



POLÍTICA DE GERENCIAMENTO DE RISCOS DA LG INFORMÁTICA S.A.

1. APRESENTAÇÃO

Esta Política de Gerenciamento de Riscos (“Política”), aprovada em reunião do Conselho de Administração da LG Informática S.A. (“Companhia”), tem como objetivo formalizar e divulgar os princípios, diretrizes e responsabilidades para fins de identificação, controle e mitigação dos riscos aos quais a Companhia está exposta.

2. APLICABILIDADE E ABRANGÊNCIA

Esta Política se aplica à Companhia e suas controladas, e deverá ser observada por todos os seus respectivos colaboradores.

3. FUNDAMENTO

Esta Política tem como fundamento: **(i)** a Metodologia COSO – ERM: Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Management Framework; **(ii)** recomendações de normas de gerenciamento de risco empresarial reconhecidas no mercado, especialmente a ISO 31000:2009; **(iii)** a ISO 27000:2018, no que toca à gestão da segurança da informação; e **(iv)** o Regulamento do Novo Mercado da B3 S.A. – Brasil, Bolsa, Balcão.

4. PRINCÍPIOS E OBJETIVOS DO GERENCIAMENTO DE RISCOS

As atividades de controle e de gerenciamento dos riscos devem ser desempenhadas em todos os níveis da Companhia e em vários estágios dentro dos processos corporativos, observados os procedimentos específicos e as responsabilidades de cada órgão descritos nos itens 6 e 7 desta Política.

A Companhia está comprometida com o contínuo desenvolvimento e aprimoramento de suas práticas de gerenciamento de riscos em todo o negócio, visando à implementação e manutenção de uma estrutura formal de gerenciamento de riscos através da qual a Companhia:

- Proativamente identifica cenários de riscos potenciais;
- Avalia a probabilidade de ocorrência dos riscos identificados, bem como os eventuais impactos de sua concretização nos negócios da Companhia;
- Esforça-se para reduzir, tanto quanto possível, a exposição ao risco dentro de um apetite de risco predeterminado;
- Procura reconhecer e obter o benefício máximo de quaisquer oportunidades presentes; e
- Busca excelência em governança corporativa, gerenciando o risco de forma eficaz e por meio de um processo contínuo.

5. RISCOS AOS QUAIS A COMPANHIA ESTÁ EXPOSTA

Risco é o efeito que uma incerteza tem sobre a Companhia, no que se refere ao atingimento de seus objetivos de negócios. O risco pode surgir de todas as atividades da Companhia, apresentando-se sob a forma de uma ameaça ou de uma oportunidade, ambas com potencial de afetar a consecução dos objetivos sociais.

A Companhia monitora os riscos aos quais está exposta e busca prevenir, mitigar e tratar todo e qualquer tipo de risco que possa impactar, de forma negativa, as suas atividades e operações, o alcance dos seus objetivos e os padrões de geração de valor estabelecidos no seu plano estratégico. Para referência, os riscos são classificados da seguinte forma:

- **Riscos Estratégicos:** São aqueles associados à estratégia da Companhia na busca de criação, proteção e crescimento de valor. Trata-se da possibilidade de implementação de uma estratégia equivocada, inadequada ou ineficaz, que não atinja os objetivos esperados.
- **Riscos Operacionais:** São aqueles decorrentes da inadequação ou falha na gestão de processos internos e de pessoas que possam dificultar ou impedir o alcance dos objetivos da Companhia e estão associados tanto à operação do negócio (como marketing, vendas, comercial), quanto à gestão de áreas de suporte ao negócio (como contabilidade, controladoria, controles, suprimentos, gestão de capital humano, e saúde e segurança do trabalho).
- **Riscos Tecnológicos:** São aqueles relacionados ao ambiente de tecnologia da informação (infraestrutura, gestão de acessos, segurança da informação) da Companhia, incluindo *ciberataques*, vazamentos, indisponibilidade do ambiente de TI e obsolescência tecnológica, que impactar os negócios da Companhia.
- **Risco de Dados:** São aqueles relacionados à perda, ao mau uso ou à divulgação não autorizada de dados pessoais ou sensíveis de clientes, fornecedores, parceiros de negócio, que possam causar danos ou transtornos a qualquer indivíduo, ameaçar os negócios da Companhia ou prejudicar sua reputação.
- **Risco de Imagem:** São aqueles relacionados à perda de credibilidade e reputação perante os clientes, concorrentes, fornecedores, órgãos governamentais, mercado de atuação ou comunidade, decorrentes de ações, atos e atitudes indevidas e impróprias que se refletem em perdas de receita, aumento de custos de operação, capital ou regulatórios e destruição de valor de mercado;
- **Riscos Financeiros:**
 - Riscos de Mercado: Risco de que alterações nos preços de mercado, tais como taxas de juros e índices de correção, possam afetar os ganhos da Companhia ou o valor de seus instrumentos financeiros;
 - Risco de Crédito: A possibilidade de perda resultante da incerteza quanto ao recebimento de valores pactuados com contrapartes de contratos ou emissões de títulos; e
 - Risco de Liquidez: Possibilidade de perda decorrente da incapacidade de realizar uma transação em tempo razoável e sem perda significativa de valor ou da falta de recursos para honrar compromissos assumidos em função do descasamento entre ativos e passivos.

