POLÍTICA ORGANIZACIONAL

Assunto: Gestão de Riscos e Controles Internos	**Identificação:** PO-GC-03 Versão: 01
Diretoria Responsável: Diretoria de Controles Internos, Riscos e Compliance	**Publicado em:** 19/06/2019
Normas vinculadas:	**Revisão até:** 19/06/2021

1. Objetivo

Esta política tem por objetivo estabelecer os princípios, as diretrizes e responsabilidades a serem observadas no processo de gerenciamento de riscos corporativos e de controles internos, de forma a assegurar a adequada identificação, análise, avaliação, tratamento, monitoramento e comunicação dos riscos corporativos.

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 ao Grupo TOTVS (TOTVS S.A e suas controladas, no Brasil e no exterior, incluindo coligadas e filiais).

3. Referências

CODEC: Código de Ética e Conduta da TOTVS, tem por objetivo estabelecer as condutas e princípios éticos que orientam o compromisso da TOTVS com a integridade dos seus negócios e nos relacionamentos internos e externos.

COSO Controles Internos - 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.

ABNT (Associação Brasileira de Normas Técnicas) NBR ISO 31000:2018: Gestão de Riscos – Princípios e Diretrizes.

IBGC Instituto Brasileiro de Governança Corporativa: Cadernos de Governança Corporativa, Gerenciamento de Riscos Corporativos: Evolução em Governança e Estratégia.

4. Conceitos

Risco: Evento que possa afetar negativamente os resultados da Companhia e sua capacidade de atingir seus objetivos estratégicos e de negócios.

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

Assunto: Gestão de Riscos e Controles Internos	**Identificação:** PO-GC-03 Versão: 01

Risco inerente: nível de risco intrínseco ao negócio ou à atividade, sem considerar a execução de controles mitigatórios.
Risco residual: nível de risco apurado considerando os controles mitigatórios utilizados.
Ficha de Risco: documento que formaliza para a Administração os riscos identificados, com a descrição detalhada do risco, o seu impacto, probabilidade e classificação final.
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 riscos.
Tolerância a riscos: nível máximo de exposição à riscos que a Companhia é capaz de incorrer no aproveitamento de oportunidades e na busca e realização de sua estratégia.
Atividades de Controle: atividades periódicas ou contínuas executadas visando a mitigação de um risco. Compreendem políticas, normas e procedimentos para assegurar que as diretrizes e objetivos, definidos pela Companhia para minimizar seus riscos que estão sendo observados nas atividades executadas. As atividades de controle ocorrem em todos níveis da Companhia.
Cultura de gestão 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.
***Control Self Assessment*:** questionário respondido pelo gestor das áreas responsáveis pelos processos e controles internos, com a finalidade de atestar a fidedignidade das informações prestadas no mapeamento de processos e controles internos e as documentações fornecidas para os testes de efetividade de desenho (*Walkthroughs*).
Linhas de defesa: conceito que define papéis e responsabilidades no gerenciamento de riscos e fortalecimento da governança, bem como a interação desses papéis com todos os níveis da Organização.
Dono do risco: responsável pela execução dos controles internos para garantir que o risco seja gerenciado adequadamente e pela definição e implementação dos planos de ação necessários para a remediação e/ ou minimização dos riscos, bem como pelo monitoramento contínuo e identificação de novos riscos.
Exposição ao risco: quantificação da possibilidade de a Companhia ser afetada por um determinado risco.
Governança de gestão de riscos: diz respeito aos papéis e responsabilidades na gestão de riscos da Companhia, desde os funcionários envolvidos na execução, que devem ser responsáveis por controlar riscos diretos de suas atividades, até os membros da Administração, Comitê de Auditoria e Conselho de Administração. O fluxo de informações relativas ao controle de riscos e à transparência desses dados, desde a identificação até o reporte às alçadas competentes.
Controles internos: é o conjunto de atividades e controles manuais e sistêmicos que compõem uma barreira de proteção para que as atividades operacionais e tomadas de decisões sejam realizadas em um ambiente seguro e para que os riscos sejam rapidamente identificados e tratados.
Probabilidade: nível qualitativo ou quantitativo que define a possibilidade de materialização de um evento de risco.
Impacto: refere-se ao resultado ou consequência caso ocorra a materialização de um evento de risco. O impacto do risco é analisado em diferentes esferas, conforme a régua definida.
Planos de Ação: ações ou conjunto de ações visando a mitigação ou redução do nível de exposição de um risco identificado.
Matriz de riscos: consiste em um inventário dos riscos mapeados pela Companhia, classificados de acordo com sua probabilidade e impacto.
Ciclo de Avaliação: refere-se ao ciclo anual de identificação, avaliação, análise, tratamento, monitoramento e reporte de riscos.

