Assunto: Gestão de Riscos e Controles Internos	**Identificação:** PO-GC-03 Versão: 00
Diretoria Responsável: Diretoria de Controles Internos, Riscos e Compliance	**Publicado em:** 06/07/2017
Normas vinculadas:	**Revisão:** 06/07/2019

1. Objetivo

Esta política tem por objetivo estabelecer diretrizes e responsabilidades a serem observadas no gerenciamento de riscos da TOTVS assegurando que os riscos inerentes às atividades da Companhia sejam identificados, avaliados, tratados, monitorados e comunicados à Administração em tempo adequado para tomada de decisões, minimizando o impacto do risco e ou explorando melhor as oportunidades, através de seus controles internos e adequada governança de riscos.

Este documento não estabelece o modelo de apetite ao risco e limites aceitáveis da Companhia para cada tipo de risco identificado, bem como apresentação do dicionário de riscos e procedimentos para gerenciamento e reporte, visto que são considerados aspectos de caráter confidencial e de gestão operacional, cujas definições estão descritas em norma de gestão de riscos de uso interno.

2. Abrangência

Esta Política aplica-se a todas as áreas do Grupo TOTVS (Matriz, Subsidiárias, Unidades Próprias, Filiais, Franquias e Empresas Subsidiárias). A observância destas diretrizes é obrigatória.

3. Referências

COSO-Committee of Sponsoring Organizations of the Treadway Commission: entidade sem fins lucrativos, dedicada à melhoria dos relatórios financeiros através da ética, efetividade dos controles internos e governança corporativa, para prevenir e evitar fraudes nas demonstrações contábeis das empresas;
COSO ERM-Committee of Sponsoring Organizations of the Treadway Commission: Enterprise Risk Management Framework - Metodologia desenvolvida pelo COSO para o mapeamento e gerenciamento de riscos corporativos;
IBGD - Gerenciamento de Riscos Corporativos: Evolução em governança e estratégia.

4. Conceitos

Risco: possibilidade de ocorrência de evento que afete a capacidade da companhia de atingir seus objetivos;
Oportunidade: evento que possa impactar positivamente a realização dos objetivos da Companhia, contribuindo para a criação e preservação de valor;
Fator de risco: fatores internos ou externos que podem originar os eventos de riscos;
Apetite a riscos: nível de riscos que a Organização está disposta a aceitar para atingir suas metas e objetivos e criar valor à Companhia;
Tolerância a riscos: desvios em relação ao nível de riscos determinados como aceitáveis;

Assunto: Gestão de Riscos e Controles Internos	**Identificação:** PO-GC-03 Versão: 00

Atividades de Controle: políticas, procedimentos, atividades e mecanismos, desenvolvidos para assegurar que os objetivos de negócios sejam atingidos e que eventos indesejáveis sejam prevenidos ou detectados e corrigidos;
Cultura de riscos: conjunto de padrões éticos, valores, atitudes e comportamentos aceitos e praticados, e à disseminação da gestão de riscos como parte do processo de tomada de decisão em todos os níveis;
Linhas de defesa: conceito que define papéis, responsabilidades no gerenciamento de riscos e fortalecimento da governança, bem como a interação desses papéis em todos os níveis da Organização. A primeira linha é representada pelos gestores das áreas e/ou negócios, responsáveis diretos pela execução de seus processos e respectivos riscos. A segunda é a área de Controles Internos e Compliance, que atua na identificação de falhas de performance de controles e de identificação de desvios de políticas e procedimentos internos, e a terceira é a área de Auditoria Interna, que atua na realização de testes substantivos de controles internos e identificação de desvios operacionais e financeiros decorrentes de falhas e/ou fraudes;
Dono do risco: é o responsável pela identificação e efetiva gestão de riscos de seu processo ou área de atuação. Deve ter papéis e responsabilidades definidos para escolher e aplicar respostas a esses riscos e autoridade suficiente para priorizar ações relativas à gestão de riscos de sua área e estar integrado ao processo geral de governança de riscos da companhia;
Exposição ao risco: possibilidade de a Companhia ser afetada por um determinado risco;
Governança de gestão de riscos: diz respeito aos papéis e responsabilidades de cada um dos agentes de governança corporativa da Companhia, desde os funcionários envolvidos na execução, que devem ser responsáveis por controlar riscos diretos de suas atividades, até os membros do Conselho de Administração, Comitê de Auditoria e da Diretoria executiva. O fluxo de informações relativas ao controle de riscos e à transparência desses dados também é parte da governança de Gestão de Riscos da companhia, que trata de quais são os fóruns de decisão, quais as alçadas desses fóruns, quais são os seus papéis e responsabilidades e como são compostos;
Controles internos: é o conjunto de atividades e controles manuais e sistêmicos que desenvolvem uma barreira de proteção para que as atividades operacionais e tomadas de decisões sejam realizadas em um ambiente seguro cujas interferência e riscos sejam rapidamente identificados e tratados.

