrepâncias), análises de variação (comparando resultados reais com previsões ou benchmarks) e auditorias internas.



Além disso, os controles internos podem ser manuais (realizados por pessoas) ou automatizados (realizados por sistemas de TI).

Os controles internos devem ser monitorados e avaliados regularmente para garantir que estão funcionando conforme o esperado e para identificar oportunidades de melhoria. Esse processo de monitoramento e avaliação é muitas vezes uma função do sistema de controle interno de uma organização, e pode ser realizado através de atividades de autoavaliação, revisões de controle de qualidade, e auditorias internas e externas.

- o objetivo do auditor é comunicar apropriadamente, aos responsáveis pela governança e à administração, as deficiências de controle interno que o auditor identificou durante a auditoria e que, no seu julgamento profissional, são de importância suficiente para merecer a atenção deles.

- Os controles contábeis compreendem o plano de organização e todos os métodos e procedimentos utilizados para salvaguardar o patrimônio e a propriedade dos itens que o compõem. São elementos dos controles contábeis:
    - Segregação de funções: cria independência entre as funções de execução operacional, custódia dos bens patrimoniais e sua contabilização;
    - Sistema de autorização: controla as operações através de aprovações, de acordo com as responsabilidades e riscos envolvidos;
    - Sistema de registros: compreende a classificação dos dados dentro de uma estrutura formal de contas, a existência de um plano de contas que facilite o registro e preparação das demonstrações contábeis, e a utilização de um manual descritivo para o uso das contas.

Como o objetivo principal do auditor externo ou independente é emitir uma opinião sobre as demonstrações financeiras auditadas, ele deve avaliar somente os controles relacionados com estas demonstrações, ou seja, os controles contábeis. No entanto, se algum controle administrativo tiver influência nos relatórios da contabilidade, o auditor deverá considerar também a possibilidade de os avaliar.

- As deficiências de controle interno que o auditor identificou durante a auditoria e que, no seu julgamento profissional, são de importância suficiente para merecer a atenção deverão ser comunicadas apropriadamente aos responsáveis pela governança e à administração.

São exemplos de controles contábeis:

✓ Sistemas de conferência, aprovação e autorização;

✓ Segregação de funções (pessoas que têm acesso aos registros contábeis não podem custodiar ativos da empresa);

✓ Controles físicos sobre ativos;

✓ Auditoria interna.

São exemplos de controles administrativos:

✓ Análises estatísticas de lucratividade por linha de produtos;

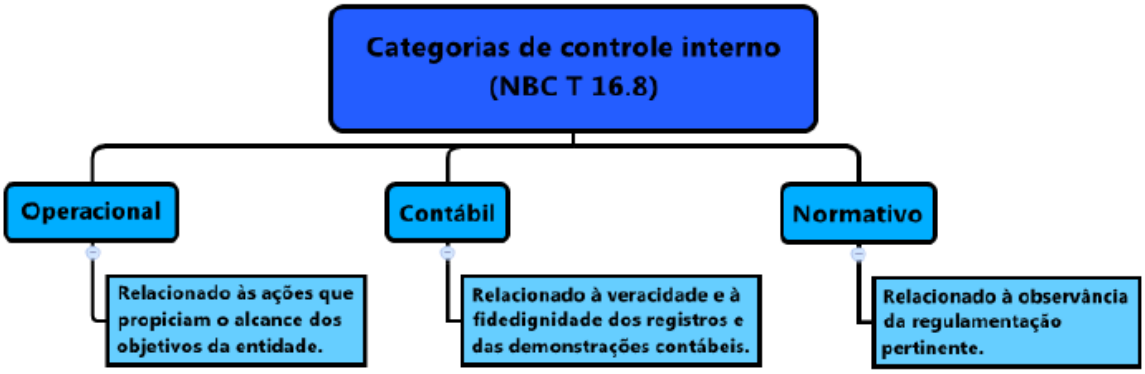
✓ Controle de qualidade;

✓ Treinamento de pessoal;

✓ Estudos de tempos e movimentos;

✓ Análise das variações entre os valores orçados e os incorridos;

✓ Controle dos componentes assumidos, mas ainda não realizados economicamente.