Assunto: Gestão de Riscos e Controles Internos	**Identificação:** PO-GC-03 Versão: 01

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 mitigação ou redução do nível de exposição aos riscos e a adequada priorização de ações.

- As informações utilizadas para gerenciamento dos riscos e controles internos 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, bem como reportados tempestivamente. O processo de comunicação dos riscos deve ser claro e eficiente, e conter informações suficientes para tomada de decisão apropriada.

- Cabe aos órgãos de gestão garantir recursos aptos a operacionalização dos processos de identificação, avaliação, análise, tratamento, monitoramento e controle 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 devem ser priorizados aqueles que mais se adaptem aos respectivos processos, bem como à estrutura e recursos disponíveis.

Todas as informações e reportes resultantes do processo de gestão de riscos são classificadas como restritas ao uso interno e devem possuir repositório e guarda adequada. 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.

5.1 Categoria de Riscos

A Companhia categoriza seus riscos conforme as diretrizes abaixo, e considera os fatores externos e internos em cada categoria:

Risco Estratégico: eventos de riscos associados às decisões estratégicas e que afetam a estratégia de negócios ou os objetivos estratégicos da Companhia, considerando ambiente interno e externo.

Risco Operacional: os riscos operacionais referem-se às possíveis perdas resultantes de falhas, deficiências ou inadequação de processos internos, pessoas, ambiente tecnológico ou provocadas por eventos externos.

Risco Financeiro: está associado à exposição a potenciais perdas financeiras da Companhia, bem como à confiabilidade dos lançamentos contábeis e das suas demonstrações financeiras. Pode se materializar, por exemplo, em decorrência da não efetividade na administração dos fluxos de caixa visando a maximização e a geração de caixa operacional, perdas em negócios, inadimplência de clientes, retornos das transações financeiras, oscilações em índices de mercado aplicados a seus contratos, 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.

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

Risco Regulatório/de Compliance: riscos de sanções legais ou regulatórias, de perda financeira ou de reputação que a Companhia pode sofrer como resultado de falhas no cumprimento da aplicação de leis, acordos, regulamentos, Código de Ética e Conduta, dentre outros.

Riscos de Tecnologia da Informação: riscos relacionados ao ambiente de tecnologia da informação (infraestrutura, gestão de acessos, segurança da informação) que podem impactar os negócios da Companhia, como a ocorrência de *ciberataques*, vazamento e/ou perda de integridade de informações, indisponibilidade do ambiente de TI e obsolescência tecnológica.

5.2 Metodologia e Processo de Gestão de Riscos

A metodologia aplicada na Companhia é suportada pelos componentes descritos no COSO ERM (*Enterprise Risk Management*) e ISO 31000 e compreende 6 etapas essenciais, além de aspectos de cultura e governança na gestão de riscos, conforme detalhado nos itens a seguir:

5.2.1 Estabelecimento do Contexto

Etapa inicial do processo de gestão de riscos, compreende a captura e entendimento dos objetivos estratégicos de curto, médio e longo prazo da Companhia, considerando o ambiente interno e externo.

5.2.2 Identificação de Riscos

O processo de captura e identificação de riscos consiste na utilização de ferramentas específicas, como mapeamento de processos, entrevistas com os gestores responsáveis de cada área/segmento de negócio e o levantamento de perdas ocorridas no passado, com o intuito de estabelecer as matrizes de riscos e controles e mantê-las constantemente atualizadas, com base nos eventos que possam impactar os objetivos estratégicos e de negócio da Companhia.

5.2.3 Análise e Avaliação de Riscos

Os riscos devem ser avaliados de acordo com seu impacto e probabilidade, bem como os fatores de risco associados, considerando as seguintes premissas:

- Impacto: A avaliação de impacto deve considerar a análise de cada fator de risco identificado, projetando as consequências da materialização de determinado risco em cada uma das seguintes esferas: (i) Financeira; (ii) Reputacional; (iii) Legal/*Compliance*; e (iv) Interrupção da Operação. As esferas são classificadas de forma independente e o maior impacto, dentre as quatro esferas, deve ser considerado para determinação da classificação final do risco na matriz. A classificação do impacto possível é determinada pela aplicação de uma régua de severidade, em quatro níveis: Baixo; Médio; Alto; e Muito Alto.

