CRCCE

CONSELHO REGIONAL DE CONTABILIDADE
DO CEARÁ

Controles internos nas organizações

- Professor André Marinoni Ribeiro de Sousa

Introdução aos Controles Internos

➢ Os controles internos são mecanismos, geralmente formalizados por escrito nas políticas e procedimentos da empresa, que, além de minimizar riscos operacionais e de integridade, asseguram que os livros e registros contábeis e financeiros reflitam completa e precisamente os negócios e operações da empresa. Entre outras coisas, os controles internos estabelecem as regras para revisão e aprovação de atividades (especialmente aquelas ligadas a compromissos contratuais e despesas), existência das atividades (para se evitar pagamentos por serviços não-prestados, por exemplo), documentação suporte, processamento e registro das transações.

- Os Controles Internos são influenciados pelas pessoas em todos os níveis das empresas. Políticas, manuais, formulários, processos não existem sem pessoas.;
- Os Controles Internos visam a realização de objetivos em um ou mais processos que podem ser separados ou sobrepostos.

➢ Os Controles Internos podem ser considerados eficientes e eficazes se a Alta Direção tiver uma segurança razoável de que:

- Os objetivos das operações da empresa estão sendo alcançados (objetivos das operações);
- As demonstrações financeiras publicadas são preparadas de maneira confiável (objetivos de relatórios financeiros);
- As leis e regulamentos aplicáveis estão sendo cumpridos (objetivo de conformidade).

Os principais pilares de um sistema efetivo de Controles Internos numa empresa.

Relação Custo/Benefício:

- O benefício de um controle interno consiste na redução do risco de falhas e no cumprimento dos objetivos e metas de uma atividade;
- O conceito básico de custo/benefício reconhece que custo de um controle não deve exceder os benefícios que ele possa proporcionar. Desta maneira, todos os controles devem ser avaliados e a implementação de novos controles deve passar por uma análise de custo/benefício.

Definição de Responsabilidades e Autoridade:

As atribuições e responsabilidades dos colaboradores em uma empresa devem ser bem claras e estabelecidas, bem como a autoridade decorrente das suas funções. Assim sendo, deve haver:

- Procedimentos claramente determinados;
- Um organograma adequado em que a linha de autoridade e a consequente responsabilidade sejam bem definidas;
- A delineação de funções ou atividades, embora possa ser informal, deve, preferivelmente, ser definida em manuais de procedimentos, visto que estes propiciam a eficiência do sistema e evitam erros.

Segregação de Funções:

• Um sistema de controle interno adequado é aquele que elimina a possibilidade de ocorrência de erros ou irregularidades. Assim sendo, os procedimentos destinados a detectar tais erros ou irregularidades devem ser executados por colaboradores que não estejam em posição de praticá-los.
• De uma maneira geral, o sistema de controle interno deve prever segregação entre as funções de aprovação de operações e sua execução e controle, de modo que nenhum colaborador possa ter completa autoridade sobre uma parcela significativa de qualquer operação e/ou atividade

Acesso aos Ativos:

• Para se atingir um grau de segurança adequado, o acesso aos ativos de uma empresa deve ser limitado ao pessoal autorizado.
• O número e o nível dos colaboradores a quem o acesso deve ser autorizado e dependem da natureza do ativo e de sua vulnerabilidade a perdas por meio de erros e irregularidades.
• A limitação ao acesso indireto requer procedimentos de controle onde o conceito de separação de funções seja aplicado.

Estabelecimento de Comprovações e Provas Independentes:

Os procedimentos referentes a determinada atividade devem prever processos de comprovações rotineiras e obtenção, independentemente de informações de controle.

Os registros preparados por uma área para informar sobre os seus resultados são meios de controles eficazes somente quando produzidos por um sistema adequado, que permita assegurar a veracidade das informações por meio de registros produzidos por fontes independentes.

•Exemplo:

Comparação do relatório sobre os resultados de um setor de produção com o relatório do setor de controle de qualidade.

