

Política de Compliance, Integridade e Anticorrupção

Lei Anticorrupção • ISO 37001:2025 • ISO 37301:2021 • referências CertiGov

Padrão de conduta para prevenir, detectar e responder a suborno, fraude e demais desvios, preservando independência, confiança e legalidade nas relações públicas e privadas.

ORGANIZAÇÃO	VOLK E GIFFONI FERREIRA SOCIEDADE DE ADVOGADOS — CNPJ 23.637.778/0001-01
ELABORAÇÃO	Time Técnico Operacional • 16 de setembro de 2025
APROVAÇÃO	Diretoria e Comitê multidisciplinar
SITUAÇÃO	Aprovado • uso institucional e comunicação ao mercado

Nota de integridade documental. Este instrumento estabelece compromissos e requisitos de governança. Alinhamento normativo não significa certificação, atestado de conformidade ou prova isolada de implementação.

1. Controle e identificação do documento

Campo	Informação
Título	Política de Compliance, Integridade e Anticorrupção
Código	VGF-COM-003
Versão vigente	2.0
Data de elaboração/revisão	16 de setembro de 2025
Elaboração	Time Técnico Operacional
Aprovação	Diretoria e Comitê multidisciplinar
Periodicidade de revisão	Anual ou antes, diante de alteração legal, normativa, operacional, tecnológica ou de risco relevante
Classificação	Público institucional, ressalvados anexos e evidências operacionais classificados
Proprietário do documento	Função de Compliance, com supervisão da Diretoria

1.1 Histórico de versões

Versão	Data	Síntese da alteração	Aprovação
1.0	14 de abril de 2025	Emissão inicial e estruturação dos compromissos institucionais.	Diretoria
2.0	16 de setembro de 2025	Atualização à ISO 37001:2025, fortalecimento do CMS, interação com agentes públicos, diligência, canal, investigações e evidências CertiGov. Inclusão de fluxo executivo ilustrado e catálogo ampliado de requisitos, controles e evidências.	Diretoria e Comitê multidisciplinar

LEITURA CORRETA A versão 2.0 substitui versões anteriores. Cópias impressas são não controladas; a validade deve ser conferida no repositório oficial.

2. Objetivo, escopo e aplicação

Esta Política estabelece o Programa de Integridade e o Sistema de Gestão de Compliance (CMS) da VGF, com abordagem baseada em risco para prevenir, detectar, responder e melhorar controles relativos a suborno, corrupção, fraude, conflito de interesses, lavagem de dinheiro, conluio, infrações concorrenciais e demais obrigações aplicáveis.

Aplica-se à Diretoria, sócios, advogados, estagiários, empregados, prestadores, correspondentes, consultores, parceiros e terceiros que atuem em nome ou no interesse da VGF, observadas a natureza do vínculo, as responsabilidades contratuais e a legislação aplicável. Também orienta a relação com clientes, titulares de dados, fornecedores, autoridades, comunidade e demais partes interessadas.

- Abrange atos praticados direta ou indiretamente, no Brasil ou exterior, perante agentes públicos, clientes, contrapartes, fornecedores, tribunais e entidades privadas.
- Aplica-se a presentes, hospitalidades, viagens, doações, patrocínios, contribuições, comissões, contratação, pagamentos, licitações, obtenção de licenças, investigações e uso de terceiros.
- As referências CertiGov são critérios de preparação e melhoria; não constituem declaração de certificação ou elegibilidade.

HIERARQUIA Em caso de conflito, prevalecem a lei, as normas profissionais da OAB, decisões de autoridade competente e obrigações contratuais mais protetivas. Dúvidas devem ser elevadas ao proprietário do documento antes da ação.

3. Fundamentos, princípios e responsabilidades

3.1 Fundamentos e princípios

Resultados, urgência, prática de mercado, hierarquia ou interesse de cliente jamais justificam vantagem indevida, registro falso, obstrução, fraude ou violação de dever profissional.

- legalidade, ética, boa-fé, independência e exemplo da liderança;
- proibição absoluta de suborno e pagamentos de facilitação;
- segregação de funções, controles proporcionais e rastreabilidade;
- due diligence e gestão responsável de terceiros;
- speak-up, proteção ao denunciante e apuração imparcial;
- responsabilização, remediação e melhoria contínua.