Em resumo, a noção de controle interno é fundamental para a gestão de qualquer organização, pois fornece um mecanismo para gerenciar riscos e aumentar a probabilidade de a organização atingir seus objetivos.

14) PROCESSO DE ANÁLISE E TOMADA DE DECISÃO

Tomar decisões é escolher entre diversas alternativas existentes, com o objetivo de resolver problemas ou aproveitar oportunidades.

Em outras palavras, a decisão sempre envolve escolher um caminho (curso de ação ou comportamento a ser seguido) entre duas ou mais alternativas (opções) diferentes.

Nesse sentido, se não existirem alternativas a serem escolhidas (ou seja, se existe apenas uma única opção disponível), não há decisões a serem tomadas.

Ao escolher uma alternativa, é importante que o gestor leve em consideração o "custo de oportunidade" daquela decisão.

O Custo de Oportunidade é uma maneira de "mensurar o custo" de determinada escolha. Em outras palavras, o Custo de Oportunidade busca indicar o "valor que se perdeu" ("valor que se deixou de ganhar") em função de se ter optado por uma alternativa ao invés de outra.

14.1 – Elementos do Processo Decisório

O processo decisório envolve 06 elementos básicos:

- Tomador de decisão: É a pessoa que faz uma escolha ou opção entre várias alternativas futuras de ação.
- Objetivos: São os objetivos que o tomador de decisão pretende alcançar com suas ações.
- Preferências: São os critérios que o tomador de decisão usa para fazer sua escolha.
- Estratégia: É o curso de ação que o tomador de decisão escolhe para atingir seus objetivos. O curso de ação é o caminho escolhido e depende dos recursos que o tomador de decisões dispõe.
- Situação: São os aspectos do ambiente que envolve o tomador de decisão e que afetam sua escolha. Alguns desses aspectos estão fora do seu controle, conhecimento ou compreensão.
- Resultado: É a consequência ou resultado de determinada estratégia.

Alguns autores ainda incluem mais um elemento (nesse caso, seriam 07 elementos):

Estado da Natureza: são as condições de incerteza, risco ou certeza que existem no ambiente de decisão que o tomador de decisão deve enfrentar

14.2 – Tipos de decisão: Decisões Programadas x Decisões não programadas

- Decisões Programadas (Decisões Programáveis / Decisões Estruturadas):
  - Tratam-se de decisões rotineiras e repetitivas, utilizadas para resolver problemas cotidianos. Ou seja, são decisões "padronizadas", utilizadas para responder a situações que ocorrem regularmente. São utilizadas para situações de certeza e previsibilidade, em que existem dados (informações) adequados e suficientes.
    - São decisões baseadas em um "acervo de soluções" da organização.
    - Esse tipo de decisão "limita" a liberdade dos indivíduos para decidirem.
- Decisões Não Programadas (Decisões Não Programáveis / Decisões Não Estruturadas):
  - Tratam-se de decisões novas e não repetitivas, utilizadas para resolver problemas não rotineiros. Ou seja, são decisões mais "complexas", utilizadas para responder a situações "excepcionais"/"extraordinárias" (que não ocorrem regularmente). São utilizadas para situações de maior risco, incerteza e imprevisibilidade, em que existem dados (informações) inadequados e insuficientes.
    - Esse tipo de decisão é mais complexa, e envolve criatividade, inovação e improvisação.
    - As decisões não programadas são utilizadas quando as respostas "padronizadas" (ou seja, as decisões programadas) não funcionam bem para o tipo de situação enfrentada.

- As decisões não programadas costumam ser "centralizadas" nos gestores da organização e predominam no nível estratégico das organizações.

14.3 Níveis de decisão: Decisões Estratégicas x Decisões Táticas x Decisões Operacionais

- Decisões Estratégicas:
  - São as decisões tomadas no nível estratégico, pelos gestores da alta cúpula da administração (diretores, presidentes, CEO´s). As decisões se referem a assuntos que envolvem a organização como um todo, bem como a assuntos que envolvem as relações da empresa com o ambiente externo.
    - São decisões genéricas e amplas, que norteiam o caminho da organização como um todo. O foco das decisões está no longo prazo.
    - Por exemplo: decisões sobre os objetivos estratégicos, comportamento dos concorrentes, políticas da organização, etc.

