

POLÍTICA DE CONTROLES INTERNOS E GESTÃO DE RISCOS

Versão: 1.0

Início de vigência: 11 de junho de 2026

1. OBJETIVO

Esta Política tem por objetivo estabelecer diretrizes, princípios, responsabilidades, critérios e procedimentos para a estruturação, manutenção e aprimoramento dos controles internos e da gestão de riscos no âmbito da Check Media.

A presente Política visa assegurar que os riscos relevantes sejam identificados, avaliados, tratados, monitorados e comunicados de forma adequada, proporcional ao porte, à estrutura, às atividades e ao perfil de risco da empresa, contribuindo para a prevenção de irregularidades, a proteção da reputação institucional, a conformidade legal e contratual, a segurança das operações, a qualidade das entregas e a melhoria contínua do programa de integridade.

2. ABRANGÊNCIA

Esta Política aplica-se a todos os sócios, administradores, membros de comitês, empregados, colaboradores, consultores, representantes, parceiros, fornecedores, prestadores de serviços, terceiros contratados e quaisquer pessoas físicas ou jurídicas que atuem em nome, no interesse, em benefício ou em representação da Check Media, ou que com ela mantenham relação institucional, funcional, contratual ou comercial.

Aplica-se, igualmente, aos processos, atividades, contratos, projetos, operações, decisões, sistemas, fluxos, controles, relacionamentos com terceiros, interações com o setor público, tratamento de dados, registros, aprovações internas e demais situações que possam impactar os objetivos, a conformidade, a integridade, a reputação ou a continuidade das atividades da Check Media.

3. BASE NORMATIVA E INTERPRETAÇÃO SISTÊMICA

Esta Política deverá ser interpretada e aplicada em conformidade com a legislação vigente sobre integridade, responsabilização de pessoas jurídicas por atos lesivos contra a Administração Pública, governança corporativa, contratações públicas, proteção de dados pessoais, segurança da informação, obrigações trabalhistas, fiscais, contratuais e demais normas aplicáveis às atividades da Check Media.

Sua aplicação deverá ocorrer em harmonia com os atos normativos, políticas, manuais, procedimentos e demais instrumentos internos aplicáveis ao programa de integridade da Check Media, devendo prevalecer interpretação que reforce a prevenção de riscos, a

conformidade, a rastreabilidade, a transparência, a responsabilidade institucional e a melhoria contínua.

4. PRINCÍPIOS

A estrutura de controles internos e gestão de riscos da Check Media observará, no mínimo, os seguintes princípios:

- I. integridade;
- II. legalidade;
- III. boa-fé;
- IV. prevenção;
- V. proporcionalidade;
- VI. abordagem baseada em risco;
- VII. rastreabilidade;
- VIII. transparência;
- IX. responsabilidade individual e institucional;
- X. segregação de funções, quando aplicável e operacionalmente possível;
- XI. documentação adequada;
- XII. proteção das informações;
- XIII. melhoria contínua;
- XIV. adequação à realidade, ao porte e ao perfil de risco da empresa.

5. DEFINIÇÕES

Para fins desta Política, consideram-se:

Risco: possibilidade de ocorrência de evento, conduta, falha, omissão, circunstância ou condição capaz de afetar negativamente os objetivos, atividades, contratos, obrigações, reputação, conformidade, continuidade ou integridade da Check Media.

Risco de integridade: possibilidade de ocorrência de fraude, corrupção, vantagem indevida, conflito de interesses, assédio, discriminação, retaliação, irregularidade em relacionamento com o setor público, descumprimento de normas internas ou qualquer outro desvio ético ou de conduta capaz de comprometer a integridade institucional da Check Media.

Risco inerente: nível de risco existente antes da aplicação de controles, medidas de mitigação ou respostas institucionais.

Risco residual: nível de risco remanescente após a aplicação de controles, medidas de mitigação ou respostas institucionais.

Controle interno: política, procedimento, aprovação, validação, segregação, registro, conferência, monitoramento, restrição, trilha de auditoria, documentação ou qualquer outra medida destinada a prevenir, detectar, corrigir ou mitigar riscos.

Controle preventivo: controle destinado a evitar que o risco se materialize ou a reduzir sua probabilidade de ocorrência.

Controle detectivo: controle destinado a identificar falhas, desvios, inconsistências, irregularidades ou sinais de alerta após sua ocorrência ou durante sua execução.