3.2 Estrutura de responsabilidades

Papel	Responsabilidades centrais	Prestação de contas
Diretoria	Aprovar programa, recursos, independência da função e riscos significativos.	Tom da liderança, análise crítica e decisões.
Função de Compliance	Manter riscos, orientar, monitorar, receber relatos, coordenar diligências e reportar.	Acesso direto à Diretoria e relatórios independentes.
Comitê multidisciplinar	Apoiar decisões sobre conflitos, terceiros, investigações, remediação e disciplina.	Atas, impedimentos e deliberações.
Financeiro/Administrativo	Aplicar alçadas, documentação, conciliações e controles de pagamento.	Livros íntegros, exceções e testes.
Gestores e contratantes	Conhecer parceiro, escopo, preço, entrega e sinais de alerta.	Dossiê de contratação e supervisão.
Todos os profissionais e terceiros	Recusar vantagem indevida, declarar conflitos e reportar suspeitas.	Termos, treinamento e cooperação.

3.3 Fluxo executivo de aplicação

O fluxo abaixo resume a sequência decisória esperada. Ele não substitui os procedimentos específicos, mas orienta o leitor sobre quando registrar, consultar, controlar, escalar e aprender.

Ciclo executivo de integridade e compliance

Prevenir, detectar, responder e melhorar com independência



Ciclo contínuo: evidências e indicadores retroalimentam riscos, controles, treinamento e revisão.

Figura 1 — Ciclo executivo do Programa de Integridade.

4. Diretrizes institucionais

O programa deve ser adequado ao perfil de risco da VGF e demonstrado na prática por decisões, controles, entrevistas, testes e remediações.

4.1 Compromisso da liderança e autonomia

A Diretoria demonstra apoio visível e inequívoco, provê recursos e assegura que a função de Compliance possa questionar decisões e reportar sem interferência.

- Incluir integridade em pautas, mensagens, metas, contratações e decisões relevantes.
- Não premiar resultado alcançado por meio impróprio.
- Gerir conflitos da função e permitir acesso a informação, pessoas e documentação.

4.2 Avaliação de riscos de compliance e suborno

Riscos devem ser avaliados periodicamente e antes de novas jurisdições, clientes, serviços, intermediários, licitações ou operações relevantes.

- Considerar interação pública, valor, urgência, remuneração variável, reputação, país, setor, canal, decisão e histórico.
- Definir proprietário, controles, risco residual, plano, prazo e aceitação competente.
- Revisar ao menos anualmente e após incidente ou mudança significativa.

4.3 Proibição de suborno e pagamentos de facilitação

É proibido oferecer, prometer, autorizar, solicitar, receber ou aceitar vantagem indevida, pecuniária ou não, para influenciar ato, decisão, omissão ou obter benefício impróprio.

- A proibição alcança agentes públicos e privados, direta ou indiretamente.
- Pagamentos de facilitação são vedados, ainda que costumeiros ou de baixo valor.
- Situações de ameaça à saúde ou segurança devem ser priorizadas e reportadas assim que seguro, com registro completo.

ALERTA Honorários, êxito, comissões e reembolsos não podem ocultar vantagem indevida. Estrutura incomum, pagamento a terceiro ou conta sem vínculo exigem interrupção e revisão.

4.4 Brindes, presentes, hospitalidades e viagens

Somente são admissíveis quando lícitos, modestos, ocasionais, transparentes, vinculados a propósito legítimo e incapazes de influenciar decisão.

- Proibir dinheiro, equivalentes, itens pessoais relevantes e benefícios durante decisão sensível.
- Exigir aprovação prévia conforme matriz de alçadas e registro de oferta, aceitação ou recusa.
- Aplicar padrão mais restritivo quando envolver agente público, magistrado, membro de tribunal, cliente ou autoridade.

4.5 Doações, patrocínios e ações sociais

Apoios devem ter finalidade legítima, beneficiário identificado, diligência, contrato, aprovação e prestação de contas.

- Proibir contrapartida indevida, indicação para influenciar decisão e repasse oculto.
- Verificar beneficiários finais, vínculos públicos, reputação e aplicação dos recursos.

- Doações políticas pela pessoa jurídica são vedadas; manifestação pessoal deve ser separada da VGF.