5. Diretrizes

- O processo de gerenciamento de riscos segue os princípios éticos da Companhia, valores e cultura, e as informações geradas pelo sistema de gestão de riscos devem ser confiáveis, seguir as orientações legais, e fornecer subsídios para tomada de decisões visando a redução do grau de exposição aos riscos e priorização de ações;
- Cabe aos órgãos de gestão garantir recursos aptos a operacionalização dos processos de identificação, avaliação, tratamento e monitoramento dos riscos;
- A mitigação de riscos depende de implementação de controles, sistemas e mecanismos de proteção que não possuem forma ou modelo único, e sempre deve ser priorizado aquele que mais adapte-se ao processo, estrutura e recursos disponíveis no momento de acionamento;
- Eventos de riscos de grande dimensão ou riscos inaceitáveis pela Companhia que podem comprometer sua perenidade, reputação e valores devem contemplar em seu gerenciamento iniciativas de gestão de continuidade de negócios, gestão de crises, bem como ações de compartilhamento dos riscos como contratação de apólice de seguros;

Assunto: Gestão de Riscos e Controles Internos	**Identificação:** PO-GC-03 Versão: 00

- Todas as informações e reportes resultantes do processo de gestão de riscos devem possuir repositório e guarda adequada. Deverão ser classificadas como informações restritas ao uso interno, e as informações cujo reporte será externo, como Formulário de Referência e Relato Integrado devem refletir a metodologia e os resultados de exposição identificada no processo de gestão de riscos.

Categoria de Riscos

A TOTVS categoriza seus riscos conforme as diretrizes abaixo, e considera os fatores externos e internos em cada categoria:
Risco Estratégico: riscos que afetam os objetivos estratégicos, considerando ambiente interno e externo;
Risco Operacional: riscos relacionados à operação da Companhia (processos, pessoas e tecnologia), que afetam a eficiência operacional e utilização efetiva e eficiente de recursos. Podem se manifestar de diversas maneiras, como por exemplo, atos fraudulentos, interrupção do negócio, conduta incorreta de funcionários, deficiência em contratos, resultando em perdas financeiras, comerciais, multas fiscalizatórias e/ou impactos jurídicos e reputacionais;
Risco Financeiro: está associado à exposição das operações financeiras/contábeis da Companhia e confiabilidade do balanço patrimonial. Pode se materializar em decorrência da não efetividade na administração dos fluxos de caixa visando a maximização e a geração de caixa operacional, retornos das transações financeiras, captação/aplicação de recursos financeiros, possibilidade de emissão de relatórios financeiros, gerenciais e fiscais incompletos, não-exatos ou intempestivos, expondo a Companhia à multas e penalidades;
Risco Regulatório/de Compliance: riscos relacionados ao cumprimento de normas e legislação, considerando leis aplicáveis ao setor de atuação e leis gerais, nacionais e internacionais (ambiental, trabalhista, cível e tributário/ fiscal).