Controle corretivo: controle destinado a corrigir falhas, interromper irregularidades, reparar fragilidades, tratar causas e prevenir recorrências.

Matriz de riscos e controles: instrumento que consolida os riscos relevantes identificados, seus impactos, probabilidades, controles existentes, responsáveis, nível de risco, medidas de mitigação, plano de ação e status de acompanhamento.

Plano de ação: conjunto de medidas, responsáveis, prazos e evidências destinado ao tratamento, mitigação, redução ou monitoramento de riscos e fragilidades de controle.

Apetite ao risco: nível de risco que a Check Media está disposta a aceitar para atingir seus objetivos, observados seus valores, obrigações legais, compromissos contratuais e programa de integridade.

Tolerância ao risco: limite aceitável de variação em relação a determinado risco, processo ou controle, sem prejuízo da adoção de medidas de acompanhamento ou correção.

6. DIRETRIZ GERAL

A Check Media adotará estrutura de controles internos e gestão de riscos compatível com seu porte, sua estrutura, suas atividades, seu grau de exposição, sua interação com o setor público, sua relação com terceiros e a criticidade de seus processos.

A gestão de riscos e controles internos deverá ser prática, documentada, proporcional e orientada à prevenção, detecção e correção de fragilidades, sem criar burocracia incompatível com a realidade operacional da empresa.

A existência de controles internos não substitui a responsabilidade individual de todos os envolvidos em agir com ética, diligência, transparência e conformidade.

A Check Media não admite, como risco aceitável, a prática de corrupção, fraude, suborno, pagamento de facilitação, vantagem indevida, retaliação, assédio, discriminação, obstrução de apuração, falsificação de registros, burla deliberada de controles ou qualquer

conduta incompatível com a integridade institucional, ainda que eventual decisão de negócio envolva análise de risco residual em outras matérias.

7. CATEGORIAS DE RISCOS

A Check Media poderá considerar, entre outras, as seguintes categorias de riscos:

- I. riscos de integridade;
- II. riscos de corrupção, fraude e vantagem indevida;
- III. riscos de conflito de interesses;
- IV. riscos relacionados ao setor público, licitações e contratos administrativos;
- V. riscos reputacionais;
- VI. riscos contratuais;
- VII. riscos operacionais;
- VIII. riscos financeiros e contábeis;
- IX. riscos trabalhistas;
- X. riscos relacionados a terceiros e subcontratados;
- XI. riscos de proteção de dados pessoais e segurança da informação;
- XII. riscos concorrenciais;
- XIII. riscos socioambientais e de direitos humanos, quando aplicáveis;
- XIV. riscos regulatórios e legais;
- XV. riscos de continuidade das atividades.

A categorização dos riscos não impede a identificação de outras classes ou subcategorias conforme a evolução das atividades da Check Media.

8. RESPONSABILIDADES GERAIS

A gestão de riscos e controles internos é responsabilidade compartilhada e deverá envolver, conforme o caso, a administração da Check Media, o Comitê de Integridade e Compliance, gestores, responsáveis por processos, colaboradores, terceiros e demais pessoas sujeitas às normas internas.

Cada pessoa sujeita a esta Política deverá atuar de forma diligente para prevenir, identificar, comunicar e tratar riscos e fragilidades de controle relacionados às suas atividades.

A omissão deliberada diante de risco relevante, fragilidade de controle, irregularidade, tentativa de burla ou descumprimento de norma interna poderá ensejar apuração e adoção de medidas cabíveis.

9. GOVERNANÇA E RESPONSABILIDADES

A governança da estrutura de controles internos e gestão de riscos da Check Media observará as competências, atribuições e responsabilidades estabelecidas nos atos constitutivos do Comitê de Integridade e Compliance, nas normas internas da empresa e nos demais instrumentos de governança aplicáveis.

Compete aos órgãos, áreas e responsáveis envolvidos exercer suas atribuições de forma coordenada, observando os princípios desta Política e colaborando para a identificação, avaliação, tratamento, monitoramento e comunicação dos riscos relacionados às atividades da Check Media.

Sem prejuízo das atribuições específicas previstas nos instrumentos próprios de governança, todos os colaboradores, gestores, administradores, parceiros, fornecedores e terceiros sujeitos a esta Política são responsáveis por atuar com diligência na prevenção, identificação e comunicação de riscos, fragilidades de controle e situações que possam comprometer a integridade, a conformidade ou os objetivos institucionais da empresa.

