DIONETE FRANCESCHI

# A IMPORTÂNCIA DO GERENCIAMENTO DOS RISCOS EMPRESARIAIS, EMBASADA NO MODELO COSO (*COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION)*

Monografia apresentada ao Departamento de Ciências Contábeis, do Setor de Ciências Sociais Aplicadas da UFPr, como requisito parcial para a obtenção do título de especialista no Curso de Pós-Graduação em Gestão de Negócios.

Orientador: Prof. Dr. Vicente Pacheco

CURITIBA

2005

# RESUMO

Franceschi, Dionete. **A importância do gerenciamento dos riscos empresariais, embasada no modelo COSO (*Committee of Sponsoring Organizations of the Treadway Commission).*** Há riscos em todos os ambientes, em todos os lados, que podem impactar negativamente o negócio da sua companhia. Devido a esse fato, e a regulamentações propostas a auxiliar os empresários a criar uma visão de riscos e de governança corporativa, cada vez mais as empresas estão preocupadas em gerenciar os riscos, adotando controles internos, podendo dessa forma criar oportunidades de melhoria significativas para as empresas, bem como aumentar a competitividade no mercado e facilitar o desenvolvimento de um planejamento estratégico em linha com seus objetivos.

Sendo o gerenciamento de riscos, por intermédio de controles internos embasados no modelo COSO (*Committee Of Sponsoring Organizations Of The Treadway Commission),* o objetivo do trabalho ora apresentado. O COSO é um *framework* que visa atender a lei americana *Sarbanes Oxley*, sendo inclusive o modelo de controles internos sugerido pela mesma voltada para objetivos de negócios, buscando mitigar por meio de controles internos os riscos inerentes ao negócio da empresa.

Os objetivos para implementação de controles internos evidenciados no modelo COSO são:

- ✓ Eficiência e efetividade operacional;
- ✓ Confiança nos registros contábeis/financeiros;
- ✓ Conformidade.

**Palavras-chave:** sistema; controles; auditoria; qualidade; planejamento.

## SUMÁRIO

# 1. INTRODUÇÃO

O mundo empresarial se modifica e se ajusta aos ciclos das grandes quebras e dos escândalos financeiros que vêm abalando o mundo ao longo dos últimos anos e foram protagonizados por grandes potências mundiais, como a Enron, World-Comm, Parmalat, Arthur Andersen e mais recentemente a WEG, empresa do setor metal mecânico, instalada em Jaraguá do Sul, Santa Catarina, anunciou a ocorrência de fraude em seus controles internos, gerando perda financeira de R$ 2 milhões no ano de 2005.

Os riscos estão em todos os lados, sejam decorrentes de fatores internos ou externos, daí a importância de se gerenciar corretamente os riscos das mais diversas naturezas e origens, por intermédio da adoção de controles internos, podendo dessa forma criar oportunidades de melhoria significativas para a empresa, bem como aumentar a competitividade no mercado.

Se houvesse maior divulgação e transparência no gerenciamento dos riscos dos negócios, todos os tipos de negócios poderiam evoluir entre a especulação necessária e o equilíbrio suficiente e ficar mais saudáveis, seguros e eficientes.

A consciência internacional de riscos já está bastante desenvolvida, porém no Brasil, os passos têm sido bastante lentos, podendo as empresas brasileiras estar perdendo competitividade no mercado.

A questão adquire feições altamente complexas quando se percebe a extraordinária amplitude do conceito de risco, levando-se em consideração qualquer fato que possa ter impacto nos resultados de uma organização. Em vista das múltiplas ameaças potenciais à saúde e à continuidade dos negócios, tem-se observado, portanto, uma crescente iniciativa do mundo empresarial no sentido de aprimorar as práticas de gestão responsável e transparente, de modo a mitigar riscos e reforçar a segurança operacional, agregando maior segurança nas estratégias da organização.

E com o intuito de refrear o advento de novos escândalos contábeis e a lavagem de dinheiro, valorizando os controles internos, está em curso um enorme esforço de adesão a regulamentações emergentes. Organizações de todos os ramos

econômicos, em todo o planeta, estão às voltas com a missão de atender a rigorosos requerimentos, fundamentados em boas práticas.

Destacando-se nesse sentido a Lei *Sarbanes Oxley* de 2002, a qual afeta todas as empresas americanas e estrangeiras, com ações nas bolsas dos Estados Unidos. Em caso de não cumprimento da legislação, administradores, auditores e consultores estão sujeitos a severas penalidades. Similarmente, na União Européia, as firmas locais estão sendo compelidas a aderir à norma IAS 2005 – *International Accounting Standards*.

Além de essas regulamentações terem sido desenvolvidas para controlar riscos e gerar maior transparência no mercado financeiro, induzindo o gerenciamento eficaz, são também grandes aliadas dos executivos, auxiliando no planejamento estratégico coerente, com foco em controles internos e nas possíveis exposições aos riscos inerentes ao negócio e aos seus processos.

Reuniremos no trabalho ora apresentado, uma visão integrada de riscos, da necessidade do gerenciamento de riscos e de oportunidades de melhoria, e de controles internos embasados no modelo COSO.

# 2. GOVERNANÇA: UMA QUESTÃO DE CONTINUIDADE DOS NEGÓCIOS

## 2.1 Governança por Intermédio de Regulamentações

Diante das pressões regulatórias e das múltiplas ameaças à continuidade dos negócios, as corporações movimentam-se hoje no sentido de aprimorar processos, fortalecer controles internos e ganhar eficiência operacional.

Gerenciar pró-ativamente os riscos para incrementar negócios com transparência e credibilidade é, definitivamente, a diretiva que hoje mobiliza os segmentos mais dinâmicos do mundo empresarial, tornando cada vez mais vitais e sinérgicas as boas práticas de governança corporativa e tecnológica.

De acordo com o IBGC, "Governança Corporativa é o sistema pelo qual as sociedades são dirigidas e monitoradas, envolvendo os relacionamentos entre Acionistas/Cotistas, Conselho de Administração, Diretoria, Auditoria Independente e Conselho Fiscal."

As boas práticas de governança corporativa têm a finalidade de aumentar o valor da sociedade, facilitar seu acesso ao capital e contribuir para a sua continuidade.

Tirando proveito do esforço de *compliance* com os numerosos marcos regulatórios existentes, com destaque para a Lei *Sarbanes-Oxley* e para o Acordo da Basiléia 2, este por sua vez direcionado para os riscos financeiros e operacionais no setor de serviços financeiros, as organizações empenham-se em abraçar a cultura de gestão de riscos. A ordem agora é redesenhar e aprimorar os processos internos, elevar a produtividade e a eficiência, potencializando assim as vantagens competitivas.

"O mercado tem de cumprir as regulamentações, mas a maior parte das empresas quer ir além, almejando obter benefícios para os negócios", afiança Ricardo Balkins, sócio-diretor de consultoria em gestão de riscos empresariais da Deloitte. Daqui a certo tempo, não será a legislação, mas sim o *business* em si que vai requisitar maior transparência.

Está-se falando, em última instância, de assegurar nada menos que a continuidade dos negócios das companhias. Vale dizer, a missão é levantar, quantificar e monitorar a ocorrência de todo tipo de evento, externo ou interno, envolvendo processos, sistemas e pessoas, que possa acarretar impactos na geração de receitas e lucros.

Em decorrência direta dessas demandas, começaram no Brasil implementações efetivas de modelos padronizados de gestão, como o COSO (*Committee of Sponsoring Organizations of The Treadway Commission*), este por sua vez, é o principal objeto de estudo do trabalho em questão, e orientado para a governança corporativa, apontado na Lei *Sarbanes-Oxley* como *benchmark* de referência.

Para que as empresas se adaptem aos modelos padronizados de gestão, deve-se fazer um trabalho meticuloso de auditoria de processos, com a finalidade de assimilar o negócio da empresa e fixar os controles indicados. No passo seguinte, surgirão mudanças de procedimentos mais aprofundadas, bem como a mudança cultural, necessitando participação efetiva da presidência, gestores e pessoal operacional para que tornem efetivas as práticas de monitoração, visando à continuidade dos negócios. "Detectar quais são os riscos presentes e quais as reações diante deles é tarefa afeita a toda a organização. É preciso que se mantenha uma atitude de alerta permanente e que uma série de ações preventivas sejam tomadas", preceitua Edgar D'Andrea, sócio da área de gestão de riscos tecnológicos da PricewaterhouseCoopers.

## 2.2 Regulamentações

As regulamentações propostas vêm auxiliar os empresários a criar uma visão focada em riscos e governança corporativa e, conseqüentemente, a educar as empresas a agregar valor através do gerenciamento dos riscos, gerando oportunidades e facilitando o desenvolvimento de um planejamento estratégico em linha com seus objetivos.

## *2.3 Sarbanes Oxley*

A lei americana *Sarbanes Oxley* de 2002, tem como objetivo principal reduzir fraudes e insuficiências nos balanços empresariais e resgatar a confiança dos investidores. Atinge todas as empresas dos Estados Unidos e estrangeiras, com receita superior a US$ 75 milhões, listadas na Bolsa de Nova York, Amex ou Nasdaq.

Segmentada em numerosas seções, a *Sarbanes Oxley* obriga as corporações a aprimorarem o gerenciamento, conferirem transparência aos resultados financeiros e contábeis, além de monitorarem de perto o desempenho dos negócios. Responsabiliza os conselhos diretivos, que ficam sujeitos a penalidades legais (que podem variar de 10 a 20 anos de prisão ou multa de 1 a 5 milhões de dólares americanos), pela exatidão dos relatórios financeiros e pelo correto funcionamento dos controles internos, os quais devem ser periodicamente fiscalizados por auditorias externas. A transparência é requerida nos resultados, nos processos e dados operacionais que geram os resultados.

Fato a notar é que o escopo da Seção 302 da lei *Sarbanes Oxley*, que trata da responsabilidade corporativa pelos relatórios, inclui também informações não-financeiras como o ambiente competitivo e regulatório, condições macroeconômicas, objetivos de negócios, metas e estratégias, problemas de governança, investimentos e aquisições planejados e mudanças nas linhas de negócios, entre outros pontos.

## 2.4 IAS 2005

Na União Européia, as empresas listadas nas bolsas têm a obrigação de publicar a partir de 2005, todos os seus relatórios financeiros consolidados em conformidade com a IAS – *International Accounting Standards,* norma editada pela IASB - *International Accounting Standards Board.* Por meio de um único *framework* para gerar relatórios, a meta é tornar os resultados mutuamente comparáveis,

transparentes e confiáveis, emprestando maior eficiência ao mercado de capitais europeu e facilitando a integração entre as bolsas dos diferentes estados membros.

Não se trata apenas de reordenar as informações existentes e rearranjar os sistemas contábeis, mas sim de alterar o modo como uma empresa se apresenta publicamente, com impactos na aferição do desempenho, na relação com os investidores e nas transações de negócios.

## 2.5 Acordo da Basiléia 2

As práticas de gerenciamento preceituadas pelo Grupo de Gestão de Riscos do Comitê da Basiléia sobre Supervisão Bancária, vinculado ao BIS *(Bank for International Settlements)* enfeixadas no chamado acordo da Basiléia 2 – visam responder à maior diversidade e complexidade na atuação dos bancos e no seu perfil de riscos, em decorrência da globalização e desregulamentação dos serviços financeiros e da sofisticação tecnológica que marca o setor, tendo como objetivo principal a mitigação de riscos de fraudes e de falhas sistêmicas. O prazo de aderência ao *compliance* é 2006.

A empresa de auditoria e consultoria empresarial Deloitte Touche Tohmatsu define *compliance* como "o sistema designado para prevenir e detectar a falta de conformidade com leis e regulamentações externas ou internas existentes no negócio, que possam ser cometidas pelos seus funcionários e outros agentes".

Basiléia 2 busca dotar os bancos de um *framework* para supervisionar o gerenciamento efetivo dos riscos operacionais - riscos de perdas oriundas de eventos externos, de falhas ou inadequações envolvendo processos internos, pessoas e sistemas - dos riscos de crédito e de mercado. Encoraja as instituições a utilizar aplicações de avaliação e quantificação de riscos para calcular a alocação de capital necessário.

Ressalvando as diferenças de uma instituição para outra, a meta é estimular uma forte cultura de risco operacional, de controle e reporte interno, o que inclui, entre outras coisas, delimitar linhas de responsabilidade claras e segregar funções, além da adoção de planos de contingências eficazes.

## 2.6 Reflexos das Regulamentações no Brasil

No Brasil, as subsidiárias das multinacionais americanas e as companhias brasileiras com ADRs (*American Depository Receipts)*, listados na Bolsa de Nova York já se mobilizam tendo em vista a adesão a lei *Sarbanes Oxley.*

No segmento financeiro, a Febraban (Federação Brasileira dos Bancos), inicia um trabalho intensivo de preparação para dar provimento aos preceitos do Acordo Basiléia 2. Algumas instituições nacionais de grande porte, como o Bradesco, Itaú e Unibanco, lançaram seus projetos, antecipando-se na adesão ao acordo Basiléia 2.

Afora essas movimentações mais evidentes, pressões regulatórias partem também de outras frentes, abrangendo várias áreas da economia, como as provenientes de entidade como Anatel – Agência Nacional de Telecomunicações, Anaeel – Agência Nacional de Energia Elétrica, CVM – Comissão de Valores Mobiliários, sem mencionar o que está sacramentado no novo código civil.

Em decorrência direta dessas demandas, começam a deslanchar as implementações de *frameworks* de gestão como o COSO *(Committee of Sponsoring Organizations of The Treadway Commission)*, orientado para a governança corporativa, e o COBIT *(Control Objectives for Information and Related Technology)*, centrado na governança tecnológica.

A *Sarbanes-Oxley*, aliás, recomenda explicitamente o COSO para se efetuar os controles e a avaliação de riscos, o que fez despertar um grande interesse em seu estudo, o qual ganha proporções maiores no capítulo 5 deste. Já o COBIT recebeu expressivo empurrão ao ser indicado pelo Banco Central do Brasil como instrumento de auditoria e *compliance.*

Como é óbvio, essa ênfase no trato dos riscos e a severidade regulatória adquirem pleno sentido diante da complexidade e volatilidade dos mercados e nos ambientes de negócios. Em termos macroeconômicos, a desregulamentação e globalização, ao ensejarem a abertura das fronteiras na atuação das empresas, fundaram um marco estratégico inteiramente distinto.

Os riscos cresceram exponencialmente, sobretudo nos mercados em que a globalização incidiu de maneira mais agressiva. Eventos tão díspares como guerras, conflitos, atentados, ataques de *hackers*, fraudes, lavagem de dinheiro, desastres

ambientais, epidemias, entre tantos outros, não raro têm de passar pelo crivo dos conselhos diretivos.

A finalidade é garantir boas práticas de administração e, ao mesmo tempo, transparência. Evitando que investidores, acionistas e parceiros de negócios evidenciem empresas aparentemente sólidas, se desmanchando no ar pela ausência de uma gestão ética, profissional e pró-ativa. Não bastando apenas antecipar-se aos riscos, mas comprovar organização aos investidores, em suma, demonstrar que a administração está preocupada com a continuidade dos negócios.

# 3. RISCOS E OPORTUNIDADES

## 3.1 Definição de Riscos e Oportunidades

Riscos empresariais, de acordo com Paulo Baraldi, "são todos os eventos e expectativas de eventos que impedem que a empresa e as pessoas da empresa de ganharem dinheiro e respeito." Os riscos empresariais podem levar a empresa a falência e conseqüentemente, prejudicar a todos os *stakeholders* (clientes, acionistas, colaboradores, mercado e investidores).

Após o estouro da bolha do mercado de ações das empresas ponto.com, os acontecimentos de 11 de setembro, o colapso das empresas Enron e Arthur Andersen, os casos corriqueiros de fraude e até mesmo a explosão da Base de Alcantâra, no Maranhão, duas coisas sobre risco devem ficar bem entendidas:

- ✓ Eventos negativos com impactos que vão desde um pequeno transtorno até uma catástrofe podem afetar sua empresa onde quer que ela esteja localizada.
- ✓ Eventos negativos podem assumir diversas formas, sendo que cada evento afetará uma organização de maneira diferente, causando um impacto que poderá significar um pequeno transtorno para uma e uma grande catástrofe para outra.

Com isso em mente, é importante lembrar que um fator de risco que se transforme em um evento negativo real tem a possibilidade de transtornar os processos de sua organização, deixando-a incapaz de atender aos requisitos dos clientes, acionistas e investidores.

Os impactos dos eventos podem ser negativos, positivos, ou os dois. Eventos com impacto negativos podem inibir a criação de valor para o negócio, já os eventos com impacto positivo, podem compensar eventos negativos ou representar oportunidades, que se bem aproveitadas, podem aumentar o valor da sociedade e contribuir para a perenidade da companhia, vale ressaltar, portanto que "se o risco gerenciado causa a oportunidade de ganho ou redução de perda, a identificação de oportunidades causa riscos a serem gerenciados" [Paulo Baraldi].

## 3.2 Gestão de Riscos e Oportunidades

Conforme definido pela *Enterprise Risk Management Framework* – do *Committee of Sponsoring Organization of the Treadway Commission (COSO)* e citado por Paulo Baraldi: "o gerenciamento de riscos empresariais é um processo efetuado por pessoas (diretoria, gerência e outras), aplicado no estabelecimento de estratégia através da empresa, desenhado para identificar eventos potenciais que podem afetar a entidade e gerenciar os riscos dentro do apetite da empresa e fornecer segurança razoável com respeito à realização dos objetivos da empresa".

A gestão de riscos não deve, em absoluto, ser entendida sob uma conotação negativa, pela qual se visaria tão só identificar e abrandar ameaças. Ela pode, pelo contrário, aportar vantagens estratégicas e diferenciais competitivos. As companhias pró-ativas não monitoram riscos apenas por motivos regulatórios ou pra garantir a governança corporativa, mas sim, adotam essa iniciativa para agregar valor e alavancar oportunidades. No entanto, para que tudo isso ocorra automaticamente e da maneira prevista o gestor precisa enxergar e conhecer bem os riscos, para que possa vislumbrar os melhores caminhos.

Num cenário em que a informação *on-line* torna tudo instantâneo, identificar primeiro os riscos pode significar sair na frente ou perder mercado. Os investimentos no câmbio e o uso da Internet no suporte as transações são exemplos de como é possível incrementar receitas, desde que os riscos estejam sob absoluta vigilância.

Para o bom gerenciamento dos riscos e das oportunidades, faz-se necessário mapear, avaliar o impacto e a probabilidade de os mesmos acontecerem, acompanhá-los e aperfeiçoá-los, bem como o envolvimento, o comprometimento de todos (gestores, diretores, presidência, e obviamente do pessoal operacional) para com os objetivos estratégicos da corporação.

O que está acontecendo atualmente demonstra que o tema risco deixou de se ater a um setor especifico para adquirir importância vital no âmbito de toda a corporação e, portanto, os CIOs, por exemplo, têm de trabalhar com um conceito mais amplo e consistente de riscos, de modo a conseguir gerar maior valor.

Outro ponto decisivo vem de que, ao se tornarem mais transparentes e angariarem a confiança de clientes, investidores e fornecedores, as empresas

podem desfrutar de ambiente de negócios menos hostil, uma vez que companhias que tem maior solidez e confiabilidade conseguem convencer o mercado de que sua operação está alinhada com suas estratégias.

Foi o que aconteceu com a empresa multinacional brasileira Weg S/A, que demonstrou transparência ao comunicar publicamente a fraude incorrida internamente, ocasionando o rombo de R$ 2 milhões em seus cofres, sendo a fraude constatada por meio da auditoria interna da companhia. A trama ardilosa contemplava a emissão de notas fiscais de falsos fornecedores e o efetivo pagamento em contas de quatorze "laranjas", todos funcionários da companhia e devidamente subornados pelos suspeitos: um funcionário recém contratado como auxiliar do setor financeiro da fábrica de Jaraguá do Sul (SC) e seu irmão gêmeo, ex-estagiário da Weg.

Felizmente, grande parte do montante desviado (cerca de 70%), já fora recuperado, porém o que paira no ar, é a falta de controles preventivos da companhia, como a correta segregação de funções, restringindo os acessos sistêmicos às transações críticas como emissão de pedido de compra, aprovação para o pedido, recebimento fiscal (sistêmico) e efetivação do pagamento das notas fiscais forjadas.

## 3.3 Mudança Cultural

Se num primeiro momento as novas práticas de gerenciamento de riscos são impostas por uma repressão legal, ao longo do tempo elas devem contribuir para uma mudança cultural mais profunda. Num estágio mais avançado, as organizações se moverão pela consciência de que isso reforça sua credibilidade, segurança e solidez.

O propósito da lei nada mais é do que educar as organizações, fazendo-as entender que ao cumprirem os requerimentos de *compliance*, estarão preparadas para tomadas de decisões mais precisas e eficazes. E mais, monitorar tendências e indicadores, fazer os ajustes necessários, obter informações precisas e automatizar processos representam um diferencial no mercado atual.

Por esse conjunto de atributos, a gestão de riscos deve adquirir a mesma relevância que a onda de busca de qualidade, nos moldes da ISO, que mobilizou as empresas no passado recente, pois este modelo de gestão se tornará um requisito nos negócios, ultrapassando o mero cumprimento da regulação. Já na visão tecnológica, o cuidado com os riscos pode ser visto como o caminho natural da evolução gerencial do setor corporativo. Essa dinâmica teve inicio com a modernização e automatização de processos, passou pelas etapas de integração, planejamento, colaboração e análise de desempenho.

O conhecimento e a prevenção de riscos inerentes a investimentos, informações e segurança, vieram atender às necessidades de negócios e reflete o amadurecimento do mercado e das empresas.

## 3.4 Efeito em Cadeia

De acordo com especialistas em gestão de riscos empresarias da Deloitte Touche Tohmatsu prevêem a ocorrência de um "efeito em cadeia", pelo qual, mesmo as empresas não diretamente expostas às novas regulações, acabarão por enquadrar-se devido à exigência do mercado e à valorização da pratica de gestão transparente.

De imediato, no Brasil, o aperto regulatório afetará diretamente as subsidiárias das multinacionais, que passarão a se orientar pelas normas que regem as matrizes, incorporando a mesma ótica para tratar de números e processos. Na seqüência, as transacionais inseridas em cadeias produtivas no país deverão exigir que seus fornecedores de primeira linha também reportem seus números sob a mesma estrutura, devido ao elevado grau de dependência desses fornecedores.

É importante ressaltar, que a exigência no sentido de seguir padrões internacionais não concerne apenas à qualificação dos produtos adquiridos, mas também aos relatórios financeiros dos provedores, de modo que estes terão igualmente de dar mostras de solidez e transparência. A *Sarbanes Oxley* se aplica também às empresas que planejam abrir seu capital, bem como as que se encontra em indústrias reguladas. As práticas de controle podem ajudar até as firmas de

capital fechado a se verem livres de acusações de fraudes, uma vez que seus parceiros podem insistir em maior profissionalismo gerencial e impor a obediência à regulamentação como condição para fechar negócios.