- Probabilidade: nível de exposição que considera a análise qualitativa do profissional responsável pela avaliação do risco, bem como o histórico da frequência de ocorrências, se houver, e a situação atual dos fatores de risco identificados. A classificação da probabilidade é determinada pela aplicação de uma régua de expectativa da ocorrência, em quatro níveis: Baixa; Média; Alta; e Muito Alta.

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

A classificação final do risco é determinada pelo cruzamento de sua posição nos eixos de probabilidade e impacto, resultando em 5 níveis: (i) Muito Baixo; (ii) Baixo; (iii) Médio; (iv) Alto; e (v) Crítico, conforme demonstrado a seguir:

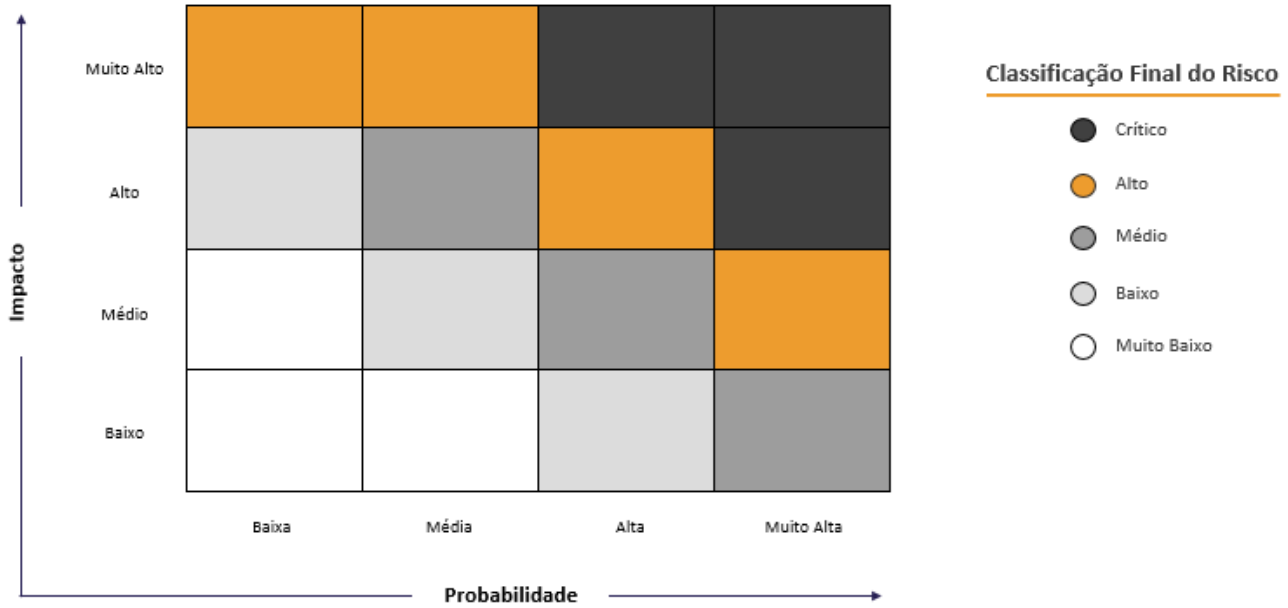

Figura 1: Matriz de classificação de probabilidade e impacto.

5.2.4 Tratamento dos Riscos

Os riscos identificados devem ser gerenciados de forma adequada e a definição de resposta deve ser realizada de acordo com a sua criticidade. Esta fase envolve a seleção, formalização e implementação de um ou mais planos de ação para redução ou mitigação dos eventos de riscos, pelas respectivas áreas responsáveis.

Os riscos Altos e Críticos devem ser objeto de planos de ação de redução ou mitigação do risco, com prazo máximo de 60 dias a partir da sua identificação para a realização das ações iniciais que reduzam a classificação do risco, exceto planos que dependam de recursos não disponíveis, projetos de TI de alta complexidade ou mudança organizacional, hipótese na qual os prazos poderão ser estendidos, mediante aprovação do Comitê de Auditoria e a aceitação da permanência do risco residual como alto ou crítico deve ser submetida, por recomendação do Vice-Presidente da área responsável e do Diretor Presidente, para conhecimento e aprovação do Conselho de Administração.