COSO – Commitee of Sponsoring Organizations of Treadway Commission:

O COSO - Committee of Sponsoring Organizations of the Treadway Commission (em português: **Comitê das Organizações Patrocinadoras da Comissão Treadway**) é um direcionador de Sistema de Controles Internos, elaborado por uma entidade norte-americana, dedicada à melhoria dos relatórios financeiros por meio da observância de princípios éticos e da efetividade dos Controles Internos e Governança Corporativa. Usualmente, as organizações se baseiam na metodologia do **COSO** para definirem seus controles internos, de maneira integrada à gestão de riscos. Isso também se aplica à definição dos controles dentro de um Programa de Integridade, cujos principais objetivos são:

- Proteger a organização e seus colaboradores; e
- Mitigar os riscos inerentes da sua atuação e do exercício das atividades por parte de colaboradores, parceiros e fornecedores.

COSO – Commitee of Sponsoring Organizations of Treadway Commission:

O COSO - Committee of Sponsoring Organizations of the Treadway Commission (em português: **Comitê das Organizações Patrocinadoras da Comissão Treadway**) é um direcionador de Sistema de Controles Internos, elaborado por uma entidade norte-americana, dedicada à melhoria dos relatórios financeiros por meio da observância de princípios éticos e da efetividade dos Controles Internos e Governança Corporativa. Usualmente, as organizações se baseiam na metodologia do **COSO** para definirem seus controles internos, de maneira integrada à gestão de riscos. Isso também se aplica à definição dos controles dentro de um Programa de Integridade, cujos principais objetivos são:

• Proteger a organização e seus colaboradores; e

• Mitigar os riscos inerentes da sua atuação e do exercício das atividades por parte de colaboradores, parceiros e fornecedores.

COSO – Estrutura

COSO – Elementos

- Ambiente de Controle (postura da organização e conscientização dos colaboradores);
- Avaliação de Riscos (identificação e avaliação de riscos relevantes para alcançar os objetivos definidos);
- Atividades de Controle (políticas e procedimentos para garantir a observância das diretrizes e medidas de prevenção dos riscos);
- Informações e Comunicações (fluxos das informações e comunicações dentro da organização);
- Monitoramento (Processos de monitoramento e avaliação do sistema e dos demais processos).

COSO – Categorias

• Estratégicos – Foco nos objetivos e minimiza os perigos e surpresas no seu percurso;
• Operacional – Eficácia e à eficiência das operações;
• Comunicação – Divulgação financeira e não financeira, interna e externa (confiabilidade, transparência etc.);
• Conformidade – Cumprimento de leis e regulamentações.

COSO – Benefícios

- Uniformiza definições de controle interno;
- Define componentes, objetivos e objetos do controle interno em um modelo integrado;
- Esboça responsabilidades da administração;
- Estabelece padrões para implementação e validação;
- Cria um meio para monitorar, avaliar e reportar controles internos.

Importância dos controles internos para programas de integridade:

- Como vimos anteriormente, uma boa gestão de controles internos é muito importante para o sucesso do Programa de Integridade!
- Pois são através desses controles que a empresa pode mitigar os seus riscos de integridade e garantir a efetividade do seu Programa de Integridade. Esses controles podem ser classificados de acordo com seus propósitos:

Modelo: Classificação dos controles em preventivo e detectivo

Propósito do controles	Exemplos
Preventivo	▪ Assinatura periódica por todos os colaboradores, atestando a ciência e concordância com o Código de Conduta. ▪ Aprovação dos pedidos de concessão de brindes e hospitalidades. ▪ Controle de presença nos treinamentos de integridade. ▪ Execução da "due diligence" antes das contratação de um parceiro comercial.
Detectivo	▪ Aprovação de pagamentos considerados de alto risco. ▪ Verificação das transações nas contas-correntes do último período. ▪ Verificação da contabilização das despesas de patrocínios.