- Decisões Táticas (Decisões Administrativas):
  - São as decisões tomadas no nível tático, pelos gerentes e chefes de departamento/divisão. As decisões se referem a assuntos que envolvem determinada unidade organizacional (departamento).
    - As decisões tomadas nesse nível têm por objetivo colocar em prática aquilo que foi decidido pelos gestores do nível estratégico, ou seja, colocar em prática o que foi decidido pelas "decisões estratégicas".
    - São decisões que norteiam o caminho de determinada unidade (departamento) da organização.
    - O foco das decisões, normalmente, está no médio prazo.

- Decisões Operacionais:
  - São as decisões tomadas no nível operacional, pelos supervisores. As decisões se referem a assuntos que envolvem a execução de tarefas ou determinada atividade específica.
    - As decisões tomadas nesse nível têm por objetivo colocar em prática aquilo que foi decidido pelos gestores do nível tático, ou seja, colocar em prática o que foi decidido pelas "decisões táticas".
    - São decisões relacionadas às tarefas do dia a dia (tarefas rotineiras). Isto é, esse tipo de decisão preocupa-se com a execução das tarefas, operações, rotinas, etc.
    - O foco das decisões está no curto prazo.

14.4 – Estilos Decisórios

- Estilo Analítico:
  - O tomador de decisões é racional e tem em alta tolerância à ambiguidade (tem alta complexidade cognitiva). Ele é cuidadoso e tem capacidade de se adaptar a novas situações. Suas decisões são tomadas com base em muitas informações e muitas alternativas são avaliadas. É orientado para as tarefas (desempenho).

- Estilo Diretivo:
  - O tomador de decisões é racional e tem em baixa tolerância à ambiguidade (tem baixa complexidade cognitiva). Ele é eficiente, lógico e toma decisões rapidamente. Suas

decisões são tomadas com base em poucas informações e poucas alternativas são avaliadas. Foca no curto prazo e é orientado para as tarefas (desempenho).

- Estilo Conceitual:
  - O tomador de decisões é intuitivo e tem em alta tolerância à ambiguidade (tem alta complexidade cognitiva). Ele é criativo e tem uma visão ampla das coisas. Suas decisões são tomadas com base em muitas informações e muitas alternativas são avaliadas. Foca no longo prazo é orientado para as pessoas (relações pessoais).

- Estilo Comportamental:
  - O tomador de decisões é intuitivo e tem em baixa tolerância à ambiguidade (tem baixa complexidade cognitiva). Ele se preocupa com as pessoas e com o desenvolvimento de sua equipe. Além disso, ele evita conflitos e busca a aceitação. Ele despreza a utilização de dados e informações para a tomada de decisões. Foca no curto prazo e é orientado para as pessoas (relações pessoais).

14.5 – Ferramentas de Auxílio ao Processo Decisório

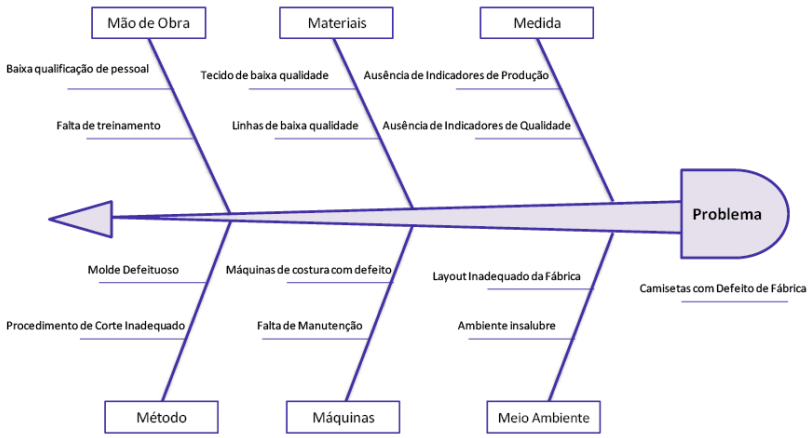
14.5.1 Diagrama de Ishikawa (Diagrama de Causa-Efeito)

O Diagrama de Ishikawa, também conhecido como Diagrama de Causa-Efeito, "Gráfico Espinha de Peixe", Método 4M ou Método 6M, é uma ferramenta que auxilia o tomador de decisão a identificar as causas de determinado problema. Ou seja, essa ferramenta auxilia o gestor a identificar as causas e, consequentemente, "compreender" melhor um processo ou um problema.