5.2.5 Monitoramento e Reporte

O adequado monitoramento dos riscos consiste no acompanhamento constante do ambiente de controles da Companhia e das ações de resposta aos riscos (planos de ação).

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.

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

As ações de melhorias (planos de ação) e sua efetividade devem ser acompanhadas pelas áreas responsáveis com o devido suporte da Gerência de Controles Internos, Riscos e Compliance, por meio de *follow-up* trimestrais, apresentados ao Comitê de Auditoria. A prorrogação de prazos de conclusão de planos de ação deve ser precedida de justificativa formal pela área responsável e devidamente reportado ao Comitê de Auditoria. Para riscos Altos e Críticos o Comitê de Auditoria deve ser informado a respeito da prorrogação solicitada e comunicar ao Conselho os motivos e a nova previsão de conclusão dos referidos planos.

5.3 Controles Internos

Os controles internos contribuem para a mitigação dos riscos, propiciando um ambiente mais seguro e eficaz, no que tange a eficiência operacional e integridade dos registros e informações, considerando principalmente os seguintes aspectos: (i) os objetivos estratégicos da Companhia; (ii) composição e natureza das contas contábeis; (iii) possibilidade de perdas decorrentes de erros e fraudes; e (iv) complexidade nas transações das contas contábeis.

Para atingimento dos seus objetivos, a gestão dos controles internos da Companhia está estruturada em um modelo integrado de 3 Linhas de Defesa, sendo:

- 1ª Linha de Defesa: São as Áreas de Negócio, responsáveis por identificar e reportar os riscos de suas operações e zelar pelo atendimento dos seus objetivos de negócio, bem como o adequado funcionamento da sua estrutura de controles internos;

- 2ª Linha de Defesa: Representada pela Gerência de Controles Internos, Riscos e Compliance, utiliza a documentação suporte produzida pela 1ª Linha de Defesa como subsídio para revisão do ambiente de controles. Atua de forma consultiva apoiando as áreas de negócio no desenvolvimento e implementação dos processos e controles;

- 3ª Linha de Defesa: Auditoria Interna, responsável por analisar e avaliar de forma independente o ambiente de controles internos com base nos trabalhos executados pela 1ª e 2ª linhas de defesa. Pode executar trabalhos adicionais conforme necessidade identificada.

5.3.1 Etapas da Gestão de Controles Internos

A Gerência de Controles Internos, Riscos e *Compliance* é responsável pelo mapeamento de Processos, controles e pelos testes de desenho dos controles ("*walkthroughs*"), com a finalidade de confirmar o entendimento dos processos mapeados, bem como se os controles estão implementados e funcionando de forma adequada.

Os controles inexistentes ou considerados insatisfatórios para mitigação dos riscos identificados nos processos de negócio são reportados para as áreas responsáveis para elaboração de planos de ação (seja a criação do novo controle ou o aperfeiçoamento dos controles existentes).

Concluídas estas etapas, os responsáveis pelos processos devem realizar anualmente o *Control Self Assessment*, bem como disponibilizar as evidências de execução dos controles no sistema utilizado pela TOTVS e, quando for o caso, apontar novos riscos por eles identificados em seus processos ou atividades.

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

Os processos e controles mapeados pela Gerência de Controles Internos, Riscos e Compliance são ferramenta fundamental para o planejamento da Auditoria Interna. Com base no mapeamento, a Auditoria Interna define a estratégia e os testes de efetividade que serão realizados (denominados "Testes de Controles"), com o objetivo de avaliar a correta aplicação e eficiência operacional dos controles na prevenção ou detecção de distorções relevantes.

Todo o processo de mapeamento, revisão dos controles e seus respectivos resultados são reportados ao Comitê de Auditoria da Companhia.

6. Responsabilidades

Conselho de Administração

- Definir os objetivos estratégicos da companhia que nortearão o trabalho de identificação dos riscos da organização;
- Aprovar a Política de Gestão de Riscos e Controles Internos;
- Aprovar a metodologia de gestão de riscos e de controles internos da Companhia;
- 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 a tolerância aos riscos;
- Aprovar o mapa de riscos (estratégicos e operacionais) e os principais fatores de risco aos quais a Companhia esteja exposta;
- Validar documentação de informações públicas sobre o modelo de gestão de riscos e transparência de informações prestadas ao público interno e externo.