4.6 Interação com agentes públicos e sistema de justiça

Toda interação deve respeitar legalidade, impessoalidade, transparência compatível com o sigilo e as prerrogativas profissionais.

- Registrar reuniões institucionais relevantes, participantes, pauta e desdobramentos, quando apropriado.
- Não usar relacionamento, promessa de acesso, informação privilegiada ou ex-agente para vantagem imprópria.
- Cumprir regras de presentes, conflito, quarentena, representação e protocolo do órgão.

4.7 Licitações, contratos públicos e vendas ao governo

Participação em contratação pública deve observar edital, Lei nº 14.133/2021, competição justa, documentação verdadeira e controles compatíveis com referências CertiGov.

- Proibir conluio, cobertura de proposta, ajuste de preço, divisão de mercado, fraude documental ou influência indevida.
- Revisar declarações, impedimentos, sanções, subcontratados, composição de preço e execução.
- Manter evidências de entrega, comunicação, medição, faturamento e alterações contratuais.

4.8 Conflitos de interesses

Conflito real, potencial ou aparente deve ser declarado antes da decisão, contratação, caso ou relacionamento afetado.

- Manter cadastro periódico e declaração por evento.
- Aplicar impedimento, segregação, supervisão, consentimento informado ou afastamento conforme natureza.
- Tratar conflitos profissionais conforme Estatuto e Código de Ética da OAB.

4.9 Due diligence de terceiros e parceiros

Terceiros são avaliados antes e durante a relação, de forma proporcional ao risco e sem substituir julgamento profissional.

- Verificar identidade, beneficiário final, reputação, sanções, agentes públicos, capacidade, conflitos e justificativa comercial.
- Contrato deve definir escopo, remuneração, anticorrupção, auditoria, registros, subcontratação e rescisão.
- Sinais de alerta devem ser resolvidos, mitigados e aprovados antes da contratação ou pagamento.

4.10 Controles financeiros e não financeiros

Pagamentos e decisões devem possuir propósito, documento, aprovação, segregação e correspondência com entrega.

- Proibir caixa paralelo, descrição falsa, nota sem serviço, arredondamento suspeito ou reembolso sem suporte.

- Controlar fornecedores, dados bancários, dupla aprovação, conciliação, despesas, adiantamentos e exceções.
- Aplicar controles não financeiros em contratação, procurações, acesso, propostas, marketing e doações.

4.11 Livros, registros e preservação de evidências

Registros devem ser completos, verdadeiros, tempestivos e suficientemente detalhados para reconstruir a decisão e a transação.

- Não alterar, ocultar, destruir ou fabricar documento relacionado a auditoria, denúncia, processo ou investigação.
- Aplicar retenção, legal hold, controle de versão e acesso mínimo.
- Corrigir erro de modo rastreável, sem apagar o histórico.

4.12 Lavagem de dinheiro, sanções e fraude

A VGF deve conhecer cliente e contraparte conforme risco e observar deveres profissionais e legais aplicáveis, sem assumir obrigação regulatória inexistente.

- Avaliar identidade, beneficiário, origem e propósito quando houver sinal de alerta.
- Escalonar pagamento incompatível, estrutura opaca, jurisdição de risco, pressa anormal ou solicitação de segredo.
- Não avisar indevidamente pessoa sobre apuração protegida ou frustrar medida legítima.

4.13 Concorrência leal e informação de mercado

É proibido acordar preço, cliente, território, proposta, salário ou informação competitivamente sensível com concorrente fora de fundamento legítimo.

- Reuniões associativas devem ter pauta, propósito e cuidado com informação sensível.
- Dados de concorrentes devem vir de fonte lícita e documentada.
- Suspeita de conluio exige interrupção da conversa e comunicação a Compliance.

4.14 Canal, não retaliação e investigação

A Ouvidoria (ouvidoria@vgfadv.com.br) recebe relatos. Apurações devem ser independentes, confidenciais, proporcionais, imparciais e conduzidas por pessoas sem conflito.

- Definir triagem, preservação, escopo, plano, entrevistas, análise, conclusão, decisão e remediação.
- Proteger denunciante, testemunhas e investigados contra retaliação e exposição indevida.
- Encaminhar às autoridades quando legalmente devido ou decidido por instância competente.

4.15 Consequências, remediação e incentivos

Violações podem resultar em orientação, treinamento, advertência, suspensão, desligamento, rescisão, restituição e medidas legais, conforme vínculo, gravidade e devido processo.