As competências específicas do Comitê de Integridade e Compliance, da Administração, dos gestores e dos demais envolvidos são aquelas previstas em seus respectivos atos de constituição, regimentos internos e demais documentos normativos da Check Media.

9. PROCESSO DE GESTÃO DE RISCOS

A gestão de riscos da Check Media observará, sempre que possível e aplicável, as seguintes etapas:

- I. definição do contexto;
- II. identificação dos riscos;
- III. análise dos riscos;
- IV. avaliação e priorização dos riscos;
- V. definição de respostas e controles;
- VI. implementação de medidas de tratamento;
- VII. monitoramento e revisão;
- VIII. comunicação e reporte.

O processo deverá ser aplicado de forma proporcional à criticidade da atividade, à complexidade do processo, ao grau de exposição da empresa e à sensibilidade da matéria.

10. IDENTIFICAÇÃO DE RISCOS

A identificação de riscos poderá ocorrer por meio de:

- I. análise de processos, contratos, projetos e atividades;
- II. mapeamento de interações com o setor público;
- III. análise de terceiros, fornecedores e parceiros;
- IV. denúncias, relatos, consultas ou manifestações recebidas;
- V. resultados de investigações internas;
- VI. auditorias, monitoramentos ou revisões;
- VII. incidentes, falhas, desvios ou não conformidades;
- VIII. mudanças legais, regulatórias, contratuais ou operacionais;
- IX. avaliação de dados, registros, indicadores e controles;
- X. percepção de gestores, colaboradores, terceiros ou membros do Comitê;
- XI. recomendações da administração, do jurídico, do compliance, de consultores ou de auditorias.

11. ANÁLISE E AVALIAÇÃO DE RISCOS

Os riscos identificados deverão ser analisados considerando, quando cabível:

- I. probabilidade de ocorrência;
- II. impacto potencial;
- III. causa ou fator gerador;
- IV. controles existentes;
- V. efetividade dos controles;
- VI. risco inerente;
- VII. risco residual;
- VIII. exposição reputacional, regulatória, contratual, financeira, operacional ou institucional;
- IX. existência de interface com o setor público;
- X. envolvimento de terceiros, PEPs, agentes públicos ou situações sensíveis;
- XI. histórico de ocorrências, denúncias, falhas ou irregularidades;

XII. necessidade de tratamento, monitoramento ou aceitação formal.

A avaliação poderá utilizar escala qualitativa ou quantitativa, conforme a maturidade do processo e a disponibilidade de informações.

12. CLASSIFICAÇÃO DE RISCOS

Os riscos poderão ser classificados, conforme avaliação documentada, como:

- I. risco baixo;
- II. risco médio;
- III. risco alto;
- IV. risco crítico.

A classificação deverá orientar o nível de controle, a urgência de tratamento, a necessidade de aprovação, o grau de monitoramento e o reporte à instância competente.

Riscos altos ou críticos deverão ser submetidos a acompanhamento reforçado e, quando cabível, ao Comitê de Integridade e Compliance ou à administração.

13. TRATAMENTO DE RISCOS

O tratamento dos riscos poderá envolver, conforme o caso:

- I. eliminar a atividade ou causa do risco;
- II. reduzir a probabilidade de ocorrência;
- III. reduzir o impacto potencial;
- IV. transferir ou compartilhar o risco de forma legítima e contratualmente adequada;
- V. aceitar o risco, desde que dentro do apetite e da tolerância definidos;
- VI. implementar controle preventivo, detectivo ou corretivo;
- VII. revisar política, procedimento, contrato, fluxo ou alçada;
- VIII. reforçar treinamento, comunicação ou supervisão;
- IX. restringir escopo, acesso, atuação ou responsabilidade;
- X. criar plano de ação específico;
- XI. monitorar o risco de forma contínua ou periódica.

A aceitação de risco relevante deverá ser justificada, documentada e aprovada pela instância competente, especialmente quando envolver integridade, setor público, dados pessoais, terceiros sensíveis ou exposição reputacional relevante.

A aceitação formal de risco somente poderá ocorrer em relação a riscos residuais compatíveis com a legislação, com as normas internas e com os valores institucionais da Check Media. Não poderá ser aceita, como decisão de gestão, situação que represente violação legal, vantagem indevida, fraude, corrupção, retaliação, obstrução de apuração ou burla deliberada de controles internos.

