

# QUESTÕES COMPLIANCE

Autor: Leonardo Costa Passos

Data: junho 2023

Coleção de 30+ questões de concurso da disciplina COMPLIANCE selecionadas de bancas variadas, debulhadas no detalhe de cada item e com classificação por cores.

*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](mailto:leonardx@gmail.com)

1. (CS UFG – Auditor (UFG) – 2017) A gestão de riscos refere-se ao processo de aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, estabelecimento do contexto, avaliação, tratamento, monitoramento e análise crítica dos riscos.

A gestão de riscos envolve também a contínua avaliação da eficácia dos controles internos implantados na organização para

a) uniformizar os riscos gerenciais.

**b) mitigar os riscos relevantes.**

c) eliminar os riscos críticos.

d) corrigir os riscos inerentes.

Comentários:

A 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.

Além da identificação e decisão quanto ao tratamento dos riscos, a gestão de riscos envolve também a contínua avaliação da eficácia dos controles internos implantados na organização para mitigar os riscos relevantes. [grifo nosso]

Gabarito: B

2. (Prefeitura de Recife – Analista – 2019) Um dos conceitos contemporâneos ligados à gestão de riscos no âmbito das organizações públicas e privadas é o de compliance, que significa

- a) mecanismo de aplicação de sanções aos responsáveis por condutas antiéticas e responsabilização judicial.
- b) compromisso com as finalidades institucionais, objetivando evitar o risco de baixa produtividade.
- c) controle de qualidade, focado na prevenção e tratamento dos riscos de perdas e de falhas de produção.
- d) atuação conforme as normas e regras fixadas, tendo como escopo evitar fraudes, ilícitos e desvios de conduta.
- e) governança corporativa, ou seja, o envolvimento de todos os stakeholders (agentes) no processo decisório.

Comentários:

Compliance significa estar em conformidade com as leis, os regulamentos internos e externos e os princípios corporativos que garantem as melhores práticas do mercado. Dentre as assertivas, a que mais se assemelha ao conceito apresentado é a letra D.

Gabarito: D.

3. (CM Nova Friburgo – Auditor de Controle Interno – 2017) A auditoria interna pode ser classificada em diversos tipos. A auditoria que tem como foco a verificação do cumprimento das normas aplicáveis à entidade e os seus regulamentos é definida como:

- a) Contábil
- b) Financeira:
- c) Operacional.
- d) De Compliance.**

Comentários:

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

Gabarito: D.

4. (CELESC – Administrador – 2018) Sobre políticas de compliance no ambiente organizacional, é correto afirmar:

- a) A política de compliance não tem relação direta com governança corporativa.
- b) As políticas de compliance 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).**
- c) A política de compliance tem sua ênfase principal na relação da empresa com o seu ambiente interno.
- d) As políticas de compliance vêm sendo amplamente utilizadas por empresas no Brasil desde 1940.
- e) As políticas de compliance são voltadas especialmente à área financeira e contábil das empresas.

Comentários:

Mais uma que associa o conceito de Compliance ao cumprimento de regras (normas, leis, controles políticas, diretrizes, etc.).

Gabarito: B.

5. (BACEN – 2009) Compliance tem por objetivo assegurar, em conjunto com as demais áreas, a adequação, o fortalecimento e o funcionamento do Sistema de Controles Internos da instituição, procurando mitigar os riscos de acordo com a complexidade de seus negócios, bem como disseminar a cultura de controles para assegurar o cumprimento de leis e regulamentos existentes. Cabe à área de compliance:

**A) 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.**

[CERTO]: A área de compliance tem como 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.

**B) efetuar seus trabalhos de forma periódica e temporal por meio de amostragens, a fim de certificar o cumprimento das normas e processos instituídos pela alta administração.**

[ERRADO]: A área de compliance tem um papel mais abrangente e contínuo, não se limitando a verificações periódicas e temporais através de amostragens.

**C) substituir as atividades realizadas pela auditoria interna, dado o seu caráter mais amplo e permanente na instituição, assegurando o cumprimento da normatização existente.**

[ERRADO]: A área de compliance não substitui a auditoria interna. Ambas desempenham papéis distintos e complementares na instituição, sendo a auditoria responsável pela revisão e avaliação dos controles internos, enquanto a compliance se concentra no cumprimento das normas e na prevenção de riscos.

**D) atender as necessidades de informação e segurança da diretoria executiva, mediante relatórios periódicos, fortalecendo os resultados, bem como o crescimento e o desenvolvimento sustentável da instituição.**

[ERRADO]: Embora a área de compliance possa fornecer informações à diretoria executiva, sua principal função não é atender às necessidades de informação e segurança da diretoria, mas sim garantir o cumprimento das normas e a prevenção e controle de riscos.

**E) ser o braço da diretoria executiva da instituição, acompanhando as atividades desenvolvidas pelas áreas fins, assegurando o cumprimento dos objetivos de cada unidade e garantindo o menor nível de perdas com os riscos inesperados.**

[ERRADO]: A área de compliance, embora possa trabalhar em conjunto com a diretoria executiva, tem como foco principal o cumprimento das normas e a prevenção e controle de riscos, e não o acompanhamento das atividades desenvolvidas pelas áreas fins e a garantia do cumprimento dos objetivos de cada unidade.

Comentários:

Conforme publicado pelo "THE INSTITUTE OF INTERNAL AUDITORS" dos EUA, a Auditoria Interna é uma atividade independente, de avaliação objetiva e de consultoria, destinada a acrescentar valor e

melhorar as operações de uma organização. A Auditoria Interna assiste a organização na consecução dos seus objetivos, através de uma abordagem sistemática e disciplinada, na avaliação da eficácia da gestão de risco, do controle e dos processos de governança.

Contudo, para executar seu trabalho é preciso que o profissional da Auditoria Interna esteja inteirado sobre as atividades desenvolvidas pelo "Compliance", com o estabelecimento de um trabalho em parceria, coordenado onde, quando de suas visitas, a Auditoria possa munir-se das informações relevantes, principalmente sobre o resultado da identificação e avaliação dos controles e riscos.

As atividades desenvolvidas por estas áreas não são idênticas, mas sim complementares, pois enquanto a Auditoria Interna efetua seus trabalhos de forma aleatória e temporal, por meio de amostragens, a fim de certificar o cumprimento das normas e processos instituídos pela Alta Administração, 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. Compliance é um braço dos Órgãos Reguladores junto a Administração, no que se refere à segurança, respeito à normas e controles, na busca da conformidade.

Gabarito: A.

6. (TRANSPETRO – 2011) A Lei Sarbanes-Oxley assumiu valores que foram assumidos pela Governança Corporativa. 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, refere-se ao valor denominado

**A) accountability**

[ERRADO]: Accountability refere-se à responsabilização e transparência das ações dos gestores e diretores da empresa perante os stakeholders. Não está diretamente relacionado ao código de ética mencionado na questão.

**B) compliance**

[CERTO]: Compliance é o valor relacionado ao cumprimento de leis, regulamentos e normas, bem como a adoção de um código de ética, conforme mencionado na questão.

**C) disclosure**

[ERRADO]: Disclosure refere-se à transparência e divulgação de informações financeiras e não financeiras relevantes aos stakeholders. Não está diretamente relacionado ao código de ética mencionado na questão.

**D) essential**

[ERRADO]: "Essential" não é um termo específico no contexto da Governança Corporativa e não se aplica diretamente aos valores mencionados na questão.

**E) fairness**

[ERRADO]: Fairness é um valor relacionado à equidade e tratamento justo de todas as partes interessadas (stakeholders) da empresa. Embora possa ser considerado um aspecto importante de um código de ética, não é o termo que melhor descreve a adoção de um código de ética para executivos mencionado na questão. Compliance é a opção mais adequada.

**Comentários:**

Questão aborda aspectos gerais da Lei Sarbanes-Oxley. Iremos fazer uso de parte do artigo "Governança corporativa e lei Sarbanes Oxley no Brasil". Veja: "A Lei Sarbanes Oxley foi sancionada em 30 de Julho de 2002 pelo presidente dos Estados Unidos George W.Bush, e seus idealizadores foram o senador Paul Sarbanes e o deputado Michael G.Oxley.Essa legislação vem estabelecer novos padrões ou aperfeiçoar os já existentes para as companhias norte-americanas, conselhos de



administração, diretoria e empresas de auditoria externa; aplica-se ainda a empresas estrangeiras que comercializam seus títulos no mercado financeiro.