Em outras palavras, o Diagrama de Ishikawa permite ao gestor "visualizar" e "entender" quais são as causas que estão gerando determinados efeitos (problemas).

As causas (origens dos problemas / origens dos "efeitos") dividem-se em 06 diferentes categorias (6Ms):

- Mão de obra
- Método
- Materiais
- Máquinas
- Mensuração
- Meio ambiente



14.5.2 Diagrama de Pareto (Princípio de Pareto)

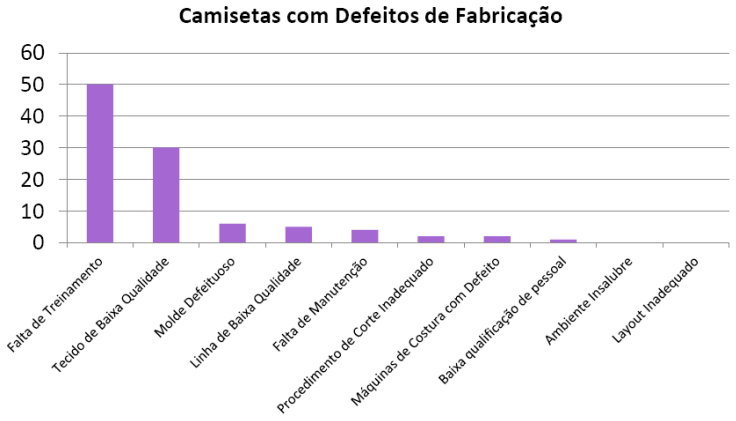
O Diagrama de Pareto, também chamado de Princípio de Pareto ou Regra do 80/20, é uma ferramenta que pode ser utilizada pelos tomadores de decisão para identificar quais são as causas prioritárias (ou seja, quais as "causas" que geram maiores "problemas").

Segundo a Regra do 80/20, 80% dos "resultados" ("problemas") provêm de 20% de "causas". Por sua vez, os outros 80% de "causas" geram apenas 20% de "resultados" ("problemas").

Em outras palavras, a ideia do Diagrama de Pareto é de que "poucas" causas significativas (20%) geram a maior parte dos problemas (80%); enquanto que "muitas" causas insignificantes (80%) geram a menor parte dos problemas (20%).

A ferramenta consiste em um gráfico de barras que ordena as "causas dos problemas" de forma decrescente (ou seja, do maior para o menor – da esquerda para a direita).

O Diagrama de Pareto é uma ferramenta que auxilia o gestor a "focar" (priorizar) nos aspectos que mais geram impacto na situação analisada.