- Aplicar critérios consistentes, inclusive à liderança e a quem ignorou sinais.
- Reconhecer condutas íntegras, consulta prévia, recusa de risco e cooperação de boa-fé.
- Corrigir causa raiz, controles, contratos, supervisão e cultura.

4.16 Ética profissional e marketing jurídico

A atuação deve respeitar independência, lealdade, sigilo, conflito, veracidade e limites de publicidade da advocacia.

- Não prometer resultado, mercantilizar, captar clientela ou usar caso concreto de forma vedada.
- Informação pública deve ser objetiva, verdadeira, sóbria e comprovável.
- Reconhecimentos e certificações somente podem ser divulgados quando válidos, verificáveis e no escopo correto.

5. Governança, aplicação, monitoramento e rastreabilidade

5.1 Comunicação, educação e aceite

A VGF disponibiliza conteúdo, trilhas de aprendizagem e assinatura eletrônica de termos na Academy Volk (<https://academyvolk.ultramidnal.com.br/>), sem prejuízo de orientações presenciais ou em outros canais oficiais.

- Capacitação no ingresso e reciclagem ao menos anual, com módulos proporcionais à função e ao risco.
- Registro de convocação, participação, conclusão, avaliação de aprendizagem e aceite da versão vigente.
- Conteúdo extraordinário quando houver incidente, alteração relevante, nova tecnologia, serviço ou requisito.

5.2 Canal, consulta, relato e não retaliação

Dúvidas e relatos podem ser encaminhados à liderança competente ou à Ouvidoria (ouvidoria@vgfadv.com.br). Questões de dados pessoais devem ser dirigidas aos canais do DPO (lgpd@vgfadv.com.br | sancle.albuquerque@midnal.com.br).

- Relatos de boa-fé devem ser recebidos com respeito, confidencialidade, independência e proibição de retaliação.
- A identidade será restrita ao necessário; anonimato será preservado quando oferecido e juridicamente possível.
- Urgências de segurança, integridade física, fraude ou destruição de evidências exigem escalonamento imediato.

5.3 Monitoramento, desvios e melhoria contínua

A efetividade é monitorada por indicadores, testes amostrais, avaliações de risco, reclamações, incidentes, auditorias, diligências e análise crítica da liderança.

- Não conformidades devem ser registradas, contidas, analisadas quanto à causa e tratadas com responsável e prazo.
- Medidas disciplinares são proporcionais, coerentes, documentadas e aplicadas com contraditório quando cabível.
- Resultados relevantes alimentam revisão de riscos, controles, treinamento e documentação.

5.4 Gestão documental e exceções

Somente documentos aprovados e vigentes podem orientar a operação. Exceções devem ser raras, justificadas, temporárias, avaliadas quanto ao risco e aprovadas por autoridade competente.

- Preservar autoria, aprovação, versão, data, classificação, local oficial e prazo de revisão.
- Retirar ou identificar cópias obsoletas e impedir uso não intencional.
- Registrar aceite de risco, controles compensatórios, responsável e data de expiração da exceção.

5.5 ISO 37001:2025 — sistema antissuborno

Cobertura das cláusulas do sistema de gestão e dos controles operacionais essenciais antissuborno.

USO DA MATRIZ Os identificadores facilitam rastreabilidade e auditoria. As descrições são sínteses executivas e não substituem a aquisição, leitura e interpretação da norma oficial aplicável.