Após a constatação de práticas de manipulação em várias empresas em todo o mundo, o nível de confiança nas informações contábeis reduziu consideravelmente, essa situação pressionou os governos de vários países a tomar medidas legislativas, destacando-se a criação da Lei Sarbanes-Oxley.

O objetivo da Lei é a proteção dos acionistas das empresas com ações negociadas na bolsa exigindo dessas companhias o aprimoramento da estrutura de controles internos financeiros, a melhoria nos processos e maior transparência das atividades.

A pretensão específica da Lei é aplicar exigências de governança corporativa e assim cobrir abusos, tranquilizar os investidores por meio da implementação de mudanças efetivas e sustentáveis, aumentarem a transparência das informações geradas pelas empresas, além de exigir responsabilidade dos executivos sobre atividades duvidosas.

Entretanto, com a incorporação dessa lei, as empresas nacionais com papéis negociados no mercado de capitais americano devem pagar em média US\$ 3 milhões para se adequar às normas da lei americana Sarbanes-Oxley de governança corporativa.

Andrade e Paschoal (2004, p.85), enfatizam os principais focos da lei: a Lei Sarbanes Oxley promoveu ampla regulação na vida corporativa, fundamentada nas boas práticas de governança. Seus focos são exatamente os quatro valores que há duas décadas vinham sendo enfatizados pelo ativismo pioneiro. Vale repeti-los:

1. Compliance, conformidade legal;
2. accountability, prestação responsável de contas;
3. Disclosure, mais transparência;
4. Fairness, senso de justiça.

A conformidade legal adota um código de ética para seus executivos onde deverão conter as questões relacionadas aos conflitos de interesses, divulgação de informações e cumprimento de leis e regulamentos. Nos relatórios periódicos previstos em lei a prestação de contas responsável entra como um fator determinante para que estes relatórios sejam revisados para que não existam falsas omissões ou declarações falsas. As demonstrações financeiras devem revelar adequadamente a posição financeira, os resultados e os fluxos de caixa, os auditores devem receber informações importantes como deficiências nos controles internos, fraudes evidenciadas ou mudanças após avaliação."

Gabarito: B.

7. (CESPE - Auditor Estadual (TCM-BA) / Infraestrutura - 2018) De acordo com o COSO (Committee of Sponsoring Organizations of the Treadway Commission), o controle interno é um processo conduzido pela estrutura de governança, administração e outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade. O componente de controle interno em que se avaliam e se comunicam as deficiências no controle interno aos responsáveis por tomar ações corretivas, inclusive a estrutura de governança e alta administração, é designado

- a) ambiente de controle.
- b) avaliação de riscos.
- c) atividades de controle.
- d) informação e comunicação.
- e) atividades de monitoramento.**

#### Comentários

COSO é o Comitê das Organizações Patrocinadas, da Comissão Nacional sobre Fraudes em Relatórios Financeiros. É uma entidade do setor privado, sem fins lucrativos, voltada para o aperfeiçoamento da qualidade de relatórios financeiros.

Segundo o COSO I, “existe uma relação direta entre os objetivos, que são o que a entidade busca alcançar, os componentes, que representam o que é necessário para atingir os objetivos, e a estrutura organizacional da entidade (as unidades operacionais e entidades legais, entre outras). Essa relação pode ser ilustrada na forma de um cubo.”

A Estrutura estabelece 17 princípios, que representam os conceitos fundamentais associados a cada componente. Como esses princípios são originados diretamente dos componentes, uma entidade poderá ter um controle interno eficaz ao aplicar todos os princípios. Todos os princípios aplicam-se aos objetivos operacionais, divulgação e conformidade. Os princípios que apoiam os componentes do controle interno estão relacionados a seguir.

#### a) AMBIENTE DE CONTROLE:

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.

b) 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.

c) ATIVIDADE DE CONTROLE:

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.

d) INFORMAÇÃO e COMUNICAÇÃO:

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.

e) ATIVIDADES de MONITORAMENTO:

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]

Gabarito: "E".

8. (CESPE - Auditor Estadual (TCM-BA) / Infraestrutura - 2018) Um sistema de controle interno eficaz reduz, a níveis aceitáveis, o risco de não se atingir o objetivo de uma entidade e pode estar relacionado a uma, a duas ou a todas as três categorias de objetivos. Nesse contexto, a 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 refere-se

A) à presença.

[ERRADO]: A presença refere-se à existência de políticas, procedimentos e estruturas de controle interno estabelecidos, mas não trata da continuidade dos componentes e princípios na operação e na condução do sistema de controle interno para atingir objetivos específicos.

B) ao funcionamento.

[ERRADO]: O funcionamento se refere à eficácia dos controles internos em operação, mas não aborda diretamente a determinação de que os componentes e princípios relacionados continuem a existir na operação e na condução do sistema de controle interno para atingir objetivos específicos.

C) ao monitoramento.

[CERTO]: O monitoramento é um componente essencial do sistema de controle interno eficaz, que garante a continuidade dos componentes e princípios em operação e na condução do sistema de controle interno para atingir os objetivos especificados. O monitoramento envolve a avaliação contínua dos controles internos e a identificação e correção de deficiências, garantindo que os controles sejam efetivos e que a entidade continue a atingir seus objetivos.

D) à abrangência.

[ERRADO]: A abrangência refere-se à extensão em que os controles internos cobrem diferentes áreas, processos e atividades da entidade, mas não trata diretamente da continuidade dos componentes e princípios na operação e na condução do sistema de controle interno para atingir objetivos específicos.

E) à estrutura.

[ERRADO]: A estrutura se refere ao conjunto de políticas, procedimentos e práticas estabelecidas para garantir o controle interno, mas não aborda diretamente a determinação de que os componentes e princípios relacionados continuem a existir na operação e na condução do sistema de controle interno para atingir objetivos específicos.

9. (TRANSPETRO – 2011) A Lei Sarbanes-Oxley assumiu valores que foram assumidos pela Governança Corporativa. 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, refere-se ao valor denominado

A) à presença.

[ERRADO]: A presença se refere à determinação da existência dos componentes e princípios relacionados no desenho e na implementação do sistema de controle interno, não está diretamente relacionada à garantia de que eles continuem a existir na operação e na condução do sistema de controle interno.

B) ao funcionamento.

[CERTO]: 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. A questão trata exatamente deste aspecto.

C) ao monitoramento.

[ERRADO]: O monitoramento é o processo que avalia a eficácia dos componentes do sistema de controle interno, e embora esteja relacionado ao funcionamento do sistema, não é o termo que melhor descreve o conceito mencionado na questão.

D) à abrangência.

[ERRADO]: A abrangência se refere à extensão e alcance do sistema de controle interno em relação aos objetivos da entidade, mas não está diretamente relacionada à garantia de que os componentes e princípios continuem a existir na operação e na condução do sistema de controle interno.

E) à estrutura.

[ERRADO]: A estrutura se refere à organização e disposição dos componentes e princípios relacionados ao sistema de controle interno, mas não está diretamente ligada à garantia de que eles continuem a existir na operação e na condução do sistema de controle interno.

## Comentários

O Sumário Executivo de Controle Interno – Estrutura Integrada (2013, p.11), do Committee of Sponsoring Organization, Coso I, estabelece os requisitos para um sistema eficaz de controle interno. A questão aborda um desses requisitos – o funcionamento.

Veja:

Controle interno eficaz

A Estrutura estabelece os requisitos para um sistema eficaz de controle interno, que proporciona segurança razoável acerca da realização dos objetivos da entidade. Um sistema de controle interno eficaz reduz, a um nível aceitável, o risco de não se atingir o objetivo de uma entidade e pode estar relacionado a uma, duas ou todas as três categorias de objetivos. O sistema requer:

- A presença e o funcionamento de cada um dos cinco componentes e princípios relacionados. “Presença” refere-se à determinação da existência dos componentes e princípios relacionados no desenho e na implementação do sistema de controle interno para atingir objetivos especificados. “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;
- Os cinco componentes operam em conjunto de forma integrada. “Operam em conjunto” refere-se à determinação de que todos os cinco componentes, em conjunto, reduzam a um nível aceitável o risco de não se atingir o objetivo. Os componentes não devem ser considerados de forma separada; eles operam em conjunto como um sistema integrado.

Os componentes são interdependentes e contam com uma profusão de inter-relacionamentos e ligações entre si, especialmente a maneira como os princípios interagem dentro e entre todos os componentes. [...]

Ressalta-se que o controle interno da entidade é composto por cinco componentes interrelacionados, quais sejam: Ambiente de controle, Processo de avaliação de risco da entidade, Sistema de informação e comunicação, Atividade de controle e Monitoramento.

