POLÍTICA ORGANIZACIONAL

Assunto: Gestão de Riscos, Controles Internos e Compliance	**Identificação:** PO-GC-03 **Versão:** 04
Diretoria Responsável: Controles Internos, Riscos e Compliance	**Publicado em:** 05/05/2023
Normas vinculadas:	**Revisão até:** 05/05/2026

1. Objetivo

Esta política tem por objetivo estabelecer os princípios, as diretrizes e responsabilidades a serem observadas no processo de gestão de riscos corporativos, controles internos e compliance, bem como disseminar a cultura de Gestão de Riscos e o Programa de integridade por todos os níveis do Grupo TOTVS.

2. Abrangência

Esta Política aplica-se a todas as áreas do Grupo TOTVS, aos seus respectivos empregados e administradores, bem como às suas subsidiárias integrais, sendo que as regras aqui estabelecidas deverão ser reproduzidas nas políticas das controladas diretas e indiretas, no Brasil e nos demais países, sempre respeitando seus documentos constitutivos e a legislação local aplicável.

Deve-se garantir, ainda, que Terceiros, subcontratados, representantes, consultores, fornecedores e prestadores de serviços de qualquer natureza, quando do seu relacionamento com ou representando o Grupo TOTVS, também pautem suas ações no disposto nesta Política.

3. Referências

- ABNT (Associação Brasileira de Normas Técnicas) NBR ISO 31000:2018: Gestão de Riscos – Princípios e Diretrizes;
- CODEC - Código de Ética e Conduta do Grupo TOTVS;
- Código Brasileiro de Governança Corporativa das Companhias Abertas - Instituto Brasileiro de Governança Corporativa – "IBGC";
- COSO ERM - Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management Framework;
- Decreto 11.129/22 – Decreto que regulamenta a Lei Anticorrupção;
- Estatuto Social da TOTVS e demais estatutos sociais das empresas do Grupo TOTVS;
- IBGC: Cadernos de Governança Corporativa, Gerenciamento de Riscos Corporativos e Compliance à luz da Governança Corporativa;
- Lei 12.846/13 – Lei Anticorrupção Brasileira; e
- Portaria CGU 909 – Avaliação de programas de integridade de pessoas jurídicas.

4. Definições

Alta Administração: Presidente e Vice-Presidentes do Grupo TOTVS.
Apetite ao risco: se refere ao nível de risco que a Companhia está disposta a incorrer para atingir seus objetivos estratégicos. O apetite a risco na Companhia é definido e mensurado de forma qualitativa.
Canal de Ética e Conduta: canal para que toda pessoa que se relaciona direta ou indiretamente com o Grupo TOTVS (incluindo colaboradores, acionistas, clientes, fornecedores, franqueados e parceiros e seus colaboradores e quaisquer terceiros) possam comunicar de forma confidencial, situações que possam caracterizar violação do

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

Código de Ética e Conduta do Grupo TOTVS ou qualquer outro ato que infrinja ou possa infringir a Legislação e/ou Regulamentação vigentes.

Companhia ou TOTVS: TOTVS S.A.

Compliance: deriva do verbo inglês "*to comply*", que significa conformidade, que é o dever de cumprir e fazer cumprir leis, decretos, regulamentos e instruções aplicáveis às atividades do Grupo TOTVS.

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.

***Control Self Assessment*:** questionário respondido pelos gestores com a finalidade de auto avaliar os controles internos dos processos sob sua responsabilidade.

Cronograma anual de Compliance: roteiro estabelecido visando determinar a priorização das ações previstas no Programa de Integridade.

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.

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.

Entes Públicos: qualquer órgão ou entidade de qualquer dos Poderes da União, do Distrito Federal, dos Estados ou dos Municípios; pessoas jurídicas controladas, direta ou indiretamente, por quaisquer dessas esferas de governo; ou qualquer órgão, entidade ou representação diplomática de país estrangeiro, bem como as pessoas jurídicas controladas, direta ou indiretamente, pelo poder público de país estrangeiro. Consideram-se também como Entes Públicos, para fins desta Política, pessoas jurídicas privadas que não integram a estrutura da administração direta ou indireta, mas colaboram com o Estado no desempenho de atividades de interesse público, mas não exclusivas de Estado, de natureza não lucrativa, bem como partidos políticos.