Referência	Controle / requisito	Aplicação executiva na VGF	Evidências e verificação
Cl. 4	Contexto da organização	Definir escopo do sistema antissuborno, partes interessadas, requisitos e interfaces relevantes para prevenção, detecção e resposta ao suborno.	Escopo aprovado, mapa de partes interessadas, requisitos e processos.
Cl. 5	Liderança	Demonstrar compromisso, aprovar política, atribuir papéis e integrar prevenção, detecção e resposta ao suborno às decisões da VGF.	Política, organograma, atas, comunicações e provisão de recursos.
Cl. 6	Planejamento	Avaliar riscos e oportunidades, definir objetivos mensuráveis e planejar mudanças relacionadas a prevenção, detecção e resposta ao suborno.	Matriz de riscos, objetivos, indicadores, planos e aceites de risco.
Cl. 7	Apoio	Assegurar recursos, competência, conscientização, comunicação e informação documentada controlada.	Orçamento, competências, Academy, comunicações e controle documental.
Cl. 8	Operação	Planejar, executar e controlar processos e terceiros que materializam prevenção, detecção e resposta ao suborno, inclusive mudanças e exceções.	Procedimentos, contratos, tickets, aprovações, testes e registros operacionais.
Cl. 9	Avaliação de desempenho	Monitorar indicadores, realizar auditoria interna proporcional e promover análise crítica da liderança.	Dashboards, testes, auditorias, atas e planos de correção.
Cl. 10	Melhoria	Tratar não conformidades e incidentes, eliminar causas, verificar eficácia e melhorar continuamente.	Registro de desvios, causa raiz, ações, verificação e lições aprendidas.
AB-01	Função antissuborno independente	Assegurar competência, autoridade, acesso à liderança e ausência de conflito.	Designação, currículo, reporte e atas.
AB-02	Avaliação de risco de suborno	Avaliar países, setores, transações, terceiros, agentes públicos e controles.	Matriz, metodologia, planos e revisão.
AB-03	Due diligence	Aprofundar análise de pessoas, transações, projetos e parceiros conforme risco.	Dossiê, alertas, decisão e atualização.
AB-04	Controles financeiros	Aplicar segregação, alçadas, documentos, conciliações e pagamento rastreável.	ERP, aprovações, amostras e exceções.
AB-05	Controles não financeiros	Controlar contratação, proposta, procuração, acesso, entrega e seleção.	Workflows, contratos, checklists e testes.
AB-06	Presentes e hospitalidades	Definir proibições, limites, aprovação e registro, com rigor para agentes públicos.	Registro, recusas, aprovações e revisão.
AB-07	Doações e patrocínios	Verificar beneficiário, finalidade, conflito, contrapartida e prestação.	Diligência, contrato, pagamento e relatório.
AB-08	Terceiros controlados ou associados	Comunicar requisitos e exigir controles proporcionais ou compromissos contratuais.	Cláusulas, treinamento, certificações e auditoria.
AB-09	Canal e proteção	Disponibilizar relato seguro, confidencial e sem retaliação.	Regulamento, casos, SLA e pesquisa de confiança.
AB-10	Investigação	Preservar independência, competência, evidência e decisão.	Plano, cadeia de custódia, relatório e ata.

AB-11	Consequência e remediação	Aplicar medida proporcional e corrigir causa e controle.	Decisão, CAPA, teste de eficácia e comunicação.
-------	---------------------------	--	---

5.6 ISO 37301:2021 — sistema de gestão de compliance

Cobertura integral das cláusulas 4 a 10 e dos elementos que sustentam cultura, obrigações e desempenho de compliance.

USO DA MATRIZ Os identificadores facilitam rastreabilidade e auditoria. As descrições são sínteses executivas e não substituem a aquisição, leitura e interpretação da norma oficial aplicável.

Referência	Controle / requisito	Aplicação executiva na VGF	Evidências e verificação
Cl. 4	Contexto da organização	Definir escopo do CMS, partes interessadas, requisitos e interfaces relevantes para obrigações de compliance.	Escopo aprovado, mapa de partes interessadas, requisitos e processos.
Cl. 5	Liderança	Demonstrar compromisso, aprovar política, atribuir papéis e integrar obrigações de compliance às decisões da VGF.	Política, organograma, atas, comunicações e provisão de recursos.
Cl. 6	Planejamento	Avaliar riscos e oportunidades, definir objetivos mensuráveis e planejar mudanças relacionadas a obrigações de compliance.	Matriz de riscos, objetivos, indicadores, planos e aceites de risco.
Cl. 7	Apoio	Assegurar recursos, competência, conscientização, comunicação e informação documentada controlada.	Orçamento, competências, Academy, comunicações e controle documental.
Cl. 8	Operação	Planejar, executar e controlar processos e terceiros que materializam obrigações de compliance, inclusive mudanças e exceções.	Procedimentos, contratos, tickets, aprovações, testes e registros operacionais.
Cl. 9	Avaliação de desempenho	Monitorar indicadores, realizar auditoria interna proporcional e promover análise crítica da liderança.	Dashboards, testes, auditorias, atas e planos de correção.
Cl. 10	Melhoria	Tratar não conformidades e incidentes, eliminar causas, verificar eficácia e melhorar continuamente.	Registro de desvios, causa raiz, ações, verificação e lições aprendidas.
CMS-01	Cadastro de obrigações	Identificar leis, contratos, normas profissionais, compromissos e responsáveis.	Matriz legal, alertas e avaliações.
CMS-02	Cultura de compliance	Alinhar liderança, incentivos, decisões, comunicação e consequência.	Pesquisa, mensagens, metas e casos.
CMS-03	Objetivos e indicadores	Definir metas de prevenção, detecção, tempo, qualidade e eficácia.	Dashboard, método e análise crítica.
CMS-04	Controles e procedimentos	Converter obrigação e risco em controle executável e verificável.	Matriz risco-controle, procedimento e amostras.
CMS-05	Relato e aconselhamento	Facilitar consulta antes da decisão e relato de boa-fé.	Canal, pareceres, consultas e métricas.
CMS-06	Investigações e resposta	Investigar, decidir, comunicar, remediar e preservar direitos.	Dossiês, decisões, CAPA e lições.
CMS-07	Auditoria e melhoria	Testar desenho e eficácia e tratar lacunas até o fechamento.	Plano, achados, responsáveis e reteste.