Portanto, alternativa correta é B.

Gabarito: “B”.

10. (CESPE - Auditor Estadual (TCM-BA) /Controle Externo - 2018) A metodologia de avaliação dos controles internos de determinada entidade, que tem por objetivo garantir a adequação e a consistência desses controles, prevê a execução de diversas etapas, em uma sequência lógica. Nessa avaliação, a última etapa a ser executada consiste na

**A) realização de testes de observância das normas internas e legais.**

[CERTO]: Os testes de observância são uma parte fundamental do monitoramento, que é a etapa final do controle interno no COSO I. Esses testes visam garantir que os controles internos estabelecidos pela administração estejam funcionando efetivamente e sendo cumpridos pelos funcionários e administradores da entidade.

**B) execução de entrevistas com os empregados da entidade.**

[ERRADO]: As entrevistas com os empregados da entidade são realizadas durante as etapas iniciais do processo de avaliação dos controles internos e não estão diretamente relacionadas à etapa final de monitoramento.

**C) elaboração de fluxogramas.**

[ERRADO]: A elaboração de fluxogramas ocorre durante as etapas iniciais do processo de avaliação dos controles internos e não está diretamente relacionada à etapa final de monitoramento.

**D) identificação dos controles essenciais ao sistema.**

[ERRADO]: A identificação dos controles essenciais ao sistema ocorre antes da etapa final de monitoramento, durante a análise dos fluxogramas e a realização de testes de observância.

**E) inspeção física da operação normal da entidade.**

[ERRADO]: A inspeção física da operação normal da entidade pode ser parte do processo de monitoramento, mas não é tão específica quanto a realização de testes de observância das normas internas e legais mencionada na alternativa A.

#### Comentários

Tomando por base o COSO I, a etapa (ou componente) final do controle interno seria o Monitoramento. Nessa fase, são efetuadas avaliações contínuas, independentes, ou uma combinação das duas, para se certificar da presença e do funcionamento de cada um dos cinco componentes de controle interno, inclusive a eficácia dos controles nos princípios relativos a cada componente.

Nesse contexto, os testes de observância visam à obtenção de razoável segurança de que os controles internos estabelecidos pela administração estão em efetivo funcionamento, inclusive quanto ao seu cumprimento pelos funcionários e administradores da entidade.

Dessa forma, a assertiva mais aplicável ao contexto das atividades de monitoramento é a letra A (testes de observância das normas internas e legais).

Gabarito: "A".

11. (CESPE – Auditor do Estado (CAGE RS) – 2018)

Entre as quatro categorias de objetivos organizacionais estabelecidas pelo COSO inclui-se a categoria dos objetivos operacionais, cujo propósito é

a) assegurar o cumprimento das leis e dos regulamentos.

ERRADA. Este item descreve objetivos de conformidade, não objetivos operacionais. Conformidade: cumprimento de leis e regulamentos aplicáveis.

b) utilizar de forma eficaz e eficiente os recursos.

CERTO: Esta opção descreve corretamente o propósito dos objetivos operacionais, que envolvem o uso eficiente e eficaz dos recursos da organização.

c) viabilizar o atingimento de metas no nível mais elevado, alinhando-se e fornecendo apoio à missão.

ERRADA. Este item está mais relacionado aos objetivos estratégicos, que envolvem o alinhamento e apoio à missão da organização.

d) evitar a perda de ativos ou recursos da organização.

ERRADA. A preservação de ativos e recursos é uma parte dos objetivos operacionais, mas não descreve completamente o propósito dos objetivos operacionais como a alternativa B.

e) atestar a confiabilidade dos relatórios.

ERRADA. Relaciona-se com a Comunicação.

#### Comentários

Inicialmente, podemos identificar que o enunciado está fazendo menção ao COSO II, que prevê quatro categorias de objetivos (o COSO I prevê apenas 3 categorias de objetivos).

Segundo o Manual de Gerenciamento de Riscos Corporativos — Estrutura Integrada (COSO II):

Com base na missão ou visão estabelecida por uma organização, a administração estabelece os planos principais, seleciona as estratégias e determina o alinhamento dos objetivos nos níveis da organização. Essa estrutura de gerenciamento de riscos corporativos é orientada a fim de alcançar os objetivos de uma organização e são classificados em quatro categorias:

Estratégicos – metas gerais, alinhadas com o que suportem à sua missão.

Operações –

Comunicação – confiabilidade de relatórios.

Conformidade –

Gabarito: “B”.



12. (CESPE – Auditor do Estado (CAGE RS) – 2018) Determinado componente do gerenciamento de riscos corporativos permite que a organização considere até que ponto eventos em potencial podem impactar o atingimento de seus objetivos. O COSO denomina esse componente de

a) monitoramento.

[ERRADO]: O monitoramento é um componente que envolve a revisão contínua e a avaliação do sistema de gerenciamento de riscos corporativos para garantir sua eficácia e aprimorá-lo quando necessário.

b) atividades de controle.

[ERRADO]: As atividades de controle são políticas e procedimentos estabelecidos para ajudar a garantir que as ações de gerenciamento de riscos sejam executadas conforme planejado.

c) avaliação de riscos.

[CERTO]: A avaliação de riscos é o componente que permite que uma organização considere até que ponto eventos em potencial podem impactar o atingimento de seus objetivos.

d) identificação de eventos.

[ERRADO]: A identificação de eventos envolve o reconhecimento e a descrição de eventos internos e externos que podem afetar a organização no atingimento de seus objetivos.

e) informações e comunicações.

[ERRADO]: Informações e comunicações são processos que garantem o fluxo adequado de informações dentro da organização, bem como o compartilhamento de informações com partes externas, quando apropriado.

Comentários

A questão aborda um dos oito componentes que compõem o gerenciamento de riscos corporativos. De acordo com o COSO II:

O gerenciamento de riscos corporativos é constituído de oito componentes interrelacionados, que se originam com base na maneira como a administração gerencia a organização, e que se integram ao processo de gestão. Esses componentes são os seguintes:

Ambiente Interno – A administração estabelece uma filosofia quanto ao tratamento de riscos e estabelece um limite de apetite a risco. O ambiente interno determina os conceitos básicos sobre a forma como os riscos e os controles serão vistos e abordados pelos empregados da organização.

**Fixação de Objetivos** – Os objetivos devem existir antes que a administração identifique as situações em potencial que poderão afetar a realização destes.

**Identificação de Eventos** – Os eventos em potencial que podem impactar a organização devem ser identificados, uma vez que esses possíveis eventos, gerados por fontes internas ou externas, afetam a realização dos objetivos.

**Avaliação de Riscos** – Os riscos identificados são analisados com a finalidade de determinar a forma como serão administrados e, depois, serão associados aos objetivos que podem influenciar.

**Resposta a Risco** – Os empregados identificam e avaliam as possíveis respostas aos riscos: evitar, aceitar, reduzir ou compartilhar. A administração seleciona o conjunto de ações destinadas a alinhar os riscos às respectivas tolerâncias e ao apetite a risco.

**Atividades de Controle** – Políticas e procedimentos são estabelecidos e implementados para assegurar que as respostas aos riscos selecionados pela administração sejam executadas com eficácia.

**Informações e Comunicações** – A forma e o prazo em que as informações relevantes são identificadas, colhidas e comunicadas permitam que as pessoas cumpram com suas atribuições.

**Monitoramento** – A integridade do processo de gerenciamento de riscos corporativos é monitorada e as modificações necessárias são realizadas. Desse modo, a organização poderá reagir ativamente e mudar segundo as circunstâncias. O monitoramento é realizado por meio de atividades gerenciais contínuas, avaliações independentes ou uma combinação desses dois procedimentos.

Ainda de acordo com a publicação, a avaliação de riscos permite que uma organização considere até que ponto eventos em potencial podem impactar a realização dos objetivos.

Portanto, alternativa correta é C.

Gabarito: “C”.

13. (CESPE – Auditor do Estado (CAGE RS) – 2018) Diversos tipos de alterações, como, por exemplo, nas condições demográficas, nos costumes sociais, nas estruturas das famílias, nas prioridades de trabalho, podem provocar mudanças na demanda de produtos e serviços, novos locais de compra, demandas relacionadas a recursos humanos e paralisações da produção. De acordo com o COSO, as relações entre essas alterações e seus efeitos são consideradas eventos

a) políticos.

eleição de agentes do governo com novas agendas políticas e novas leis e regulamentos, resultando, por exemplo, na abertura ou na restrição ao acesso a mercados estrangeiros, ou elevação ou redução na carga tributária.

b) de meio ambiente.

refere-se aos seguintes eventos: incêndios, inundações ou terremotos, que provocam danos a fábricas ou edificações, restrição quanto ao uso de matérias-primas e perda de capital humano.