Estrutura Normativa Interna: composta pelos documentos normativos que estabelecem diretrizes, regras, procedimentos, modelos e métodos com a finalidade de direcionar a interação dos TOTVERS em suas atividades, em consonância com os valores, cultura, estratégia do Grupo TOTVS e de acordo com a regulamentação vigente.

Exposição ao risco: quantificação da possibilidade do Grupo TOTVS ser afetado por determinado risco.

Fator de risco: fator interno ou externo que pode originar os riscos.

Grupo TOTVS: a TOTVS S.A., subsidiárias e sociedades controladas.

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.

Indicadores Chave de Risco – KRIs: indicadores utilizados para medir e monitorar dados associados aos riscos, podendo ser de caráter preditivo/preventivo, quando possuem métricas que apontam uma tendência à sua materialização, ou detectivo, no caso de indicadores que informam riscos já materializados.

Matriz de Riscos: consiste em uma representação gráfica do inventário dos riscos mapeados, classificados em quadrantes de acordo com suas probabilidades de materialização e seus impactos.

Oportunidade: evento que possa impactar positivamente a realização dos objetivos do Grupo TOTVS, contribuindo para a criação e preservação de valor.

Plano de Ação: ação ou conjunto de ações visando a mitigação ou redução do nível de exposição de um risco identificado.

Probabilidade: nível qualitativo ou quantitativo que define a possibilidade de materialização de um evento de risco.

Programa de Integridade: conjunto de mecanismos internos de integridade, com o objetivo de prevenir, detectar e combater fraudes, corrupção e demais atos ilícitos praticados no âmbito privado ou público, conforme regulamentação vigente, no Brasil e/ou no exterior, nos locais em que o Grupo TOTVS possui atuação.

Risco: Evento que possa afetar negativamente os resultados do Grupo TOTVS e sua capacidade de atingir seus objetivos estratégicos e de negócios.

Risco residual: nível de risco apurado considerando os controles mitigatórios utilizados.

Terceiro(s): qualquer pessoa física (que não seja TOTVER) ou jurídica que tenha qualquer relação com a TOTVS.

Tolerância a riscos: nível máximo de exposição à riscos que a entidade está disposta a incorrer no aproveitamento de oportunidades e na busca e realização de sua estratégia.

TOTVER: para fins desta Política é todo empregado que trabalha no Grupo TOTVS.

Assunto: Gestão de Riscos, Controles Internos e Compliance	**Identificação:** PO-GC-03 **Versão:** 04

5. Diretrizes

- O Grupo TOTVS é comprometido com uma conduta ética em seu relacionamento com colaboradores, clientes, parceiros, fornecedores, investidores, Entes Públicos e demais partes interessadas e com o cumprimento das leis e regulamentação aplicável, incluindo, mas não se limitando, à lei anticorrupção, e as Políticas, Normas e Procedimentos internos do Grupo TOTVS;
- O processo de gerenciamento de riscos e controles internos deve 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 o gerenciamento dos riscos e controles internos devem ser íntegras e corretas, representando a situação atual das operações do Grupo TOTVS;
- Os riscos da Companhia devem ser comunicados a todos os envolvidos em seu gerenciamento e monitoramento, bem como reportados tempestivamente.
- A área de Controles Internos, Riscos e Compliance respondendo diretamente ao CEO da TOTVS, goza de independência e autonomia para executar as atividades relativas ao Programa de Integridade, dispondo, inclusive, de acesso irrestrito às informações necessárias para suas atribuições, sendo as referidas premissas ratificadas pelo apoio da Alta Administração do Grupo TOTVS.