- **Riscos Legais e de Conformidade:** São os riscos de imposição de sanções legais ou regulatórias, de perda financeira que a Companhia pode sofrer como resultado do descumprimento de leis ou regulamentação aplicáveis, bem como de suas próprias políticas e procedimentos internos. Incluem os riscos no âmbito de processos trabalhistas e de questões tributárias, de fraudes em demonstrações financeiras e de desvios de ativos, de corrupção, entre outros.

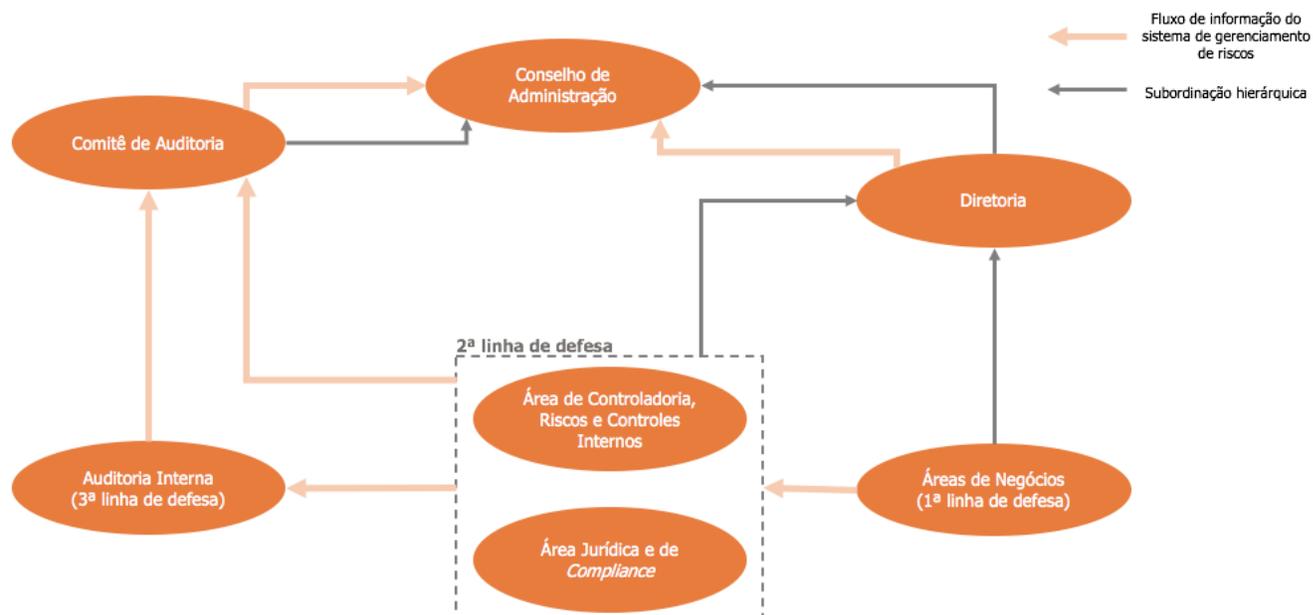
6. ESTRUTURA PARA GERENCIAMENTO DE RISCOS

Esta Política define e comunica os papéis e responsabilidades dos principais agentes envolvidos no processo de gestão de riscos, com o objetivo de construir e implantar um modelo que capture as experiências, percepções e os melhores conjuntos de informações disponíveis para a tomada de decisão.