14. MATRIZ DE RISCOS E CONTROLES

A Check Media poderá manter matriz de riscos e controles compatível com seu porte, sua estrutura e seu perfil de risco.

A matriz poderá conter, entre outros campos:

- I. identificação do risco;
- II. categoria do risco;
- III. descrição do evento de risco;
- IV. causas;
- V. consequências;
- VI. área, processo, contrato ou atividade relacionada;
- VII. responsável pelo risco;
- VIII. controles existentes;
- IX. avaliação de probabilidade;
- X. avaliação de impacto;
- XI. nível de risco inerente;
- XII. nível de risco residual;
- XIII. medidas de tratamento;
- XIV. responsável pelo plano de ação;
- XV. prazo;
- XVI. status;
- XVII. evidências de implementação;
- XVIII. data de revisão.
- XIX. responsável pelo controle;
- XX. periodicidade de execução do controle;
- XXI. periodicidade de teste ou revisão do controle;

XXII. evidência esperada de execução;

XXIII. critério de aceitação, tratamento ou escalonamento do risco.

A matriz deverá ser atualizada sempre que houver alteração relevante no processo, surgimento de novo risco, incidente relevante, mudança normativa, recomendação do Comitê ou revisão periódica.

15. CONTROLES INTERNOS MÍNIMOS

Os controles internos deverão ser proporcionais ao risco e poderão incluir, entre outros:

- I. definição clara de responsabilidades;
- II. alçadas de aprovação;
- III. segregação de funções, quando aplicável;
- IV. dupla validação em processos sensíveis;
- V. formalização documental de decisões relevantes;
- VI. registro e rastreabilidade de interações sensíveis;
- VII. controle de acesso a informações, sistemas e documentos;
- VIII. cláusulas contratuais de integridade;
- IX. due diligence de terceiros;
- X. validação jurídica ou de compliance em matérias sensíveis;
- XI. conferência de documentos, entregas, medições e pagamentos;
- XII. controle de brindes, presentes, hospitalidades e cortesias;
- XIII. registro de reuniões com agentes públicos, quando cabível;
- XIV. canal de denúncias;
- XV. investigação interna e plano de remediação;
- XVI. treinamento e comunicação;
- XVII. monitoramento de indicadores;
- XVIII. revisão periódica de políticas e procedimentos.

16. CONTROLES EM PROCESSOS SENSÍVEIS

Deverão receber atenção reforçada os controles relacionados a:

- I. relacionamento com agentes públicos;

- II. licitações, contratos públicos e execução contratual;
- III. terceiros com interface com o setor público;
- IV. contratação, renovação e monitoramento de fornecedores e prestadores de serviços;
- V. pagamentos, reembolsos, medições e aprovações financeiras;
- VI. patrocínios, doações, apoios institucionais e contribuições;
- VII. brindes, presentes, hospitalidades e cortesias;
- VIII. tratamento de dados pessoais e informações confidenciais;
- IX. acesso a sistemas, documentos e bases sensíveis;
- X. conflitos de interesses;
- XI. processos que envolvam PEPs, familiares, estreitos colaboradores ou pessoas jurídicas relacionadas;
- XII. resposta a denúncias, investigações e medidas disciplinares.

17. SEGREGAÇÃO DE FUNÇÕES E ALÇADAS

A Check Media adotará, sempre que possível e proporcional à sua estrutura, segregação de funções em processos críticos, de modo a evitar que uma única pessoa concentre, sem controle compensatório, etapas incompatíveis de solicitação, aprovação, execução, conferência e pagamento.

Quando a segregação plena não for operacionalmente possível, deverão ser adotados controles compensatórios, tais como:

- I. validação por superior ou instância independente;
- II. registro formal da decisão;
- III. revisão periódica;
- IV. dupla aprovação;
- V. monitoramento por amostragem;
- VI. reporte ao Comitê ou à administração, quando cabível.

As alçadas de aprovação deverão ser compatíveis com a natureza, o valor, o risco e a sensibilidade da matéria.

18. REGISTROS, DOCUMENTAÇÃO E EVIDÊNCIAS

Os controles internos deverão ser documentados em nível suficiente para demonstrar sua existência, execução e efetividade, quando cabível.

Os registros poderão incluir aprovações, atas, relatórios, evidências de conferência, comunicações, pareceres, formulários, registros sistêmicos, logs, documentos contratuais, matrizes, planos de ação e demais elementos necessários à rastreabilidade.