5.1 Gestão de Riscos

5.1.1. Categoria de Riscos

A Companhia categoriza seus riscos conforme descritos abaixo, considerando fatores externos e internos:

Risco Estratégico: eventos de riscos associados às decisões que afetam a estratégia de negócios ou os objetivos estratégicos do Grupo TOTVS, considerando o 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 do Grupo TOTVS.
Risco Regulatório/de Compliance: riscos de sanções legais ou regulatórias, de perda financeira ou de reputação que o Grupo TOTVS 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 do Grupo TOTVS, como a ocorrência de ciberataques, vazamentos, indisponibilidade do ambiente de TI e obsolescência tecnológica.

5.1.2. Metodologia e Processo de Gestão de Riscos

A metodologia aplicada no Grupo TOTVS 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 a seguir:

5.1.2.1. 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, considerando o ambiente interno e externo.

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

5.1.2.2. Identificação de Riscos

O processo de 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 com a Alta Administração, bem como o levantamento do histórico de perdas e de materialização de eventos de risco, 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 Grupo TOTVS.

5.1.2.3. Análise e Avaliação de Riscos

Os riscos e respectivos fatores de risco associados são avaliados de acordo com a sua probabilidade e impacto, considerando diferentes esferas, sendo a classificação final do risco 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.

5.1.2.4. Tratamento dos Riscos

A definição de resposta ao risco envolve a seleção, formalização e implementação de um ou mais planos de ação para mitigação dos eventos de riscos pelas respectivas áreas responsáveis, bem como a criação de controles compensatórios, conforme o caso.

Os riscos classificados como Altos e Críticos devem ser objeto de planos de ação para sua eliminação ou redução da classificação do risco, sendo que as ações iniciais e controles compensatórios devem ocorrer no prazo máximo de 60 dias a partir da formalização do respectivo plano. Planos estruturantes para mitigação de riscos Altos e Críticos, que dependam de recursos não disponíveis, projetos de TI de alta complexidade ou mudança organizacional, poderão ter prazos estendidos, mediante recomendação do Vice-Presidente da área responsável e aprovação do Comitê de Auditoria Estatutário. Neste caso, no prazo de 60 dias, devem ser adotados controles compensatórios temporários até a conclusão dos planos de ação definitivos.

O aceite de riscos pelo Grupo TOTVS deve obedecer às alçadas de aprovação abaixo:

<table>
<tr><td rowspan="2">Classificação do Risco</td><td colspan="3">Alçada para assunção de riscos - Grupo TOTVS</td></tr>
<tr><td>Recomendação</td><td>Aprovação do Aceite</td><td>Reporte/Informação</td></tr>
<tr><td>Crítico</td><td rowspan="2">CEO TOTVS e Comitê de Auditoria Estatutário</td><td rowspan="2">Conselho de Administração</td><td rowspan="2">-</td></tr>
<tr><td>Alto</td></tr>
<tr><td>Médio</td><td>Vice-Presidente Responsável pelo risco</td><td>CEO TOTVS</td><td>Comitê de Auditoria Estatutário</td></tr>
</table>

Baixo Muito Baixo	Diretor ou Head responsável pelo risco	Vice-Presidente Responsável pelo risco	CEO TOTVS

5.1.2.5. Monitoramento e Reporte

O adequado monitoramento dos riscos consiste nos seguintes componentes:

- Acompanhamento constante do ambiente de controles da Companhia, por meio do mapeamento de riscos e controles;
- Execução e monitoramento das ações de resposta aos riscos (planos de ação), cuja efetividade deve ser acompanhada pelas áreas responsáveis, com o suporte da área de Controles Internos, Riscos e Compliance, responsável por reportar o status consolidado ao Comitê de Auditoria Estatutário da TOTVS; e
- Estruturação e monitoramento de Indicadores Chave de Risco - KRIs, definidos pelas áreas responsáveis pelos riscos em conjunto com a área de Controles Internos, Riscos e Compliance. Os KRIs geram determinadas métricas para subsidiar a avaliação e aferição da classificação final dos níveis de probabilidade e impacto dos riscos e na identificação da necessidade da formulação de planos de ação adicionais, visando manter os riscos em níveis considerados aceitáveis pelo Grupo TOTVS. Os KRIs devem ser compartilhados com os donos dos riscos para auxiliar na tomada de decisão, bem como na disseminação da cultura de gestão de riscos.