5.7 Lei Anticorrupção, Decreto 11.129/2022 e CertiGov

Rastreabilidade dos principais elementos legais e de preparação para avaliações externas de integridade em relações com o setor público.

USO DA MATRIZ Os identificadores facilitam rastreabilidade e auditoria. As descrições são sínteses executivas e não substituem a aquisição, leitura e interpretação da norma oficial aplicável.

Referência	Controle / requisito	Aplicação executiva na VGF	Evidências e verificação
Lei 12.846, art. 5º	Atos lesivos	Proibir vantagem, fraude à licitação, obstrução e uso de interposta pessoa.	Treinamento, controles, casos e diligência.
Lei 12.846, arts. 6–7	Sanções e programa de integridade	Conhecer consequências e demonstrar programa efetivo, não apenas documental.	Evidências de execução e melhoria.
Dec. 11.129, art. 56	Programa de integridade	Prevenir, detectar e sanar desvios e fomentar cultura.	Políticas, riscos, canal, auditoria e remediação.
Dec. 11.129, art. 57	Parâmetros de avaliação	Cobrir liderança, padrões, terceiros, treinamento, registros, controles, canal e monitoramento.	Matriz de aderência e amostras.
Lei 14.133/2021	Contratações públicas	Assegurar proposta verdadeira, competição, execução, integridade e sustentabilidade.	Dossiê de licitação e execução.
CertiGov-01	Conhecimento do negócio público	Mapear órgãos, agentes, concorrentes, regras, canais e riscos.	Mapa de interação e matriz de risco.
CertiGov-02	Gestão de terceiros e colaboradores	Aplicar diligência, treinamento, contratos e entrevistas de cultura.	Dossiês, Academy, termos e entrevistas.
CertiGov-03	Canal e tratativas	Demonstrar acesso, confiança, independência e resposta.	Regulamento, métricas e casos anonimizados.
CertiGov-04	Controles comerciais e comissões	Justificar preço, comissão, parceiro, entrega e pagamento.	Proposta, contrato, cálculo e aprovação.
CertiGov-05	Eficácia e melhoria	Comprovar uso real por teste, entrevista, incidente e correção.	Auditorias, CAPA, atas e indicadores.

5.8 Referências normativas e informacionais

As referências abaixo orientam a interpretação e a atualização deste documento. Normas técnicas são aplicadas de forma proporcional ao contexto da VGF e não representam declaração de certificação.