**c) sociais.**

são alterações nas condições demográficas, nos costumes sociais, nas estruturas da família, nas prioridades de trabalho/ vida e a atividade terrorista, que, por sua vez, podem provocar mudanças na demanda de produtos e serviços, novos locais de compra, demandas relacionadas a recursos humanos e paralisações da produção.

d) pessoais.

Não existe essa categoria de evento.

e) econômicos.

os eventos relacionados contemplam: oscilações de preços, disponibilidade de capital, ou redução nas barreiras à entrada da concorrência, cujo resultado se traduz em um custo de capital mais elevado ou mais reduzido, e em novos concorrentes.

Além desses existem os eventos Tecnológicos:

- **Tecnológicos** – são novas formas de comércio eletrônico, que podem provocar aumento na disponibilidade de dados, reduções de custos de infraestrutura e aumento da demanda de serviços com base em tecnologia.

Portanto, alternativa correta é C.

Gabarito: "C".

14. (CESPE – Auditor do Estado (CAGE RS) – 2018) A administração de uma universidade estadual identificou e avaliou os riscos associados com a gerência da residência estudantil: concluiu que a referida gerência não possuía internamente os requisitos necessários e as funcionalidades para administrar eficazmente essa grande propriedade residencial, razão pela qual optou por terceirizar a administração da residência para uma empresa especializada, que, entre outros fatores, tivesse condições de reduzir o impacto e a probabilidade de riscos.

De acordo com o COSO, a categoria de resposta a risco descrita na situação hipotética apresentada é

**a) compartilhar.**

CERTO: Redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento de uma porção do risco. As técnicas comuns compreendem a aquisição de produtos de seguro, a realização de transações de hedging ou a terceirização de uma atividade.

**b) evitar.**

ERRADO: Descontinuação das atividades que geram os riscos. Evitar riscos pode implicar a descontinuação de uma linha de produtos, o declínio da expansão em um novo mercado geográfico ou a venda de uma divisão.

**c) reduzir.**

ERRADO: São adotadas medidas para reduzir a probabilidade ou o impacto dos riscos, ou, até mesmo, ambos. Tipicamente, esse procedimento abrange qualquer uma das centenas de decisões do negócio no dia-a-dia.

**d) aceitar.**

ERRADO: Nenhuma medida é adotada para afetar a probabilidade ou o grau de impacto dos riscos.

**e) acolher.**

ERRADO: não existe essa resposta ao risco.

15. (CESPE - Analista de Controle (TCE-PR)/Contábil - 2016) A respeito de controles internos, de acordo com o Manual de Gerenciamento de Riscos Corporativos — Estrutura Integrada (COSO II), do Committee of Sponsoring Organization, assinale a opção correta.

a) Nas atividades de monitoramento, a organização deve escolher e executar avaliações para averiguar se os componentes do controle externo estão em operação.

ERRADA. Na fase de monitoramento, é averiguado se os demais componentes do controle INTERNO estão em operação.

b) Segundo o COSO II, são quatro os componentes para o gerenciamento de riscos corporativos: ambiente externo; fixação de objetivos; estabelecimento de riscos; atividades de controle; e monitoramento.

ERRADA. Segundo o COSO II, são 08 (oito) os componentes do Gerenciamento de Riscos Corporativos.

c) No gerenciamento de riscos corporativos, a fixação dos objetivos será realizada após a identificação dos eventos, a fim de se determinar quais ações serão realizadas para cada tipo de risco.

ERRADA. A fixação de objetivos é feita ANTES da identificação de eventos, pois é necessário estabelecer os objetivos da organização antes de identificar os eventos que possam afetar o atingimento desses objetivos.

d) Risco inerente é aquele que perdura mesmo depois da resposta dos dirigentes da organização.

ERRADA.

- RISCO INERENTE: risco que existe antes de qualquer ação de gerenciamento de riscos.
- RISCO RESIDUAL: risco que perdura após a resposta dos dirigentes da organização.

**e) Em uma organização, o gerenciamento de riscos corporativos, processo conduzido pelos seus membros, consiste em estabelecer estratégias para identificar e administrar potenciais eventos capazes de afetá-la.**

CORRETA. Esta afirmação descreve corretamente o gerenciamento de riscos corporativos como um processo conduzido pelos membros da organização, focado em identificar e administrar eventos que possam afetar a organização.

16. (CESPE – TCE PR – Analista de Controle – Contábil – 2016) Assinale a opção correta, a respeito de governança no setor público.

a) A auditoria é entendida como um instrumento de verificação da governança.

[CERTO]: A auditoria é um processo que busca avaliar a eficácia, eficiência e conformidade dos controles internos, bem como a qualidade da governança dentro de uma organização. Portanto, a auditoria é um instrumento de verificação da governança.

b) Um dos princípios de governança no setor público, a prestação de contas por responsabilidade conferida ao gestor público será obrigatória apenas em determinadas situações.

[ERRADO]: A prestação de contas é um princípio fundamental da governança no setor público e é obrigatória para todos os gestores públicos, independentemente da situação.

c) As instâncias externas de governança responsáveis pelo exercício de fiscalização e controle são autônomas, mas podem depender de outras organizações.

[ERRADO]: As instâncias externas de governança, como os órgãos de controle externo, são autônomas e independentes, e não dependem de outras organizações.

d) As instâncias internas de governança responsáveis pela avaliação de estratégias e políticas e pelo monitoramento de conformidade estão impedidas de atuar nas situações em que desvios forem identificados.

[ERRADO]: As instâncias internas de governança, como as auditorias internas, têm como função identificar e atuar em situações de desvios, de modo a garantir a conformidade com as políticas e regulamentações.

e) No setor público, a governança é analisada sob três perspectivas: sociedade e Estado; atividades extraorganizacionais; e órgãos e entidades.

[ERRADO]: A governança no setor público pode ser analisada sob diversas perspectivas, porém essa classificação não é amplamente reconhecida e não abrange todas as possíveis perspectivas de análise.

#### Comentários

Segundo o Referencial Básico de Governança aplicável a órgãos e entidades da administração pública, “o sistema de governança reflete a maneira como diversos atores se organizam, interagem e procedem para obter boa governança. Envolve, portanto, as estruturas administrativas (instâncias), os processos de trabalho, os instrumentos (ferramentas, documentos etc.), o fluxo de informações e o comportamento de pessoas envolvidas direta, ou indiretamente, na avaliação, no direcionamento e no monitoramento da organização. De forma simplificada, esse sistema pode ser assim representado (Figura 5):”

Além disso, na mesma direção, esse Referencial explica que: Nota-se, nesse sistema, que algumas instâncias foram destacadas: as instâncias externas de governança; as instâncias externas de apoio à governança; as instâncias internas de governança; e as instâncias internas de apoio à governança.

a) As instâncias externas de governança são responsáveis pela fiscalização, pelo controle e pela regulação, desempenhando importante papel para promoção da governança das organizações públicas. São autônomas e independentes, não estando vinculadas apenas a uma organização. Exemplos típicos dessas estruturas são o Congresso Nacional e o Tribunal de Contas da União.

b) As instâncias externas de apoio à governança são responsáveis pela avaliação, auditoria e monitoramento independente e, nos casos em que disfunções são identificadas, pela comunicação dos fatos às instâncias superiores de governança. Exemplos típicos dessas estruturas as auditorias independentes e o controle social organizado.

c) As instâncias internas de governança são responsáveis por definir ou avaliar a estratégia e as políticas, bem como monitorar a conformidade e o desempenho destas, devendo agir nos casos em que desvios forem identificados. São, também, responsáveis por garantir que a estratégia e as políticas formuladas atendam ao interesse público servindo de elo entre principal e agente. Exemplos típicos dessas estruturas são os conselhos de administração ou equivalentes e, na falta desses, a alta administração.

d) As instâncias internas de apoio à governança realizam a comunicação entre partes interessadas internas e externas à administração, bem como auditorias internas que avaliam e monitoram riscos e controles internos, comunicando quaisquer disfunções identificadas à alta administração. Exemplos típicos dessas estruturas são a ouvidoria, a auditoria interna, o conselho fiscal, as comissões e os comitês. [grifo nosso]

Após essas considerações iniciais, analisaremos cada alternativa:

Letra A) CORRETA. Tanto a auditoria externa (instância externa) quanto à interna (instância interna) servem de instrumento de verificação da governança, uma vez que ambos compõem o Sistema de Governança e estão em conformidade com o Referencial.