A tendência por sinal, é que se intensifique o processo de cobrança mútua entre as organizações parceiras e cliente, no sentido de manterem os seus respectivos riscos sob controle. Os bancos, por exemplo, já pedem relatórios auditados de seus clientes sobre responsabilidade social e ambiental, de maneira a ter maior segurança sobre o recebimento de seus créditos. Essa cobrança pode, se mal administrada, virar uma caça às bruxas indiscriminada ou um mecanismo de coerção. Por outro lado, pode ser saudável no processo de desenvolvimento do conhecimento e de melhores práticas locais.

# 4. IMPLANTAÇÃO DO MODELO PROPOSTO PELA *SARBANES OXLEY*

A Lei *Sarbanes Oxley* e as regras relacionadas emitidas pela SEC (*Securities and Exchange Commission,* instituição equivalente à brasileira Comissão de Valores Mobilários – CVM) são leis e regulamentações complexas que geraram confusão e consternação na comunidade empresarial. Mas, por trás de todas as regras e regulamentações, a Lei *Sarbanes Oxley* é simplesmente uma forma encontrada pelo governo para estabelecer recursos legais nos preceitos básicos da boa governança corporativa e das práticas empresariais éticas.

O estabelecimento desses novos procedimentos para os controles internos e para a certificação executiva representa uma correção de curso essencial para as companhias de capital aberto, determinando processos cuja adoção as companhias deveriam ter considerado em primeiro lugar, além de despertar o senso empresarial através da concentração do foco na boa governança corporativa e na transparência das informações financeiras.

No entanto, as novas regras impõem um custo: essas mudanças necessitarão de alterações significativas nos procedimentos e nas práticas, bem como na vida cotidiana de muitos executivos e de pessoas que a eles se reportam. Entretanto, muitas companhias não vão começar do zero, elas estarão aptas a adaptar processos já existentes para cumprir as exigências de controles internos da Lei *Sarbanes Oxley*.

Talvez a realização mais importante seja a mudança significativa e permanente da obrigatoriedade da aplicação da Lei *Sarbanes Oxley*. Para uma companhia de capital aberto, a obediência a essa Lei não é negociável. Para os Comitês de Auditoria e para a Alta Administração de companhias de capital aberto, particularmente Diretores Executivos e Diretores Financeiros, as definições de administradores financeiros e responsabilidade pessoal tornaram-se mais explícitas e os riscos significativos mais altos.

Não só suas obrigações estão claras, mas também as suas oportunidades. Ao percorrer de forma eficaz esse novo tempo, o potencial para revisar e perceber as novas visões corporativas e atingir novos níveis de excelência corporativa é inesgotável. A Lei *Sarbanes Oxley* codifica a concepção de que a administração da

companhia deve estabelecer as informações materiais arquivadas na SEC e distribuídas aos investidores, e deve, também, responsabilizar-se pela probidade, profundidade e precisão dessas informações.

Executivos que têm o pensamento inovador procurarão aproveitar as mudanças impostas para melhorar o desempenho operacional. Companhias de capital fechado, embora não obrigadas legalmente a cumprir a nova lei, também podem optar pela adoção de determinados componentes como parte de um plano geral para o aperfeiçoamento das operações de seu negócio.

Embora se dê grande enfoque, assim como a própria Lei *Sarbanes Oxley*, aos controles internos, eles constituem apenas em um dos muitos componentes da boa governança corporativa. Inúmeras outras considerações também entram em discussão: integridade e valores éticos; filosofia da administração e estilo operacional; estrutura organizacional; papéis e responsabilidades bem definidos para diretores, administração e funcionários; compromissos com a excelência; diretorias e comitês eficazes e pró-ativos; e muito mais.

É importante que os administradores das companhias tratem o cumprimento da Lei *Sarbanes Oxley* como prioridade. Essa nova ênfase nos controles internos e na divulgação transparente não é um modismo. A Lei *Sarbanes Oxley* muda fundamentalmente o cenário empresarial e as companhias não podem subestimar a tarefa que têm pela frente. É necessário tomar ações imediatas. Muitas medidas da nova Lei ainda estão em fase de formulação, e novas regras e regulamentações serão promulgadas. Sem dúvida, os efeitos da Lei *Sarbanes Oxley* serão sentidos no futuro.

## 4.1 Governança e as Atividades de Controles

A Lei *Sarbanes Oxley* torna os executivos explicitamente responsáveis por estabelecer, avaliar e monitorar a eficácia da estrutura de controles internos das companhias. Para muitos executivos, as complexidades que envolvem o cumprimento das regras e as implicações de seu descumprimento podem ser desanimadoras.

Contudo, a situação pode não ser tão grave quanto se imagina. Isso porque quase todas as companhias de capital aberto já possuem algum tipo de estrutura de controles internos. Por exemplo, sempre que um membro do departamento financeiro utiliza uma senha exclusiva para obter acesso ao sistema financeiro da companhia, um controle está sendo executado. Além disso, a maior parte das companhias já implementou algum nível de monitoramento. Por exemplo, utilizando o exemplo mencionado, sempre que um supervisor revisa as trilhas de auditoria *(logs)* do usuário para verificar se o acesso apropriado ao sistema está sendo mantido, ocorre um monitoramento.

Embora a situação possa não ser tão crítica, está longe de ser ótima. Em muitas companhias existe uma lacuna significativa entre os funcionários que executam as atividades de controle e os executivos que tomam as decisões estratégicas de governança corporativa. A maior parte das companhias não possuem, e antes da Lei *Sarbanes Oxley* não estavam obrigadas a ter, vínculo direto das atividades de governança da Diretoria e da Alta Administração com as atividades de controle da organização. Mas agora é importante para o cumprimento das regras que se estabeleça esse vínculo, já que a Lei *Sarbanes Oxley* exige que os altos executivos demonstrem, pelos registros efetivados, a funcionalidade da estrutura de controles internos.

O primeiro passo para a implantação do modelo proposto pela *Sarbanes Oxley* é a empresa conseguir criar uma visão geral de um programa de controles internos e infra-estrutura para poderem adaptar esta nova realidade aos seus recursos, processos e tecnologias já existentes, criando, conseqüentemente, o vínculo que antes era inexistente e que conecta atividades de controle sólidas com governança corporativa.

É recomendável que a empresa crie comitês, adotando os princípios presentes na lei e obtendo as informações organizacionais para que consigam monitorar suas atividades. Além disso, é necessário mapear detalhadamente uma trajetória que conduza a uma ampliada estrutura de controles.

Os benefícios podem exceder o simples cumprimento da Lei *Sarbanes Oxley*. Na verdade, uma forte estrutura de controles internos pode ajudar a companhia a:

- ✓ Tomar melhores decisões operacionais e obter informações mais pontuais;

- ✓ Conquistar ou reconquistar a confiança dos investidores;
- ✓ Evitar a evasão de recursos;
- ✓ Cumprir leis e regulamentos aplicáveis;
- ✓ Obter vantagem competitiva através de operações dinâmicas; e
- ✓ Realizar um planejamento estratégico mais realista com suas necessidades.

Inversamente, as companhias que se negam a instituir os controles exigidos podem se colocar em situações similares àquelas que levaram à promulgação da Lei *Sarbanes Oxley*, o que acarretará:

- ✓ Maior exposição à fraude;
- ✓ Penalidades impostas pela SEC;
- ✓ Publicidade desfavorável;
- ✓ Impacto negativo sobre o valor do acionista; e
- ✓ Queixas ou outras ações judiciais impetradas por acionistas.

## 4.2 Controles Internos

O *Committee of Sponsoring Organizations of the treadway Commission,* o COSO, de uma forma ampla e bem aceita no mercado, define controles internos como sendo "um processo efetuado pelo conselho de administração, pela administração ou por outras pessoas da companhia, que visa fornecer segurança razoável quanto à possibilidade de atingir objetivos nas seguintes categorias:

- ✓ Eficácia e Eficiência das operações;
- ✓ Confiabilidade dos relatórios financeiros;
- ✓ Cumprimento de leis e regulamentações aplicáveis".

Já a SEC propõem definir controles internos e procedimentos para a emissão de relatórios financeiros como "controles relativos à preparação de demonstrações financeiras para fins externos que são apresentados de maneira apropriada e em conformidade com os princípios contábeis nacionais".

O termo "controles e procedimentos de divulgação" foi recentemente apresentado pela SEC após o decreto da lei *Sarbanes Oxley*, os controles e procedimentos de divulgação "são desenhados para assegurar que as informações

que uma companhia precisa divulgar nos relatórios arquivados por ela segundo o *Exchange Act* são registradas, processadas, resumidas e reportadas dentro dos prazos estipulados pela SEC." Essa definição inclui tanto as divulgações financeiras quanto as não-financeiras.

Sob o figurino da governança, devem-se elaborar, mapear e testar os controles. A todo risco deve ser associado um controle, em conformidade com o grau desse risco: baixo, médio ou alto, embasados na probabilidade e no impacto de tal risco. Cada área operacional deve aquilatar seus riscos e as formas de acompanhá-los, reservando-se à área de TI a missão de dar suporte a essa rede de monitoração.

O grande obstáculo, a juízo de D'Andrea, é que as empresas tratam desses problemas por meio de soluções fragmentadas, em meio aos vários departamentos corporativos. "O que ocorre hoje é que os sistemas de gestão de riscos só se falam por interfaces. Não se percebe que uma fraude pode não ser captada por sistemas isolados", adverte ele.

Por isso, o consultor da PricewaterhouseCoopers prevê que haverá em breve a necessidade de integrar essas soluções segregadas em uma espécie de "ERP" *(Enterprise Resource Planning)* dedicado a cuidar dos riscos. Assim como a implantação dos ERPs tradicionais possibilitou interligar processos antes confinados por departamentos, um fenômeno similar deverá ter lugar na monitoração de riscos. "O COSO será o esqueleto geral de toda essa integração. Basicamente, é o único *framework* maduro para ser usado com esse escopo", conclui D'Andrea.

Por fim, é de se notar que, entre as mudanças organizacionais de maior vulto, está a aproximação dos controles internos da alta administração e dos principais executivos. Nos moldes da Lei Sarbanes-Oxley, decisões antes delegadas e atribuíveis exclusivamente a subordinados não podem mais sê-lo.

No contexto das severas exigências regulatórias, tem de ficar claro como e por que uma decisão foi tomada. Criam-se níveis hierárquicos e de alçada para a aprovação de certas iniciativas, de maneira que um processo decisório tenha de seguir um percurso adequado, rastreável e justificável.

## 4.3 Lei Sarbanes Oxley

## 4.4 Seção 302

A Seção 302, em vigor desde agosto de 2002, visa a certificação trimestral e anual dos controles e procedimentos de divulgação e impõe novos níveis de responsabilidade aos Diretores Executivos e Diretores Financeiros, que agora devem declarar pessoalmente que a divulgação dos controles e procedimentos foi implementada e avaliada. As regras também foram alteradas: o Diretor Executivo deve agora reconhecer diretamente a responsabilidade pelos controles internos que antigamente era amplamente delegada ao Diretor Financeiro.

Em cada arquivo trimestral ou anual, o Diretor Executivo e o Diretor Financeiro devem declarar que:

- ✓ são responsáveis pelos controles e procedimentos de divulgação;
- ✓ desenharam esses controles (ou supervisionaram seu desenho) para assegurar que as informações materiais cheguem ao seu conhecimento;
- ✓ avaliaram a eficácia desses controles a cada trimestre;
- ✓ apresentaram suas conclusões em relação à eficácia desses controles;
- ✓ divulgaram ao seu Comitê de Auditoria e aos seus auditores independentes todas as deficiências significativas encontradas nos controles, as insuficiências materiais e os atos de fraude envolvendo funcionários da administração ou outros funcionários que desempenham papéis significativos nos controles internos da companhia;
- ✓ indicaram no arquivamento na SEC todas as alterações significativas efetuadas nos controles.

## 4.5 Seção 404

A seção 404 da Lei *Sarbanes Oxley*, determina uma avaliação anual dos controles e procedimentos internos para a emissão de relatórios financeiros. Exige que os diretores executivos e os diretores financeiros avaliem e atestem periodicamente a eficácia desses controles. A seção 404 obriga as companhias a

incluir em seus relatórios anuais um relatório sobre controles internos emitido pela administração que:

- ✓ Afirme sua responsabilidade pelo estabelecimento e pela manutenção de controles e procedimentos internos para a emissão de relatórios financeiros;
- ✓ Avalie e atinja conclusões acerca da eficácia dos controles e procedimentos internos para a emissão de relatórios financeiros;
- ✓ Declare que o auditor independente da companhia atestou e reportou a avaliação feita pela administração sobre seus controles e procedimentos internos para a emissão de relatórios financeiros.

## 4.6 Seção 906

A Seção 906 entrou em vigor em agosto de 2002. Essa seção exige responsabilidade corporativa pelos relatórios financeiros, ou seja, que Diretores Executivos e Diretores Financeiros assinem e certifiquem o relatório periódico contendo as demonstrações financeiras. A certificação executiva declara que o relatório cumpre as exigências de emissão de relatórios determinadas pela SEC e que representam adequadamente a condição financeira da companhia, bem como os resultados de suas operações. O descumprimento dessa seção: multa de até US$5 milhões e até 20 anos de prisão podem ser as penas impostas para o descumprimento intencional, servindo como uma medida de sustento à engrenagem da lei.

## 4.7 Adesão a Lei SOX

Além da adesão as seções acima descritas, a Lei *Sarbanes-Oxley* exige que um auditor independente da companhia preencha um relatório individual que ateste a avaliação da administração sobre a eficácia dos controles e procedimentos internos para a emissão de relatórios financeiros.

Já que o Diretor Executivo e o Diretor Financeiro de sua companhia devem fazer declarações públicas em relação à eficácia dos controles internos, é preciso

manter suporte e documentação substanciais relacionados com a estrutura de controles internos e também com a sua avaliação.

Vale lembrar que o parecer sem ressalvas na última auditoria das demonstrações financeiras não é um atestado para a eficácia dos controles internos. Quando os auditores independentes emitem opinião acerca das demonstrações financeiras, não estão validando a estrutura de controles internos. Portanto, os procedimentos de testes que executam não são desenhados para atender às exigências da certificação.

Para que o auditor independente faça a certificação e prepare a própria avaliação, é preciso adotar uma estrutura de controles internos que contenha critérios objetivos os quais possam ser medidos e avaliados. Acredita-se que as recomendações do *Committee of Sponsoring Organizations of the Treadway Commission* – COSO seja a estrutura mais adequada e com maior freqüência utilizada pelos auditores.

A avaliação fornecida aos auditores independentes deve ser substantiva, bem documentada e abrangente. Um *checklist* resumido inclui:

- ✓ Informações acerca do ambiente de controles gerais (ambiente tecnológico) da companhia;
- ✓ Descrição completa dos objetivos de controle criados pela administração para identificar, classificar e avaliar riscos que possam impedir que a companhia alcance seus objetivos de emissão de relatórios financeiros;
- ✓ Descrição completa dos objetivos de controle criados pela administração para direcionar os riscos identificados e as respectivas atividades de controle;
- ✓ Descrição dos sistemas de informática e procedimentos de comunicação adotados para fornecer suporte ao tópico anterior;
- ✓ Resultados e documentação-suporte da avaliação mais recente feita pela administração sobre a eficácia do desenho e das operações das atividades individuais de controle;
- ✓ Relação de todas as deficiências encontradas no desenho e na implementação das atividades de controle, bem como os procedimentos propostos para sua correção;

- ✓ Descrição do processo adotado para comunicar deficiências significativas e insuficiências materiais aos auditores independentes e ao Comitê de Auditoria;
- ✓ Descrição dos procedimentos de monitoramento executados para assegurar que a estrutura de controles internos está operando conforme planejado e que os resultados dos procedimentos de monitoramento são revisados e executados;
- ✓ Descrição do processo de criação da divulgação e das atividades de controle relacionadas.

## 4.8 Estratégia Eficaz

Agora, com uma compreensão mais abrangente das Seção 302 e 404, torna-se clara uma estratégia eficaz, as determinações de ambas as seções podem ser direcionadas através de uma única metodologia. Um programa de controles internos que focaliza simultaneamente a divulgação e a emissão de relatórios financeiros pode atender às exigências trimestrais da Seção 302 e as exigências anuais da Seção 404, bem como suprir as necessidades dos auditores independentes para executar seus procedimentos de certificação.

A reivindicação para um alinhamento mais próximo das exigências das duas seções da Lei *Sarbanes-Oxley* tem sido unânime entre a comunidade empresarial, e a maioria dos observados espera que a SEC continue caminhando nessa direção.

Essa nova ênfase nos controles internos e no cumprimento das regras deve ser disseminada por toda a organização. Companhias de menor porte, que muito provavelmente não possuem uma infra-estrutura forte e um grande *staff* pode julgar essa adaptação especialmente difícil. Companhias de todos os portes serão obrigadas a destinar recursos significativos a esse trabalho – tempo, dinheiro e pessoal.

Os custos financeiros para o cumprimento das regras serão consideráveis, mas deve-se observar que não serão tão altos quanto os custos provocados pelo

descumprimento delas. Custos diretos podem incluir o tempo dispensado por consultores e funcionários para:

- ✓ Avaliação, implementação e monitoramento;
- ✓ Instrução de funcionários acerca dos controles internos;
- ✓ Despesas com a nova tecnologia para suportar o programa de controles internos; e
- ✓ Honorários pagos aos auditores independentes para exercitar os testes dos controles que visam atestar sua asserção quanto à eficácia de seus controles internos.

Custos indiretos podem incluir o remanejamento de pessoal e o realinhamento de outros recursos na organização para criar e manter uma melhor estrutura de controles internos. Entretanto, como já mencionado, a maior parte das companhias de capital aberto, já possui algum tipo de estrutura de controles internos em vigor. É possível que as organizações não precisem comprar sistemas totalmente novos ou desenvolver novos processos, podendo adaptar os recursos já existentes e integrá-los à nova estrutura de controles internos.

# 5. ESTRUTURAS DE CONTROLES INTERNOS – *FRAMEWORKS*

## 5.1 O papel do *Framework*

Independente dos objetivos específicos que mobilizam a escolha da instituição, o primeiro e mais tangível benefício em se adotar qualquer das estruturas descritas no sub-título 5.2, é garantir que haja uma linguagem comum entre as diversas áreas envolvidas mais diretamente com a gestão de riscos, geralmente as área de Auditoria Interna, *Compliance*, Riscos e a própria Administração. Como conseqüência, os resultados obtidos para a definição, avaliação e implementação dos controles internos, que são os elementos centrais de todo o processo, podem ser comunicados adequadamente a partir das camadas estratégicas para as operacionais e vice-versa, configurando-se essa estrutura (*framework*) como uma referência global para o processo de gestão de riscos corporativos. O resultado desse entendimento contribui positivamente para que todas essas funções desempenhem o seu papel efetivo nesse processo, tornando a gestão de riscos um verdadeiro pilar para a Governança Corporativa.

A adoção do *framework* ideal em muito contribui para as seguintes funções relacionadas à Governança Corporativa:

- ✓ Administração - exercer sua responsabilidade no processo, que é: buscar um Sistema de Controles Internos apropriado ao risco de seus negócios, a fim de proporcionar segurança operacional e maior confiabilidade aos seus investidores e clientes.
- ✓ *Compliance* - viabilizar sua missão, que é: assegurar, em conjunto com as demais áreas, a adequação, o fortalecimento e o funcionamento do Sistema de Controles Internos, procurando mitigar os Riscos de acordo com a complexidade de seus negócios, bem como disseminar a cultura de controles para garantir o cumprimento de leis e regulamentos existentes.
- ✓ Auditoria Interna - desempenhar seu papel de fiscalização e consultoria às demais áreas: o Sistema de Controles Internos, baseado em um *framework* apropriado, viabiliza a atividade de complementação da gestão de riscos e de

*compliance*, uma vez que estabelece os parâmetros e controles que a área necessita para verificar a conformidade, o uso prático e a adequação dos controles para as respectivas atividades operacionais.

Abordaremos, a seguir, as características e benefícios dos principais *frameworks* utilizados para tratar do assunto gestão de riscos.

## 5.2 Seleção do Modelo de *Framework*

Quer esteja começando da estaca zero ou aperfeiçoando a estrutura de controles internos já existentes, a companhia deve objetivar o desenvolvimento de um sistema que preencha os critérios de:

- ✓ Objetividade
- ✓ Mensuração
- ✓ Integridade
- ✓ Pertinência

Hodiernamente, há cinco principais modelos de *frameworks* conhecidos no mercado, voltados para alcançar os objetivos de negócio ou da área de Segurança da Informação, sendo definidos por Colbert and Bowen:

- ✓ COSO: *Internal Control – Integrated Framework*, as diretrizes foram puplicadas em 1991, e editadas em 1992 pelo *Committee of Sponsoring Organizations of the Treadway Commission*. Faz recomendações para a gestão de avaliar, relatar e melhorar os sistemas de controle.
- ✓ CoCo: *Criteria of Control Board – Guidance on Assessing Control – The CoCo Principles*, editado em Junho de 1997 por *The Canadian Institute of Chartered Accountants*. Qualquer um dos modelos de *frameworks* pode ser utilizado no desenho e implementação de um sistema de controle interno, contudo, muitas companhias constroem sua estrutura de controles internos em torno do *Committee of Sponsoring Organizations of the Treadway Commission* – COSO, pelo fato de o mesmo ser o único com foco em toda a organização, tendo várias referências à sua universalidade e também por ter sido

introduzido pela Comissão Européia como modelo de suporte ao seu sistema de controle interno (Moran 2001). É ainda aceito, recomendado e utilizado por grande parte dos profissionais de auditoria como uma estrutura de controle efetiva.