É vedada a utilização de registros paralelos, documentos fictícios, aprovações genéricas, justificativas incompatíveis com a realidade ou qualquer forma de ocultação, fragmentação ou dissimulação de atos relevantes.

19. MONITORAMENTO DOS CONTROLES

Os controles internos deverão ser monitorados de forma proporcional ao risco, à criticidade do processo e à maturidade do programa de integridade.

O monitoramento poderá ocorrer por meio de:

- I. acompanhamento de indicadores;
- II. revisão de documentos e registros;
- III. verificação de cumprimento de planos de ação;
- IV. análise de denúncias, incidentes e não conformidades;
- V. revisão de terceiros sensíveis;
- VI. testes por amostragem;
- VII. reuniões de acompanhamento;
- VIII. relatórios periódicos ao Comitê ou à administração;
- IX. revisões internas ou externas.

O detalhamento de auditorias internas, testes de efetividade e monitoramento de compliance poderá ser disciplinado em documento próprio.

20. INDICADORES DE RISCOS E CONTROLES

A Check Media poderá acompanhar indicadores relacionados a riscos e controles, tais como:

- I. quantidade de riscos identificados por categoria;
- II. quantidade de riscos altos ou críticos;
- III. status de planos de ação;
- IV. quantidade de controles revisados;

- V. quantidade de não conformidades identificadas;
- VI. denúncias relacionadas a falhas de controle;
- VII. incidentes envolvendo terceiros;
- VIII. incidentes relacionados a dados pessoais ou segurança da informação;
- IX. treinamentos realizados;
- X. prazos médios de tratamento de riscos ou planos de ação;
- XI. reincidência de falhas ou irregularidades;
- XII. medidas preventivas e corretivas implementadas;
- XIII. quantidade de riscos aceitos formalmente;
- XIV. quantidade de controles implementados, revisados ou descontinuados;
- XV. quantidade de recomendações emitidas pelo Comitê de Integridade e Compliance relacionadas a riscos, controles ou planos de ação.
- XVI. percentual de planos de ação concluídos dentro do prazo;
- XVII. quantidade de riscos materializados em incidentes, falhas ou não conformidades;
- XVIII. reincidência de falhas por área, processo, contrato, terceiro ou atividade;
- XIX. quantidade de riscos reclassificados após revisão, incidente, denúncia, investigação ou due diligence.

Os indicadores deverão ser utilizados para subsidiar decisões, priorizar recursos, aperfeiçoar controles, acompanhar a evolução do programa de integridade e demonstrar a maturidade progressiva da estrutura de gestão de riscos e controles internos da Check Media.

21. PLANOS DE AÇÃO

Quando forem identificados riscos, fragilidades ou deficiências de controle, poderá ser elaborado plano de ação.

O plano de ação deverá conter, quando cabível:

- I. descrição da fragilidade, risco ou não conformidade identificada;
- II. medida a ser adotada;
- III. responsável pela implementação;
- IV. prazo estimado;
- V. prioridade;

VI. evidência esperada;

VII. status de implementação;

VIII. necessidade de validação ou teste posterior;

IX. risco residual após a implementação;

X. eventual necessidade de reporte ao Comitê de Integridade e Compliance ou à administração.

Planos de ação relacionados a riscos altos ou críticos deverão ser acompanhados com prioridade.

O não cumprimento injustificado de plano de ação aprovado, quando relacionado a risco relevante ou fragilidade material de controle, poderá ensejar reavaliação do risco, recomendação de medidas corretivas adicionais e, quando cabível, apuração interna.

22. INCIDENTES, FALHAS E NÃO CONFORMIDADES

Falhas de controle, incidentes, não conformidades ou desvios relevantes deverão ser comunicados à instância interna competente.

Conforme a natureza do caso, poderão ser adotadas medidas de contenção, correção, apuração, remediação, revisão de controles, treinamento, reforço de supervisão ou reporte ao Comitê de Integridade e Compliance.

Quando a falha envolver possível violação ética, fraude, corrupção, conflito de interesses, retaliação, proteção de dados, terceiro sensível, relação com o setor público, descumprimento contratual relevante ou risco reputacional significativo, deverão ser observados os fluxos internos específicos aplicáveis.

A análise de falhas, incidentes e não conformidades deverá buscar não apenas a correção do evento específico, mas também a identificação de causas, fragilidades estruturais e medidas necessárias para evitar recorrência.