Metodologia de Gestão de Riscos

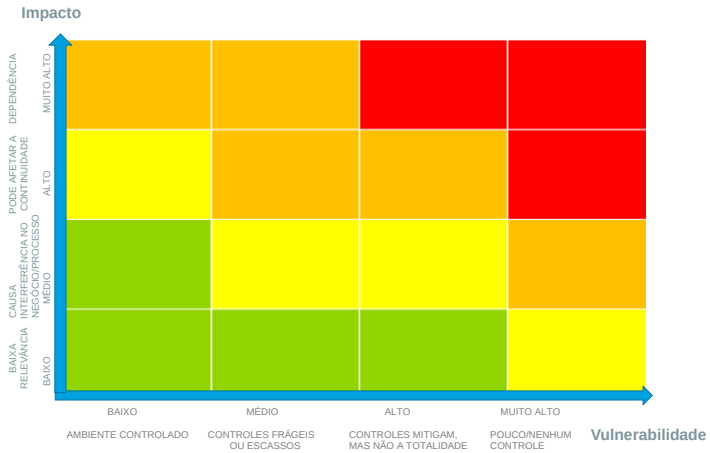
A metodologia aplicada na TOTVS é suportada pelos componentes descritos no COSO ERM (Enterprise Risk Management), sendo: Governança e cultura de risco, Risco, estratégia e definição dos objetivos, Identificação, avaliação e tratativa, Informação, comunicação e reporte e por fim, Monitoramento.
Governança e Cultura de riscos: A cultura de riscos deve ser disseminada em todos os níveis da Companhia e a gestão e monitoramento dos riscos não deve ser uma ação exclusiva de um único executivo ou departamento. Os gestores são responsáveis primários pela gestão cotidiana dos riscos associados à sua área ou processo de negócio e disseminação de cultura de gestão de riscos entre seus liderados, gerenciando a exposição aos riscos por meio de planos de ação definidos;
Risco, estratégia e definição dos objetivos: a estratégia e gerenciamento de riscos deve compreender os fatores internos e externos, bem como o impacto dos riscos que possam estar em desacordo com o direcionamento definido pela Companhia e possam afetar o atendimento dos objetivos de negócios e estratégia;
Identificação, avaliação e tratamento: os riscos devem ser periodicamente identificados, avaliados, priorizados e documentados de forma estruturada para que possam ser tratados adequadamente.

Assunto: Gestão de Riscos e Controles Internos	**Identificação:** PO-GC-03 Versão: 00

Os riscos são categorizados de acordo com sua natureza e origem, conforme Categorias de Riscos. Para tanto, é necessário descrever os processos de identificação, avaliação e tratamento dos riscos.

Identificação: O processo de captura e identificação de riscos consiste em utilização de ferramentas e metodologia COSO ERM (Enterprise Risk Management) para fins de estabelecer as matrizes de riscos e controles e mantê-las constantemente atualizadas. A Companhia deve estar atenta para o surgimento de novos riscos e/ou riscos denominados emergentes, que ao identificado, deve ser avaliado, incorporado ao processo de gestão de riscos e dependendo de sua criticidade, imediatamente reportado e tratado;
Avaliação: Os riscos devem ser avaliados de acordo com seu impacto e vulnerabilidade, considerando as premissas abaixo e a classificação final do risco será definida em função da combinação entre o resultado da vulnerabilidade e impacto.
Impacto considera a análise dos riscos em relação ao possível impacto nas operações da Companhia. O critério para definição do impacto será aplicado de acordo com premissas qualitativas que possam afetar por exemplo, o valor às partes interessadas (Impacto em clientes, fornecedores e investidores); reputação e Imagem da Companhia; não atendimento às legislações e consequências em multas e demais penalidades.
A vulnerabilidade, por sua vez, considera uma análise dos riscos em relação à magnitude em que a Companhia está exposta ou desprotegida em relação aos riscos, considerando: (i) Efetividade dos controles internos; (ii) Nível de influência da gestão em relação ao fator de risco e risco; (iii) Velocidade em que o risco pode ser materializar; (iv) Histórico de ocorrências de materialização do risco, entre outros.

Para a etapa de análise, a gradação destes aspectos deve considerar os seguintes critérios de classificação:



Tratamento: Os riscos identificados devem ser gerenciados de forma adequada e a definição de resposta deve ser realizada de acordo com a sua criticidade. A ação de resposta deve considerar a relação entre impacto e vulnerabilidade, custos e benefícios para que o risco seja adequadamente mitigado.