- ✓ CobiT: *"Control Objectives for Information and Related Technology"*, editado por *"Information Systems Audit and Control Foundation"*, em terceira edição datada em 2000. É um *"framework"* que proporciona uma estrutura para que os gestores dos processos de negócios possam cumprir eficiente e efetivamente as suas responsabilidades de controle sobre os sistemas de informação;
- ✓ SAC: *"Systems Auditability and Control"*, editado em 1991 por *"Internal Auditors research Foundation"* e revisto em 1994. Tendo como objetivo principal dar suporte aos auditores internos no controle e na auditoria de sistemas de informação e tecnologia;
- ✓ SAS 55 e 78: *"Statements on Auditing Standards"*, editados respectivamente em 1988 e 1995 por *"American Institute of Certified Public Accountants"*. Proporcionam um guia para os auditores externos relativamente ao impacto do controle interno no planejamento e execução de auditoria das demonstrações financeiras;

O quadro abaixo compara os conceitos de controle internos apresentados em cada um dos modelos de controles internos:

| Comparação de Conceitos de Controle | | | | |
|---|---|---|---|---|
| | **CobiT** | **SAC** | **COSO** | **SASs 55/78** |
| **Audiência primária** | Administração de usuários e de sistemas de informação; auditoria de sistemas; | Auditoria Interna | Gerenciamento | Auditoria Externa |
| **Visão de Controle interno** | Estabelecimento de processos, inclusive políticas, procedimentos, práticas, e estruturas | Estabelecimento de processos, subsistemas, e pessoas; | Processo | Processo |

| Comparação de Conceitos de Controle | | | | |
|---|---|---|---|---|
| | **CobiT** | **SAC** | **COSO** | **SASs 55/78** |
| | organizacionais. | | | |
| **Controles Internos como Objetivos Organizacionais** | Operações Efetivas & Eficientes Confidência, Integridade e disponibilidade de informação Segurança das Informações financeiras; Concordância com leis e regulamentações | Operações Efetivas & Eficientes Segurança das Informações financeiras Concordância com leis e regulamentações | Operações Efetivas & Eficientes Segurança das Informações financeiras Concordância com leis e regulamentações | Operações Efetivas & Eficientes Segurança das Informações financeiras Concordância com leis e regulamentações |
| **Componentes ou Domínios** | Domínios: Planejamento e organização; Aquisição e implementação; Entrega e suporte; Monitoramento; | Componentes: Ambiente de Controle; Manual & Automatizado; Sistemas de Controle e Procedimentos; | Componentes: Ambiente de Controle; Controle e Gerenciamento do Risco; Atividades de Informação & Monitoramento da Comunicação | Componentes: Ambiente de Controle; Controle e Gerenciamento do Risco; Atividades de Informação & Monitoramento da Comunicação |
| **Foco** | Tecnologia da Informação | Tecnologia da Informação | Entidade Global | Demonstração Financeira |
| **Avaliação da Efetividade dos Controles Internos** | Para um período de tempo | Para um período de tempo | Para um período de tempo | Para um período de tempo |
| **Responsabilida de pelo Sistema de Controles** | Gerência | Gerência | Gerência | Gerência |

Fonte: Artigo de Comparação de Controles Internos: COBIT®, SAC, COSO e SAS 55/78, por Janet L. Colbert, Ph.D., AI, CIA, e Paul L. Bowen, Ph.D., AI.

Além do COSO e CoCo, de acordo com o Guia para Melhorar a Governança Corporativa através de Eficazes Controles Internos (Deloitte Touche Tohmatsu, 2003) há disponível no mercado outras três estruturas proeminentes para a avaliação dos controles internos voltadas para objetivos de negócios:

- ✓ *Turnbull Report* – Controles Internos: Diretrizes para Diretores sobre o Código Combinado: Desenvolvido pelo *Committee on Corporate Governance of the Institute of Chartered Accountants in England & Wales*, em parceria com a *London Stock Exchange*, o guia foi publicado em 1999. O *Turnbull* exige que as companhias identifiquem, avaliem e administrem seus riscos significativos e avaliem a eficácia do sistema de controles internos relacionado.

- ✓ ACC – *Australian Criteria of Control*: Emitido em 1998 pelo *Institute of Internal Auditors* – Austrália, o ACC enfatiza a competência da administração e dos funcionários para desenvolver e operar a estrutura de controles internos. Trata-se de um controle independente, que inclui atributos como atitudes, comportamentos e competência, e é promovido como o enfoque mais compensador em termos de custo para os controles internos.
- ✓ *King Report* – Expedido pelo *King Committee on Corporate Governance* em 1994, promove padrões gerais para governança corporativa na África do Sul. O *King Report* ultrapassa os aspectos financeiros e reguladores usuais da governança corporativa, direcionando questões sociais, éticas e ambientais.

## 5.3 Auferição de poderes ao Comitê de Divulgação

A formação e as atividades de um comitê de divulgação representam um dos controles mais importantes que uma companhia pode implementar para assegurar que seus registros sejam claros, precisos, pontuais e completos. Na verdade, as questões quanto à divulgação fornecem grande parte das direções anteriores à Lei Sarbanes Oxley. Conforme já foi mencionado, a seção 302 desta lei determina que os diretores executivos e os diretores financeiros certifiquem que os controles e procedimentos de divulgação são apropriados e eficazes. Além disso, é possível que a SEC exija que o auditor independente da companhia ateste a eficácia dos controles e procedimentos internos para a emissão de relatórios financeiros. Na verdade, a SEC realmente considera a questão da divulgação tão importante, que aconselha todas as companhias de capital aberto a criarem um comitê dedicado à supervisão das atividades de divulgação. Os comitês de divulgação eficazes são compostos por pessoas que:

- ✓ Estão familiarizadas com as regras da SEC;
- ✓ Estão instruídas quanto aos aspectos primários dos negócios da companhia;
- ✓ Estão familiarizadas com as práticas de divulgação de companhias similares; e

- ✓ Ocupam posições dentro da companhia que lhes permitem agir quando necessário.

O porte da companhia determinará parcialmente a composição do comitê de divulgação. É possível que companhias maiores tenham um complemento total de pessoal com os cargos relacionados a seguir. Companhias menores podem ter pessoas cujas descrições de cargos se enquadrem em vários títulos. Alguns possíveis membros do comitê de divulgação incluem:

- ✓ Diretor Contábil ou Controller;
- ✓ Conselheiro geral ou outro superior jurídico responsável pelos registros na SEC que se reporte ao conselheiro geral;
- ✓ Diretor de Avaliação de Riscos;
- ✓ Diretor de Investimentos;
- ✓ Diretor Operacional;
- ✓ Outros funcionários que a companhia julgar apropriados. Algumas dessas pessoas podem ser líderes operacionais-chave de unidades, líderes de regiões geográficas, representantes de desenvolvimento operacionais ou representantes de recursos humanos.

Outras partes como auditores independentes e consultores jurídicos externos, podem atuar como conselheiros valiosos para o comitê de divulgação, mas não devem tomar decisões ou assumir funções como membros do grupo com direito a voto. O comitê de divulgação exerce inúmeras funções, incluindo:

- ✓ Determinação da pertinência das divulgações nos esboços de todas as informações difundidas publicamente;
- ✓ Supervisão do processo pelo quais as divulgações são criadas e revisadas;
- ✓ Identificação do que constitui transações ou eventos "significativos";
- ✓ Identificação de que constitui uma "deficiência significativa" e "insuficiência material" no desenho ou na operação dos controles internos;
- ✓ Certificação de que o diretor executivo e o diretor financeiro estejam cientes das informações materiais que podem afetar as divulgações.
- ✓ Revisão das deficiências dos controles com o diretor executivo e com o diretor financeiro para verificar se, individual ou globalmente, elas constituem uma

insuficiência material, e realização de recomendações quanto à sua divulgação nos registros na SEC.

Uma das ações preliminares do comitê de divulgação será definir sua missão. Para operar de forma eficaz, o comitê deve desenvolver uma descrição clara do escopo de suas responsabilidades. Ele deve também obter a confirmação formal de sua compreensão como diretor executivo e o diretor financeiro.

A tarefa mais importante que o comitê de divulgação terá pela frente será a certificação de que os processos estão em operação para obter e analisar as informações, visando verificar se ocorreu uma divulgação apropriada. Entre outros itens, o comitê deve revisar:

- ✓ Todos os registros da SEC, incluindo todos os registros da *Exchange Act* de 1934 e as demonstrações de registro do *Securities Act* de 1933;
- ✓ Avaliações efetuadas trimestral ou anualmente pela administração dos controles e procedimentos de divulgação e dos controles e procedimentos internos para emissão de relatórios financeiros;
- ✓ Todos os releases que forneçam informações financeiras ou diretrizes, informações sobre aquisições materiais, disposições ou outros eventos que sejam materiais para a companhia;
- ✓ A correspondência amplamente divulgada aos acionistas;
- ✓ Todas as apresentações para conferência dos investidores ou analistas, de acordo com a Regulamentação FD (*Full Disclosure*);
- ✓ Todas as apresentações para agências de classificação e agentes de crédito;
- ✓ Relatórios de auditoria interna;
- ✓ Livros de instruções específicas da administração;
- ✓ Livros de instruções específicas do conselho de administração e do comitê de auditoria;
- ✓ Políticas de divulgação adotadas pela companhia para as informações incluídas nos sites de suas relações com seus investidores / associados.

Embora o comitê de divulgação esteja sob a responsabilidade do diretor executivo e do diretor financeiro, um de seus membros pode reunir-se periodicamente com o comitê de auditoria para discutir:

- ✓ As atividades do Comitê de Divulgação;

- ✓ A qualidade das divulgações incluídas nos registros da companhia;
- ✓ Discordâncias com o diretor executivo e com o diretor financeiro;
- ✓ Discordâncias com especialistas externos, como consultores jurídicos ou auditores independentes.

O comitê de auditoria também pode assumir um papel nas resoluções de discordâncias significativas, por exemplo, se o comitê de divulgação recomenda a divulgação de uma determinada informação, mas o diretor executivo ou o diretor financeiro discorda, o comitê de auditoria pode ser chamado para ajudar a resolver o impasse.

## 5.4 Comitês de Importância Crucial

Iniciar ou aprimorar um programa de controles internos pode exigir uma distribuição (ou redistribuição) de pessoal. É recomendável a criação de vários novos comitês para auxiliar no processo.

- ✓ Comitê Diretor de Trabalho – Um grupo de nível geral, que supervisiona e coordena todas as atividades de controles internos. Em companhias pequenas, esse comitê pode consistir apenas do Diretor Executivo e do Diretor Financeiro. Organizações de maior porte, podem ter proporcionalmente um número maior de integrantes.
- ✓ Comitê de Divulgação – A SEC aconselha todas as companhias de capital aberto a criar um Comitê de Divulgação para assegurar que os registros da companhia sejam claros, precisos, pontuais e completos. O comitê estipula parâmetros para a divulgação e verifica a pertinência das divulgações em todas as informações difundidas publicamente.
- ✓ Equipe de Gerenciamento do Programa de Controles Internos – Responsável por uma grande parte do trabalho dos controles internos. As atividades da equipe incluem avaliação, desenvolvimento, implementação e correção dos controles internos.

## 5.5 Estabelecimento de Programa de Controles Internos

Para muitas companhias, o cumprimento das medidas da Lei *Sarbanes Oxley* relativas aos controles internos exigirá um esforço significativo. Na verdade, o trabalho inicial de desenvolver um programa de controles internos e a infra-estrutura suporte, pode ser intensivo. Entretanto, uma vez que o programa esteja bem estabelecido, a carga será amenizada e a estrutura e os processos tornar-se-ão parte dos procedimentos operacionais padrão de sua companhia.

As etapas relacionadas a seguir, e posteriormente detalhadas, podem ser seguidas ao se estabelecer um programa de controles internos:

- ✓ Planejar o programa
- ✓ Avaliar o ambiente de controles
- ✓ Definir o Escopo
- ✓ Constituir um repositório de controles
- ✓ Executar testes iniciais e contínuos
- ✓ Monitorar

### 5.5.1 Planejar o Programa

É recomendável a formação de uma equipe de gerenciamento do programa de controles internos para estabelecer o programa especifico sobre o assunto. O porte e a complexidade de sua companhia determinarão à alocação dos recursos pessoais para a equipe. Em uma pequena companhia, provavelmente, será necessária pouca estrutura organizacional. A equipe poderá ser constituída apenas por membros que trabalhem meio expediente, talvez um gerente de projeto e mais alguns funcionários. Entretanto, para companhias maiores, será necessário dispor de um número significativo de pessoas em funções que exijam dedicação integral.

Para muitas companhias que já possuem um grupo responsável pelos controles internos, talvez não seja necessário formar uma nova equipe de gerenciamento do programa de controles internos. Contudo, o comitê diretor de

trabalho deve avaliar se o grupo responsável pelos controles internos existentes possui o pessoal apropriado para conduzir as etapas selecionadas pela companhia.

Após a formação da equipe, um plano de projeto deve ser criado. Em nível geral, o processo global de planejamento deve resultar no seguinte:

- ✓ Entendimento e consenso acerca de objetivos, distribuições, escopo, custos e enfoque do projeto;
- ✓ Compromisso de que os recursos necessários estejam disponíveis quando solicitados;
- ✓ Consenso sobre a utilização de recursos externos e uma descrição dessas funções;
- ✓ Uma linha de base do projeto com a qual o progresso possa ser comparado;
- ✓ Consenso acerca dos processos e das metodologias utilizadas para gerenciar o projeto.

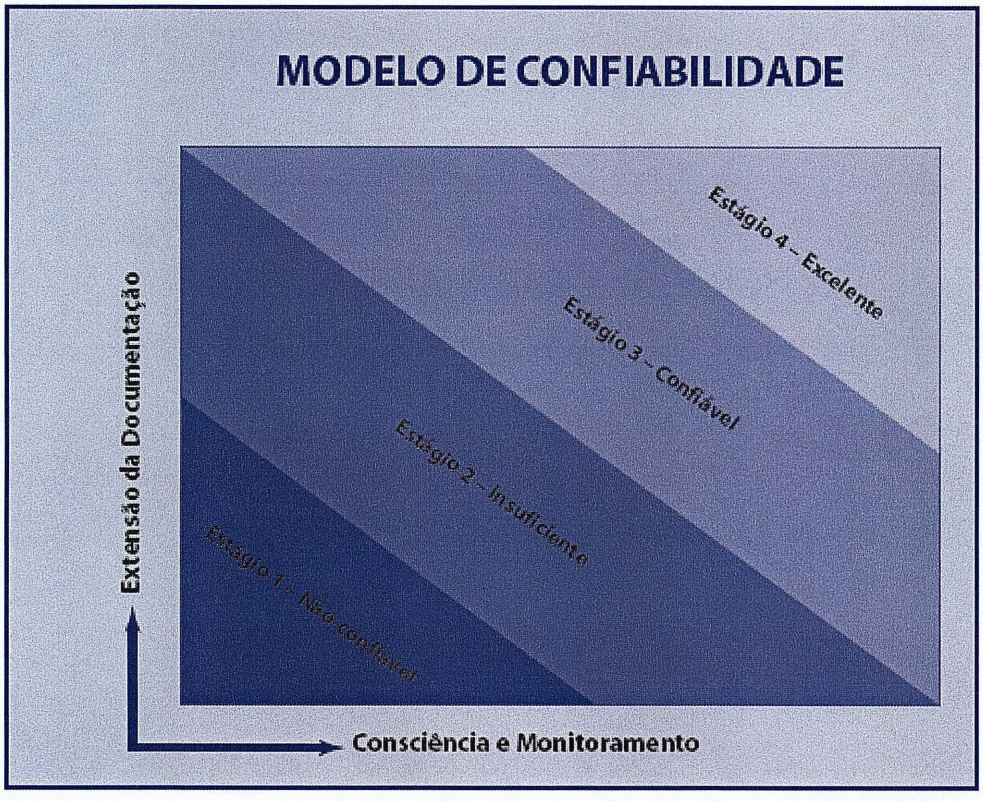
Muitas companhias já possuem uma equipe de auditoria interna e, levando em consideração as recentes propostas apresentadas por determinadas bolsas de valores, é provável que no futuro um número ainda maior de companhias estabeleça essa função. Os membros da auditoria interna podem exercer um papel importante nas atividades de uma companhia em relação às regras determinadas pela Lei *Sarbanes Oxley*, contribuindo com seu conhecimento de processos e de controles internos, monitorando as atividades de avaliação da administração, fornecendo inputs a um processo de avaliação de riscos e atuando como um importante elo com o Comitê de Auditoria.

Ao desenvolver um plano para o projeto, a Equipe de Gerenciamento do Programa de Controles Internos pode utilizar uma ferramenta como o Modelo de Confiabilidade nos Controles Internos. A seguir apresentamos o modelo proposto de confiança nos controles internos:

| | Estágio 1: Não Confiável | Estágio 2: Insuficiente | Estágio 3: Confiável | Estágio 4 : Excelente |
|---|---|---|---|---|
| Características | Controles, políticas e procedimentos relacionados não foram adotados nem documentados.<br><br>Não há um processo de criação para a divulgação.<br><br>Os funcionários não têm consciência de suas responsabilidades pelas atividades de controle.<br><br>A eficácia operacional das atividades de controle não é avaliada em uma base regular.<br><br>As deficiências dos controles não são identificadas. | Controles, políticas e procedimentos relacionados foram adotados, mas não estão completamente documentados.<br><br>Há um processo de criação para a divulgação, mas não está totalmente documentado.<br><br>É possível que os funcionários não tenham consciência de suas responsabilidades pelas atividades de controle.<br><br>A eficácia operacional das atividades de controle não é adequadamente avaliada em uma base regular e o processo não está completamente documentado.<br><br>É possível identificar as deficiências dos controles, mas elas não são prontamente corrigidas. | Controles, políticas e procedimentos relacionados foram adotados e estão completamente documentados.<br><br>Há um processo de criação para a divulgação, que está documentado de forma apropriada.<br><br>Os funcionários têm consciência de suas responsabilidades pelas atividades de controle.<br><br>A eficácia operacional das atividades de controle é avaliada em uma base periódica, ou seja, trimestralmente, e o processo está documentado de forma apropriada.<br><br>As deficiências dos controles são identificadas e prontamente corrigidas. | Abrange todas as características apresentadas no Estágio 3.<br><br>Existe um programa de gerenciamento de riscos e controles que abrange toda a companhia, de modo que controles e procedimentos são documentados e continuamente reavaliados para refletir um processo maior ou mudanças organizacionais.<br><br>Um processo de auto-avaliação é utilizado para avaliar o desenho e a eficácia dos controles.<br><br>A tecnologia é alavancada para documentar processos, objetivos de controle e atividades, bem como identificar falhas e avaliar a eficácia dos controles. |
| Implicações | Documentação insuficiente para suportar a certificação e a garantia da administração.<br><br>O nível de esforço para documentar, testar e corrigir controles é significativo. | Documentação insuficiente para suportar a certificação e a garantia da administração.<br><br>O nível de esforço para documentar, testar e corrigir controles é significativo. | Documentação suficiente para suportar a certificação e a garantia da administração.<br><br>O nível de esforço para documentar, testar e corrigir controles pode ser significativo, dependendo das circunstâncias da companhia. | Implicações do Estágio 3.<br><br>Tomada de decisões aperfeiçoada em virtude de informações pontuais e de alta qualidade.<br><br>Utilização eficiente de recursos internos. Monitoramento em tempo real. |

Esse modelo, que visualmente retrata o grau de confiabilidade dos controles internos, pode ser aplicado a qualquer unidade para a qual um plano esteja sendo criado, por exemplo, a companhia como um todo, ou uma unidade operacional ou uma subsidiária. Uma versão do Modelo de Confiabilidade nos Controles Internos foi

desenhada para categorizar a confiabilidade dos controles internos nos quatro estágios:




Fonte: Guia para Melhorar a Governança Corporativa através de Eficazes Controles Internos, Deloitte Touche Tohmatsu.

Ao utilizar o Modelo de Confiabilidade nos Controles Internos, deve-se avaliar minuciosamente as características da unidade que está sendo avaliada e determinar o estágio que mais se assemelha ao status dos controles internos dessa unidade. Se os controles internos forem classificados como não-confiáveis ou insuficientes, provavelmente a estrutura de controles internos não é suficiente para suportar as exigências de certificação anual. Sob tais circunstâncias, recomenda-se que a equipe do projeto comece a implementar imediatamente o plano do projeto. Se essa implementação demorar, pode ser que a companhia não esteja preparada para apresentar seu relatório anual acerca dos controles internos ou para atender às exigências de certificação do auditor independente.

Atingir o estágio 3, significa que os controles internos da companhia são confiáveis, mas não determina o fim do processo. Ao contrário, é o Estágio 4 que representa o propósito da Lei *Sarbanes-Oxley*, por meio do qual a governança corporativa está vinculada a atividades de controle eficazes.

Além de fornecer informações úteis que a equipe do projeto pode utilizar ao desenvolver o seu plano de projeto, o Modelo de Confiabilidade nos Controles Internos pode servir para várias outras finalidades, incluindo:

- ✓ Servir como um modelo comum para a discussão entre a administração e o auditor independente, em relação à confiabilidade dos controles internos da companhia, para a avaliação dos controles pela administração e certificação do auditor independente;
- ✓ Fornecer uma descrição altamente visual sobre a confiabilidade dos controles internos da companhia para o Conselho de Administração e para Alta Administração executiva.

### 5.5.2 Avaliar o Ambiente de Controle

Obviamente, políticas e procedimentos expressos são importantes e exercerão um papel principal na eficácia de sua estrutura de controles internos. Na verdade, grande parte do sucesso ou do fracasso de um programa de controles internos pode depender da documentação escrita. Mas também são críticos os atributos menos tangíveis de cultura, conduta e atitude, coletivamente chamados de Ambiente de Controle. Contribuindo com o Ambiente de Controle encontram-se elementos como integridade, valores éticos e competência dos funcionários de sua companhia; filosofia e estilo operacional da administração; delegação de autoridade e responsabilidade; e atenção e direção fornecidas pelo Conselho de Administração. O Ambiente de Controle constitui a base para todos os demais componentes dos controles internos.

Para facilitar a compreensão do Ambiente de Controle, é recomendável a execução de uma avaliação cultural. Ao pesquisar a Alta Administração e os funcionários de toda a organização, é possível obter rapidamente uma compreensão sobre a atitude dessas pessoas acerca do compromisso da companhia em criar um ambiente de controle eficaz. Se os resultados da avaliação cultural sugerirem que a companhia não possui um ambiente de controle consistente, é necessário adotar medidas corretivas, como:

- ✓ Comunicar a importância dos controles internos;

- ✓ Reforçar seu código de conduta e ética, bem como o programa de cumprimento de regras;
- ✓ Restabelecer o apropriado jargão "o exemplo vem de cima";
- ✓ Conduzir programas de treinamento e conscientização;
- ✓ Estabelecer canais para comunicação aberta (incluindo mecanismos que possibilitem a informação anônima).

Inversamente, se os resultados da avaliação cultural indicar que a companhia possui um sólido ambiente de controle, ela terá uma base concreta sobre a qual construirá seu programa de controles internos.

### 5.5.3 Definir o Escopo

O objetivo do processo de definição do escopo é identificar e inventariar os riscos relacionados com a divulgação e emissão de relatórios financeiros. Isso permitirá que a equipe de Gerenciamento do Programa de Controles Internos concentre seus esforços na identificação ou no desenho de controles para direcionar esses riscos.

Embora algumas companhias já possuam um programa formal ou informal de avaliação de riscos, o programa deve ser revisado pela equipe do projeto para assegurar que ele engloba o processo abrangente de identificação de todos os riscos financeiros e de divulgação. A equipe do projeto deve começar o processo de definição do escopo pela identificação de todas as principais unidades operacionais, localidades e subsidiárias da companhia. Em seguida, deve entrevistar o pessoal da administração dessas unidades operacionais para identificar riscos na emissão de relatórios financeiros e na divulgação, que poderiam afetar de maneira adversa a capacidade da entidade de reportar com precisão dados financeiros e não financeiros consistentes com o objetivo de que todos os valores e divulgações são precisos, completos, justos e pontuais.