A prorrogação de prazos para conclusão de planos de ação deve ser precedida de justificativa formal pela área responsável e reportada ao Comitê de Auditoria Estatutário. Em se tratando de riscos classificados como Altos e Críticos, o Comitê de Auditoria Estatutário deve comunicar ao Conselho de Administração da TOTVS os motivos e a nova previsão de conclusão dos referidos planos.

5.1.3. Ciclo de Revisão e Avaliação da Matriz de Riscos

A revisão da matriz de riscos deve ser realizada anualmente pela área de Controles Internos, Riscos e Compliance, observando os critérios de análise presentes nesta política, e avaliada pelos Vice-Presidentes e CEO da TOTVS sendo posteriormente submetida ao exame/recomendação do Comitê de Auditoria Estatutário e à aprovação do Conselho de Administração.

Os riscos contidos na nova Matriz devem ser objeto de planos de ação apresentados ao Comitê de Auditoria Estatutário e trimestralmente acompanhados quanto ao status de conclusão e análise da movimentação dos riscos na Matriz. Cabe a Auditoria Interna verificar a implementação de tais planos de ação.

A área de Controles Internos, Riscos e Compliance deve também reportar semestralmente ao Conselho de Administração a evolução dos planos de ação, os Indicadores Chave de Risco – KRIs apurados e o nível de exposição aos riscos.

As apresentações e reportes para o Comitê de Auditoria Estatutário e Conselho de Administração devem obrigatoriamente constar na pauta anual do Comitê de Auditoria Estatutário e do Conselho de Administração, de acordo com o cronograma definido para cada exercício.

5.2 Controles Internos

A estrutura de controle interno deve ser avaliada periodicamente, a fim de verificar a eficiência dos controles internos existentes e potenciais impactos decorrentes de mudanças no ambiente interno e/ou externo, considerando: (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.

5.2.1. Etapas da Gestão de Controles Internos

A área de Controles Internos, Riscos e Compliance deve mapear os processos, controles e realizar os testes de desenho dos controles ("walkthroughs") e os testes de efetividade ("Testes de Controles"), 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 são reportados para as áreas responsáveis para elaboração de planos de ação visando a redução da exposição aos riscos e a melhora do ambiente de controles.

Concluídas estas etapas, os responsáveis pelos processos devem realizar anualmente o Control Self Assessment no sistema utilizado pelo Grupo TOTVS e, quando for o caso, apontar novos riscos identificados em seus processos ou atividades.

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

5.3 Compliance

5.3.1 Programa de Integridade

O Programa de Integridade visa a assegurar que a legislação e regulamentação aplicáveis e as diretrizes e regras de conduta do Grupo TOTVS sejam conhecidas e cumpridas por todos os TOTVERS, bem como zelar para que os Terceiros com os quais a Companhia se relaciona compartilhem dos princípios éticos adotados pelo Grupo TOTVS.

Anualmente, a área de Controles Internos, Riscos e Compliance reavalia as ações de cada um dos pilares do Programa de Integridade com o objetivo de identificar melhorias em seus processos. A referida avaliação ocorre mediante o monitoramento dos resultados e indicadores do Programa reportados aos órgãos de governança durante o ciclo anterior.

O Programa de Integridade do Grupo TOTVS está estruturado em 5 (cinco) pilares, conforme descrito a seguir:

5.3.1.1 Cultura de Integridade

Este pilar tem por objetivo fortalecer e disseminar uma cultura que esteja em conformidade com os padrões de ética e de integridade do Grupo TOTVS, por meio do engajamento e apoio constante da Alta Administração e das principais lideranças do Grupo TOTVS.