Comitê de Auditoria

- Propor alterações na Política de Gestão de Riscos e Controles Internos e submetê-las ao Conselho de Administração;
- Auxiliar a Administração na definição das diretrizes e metodologia de gestão de riscos e controles internos, além das métricas de mensuração da tolerância e apetite aos riscos, apresentando ao Conselho de Administração sua recomendação de aprovação;
- Avaliar os planos de ação elaborados para os riscos classificados como "alto" e "crítico".
- Acompanhar e recomendar ao Conselho de Administração sobre a aceitação das respostas aos riscos altos e críticos;
- Avaliar o mapa de riscos (estratégicos e operacionais) e os principais fatores de risco aos quais a Companhia esteja exposta, apresentando ao Conselho de Administração suas recomendações;
- Supervisionar e acompanhar periodicamente os resultados dos testes de controles e os planos de ação mitigatórios, reportando ao Conselho de Administração desvios e ocorrências consideradas relevantes;
- Acompanhar as ações de gerenciamento dos riscos conforme direcionamento de negócios da Companhia.

Gerência de Controles Internos, Riscos e Compliance

- Propor e aplicar a metodologia de Gestão de Riscos, criando um sistema eficaz de monitoramento;
- Conduzir junto às áreas pertinentes a identificação, avaliação, tratamento, monitoramento e comunicação dos riscos estratégicos e operacionais;

- Reportar os riscos Estratégicos e Operacionais à Diretoria Executiva, Comitê de Auditoria e Conselho de Administração;
- Propor alterações e submeter às aprovações a Política de Gestão de Riscos e Controles Internos;
- 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;
- Realizar o acompanhamento e reporte trimestral de todas as ações desenvolvidas para os riscos classificados como "Médio", "Alto" e "Crítico";
- Acompanhar e reportar periodicamente o andamento dos planos de ação desenvolvidos;
- 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 possam agravar o ambiente de controles;
- Conscientizar os gestores sobre a importância da gestão de riscos e controles internos e a responsabilidade inerente aos administradores, funcionários, estagiários e demais TOTVERS.

Auditoria Interna

- Utilizar o Mapa de Riscos como subsídio para o plano anual de auditoria dos processos da Companhia, de suas subsidiárias e controladas;
- Auditar o processo de Gestão de Riscos da Companhia com pareceres imparciais, independentes e tempestivos;
- Realizar o monitoramento do ambiente de controles internos e a efetividade da gestão de riscos com base nos trabalhos executados pelas Áreas de Negócios e Gerência de Controles Internos, Riscos e Compliance;
- Executar os testes de controles de acordo com o planejamento da auditoria e reportar os resultados ao Comitê de Auditoria;
- Verificar a implementação dos planos de ação e sua eficácia;
- Identificar a necessidade de priorização de ações a partir dos resultados dos processos de riscos em execução, bem como ampliar o ambiente de testes substantivos ou monitoramento contínuo em função de novos riscos ou agravamento de riscos previamente mapeados;
- Identificar e apontar oportunidades de melhorias nos processos de controle internos e de gestão de riscos;
- Emitir opinião formal sobre os controles internos testados no ciclo anual de auditoria.

Donos dos Riscos/Áreas de Negócios e Operacionais

- Identificar continuamente e documentar os riscos sob sua gestão;
- Realizar o Control Self Assessment e disponibilizar as evidências necessárias;
- Avaliar anualmente a performance e resultados dos riscos e controles sob sua gestão;
- Comunicar a Gerência de Controles Internos, Riscos e Compliance novos riscos identificados e qualquer alteração em seu processo de negócio;
- Estabelecer controles adequados para gerenciamento dos riscos;
- Dar cumprimento aos planos de ação sob sua responsabilidade;
- Assegurar que as ações implementadas sejam efetivas e resultem em redução do grau de exposição aos riscos a níveis aceitáveis.

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

Assunto: Gestão de Riscos e Controles Internos	**Identificação:** PO-GC-03 Versão: 01

7. Aprovações (Documento)

Nome / Cargo	Descrição
Marcos Corradi Gerente de Controles Internos, Riscos e Compliance	Elaboração
Ricardo Guerino Diretor de Planejamento, Controladoria, Controles Internos, Riscos e Compliance	Revisão
Claudia Karpat Diretora Jurídica	Revisão
Gilsomar Maia Sebastião Vice-Presidente Executivo Financeiro	Revisão/Recomendação
Comitê de Auditoria	Recomendação
Conselho de Administração	Aprovação

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