Durante o processo de entrevistas, a administração deve estar preparada para abordar os seguintes pontos, entre outros:

- ✓ Riscos que podem impedir que a companhia alcance seus objetivos operacionais.
- ✓ Riscos na emissão de relatórios financeiros e nas divulgações, considerando o seguinte:
    - Principais processos e sistemas operacionais, incluindo aplicativos e processos terceirizados;
    - Riscos e processos não sistemáticos (por exemplo, lançamentos no diário e responsabilidade por contratos);
    - Padrões contábeis significativos;
    - Regulamentações da SEC e do ramo de atividade;
    - Exemplos de descumprimento de políticas e procedimentos da companhia;
    - Questões fortemente relacionadas com avaliações que dependem do julgamento profissional;
    - Sistemas e tecnologias de informação mais importante;
    - Situações nas qual a administração pode desconsiderar os controles.

A equipe do projeto deve então documentar e priorizar cada risco identificado na emissão de relatórios financeiros e na divulgação, pesando a importância relativa e a probabilidade de um efeito potencialmente adverso, sem levar em consideração a eficácia dos controles internos da companhia. Fatores que devem ser considerados ao priorizar os riscos na emissão de relatórios financeiros e na divulgação incluem:

- ✓ Risco relativo para a companhia;
- ✓ Materialidade das demonstrações financeiras;
- ✓ Probabilidade de ocorrência.

Com o passar do tempo, a companhia pode considerar a integração do processo de priorização de riscos na emissão de relatórios financeiros e na divulgação com um programa de avaliação de riscos em toda a empresa, que direcione todos os elementos da estrutura do COSO.

### 5.5.4 Constituir um repositório de Controles

O repositório de controles servirá como uma central de informações e atividades relacionadas com os controles internos. Ele conterá a documentação sobre os objetivos de controle, o desenho e a implementação das atividades de controle, bem como os métodos para testar a eficácia dessas atividades. Será o banco de dados no qual trimestral e anualmente as avaliações da administração se basearão, conforme determinado pelas Seções 302 e 404.

Para desenvolver esse repositório de controles, são recomendáveis que as seguintes etapas sejam seguidas:

a. Definir os principais objetivos de controle.
b. Mapear as atividades de controle existentes e compará-las com os objetivos de controle.
c. Identificar áreas em que os controles necessários estão ausentes e corrigi-las.

#### a. Definir os principais objetivos de controle

Como resultado do processo de definição do escopo, deve ser produzido um inventário dos principais riscos na emissão de relatórios financeiros e na divulgação. A Equipe de Gerenciamento do Programa de Controles Internos deve trabalhar sistematicamente os riscos, a fim de definir os principais objetivos de controle. É aconselhável que, em primeiro lugar, a equipe focalize os riscos que foram considerados "prioridade máxima" e prossiga seu trabalho abrangendo as outras categorias em etapas sucessivas, de acordo com a necessidade do seu ambiente.

Um objetivo de controle descreve as metas que a administração procura atingir. Na área de emissão de relatórios financeiros, alguns exemplos de objetivos gerais de controle incluem:

- ✓ Autorização: as transações são executadas de acordo com autorização geral ou específica da administração.
- ✓ Registro: todas as transações autorizadas são registradas pelos valores corretos, no período correto e na conta apropriada, a fim de permitir a

preparação das demonstrações financeiras de acordo com os princípios contábeis geralmente aceitos.

- ✓ Salvaguarda: a responsabilidade pela custódia física dos ativos é designada a pessoas específicas e independentes das funções de manutenção dos registros.
- ✓ Reconciliação: ativos registrados são comparados com ativos existentes em intervalos razoáveis e são tomadas ações apropriadas em relação a quaisquer diferenças verificadas.

Outros exemplos de objetivos de controles acionáveis incluem também:

- ✓ Processo de Gerenciamento de Pedidos: pedidos de venda somente são processados dentro dos limites de crédito aprovados para o cliente.
- ✓ Processo de Compra: os valores lançados nas contas a pagar representam bens adquiridos.

b. Mapear as atividades de controle existentes e compará-las com os objetivos de controle

As atividades de controle são políticas e procedimentos que ajudam a companhia a atingir determinados objetivos de controle. Elas devem ser incorporadas nas operações do negócio e utilizadas para reduzir, a níveis razoáveis, os riscos na emissão de relatórios financeiros e na divulgação. Alguns exemplos de atividades de controle incluem:

- ✓ Aprovações, autorizações e verificações.
- ✓ Gerenciamento funcional direto ou gerenciamento de atividades.
- ✓ Revisão dos indicadores de desempenho.
- ✓ Segurança de ativos.
- ✓ Segregação de funções.
- ✓ Controles dos sistemas de informática.

O objetivo dessa etapa é fazer um inventário das atividades de controle existentes que são praticadas na organização e compará-las com a lista abrangente de objetivos de controle desenvolvida na etapa anterior.

c. Identificar áreas em que os controles necessários são inexistentes e corrigir o problema

Após comparar todas as atividades de controle existentes com os objetivos de controle, é provável que haja objetivos para os quais não existem atividades de controle correspondentes. Essas falhas devem ser identificadas e documentadas para correção. Ou, de modo inverso, é possível haver atividades de controle identificadas que não podem ser comparadas com um objetivo. Nesse contexto, elas poderiam ser atividades de controle desnecessárias e, portanto, podem ser eliminadas, ou, ainda, o indício de que um objetivo de controle necessário não foi identificado.

Todas as falhas descritas anteriormente devem ser corrigidas através de um processo sistemático, começando pelos objetivos de controle de prioridade máxima, até que todos os objetivos de controle significativos tenham atividades de controle para direcioná-los.

### 5.5.5 Executar testes iniciais e contínuos

Depois de ter desenvolvido o repositório de Controles, a eficácia operacional das atividades de controle deve ser avaliada. Essa avaliação pode ser executada por pessoas responsáveis pelo desempenho dos controles, pela administração da companhia ou pela Equipe de Gerenciamento do Programa de Controles Internos. Os objetivos dessas atividades iniciais de teste são:

- ✓ Assegurar que as atividades de controle estão operando de forma apropriada.
- ✓ Fornecer informações para suportar medidas corretivas posteriores quando os testes das atividades revelarem deficiências nos controles internos.
- ✓ Desenvolver um programa de testes sustentável que forneça suporte para as avaliações trimestrais e anuais da administração.

Com a finalidade de fornecer suporte para a avaliação trimestral e anual dos controles internos, deve ser conduzida uma análise da estrutura desses controles, visando assegurar que não ocorreram mudanças significativas desde o último

período de avaliação. Caso sejam verificados processos operacionais ou mudanças organizacionais (por exemplo, uma aquisição), será necessário repetir as etapas anteriores para modificar a estrutura de controles internos e direcionar essas mudanças.

As pessoas responsáveis pelas atividades de controle devem avaliar sua eficácia como parte do processo formal de auto-avaliação dos controles internos. Para tanto, é recomendável que a eficácia operacional das atividades de controle individuais seja testada e que a documentação apropriada seja retida, de maneira que possa ser revisada pelos auditores independentes como parte de seus procedimentos para o trabalho de certificação.

### 5.5.6 Monitorar

Para muitas companhias, a função de auditoria interna desempenhará um importante papel no monitoramento e na emissão de relatórios sobre a eficácia da estrutura dos controles internos. As companhias que não possuem uma função de auditoria interna podem avaliar a utilização da Equipe de Gerenciamento do Programa de Controles Internos para executar essas tarefas. As atividades de monitoramento que devem ser executadas incluem:

- ✓ Avaliação independente da pertinência dos dados contidos no repositório de controles;
- ✓ Verificação das atividades de testes, ou seja, se elas são completas, precisas e pontuais;
- ✓ Confirmação de que as pessoas que avaliaram as atividades de controle o fizeram de modo pontual e com a compreensão total e completa das implicações decorrentes desse tipo de confirmação;

Comprovação de que a documentação completa e precisa é mantida.

# 6. COSO "Committee of Sponsoring Organizations of the Treadway Commission"

## 6.1 O que é COSO

Em 1985, foi criada, nos Estados Unidos, a *National Commission on Fraudulent Financial Reporting* (Comissão Nacional sobre Fraudes em Relatórios Financeiros), uma iniciativa independente, para estudar as causas da ocorrência de fraudes em relatórios financeiros/contábeis. Esta comissão era composta por representantes das principais associações de classe de profissionais ligados à área financeira. Seu primeiro objeto de estudo foram os controles internos. Em 1992 publicaram o trabalho *"Internal Control - Integrated Framework"* (Controles Internos – Um Modelo Integrado), tornando-se referência mundial para o estudo e aplicação dos controles internos.

Posteriormente a Comissão transformou-se em Comitê, que passou a ser conhecido como COSO – The Comitee of Sponsoring Organizations (Comitê das Organizações Patrocinadoras). O COSO é uma entidade sem fins lucrativos, dedicada à melhoria dos relatórios financeiros através da ética, efetividade dos controles internos e governança corporativa. É patrocinado por cinco das principais associações de classe de profissionais ligados à área financeira nos Estados Unidos, a saber:

- ✓ AICPA: "American Institute of Certified Public Accounts" (Instituto Americano de Contadores Públicos Certificados);
- ✓ AAA: *"American Accounting Association"* (Associação Americana de Contadores);
- ✓ FEI: *"Financial Executives Internacional"* (Executivos Financeiros Internacional);
- ✓ IIA: *"The Institute of Internal Auditors"* (Instituto dos Auditores Internos);
- ✓ IMA: *"Institute of Management Accountants"* (Instituto dos Contadores Gerenciais).

O Comitê trabalha com independência, em relação a suas entidades patrocinadoras. Seus integrantes são representantes da indústria, dos contadores,

das empresas de investimento e da Bolsa de Valores de Nova York. O primeiro presidente foi James C. Treadway, de onde veio o nome "Treadway Comission". Atualmente John Flaherty ocupa a presidência.

## 6.2 O Trabalho do COSO

No entendimento da Deloitte Touche Tohmatsu, a estrutura divulgada por "*Committee of Sponsoring Organizations of the Treadway Commission* - COSO", é amplamente divulgada e utilizada nos Estados Unidos, sendo adotada pela maioria das empresas com capital aberto na SEC.

O modelo COSO *"Internal Control – Integrated Framework"* (Controles Internos – Um Modelo Integrado), editado por *"Committee of Sponsoring Organizations of the Treadway Commission"* estabelece uma seqüência de eventos para a gestão de processos de negócio em ambiente de controle [Namee 1997]:

- ✓ Definição dos objetivos da organização;
- ✓ Avaliação do risco;
- ✓ Determinação dos controles necessários para melhoria contínua dos processos.

Os integrantes do COSO definem controle interno como "um processo, desenvolvido para garantir, com razoável certeza, que sejam atingidos os objetivos da empresa, nas seguintes categorias":

- ✓ Eficiência e efetividade operacional (objetivos de desempenho ou estratégia): esta categoria está relacionada com os objetivos básicos da entidade, inclusive com os objetivos e metas de desempenho e rentabilidade, bem como da segurança e qualidade dos ativos;
- ✓ Confiança nos registros contábeis/financeiros (objetivos de informação): todas as transações devem ser registradas, todos os registros devem refletir transações reais, consignadas pelos valores e enquadramentos corretos;
- ✓ Conformidade (objetivos de conformidade) com leis e regulamentos ou normativos aplicáveis à entidade e sua área de atuação.

As diretrizes do COSO, publicadas em 1992, não se referem explicitamente aos controles e procedimentos de divulgação. Ao contrário, a estrutura descrita pelo COSO é mais abrangente, incluindo tanto os controles e procedimentos de divulgação quanto os controles e procedimentos internos para a emissão de relatórios financeiros.

Segundo o COSO, os controles internos devem ser estabelecidos para minimizar a exposição aos riscos que podem prejudicar o atendimento dos objetivos da organização. Esses objetivos devem ser definidos previamente, considerando o perfil e os aspectos estratégicos e operacionais do negócio, os processos, os sub-processos e as atividades da organização.

Um modelo de controle interno quando aplicado com cuidado, discernimento e visão pode ser à base de um sistema de controle interno que suporte diretamente o sucesso da organização. Se aplicado mecanicamente, o sistema de controle interno resultante pode suportar um bom controle, mas não suportará necessariamente o sucesso organizacional [Galloway 1994].

Controle interno proporciona uma garantia razoável, porém não consegue dar garantia absoluta aos riscos inerentes ao negócio. Controle interno efetivo auxilia a entidade na consecução de seus objetivos, mas não garante que eles serão atingidos, e vários são os motivos, sendo alguns elencados abaixo:

- ✓ Custo/benefício: todo controle tem um custo, que deve ser inferior à perda decorrente da consumação do risco controlado;
- ✓ Conluio entre empregados: da mesma maneira que as pessoas são responsáveis pelos controles, estas pessoas podem valer-se de seus conhecimentos e competências para burlar os controles, com objetivos ilícitos.
- ✓ Eventos externos: eventos externos estão além do controle de qualquer organização. Exemplo disso foram os acontecimentos do dia 11/09/2001, nos Estados Unidos. Quem poderia prever ou controlar os fatos ocorridos?

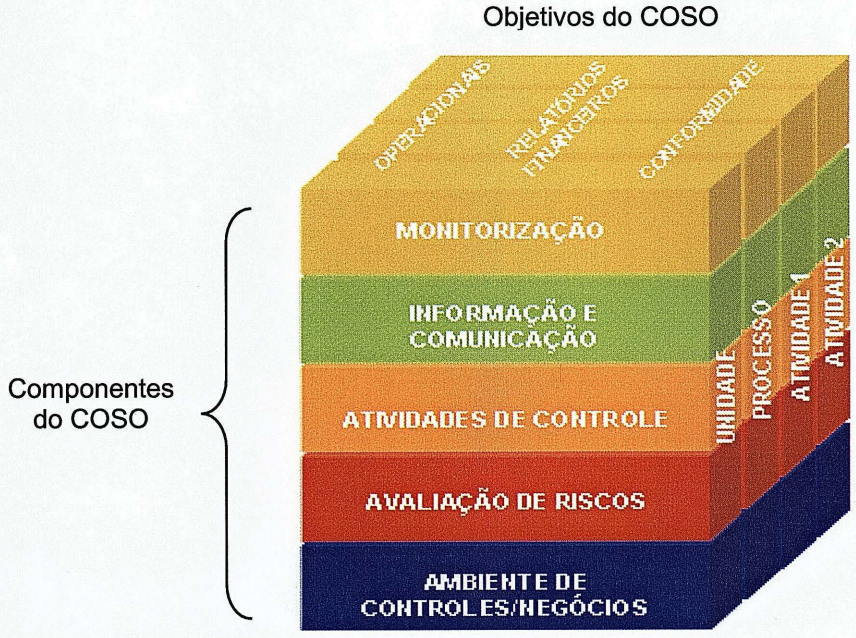
## 6.3 Relacionamento de Objetivos e Componentes

Há um relacionamento direto entre os objetivos que representam aquilo que uma entidade se esforça para atingir, e os componentes que representam o que é necessário pra atingir os objetivos.

As informações são necessárias para todas as três categorias de objetivos: administrar as operações empresariais de maneira eficaz, preparar demonstrações financeiras de forma confiável e verificar o cumprimento das regras.

A estrutura do COSO divide os controles internos eficazes em cinco componentes inter-relacionados, com o objetivo de simplificar a tarefa de gerenciamento das atividades que fazem parte de uma estrutura de controles internos, conforme evidenciado na figura 1:

**FIGURA 1 – ESTRUTURA DE CONTROLE COSO**




Fonte: www.coso.org

O controle interno é pertinente para a companhia como um todo ou para qualquer uma de suas unidades ou atividades e os cinco componentes são aplicáveis e importantes para o alcance dos objetivos operacionais.

## 6.4 Detalhamento dos Componentes do Coso

### 6.4.1 Ambiente de Controle


A visão da Empresa determina a cultura de seus colaboradores no tratamento de aspectos relacionados à sua estrutura de controles internos, influenciando a manutenção de uma estrutura eficiente e alinhada com os objetivos e riscos da Empresa.

O ambiente de controle é a base para todos os outros componentes da estrutura de controles, estabelecendo o desenho, o gerenciamento, a monitorização e a disciplina dos colaboradores em relação à estrutura de controles internos.

Os fatores relacionados à definição do ambiente de controle contemplam:

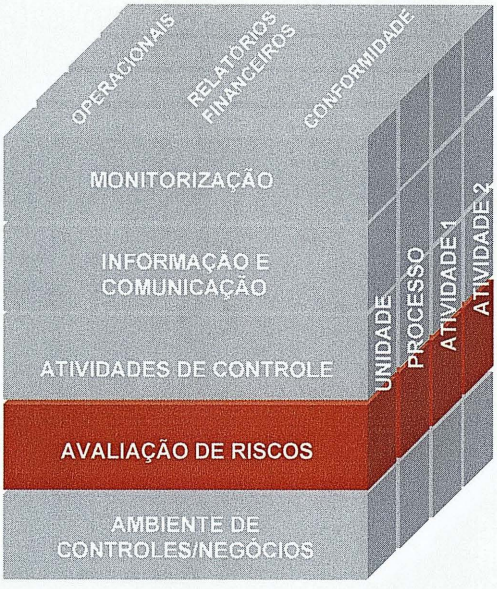
- ✓ Integridade e Valores Éticos: Alta Administração da Empresa, como modelo de ética para seus colaboradores, clientes, fornecedores, investidores e público em geral e estabelecimento de políticas e códigos de ética, formalizando e comunicando esses valores éticos aos colaboradores.
- ✓ Comprometimento com a Competência: definição formal das atribuições e responsabilidades dos colaboradores associadas à descrição dos conhecimentos e das habilidades necessárias para a execução das atividades da Empresa.

- ✓ Conselho de Administração e Comitê de Auditoria: o Conselho de Administração/Comitê de Auditoria independente, atuando de forma integrada com os auditores internos e externos, para possibilitar avaliações e julgamentos imparciais sobre as questões mais significativas da Empresa.
- ✓ Filosofia e Estilo de Gestão: perfil da Alta Administração diante dos riscos, dos princípios contábeis adotados e das decisões operacionais na Empresa.
- ✓ Estrutura Organizacional: adequação da estrutura às operações da Empresa, garantindo inclusive o bom fluxo de informações e a atuação dos elementos de monitorização da estrutura de controles.
- ✓ Autoridade e Responsabilidade: definição dos limites de autoridade, considerando a adequação dos aspectos de responsabilidade em relação à autoridade dos colaboradores.
- ✓ Políticas e Procedimentos de Recursos Humanos: práticas que indiretamente direcionam os colaboradores quanto aos níveis esperados de seu comportamento considerando os aspectos de integridade, ética e competência. Essas práticas abrangem as políticas e os procedimentos de contratação, treinamento, avaliação de desempenho, promoção e remuneração dos colaboradores.

O ambiente de controle deficiente pode incapacitar toda a estrutura de controles internos da Empresa, pois mesmo que os demais componentes da estrutura tenham sido, conceitualmente, bem implementados, somente uma cultura organizacional focada nos aspectos de controle irá determinar a utilização eficiente dessa estrutura.

A postura da alta administração nesse componente, desempenha papel determinante, devendo fornecer de forma clara e objetiva aos seus colaboradores, quais as políticas, procedimentos, Código de Ética e Código de Conduta a serem adotados.

### 6.4.2 Avaliação de Riscos




As principais funções do controle interno, conforme visto anteriormente, estão diretamente relacionadas ao cumprimento dos objetivos da entidade. Portanto, a existência de objetivos e metas é condição *sine qua non* para a existência dos controles internos. Se a entidade não contempla objetivos e metas definidos de forma clara, não há necessidade de controles internos. Uma vez estabelecidos e clarificados os objetivos, deve-se:

- ✓ identificar os riscos que ameacem o seu cumprimento; e
- ✓ tomar as ações necessárias para o gerenciamento dos riscos identificados.

Avaliação de riscos é a identificação e análise dos riscos associados ao não cumprimento das metas e objetivos operacionais, de informação e de conformidade. Este conjunto forma a base para definir como estes riscos serão gerenciados.

As organizações, em todos os seus níveis, enfrentam riscos internos e externos que ameaçam a capacidade de competição, a saúde financeira, a imagem e a manutenção da qualidade de seus produtos, serviços e colaboradores.

Os administradores devem definir os níveis de riscos operacionais, de informação e conformidade que estão dispostos a assumir. A avaliação de riscos é

uma responsabilidade da administração, mas cabe à Auditoria Interna fazer uma avaliação própria dos riscos, confrontando-a com a avaliação feita pelos administradores. A identificação e gerenciamento dos riscos é uma ação pró-ativa, que permite evitar surpresas desagradáveis.

O processo de análise geral de riscos é dinâmico, interativo e freqüentemente integrado ao processo de planejamento estratégico da Empresa, e sua elaboração deve considerar os seguintes aspectos:

- ✓ Identificação dos Riscos: mapeamento dos riscos inerentes, nos níveis estratégicos e operacionais, através da identificação da exposição da Empresa aos fatores de risco internos e externos. Para a identificação dos riscos, deve-se responder a perguntas como: o que pode dar errado, como e onde podemos falhar, onde somos vulneráveis, como poderiam interromper nossas operações, quais as informações mais importantes, onde gastamos nosso dinheiro, quais as atividades mais complexas, temos risco legal, quais atividades estão regulamentadas, entre outras.
- ✓ Análise de Riscos: estimativa dos impactos dos riscos e da probabilidade de sua ocorrência na Empresa, além de avaliações quanto a forma de gerenciamento dos riscos, ações necessárias para sua redução e respectivo custo dessas ações.
- ✓ Gestão de Mudanças: alterações na estrutura interna, na indústria, no cenário econômico ou em outros elementos externos podem alterar a exposição da Empresa aos riscos; assim, essas mudanças devem ser continuamente monitorizadas para que seus impactos sejam identificados e endereçados dentro da análise de riscos da Empresa.

A eliminação total dos riscos é, na prática, impossível, pois a própria existência da Empresa é um fator gerador de riscos. Nesse contexto, a análise geral de riscos fornece um mapa dos riscos da Empresa, proporcionando um mecanismo para priorização desses riscos e, conseqüentemente, uma ferramenta de direcionamento dos esforços para minimizar os riscos mais significativos através de uma estrutura de controles internos alinhada aos riscos da Empresa.

### 6.4.3 Atividades de Controle


São aquelas atividades que, quando executadas a tempo e maneira adequados, permitem a redução ou administração dos riscos. As atividades de controle compreendem o que, na sistemática de trabalho anterior à do COSO, era tratado como controle interno.