5.3.1.2. Avaliação de Riscos

Este pilar visa identificar e avaliar os principais riscos do ponto de vista anticorrupção/compliance aos quais o Grupo TOTVS está exposto, assim como mensurar seus impactos e recomendar medidas mitigatórias, considerando o cumprimento da legislação anticorrupção aplicável e as diretrizes de conduta estabelecidas no Código de Ética e Conduta e nas demais Normas do Programa de Integridade.

Os riscos de compliance são reavaliados anualmente pela área de Controles Internos, Riscos e Compliance, visando monitorar os riscos relativos ao ciclo anterior, bem como identificar e tratar novos riscos eventualmente identificados.

5.3.1.3 Código de Ética e Conduta, Políticas e Procedimentos

Este pilar tem por objetivo estabelecer e formalizar as diretrizes, regras e procedimentos internos que devem ser seguidos pelos TOTVERS e Terceiros no âmbito do Programa de Integridade, formando a base de referência para que os mecanismos e controles de integridade sejam implementados e/ou otimizados.

5.3.1.4. Comunicação e Treinamento

O pilar de Comunicação e Treinamento visa a conscientizar e facilitar a compreensão dos TOTVERS quanto às diretrizes, regras e responsabilidades a serem cumpridas no âmbito do Programa de Integridade da TOTVS.

A área de Controles Internos, Riscos e Compliance deve elaborar e executar o Plano Anual de Comunicação e Treinamento considerando: (i) criticidade e complexidade do tema tratado; (ii) público-alvo; (iii) periodicidade; (iv) nível de riscos de compliance de determinada área ou atividade; e (iv) histórico de ocorrência de violações relacionadas ao tema, se aplicável.

O Plano Anual de Comunicação e Treinamento deverá ser submetido à apreciação e validação do Comitê de Auditoria Estatutário e Conselho de Administração, órgãos responsáveis pela supervisão da execução do plano por meio dos reportes da área de Controles Internos, Riscos e Compliance.

5.3.1.5 Detecção e Remediação

Este pilar visa identificar a ocorrência de condutas irregulares, ilegais, fraudes ou quaisquer outros descumprimentos à legislação e regulamentação aplicável e às Normas do Grupo TOTVS, bem como garantir a interrupção de tais condutas e a aplicação de medidas disciplinares e/ou corretivas, utilizando como principal instrumento um Canal independente ("Canal de Ética e Conduta") para recepção e tratamento de denúncias, disponível ao público interno e externo pelos telefones 0800 721 5966, no Brasil, e +55 11 3232 0766, para demais localidades, ou através do site: https://www.canalconfidencial.com.br/totvs/.

A gestão do Canal de Ética e Conduta é realizada pela área de Controles Internos, Riscos e Compliance, a qual tem como atribuições principais (i) recepcionar as denúncias para apuração das áreas responsáveis, de acordo com a natureza dos relatos; (ii) conduzir investigações nos relatos que tenham como objeto desvios comportamentais; e (iii) reportar as denúncias recebidas à Comissão de Ética e Conduta e aos demais órgãos de governança eventualmente aplicáveis.

Os casos de condutas irregulares são objeto de avaliação pela Comissão de Ética e Conduta do Grupo TOTVS, sendo que a área de Controles Internos, Riscos e Compliance possui independência funcional e pode ter acesso às reuniões, números de investigações e tratativas de gestão de consequências.

6. Gestão de Consequências

Em caso de descumprimento desta Política ou os demais documentos que compõem a Estrutura Normativa Interna e a legislação e regulamentação aplicável, serão adotadas medidas de gestão de consequências Trabalhistas, Cíveis, Criminais e Administrativas eventualmente aplicáveis aos responsáveis pelas ilicitudes, incluindo a possibilidade de demissão por justa causa e ruptura contratual por justo motivo no caso de franqueados e quaisquer Terceiros com os quais haja vínculo contratual.