Letra B) ERRADA. Segundo o Referencial, todas as pessoas ou entidades que tenham recebido recursos públicos devem prestar contas. Veja:

Accountability: As normas de auditoria da Intosai conceituam accountability como a obrigação que têm as pessoas ou entidades às quais se tenham confiado recursos, incluídas as empresas e organizações públicas, de assumir as responsabilidades de ordem fiscal, gerencial e programática que lhes foram conferidas, e de informar a quem lhes delegou essas responsabilidades (BRASIL, 2011). Espera-se que os agentes de governança prestem contas de sua atuação de forma voluntária, assumindo integralmente as consequências de seus atos e omissões (IBGC, 2010).

Letra C) ERRADA. As instâncias externas são autônomas e independentes, não estando vinculadas apenas a uma organização.

Letra D) ERRADA. As instâncias internas de governança são responsáveis por definir ou avaliar a estratégia e as políticas, bem como monitorar a conformidade e o desempenho destas, devendo agir nos casos em que desvios forem identificados.

Letra E) ERRADA. São quatro perspectivas, ao invés de três. Uma das perspectivas são as atividades intraorganizacionais (e não extraorganizacionais). Veja: De forma geral os três mecanismos propostos (liderança, estratégia e controle) podem ser aplicados a qualquer uma das quatro perspectivas de observação (sociedade e Estado; entes federativos, esferas de poder e políticas públicas; órgãos e entidades; e atividades intraorganizacionais), devendo, no entanto, estarem alinhados de forma a garantir que direcionamentos de altos níveis se reflitam em ações práticas pelos níveis subalternos.

[grifo nosso]

Gabarito: "A".

17. (FUNDATEC / BRDE – Analista de Projetos – 2017) De acordo com o Committee Of Sponsoring Organizations Of The Treadway Commission (COSO), são componentes de gerenciamento de riscos:

- a) Estrutura Organizacional, Filosofia de Gerenciamento, Classificação de Riscos e Appetite ao Risco.
- b) Atividade de Controle, Identificação de Eventos, Gestão Financeira de Liquidez e Avaliação.
- c) Ambiente Interno, Fixação de Objetivos, Identificação de Eventos, Avaliação de Riscos, Resposta aos Riscos, Atividade de Controle, Informações e Comunicações.
- d) Análise de Riscos, Probabilidade e Impacto, Tolerância e Appetite ao Risco.
- e) Identificação de Eventos, Avaliação de Riscos, Atividades Gerenciais Contínuas, Avaliações Independentes e Processos Informatizados.

#### Comentários

Segundo o COSO II, o gerenciamento de riscos corporativos é constituído de oito componentes inter-relacionados, que se originam com base na maneira como a administração gerencia a organização, e que se integram ao processo de gestão. Esses componentes são os seguintes: Ambiente Interno; Fixação de Objetivos; Identificação de Eventos; Avaliação de Riscos; Resposta a Risco; Atividades de Controle; Informações e Comunicações; e Monitoramento.

Gabarito: "C".



18. (FUNDATEC / CAGE RS – Auditor – 2014) Ambiente de controle, estabelecimento de metas, identificação de problemas, avaliação de risco, atividades de controle, informação, comunicação e monitoramento são as oito dimensões do modelo internacional que serve de parâmetro para a auditoria na avaliação da estrutura de controles internos.

Assim, este modelo denomina-se:

**a) COSO: Committee of Sponsoring Organizations of the Treadway Commission**

CERTO: uma iniciativa conjunta de cinco organizações de contabilidade e auditoria dos Estados Unidos que desenvolveu o COSO Internal Control-Integrated Framework, um modelo de controle interno amplamente reconhecido.

**b) COBIT: Control Objectives for Information and Related Technology**

ERRADO: é um framework desenvolvido pelo ISACA (Information Systems Audit and Control Association) que fornece melhores práticas para governança e gestão de TI, ajudando as organizações a alinhar seus objetivos de negócio com as estratégias e práticas de TI.

**c) SOX: Sarbanes-Oxley**

ERRADO: é uma lei dos Estados Unidos promulgada em 2002 que estabelece requisitos de governança corporativa e responsabilidade financeira para as empresas de capital aberto. A SOX visa melhorar a confiabilidade e transparência nos relatórios financeiros e prevenir fraudes corporativas.

**d) SEC: Security Exchange Commission**

ERRADO: é uma agência independente do governo dos Estados Unidos responsável por regular e supervisionar os mercados de valores mobiliários, proteger os investidores e facilitar a formação de capital.

**e) AICPA: American Institute of Certified Public Accountants**

ERRADO: é a principal organização profissional dos contadores públicos certificados nos Estados Unidos. O AICPA estabelece padrões éticos e profissionais para a prática da contabilidade e auditoria, bem como desenvolve e classifica exames uniformes para a certificação de contadores públicos.

**Comentários**

Enunciado apresenta um “mix” dos componentes do Controle Interno trazidos pelo COSO I e dos componentes da Gestão de Riscos Corporativos trazidos pelo COSO II.

Gabarito: “A”.

19. (FUNDATEC / CAGE RS – Auditor – 2014) Por meio do Enterprise Risk Management (ERM), é possível fazer-se o gerenciamento dos riscos corporativos. Vários são os seus componentes. Assim, NÃO faz parte do gerenciamento de riscos:

- a) Identificação de eventos.
- b) Fixação de objetivos.
- c) Aproveitamento das oportunidades.
- d) Atividades de controle.
- e) Informações e comunicações.

#### Comentários

Todas as assertivas, com exceção da letra C, trazem componentes do gerenciamento de riscos corporativos trazidos pelo COSO II.

Gabarito: "C".

20. (FGV / CM Salvador – Analista Legislativo – 2018) A estrutura integrada de controle interno e gerenciamento de risco proposta pelo Committee Of Sponsoring Organizations of the Treadway Commission (COSO) está baseada em quatro categorias de objetivos.

A categoria de objetivo relacionada à sobrevivência, continuidade e sustentabilidade organizacional é o(a):

a) comunicação;

ERRADO: confiabilidade de relatórios.

b) conformidade;

ERRADO: cumprimento de leis e regulamentos aplicáveis.

c) desempenho;

ERRADO: não existe essa categoria

d) estratégica;

CERTO: metas gerais, alinhadas com o que suportem à sua missão.

e) operacional.

ERRADO: utilização eficaz e eficiente dos recursos.

#### Comentários

Inicialmente, podemos identificar que o enunciado está fazendo menção ao COSO II, que prevê quatro categorias de objetivos (o COSO I prevê apenas 3 categorias de objetivos). Segundo o Manual de Gerenciamento de Riscos Corporativos — Estrutura Integrada (COSO II):

Essa estrutura de gerenciamento de riscos corporativos é orientada a fim de alcançar os objetivos de uma organização e são classificados em quatro categorias:

Estratégicos –

Operações –

Comunicação –

Conformidade –

Apesar do COSO II não utilizar as expressões “sobrevivência”, “continuidade” e “sustentabilidade organizacional”, podemos tranquilamente associá-las ao nível mais macro de categorias de objetivos: os objetivos estratégicos.

Gabarito: “D”.

21. (FGV / CM Salvador – Analista Legislativo – 2018) A Estrutura Integrada de Controle Interno proposta pelo Committee Of Sponsoring Organizations of the Treadway Commission (COSO) organiza o controle interno em cinco componentes.

Quando uma entidade que organizou o seu controle interno a partir da estrutura do COSO realiza avaliações contínuas e/ou independentes para se certificar da presença e do funcionamento dos componentes do controle interno, está atendendo diretamente ao componente de:

A) ambiente de controle;

[ERRADO]: O ambiente de controle estabelece a base para os demais componentes do controle interno, mas não se refere às avaliações contínuas e independentes.

B) avaliação de riscos;

[ERRADO]: A avaliação de riscos envolve a identificação e análise de riscos relevantes para o alcance dos objetivos da entidade, mas não inclui as avaliações contínuas e independentes.

C) atividades de controle;

[ERRADO]: As atividades de controle são ações estabelecidas para ajudar a garantir que as respostas aos riscos sejam executadas de forma eficaz, mas não incluem as avaliações contínuas e independentes.

D) atividades de monitoramento;

[CERTO]: O componente de atividades de monitoramento envolve a realização de avaliações contínuas e/ou independentes para garantir que os outros componentes do controle interno estejam funcionando adequadamente e de acordo com a estrutura do COSO.