As atividades de controle ocorrem em todos os níveis da Empresa e abrangem atividades como aprovações, autorizações, verificações, reconciliações, revisões de performance operacional, segurança de ativos e segregação de funções.

As atividades podem ser de duas naturezas: preventivas ou detectivas. As principais atividades de controle, e suas respectivas naturezas, são:

a) Alçadas (prevenção): são os limites determinados a um funcionário, quanto a possibilidade deste aprovar valores ou assumir posições em nome da instituição, como por exemplo: estabelecer o valor máximo para um caixa pagar um cheque; estabelecer tetos assumidos por um operador de mercado para cada horizonte de investimento; estabelecimento de alçada operacional para o Comitê de Crédito de uma agência.
b) Autorizações (prevenção): a administração determina as atividades e transações que necessitam de aprovação de um supervisor para que

sejam efetivadas. A aprovação de um supervisor, de forma manual ou eletrônica, implica que ele (ou ela) verificou e validou a atividade ou transação, e assegurou que a mesma está em conformidade com as políticas e procedimentos estabelecidos. Os responsáveis pela autorização devem verificar a documentação pertinente, questionar itens pouco usuais, e assegurarem-se de que as informações necessárias à transação foram checadas, antes de darem sua autorização. Jamais devem assinar em branco ou fornecerem sua senha eletrônica.

c) Conciliação (detecção): é a confrontação da mesma informação com dados vindos de bases diferentes, tanto informações estratégicas, quanto operacionais, adotando as ações corretivas, quando necessário.

d) Revisões de Desempenho (detecção): Acompanhamento de uma atividade ou processo, para avaliação de sua adequação e/ou desempenho, em relação às metas, aos objetivos traçados e aos *benchmarks*, assim como acompanhamento contínuo do mercado financeiro (no caso de bancos), de forma a antecipar mudanças que possam impactar negativamente a entidade. Exemplos: monitoração do comportamento de usuários de cartões de crédito (lugares inusitados, produtos diferentes etc.); monitoração e questionamento de flutuações abruptas nos resultados de agências, produtos, carteiras próprias e de terceiros; monitoração de valores realizados e orçados em unidades, com o objetivo de identificar dificuldades/problemas; acompanhamento da concorrência, visando o lançamento de novos produtos.

e) Segurança Física (prevenção e detecção): os valores de uma entidade devem ser protegidos contra uso, compra ou venda não-autorizados. Um dos melhores controles para proteger estes ativos é a segurança física, que compreende controle de acessos, controle da entrada e saída de funcionários e materiais, senhas para arquivos eletrônicos, *call-back* para acessos remotos, criptografia e outros. Incluem-se neste controle os processos de inventário dos itens mais valiosos para a entidade (p.ex., conferência de numerário).

f) Segregação de Funções (prevenção): a segregação é essencial para a efetividade dos controles internos. Ela reduz tanto o risco de erros humanos quanto o risco de ações indesejadas. Contabilidade e conciliação, informação e autorização, custódia e inventário, contratação e pagamento, administração de recursos próprios e de terceiros, normatização (gerenciamento de riscos) e fiscalização (auditoria) devem estar segregadas entre os funcionários.

g) Sistemas Informatizados (prevenção e detecção): controles feitos através de sistemas informatizados dividem-se em dois tipos:
   - ✓ controles gerais: pressupõe os controles nos centros de processamentos de dados e controles na aquisição, desenvolvimento e manutenção de programas e sistemas. Exemplos: organização e manutenção dos arquivos de back-up, arquivo de log do sistema, plano de contingência;
   - ✓ controles de aplicativos: são os controles existentes nos aplicativos corporativos, que têm a finalidade de garantir a integridade e veracidade dos dados e transações. Exemplos: validação de informações (checagem das informações com registros armazenados em banco de dados).

h) Normatização Interna (prevenção): é a definição, de maneira formal, das regras internas necessárias ao funcionamento da entidade. As normas devem ser de fácil acesso para os funcionários da organização, e devem definir responsabilidades, políticas corporativas, fluxos operacionais, funções e procedimentos.

i) Controles Físicos (detecção): contagens periódicas e comparações com os registros de controle de inventários, ativos fixos, valores em espécie e outros ativos.

As atividades de controle devem ser implementadas de maneira ponderada, consciente e consistente. Nada adianta implementar um procedimento de controle, se este for executado de maneira mecânica, sem foco nas condições e problemas que motivaram à sua implantação. Também é essencial que as situações adversas

identificadas pelas atividades de controles sejam investigadas, adotando-se tempestivamente as ações corretivas apropriadas.

Apesar da grande variedade de formas de atividades de controle, todas são baseadas em dois elementos principais: políticas - estabelecendo quais ações devem ser executadas e procedimentos - apresentando como são executadas essas ações. As políticas e, principalmente, os procedimentos devem ser reavaliados sempre que ocorrerem mudanças significativas na estrutura da Empresa, em seus processos, sistemas e modelos de negócio.

As atividades de controle são funções dos riscos identificados no processo de análise geral de riscos. Dessa forma, o desenho das atividades de controle deve refletir a priorização dos riscos e sua eficácia deve ser avaliada continuamente, através de ações de monitorização, para garantir que os riscos estão sendo efetivamente minimizados.

### 6.4.4 Informação e Comunicação

São as práticas utilizadas pela Empresa para capturar e comunicar as informações pertinentes, em formato e prazo que possibilitem a execução das responsabilidades dos colaboradores.

A informação é necessária em todos os níveis da Empresa para execução das atividades e atendimento aos objetivos do negócio. Os sistemas de informação capturam, processam e reportam a informação, considerando atividades e eventos internos e externos à Empresa, necessários aos processos operacionais, à tomada de decisão e à emissão de relatórios externos.

Dessa forma, as práticas de controle sobre os sistemas de informação devem garantir os seguintes aspectos:

- ✓ Relevância: o conteúdo da informação é apropriado e relevante ao pessoal que a utiliza.
- ✓ Disponibilidade e Acesso: a informação está disponível quando necessária e somente é acessada por pessoal autorizado.
- ✓ Exatidão: a informação é a mais atual e correta possível.

A comunicação eficiente também deve fluir em todos os níveis e em todos os sentidos na Empresa; dessa forma, os meios de comunicação devem estar disponíveis a todos os seus colaboradores e os canais com clientes, fornecedores e outros agentes externos devem ser abertos e eficientes.

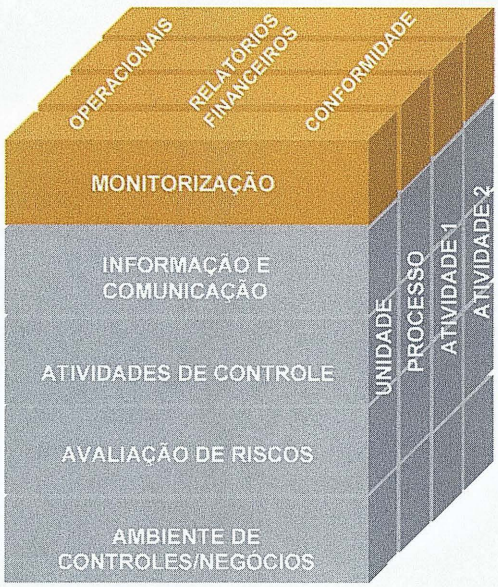
Os principais aspectos que devem ser implementados para garantir a comunicação eficiente são:

- ✓ Mecanismos de Divulgação: meios de disponibilização de informações. As principais informações que podem ser divulgadas através desses meios são, entre outras, visão e missão, políticas e procedimentos, responsabilidades dos colaboradores, estrutura organizacional, plano de benefícios, recrutamento interno e externo e níveis de alçada.
- ✓ Ferramentas de Sugestões: mecanismos para os colaboradores comunicarem suas idéias para o aprimoramento dos processos internos e outras informações relevantes.
- ✓ Canais de Comunicação Externos: meios de divulgação de informações de interesse geral ao público, agentes reguladores, acionistas, etc. Esse

aspecto engloba também os mecanismos de informação com clientes e fornecedores como "*call centers*" e mecanismos de B2B e B2C.

Os aspectos de informação e comunicação dentro da estrutura de controles internos da empresa são as bases para que os colaboradores entendam seu papel dentro dessa estrutura e tenham disponíveis as informações necessárias e assertivas para a execução de suas atividades, em suma, a informação é o combustível que move as organizações.

### 6.4.5 Monitorização




A estrutura de controles internos sofre mudanças e evolui com o tempo. Assim, um controle eficaz em um cenário passado pode se tornar menos eficaz ou até obsoleto, dependendo das mudanças ocorridas na Empresa, em sua indústria de atuação ou no ambiente externo.

Dessa forma, a estrutura de controles internos deve ser monitorizada para avaliar a qualidade e a atualização dos controles no tempo. Esse objetivo é atingido com atividades recorrentes de monitorização ou procedimentos de avaliações independentes periódicas ou, ainda, uma combinação desses dois mecanismos.

A freqüência dos procedimentos de avaliações independentes depende de uma análise dos riscos aplicáveis aos processos, bem como da eficiência das atividades recorrentes de monitorização.

Em ambos os casos, as deficiências dos controles internos devem ser reportadas tempestivamente à Gerência e, dependendo do impacto dessas deficiências, à Alta Administração.

As principais atividades de monitorização incluem:

- ✓ Conciliações: comparações entre os valores registrados nos relatórios das áreas operacionais e os valores apresentados pelos demonstrativos

contábeis fornecem mecanismos de verificação de erros e exceções que podem identificar falhas na estrutura de controles internos da Empresa.

- ✓ Agentes Externos: comunicações de agentes externos (clientes, fornecedores, órgãos reguladores, instituições financeiras, etc.) comparados com os relatórios internos podem identificar inconsistências e falhas na estrutura de controles internos.
- ✓ Inventário Periódico: dados dos sistemas de informação da Empresa são comparados com contagens físicas periódicas e a análise das divergências fornece base para identificação de falhas na estrutura de controles internos.
- ✓ Auditores Internos e Externos: revisões realizadas pelos auditores identificam oportunidades de melhoria nos controles internos da Empresa.
- ✓ *Self-assessments*: auto-avaliações das áreas operacionais realizadas pelos colaboradores que executam as atividades de controle podem identificar pontos de melhoria e atualização da estrutura de controles internos.

Os aspectos de monitorização são essenciais para avaliar a estrutura de controles internos, verificando sua eficiência em minimizar a exposição da empresa aos seus riscos internos e externos.

# 7. CONCLUSÃO

O movimento em torno das boas práticas de controles internos veio para ficar e não pode ser identificado como mais uma onda da administração. Desde seu nascimento, nos Estados Unidos na década de 80, os mecanismos de governança corporativa vem proporcionando melhoras significativas na gestão das empresas e no ambiente regulatório, além de mais proteção aos investidores.

Os grandes escândalos nos Estados Unidos demonstram que apesar dos grandes avanços nos último anos, os acionistas ainda estão propensos a serem expropriados mediante práticas não recomendáveis. Os estudiosos das teorias de governança corporativa passam por um momento de grande desafio.

O grande desafio dos teóricos e estudiosos de governança corporativa e teoria das organizações atualmente é encontrar uma maneira de alinhar esses interesses, criando mecanismos de monitoramento que permitam um maior controle da gestão. As autoridades americanas optaram por endurecer as penas aos infratores, mas essa é a solução mais prática e fácil. A solução definitiva deve passar por uma intensa investigação e inúmeras pesquisas, sendo esse tema de grande importância para futuros estudos.

O papel desempenhado por um framework acaba por fazer com que os novos objetivos permeiem as atividades em todos os níveis: estratégico, tático e operacional. A adoção de um framework e uma metodologia costuma levar as instituições a inserir esses novos componentes inclusive nas atividades de planejamento e gestão, daí a importância de implantar da forma correta o Sistema de Controles Internos.

Como ponto de partida, a assimilação dessa nova cultura é, portanto, fator fundamental para formar o ambiente de controle favorável a essa mudança.

Considera-se, ainda, que existem fatores que tornam o processo de implantação mais fácil, tal como o reconhecimento de que os controles existentes na instituição podem fazer parte do novo sistema, bem como o uso de ferramentas que podem aumentar a abrangência e a profundidade das avaliações.

Embora os controles internos possam ajudar a atenuar riscos, eles não os eliminam completamente. Controles internos somente podem fornecer segurança

razoável – mas não absoluta – de que os objetivos de uma companhia foram alcançados. Os controles internos são, afinal de contas, construídos por processos que envolvem pessoas e, assim, estão sujeitos a todas as limitações pertinentes ao envolvimento humano. Os controles internos podem ser deliberadamente logrados por atos fraudulentos praticados por pessoas ou por conspirações entre funcionários.

Esses controles podem ser inadvertidamente enfraquecidos por julgamento equivocado, negligência, distração ou outras falhas nos processos ou procedimentos.

E também podem ser debilitados ou até mesmo eliminados por restrições de recursos. Os custos relativos e os benefícios dos controles internos devem ser continuamente reavaliados.

A Lei Sarbanes-Oxley e as suas regras e regulamentações complexas que gera confusão e consternação na comunidade empresarial é simplesmente uma forma encontrada pelo governo para estabelecer recursos legais nos preceitos básicos das práticas empresariais. E a concentração do foco especialmente na governança corporativa e na transparência das informações financeiras simplesmente faz despertar o senso empresarial ético.

O estabelecimento desses novos procedimentos para os controles internos e para a certificação executiva representa uma alteração de curso essencial para as companhias de capital aberto. Para aquelas empresas que não tinham uma estrutura básica para atender a esses processos agora correm contra o tempo para atende-las. Mas muitas companhias não vão precisar começar do ponto zero, elas estarão aptas a adaptar processos já existentes para cumprir as exigências de controles internos da nova Lei.

Mas as novas regras impõem um custo: essas mudanças necessitarão de alterações significativas nos procedimentos e nas práticas, bem como na vida cotidiana de muitos executivos e de pessoas que a eles se reportam.

E por fim, na e complexidade da Lei residem uma premissa simples: a boa governança corporativa e as práticas éticas do negócio não são mais requintes – são leis. E o cumprimento dessa Lei não é uma tarefa difícil desde que se adotem o procedimento de uma Governança Corporativa.

## 8. REFERÊNCIAS BIBLIOGRÁFICAS


Baraldi, Paulo. *Gestão de Riscos*. 1ª. ed. São Paulo: Editora Campus, 2004

DUARTE JR., Antonio M. *Gestão de Riscos no Brasil*. 1ª. ed. Rio de Janeiro: Financial Consultoria, 2003.

Committee of Sponsoring Organization of the Treadway Commission (COSO). *Enterprise risk management framework,* 2003.

Bernstein, Peter L. *Desafio dos Deuses.* São Paulo: Editora Campus, 1997.

Lam James. *Enterprise Risk Management*: from incetives to controls. Jonh Wiley & Sons, 2003.

DeLoach, James. *Enterprise-wide Risk Management*: strategies for linking risk and opportunity. Financial Times. Prentice Hall, 2000.

Cicco, Francesco de. Revista E-manager. *A Gestão de Riscos no Século XXI* - Edição 01/2003.

COMISSÃO DE VALORES MOBILIÁRIOS, disponível em www.cvm.gov.br, consultado em 30/01/2006.

DELOITTE TOUCHE TOHMATSU, disponível em www.deloitte.com.

IBGC. Código Brasileiro de Melhores Práticas de Governança Corporativa. Edição Ampliada , 2004, disponível em www.ibgc.org.br , consultado em 15/03/2006.

LA PORTA, R. LOPEZ-DE-SILANES, F. SHLEIFER, A. VISHNY, R. Investor Protection and Corporate Governance. Nber Working Paper, disponível em www.nber.org.

LA PORTA, R. LOPEZ-DE-SILANES, F. SHLEIFER, A. VISHNY, R. Legal Determinants of External Finance. The journal of Finance, Vol. LII n 3, july, 1997.

LODI, J.B. Governança Corporativa – O governo da Empresa e o Conselho de Administração. Rio de Janeiro: Editora Campus, 2000.

LUSTOSA, E.A. O papel dos Fundos de Pensão. I *workshop* Internacional Investidores Institucionais: Governança Corporativa & Relações com Investidores. Rio de Janeiro, outubro de 2000.

MAHONEY, W.F. Relações com Investidores. Rio de Janeiro: IMF Editora 1997.

MALUF, J.A. Seminário sobre Governança Corporativa. Organizado pela Bradesco Templeton Asset Management, São Paulo, 2000.

MARTINS, G. A. e LINTZ A. Guia para Elaboração de Monografias e Trabalhos de Conclusão de Curso. São Paulo: Editora Atlas, 2000.

MB ASSOCIADOS. Desafios e Oportunidades para o Mercado de Capitais Brasileiro. Projeto realizado par aa Bolsa de Valores de São Paulo. São Paulo. Maio, 2000.

MCKINSEY & COMPANY. Investor Opinion Survey on Corporate Governance. London, July, 2002.

MERRIL LYNCH & CO. Tell Sid to tell João to buy Stocks. Merril Lynch Latin America, October, 2000.

NEW YORK STOCK EXCHANGE, disponível em www.nyse.com , consultado em 15/02/2006.

OECD - *ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT*. OECD *Principles of Corporate Governance*, Paris, 1999.

ROCCA, C. A. e outros. Mercado de Capitais e a retomada do crescimento econômico – Os novos desafios da Bovespa. Trabalho realizado pra a Bolsa de Valores de São Paulo. São Paulo, Abril 1998.

ROSENBERG, H. Mudança de Lado – A luta de Robert A. G. Monks pela Governança Corporativa nos EUA. Rio de Janeiro, Editora Campus, 2000.

VALOR ECONÔMICO. Sarbanes-Oxley é uma reação aos escândalos. Valor Econômico, Ano 3, número 614, caderno de finanças, 11/11/2002.

YIN, R. K. Estudo de Caso – Planejamento e Métodos. 2ª Edicao. Porto Alegre: Bookman, 2001.

ZINGALES, L. Corporate Governance. NBER Working Paper 6309, consultado no www.nber.org/papers/w6309 em 30/01/2006.

Aveiro, D. (2002). Organização da Função Informática. Instituto Superior Técnico. Lisboa, Universidade Técnica de Lisboa.

Castela, N. (2001). Recolha, Análise e Validação de Informação para Modelação de Processos de Negócio. Instituto Superior Técnico. Lisboa, Universidade Técnica de Lisboa.

Champlain, J. J. (1998). Auditing Information Systems: a comprehensive reference guide. New York, John Wiley & Sons, Inc.

Colbert, J. L. and P. L. Bowen, Eds. (2002). *A Comparison of Internal Controls: COBIT, SAC, COSO and SAS 55/78, Information Systems Audit and Control Association.*

Curtis, M. B. and F. H. Wu (2000). *"The Components of a Comprehensive Framework of Internal Control."* CPA Journal.

Galloway, D. J. (1994). Control Models in Perspective. The Internal Auditor. 51: pp. 46-52.

Hermanson, H. M. (2003). "COSO: *More Relevante Now Than Ever." Internal Auditing* 18(4): pp. 3-6.

Mendes, R. (2001). Modelação de Estratégia de Negócio: Representação, Alinhamento e Operacionalização. Instituto Superior Técnico. Lisboa, Universidade Técnica de Lisboa.

Moran, J. (2001). *"Applying Best Practice Internal Control in the European Commission." Accountancy Ireland.*

Namee, D. M. (1997). *Risk-Based Auditing. Internal Auditor.* 54: pp. 22-27.

O'Connel, P. (1999). *Internal Control Standards.*

Pathak, J. (2003). *"Internal Audit E-Commerce Controls." Internal Auditing.*

Sinogas, P. (2002). Modelação de Processos de Negócio. Instituto Superior Técnico. Lisboa, Universidade Técnica de Lisboa.

Vasconcelos, A. (2001). Arquitectura de Sistemas de Informação no Contexto do Negócio. Instituto Superior Técnico. Lisboa, Universidade Técnica de Lisboa.

Weigand, H. and A. d. Moor (2001). *Framework for the Normative Analysis of Workflow Loops. Sixth International Workshop on the Language-Action Perspective on Communication Modelling* (LAP 2001), Montreal - Canada.

GUIA PARA MELHORAR A GOVERNANÇA CORPORATIVA ATRAVÉS DE EFICAZES CONTROLES INTERNOS – LEI SARBANES-OXLEY. São Paulo. Deloitte Touche Tohmatsu Auditores Independentes.

JORNAL VALOR ECONÔMICO – Cad. F – Especiais – 11/08/2004 – Pág. 1 e 2 – F2, Especial Sarbanes Oxley.

Adaptação à Lei Sarbanes-Oxley, acesso em 22/03/06 às 17h08 <http://especiais.valoronline.com.br/seminarios/Sarbanes_Oxley/pdf.htm>.

Governança Brasileira Está em Primeiro na AL, acesso: 15/03/2006 às 13h15 <http://www.ibgc.org.br/ibConteudo.asp?IDArea=534&IDp=109>.

Guide Risk Management.

Gestão de Riscos - AS/NZS 4360

FERREIRA, LUIZ EDUARDO ALVES; VALENTE, ALCEU NORBERTO. *Manual da Audit – versão 1.3 "Internal Control - Integrated Framework"* - http://www.coso.org; Artigo reproduzido no dia 05 de abril de 2002. GRA CAMPINAS (SP) por Grupo de Risco.

GHERMAN, MARCELO. Controles Internos - Buscando a solução adequada - Parte II. artigo publicado em 16/03/2005.

Enterprise Risk Management - Integrated Framework - Executive Summary - September 2004, dados extraídos do site: http://www.checkuptool.com.br/artigo_06.htm.

American Institute of Certified Public Accountants (AICPA). 1983. Audit Risk and Materiality in Conducting an Audit (SAS 47).

American Institute of Certified Public Accountants (AICPA). 1988a. Communication of Internal Control Structure Related Matters Noted in an Audit (SAS 60).

American Institute of Certified Public Accountants (AICPA). 1988b. Consideration of the Internal Control Structure in a Financial Statement Audit (SAS 55).

American Institute of Certified Public Accountants (AICPA). 1990. Consideration of the Internal Control Structure in a Financial Statement Audit (Audit Guide for SAS 55).

American Institute of Certified Public Accountants (AICPA). 1993. Reporting on an Entity's Internal Control Structure over Financial Reporting (Statement on Standards for Attestation Engagements 2).

American Institute of Certified Public Accountants (AICPA). 1995. "Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS No. 55" (SAS 78).

Committee of Sponsoring Organizations of the Treadway Commission (CSOTC). 1992. Internal Control - Integrated Framework (COSO Report).

Information Systems Audit and Control Foundation (ISACF). 1995. COBIT: Control Objectives for Information and related Technology.

Institute of Internal Auditors Research Foundation (IIARF). 1991, revised 1994. Systems Auditability and Control.

Winters, A.J., and D.M. Guy. 1992. Internal Control: Progress and Perils. Proceedings of the 1992 Deloitte & Touche/University of Kansas Symposium on Auditing Problems, pp.177-191.