23. COMUNICAÇÃO E REPORTE

A comunicação sobre riscos e controles deverá ser clara, objetiva, tempestiva e compatível com a sensibilidade da informação.

O Comitê de Integridade e Compliance poderá receber, conforme a necessidade e a maturidade do programa:

I. matriz de riscos e controles;

II. relatórios de riscos relevantes;

III. status de planos de ação;

IV. indicadores de controles;

V. registros de incidentes e não conformidades;

VI. informações sobre terceiros sensíveis;

VII. recomendações de melhoria;

VIII. temas que demandem decisão da administração;

IX. informações sobre riscos emergentes, alterações normativas ou mudanças relevantes no ambiente operacional da Check Media.

As comunicações relacionadas a riscos críticos, falhas materiais de controle, potenciais ilícitos, exposição relevante perante o setor público ou situações de elevada sensibilidade institucional deverão ser encaminhadas com prioridade à instância competente.

24. PROTEÇÃO DE DADOS, CONFIDENCIALIDADE E SEGURANÇA DA INFORMAÇÃO

As atividades de gestão de riscos e controles internos deverão observar a legislação aplicável à proteção de dados pessoais e as normas internas de privacidade e segurança da informação.

As informações coletadas, produzidas ou analisadas no âmbito desta Política deverão ser tratadas com confidencialidade, proporcionalidade, finalidade legítima e acesso limitado às pessoas autorizadas.

Registros de riscos, controles, incidentes, falhas, investigações, terceiros, dados pessoais ou informações estratégicas deverão ser protegidos contra acesso indevido, alteração, perda, divulgação não autorizada ou uso incompatível.

O acesso a informações sensíveis deverá observar o critério de necessidade de conhecimento e, sempre que possível, permitir rastreabilidade quanto à pessoa que acessou a informação, à finalidade do acesso e ao eventual compartilhamento realizado.

25. TREINAMENTO E CULTURA DE CONTROLE

A Check Media poderá promover ações de comunicação, orientação e treinamento sobre controles internos, gestão de riscos, integridade, registros, reporte de falhas, responsabilidades individuais e prevenção de irregularidades.

Poderão receber tratamento prioritário os públicos envolvidos em processos sensíveis, contratos públicos, relacionamento com agentes públicos, gestão de terceiros, pagamentos, tratamento de dados, aprovações internas e demais atividades de maior exposição.

As ações de treinamento e comunicação deverão buscar a disseminação de uma cultura prática de controle, na qual a gestão de riscos seja compreendida como instrumento de proteção institucional, e não como mera formalidade documental.

26. INTEGRAÇÃO COM DENÚNCIAS, INVESTIGAÇÕES E DUE DILIGENCE

A gestão de riscos e controles internos deverá se integrar aos fluxos de denúncias, investigações internas, medidas disciplinares, due diligence de terceiros e demais mecanismos do programa de integridade.

Achados decorrentes de denúncias, investigações, auditorias, incidentes, due diligence ou monitoramentos poderão gerar:

- I. atualização da matriz de riscos;
- II. revisão de controles;
- III. criação de plano de ação;
- IV. recomendação de treinamento;
- V. ajuste de política, procedimento ou contrato;
- VI. revisão de alçadas;
- VII. reforço de monitoramento;
- VIII. adoção de medidas preventivas, corretivas, disciplinares ou contratuais;
- IX. reclassificação de risco de processo, contrato, terceiro, área ou atividade;
- X. recomendação de reporte à administração, quando a criticidade assim exigir.

27. REVISÃO E MELHORIA CONTÍNUA

A estrutura de controles internos e gestão de riscos deverá ser revista sempre que necessário, especialmente diante de:

- I. mudanças relevantes nas atividades da Check Media;
- II. alterações legais, regulatórias ou contratuais;
- III. novos projetos, contratos ou clientes;
- IV. ampliação de interação com o setor público;
- V. contratação de terceiros sensíveis;
- VI. incidentes ou não conformidades relevantes;
- VII. denúncias ou investigações com achados estruturais;
- VIII. fragilidades identificadas em controles;
- IX. recomendações do Comitê de Integridade e Compliance, da administração, de auditoria ou de consultores especializados;

X. alteração significativa no perfil de risco da empresa.

A melhoria contínua deverá considerar a efetividade prática dos controles, a proporcionalidade das medidas adotadas, a experiência acumulada pela empresa e a evolução do programa de integridade.