E) informação e comunicação;

[ERRADO]: A informação e comunicação envolvem a identificação, captura e comunicação de informações relevantes para permitir que as pessoas cumpram suas responsabilidades, mas não incluem as avaliações contínuas e independentes.

#### Comentários

Segundo o COSO I, o controle interno consiste em 05 (cinco) componentes integrados, conforme descrito a seguir:

a) Ambiente de controle

b) Avaliação de riscos

c) Atividades de controle

d) Informação e comunicação

e) Atividades de monitoramento: uma organização utiliza avaliações contínuas, independentes, ou uma combinação das duas, para se certificar da presença e do funcionamento de cada um dos cinco componentes de controle interno, inclusive a eficácia dos controles nos princípios relativos a cada componente. As avaliações contínuas, inseridas nos processos corporativos nos diferentes níveis da entidade, proporcionam informações oportunas. As avaliações independentes, conduzidas periodicamente, terão escopos e frequências diferentes, dependendo da avaliação de riscos, da eficácia das avaliações contínuas e de outras considerações da administração.

Percebe-se, claramente, que o enunciado faz menção ao componente Monitoramento. (ou Atividades de Monitoramento).

Gabarito: "D".

22. (FGV / ALERJ – Especialista Legislativo – 2017) Na avaliação de sistemas de controle interno concebidos a partir da Estrutura Integrada proposta pelo Committee of Sponsoring Organizations of the Treadway Commission (COSO), a análise sobre as iniciativas da organização para que as pessoas assumam responsabilidade por suas funções de controle interno na busca por objetivos está relacionada ao componente:

**A) avaliação de riscos;**

[ERRADO]: A avaliação de riscos envolve a identificação e análise de riscos relevantes para o alcance dos objetivos da entidade, mas não se refere às iniciativas da organização para que as pessoas assumam responsabilidade por suas funções de controle interno.

**B) atividades de controle;**

[ERRADO]: As atividades de controle são ações estabelecidas para ajudar a garantir que as respostas aos riscos sejam executadas de forma eficaz, mas não incluem as iniciativas da organização para que as pessoas assumam responsabilidade por suas funções de controle interno.

**C) ambiente de controle;**

[CERTO]: O ambiente de controle estabelece a base para os demais componentes do controle interno e inclui as iniciativas da organização para que as pessoas assumam responsabilidade por suas funções de controle interno na busca por objetivos.

**D) fixação de objetivos;**

[ERRADO]: A fixação de objetivos envolve a definição de metas claras e alcançáveis para a organização, mas não se refere às iniciativas da organização para que as pessoas assumam responsabilidade por suas funções de controle interno.

**E) monitoramento;**

[ERRADO]: O monitoramento envolve avaliações contínuas e/ou independentes para garantir que os componentes do controle interno estejam funcionando adequadamente, mas não se refere às iniciativas da organização para que as pessoas assumam responsabilidade por suas funções de controle interno.

**Comentários**

A Estrutura (COSO I) estabelece 17 princípios, que representam os conceitos fundamentais associados a cada componente (ambiente de controle, avaliação de riscos, atividades de controle, informação e comunicação, e monitoramento). Um dos princípios associados ao Ambiente de controle é justamente o trazido pelo enunciado. Veja:

**a) Ambiente de controle:**

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.

(...)

Gabarito: "C".

23. (FGV / ALERJ – Especialista Legislativo – 2017) O governo de um ente estatal definiu como uma das políticas quadrienais o desenvolvimento do artesanato em uma região do Estado, conhecida pela tradição com cerâmicas, rendas e bordados. Para tanto, ele pretende subsidiar recursos para treinamento, construção de instalações e aquisição de matérias-primas.

O governo estadual, por meio da Secretaria Estadual de Desenvolvimento Econômico e Social, realizou uma análise quanto à disponibilidade de pessoal para compor um departamento apropriado para implementar, conduzir e acompanhar a operação de concessão de subsídios.

Sob a perspectiva do documento Guidelines for Internal Control Standards for the Public Sector, emitido pelo International Organization of Supreme Audit Institutions (INTOSAI), a análise efetuada está relacionada ao seguinte componente:

**A) monitoramento;**

[ERRADO]: O monitoramento envolve avaliações contínuas e/ou independentes para garantir que os componentes do controle interno estejam funcionando adequadamente, mas não se refere à análise da disponibilidade de pessoal para a implementação de políticas.

**B) avaliação de riscos;**

[ERRADO]: A avaliação de riscos envolve a identificação e análise de riscos relevantes para o alcance dos objetivos da entidade, mas não se refere à análise da disponibilidade de pessoal para a implementação de políticas.

**C) ambiente de controle;**

[CERTO]: O ambiente de controle inclui a análise da disponibilidade de pessoal para compor um departamento apropriado para implementar, conduzir e acompanhar a operação de concessão de subsídios. A organização e estrutura de pessoal são aspectos importantes do ambiente de controle.

**D) informação e comunicação;**

[ERRADO]: A informação e comunicação envolvem a identificação, captura e comunicação de informações relevantes para permitir que as pessoas cumpram suas responsabilidades, mas não se referem à análise da disponibilidade de pessoal para a implementação de políticas.

**E) procedimentos de controle;**

[ERRADO]: Procedimentos de controle são ações estabelecidas para ajudar a garantir que as respostas aos riscos sejam executadas de forma eficaz, mas não incluem a análise da disponibilidade de pessoal para a implementação de políticas.



## Comentários

O documento *Guidelines for Internal Control Standards for the Public Sector* (da Intosai) traz informações alinhadas às diretrizes do COSO I, com algumas diferenças. Vejamos alguns de seus pontos importantes:

Controle interno é um processo integrado efetuado pela direção e corpo de funcionários, e é estruturado para enfrentar os riscos e fornecer razoável segurança de que na consecução da missão da entidade os seguintes objetivos gerais serão alcançados:

- execução ordenada, ética, econômica, eficiente e eficaz das operações;
- cumprimento das obrigações de accountability;
- cumprimento das leis e regulamentos aplicáveis;
- salvaguarda dos recursos para evitar perdas, mau uso e dano.

Percebam que são apresentados 04 (quatro) “objetivos gerais” (ao invés das 03 “categorias de objetivos trazidas pelo COSO I).

Já os componentes do Controle Interno são os mesmos 05 previstos no COSO I (ambiente de controle, avaliação de riscos, procedimentos de controle, informação e comunicação, e monitoramento).

O documento prevê ainda, como elementos do ambiente de controle, o seguinte:

- (1) a integridade pessoal e profissional e os valores éticos da direção e do quadro de pessoal, incluindo uma atitude de apoio ao controle interno, durante todo o tempo e por toda a organização;
- (2) competência;
- (3) o “perfil dos superiores” (ou seja, a filosofia da direção e o estilo gerencial);
- (4) estrutura organizacional;
- (5) políticas e práticas de recursos humanos.

Reparem então que a “análise quanto à disponibilidade de pessoal para compor um departamento” está ligada ao componente Ambiente de controle, uma vez que este inclui, entre outros elementos, integridade, valores éticos e competência das pessoas, a maneira pela qual a gestão delega autoridade e responsabilidades, a estrutura de governança organizacional e as políticas e práticas de recursos humanos.

Gabarito: “C”.

24. (FGV / TCM SP – Agente de Fiscalização – 2015) O Comitê das Organizações Patrocinadoras da Comissão Treadway (COSO, na sigla em inglês) apresentou, em 1992, um modelo amplamente aceito para o estabelecimento de controles internos denominado “Controle Interno – Estrutura Integrada” – aplicável a entidades de grande, médio e pequeno portes, com ou sem fins lucrativos, bem como ao setor público –, que ficou popularmente conhecido como COSO I.

Segundo esse modelo, controle interno:

A) é um processo de trabalho que deve ficar a cargo da unidade de auditoria interna de cada entidade;

[ERRADO]: O controle interno não é apenas um processo de trabalho a cargo da unidade de auditoria interna, mas envolve todos os membros da organização e suas atividades.

B) é um processo conduzido pela estrutura de governança, pela administração e por pessoas da organização;

[CERTO]: O controle interno é um processo conduzido pela estrutura de governança, pela administração e por pessoas da organização, projetado para fornecer segurança razoável em relação ao alcance dos objetivos da entidade.

C) é um processo que consiste de tarefas que devem ser realizadas ao menos uma vez em cada exercício financeiro;

[ERRADO]: O controle interno é um processo contínuo, não se limita a tarefas que devem ser realizadas apenas uma vez em cada exercício financeiro.