Reduzir o risco - Riscos que possam impactar significativamente os objetivos estratégicos da Companhia e/ou sua operação. Devem ser controlados e reduzidos a níveis aceitáveis por meio de melhorias no processo, eficiência dos controles internos diretamente relacionados ao fator de risco;

Aceitar o risco – Riscos cujo impacto seja menor que o custo/benefício do seu gerenciamento, podem ser mantidos, desde que conhecidos e aceitos pelo Comitê de Auditoria e Alta Administração. No entanto, o monitoramento deve ser contínuo e caso o impacto ou a vulnerabilidade aumente, novas decisões em relação a tratativas devem ser tomadas.

Assunto: Gestão de Riscos e Controles Internos	**Identificação:** PO-GC-03 Versão: 00

Informação e comunicação – As informações utilizadas para gerenciamento dos riscos devem ser íntegras e corretas, representando a situação atual das operações da Companhia, para que todos os colaboradores entendam seu papel dentro da estrutura de controle e tenham disponíveis as informações necessárias e assertivas para a execução de suas atividades e gestão de seus riscos. Os riscos da Companhia devem ser comunicados e conhecidos por todos os envolvidos em seu gerenciamento e monitoramento, devem ser reportados tempestivamente. O processo de comunicação dos riscos deve ser claro e eficiente, o conteúdo das informações suficientes para tomada de decisão apropriada;
Monitoramento – Os riscos devem ser monitorados continuamente para evitar que a exposição da Companhia aos riscos aumente e impeça a continuidade de negócios. O adequado monitoramento dos riscos consiste no acompanhamento constante do ambiente de controle da Companhia e ações de resposta aos riscos.
A estrutura de controle interno deve ser avaliada periodicamente, verificando a eficiência dos controles internos existentes e influências decorrentes de potenciais mudanças no ambiente interno da Companhia e/ou ambiente externo.
As ações de melhorias (planos de ação), bem como sua efetividade devem ser acompanhadas, garantindo o atingimento do propósito inicial, prazo de implementação, e eficiência para redução do risco. Essa avaliação deve ser realizada semestralmente para os riscos considerados muito altos e altos e anualmente para os médios e baixos. Quando do Planejamento Estratégico da TOTVS, deve ser realizada uma revisão sistêmica do processo de gestão de riscos por agente externo à Companhia.

6. Responsabilidades

Conselho de Administração

- Definir os objetivos estratégicos da companhia que nortearão o trabalho de identificação dos riscos da organização;
- Acompanhar as ações de gerenciamento dos riscos conforme direcionamento de negócios da Companhia;
- Determinar e validar os ciclos de revisão do sistema de controle de riscos e sua eficácia;
- Determinar o apetite e tolerância aos riscos;
- Validar documentação de informações públicas sobre o modelo de gestão de riscos e transparência de informações prestadas ao Público interno e externo;
- Alocar os recursos necessários para a gestão de risco.

Comitês técnicos de assessoramento do Conselho de Administração

Comitê de Auditoria, Comitê Estratégia e Tecnologia, Comitê de Gente e Remuneração, Comitê de Governança e Indicação

- Acompanhar e recomendar sobre a aceitação das respostas aos riscos;
- Auxiliar a Administração na definição das diretrizes de gestão de riscos, métricas de mensuração da tolerância e apetite aos riscos;
- Acompanhar ações de implementação de planos de ação mitigatórios;
- Reportar suas conclusões ao Conselho de Administração.

Este documento é de propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é de propriedade da TOTVS. Todos os direitos reservados. ©

Assunto: Gestão de Riscos e Controles Internos	**Identificação:** PO-GC-03 Versão: 00

Adicionalmente, ao Comitê de Auditoria

- Aprovar o dicionário de riscos, linguagem comum dos riscos e fortalecer a cultura de gestão de riscos;
- Acompanhar as ações de gerenciamento dos riscos conforme apetite da Companhia;
- Acompanhar e estimular o desenvolvimento de estruturas e mecanismos de proteção de riscos;
- Propor alterações na Política de Gestão de Riscos e submetê-las ao Conselho de Administração;
- Assegurar a operacionalização dos mecanismos e controles relacionados ao gerenciamento de riscos;
- Assegurar a coerência das políticas financeiras com as diretrizes estratégicas e o perfil de risco do negócio;

Diretoria

- Aprovar riscos assumidos dentro de sua alçada e se necessário, submetê-las ao Comitê de Auditoria;
- Definir a Metodologia de Gestão de Riscos da Companhia;
- Monitorar as ações de implementação de controles internos para gerenciamento dos riscos;
- Conscientizar os TOTVERS sobre a importância da gestão de riscos.