- Portal institucional da VGF Advogados — <https://www.vgfadv.com.br>
- Código de Ética e Disciplina da OAB — <https://www.oab.org.br/leisnormas/legislacao/resolucoes/02-2015>
- Provimento CFOAB nº 205/2021 — publicidade e informação da advocacia — <https://www.oab.org.br/leisnormas/legislacao/provimentos/205-2021>
- Lei nº 12.846/2013 — Lei Anticorrupção — https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm
- Decreto nº 11.129/2022 — https://planalto.gov.br/ccivil_03/_ato2019-2022/2022/decreto/d11129.htm
- Lei nº 14.133/2021 — Licitações e Contratos — https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14133.htm
- Programa de Integridade — diretrizes CGU — <https://www.gov.br/cgu/pt-br/assuntos/integridade-privada/materiaisdeorientacao>
- ISO 37001:2025 — antissuborno — <https://www.iso.org/standard/37001>
- ISO 37301:2021 — compliance — <https://www.iso.org/standard/75080.html>
- Referências públicas CertiGov — <https://certigov.com.br/como-a-certificacao-certigov-pode-diferenciar-sua-empresa-em-licitacoes-publicas/>

5.9 Matriz de rastreabilidade para avaliações de terceiros

A matriz indica onde o compromisso está definido e qual evidência operacional deve corroborar eventual resposta a questionários. A política, isoladamente, demonstra desenho de controle; a efetividade depende de registros atuais, amostras, configurações, contratos, relatórios ou entrevistas.

Formulário / item	Tema avaliado	Referência neste documento	Evidência recomendada
CertiGov / cultura	Liderança, política, treinamento e entrevistas.	4.1; 5.1; 5.3	Mensagens, atas, trilhas Academy, entrevistas e indicadores.
CertiGov / riscos	Riscos de integridade e interação pública.	4.2; 4.6–4.7	Matriz de riscos, planos, mapa de agentes públicos e licitações.
CertiGov / terceiros	Due diligence, parceiros e comissões.	4.8–4.10	Dossiê KYP, beneficiário final, contrato, aprovação e monitoramento.
CertiGov / canal	Denúncia, não retaliação e tratativas.	4.14–4.15; 5.2	Regulamento do canal, casos anonimizados, SLA, investigação e remediação.
Maturidade 15.1	Inventário e gestão de provedores.	4.9; 5.3	Cadastro, classificação, dono, revisão e riscos do fornecedor.
Requisitos públicos	Licitação, competição, entrega e registros.	4.6–4.7; 4.10–4.11	Edital, proposta, declarações, aprovações, execução, faturamento e auditoria.

5.C01 Caderno de controle — liderança, independência e cultura de integridade

LEITURA EXECUTIVA Este caderno converte o compromisso sobre liderança, independência e cultura de integridade em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para liderança, independência e cultura de integridade é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para liderança, independência e cultura de integridade.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de liderança, independência e cultura de integridade estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema liderança,

independência e cultura de integridade deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C02 Caderno de controle — avaliação de riscos de compliance e suborno

LEITURA EXECUTIVA Este caderno converte o compromisso sobre avaliação de riscos de compliance e suborno em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para avaliação de riscos de compliance e suborno é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para avaliação de riscos de compliance e suborno.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de avaliação de riscos de compliance e suborno estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema avaliação de

riscos de compliance e suborno deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C03 Caderno de controle — cadastro e atualização de obrigações

LEITURA EXECUTIVA Este caderno converte o compromisso sobre cadastro e atualização de obrigações em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para cadastro e atualização de obrigações é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para cadastro e atualização de obrigações.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de cadastro e atualização de obrigações estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema cadastro e atualização de obrigações deve integrar a avaliação de entrada. Se a resposta depender de premissa não

confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C04 Caderno de controle — políticas, procedimentos e controles documentados

LEITURA EXECUTIVA Este caderno converte o compromisso sobre políticas, procedimentos e controles documentados em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para políticas, procedimentos e controles documentados é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para políticas, procedimentos e controles documentados.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de políticas, procedimentos e controles documentados estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema políticas,

procedimentos e controles documentados deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C05 Caderno de controle — due diligence de clientes e partes relacionadas

LEITURA EXECUTIVA Este caderno converte o compromisso sobre due diligence de clientes e partes relacionadas em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para due diligence de clientes e partes relacionadas é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para due diligence de clientes e partes relacionadas.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de due diligence de clientes e partes relacionadas estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema due diligence

de clientes e partes relacionadas deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C06 Caderno de controle — due diligence de fornecedores, parceiros e correspondentes

LEITURA EXECUTIVA Este caderno converte o compromisso sobre due diligence de fornecedores, parceiros e correspondentes em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para due diligence de fornecedores, parceiros e correspondentes é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para due diligence de fornecedores, parceiros e correspondentes.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de due diligence de fornecedores, parceiros e correspondentes estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema due diligence

de fornecedores, parceiros e correspondentes deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C07 Caderno de controle — interação com agentes públicos e autoridades