D) visa proporcionar certeza de que os objetivos da entidade serão alcançados;

[ERRADO]: O controle interno visa proporcionar segurança razoável, e não certeza, de que os objetivos da entidade serão alcançados.

E) não auxilia a organização a prever eventos externos que possam afetar negativamente o alcance de seus objetivos.

[ERRADO]: O controle interno auxilia a organização na identificação e na avaliação de riscos, incluindo eventos externos que possam afetar negativamente o alcance de seus objetivos. Embora não possa prever todos os eventos externos, contribui para uma melhor tomada de decisão e gerenciamento de riscos.

Comentários: De acordo com o COSO I, Controle interno é um processo conduzido pela estrutura de governança, administração e outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade.

25. (FGV / TCM SP – Agente de Fiscalização – 2015) O Comitê das Organizações Patrocinadoras da Comissão Treadway (COSO, na sigla em inglês) publicou, em 2004, o modelo denominado “Gerenciamento de Riscos Corporativos” (ERM, na sigla em inglês), popularizado como COSO II.

Segundo esse modelo, as quatro categorias de objetivos comuns à maioria das organizações são:

A) objetivos contábeis; objetivos de controle; objetivos estratégicos e objetivos de salvaguarda de ativos;

[ERRADO]: Essas não são as categorias de objetivos estabelecidas pelo modelo COSO II.

B) objetivos estratégicos; objetivos sociais; objetivos de lucro e objetivos de divulgação;

[ERRADO]: Essas não são as categorias de objetivos estabelecidas pelo modelo COSO II.

C) objetivos estratégicos; objetivos operacionais; objetivos de comunicação e objetivos de conformidade;

[CERTO]: De acordo com o Manual de Gerenciamento de Riscos Corporativos — Estrutura Integrada (COSO II), as categorias de objetivos são: objetivos estratégicos, objetivos operacionais, objetivos de relatórios (comunicação) e objetivos de conformidade.

D) objetivos de conformidade; objetivos de comunicação; objetivos de relacionamento com partes interessadas e objetivos ambientais e de sustentabilidade;

[ERRADO]: Essas não são as categorias de objetivos estabelecidas pelo modelo COSO II.

E) objetivos de comunicação; objetivos operacionais; objetivos de relacionamento com partes interessadas e objetivos ambientais e de sustentabilidade.

[ERRADO]: Essas não são as categorias de objetivos estabelecidas pelo modelo COSO II.

#### Comentários

Segundo o Manual de Gerenciamento de Riscos Corporativos — Estrutura Integrada (COSO II): Essa estrutura de gerenciamento de riscos corporativos é orientada a fim de alcançar os objetivos de uma organização e são classificados em quatro categorias:

Estratégicos – metas gerais, alinhadas com o que suportem à sua missão.

Operações – utilização eficaz e eficiente dos recursos.

Comunicação – confiabilidade de relatórios.

Conformidade – cumprimento de leis e regulamentos aplicáveis.

Gabarito: “C”.

26. (FGV / CODEMIG – Analista de Desenvolvimento Econômico – 2015) A definição mais amplamente aceita de controles internos é a proposta pelo Committee of Sponsoring Organizations of the Treadway Commission (COSO), que concebe o controle interno como um processo integrado, executado pela administração e outras pessoas da entidade, desenhado para fornecer razoável segurança sobre o alcance de objetivos nas seguintes categorias: eficácia e eficiência operacional, mensuração de desempenho e divulgação financeira, proteção de ativos e cumprimento de leis e regulamentações.

Quando, em uma entidade, se procede à avaliação quanto à definição adequada de competências e atribuições de cada função no regimento interno de uma entidade, o componente do Controle Interno da Estrutura de COSO contemplado é:

**a) ambiente de controle;**

[CERTO]: O ambiente de controle é o componente do Controle Interno da Estrutura de COSO que estabelece a base para o sistema de controle interno, incluindo a definição de estrutura organizacional, atribuição de autoridade e responsabilidade, e políticas e procedimentos.

**b) avaliação de riscos;**

[ERRADO]: A avaliação de riscos é o processo de identificar e analisar riscos relevantes para o alcance dos objetivos, o que não é o foco nesta situação.

**c) procedimentos de controle;**

[ERRADO]: Procedimentos de controle são atividades que ajudam a garantir que as ações gerenciais necessárias sejam tomadas para lidar com os riscos identificados, não abordando diretamente a definição de competências e atribuições.

**d) informação e comunicação;**

[ERRADO]: Informação e comunicação é o componente que trata da identificação, captura e comunicação de informações relevantes, não abordando diretamente a definição de competências e atribuições.

**e) monitoramento;**

[ERRADO]: Monitoramento é o processo de avaliação contínua e/ou independente do funcionamento dos componentes do controle interno, não abordando diretamente a definição de competências e atribuições.

Comentários: Como vimos ao longo da aula, competência (atração, retenção e desenvolvimento de talentos competentes) e atribuição de funções (delegação de autoridade e responsabilidade) são elementos do Ambiente de Controle. Gabarito: "A".

27. (FGV / TJ PI – Auditor – 2015) Uma entidade fez a opção de implantar seu sistema de controle interno a partir da Estrutura Integrada de Controle Interno proposta pelo COSO. A Estrutura proposta pelo COSO se desdobra em princípios, que representam os conceitos fundamentais associados a cada componente do Controle Interno.

Dentre as iniciativas da entidade, está a criação de um plano para desenvolvimento e retenção de talentos humanos. Essa iniciativa está em consonância com o componente:

**a) ambiente de controle;**

[CERTO]: 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 o desenvolvimento e retenção de talentos humanos.

**b) atividades de controle;**

[ERRADO]: Atividades de controle são ações que ajudam a garantir que as ações gerenciais necessárias sejam tomadas para lidar com os riscos identificados, não abordando diretamente o desenvolvimento e retenção de talentos humanos.

**c) avaliação de riscos;**

[ERRADO]: A avaliação de riscos é o processo de identificar e analisar riscos relevantes para o alcance dos objetivos, não abordando diretamente o desenvolvimento e retenção de talentos humanos.

**d) informação e comunicação;**

[ERRADO]: Informação e comunicação é o componente que trata da identificação, captura e comunicação de informações relevantes, não abordando diretamente o desenvolvimento e retenção de talentos humanos.

**e) monitoramento;**

[ERRADO]: Monitoramento é o processo de avaliação contínua e/ou independente do funcionamento dos componentes do controle interno, não abordando diretamente o desenvolvimento e retenção de talentos humanos.

**Comentários**

Um dos princípios que apoiam os componentes do Controle Interno, relacionado ao Ambiente de controle, é o comprometimento que a organização demonstra para atrair, desenvolver e reter talentos competentes, em linha com seus objetivos. Gabarito: "A".

28. (FGV / CM Recife – Consultor Legislativo – 2014) De acordo com as diretrizes para as normas de controle interno divulgadas pelo COSO (Committee of Sponsoring Organizations of the Treadway Commission) e pela INTOSAI (International Organisation of Supreme Audit Institutions), o controle interno é estruturado para oferecer segurança razoável de que os objetivos gerais da entidade estão sendo alcançados e compreende cinco componentes interrelacionados. O princípio que preconiza que a organização faz com que as pessoas assumam responsabilidade por suas funções de controle interno na busca pelos objetivos está relacionado ao componente de:

**a) ambiente de controle;**

[CERTO]: 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.

**b) atividades de controle;**

[ERRADO]: Atividades de controle são ações que ajudam a garantir que as ações gerenciais necessárias sejam tomadas para lidar com os riscos identificados, não abordando diretamente a responsabilidade das pessoas por suas funções de controle interno.

**c) atividades de monitoramento;**

[ERRADO]: Monitoramento é o processo de avaliação contínua e/ou independente do funcionamento dos componentes do controle interno, não abordando diretamente a responsabilidade das pessoas por suas funções de controle interno.

**d) avaliação de riscos;**

[ERRADO]: A avaliação de riscos é o processo de identificar e analisar riscos relevantes para o alcance dos objetivos, não abordando diretamente a responsabilidade das pessoas por suas funções de controle interno.

**e) informação e comunicação;**

[ERRADO]: Informação e comunicação é o componente que trata da identificação, captura e comunicação de informações relevantes, não abordando diretamente a responsabilidade das pessoas por suas funções de controle interno.

**Comentários**

Um dos princípios que apoiam os componentes do Controle Interno, relacionado ao Ambiente de controle, é o que preconiza que a organização faz com que as pessoas assumam responsabilidade por suas funções de controle interno na busca pelos objetivos. Gabarito: "A".