*Janet L. Colbert, Ph.D., CPA, CIA* is the Meany-Holland professor of accounting at Western Kentucky University in Bowling Green, KY, USA.

*Paul L. Bowen, Ph.D., CPA* is a lecturer in the department of commerce at the University of Queensland in Brisbane, Queensland, Australia.

## 9. GLOSSÁRIO

SEC - (*Securities and Exchange Commission,* instituição equivalente à brasileira Comissão de Valores Mobilários – CVM);

*Compliance* – Conformidade;

*Business* - Negócios;

IASB (*International Accounting Standards Board) -*

*Framework* - Estrutura de Controles Internos;

*Hackers* - invasores de rede de computadores, buscando informações alheias;

*Stakeholders* - termo utilizado para denominar os clientes, acionistas, colaboradores, mercado e investidores;

CIOs (Chief Information Officer) - executivo responsável pelo planejamento e pela implementação da tecnologia da informação;

*Staff* - equipe de funcionários;

Sine qua non - sem o qual, não;

# 10. ANEXOS

## 10.1 Matriz de Riscos e Controles do Ciclo de Suprimentos

| Subprocesso: Estruturação do Processo | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.01 | Atividades executadas em desacordo com as políticas, normas e procedimentos estabelecidos. | Aderência as Regras | |
| R.02 | Acesso às transações do Sistema ERP por pessoal não autorizado ou em desacordo com o limite de alçada. | Acesso/Limite de Autoridade | |
| R.03 | Informações desatualizadas e/ou não consistentes. | Integridade das Informações | |
| R.04 | Gerenciamento e/ou focalização inadequados dos processos e das atividades críticas. | Objetivos Estratégicos | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| 1.1 Documentação atualizada e formalmente aprovada pela Alta Administração e disponibilizada através de ferramentas de comunicação referentes às atividades executadas no Processo de Suprimentos. | | Atividade de Controle | | |
| 1.2 Organograma definido, detalhando as responsabilidades da área, aprovado e divulgado à <NOME DA EMPRESA CLIENTE>. | | Ambiente de Controles e Negócios | | |
| 1.3 Descrição definida e formalizada das atividades para os cargos da área contemplando as responsabilidades e dos limites de alçada para cada processo ("*job description*"). | | Ambiente de Controles e Negócios | | |
| 1.4 Segregação de funções entre os responsáveis por:<br>• Seleção e homologação de fornecedores.<br>• Manutenção do cadastro de fornecedores.<br>• Emissão de pedidos de compra.<br>• Contratação de fornecedores.<br>• Gerenciamento dos contratos.<br>• Liberação para pagamento.<br>• Inclusão e processamento dos pagamentos. | | Atividade de Controle | | |
| 1.4 Segregação de funções entre os responsáveis por:<br>• Seleção e homologação de fornecedores.<br>• Manutenção do cadastro de fornecedores.<br>• Emissão de pedidos de compra.<br>• Contratação de fornecedores. | | Atividade de Controle | | |

| Subprocesso: Estruturação do Processo | | | |
|---|---|---|---|
| **Riscos Identificados** | | **Categoria do Risco** | **Avaliação do Risco** |
| **R.01** | Atividades executadas em desacordo com as políticas, normas e procedimentos estabelecidos. | Aderência as Regras | |
| **R.02** | Acesso às transações do Sistema ERP por pessoal não autorizado ou em desacordo com o limite de alçada. | Acesso/Limite de Autoridade | |
| **R.03** | Informações desatualizadas e/ou não consistentes. | Integridade das Informações | |
| **R.04** | Gerenciamento e/ou focalização inadequados dos processos e das atividades críticas. | Objetivos Estratégicos | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| **Descrição** | **Status** | **Componente COSO** | | |
| • Gerenciamento dos contratos.<br>• Liberação para pagamento.<br>• Inclusão e processamento dos pagamentos. | | | | |
| 1.5 Estrutura de perfis de acesso, no Sistema ERP e nos sistemas operacionais, parametrizada para permitir o acesso às transações críticas somente a usuários autorizados. | | Atividade de Controle | | |
| 1.6 Monitoramento do acesso às transações críticas do Sistema ERP, tais como:<br>• Criação de Solicitação de Ferramental.<br>• Criação de pedidos de compra.<br>• Alteração de pedidos de compra.<br>• Aprovação de pedidos de compra.<br>• Criação de documento diretamente no Contas a Pagar.<br>• Liberação de faturas bloqueadas (bloqueio "R"). | | Monitorização | | |
| 1.7 Sistema único para gerenciamento das atividades relacionadas ao Processo de Suprimentos. | | Atividade de Controle | | |
| 1.8 Gestão centralizada da quantidade e localização dos itens de ferramental e alocação aos respectivos programas específicos. | | Monitorização | | |
| 1.9 Trilha de auditoria habilitada nos sistemas que suportam as atividades do Processo de Suprimentos, armazenando todas as atividades realizadas. | | Atividade de Controle | | |
| 1.10 Cadastro único de materiais, revisado e atualizado periodicamente, que permita a identificação de itens de maneira rápida e precisa. | | Atividade de Controle | | |
| 1.11 Cadastro único de fornecedores habilitados para fornecimento de materiais e execução de serviços. | | Atividade de Controle | | |
| 1.12 Relatórios gerenciais e de exceção baseados em indicadores de desempenho para suportar as atividades e a tomada de | | Atividade de Controle | | |

| Subprocesso: Estruturação do Processo | | | |
|---|---|---|---|
| **Riscos Identificados** | | **Categoria do Risco** | **Avaliação do Risco** |
| **R.01** | Atividades executadas em desacordo com as políticas, normas e procedimentos estabelecidos. | Aderência as Regras | |
| **R.02** | Acesso às transações do Sistema ERP por pessoal não autorizado ou em desacordo com o limite de alçada. | Acesso/Limite de Autoridade | |
| **R.03** | Informações desatualizadas e/ou não consistentes. | Integridade das Informações | |
| **R.04** | Gerenciamento e/ou focalização inadequados dos processos e das atividades críticas. | Objetivos Estratégicos | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| **Descrição** | **Status** | **Componente COSO** | | |
| decisões. | | | | |
| 1.13 Indicadores de risco para a gestão do processo, considerando:<br>• Seleção e homologação de fornecedores.<br>• Subcontratação de fabricação.<br>• Gerenciamento de subcontratação.<br>• Liberação de pagamento. | | Avaliação de Riscos | | |

| Subprocesso: Desenvolvimento, Seleção e Homologação de Fornecedores | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.05 | Seleção e homologação de fornecedores que não atendam aos padrões requeridos pela <NOME DA EMPRESA CLIENTE>. | Aderência às Regras | |
| R.06 | Definição de fornecedores sem capacidade financeira ou de fornecimento de materiais e/ou serviços. | Dependência de Fornecedores/Parceiros | |
| R.07 | Acesso aos cadastros de fornecedores, materiais e serviços por pessoal não autorizado ou em desacordo com o limite de alçada. | Acesso e Segurança das Informações/Limite de Autoridade | |
| R.08 | Informações incorretas, incompletas ou redundantes no cadastro de fornecedores. | Integridade das Informações | |
| R.09 | Contratos de fornecimento de material/prestação de serviços que não assegurem o cumprimento das obrigações pelos fornecedores. | Obrigações Contratuais | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| 2.1 Definição formal de pré-requisitos a serem considerados para seleção de fornecedor. | | Ambiente de Controles/ Negócios | | |
| 2.2 Seleção de fornecedores conforme pré-requisitos formalmente estabelecidos. | | Atividade de Controle | | |
| 2.3 Avaliação formal do fornecedor antes de sua inclusão no cadastro, considerando a análise em associações comerciais. | | Atividade de Controle | | |
| 2.4 Numeração seqüencial única e atribuída automaticamente aos fornecedores cadastrados no sistema. | | Atividade de Controle | | |
| 2.5 Relacionamento estabelecido entre o serviço prestado e/ou materiais disponíveis para compra com os fornecedores habilitados em cadastro. | | Atividade de Controle | | |
| 2.6 Consistências automáticas para restringir o cadastramento de fornecedores em duplicidade e/ou o preenchimento incorreto de campos-chave (exemplo: CNPJ/CPF). | | Atividade de Controle | | |
| 2.7 Utilização de mecanismos de aprovação eletrônica para inclusão de novos fornecedores ou manutenção de seus dados críticos (exemplo: CNPJ). | | Atividade de Controle | | |
| 2.8 Identificação automática de fornecedores não utilizados por longo período, sendo efetuado o bloqueio, quando aplicável. | | Atividade de Controle | | |
| 2.9 Revisões periódicas da situação financeira, qualificação técnica e qualidade dos fornecedores. | | Atividade de Controle | | |
| 2.10 Emissão de contratos-padrão revisados pela área Jurídica. | | Atividade de Controle | | |
| 2.11 Registro em sistema dos | | Atividade de | | |

| Subprocesso: Desenvolvimento, Seleção e Homologação de Fornecedores | | | |
|---|---|---|---|
| | Riscos Identificados | Categoria do Risco | Avaliação do Risco |
| R.05 | Seleção e homologação de fornecedores que não atendam aos padrões requeridos pela <NOME DA EMPRESA CLIENTE>. | Aderência às Regras | |
| R.06 | Definição de fornecedores sem capacidade financeira ou de fornecimento de materiais e/ou serviços. | Dependência de Fornecedores/Parceiros | |
| R.07 | Acesso aos cadastros de fornecedores, materiais e serviços por pessoal não autorizado ou em desacordo com o limite de alçada. | Acesso e Segurança das Informações/Limite de Autoridade | |
| R.08 | Informações incorretas, incompletas ou redundantes no cadastro de fornecedores. | Integridade das Informações | |
| R.09 | Contratos de fornecimento de material/prestação de serviços que não assegurem o cumprimento das obrigações pelos fornecedores. | Obrigações Contratuais | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| contratos/lista de preços de fornecedores com base nas informações da cotação/licitação vencedora. | | Controle | | |
| 2.12 Cadastramento de contratos apenas após a entrega e verificação completa da documentação-<br>-suporte exigida pelas normas da <NOME DA EMPRESA CLIENTE> e pela legislação vigente (exemplos: certidões negativas, contrato social e visto de trabalho). | | Atividade de Controle | | |
| 2.13 Definição contratual da responsabilidade de empresas terceirizadas pelos pagamentos realizados a seus colaboradores (exemplos: salários e encargos). | | Atividade de Controle | | |
| 2.14 Bloqueio da emissão de contratos para fornecedores, materiais e serviços não cadastrados. | | Atividade de Controle | | |

| Subprocesso: Subcontratação de Projetos e Fabricação | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.10 | Contratação de fornecedores e/ou prestadores de serviços não autorizados ou que não atendam aos critérios (fornecimento/prestação de serviços) estabelecidos pela NOME DA EMPRESA CLIENTE. | Aderência às Regras | |
| R.11 | Definição de ferramental (projetos e fabricação) em desacordo com as necessidades da NOME DA EMPRESA CLIENTE. | Obrigações Contratuais | |
| R.12 | Contratação de fornecedores e/ou prestadores de serviços sem a documentação exigida pela legislação vigente. | Legal | |
| R.13 | Contratação de fornecedores exclusivos ou com forte dependência da NOME DA EMPRESA CLIENTE. | Legal | |
| R.14 | Solicitação de ferramental em desacordo com o limite de autoridade. | Limite de Autoridade | |
| R.15 | Informações incorretas, incompletas ou redundantes para contratação de projetos e fabricação de ferramental. | Integridade das Informações | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| 3.1 Contratação de serviços e Subcontratos pela Área por colaborador responsável. | | Atividade de Controle | | |
| 3.2 Registro em sistema da solicitação/requisição de serviços ou material pela área requisitante, considerando aspectos técnicos, quando aplicável (necessidade de compra de serviço ou material), e detalhamento da necessidade. | | Atividade de Controle | | |
| 3.3 Definição da quantidade de horas e matéria-<br>-prima a serem utilizadas na elaboração do material com base em documentos atualizados conforme histórico de execução de projetos/ fabricação. | | Atividade de Controle | | |
| 3.4 Realização de cotações e/ou concorrências para contratação de serviços e/ou aquisição de materiais com base nas requisições de materiais/ serviços aprovadas e na lista de fornecedores homologados. Nesse processo, considerar os critérios de custo, qualidade e prazos. | | Atividade de Controle | | |
| 3.5 Aprovação de requisições de compra, pedidos de compra e contratos por colaborador autorizado, de acordo com as estratégias de liberação definidas pela <NOME DA EMPRESA CLIENTE><br>Alterações em documentos aprovados submetidas à nova aprovação. | | Ambiente de Controles/ Negócios | | |
| 3.6 Registro eletrônico dos pedidos de compra emitidos. | | Atividade de Controle | | |
| 3.7 Envio formal de pedido de compra aprovado ao fornecedor, autorizando a execução do serviço/ fabricação solicitado. | | Atividade de Controle | | |

| Subprocesso: Subcontratação de Projetos e Fabricação | | | |
|---|---|---|---|
| **Riscos Identificados** | | **Categoria do Risco** | **Avaliação do Risco** |
| **R.10** | Contratação de fornecedores e/ou prestadores de serviços não autorizados ou que não atendam aos critérios (fornecimento/prestação de serviços) estabelecidos pela NOME DA EMPRESA CLIENTE. | Aderência às Regras | |
| **R.11** | Definição de ferramental (projetos e fabricação) em desacordo com as necessidades da NOME DA EMPRESA CLIENTE. | Obrigações Contratuais | |
| **R.12** | Contratação de fornecedores e/ou prestadores de serviços sem a documentação exigida pela legislação vigente. | Legal | |
| **R.13** | Contratação de fornecedores exclusivos ou com forte dependência da NOME DA EMPRESA CLIENTE. | Legal | |
| **R.14** | Solicitação de ferramental em desacordo com o limite de autoridade. | Limite de Autoridade | |
| **R.15** | Informações incorretas, incompletas ou redundantes para contratação de projetos e fabricação de ferramental. | Integridade das Informações | |

| Melhores Práticas de Controle | | | | |
|---|---|---|---|---|
| **Descrição** | **Status** | **Componente COSO** | **Situação Atual** | **Recs** |
| 3.8 Análise da composição de custo apresentada pelo fornecedor para definição do preço desejado (preço-objetivo) para contratação de serviços. | | Atividade de Controle | | |
| 3.9 Consistência automática entre requisições de serviço/materiais, cotações, pedidos de compra e contratos aprovados, a fim de impossibilitar:<br>• Contratos e/ou pedidos de compra com quantidades e/ou preços superiores aos definidos nas cotações.<br>• Pedidos de compra com valores que superem os dos contratos.<br>• Divergências nos demais campos cadastrados (exemplos: código do subcontratado e/ou do fornecedor).<br>• Contratos e/ou pedidos de compra referentes a material ou serviço não solicitado. | | Atividade de Controle | | |
| 3.10 Registro dos centros de custo na requisição, pedido ou contrato de compra (no caso de rateio por centros de custo fixos) para rateio dos valores. | | Atividade de Controle | | |
| 3.11 Revisão periódica de materiais ou dos projetos em elaboração com os desenhos aprovados ou as solicitações realizadas. | | Monitorização | | |
| 3.12 Conferência dos valores/quantidades negociados com os fornecedores com a estimativa realizada na criação Autorização de Serviço. | | Monitorização | | |
| 3.13 Revisão periódica dos fornecedores contratados, considerando a concentração/ dependência em relação à <NOME DA EMPRESA CLIENTE>. | | Monitorização | | |

| Subprocesso: Gerenciamento da Subcontratação | | | |
|---|---|---|---|
| **Riscos Identificados** | | **Categoria do Risco** | **Avaliação do Risco** |
| **R.16** | Gerenciamento inadequado das atividades desempenhadas pelo fornecedor. | Aderência às Regras | |
| **R.17** | Elevação de custos em contratos não refletindo a realidade do mercado ou o orçamento predefinido. | Obrigações Contratuais/Aderência às Regras | |
| **R.18** | Não-cumprimento das obrigações fiscais e tributárias pelas empresas contratadas (co-responsabilidade). | Legal | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| **Descrição** | **Status** | **Componente COSO** | | |
| 4.1 Acompanhamento dos serviços prestados, considerando:<br>• Execução dos serviços estabelecidos em contrato.<br>• Comparação entre os valores cobrados e os previstos.<br>• Existência de fornecedores prestando serviços após o vencimento do contrato.<br>• Reavaliação periódica dos custos dos serviços com base na realidade do mercado. | | Atividade de Controle | | |
| 4.2 Acompanhamento da quantidade de materiais em poder de terceiros (prestadores de serviços e subcontratados). | | Atividade de Controle | | |
| 4.3 Acompanhamento mensal das despesas incorridas de acordo com orçamento pré-aprovado. | | Monitorização | | |
| 4.4 Elaboração e cálculo automático de indicadores de desempenho dos fornecedores com base em critérios preestabelecidos. | | Atividade de Controle | | |
| 4.5 Acompanhamento das obrigações fiscais e tributárias pelas empresas contratadas. | | Atividade de Controle | | |

| Subprocesso: Recebimento de Projetos e Ferramental | | | |
|---|---|---|---|
| **Riscos Identificados** | | **Categoria do Risco** | **Avaliação do Risco** |
| **R.19** | Recebimento de materiais não solicitados ou em desacordo com o solicitado pela <NOME DA EMPRESA CLIENTE>. | Obrigações Contratuais | |
| **R.20** | Recebimento de materiais em desacordo com o padrão da <NOME DA EMPRESA CLIENTE>. | Aderência às Regras | |
| **R.21** | Atraso no processo de conferência e aprovação dos serviços prestados. | Obrigações Contratuais | |
| **R.22** | Registro incorreto, incompleto ou em duplicidade de informações de projetos/ferramental recebidas. | Integridade das Informações | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| **Descrição** | **Status** | **Componente COSO** | | |
| 5.1 Programação tempestiva dos projetos/ mercadorias a serem recebidos pela área de Recebimento. | | Atividade de Controle | | |
| 5.2 Consistência automática entre as quantidades recebidas (contagem "cega") e os pedidos de compra aprovados, identificando as divergências. | | Atividade de Controle | | |
| 5.3 Consistências automáticas no recebimento de materiais/serviços, a fim de evitar o registro de notas fiscais:<br>• Que não estejam vinculadas a um pedido de compra.<br>• Que apresentem quantidade e/ou preço dos itens superiores aos constantes nos pedidos.<br>• Que apresentem divergências em relação aos pedidos (exemplos: item, condição comercial, fornecedor, etc.).<br>• Com informações incorretas ou em duplicidade (exemplos: data de vencimento, valor e fornecedor). | | Atividade de Controle | | |
| 5.4 Cálculo automático da quantidade pendente do pedido de compra no caso de entregas parciais e/ou incompletas. | | Atividade de Controle | | |
| 5.5 Restrição quanto ao registro de recebimentos com data retroativa. | | Atividade de Controle | | |
| 5.6 Inspeção da qualidade do material recebido conforme os padrões de qualidade da <NOME DA EMPRESA CLIENTE>. | | Atividade de Controle | | |
| 5.7 Avaliação e correção tempestiva das pendências identificadas no recebimento. | | Atividade de Controle | | |
| 5.8 Registro eletrônico da conferência do serviço prestado por colaborador requisitante autorizado (Folha de Registro de Serviço - FRS). | | Atividade de Controle | | |
| 5.9 Centralização, em área específica, do processo de conferência da nota fiscal com a mercadoria/ serviço prestado (exemplo: para materiais, essa | | Atividade de Controle | | |

| Subprocesso: Recebimento de Projetos e Ferramental | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.19 | Recebimento de materiais não solicitados ou em desacordo com o solicitado pela <NOME DA EMPRESA CLIENTE>. | Obrigações Contratuais | |
| R.20 | Recebimento de materiais em desacordo com o padrão da <NOME DA EMPRESA CLIENTE>. | Aderência às Regras | |
| R.21 | Atraso no processo de conferência e aprovação dos serviços prestados. | Obrigações Contratuais | |
| R.22 | Registro incorreto, incompleto ou em duplicidade de informações de projetos/ferramental recebidas. | Integridade das Informações | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| conferência é realizada no recebimento físico da mercadoria). | | | | |
| 5.10 Utilização de mecanismos de aprovação eletrônica dos recebimentos para pagamento, após a conferência da execução do serviço (FRS), por colaborador responsável. | | Atividade de Controle | | |
| 5.11 Baixa automática dos pedidos de compra, após o recebimento, com base no registro das respectivas notas fiscais. | | Atividade de Controle | | |
| 5.12 Monitoramento tempestivo dos pedidos de compra em aberto, endereçando ações para solução dos casos pendentes. | | Monitorização | | |

| Subprocesso: Processamento dos Pagamentos | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.23 | Informações incorretas, incompletas ou em duplicidade registradas no Contas a Pagar. | Integridade das Informações | |
| R.24 | Autorização para pagamento de serviços e contratos não realizados ou em desacordo com o estabelecido. | Obrigações Contratuais/Limite de Autoridade | |
| R.25 | Pagamentos realizados sem a documentação-suporte adequada. | Aderência às Regras | |
| R.26 | Pagamentos e/ou alterações em informações de pagamentos realizados por pessoal não autorizado ou em desacordo com o limite de alçada. | Acesso e Segurança das Informações/Limite de Autoridade | |
| R.27 | Pagamentos não realizados ou realizados em desacordo com o estabelecido em contrato e/ou pedido de compra. | Obrigações Contratuais | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| 6.1 Estratégias de liberação para aprovação do pagamento, considerando:<br>• Limites de alçada.<br>• Critérios qualitativos (exemplos: tipo de serviço, centro de custo e usuário).<br>• Critérios quantitativos (exemplos: valor e quantidade). | | Ambiente de Controles/ Negócios | | |
| 6.2 Acesso à inclusão de pagamentos diretamente no Contas a Pagar restrito a colaboradores autorizados. | | Atividade de Controle | | |
| 6.3 Centralização do processo de conferência da documentação (exemplos: aprovação formal do serviço executado e nota fiscal com boleto bancário) e liberação de recursos (exemplos: transferências, emissão de cheques e DOCs) no Contas a Pagar. | | Atividade de Controle | | |
| 6.4 Consistências automáticas entre contratos/ pedidos de compra, pagamentos e registro de notas fiscais, a fim de impossibilitar:<br>• Pagamentos com quantidades e/ou preços superiores aos definidos em contrato/pedido de compra.<br>• Divergências nos demais campos cadastrados (exemplo: código do fornecedor). | | Atividade de Controle | | |
| 6.5 Transferência automática das informações referentes a materiais recebidos e serviços prestados para o Contas a Pagar, garantindo a integridade dos dados. | | Atividade de Controle | | |
| 6.6 Bloqueio de acesso a alterações do arquivo-<br>-texto da proposta de pagamento utilizado na integração com os bancos. | | Atividade de Controle | | |
| 6.7 Bloqueio do acesso à alteração dos dados das notas fiscais registradas no | | Atividade de Controle | | |

| Subprocesso: Processamento dos Pagamentos | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.23 | Informações incorretas, incompletas ou em duplicidade registradas no Contas a Pagar. | Integridade das Informações | |
| R.24 | Autorização para pagamento de serviços e contratos não realizados ou em desacordo com o estabelecido. | Obrigações Contratuais/Limite de Autoridade | |
| R.25 | Pagamentos realizados sem a documentação-suporte adequada. | Aderência às Regras | |
| R.26 | Pagamentos e/ou alterações em informações de pagamentos realizados por pessoal não autorizado ou em desacordo com o limite de alçada. | Acesso e Segurança das Informações/Limite de Autoridade | |
| R.27 | Pagamentos não realizados ou realizados em desacordo com o estabelecido em contrato e/ou pedido de compra. | Obrigações Contratuais | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| Contas a Pagar e da realização de pagamentos para fornecedores não cadastrados. | | | | |
| 6.8 Revisão tempestiva dos valores contratados com o fornecedor, considerando descontos de horas resultantes de retrabalhos realizados internamente. | | Atividade de Controle | | |
| 6.9 Acompanhamento mensal dos pagamentos realizados, através de relatórios, analisando:<br>• Valores de juros, multas e motivos que ocasionaram o pagamento em atraso.<br>• Variações entre o valor estimado do ferramental e o valor realmente pago ao fornecedor. | | Monitorização | | |