7. Atribuições

Conselho de Administração

- Aprovar a Política de Gestão de Riscos, Controles Internos e Compliance;
- Aprovar os objetivos estratégicos e a metodologia de gestão de riscos e controles internos e o Programa de Integridade do Grupo TOTVS;
- Determinar os níveis de apetite e de tolerância aos riscos propostos pela Diretoria e recomendados pelo Comitê de Auditoria Estatutário;
- Aprovar anualmente a Matriz de Riscos Prioritários tomando conhecimento das respectivas ações de gerenciamento adotadas e seus resultados, bem como os Indicadores Chave de Risco – KRIs a serem monitorados;
- Aprovar a documentação de informações públicas sobre o modelo de gestão de riscos e transparência de informações prestadas ao público interno e externo;
- Assegurar-se da existência de recursos adequados para o funcionamento eficaz do Programa de Integridade e garantir a autonomia da área de Controles Internos, Riscos e Compliance;
- Aprovar o plano anual de comunicação e treinamento elaborado pela área de Controles Internos, Riscos e Compliance;
- Acompanhar e deliberar sobre as recomendações do Comitê de Auditoria Estatutário a respeito dos resultados da Gestão de Riscos, Controles Internos e Compliance, além dos do Programa de Integridade; e
- Aprovar a assunção de riscos Altos e Críticos.

Comitê de Governança e Indicação

- Avaliar esta Política e apresentar recomendação ao Conselho de Administração quanto à sua aprovação.

Comitê de Auditoria Estatutário

- Avaliar esta Política e apresentar recomendação ao Comitê de Governança e Indicação quanto à sua aprovação pelo Conselho de Administração;
- Auxiliar a Diretoria 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 trabalhos de Gestão de Riscos e a construção da Matriz de Riscos Prioritários, apresentando ao Conselho de Administração suas recomendações;

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

- Avaliar e recomendar ao Conselho de Administração a fixação dos níveis de apetite e de tolerância aos riscos;
- Supervisionar e acompanhar periodicamente os resultados dos testes de controles, os planos de ação mitigatórios e os Indicadores Chave de Risco – KRIs apurados, reportando ao Conselho de Administração desvios e ocorrências consideradas relevantes;
- Discutir e aprovar o Cronograma Anual de Compliance;
- Avaliar e acompanhar os planos de ação da auditoria do Programa de Integridade;
- Reportar periodicamente, ao Conselho de Administração, casos críticos de desvios de conduta relativos à presente Política, bem como as eventuais medidas disciplinares adotadas; e
- Fazer recomendações ao Conselho de Administração quanto à assunção de riscos Altos e Críticos.

Comissão de Ética e Conduta

- Deliberar sobre a procedência e gravidade das denúncias de violação ao Código de Ética e Conduta recebidas e às demais diretrizes e regras de conduta do Grupo TOTVS;
- Efetuar recomendações a respeito dos casos de denúncias analisados; e
- Deliberar e acompanhar a aplicação de medidas disciplinares.

Vice-Presidências e Diretorias

- Conduzir práticas de negócio que atendam à legislação e regulamentação aplicáveis e à Estrutura Normativa Interna;
- Apoiar na implementação e demonstrar comprometimento ao Programa de Integridade;
- Gerir os riscos sob sua responsabilidade e auxiliar na criação de controles e ações mitigatórias; e
- Zelar para que as diretrizes de conduta do Grupo TOTVS sejam comunicadas e compreendidas pelos parceiros, franqueados, canais, Terceiros e clientes.

Controles Internos, Riscos e Compliance

- Propor alterações e submeter esta Política à aprovação;
- Estruturar, implementar, gerir e disseminar a metodologia de gestão de riscos e o Programa de Integridade;
- Monitorar e reportar os planos de ação e os Indicadores Chave de Risco – KRIs definidos para gerenciamento dos riscos;
- Conscientizar os gestores e demais TOTVERS sobre a importância da gestão de riscos, controles internos e do Programa de Integridade;
- Realizar o ciclo anual de controles internos nos termos desta Política;
- Atuar de forma independente e autônoma, de modo a garantir a imparcialidade em todas as suas atividades e reportar ao Comitê de Auditoria Estatutário caso algo interfira em sua independência;
- Compartilhar com a Auditoria Interna informações e/ou fatos sujeitos à investigação interna; e
- Gerir o Canal de Ética e Conduta e reportar as denúncias à Comissão de Ética e demais órgãos de governança aplicáveis;
- Reportar a Matriz de riscos e os resultados do Programa de Integridade à Alta Administração, ao Comitê de Auditoria Estatutário e ao Conselho de Administração.