29. (FGV / CM Recife – Gestor de Controle Interno – 2014) A Assessoria de Tecnologia da Informação de uma prefeitura municipal está desenvolvendo protocolos de segurança para envio, recebimento e armazenagem de informações relacionadas às atividades desenvolvidas pelas secretarias e demais órgãos do município. Do ponto de vista dos componentes do controle interno, esse procedimento está circunscrito ao componente de:

a) ambiente de controle;

[ERRADO]: O ambiente de controle 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, mas não trata diretamente de protocolos de segurança de informação.

b) atividades de controle;

[ERRADO]: Atividades de controle são ações que ajudam a garantir que as ações gerenciais necessárias sejam tomadas para lidar com os riscos identificados, não abordando diretamente os protocolos de segurança de informação.

c) atividades de monitoramento;

[ERRADO]: Monitoramento é o processo de avaliação contínua e/ou independente do funcionamento dos componentes do controle interno, não abordando diretamente os protocolos de segurança de informação.

d) avaliação de riscos;

[ERRADO]: A avaliação de riscos é o processo de identificar e analisar riscos relevantes para o alcance dos objetivos, não abordando diretamente os protocolos de segurança de informação.

e) informação e comunicação;

[CERTO]: Informação e comunicação é o componente que trata da identificação, captura e comunicação de informações relevantes, incluindo protocolos de segurança para envio, recebimento e armazenagem de informações.

Comentários

No caso do enunciado, a entidade está desenvolvendo uma atividade de controle, relacionada a procedimentos de segurança de informações. Vejam que, de acordo com a definição abaixo, as atividades de controle são desempenhadas também no ambiente tecnológico (como no caso do enunciado).

Segundo o COSO I, atividades de controle são ações estabelecidas por meio de políticas e procedimentos que ajudam a garantir o cumprimento das diretrizes determinadas pela

administração para mitigar os riscos à realização dos objetivos. As atividades de controle são desempenhadas em todos os níveis da entidade, em vários estágios dentro dos processos corporativos e no ambiente tecnológico. Podem ter natureza preventiva ou de detecção e abranger uma série de atividades manuais e automáticas, como autorizações e aprovações, verificações, reconciliações e revisões de desempenho do negócio.

Gabarito: “B”.



30. (CESGRANRIO – Auditor (PETROBRAS)/Júnior /2018) Tendo em vista a estrutura integrada de controle interno proposta pelo Committee of Sponsoring Organization of the Treadway Commission (COSO), o compromisso da administração em obter ou gerar e utilizar informações importantes e de qualidade, originadas tanto de fontes internas quanto externas, está relacionado ao componente de

**a) ambiente de controle**

[ERRADO]: O ambiente de controle é a base para o sistema de controle interno e inclui aspectos como integridade, valores éticos e filosofia de gestão, mas não aborda diretamente a obtenção e utilização de informações.

**b) conformidade do controle**

[ERRADO]: Essa alternativa não corresponde a um componente da estrutura integrada de controle interno proposta pelo COSO.

**c) informação e comunicação**

[CERTO]: O componente de informação e comunicação trata da identificação, captura e comunicação de informações relevantes, incluindo a obtenção e utilização de informações de qualidade originadas de fontes internas e externas.

**d) monitoramento**

[ERRADO]: O monitoramento é o processo de avaliação contínua e/ou independente do funcionamento dos componentes do controle interno, não abordando diretamente a obtenção e utilização de informações.

**e) unidade operacional**

[ERRADO]: Essa alternativa não corresponde a um componente da estrutura integrada de controle interno proposta pelo COSO.

**Comentários**

Segundo o COSO I, o controle interno consiste em 05 (cinco) componentes integrados, conforme descrito a seguir:

a) Ambiente de controle: é um conjunto de normas, processos e estruturas que fornece a base para a condução do controle interno por toda a organização. A estrutura de governança e a alta administração estabelecem uma diretriz sobre a importância do controle interno, inclusive das normas de conduta esperadas. A administração reforça as expectativas nos vários níveis da organização.

O ambiente de controle abrange a integridade e os valores éticos da organização; os parâmetros que permitem à estrutura de governança cumprir com suas responsabilidades de supervisionar a governança; a estrutura organizacional e a delegação de autoridade e responsabilidade; o processo de atrair, desenvolver e reter talentos competentes; e o rigor em torno de medidas, incentivos e recompensas por performance. O ambiente de controle resultante tem impacto pervasivo sobre todo o sistema de controle interno.

b) Avaliação de riscos: Toda entidade enfrenta vários riscos de origem tanto interna quanto externa. Define-se risco como a possibilidade de que um evento ocorra e afete adversamente a realização dos objetivos. A avaliação de riscos envolve um processo dinâmico e iterativo para identificar e avaliar os riscos à realização dos objetivos.

c) Atividades de controle: são ações estabelecidas por meio de políticas e procedimentos que ajudam a garantir o cumprimento das diretrizes determinadas pela administração para mitigar os riscos à realização dos objetivos. As atividades de controle são desempenhadas em todos os níveis da entidade, em vários estágios dentro dos processos corporativos e no ambiente tecnológico. Podem ter natureza preventiva ou de detecção e abranger uma série de atividades manuais e automáticas, como autorizações e aprovações, verificações, reconciliações e revisões de desempenho do negócio. A segregação de funções é geralmente inserida na seleção e no desenvolvimento das atividades de controle.

d) Informação e comunicação: a informação é necessária para que a entidade cumpra responsabilidades de controle interno a fim de apoiar a realização de seus objetivos. A administração obtém ou gera e utiliza informações importantes e de qualidade, originadas tanto de fontes internas quanto externas, a fim de apoiar o funcionamento de outros componentes do controle interno. A comunicação é o processo contínuo e iterativo de proporcionar, compartilhar e obter as informações necessárias. A comunicação interna é o meio pelo qual as informações são transmitidas para a organização, fluindo em todas as direções da entidade. Ela permite que os funcionários recebam uma mensagem clara da alta administração de que as responsabilidades pelo controle devem ser levadas a sério. A comunicação externa apresenta duas vertentes: permite o recebimento, pela organização, de informações externas significativas, e proporciona informações a partes externas em resposta a requisitos e expectativas.

e) Atividades de monitoramento: uma organização utiliza avaliações contínuas, independentes, ou uma combinação das duas, para se certificar da presença e do funcionamento de cada um dos cinco componentes de controle interno, inclusive a eficácia dos controles nos princípios relativos a cada componente. As avaliações contínuas, inseridas nos processos corporativos nos diferentes níveis da entidade, proporcionam informações oportunas. As avaliações independentes, conduzidas periodicamente, terão escopos e frequências diferentes, dependendo da avaliação de riscos, da eficácia das avaliações contínuas e de outras considerações da administração.

Portanto, alternativa correta é C.

Gabarito: "C".

31. (CESGRANRIO - Auditor (PETROBRAS)/Júnior /2018) Uma das necessidades para assegurar o cumprimento dos objetivos do controle interno é o monitoramento contínuo do sistema de controle adotado. Em relação ao controle interno, considere os seguintes itens de verificação:

I - A organização demonstra ter comprometimento com a integridade e os valores.

ERRADO: ambiente de controle.

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

ERRADO: atividade de controle.

III - As verificações internas protegem adequadamente os ativos da entidade contra fraudes.

CERTO: atividades de monitoramento.

IV - O potencial para fraude é considerado na avaliação dos riscos à realização dos objetivos da entidade.

ERRADO: avaliação de riscos.

V - Os controles contábeis asseguram o correto registro das transações financeiras.

CERTO: atividades de monitoramento.

Os itens de verificação que se referem a atividades típicas de monitoramento são, APENAS, as de números:

a) I e II

b) II e III

c) II e IV

d) III e V

e) IV e V

#### Comentários

Analisando os itens e relacionando-os a cada componente do controle interno, segundo a estrutura do Coso I, temos o seguinte:

I - A organização demonstra ter comprometimento com a integridade e os valores. Refere-se ao

II - A organização seleciona e desenvolve atividades gerais de controle sobre a tecnologia para apoiar a realização dos objetivos. Refere-se à

III - As verificações internas protegem adequadamente os ativos da entidade contra fraudes. Isso é feito com avaliações contínuas. Refere-se às

IV - O potencial para fraude é considerado na avaliação dos riscos à realização dos objetivos da entidade. Refere-se à

V - Os controles contábeis asseguram o correto registro das transações financeiras. Referem-se às

Portanto, alternativa correta é D.

Gabarito: "D".