Módulo Classificação dos controles de acordo com suas naturezas

Natureza dos controles	Exemplos
Controle	▪ São controles regulares de integridade que visam a **mitigação de riscos** pela entidade, principalmente através de verificação e aprovação.
Teste	▪ São processos cuja finalidade é verificar a efetividade do controle.

Frequência dos controles e testes:

É necessário estabelecer a periodicidade de realização dos controles e/ou testes de acordo com os riscos de cada processo. Naturalmente, na implementação do Programa de Integridade, costuma-se aplicar um rigor mais elevado, pois a organização ainda não tem parâmetros nem histórico anterior para balizar a definição.

Com o passar do tempo, os resultados apurados possibilitam contribuir para a flexibilização daqueles processos menos críticos, principalmente decorrentes de:

- Resultados com zero ou baixíssimo índices de falhas nas amostras;
- Baixo risco apurado no período.

“Normalmente, para os casos mais críticos, as organizações optam por frequências mensais, trimestrais ou anuais.”

Metodologia e documentação

Selecionar o método, documentar de maneira adequada e seguir com rigor os critérios estabelecidos são fundamentais nesse processo. Para isso, convém estarem explícitos e claros os seguintes itens:

- Qual o critério utilizado para seleção de amostras e análise do resultado?
- Qual o período da ocorrência dos eventos?
- Quais as amostras selecionadas e de qual universo do evento foram coletadas?
- Quais os resultados e as evidências da análise de cada amostra?
- Quais conclusões finais obtidas sobre a eficiência dos processos?

Seleção de amostras

Amostra significa o volume mínimo de ocorrências a verificar-se em um processo de avaliação, para assegurar a eficácia de um controle ou teste. Evento consiste na ocorrência de determinada atividade que caracteriza o atendimento de um ou mais requisitos do Programa de Integridade, como:

- Transação bancária;
- Um pagamento de risco;
- Realização de um treinamento;
- A assinatura de recebimento de um Código de Conduta;
- Reembolso de uma despesa;
- Aprovação de um contrato etc.

Seleção de amostras

Amostra significa o volume mínimo de ocorrências a verificar-se em um processo de avaliação, para assegurar a eficácia de um controle ou teste. Evento consiste na ocorrência de determinada atividade que caracteriza o atendimento de um ou mais requisitos do Programa de Integridade, como:

- Transação bancária;
- Um pagamento de risco;
- Realização de um treinamento;
- A assinatura de recebimento de um Código de Conduta;
- Reembolso de uma despesa;
- Aprovação de um contrato etc.

Atenção:

• Nesta etapa, é muito importante as pessoas terem habilidade suficiente para a implementação desses controles, para não gerar conflitos ou atritos desnecessários.
• Com educação e um discurso conciliador para demonstrar a importância desses processos de controles, nunca é demais.
• A implementação dos controles internos é de vital importância para a implementação do Programa de Integridade, pois é por meio desses controles que se mitiga os riscos mapeados durante a avaliação de riscos.

Lei Sarbanes Oxley (SOX):

O que é a Lei Sarbanes-oxley?

• Também conhecida como **Lei Sarbanes-Oxley**, a SOx foi sancionada em 2002 pelo Congresso dos Estados Unidos para proteger investidores e demais stakeholders dos erros das escriturações contábeis e práticas fraudulentas.

Qual o objetivo da Lei Sarbanes Oxley?

• A **Lei Sarbanes-Oxley** é uma reação da legislação americana aos escândalos financeiros da Enron, WorldCom, entre outros. Foi promulgada em janeiro de 2002, nos Estados Unidos. Esta **lei** estabelece regras para Governança Corporativa relativas à divulgação e à emissão de relatórios financeiros.

• Visa garantir a criação de mecanismos de auditoria e segurança confiáveis nas empresas, incluindo ainda regras para a criação de comitês encarregados de supervisionar suas atividades e operações, de modo a mitigar riscos aos negócios, evitar a ocorrência de fraudes ou assegurar que haja meios de identificá-las quando ocorrem, garantindo a transparência na gestão das empresas.