## 10.2 Matriz de Riscos e Controles do Ciclo de Receitas

| Subprocesso: Estruturação do Processo | | | |
|---|---|---|---|
| **Riscos Identificados** | | **Categoria do Risco** | **Avaliação do Risco** |
| **R.01** | Atividades executadas em desacordo com as políticas, normas e procedimentos estabelecidos. | Aderência às Regras | |
| **R.02** | Gerenciamento/focalização inadequada dos processos e atividades críticas. | Objetivos Estratégicos | |
| **R.03** | Aprovação por pessoa não autorizada ou não aderente aos níveis/limites de alçada pré-estabelecidos. | Limite de Autoridade | |
| **R.04** | Acesso às transações do Sistema ERP por pessoal não autorizado ou em desacordo com o limite de alçada. | Acesso e Segurança das Informações | |
| **R.05** | Informações incorretas, incompletas e/ou em duplicidade. | Integridade das Informações | |

| Melhores Práticas de Controle | | | | |
|---|---|---|---|---|
| **Descrição** | **Status** | **Componente COSO** | **Situação Atual** | **Recs** |
| 1.1 Documentação atualizada, formalmente aprovada pela alta administração e disponibilizada através de ferramentas de comunicação, referente às atividades do Processo de Receitas. | | Atividade de Controle | | |
| 1.2 Procedimentos de inclusão e manutenção de dados cadastrais centralizados em uma única área. | | Atividade de Controle | | |
| 1.3 Organograma descritivo, detalhando as responsabilidades dos envolvidos no processo, aprovado e divulgado à <NOME DA EMPRESA CLIENTE>. | | Ambiente de Controles e Negócios | | |
| 1.4 Descrição, definida e formalizada, das atividades para os cargos das áreas envolvidas, contemplando as responsabilidades e níveis/limites de alçada para cada processo ("job description"). | | Ambiente de Controles e Negócios | | |
| 1.5 Segregação entre as funções críticas do Processo de Receitas, garantindo a manutenção do nível de segurança e da independência das atividades.<br>Exemplos:<br>• Cobrança dos clientes<br>• Emissão de pedidos.<br>• Faturamento.<br>• Baixa de títulos.<br>• Conciliação bancária. | | Atividade de Controle | | |
| 1.6 Estrutura de perfis de acesso, nos sistemas ERP e legados, parametrizada de forma a permitir o acesso às transações críticas somente a usuários autorizados. | | Atividade de Controle | | |
| 1.7 Monitoramento de acesso às transações críticas, como por exemplo, do Sistema ERP: | | Monotirização | | |

| Subprocesso: Estruturação do Processo | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.01 | Atividades executadas em desacordo com as políticas, normas e procedimentos estabelecidos. | Aderência às Regras | |
| R.02 | Gerenciamento/focalização inadequada dos processos e atividades críticas. | Objetivos Estratégicos | |
| R.03 | Aprovação por pessoa não autorizada ou não aderente aos níveis/limites de alçada pré-estabelecidos. | Limite de Autoridade | |
| R.04 | Acesso às transações do Sistema ERP por pessoal não autorizado ou em desacordo com o limite de alçada. | Acesso e Segurança das Informações | |
| R.05 | Informações incorretas, incompletas e/ou em duplicidade. | Integridade das Informações | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| • xxxx | | | | |
| 1.8 Sistema único para gerenciamento das atividades relacionadas ao Processo de Receitas. | | Atividade de Controle | | |
| 1.9 Gestão centralizada do Processo de Receitas | | Monitorização | | |
| 1.10 Utilização de ferramenta de aprovação eletrônica para as atividades do processo. | | Atividade de Controle | | |
| 1.11 Trilha de auditoria habilitada nos sistemas que suportam as atividades do processo, armazenando todas as atividades realizadas. | | Atividade de Controle | | |
| 1.12 Cadastro único dos contratos, revisado e atualizado periodicamente, que permita a identificação de informações e aditivos contratuais. | | Atividade de Controle | | |
| 1.13 Cadastro único de materiais em estoque. | | Atividade de Controle | | |
| 1.14 Cadastro único de clientes e prazos disponíveis e habilitados para realização de vendas e transferência eletrônica para os demais sistemas corporativos (cadastro, gerencial e faturamento). | | Atividade de Controle | | |
| 1.15 Relatórios gerenciais e de exceção baseados em indicadores de desempenho para suportar as atividades e a tomada de decisões. | | Atividade de Controle | | |
| 1.16 Indicadores de risco para a gestão do processo, considerando:<br>• <xxxx> | | Avaliação de Riscos | | |
| 1.17 Definição de planos de capacitação dos colaboradores em suas atividades do processo de receitas. | | Atividade de Controle | | |

| Subprocesso: Análise/Concessão de Crédito e Aprovação de Clientes | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.06 | Concessão de limite de crédito em desacordo com as políticas da Companhia. | Crédito | |
| R.07 | Vendas a clientes com valores superiores ao limite de crédito. | Crédito | |
| R.08 | Vendas a clientes inadimplentes. | Crédito | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| 2.1 Limites de crédito e de financiamento formalmente estabelecidos para os clientes, considerando seu histórico de compras, capacidade de pagamento, política de prazos de vencimento, empréstimos de materiais/equipamentos concedidos. | | Atividade de Controle | | |
| 2.2 Aprovação eletrônica, por nível de alçada apropriado, quando das inclusões e modificações efetuadas nos limites de crédito cadastrados no sistema, considerando:<br>Responsabilidades do funcionário.<br>Risco da Companhia em função do limite de crédito concedido. | | Atividade de Controle | | |
| 2.3 Estabelecimento de classificação de risco para os clientes ("rating" / "credit scoring"). | | Atividade de Controle | | |
| 2.4 Determinação de prazos de validade para o limite concedido ao cliente, renovável somente após análise e aprovação formal. | | Atividade de Controle | | |
| 2.5 Cálculo automático do saldo do crédito disponível para cliente, considerando os pedidos de venda em aberto. | | Atividade de Controle | | |
| 2.6 Bloqueio automático do faturamento considerando:<br>• Validade do limite de crédito.<br>• Saldo de crédito insuficiente para o cliente.<br>• Inadimplência do cliente. | | Atividade de Controle | | |
| 2.7 Aprovação automática dos estouros de limite de crédito, conforme os níveis de alçada estabelecidos no Padrão Operacional. | | Ambiente de Controles e Negócios | | |
| 2.8 Revisão periódica dos limites de crédito estabelecidos e monitoramento das manutenções efetuadas. | | Monitorização | | |

| Subprocesso: Registro e Manutenção de Clientes (Cadastro) | | | |
|---|---|---|---|
| | Riscos Identificados | Categoria do Risco | Avaliação do Risco |
| R.09 | Ausência e/ou inadequada existência de informações cadastrais, em decorrência de:<br>– Cadastramento indevido e/ou não autorizado de clientes/prazos.<br>– Informações incorretas, incompletas ou redundantes no cadastro de clientes.<br>– Manutenção de clientes no cadastro que não atendam às políticas da Companhia. | Integridade | |
| R.10 | Prazos concedidos em desacordo com as políticas estabelecidas pela Cia. | Integridade | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| 3.1 Documentação atualizada das políticas e procedimentos para inclusão, alteração e desativação no cadastro de clientes e dos prazos concedidos. | | Atividade de Controle | | |
| 3.2 Estabelecimento de contratos de venda junto aos clientes. | | Atividade de Controle | | |
| 3.3 Cadastramento das distâncias dos destinos versus as unidades de origem, com base em aprovação formal e nível adequado de Gerência . | | Atividade de Controle | | |
| 3.4 Restrição de acesso, de acordo com as atribuições e responsabilidades dos funcionários, às principais transações que suportam o cadastro de clientes da Companhia. | | Atividade de Controle | | |
| 3.5 Segregação entre a função de modificação do cadastro de clientes e as funções de:<br>Aprovação e manutenção do limite de crédito.<br>Entrada de pedido de venda.<br>Definição de preços e descontos por cliente.<br>Liberação de pedidos bloqueados.<br>Contas a Receber (recebimento). | | Atividade de Controle | | |
| 3.6 Aprovação eletrônica, por nível de alçada apropriado, quando da inclusão de novos clientes e manutenção de seus dados críticos. | | Ambiente de Controles e Negócios | | |
| 3.7 Geração de código específico para cada cliente a cadastrar (definir em política), formado com informações básicas destes (exemplo: primeiros três números referem-se à unidade e cidade em que se encontra o cliente, e demais seguindo uma ordem seqüencial de categoria). | | Atividade de Controle | | |

| Subprocesso: Registro e Manutenção de Clientes (Cadastro) | | | |
|---|---|---|---|
| | Riscos Identificados | Categoria do Risco | Avaliação do Risco |
| R.09 | Ausência e/ou inadequada existência de informações cadastrais, em decorrência de:<br>– Cadastramento indevido e/ou não autorizado de clientes/prazos.<br>– Informações incorretas, incompletas ou redundantes no cadastro de clientes.<br>– Manutenção de clientes no cadastro que não atendam às políticas da Companhia. | Integridade | |
| R.10 | Prazos concedidos em desacordo com as políticas estabelecidas pela Cia. | Integridade | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| Revisar os códigos dos clientes já cadastrados, para aderir ao procedimento descrito acima. | | | | |
| 3.8 Classificação de clientes no cadastro, conforme segmento de mercado e potencial de relacionamento comercial com a Companhia. | | Atividade de Controle | | |
| 3.9 Inclusão do cliente no cadastro somente após aprovação do limite de crédito, conforme modalidade de recebimento (exemplo: venda a prazo). | | Atividade de Controle | | |
| 3.10 Procedimento formalizado para a classificação de clientes, de acordo com seus respectivos segmentos/categorias. | | Atividade de Controle | | |
| 3.11 Revisão periódica de segmento/categoria dos clientes cadastrados, definida em padrão, visando corroborar as condições comerciais em vigor. | | Monitorização | | |
| 3.12 Identificação automática dos clientes inativos por um longo período e de clientes com pendências cadastrais, definindo prazos-limite para sua atualização, efetuando seu bloqueio quando aplicável. | | Atividade de Controle | | |
| 3.13 Procedimento formalizado para a avaliação de eventuais pendências de recebimento quando da desativação de clientes do cadastro. | | Atividade de Controle | | |
| 3.14 Procedimento formalizado para a reintegração dos clientes desativados no sistema. | | Atividade de Controle | | |
| 3.15 Consistência automática para restringir o cadastramento de clientes em duplicidade e/ou o preenchimento incorreto de campos-chave (exemplos: CNPJ, CEP). | | Atividade de Controle | | |

| Subprocesso: Emissão dos Pedidos de Venda | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.11 | Definição de preços/condições comerciais em desvantagem para a Cia. Ou baseado em critérios divergentes dos estabelecidos. | Autoridade/Limite | |
| R.12 | Faturamento em desacordo com os valores negociados. | Autoridade/Limite | |
| R.13 | Retirada de mercadorias e/ou faturamento divergente dos valores acordados. | Autoridade/Limite | |
| R.14 | Liberação de pedidos não aprovados ou em desacordo com as políticas estabelecidas pela Companhia. | Autoridade/Limite | |
| R.15 | Alteração não autorizada das informações da programação (exemplos: preço, prazo e quantidade). | Autoridade/Limite | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| 4.1 Definição de limites de alçada em sistema para a aprovação de pedidos em desacordo com as políticas estabelecidas. | | Atividade de Controle | | |
| 4.2 Estabelecimento de prazo (horário limite) para compilação dos pedidos de venda. | | Atividade de Controle | | |
| 4.3 Disponibilização da posição dos estoques da <NOME DA EMPRESA CLIENTE> no sistema de pedidos, através de integração automática com o sistema ERP, para a confirmação de disponibilidade dos produtos para a realização da emissão do pedido de vendas. | | Atividade de Controle | | |
| 4.4 Validação da integridade dos arquivos transmitidos pelo Palmtop ao sistema ERP através de técnicas específicas (exemplos: totais de controle e verificação horizontal). | | Atividade de Controle | | |
| 4.5 Bloqueio à entrada de pedidos no sistema ERP nas seguintes condições:<br>Campos críticos não preenchidos (exemplos: cliente, produto, quantidade, desconto, prazo e operação);<br>Clientes inadimplentes ou não cadastrados;<br>Produtos ou vendedores inexistentes. | | Atividade de Controle | | |
| 4.6 Realização de consistências na transferência de arquivos dos Palmtops:<br>Registro ("log") de arquivos recebidos, e do número de pedidos existentes em cada arquivo;<br>Limitação do acesso à área da rede em que os arquivos são recebidos;<br>Conferência da transferência dos arquivos de todos os palmtops | | Atividade de Controle | | |

| Subprocesso: Emissão dos Pedidos de Venda | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.11 | Definição de preços/condições comerciais em desvantagem para a Cia. Ou baseado em critérios divergentes dos estabelecidos. | Autoridade/Limite | |
| R.12 | Faturamento em desacordo com os valores negociados. | Autoridade/Limite | |
| R.13 | Retirada de mercadorias e/ou faturamento divergente dos valores acordados. | Autoridade/Limite | |
| R.14 | Liberação de pedidos não aprovados ou em desacordo com as políticas estabelecidas pela Companhia. | Autoridade/Limite | |
| R.15 | Alteração não autorizada das informações da programação (exemplos: preço, prazo e quantidade). | Autoridade/Limite | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| anteriormente ao envio dos pedidos;<br>Verificação de arquivos recebidos em duplicidade. | | | | |
| 4.7 Numeração seqüencial dos pedidos pelo sistema. | | Atividade de Controle | | |
| 4.8 Procedimentos de inclusão e manutenção de cadastros bloqueados nos Palmtops dos vendedores. | | Atividade de Controle | | |
| 4.9 Acompanhamento do total de pedidos não liberados/emitidos (exemplos: falta de estoque, não carregamento por falha das revendas/distribuidoras). | | Atividade de Controle | | |

| Subprocesso: Faturamento e Expedição | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.16 | Ausência de definições claras em relação às políticas de gestão do Contas a Receber. | Aderência as Regras | |
| R.17 | Não recebimento e/ou recebimento inadequado (incorreções nos cálculos de juros e multa) em desacordo com as políticas estabelecidas. | Aderência as Regras | |
| R.18 | Trocas, devoluções ou reembolsos realizados de maneira incorreta ou em desacordo com as diretrizes da Companhia. | Aderência as Regras | |
| R.19 | Expedição sem faturamento ou com faturamento divergente dos pedidos de venda. | Aderência as Regras | |
| R.20 | Alteração indevida e/ou não autorizada nas informações de recebimento encaminhadas as Instituições Financeiras. | Aderência as Regras | |
| R.21 | Alterações indevidas de dados críticos dos pedidos (exemplos: preços, quantidade e condições comerciais). | Aderência as Regras | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| 5.1 Documentação atualizada das políticas e dos procedimentos relacionados ao faturamento e expedição de produtos. | | Atividade de Controle | | |
| 5.2 Cadastramento das tabelas de preço e condições comerciais no sistema de Faturamento. | | Atividade de Controle | | |
| 5.3 Restrição de acesso às transações referentes à emissão de pedidos, requisição de nota fiscal e geração de notas fiscais de venda, de acordo com as funções e responsabilidades dos funcionários.<br>• "Bandeirada" de pedidos.<br>• Emissão de nota fiscal.<br>• Faturamento por contingência. | | Atividade de Controle | | |
| 5.4 Segregação de funções entre os responsáveis por:<br>Realização de "pickings".<br>Conferência da carga.<br>Carregamento.<br>Emissão de nota fiscal. | | Atividade de Controle | | |
| 5.5 Transferência automática dos dados dos pedidos do sistema do legado para o sistema ERP (separação dos produtos a embarcar - fornecimento dos produtos). | | Atividade de Controle | | |
| 5.6 Consistência automática das informações-chave cadastradas na realização da atividade de "picking" (exemplos: idade do lote, quantidade). | | Atividade de Controle | | |
| 5.7 Baixa automática do volume de estoque à medida que é realizada a atividade de "picking". | | Atividade de Controle | | |
| 5.8 Existência, em sistema, de transação | | Atividade de | | |

| Subprocesso: Faturamento e Expedição | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.16 | Ausência de definições claras em relação às políticas de gestão do Contas a Receber. | Aderência as Regras | |
| R.17 | Não recebimento e/ou recebimento inadequado (incorreções nos cálculos de juros e multa) em desacordo com as políticas estabelecidas. | Aderência as Regras | |
| R.18 | Trocas, devoluções ou reembolsos realizados de maneira incorreta ou em desacordo com as diretrizes da Companhia. | Aderência as Regras | |
| R.19 | Expedição sem faturamento ou com faturamento divergente dos pedidos de venda. | Aderência as Regras | |
| R.20 | Alteração indevida e/ou não autorizada nas informações de recebimento encaminhadas as Instituições Financeiras. | Aderência as Regras | |
| R.21 | Alterações indevidas de dados críticos dos pedidos (exemplos: preços, quantidade e condições comerciais). | Aderência as Regras | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| específica para o acompanhamento de log's de erro gerados, devido a inconsistências na atividade de "picking". | | Controle | | |
| 5.9 Realização de contagem "cega" por pessoa independente da conferência dos produtos segregados para embarque. | | Atividade de Controle | | |
| 5.10 Bloqueio para emissão de notas fiscais de venda sem pedidos. | | Atividade de Controle | | |
| 5.11 Bloqueio de acesso a alterações dos pedidos a serem faturados, após consistências de condições comerciais e limites de crédito. | | Atividade de Controle | | |
| 5.12 Restrição de acesso a alterações das notas fiscais quando da emissão de boletos bancários. | | Atividade de Controle | | |
| 5.13 Baixa automática dos pedidos após a emissão das notas fiscais. | | Atividade de Controle | | |
| 5.14 Inutilização e arquivamento dos formulários das notas fiscais canceladas. | | Atividade de Controle | | |
| 5.15 Bloqueio de acesso ao cancelamento de notas fiscais após o prazo definido pela Companhia (em caso de erros na impressão dos formulários, o cancelamento de uma nota está vinculado à emissão de outra). | | Atividade de Controle | | |
| 5.16 Monitoramento, através de relatórios e/ou consultas ao sistema, dos pedidos pendentes de expedição. | | Monitorização | | |
| 5.17 Aprovação dos pedidos em sistema, de acordo com limite de alçada e nível adequado de gerência, com base nas modalidades de recebimento. | | Ambiente de Controles/ Negócios | | |
| 5.18 Confronto da existência física de todas as notas fiscais relacionadas nos mapas de entrega. | | Atividade de Controle | | |
| 5.19 Conferência da carga no momento | | Atividade de | | |

| Subprocesso: Faturamento e Expedição | | | | | |
|---|---|---|---|---|---|
| Riscos Identificados | | | | Categoria do Risco | Avaliação do Risco |
| R.16 | Ausência de definições claras em relação às políticas de gestão do Contas a Receber. | | | Aderência as Regras | |
| R.17 | Não recebimento e/ou recebimento inadequado (incorreções nos cálculos de juros e multa) em desacordo com as políticas estabelecidas. | | | Aderência as Regras | |
| R.18 | Trocas, devoluções ou reembolsos realizados de maneira incorreta ou em desacordo com as diretrizes da Companhia. | | | Aderência as Regras | |
| R.19 | Expedição sem faturamento ou com faturamento divergente dos pedidos de venda. | | | Aderência as Regras | |
| R.20 | Alteração indevida e/ou não autorizada nas informações de recebimento encaminhadas as Instituições Financeiras. | | | Aderência as Regras | |
| R.21 | Alterações indevidas de dados críticos dos pedidos (exemplos: preços, quantidade e condições comerciais). | | | Aderência as Regras | |
| Melhores Práticas de Controle | | | | Situação Atual | Recs |
| Descrição | | Status | Componente COSO | | |
| da saída da Unidade (dupla checagem). | | | Controle | | |

| Subprocesso: Gerenciamento de contas a receber | | | |
|---|---|---|---|
| | Riscos Identificados | Categoria do Risco | Avaliação do Risco |
| R.22 | Atrasos no C/R, decorrentes de acordos comerciais não adequadamente considerados no faturamento. | Compromissos Contratuais | |
| R.23 | Contratos que não asseguram os direitos da <NOME DA EMPRESACLIENTE>, e o cumprimento das obrigações pelos clientes-chave / regionais. | Compromissos Contratuais | |
| R.24 | Ausência de definições claras em relação às políticas de gestão do Contas a Receber. | Compromissos Contratuais | |
| R.25 | Atrasos nas informações de recebimento ocasionando bloqueio de vendas a clientes. | Compromissos Contratuais | |
| R.26 | Integridade e tempestividade das informações, decorrente de:<br>– Período para análise das informações.<br>– Atrasos no Contas a Receber, em decorrência de acordos comerciais não adequadamente considerados no faturamento.<br>– Inadequado tratamento do Contas a Receber problemático (títulos superiores há um ano) ou cobrança judicial. | Compromissos Contratuais | |
| R.27 | Aumento dos custos decorrentes de falta de produtividade no processamento das operações. | Compromissos Contratuais | |
| R.28 | Utilização e mensuração de indicadores que não estejam em linha com os objetivos da Companhia. | Compromissos Contratuais | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| 6.1 Restrição de acesso às principais transações considerando manutenção e os cancelamentos de títulos no Contas a Receber em linha com as responsabilidades dos funcionários. | | Atividade de Controle | | |
| 6.2 Segregação de funções entre as atividades de cadastro de clientes, emissão de pedidos e/ou contratos de venda, faturamento, baixa de títulos, conciliação bancária e cobrança de títulos. | | Atividade de Controle | | |
| 6.3 Aprovação, por nível de alçada apropriado, para realização de alterações/baixas parciais/manuais, prorrogação de títulos, cobrança e/ou liberação de encargos financeiros. | | Atividade de Controle | | |
| 6.4 Acompanhamento diário das formas de recebimento e dos valores devidos à Companhia. | | Atividade de Controle | | |
| 6.5 Transferência eletrônica (EDI) das informações referentes aos recebimentos pelos bancos. | | Atividade de Controle | | |
| 6.6 Confronto automático entre as informações das instituições financeiras e o valor a ser baixado (informado na prestação de contas), anteriormente à efetivação da baixa. | | Atividade de Controle | | |
| 6.7 Restrição de acesso aos arquivos referentes às baixas enviadas pelos | | Atividade de Controle | | |