A estrutura de gestão de riscos da Companhia considera a atuação conjunta de todos os colaboradores da Companhia, em seus respectivos níveis hierárquicos. Nesse sentido, diferentes departamentos e áreas da Companhia, de acordo com suas atribuições e funções, são responsáveis por identificar, avaliar, tratar e monitorar os riscos, em conformidade com esta Política. A estrutura de gestão de riscos da Companhia é baseada principalmente no COSO-ERM, que recomenda a gestão de riscos através do modelo das três linhas de defesa:

- 1ª Linha de Defesa: a primeira linha de defesa está associada à linha de frente dos negócios da Companhia e inclui todos aqueles envolvidos diretamente nas atividades operacionais da Companhia, responsáveis pela execução dos controles, constante identificação e avaliação dos Riscos e implementação das respostas aos Riscos a que a Companhia está sujeita. Trata-se das Áreas de Negócios.
- 2ª Linha de Defesa: a segunda linha de defesa refere-se aos responsáveis pelos controles da Companhia, com atribuições para fixar as diretrizes de gestão de riscos e supervisionar o cumprimento destas diretrizes. Nesta categoria estão a Área de Controladoria, Riscos e Controles Internos e a Área Jurídica e de *Compliance*, responsáveis pelas funções de riscos corporativos, controles internos e *compliance*. A Área de Controladoria, Riscos e Controles Internos e a Área Jurídica e de *Compliance* se reportam ao Comitê de Auditoria em relação a atividades relacionadas à gestão de riscos, controles internos e *compliance* e seus membros não acumulam outras atividades operacionais.
- 3ª Linha de Defesa: a terceira linha de defesa refere-se à Auditoria Interna, a quem compete avaliar, testar e supervisionar a aderência, conformidade e eficácia do processo de gestão de riscos da Companhia, bem como aferir a qualidade e a efetividade dos controles internos e governança. A Auditoria Interna se reporta ao Conselho de Administração, por meio do Comitê de Auditoria.

Dessa forma, a estrutura de gerenciamento de riscos da Companhia tem como objetivo avaliar e monitorar os riscos aos quais a Companhia está exposta, proporcionando um mecanismo para priorização desses riscos e, conseqüentemente, uma ferramenta de direcionamento dos esforços para mitigar a sua materialização. Para tanto, a referida estrutura se encontra segmentada conforme o organograma abaixo:



Sem prejuízo do disposto nesta Política, o gerenciamento dos Riscos de Tecnologia e de Dados deverá observar também a norma interna de análise, avaliação e tratamento de riscos de segurança da informação, baseada na ISO 27000:2018, assim como o Procedimento Operacional de Gestão de Riscos de Segurança da Informação e as demais normas internas que dela decorram, inclusive para fins de avaliação dos riscos.

7. PAPEIS E RESPONSABILIDADES

Os papéis e responsabilidades de cada órgão integrante da estrutura são os seguintes:

- **Conselho de Administração:** Responsável pela governança do processo de gerenciamento de riscos, tem como atribuições:
 - (i) Estabelecer a cultura da gestão do risco dentro da Companhia, especialmente com relação a novas iniciativas e riscos emergentes;
 - (ii) Tomar as decisões principais com relação ao processo de gestão de riscos da Companhia, incluindo os que possam afetar o perfil de risco ou exposição da Companhia;
 - (iii) Definir uma tolerância de risco apropriada, priorizando riscos e aprovando planos de mitigação;
 - (iv) Revisar, monitorar e aprovar as estratégias gerais da Companhia para a gestão do risco, em conjunto com o Comitê de Auditoria;
 - (v) Supervisionar e aprovar planos de resposta a riscos, quando necessário;
 - (vi) Receber, por meio do Comitê de Auditoria, o reporte das atividades da Auditoria Interna, da Área de Controladoria, Riscos e Controles Internos, da Área Jurídica e de *Compliance* e do Comitê de Gestão de Segurança da Informação em relação às atividades relacionadas ao gerenciamento de riscos da Companhia.