28. CANAL DE DÚVIDAS E DEVER DE REPORTE

Dúvidas sobre a aplicação desta Política, sobre a identificação de riscos ou sobre a execução de controles deverão ser submetidas à instância interna competente.

Qualquer pessoa sujeita às normas internas da Check Media que tome conhecimento de risco relevante, falha de controle, tentativa de burla, não conformidade, irregularidade ou situação incompatível com esta Política deverá reportar a matéria pelos canais institucionais competentes.

A comunicação de boa-fé será tratada com confidencialidade e proteção contra retaliação, nos termos das normas internas aplicáveis.

29. APURAÇÃO E MEDIDAS DECORRENTES

Situações de descumprimento desta Política serão tratadas nos termos das normas internas aplicáveis ao canal de denúncias, às investigações internas, à atuação do Comitê de Integridade e Compliance e às demais regras pertinentes do programa de integridade da Check Media.

Confirmada, total ou parcialmente, a ocorrência de infração, poderão ser recomendadas ou adotadas medidas preventivas, corretivas, disciplinares, contratuais, organizacionais ou de remediação, conforme a natureza da conduta, o risco gerado e o vínculo envolvido.

As medidas decorrentes poderão incluir, entre outras, revisão de controle, ajuste de fluxo, alteração de alçada, reforço de treinamento, restrição de acesso, revisão contratual, plano de ação, monitoramento específico, responsabilização disciplinar ou adoção de providências perante terceiros.

30. CASOS OMISSOS

Os casos omissos nesta Política serão resolvidos pelo Comitê de Integridade e Compliance, observados o sistema normativo interno aplicável ao programa de integridade da Check Media e a legislação vigente.

Verificada a necessidade de disciplina permanente sobre matéria omissa, o Comitê poderá recomendar à administração a atualização desta Política ou a edição, revisão ou complementação de manual, procedimento ou norma interna específica.

31. REVISÃO

Esta Política poderá ser revista a qualquer tempo, por iniciativa do Comitê de Integridade e Compliance ou da administração da Check Media, sempre que necessário ao aperfeiçoamento do programa de integridade, à adequação à realidade da empresa, à atualização normativa ou à melhoria dos controles internos e da gestão de riscos.

32. VIGÊNCIA

Esta Política entra em vigor na data de sua aprovação.

Brasília, 11 de junho de 2026.

PEDRO VICTOR MARQUES CRUZ

Compliance Officer

20260611 POLÍTICA DE CONTROLES INTERNOS E GESTÃO DE RISCOS.pdf

Documento número #89a590b6-71fd-4097-a37b-16b0ea621b36

Hash do documento original (SHA256): 0e61c73f26f66022c4b9dbb48552dcc2dc7a70cd2a99a44e918f9eff2605ce3c

Assinaturas**PEDRO VICTOR MARQUES CRUZ**

CPF: 035.352.161-25

Assinou como presidente em 16 jul 2026 às 10:05:54

Log

- 09 jul 2026, 11:32:22 Operador com email giovana.carvalho@checkmedia.com.br na Conta a23c9c0b-5013-4083-8857-f086350d3466 criou este documento número 89a590b6-71fd-4097-a37b-16b0ea621b36. Data limite para assinatura do documento: 08 de agosto de 2026 (11:31). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
- 09 jul 2026, 11:33:34 Operador com email giovana.carvalho@checkmedia.com.br na Conta a23c9c0b-5013-4083-8857-f086350d3466 adicionou à Lista de Assinatura: pedro.cruz@francodemenezes.com.br para assinar como presidente, via E-mail.
- Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo PEDRO VICTOR MARQUES CRUZ e CPF 035.352.161-25.
- 16 jul 2026, 10:05:54 PEDRO VICTOR MARQUES CRUZ assinou como presidente. Pontos de autenticação: Token via E-mail pedro.cruz@francodemenezes.com.br. CPF informado: 035.352.161-25. IP: 191.30.146.217. Componente de assinatura versão 1.1478.0 disponibilizado em https://app.clicksign.com.
- 16 jul 2026, 10:05:55 Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 89a590b6-71fd-4097-a37b-16b0ea621b36.

**Documento assinado com validade jurídica.**Para conferir a validade, acesse <https://www.clicksign.com/validador> e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.

As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 89a590b6-71fd-4097-a37b-16b0ea621b36, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.