| Subprocesso: Gerenciamento de contas a receber | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.22 | Atrasos no C/R, decorrentes de acordos comerciais não adequadamente considerados no faturamento. | Compromissos Contratuais | |
| R.23 | Contratos que não asseguram os direitos da <NOME DA EMPRESACLIENTE>, e o cumprimento das obrigações pelos clientes-chave / regionais. | Compromissos Contratuais | |
| R.24 | Ausência de definições claras em relação às políticas de gestão do Contas a Receber. | Compromissos Contratuais | |
| R.25 | Atrasos nas informações de recebimento ocasionando bloqueio de vendas a clientes. | Compromissos Contratuais | |
| R.26 | Integridade e tempestividade das informações, decorrente de:<br>– Período para análise das informações.<br>– Atrasos no Contas a Receber, em decorrência de acordos comerciais não adequadamente considerados no faturamento.<br>– Inadequado tratamento do Contas a Receber problemático (títulos superiores há um ano) ou cobrança judicial. | Compromissos Contratuais | |
| R.27 | Aumento dos custos decorrentes de falta de produtividade no processamento das operações. | Compromissos Contratuais | |
| R.28 | Utilização e mensuração de indicadores que não estejam em linha com os objetivos da Companhia. | Compromissos Contratuais | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| bancos e clientes (EDI). | | | | |
| 6.8 Baixa diária e automática do Contas a Receber a partir das informações recebidas dos bancos. | | Atividade de Controle | | |
| 6.9 Integração automática entre os sistemas de Faturamento e de Contas a Receber, garantindo a integridade dos dados. | | Atividade de Controle | | |
| 6.10 Conciliação automática e diária dos extratos bancários com a posição de recebimentos da Companhia. | | Atividade de Controle | | |
| 6.11 Bloqueio automático dos clientes inadimplentes com títulos em aberto, após a execução dos procedimentos de baixa. | | Atividade de Controle | | |
| 6.12 Registro das principais transações efetuadas ("log") considerando usuário, data, horário das baixas, as alterações realizadas, prorrogações e abatimentos realizados. | | Atividade de Controle | | |

| Subprocesso: Gerenciamento de contas a receber – Cobrança | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.29 | Ausência de informações para identificação e processamento das cobranças. | Integridade | |
| R.30 | Cálculo e/ou liberação de juros ou multas em desacordo com as políticas da Companhia. | Aderência às Regras | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| 7.1 Níveis/Limites de alçada para aprovação de:<br>• Prorrogações no vencimento de títulos.<br>• Descontos concedidos em títulos ou renegociação de dívidas.<br>• Baixas manuais de títulos. | | Ambiente de Controles/ Negócios | | |
| 7.2 Integração automática para transmissão dos registros de títulos a receber com a Contabilidade. | | Atividade de Controle | | |
| 7.3 Bloqueio automático do crédito dos clientes inadimplentes através de interface entre os Sistemas de Contas a Receber, Faturamento e Registro de Pedidos. | | Atividade de Controle | | |
| 7.4 Automatização da rotina de cálculo de juros do Sistema de Contas a Receber de acordo com as políticas definidas. | | Atividade de Controle | | |
| 7.5 Bloqueio do sistema para baixa de títulos sem o recebimento de encargos financeiros ou divergentes da política, requerendo aprovação eletrônica por nível de alçada adequado para liberação da baixa. | | Atividade de Controle | | |
| 7.6 Emissão periódica de relatório de títulos recebidos em atraso para verificação da cobrança de juros fora dos padrões preestabelecidos. | | Monitorização | | |
| 7.8 Inclusão de campo no sistema para registro de status/portador dos títulos em atraso. | | Atividade de Controle | | |
| 7.9 Monitoramento periódico dos títulos em atraso através da análise de relatórios emitidos pelo sistema. | | Monitorização | | |
| 7.10 Cálculo automático dos indicadores de desempenho de cobrança, com base em critérios preestabelecidos pela Companhia. | | Atividade de Controle | | |
| 7.11 Monitoramento das condições especiais concedidas aos clientes através de relatórios do sistema. | | Monitorização | | |
| 7.12 Acompanhamento dos processos judiciais da Companhia, através de sistemas integrados entre a área Jurídica | | Atividade de Controle | | |

| Subprocesso: Gerenciamento de contas a receber – Cobrança | | | | | |
|---|---|---|---|---|---|
| Riscos Identificados | | | | Categoria do Risco | Avaliação do Risco |
| R.29 | Ausência de informações para identificação e processamento das cobranças. | | | Integridade | |
| R.30 | Cálculo e/ou liberação de juros ou multas em desacordo com as políticas da Companhia. | | | Aderência às Regras | |
| Melhores Práticas de Controle | | | | Situação Atual | Recs |
| Descrição | | Status | Componente COSO | | |
| e a área de Cobrança. | | | | | |

| Subprocesso: Gerenciamento de contas a receber – Prestação de Contas | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.31 | Perda, desvio e/ou extravio de dinheiro, cheques e notas fiscais. | Eficiência | |
| R.32 | Falta de segregação de funções de atividades críticas. | Autoridade/Limite | |
| R.33 | Procedimentos inadequados na conferência de recebimentos e preparação de documentação para depósito bancário:<br>– Recebimento de numerário em condições comerciais divergentes das políticas definidas pela Organização.<br>– Erro na contagem de numerários.<br>– Falta de conferência de vinculação entre os cheques pré-datados recebidos e o sacado correspondente. | Aderência às Regras | |
| R.34 | Baixa de títulos sem o efetivo recebimento (total ou parcial) ou divergentes com depósito bancário. | Eficiência | |
| R.35 | Inadequado registro de valores recebidos. | Integridade | |
| R.36 | Ausência de vinculação entre o numerário recebido e os títulos no Contas a Receber. | Integridade | |
| R.37 | Prorrogação de títulos fora da política da Companhia e/ou de forma não autorizada. | Aderência às Regras | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| 8.1 Segregação de funções entre funcionários responsáveis pelo caixa (prestação de contas) e demais atividades do processo (exemplos: depósito de valores, emissão de notas fiscais, movimentação do Contas a Receber e conferências). | | Atividade de Controle | | |
| 8.2 Proteção física e restrição de acesso ao local de prestação de contas, conferência e guarda de valores. | | Atividade de Controle | | |
| 8.3 Definição formal de limites mínimo e máximo para as modalidades de recebimento (exemplos: cheques e boleto). | | Atividade de Controle | | |
| 8.4 Definição formal de política de recebimento de cheques:<br>Praça de aceitação.<br>Valores mínimos e máximos por cheque.<br>Nominal à <nome empresa cliente> (quando emitido pelo PDV), ou nominal ao PDV e endossado à <nome empresa cliente> (quando emitido por terceiros). | | Atividade de Controle | | |
| 8.5 Controle dos recebimentos por mapa através de formulário específico (Conferência de Numerário), considerando:<br>Emissão automática pelo Sistema de Faturamento;<br>Pré-numeração seqüencial;<br>Composição de acordo com as condições | | Atividade de Controle | | |

| Subprocesso: Gerenciamento de contas a receber – Prestação de Contas | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.31 | Perda, desvio e/ou extravio de dinheiro, cheques e notas fiscais. | Eficiência | |
| R.32 | Falta de segregação de funções de atividades críticas. | Autoridade/Limite | |
| R.33 | Procedimentos inadequados na conferência de recebimentos e preparação de documentação para depósito bancário:<br>– Recebimento de numerário em condições comerciais divergentes das políticas definidas pela Organização.<br>– Erro na contagem de numerários.<br>– Falta de conferência de vinculação entre os cheques pré-datados recebidos e o sacado correspondente. | Aderência às Regras | |
| R.34 | Baixa de títulos sem o efetivo recebimento (total ou parcial) ou divergentes com depósito bancário. | Eficiência | |
| R.35 | Inadequado registro de valores recebidos. | Integridade | |
| R.36 | Ausência de vinculação entre o numerário recebido e os títulos no Contas a Receber. | Integridade | |
| R.37 | Prorrogação de títulos fora da política da Companhia e/ou de forma não autorizada. | Aderência às Regras | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| comerciais definidas nas notas fiscais (à vista ou a prazo); | | | | |
| • Campo para registro de cheques recebidos individualizado (banco, série, número e valor)<br>• Registro das vendas de vasilhames por clientes em dinheiro (quantidade e valor);<br>Etiqueta destacável pré-numerada como controle do motorista da efetiva entrega do formulário. | | | | |
| 8.6 Arquivamento dos formulários em pastas específicas de forma seqüencial. | | Atividade de Controle | | |
| 8.7 O processo de inclusão da prestação de contas no sistema deve ser analítico e contemplar:<br>Vinculação dos cheques pré-datados recebidos aos respectivos títulos através de inclusão dos dados dos cheques via leitura e/ou digitação.<br>Os pagamentos à vista em dinheiro devem ser confrontados com o montante recebido em espécie.<br>Para os cheques pré-datados com valores divergentes dos títulos aos quais estão vinculados devem ter o seguinte tratamento pelo sistema: | | Atividade de Controle | | |
| – Se a maior, o valor será reconhecido como ganho financeiro e alocado em conta específica.<br>– Se a menor, a parcela (diferença) | | | | |

| Subprocesso: Gerenciamento de contas a receber – Prestação de Contas | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.31 | Perda, desvio e/ou extravio de dinheiro, cheques e notas fiscais. | Eficiência | |
| R.32 | Falta de segregação de funções de atividades críticas. | Autoridade/Limite | |
| R.33 | Procedimentos inadequados na conferência de recebimentos e preparação de documentação para depósito bancário:<br>– Recebimento de numerário em condições comerciais divergentes das políticas definidas pela Organização.<br>– Erro na contagem de numerários.<br>– Falta de conferência de vinculação entre os cheques pré-datados recebidos e o sacado correspondente. | Aderência às Regras | |
| R.34 | Baixa de títulos sem o efetivo recebimento (total ou parcial) ou divergentes com depósito bancário. | Eficiência | |
| R.35 | Inadequado registro de valores recebidos. | Integridade | |
| R.36 | Ausência de vinculação entre o numerário recebido e os títulos no Contas a Receber. | Integridade | |
| R.37 | Prorrogação de títulos fora da política da Companhia e/ou de forma não autorizada. | Aderência às Regras | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| será reconhecida como pagamento à vista (cheque ou dinheiro) e deverá realizar baixa parcial do título. Neste caso, o sistema deve reconhecer o valor como aumento do volume a receber à vista. | | | | |
| 8.8 Cobrança de divergências encontradas no processo de prestação de contas através de emissão automática de vale contra a transportadora/motorista. | | Atividade de Controle | | |
| 8.9 Bloqueio sistêmico de eventual alteração, pelo caixa, da condição de pagamento dos títulos. | | Atividade de Controle | | |
| 8.10 Definição de política para recebimento de numerários de forma centralizada. | | Atividade de Controle | | |
| 8.11 Formalização de todas as responsabilidades e de todos os procedimentos das pessoas envolvidas no manuseio de numerário. | | Atividade de Controle | | |
| 8.12 O responsável pela conferência e preparação dos depósitos bancários deve ter função segregada de:<br>Exclusão, baixa ou prorrogação de títulos.<br>Registro de transações que afetem o Contas a Receber.<br>Preparação e/ou revisão das conciliações bancárias. | | Atividade de Controle | | |
| 8.13 Definição de política de seguros para cobertura dos valores sob custódia da | | Atividade de Controle | | |

| Subprocesso: Gerenciamento de contas a receber – Prestação de Contas | | | |
|---|---|---|---|
| **Riscos Identificados** | | **Categoria do Risco** | **Avaliação do Risco** |
| **R.31** | Perda, desvio e/ou extravio de dinheiro, cheques e notas fiscais. | Eficiência | |
| **R.32** | Falta de segregação de funções de atividades críticas. | Autoridade/Limite | |
| **R.33** | Procedimentos inadequados na conferência de recebimentos e preparação de documentação para depósito bancário:<br>– Recebimento de numerário em condições comerciais divergentes das políticas definidas pela Organização.<br>– Erro na contagem de numerários.<br>– Falta de conferência de vinculação entre os cheques pré-datados recebidos e o sacado correspondente. | Aderência às Regras | |
| **R.34** | Baixa de títulos sem o efetivo recebimento (total ou parcial) ou divergentes com depósito bancário. | Eficiência | |
| **R.35** | Inadequado registro de valores recebidos. | Integridade | |
| **R.36** | Ausência de vinculação entre o numerário recebido e os títulos no Contas a Receber. | Integridade | |
| **R.37** | Prorrogação de títulos fora da política da Companhia e/ou de forma não autorizada. | Aderência às Regras | |

| Melhores Práticas de Controle | | | | |
|---|---|---|---|---|
| **Descrição** | **Status** | **Componente COSO** | **Situação Atual** | **Recs** |
| tesouraria. | | | | |
| 8.14 Conferência entre os valores recebidos e os dados incluídos no sistema, observando:<br>• Total dos cheques à vista;<br>• Total dos valores em espécie, atentando para montante mínimo (vendas à vista em dinheiro);<br>• Todos os cheques pré-datados atentando para:<br>– Cliente.<br>– Valor e Restrição ao uso de cheques de terceiros (limite por cheque).<br>– Dados do cheque (banco, série e número). | | Atividade de Controle | | |
| 8.15 Terceirização da custódia dos cheques pré-datados. | | Atividade de Controle | | |
| 8.16 O responsável pela função de atualização de recebíveis não deve realizar:<br>Emissão de notas fiscais;<br>Conferência e registro do caixa;<br>Manuseio de numerários;<br>Preparação e aprovação da documentação de depósito;<br>Conciliação bancária. | | Atividade de Controle | | |
| 8.17 Confronto entre o comprovante de depósito autenticado e o valor a ser baixado (informado na prestação de contas), anteriormente à efetivação da | | Atividade de Controle | | |

| Subprocesso: Gerenciamento de contas a receber – Prestação de Contas | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.31 | Perda, desvio e/ou extravio de dinheiro, cheques e notas fiscais. | Eficiência | |
| R.32 | Falta de segregação de funções de atividades críticas. | Autoridade/Limite | |
| R.33 | Procedimentos inadequados na conferência de recebimentos e preparação de documentação para depósito bancário:<br>– Recebimento de numerário em condições comerciais divergentes das políticas definidas pela Organização.<br>– Erro na contagem de numerários.<br>– Falta de conferência de vinculação entre os cheques pré-datados recebidos e o sacado correspondente. | Aderência às Regras | |
| R.34 | Baixa de títulos sem o efetivo recebimento (total ou parcial) ou divergentes com depósito bancário. | Eficiência | |
| R.35 | Inadequado registro de valores recebidos. | Integridade | |
| R.36 | Ausência de vinculação entre o numerário recebido e os títulos no Contas a Receber. | Integridade | |
| R.37 | Prorrogação de títulos fora da política da Companhia e/ou de forma não autorizada. | Aderência às Regras | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| baixa. | | | | |
| 8.18 Conciliação das baixas realizadas no Contas a Receber com os extratos bancários, envolvendo a Gerência na regularização das divergências identificadas. | | Monitorização | | |
| 8.19 Definição de política de fechamento diário incluindo:<br>Emissão de relatórios gerenciais e de exceções para conferência dos valores baixados.<br>Contabilização da movimentação.<br>Bloqueio de acesso à alteração de dados com data retroativa.<br>Cálculo automático dos encargos por atraso. | | Atividade de Controle | | |
| 8.20 Definição de políticas para:<br>Recebimento de cheques para pagamento de títulos de clientes inadimplentes.<br>Cobrança de títulos/cheques em atraso, através das diversas modalidades (exemplos: protesto e cobrança judicial), pela Sala Comercial ou empresa terceirizada de cobrança.<br>Cobrança de encargos financeiros e condições para negociação com clientes inadimplentes, bem como definição de limite de alçada para aprovação de condições especiais. | | Atividade de Controle | | |

| Subprocesso: Gerenciamento de contas a receber – Prestação de Contas | | | |
|---|---|---|---|
| Riscos Identificados | | Categoria do Risco | Avaliação do Risco |
| R.31 | Perda, desvio e/ou extravio de dinheiro, cheques e notas fiscais. | Eficiência | |
| R.32 | Falta de segregação de funções de atividades críticas. | Autoridade/Limite | |
| R.33 | Procedimentos inadequados na conferência de recebimentos e preparação de documentação para depósito bancário:<br>– Recebimento de numerário em condições comerciais divergentes das políticas definidas pela Organização.<br>– Erro na contagem de numerários.<br>– Falta de conferência de vinculação entre os cheques pré-datados recebidos e o sacado correspondente. | Aderência às Regras | |
| R.34 | Baixa de títulos sem o efetivo recebimento (total ou parcial) ou divergentes com depósito bancário. | Eficiência | |
| R.35 | Inadequado registro de valores recebidos. | Integridade | |
| R.36 | Ausência de vinculação entre o numerário recebido e os títulos no Contas a Receber. | Integridade | |
| R.37 | Prorrogação de títulos fora da política da Companhia e/ou de forma não autorizada. | Aderência às Regras | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| Descrição | Status | Componente COSO | | |
| 8.21 Segregação de funções entre o conferente e o depositante do cheque de pagamento do título em atraso e o responsável pela baixa do título. | | Atividade de Controle | | |
| 8.22 Realização de inventário periódico dos cheques em poder de empresa terceirizada de cobrança em função do volume de cheques/valor. | | Monitorização | | |
| 8.23 Reimplantação dos cheques devolvidos, vinculando-os aos títulos originais. | | Atividade de Controle | | |
| 8.24 Conciliação, pela Gerência, das inclusões de cheques devolvidos no sistema com o extrato bancário. | | Monitorização | | |
| 8.25 Obrigatoriedade da assinatura de um termo de compromisso pelos vendedores responsáveis pela cobrança dos cheques de clientes inadimplentes em seu poder. | | Atividade de Controle | | |

| Subprocesso: Administração de Recebimentos – Acordos Comerciais | | | |
|---|---|---|---|
| **Riscos Identificados** | | **Categoria do Risco** | **Avaliação do Risco** |
| **R.38** | Venda em desacordo com as políticas estabelecidas (preços e condições comerciais). | Aderência às Regras | |
| **R.39** | Concessão de descontos a clientes não autorizados. | Autoridade/Limite | |
| **R.40** | Impacto no controle do processo em função dos critérios de pagamentos dos acordos comerciais e forma de aplicação de recursos. | Eficiência | |
| **R.41** | Exposição a litígios, decorrentes de contratos e/ou transações inadequadas ou não suportadas por contratos formais. | Compromissos Contratuais | |
| **R.42** | Não atendimento/superação das expectativas dos clientes, resultando em perda de venda ou redução de market share. | Satisfação do Cliente | |

| Melhores Práticas de Controle | | | | |
|---|---|---|---|---|
| **Descrição** | **Status** | **Componente COSO** | **Situação Atual** | **Recs** |
| 9.1 Estabelecimento de procedimento único para a definição de acordos comerciais, utilizando-se de:<br>• Cláusulas a serem utilizadas nos acordos comerciais focalizando os tipos de clientes, forma de pagamento e metas de vendas.<br>• Formulário padronizado para as negociações junto aos clientes. | | Atividade de Controle | | |
| 9.2 Aprovação formal dos acordos comerciais, conforme limites de alçada previamente estabelecidos, considerando envolvimento da Área Jurídica. | | Ambiente de Controles/ Negócios | | |
| 9.3 Sistema para acompanhamento (acordos realizados/a realizar) dos acordos comerciais formalmente aprovados, considerando:<br>• Cliente/rede/loja.<br>• Preço a ser praticado.<br>• Condições comerciais.<br>• Vigência do acordo comercial. | | Atividade de Controle | | |
| 9.4 Segregação entre as funções relacionadas ao processo de negociação, aprovação e cadastramento de acordos comerciais. | | Atividade de Controle | | |
| 9.5 Cadastramento tempestivo da totalidade dos acordos comerciais em sistema. | | Atividade de Controle | | |
| 9.6 Aprovação automática dos acordos comerciais definidos no sistema, conforme os níveis de alçada preestabelecidos pela Companhia. | | Ambiente de Controles/ Negócios | | |
| 9.7 Consistência automática para restringir o cadastramento de acordos comerciais sem verba (AP), condições comerciais estabelecidas e prazo de vigência e para sua realização. | | Atividade de Controle | | |

| Subprocesso: Administração de Recebimentos – Acordos Comerciais | | | |
|---|---|---|---|
| **Riscos Identificados** | | **Categoria do Risco** | **Avaliação do Risco** |
| **R.38** | Venda em desacordo com as políticas estabelecidas (preços e condições comerciais). | Aderência às Regras | |
| **R.39** | Concessão de descontos a clientes não autorizados. | Autoridade/Limite | |
| **R.40** | Impacto no controle do processo em função dos critérios de pagamentos dos acordos comerciais e forma de aplicação de recursos. | Eficiência | |
| **R.41** | Exposição a litígios, decorrentes de contratos e/ou transações inadequadas ou não suportadas por contratos formais. | Compromissos Contratuais | |
| **R.42** | Não atendimento/superação das expectativas dos clientes, resultando em perda de venda ou redução de market share. | Satisfação do Cliente | |

| Melhores Práticas de Controle | | | Situação Atual | Recs |
|---|---|---|---|---|
| **Descrição** | **Status** | **Componente COSO** | | |
| 9.8 Integração automática entre o sistema de acordos comerciais, de preços, pedido de venda, faturamento e recebimento dos títulos, para acompanhamento dos acordos comerciais, envolvendo:<br>• Prática de preços e condições comerciais.<br>• Avaliação dos resultados.<br>• Valores pactuados.<br>• Gerenciamento de condições dos contratos comerciais. | | Atividade de Controle | | |
| 9.9 Baixa automática em sistema das parcelas ou valores totais liquidados. | | Atividade de Controle | | |
| 9.10 Impossibilidade/bloqueio de alteração dos campos críticos dos acordos comerciais, após a sua aprovação em sistema. | | Atividade de Controle | | |