- (vii) Avaliar a efetividade do sistema de controles internos, com o assessoramento do Comitê de Auditoria; e
 - (viii) Aprovar esta Política e eventuais alterações.
- **Comitê de Auditoria:** Responsável por:
 - (i) Propor ao Conselho de Administração as definições gerais das estratégias de gestão de riscos da Companhia;
 - (ii) Avaliar e monitorar a exposição da Companhia a riscos que possam afetar a sua sustentabilidade;
 - (iii) Supervisionar as atividades da Área de Controladoria, Riscos e Controles Internos, da Área Jurídica e de *Compliance*, do Comitê de Gestão de Segurança da Informação (CGSI) e da Auditoria Interna;
 - (iv) Avaliar a efetividade do modelo de gestão de riscos da Companhia e reportar suas conclusões semestralmente ao Conselho de Administração, incluindo sua avaliação sobre a confiabilidade dos controles internos da Companhia, podendo sugerir ao órgão soluções de aprimoramento dos processos internos de gerenciamento de riscos;
 - (v) Recomendar ao Conselho de Administração a revisão ou a implementação de alterações, priorizações e inclusões à matriz de riscos da Companhia;
 - (vi) Assessorar o Conselho de Administração na avaliação de políticas, limites e planos de ação;
 - (vii) Monitorar as atividades relacionadas ao Canal de Denúncias desempenhadas pela Área Jurídica e de *Compliance*, assegurando a adequada apuração das denúncias, o sigilo, o anonimato e um ambiente livre de retaliações; e
 - (viii) Avaliar e monitorar o cumprimento e a efetividade desta Política e recomendar correções ou aprimoramentos necessários ao Conselho de Administração.
 - **Auditoria Interna:** A Companhia deverá instalar área de Auditoria Interna ou contratar auditor independente, registrado na Comissão de Valores Mobiliários, para assumir as funções de auditoria interna, dentre elas:
 - (i) Elaborar um plano anual de auditoria, a fim de verificar a eficácia dos controles internos e efetividade do processo de Gerenciamento de Riscos da Companhia
 - (ii) Monitorar a qualidade e a efetividade dos processos de gerenciamento dos riscos e de governança, bem como dos controles internos da Companhia e do cumprimento das normas e regulamentos associados às suas operações;
 - (iii) Identificar e apontar oportunidades de melhorias nos processos de controles internos, riscos e *compliance* da Companhia;
 - (iv) Fornecer ao Conselho de Administração e ao Comitê de Auditoria avaliações independentes, imparciais e tempestivas; e
 - (v) Consolidar, avaliar, monitorar e comunicar periodicamente os riscos (estratégicos, operacionais, tecnológicos, de dados, de imagem, financeiros e de *compliance*) da Companhia ao Comitê de Auditoria e ao Conselho de Administração.
 - **Área de Controladoria, Riscos e Controles Internos:** Dentre outras competências previstas nas normas internas da Companhia, é responsável por:

- (i) Estabelecer o processo de gestão dos riscos da Companhia, pautada na visão integrada e sistêmica das atividades desenvolvidas pela Companhia e em linha com a estratégia de gestão de riscos aprovada pelo Conselho de Administração;
 - (ii) Garantir a vigilância constante do ambiente de risco da Companhia, reportando novos riscos ao Comitê de Auditoria, quando necessário;
 - (iii) Antecipar e planejar possíveis falhas, bem como manter uma margem prática e relevante de segurança;
 - (iv) Incentivar que a liderança da Companhia adote uma cultura de gestão de riscos;
 - (v) Reportar as atividades de gerenciamento de riscos periodicamente ao Comitê de Auditoria;
 - (vi) Tomar decisões sobre os resultados do relatório de riscos, respostas específicas a novos riscos e mudanças no planejamento de planos de mitigação de riscos;
 - (vii) Buscar melhorias no processo de gerenciamento de riscos continuamente; e
 - (viii) Supervisionar quaisquer programas necessários de treinamento e conscientização de riscos.
- **Área Jurídica e de *Compliance*:** Dentre outras competências estabelecidas pelas normas internas da Companhia, a Área Jurídica e de *Compliance* é responsável por:
 - (i) Monitorar os Riscos Legais e de Conformidade;
 - (ii) Monitorar o cumprimento e auxiliar na interpretação de normativos emanados pelos órgãos reguladores a que a Companhia esteja sujeita;
 - (iii) Mapear e conduzir treinamentos de *compliance* às áreas de interesse, os quais poderão envolver questões relacionadas às legislações trabalhista, tributária, societária, de proteção de dados, entre outras;
 - (iv) Reportar suas atividades de *compliance* periodicamente ao Comitê de Auditoria; e
 - (v) Realizar a apuração e o tratamento de denúncias recebidas através do Canal de Denúncias e reportar seus respectivos andamentos ao Comitê de Auditoria.
- **Diretoria:** Responsável por:
 - (vi) Avaliar e tomar decisões em relação à exposição aos riscos (impacto e probabilidade) e aos limites apresentados pelos proprietários dos riscos e recomendar ações de respostas;
 - (vii) Propor ao Conselho de Administração uma tolerância de risco apropriada para a Companhia (apetite por risco);
 - (viii) Acompanhar periodicamente a evolução da exposição aos riscos considerando os limites aprovados pelo Conselho de Administração;
 - (ix) Adotar riscos avaliados como ferramenta de orientação da revisão ou construção do plano estratégico;
 - (x) Disseminar a cultura da gestão de Risco em toda Companhia, através de incentivos e políticas de remuneração variável; e
 - (xi) Conduzir uma revisão e uma avaliação da efetividade desta Política e apresentar quaisquer sugestões ao Conselho de Administração
- **Áreas de Negócios:** Responsáveis por
 - (i) Identificar e avaliar os riscos e aplicar os planos de ação para tratamento dos riscos aos quais a Companhia está exposta; e

- (ii) Reportar periodicamente à Área de Controladoria, Riscos e Controles Internos a avaliação e o Gerenciamento de Riscos sob sua respectiva competência.

Além disso, é importante destacar que todos os colaboradores são considerados responsáveis pelo gerenciamento de riscos e deverão reportar prontamente eventuais riscos identificados à Área de Controladoria, Riscos e Controles Internos ou à Auditoria Interna.

8. PROCESSO DE GERENCIAMENTO DE RISCOS

A abordagem para o mapeamento dos riscos aos quais a Companhia considera **(a)** a identificação de riscos que comprometam o atendimento dos objetivos estratégicos da Companhia e **(b)** o acompanhamento dos principais riscos a partir do contexto detalhado dos processos e controles da Companhia.

Em linha com as melhores práticas de mercado, os colaboradores que fazem parte da estrutura de gerenciamento de riscos da Companhia deverão seguir as etapas abaixo:

8.1. Estabelecer o contexto de risco

O contexto de risco representa o ambiente e o escopo no qual o risco deve ser gerenciado. Uma vez que os objetivos de negócios tenham sido definidos e estejam claros para as partes interessadas, as ameaças potenciais a esses objetivos podem ser identificadas e analisadas.

8.2. Identificar os riscos

Essa etapa consiste na identificação, em tempo hábil, de cenários de riscos que possam impactar a consecução dos objetivos da Companhia.

A identificação do risco pode ocorrer dentro das seguintes abordagens, a ser determinada pela Área de Controladoria, Riscos e Controles Internos:

- **Auditorias de processos:** Os processos da Companhia são auditados e avaliados, a fim de verificar eventuais riscos aos quais está exposta. Neste processo, matrizes de riscos são criadas/atualizadas. Tais registros contribuem para a identificação de riscos dentro da Companhia, funcionando como uma fonte de possíveis ameaças/fraquezas;
- **Ciclos de entrevistas:** Os cenários de risco são identificados e discutidos com determinados colaboradores. Os resultados também são documentados como parte da avaliação;
- **Questionários de risco:** A liderança da Companhia é solicitada a preencher um questionário específico para que indique possíveis riscos aos quais a Companhia está exposta;
- **Observação:** Os cenários de risco são observados e catalogados.