Diretoria de Gestão de Riscos

- Conduzir junto às áreas pertinentes a identificação, avaliação, tratamento, monitoramento e comunicação dos riscos estratégicos;
- Acompanhar o status dos Riscos Estratégicos, Operacionais e Financeiros e de Regulatório (Compliance);
- Propor alterações e submeter às aprovações a Política de Gestão de Riscos, além de elaborar e manter atualizadas as Normas e procedimentos atinentes à gestão de riscos;
- Propor e liderar a implementação dos procedimentos operacionais relacionados à gestão de riscos em linha com as diretrizes definidas pela Administração;
- Discutir as recomendações propostas pelos Donos dos Riscos para minimizar os riscos da companhia em linha com a estratégia e objetivos definidos;
- Monitorar as ações de implementação de controles internos para gerenciamento dos riscos;
- Consolidar a avaliação de riscos da Companhia, por meio da elaboração de relatórios periódicos, e reportá-los à Diretoria Executiva, Comitê de Auditoria, Comitê de Estratégia e Tecnologia e Conselho de Administração;
- Conscientizar os gestores sobre a importância da gestão de riscos e a responsabilidade inerente aos administradores, funcionários, estagiários e demais TOTVERS.

Auditoria Interna

- Auditar o processo de Gestão de Riscos da Companhia com pareceres imparciais, independentes e tempestivos;
- Após a implementação dos planos de ação, auditar as ações para verificar se todas foram implementadas como planejado;
- Identificar novas oportunidades e processos aptos à priorização a partir dos resultados do processo de riscos em execução, bem como ampliar o ambiente testes substantivos ou monitoramento contínuo a partir da identificação de novos riscos ou agravamento de riscos já identificados.

Assunto: Gestão de Riscos e Controles Internos	**Identificação:** PO-GC-03 Versão: 00

Controles Internos

- Mapear processos e auxiliar na identificação dos riscos (operacionais e financeiros, por exemplo), além dos respectivos controles que mitiguem esses riscos;
- Acompanhar e sugerir melhorias de controles internos pelas áreas operacionais;
- Reportar inconsistência ou desatualização de desenhos de fluxos de processos, normas e procedimentos cujas alterações podem agravar o ambiente de controles.

Donos dos Riscos/Áreas de negócios e operacionais

- Identificar e documentar riscos empresariais;
- Avaliar anualmente a performance e resultados dos riscos sob sua gestão, especialmente no que concerne à revisão de riscos incorridos que tenham desviado significativamente dos parâmetros esperados;
- Comunicar a Gestão de Riscos novos riscos identificados e qualquer alteração em seu processo de negócio para que possa ser objeto de análise e identificação de novos riscos e seus respectivos controles;
- Estabelecer controles adequados para gerenciamento dos riscos;
- Dar cumprimento ao plano de ação;
- Assegurar que as ações implementadas sejam efetivas e resultem em redução do grau de exposição aos riscos a níveis aceitáveis.

7. Aprovações (documento)

Nome / Cargo	Descrição
Manuela Loeser Gerente de Controles Internos, Riscos e Compliance	Elaboração
Silvio Roberto Reis de Menezes Diretor, Ouvidoria, RCC, Processos, Riscos e Compliance	Elaboração e Revisão
Andre Rizk Diretor Jurídico	Revisão
Gilsomar Maia Sebastião Vice Presidente Executivo Financeiro	Revisão/Recomendação
Comitê de Auditoria	Recomendação
Conselho de Administração	Aprovação

Este documento é de propriedade da TOTVS. Todos os direitos reservados. ©
Este documento é de propriedade da TOTVS. Todos os direitos reservados. ©