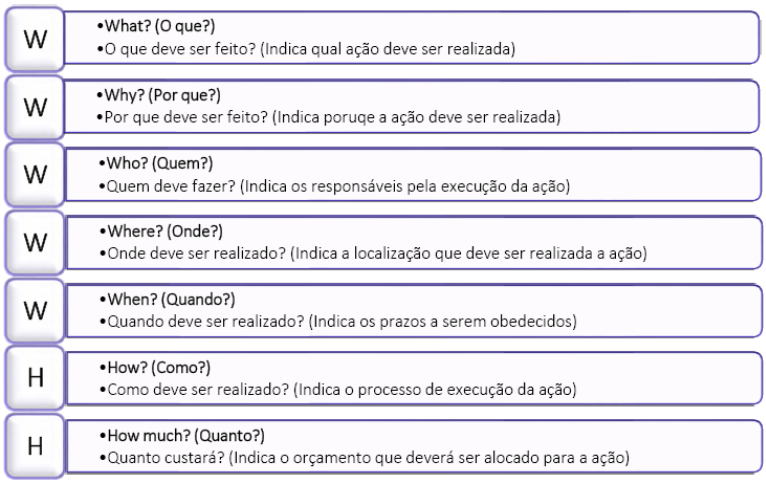


14.5.3 Ferramenta 5W2H

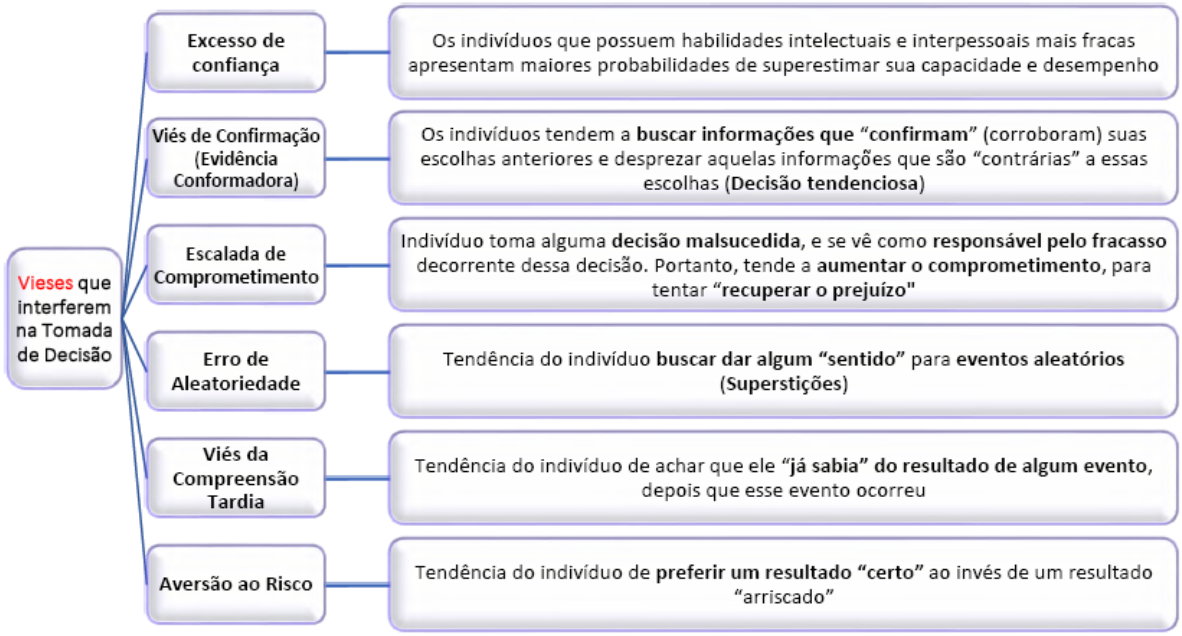
A ferramenta 5W2H tem por objetivo facilitar o planejamento das atividades. Trata-se, basicamente, de um "check-list" que auxilia o gestor a traçar os planos de ação para que os objetivos sejam alcançados.

Trata-se de uma ferramenta que também pode ser utilizada para auxiliar o gestor no processo de tomada de decisão.

Ao elaborar um plano de ação utilizando-se da ferramenta 5W2H, deve-se responder a 07 perguntas: (5W2H deriva das inicias das seguintes palavras em inglês: What, Why, Who, Where, When, How, How much).



14.5.4 Vieses que Interferem no Processo de Tomada de Decisão



15) LEI 13.709/2018 (LGPD)

A Lei 13.709/2018, também conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), foi sancionada em agosto de 2018 no Brasil, com o objetivo de regulamentar o tratamento de dados pessoais de indivíduos por parte de empresas públicas e privadas. Ela entrou em vigor em setembro de 2020.

A LGPD foi inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia e é uma resposta à crescente digitalização da sociedade, onde cada vez mais dados pessoais estão sendo coletados, processados e armazenados por organizações.

- Lei Geral de Proteção de Dados — dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, e aplica-se a qualquer operação de tratamento realizada por pessoa de direito privado, independentemente do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada no território nacional.

Os principais aspectos da LGPD incluem:

- Definições de dados pessoais e sensíveis: A LGPD define dados pessoais como informações que podem identificar uma pessoa. Dados sensíveis são um subconjunto de dados pessoais que se referem à origem racial ou étnica, convicções religiosas, opiniões políticas, saúde, vida sexual, dados genéticos ou biométricos.