Lei Sarbanes Oxley (SOX):

Requisitos da lei

1. Controlar a criação, edição e versionamento dos documentos em um ambiente de acordo com os padrões ISO, para controle de todos os documentos relativos à seção 404;

2. Cadastrar os riscos associados aos processos de negócios e armazenar os desenhos de processo;

3. Utilizar ferramentas como editor de texto e planilha eletrônica para criação e alteração dos documentos da seção 404;

4. Publicar em múltiplos websites os conteúdos da seção 404;

5. Gerenciar todos os documentos controlando seus períodos de retenção e distribuição;

6. Digitalizar e armazenar todos os documentos que estejam em papel, ligados à seção 404.

Lei Sarbanes Oxley (SOX):

Seção 404

A seção 404 determina uma avaliação anual dos controles e procedimentos internos para emissão de relatórios financeiros. Além disso, o auditor independente da companhia deve emitir um relatório distinto, que ateste a asserção da administração sobre a eficácia dos controles internos e dos procedimentos executados para a emissão dos relatórios financeiros.

Governança corporativa:

Governança corporativa: Consiste no quadro completo de processos, costumes (cultura), políticas, regulamentos, leis e instituições que monitoram a maneira como as empresas são dirigidas, administradas ou controladas. Governança também consiste no estudo sobre as relações entre os diversos atores envolvidos (os stakeholders) e os objetivos pelos quais a empresa se orienta. Os principais atores tipicamente são os acionistas, a alta administração e o conselho de administração.

Principais características da boa governança:

1. Transparência
2. Responsabilidade
3. Orientação por consenso
4. Igualdade e inclusividade
5. Efetividade e eficiência
6. Prestação de contas (accountability)

Avaliação de riscos:

1. A avaliação de riscos é um processo integrado que envolve a identificação e a análise dos riscos aos quais uma organização está exposta, bem como a elaboração e a adoção de estratégias para evitá-los, minimizá-los e enfrentá-los, caso aconteçam. De acordo com a Pesquisa Global sobre Crises, realizada em 2019 pela PwC, sete a cada dez organizações já enfrentaram, pelo menos, uma crise nos últimos cinco anos, e, entre elas, o número médio de crises enfrentadas é superior a três.

2. Estrutura fundamental para manutenção e longevidade de uma organização, pois através dessa vertente empresas procuram identificar ameaças e potencialidades para blindagem do negócio.

1. Quais a principais etapas no processo de auditoria?

2. Quais organizações são obrigadas a passar por auditoria?

3. Como ocorre o planejamento de auditoria e quais os principais aspectos de controle levados em consideração?

4. Em que consiste o relatório de controle publicado na CVM para investidores?

1. Quem é a CVM?

.

2. A qual ministério está ligada a CVM?

3. Criada pela Lei nº 6.385 de 1976.

4. Quais as principais atribuições da CVM?

5. Em que consiste o relatório de controle publicado na CVM para investidores?

1. O que é LGPD (Lei 13.709 aprovada em agosto de 2018)?

2. Qual o objetivo principal dessa lei?

3. Qual o impacto da lei para as grandes organizações?

4. Que tipo de medidas as empresas tiveram que adotar com o surgimento da lei?

5. Qual os principais controles que as empresas tiveram que adotar com o surgimento da lei?

Para continuar

Agora que você deu um giro, leia a seguir mais detalhes sobre os principais pontos apresentados na imagem acima

A LGPD é a lei nº 13.709, aprovada em agosto de 2018 e com vigência a partir de agosto de 2020. Para entender a importância do assunto, é necessário saber que a nova lei quer criar um cenário de segurança jurídica, com a padronização de normas e práticas, para promover a proteção, de forma igualitária e dentro do país e no mundo, aos dados pessoais de todo cidadão que esteja no Brasil. E, para que não haja confusão, a lei traz logo de cara o que são dados pessoais, define que há alguns desses dados sujeitos a cuidados ainda mais específicos, como os sensíveis e os sobre crianças e adolescentes, e que dados tratados tanto nos meios físicos como nos digitais estão sujeitos à regulação.