Assunto: Gestão de Riscos, Controles Internos e Compliance	**Identificação:** PO-GC-03 **Versão:** 04

Auditoria Interna

- Realizar o monitoramento do ambiente de controles internos e aferir a efetividade da gestão de riscos;
- Verificar a implementação dos planos de ação, a tempestividade de implementação e eficácia;
- Emitir opinião formal sobre os controles internos testados no ciclo anual de auditoria;
- Realizar investigações sobre denúncias e reportar o resultado à Comissão de Ética e Conduta e, periodicamente, ao Comitê de Auditoria Estatutário;
- Atuar de forma independente e autônoma, de modo a garantir a imparcialidade em todas as suas atividades e reportar ao Comitê de Auditoria Estatutário caso algo interfira em sua independência; e
- Reportar à área de Controles Internos, Riscos e Compliance riscos as não conformidades identificadas nos trabalhos de Auditoria.

Relações Humanas

- Fomentar e assegurar que os princípios do Programa de Integridade sejam difundidos junto à cultura organizacional da TOTVS.

Diretoria Jurídica

- Orientar o Grupo TOTVS em relação às normas emitidas pelos órgãos reguladores e às alterações legislativas, tanto federais, estaduais, como municipais;
- Relatar a ocorrência de ato que constitua ilícito administrativo, civil ou penal à Alta Administração e ao Conselho de Administração da TOTVS; e
- Apoiar a área de Controles Internos, Riscos e Compliance na interpretação das leis anticorrupção aplicáveis.

Donos dos Riscos/Áreas de Negócios e Operacionais

- Identificar continuamente e documentar os riscos sob sua gestão;
- Realizar anualmente o Control Self Assessment;
- Comunicar à área de Controles Internos, Riscos e Compliance novos riscos identificados e qualquer alteração em seu processo de negócio;
- Implementar, apurar e reportar periodicamente os Indicadores Chave de Risco – KRIs à área de Controles Internos, Riscos e Compliance; e
- Implementar controles e planos de ação em seus processos, assegurando que sejam efetivos e resultem em redução do grau de exposição aos riscos a níveis aceitáveis.

Demais áreas

- Todos os TOTVERS, independentemente do seu cargo, têm as seguintes responsabilidades:
- Cumprir a Estrutura Normativa Interna, a legislação e regulamentação aplicável;
- Reportar através do Canal de Ética e Conduta qualquer violação ou suspeita de violação a leis ou regulamentações aplicáveis, ou descumprimento da Estrutura Normativa Interna; e
- Apresentar todas as informações e/ou documentos corporativos dos quais estejam na posse, quando solicitados (i) pela Auditoria Interna, (ii) pela área de Controles Internos, Riscos e Compliance ou (iii) pela Comissão de Ética e Conduta, no contexto de investigação interna.

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

Assunto: Gestão de Riscos, Controles Internos e Compliance	**Identificação:** PO-GC-03 **Versão:** 04

7. Aprovações

Nome / Cargo	Descrição
Marcos Corradi Gerente Executivo de Controles Internos, Riscos e Compliance	Elaboração/Revisão
Claudia Karpat Diretora Jurídica	Revisão
Gilsomar Maia Sebastião Vice-Presidente Executivo Financeiro	Revisão/Recomendação
Dennis Herszkowicz CEO	Recomendação
Comitê de Auditoria Estatutário	Recomendação
Comitê de Governança e Indicação	Recomendação
Conselho de Administração	Aprovação

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