O estágio de identificação de riscos termina com o desenvolvimento do mapa de riscos. A Área de Controladoria, Riscos e Controles Internos avalia, anualmente, o mapa de riscos, com base no mapa do ano anterior, e o atualiza considerando: **(a)** os novos cenários interno, político, econômico, entre outros;

(b) projetos estratégicos da Companhia; (c) resultados de auditorias, entrevistas, questionários, observações e demais atividades; e (d) evolução da cultura de *compliance* (integridade) e mitigação de riscos.

8.3. Análise dos riscos

A partir da etapa de identificação, é realizada a análise do grau de cada risco, considerando o seu potencial impacto para o negócio e a probabilidade de se materializar. A metodologia definida pela Companhia considera:

- **Impacto/Consequência:** Magnitude/significado do potencial de perdas financeiras, degradação da imagem, penalidades legais e/ou interrupções operacionais, na percepção da liderança da Companhia, da Área de Controladoria, Riscos e Controles Internos, ou da Auditoria Interna;
- **Probabilidade/Vulnerabilidade:** Probabilidade de ocorrência de risco com base em quão robustos os controles internos relacionados são, considerando especialmente seu grau de implementação e a probabilidade de falharem na percepção da Área de Controladoria, Riscos e Controles Internos ou da Auditoria Interna;
- **Perfil do Risco:** Determinado ao se combinar o impacto/consequência e probabilidade/vulnerabilidade esperadas do risco.

8.4. Definir e implementar as ações de resposta

A Companhia toma a decisão sobre como cada cenário de risco é respondido, determinando a natureza específica do tratamento a ser aplicado:

- **Terminar:** Eliminar riscos, redefinir os objetivos e/ou estratégias de negócios;
- **Reduzir:** Diversificar, intensificar o nível de gestão e/ou melhorar os controles internos;
- **Aceitar:** Nenhuma ação adicional, continuar a monitorar;
- **Passar adiante:** Segurar ou transferir; ou

Então, as recomendações são desdobradas em ações detalhadas, pilotos, testes, validações e ajustes necessários para assegurar a eficácia do tratamento e controle dos riscos aos quais a Companhia está exposta.

Após todos os testes e ajustes necessários, a ação é implementada e difundida a todos os envolvidos. Neste contexto, a partir dos riscos identificados e respectivas recomendações informadas pela Área de Controladoria, Riscos e Controles Internos ou pela Auditoria Interna, as Áreas de Negócio implementam os planos de ação para garantir o tratamento dos riscos. Tais atividades e prazos são acompanhados pela Área de Controladoria, Riscos e Controles Internos, e reportados periodicamente ao Comitê de Auditoria.

8.5. Monitorar

A Área de Controladoria, Riscos e Controles Internos realiza, regularmente, o monitoramento dos riscos para reavaliar o nível de gerenciamento aplicado a cada cenário de risco e acordar outras ações de resposta. Os cenários de risco são revisados, no mínimo, anualmente, e relatados para:

- Verificar se o perfil de risco foi alterado;
- Identificar quando é necessário tratamento adicional; e
- Obter segurança de que o gerenciamento de riscos é eficaz.

8.6. Comunicar

A Área de Controladoria, Riscos e Controles Internos deve garantir que as informações apropriadas sejam repassadas às partes interessadas de maneira oportuna e proativa. Os relatórios e comunicações de riscos buscam garantir que:

- As partes interessadas conheçam a natureza e o status dos principais riscos, para que possam operar com uma maior consciência dos riscos e seus possíveis impactos à Companhia;
- Haja uma cultura de transparência de risco; e
- Haja uma cultura de responsabilização e conscientização de riscos.

9. DISPOSIÇÕES GERAIS

Quaisquer dúvidas acerca das disposições desta Política deverão ser endereçadas à Área de Controladoria, Riscos e Controles Internos.

10. VIGÊNCIA E ALTERAÇÕES

A presente Política entra em vigor a partir da data de entrada em vigor do Contrato de Participação no Novo Mercado, a ser celebrado entre a Companhia e a B3, e somente poderá ser alterada por deliberação do Conselho de Administração.

* * *