A LGPD estabelece ainda que não importa se a sede de uma organização ou o centro de dados dela estão localizados no Brasil ou no exterior: se há o processamento de conteúdo de pessoas, brasileiras ou não, que estão no território nacional, a LGPD deve ser cumprida. Determina também que é permitido compartilhar dados com organismos internacionais e com outros países, desde que isso ocorra a partir de protocolos seguros e/ou para cumprir exigências legais.

Consentimento

Outro elemento essencial da LGPD é o consentir. Ou seja, o consentimento do cidadão é a base para que dados pessoais possam ser tratados. Mas há algumas exceções a isso. É possível tratar dados sem consentimento se isso for indispensável para: cumprir uma obrigação legal; executar política pública prevista em lei; realizar estudos via órgão de pesquisa; executar contratos; defender direitos em processo; preservar a vida e a integridade física de uma pessoa; tutelar ações feitas por profissionais das áreas da saúde ou sanitária; prevenir fraudes contra o titular; proteger o crédito; ou atender a um interesse legítimo, que não fira direitos fundamentais do cidadão.

Automatização com autorização

Por falar em direitos, é essencial saber que a lei traz várias garantias ao cidadão, que pode solicitar que dados sejam deletados, revogar um consentimento, transferir dados para outro fornecedor de serviços, entre outras ações. E o tratamento dos dados deve ser feito levando em conta alguns quesitos, como finalidade e necessidade, que devem ser previamente acertados e informados ao cidadão. Por exemplo, se a finalidade de um tratamento, feito exclusivamente de modo automatizado, for construir um perfil (pessoal, profissional, de consumo, de crédito), o indivíduo deve ser informado que pode intervir, pedindo revisão desse procedimento feito por máquinas.

ANPD e agentes de tratamento

E tem mais. Para a lei a "pegar", o país contará com a Autoridade Nacional de Proteção de Dados Pessoais, a ANPD. A instituição vai fiscalizar e, se a LGPD for descumprida, penalizar. Além disso, a ANPD terá, é claro, as tarefas de regular e de orientar, preventivamente, sobre como aplicar a lei. Cidadãos e organizações poderão colaborar com a autoridade.

Mas não basta a ANPD - que está em formação - e é por isso que a Lei Geral de Proteção de Dados Pessoais também estipula os agentes de tratamento de dados e suas funções, nas organizações: tem o controlador, que toma as decisões sobre o tratamento; o operador, que realiza o tratamento, em nome do controlador; e o encarregado, que interage com cidadãos e autoridade nacional (e poderá ou não ser exigido, a depender do tipo ou porte da organização e do volume de dados tratados).

Gestão em foco

Há um outro item que não poderia ficar de fora: a administração de riscos e falhas. Isso quer dizer que quem gere base de dados pessoais terá que redigir normas de governança; adotar medidas preventivas de segurança; replicar boas práticas e certificações existentes no mercado. Terá ainda que elaborar planos de contingência; fazer auditorias; resolver incidentes com agilidade. Se ocorrer, por exemplo, um vazamento de dados, a ANPD e os indivíduos afetados devem ser imediatamente avisados. Vale lembrar que todos os agentes de tratamento sujeitam-se à lei. Isso significa que as organizações e as subcontratadas para tratar dados respondem em conjunto pelos danos causados. E as falhas de segurança podem gerar multas de até 2% do faturamento anual da organização no Brasil – e no limite de R$ 50 milhões por infração. A autoridade nacional fixará níveis de penalidade segundo a gravidade da falha. E enviará, é claro, alertas e orientações antes de aplicar sanções às organizações.