- Princípios de tratamento de dados: A LGPD estabelece dez princípios que devem orientar o tratamento de dados pessoais, incluindo finalidade, adequação, necessidade, acesso livre, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

- Direitos do titular: A lei confere vários direitos ao titular dos dados, incluindo o direito de acesso, retificação, cancelamento, anonimização, portabilidade e informação sobre o compartilhamento de seus dados.

- Consentimento: Em muitos casos, o tratamento de dados pessoais requer o consentimento do titular dos dados. O consentimento deve ser livre, informado e inequívoco. Há, no entanto, outras bases legais para o tratamento de dados pessoais.

- Transferência internacional de dados: A LGPD permite a transferência internacional de dados pessoais, desde que o país de destino proporcione um nível adequado de proteção de dados ou se certas condições forem cumpridas.

- Autoridade Nacional de Proteção de Dados (ANPD): A lei criou a ANPD, uma entidade governamental responsável por fiscalizar a aplicação da lei, emitir diretrizes normativas e aplicar sanções em caso de violações.

- Sanções: A LGPD prevê uma série de sanções para violações, que vão desde advertências até multas de até 2% do faturamento da empresa, limitado a R$ 50 milhões por infração.

A LGPD representa um marco na proteção de dados pessoais no Brasil, trazendo maior transparência, fortalecendo os direitos dos indivíduos e impondo novas obrigações às organizações. Todas as empresas que tratam dados pessoais de indivíduos no Brasil, independentemente de onde estejam localizadas, devem cumprir a LGPD.

- O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares".

o tratamento dos referidos dados pelo site poderá ser feito sem o consentimento do titular se for indispensável para proteção da vida ou da incolumidade física do titular ou de terceiro;

- anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

- transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

- dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

    - perfil comportamental: de determinada pessoa natural, se identificada, também poderão ser igualmente considerados como dados pessoais para os fins desta Lei.

15.1 Requisitos para Tratamento dos Dados Pessoais:

A Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil, Lei nº 13.709/2018, estabelece várias condições sob as quais o tratamento de dados pessoais é permitido. De acordo com o Artigo 7º da LGPD, o tratamento de dados pessoais só pode ser realizado nas seguintes situações:

- Com o consentimento do titular: O titular dos dados deve fornecer consentimento explícito e informado para o tratamento de seus dados pessoais. O consentimento deve ser dado para finalidades específicas.

- Para cumprimento de obrigação legal ou regulatória pelo controlador: Se a organização é legalmente obrigada a tratar os dados pessoais, não é necessário obter o consentimento do titular dos dados.

- Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas: Previsto em leis ou regulamentos, ou respaldado em contratos, convênios ou instrumentos semelhantes.

- Para a realização de estudos por órgão de pesquisa: Isso deve garantir, sempre que possível, a anonimização dos dados pessoais.

- Quando necessário para a execução de contrato ou procedimentos preliminares: Se os dados pessoais forem necessários para a execução de um contrato (ou para procedimentos preliminares relacionados a um contrato) ao qual o titular dos dados é parte, ou para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

- Para o exercício regular de direitos em processo judicial, administrativo ou arbitral: Isso se aplica em casos onde o tratamento de dados pessoais é necessário para o exercício de direitos legais.

- Para a proteção da vida ou da incolumidade física do titular ou de terceiros: Se os dados pessoais forem necessários para proteger a vida ou a segurança física do titular dos dados ou de um terceiro.

- Para a tutela da saúde: No caso de procedimentos realizados por profissionais de saúde ou por entidades sanitárias.

- Quando necessário para atender aos interesses legítimos do controlador ou de terceiros: Exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

- Para a proteção do crédito: Incluindo o disposto na legislação pertinente.

É importante ressaltar que, mesmo quando o tratamento de dados é permitido, a LGPD estabelece uma série de princípios e obrigações que devem ser observados, incluindo a necessidade de informar o titular sobre a coleta e o uso de seus dados, a necessidade de garantir a segurança dos dados e a responsabilidade em caso de danos decorrentes do tratamento de dados.