LEITURA EXECUTIVA Este caderno converte o compromisso sobre interação com agentes públicos e autoridades em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para interação com agentes públicos e autoridades é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para interação com agentes públicos e autoridades.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de interação com agentes públicos e autoridades estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema interação com

agentes públicos e autoridades deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C08 Caderno de controle — licitações, contratos públicos e CertiGov

LEITURA EXECUTIVA Este caderno converte o compromisso sobre licitações, contratos públicos e certigov em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para licitações, contratos públicos e certigov é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para licitações, contratos públicos e certigov.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de licitações, contratos públicos e certigov estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema licitações, contratos públicos e certigov deve integrar a avaliação de entrada. Se a resposta depender de premissa não

confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C09 Caderno de controle — presentes, hospitalidades, viagens e entretenimento

LEITURA EXECUTIVA Este caderno converte o compromisso sobre presentes, hospitalidades, viagens e entretenimento em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para presentes, hospitalidades, viagens e entretenimento é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para presentes, hospitalidades, viagens e entretenimento.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de presentes, hospitalidades, viagens e entretenimento estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema presentes,

hospitalidades, viagens e entretenimento deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C10 Caderno de controle — doações, patrocínios e investimento social

LEITURA EXECUTIVA Este caderno converte o compromisso sobre doações, patrocínios e investimento social em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para doações, patrocínios e investimento social é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para doações, patrocínios e investimento social.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de doações, patrocínios e investimento social estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema doações, patrocínios e investimento social deve integrar a avaliação de entrada. Se a resposta depender de premissa não

confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C11 Caderno de controle — contribuições políticas e neutralidade institucional

LEITURA EXECUTIVA Este caderno converte o compromisso sobre contribuições políticas e neutralidade institucional em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para contribuições políticas e neutralidade institucional é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para contribuições políticas e neutralidade institucional.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de contribuições políticas e neutralidade institucional estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema contribuições

políticas e neutralidade institucional deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C12 Caderno de controle — conflitos de interesses e partes relacionadas

LEITURA EXECUTIVA Este caderno converte o compromisso sobre conflitos de interesses e partes relacionadas em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para conflitos de interesses e partes relacionadas é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para conflitos de interesses e partes relacionadas.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de conflitos de interesses e partes relacionadas estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema conflitos de

interesses e partes relacionadas deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C13 Caderno de controle — comissões, indicações e remuneração de intermediários

LEITURA EXECUTIVA Este caderno converte o compromisso sobre comissões, indicações e remuneração de intermediários em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para comissões, indicações e remuneração de intermediários é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para comissões, indicações e remuneração de intermediários.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de comissões, indicações e remuneração de intermediários estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema comissões,

indicações e remuneração de intermediários deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C14 Caderno de controle — controles financeiros, pagamentos e reembolsos

LEITURA EXECUTIVA Este caderno converte o compromisso sobre controles financeiros, pagamentos e reembolsos em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para controles financeiros, pagamentos e reembolsos é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para controles financeiros, pagamentos e reembolsos.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de controles financeiros, pagamentos e reembolsos estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema controles

financeiros, pagamentos e reembolsos deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C15 Caderno de controle — controles não financeiros e segregação de funções

LEITURA EXECUTIVA Este caderno converte o compromisso sobre controles não financeiros e segregação de funções em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para controles não financeiros e segregação de funções é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para controles não financeiros e segregação de funções.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de controles não financeiros e segregação de funções estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema controles não

financeiros e segregação de funções deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C16 Caderno de controle — livros, registros, documentos e rastreabilidade

LEITURA EXECUTIVA Este caderno converte o compromisso sobre livros, registros, documentos e rastreabilidade em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para livros, registros, documentos e rastreabilidade é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para livros, registros, documentos e rastreabilidade.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de livros, registros, documentos e rastreabilidade estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema livros,

registros, documentos e rastreabilidade deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C17 Caderno de controle — prevenção à lavagem de dinheiro no contexto aplicável

LEITURA EXECUTIVA Este caderno converte o compromisso sobre prevenção à lavagem de dinheiro no contexto aplicável em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para prevenção à lavagem de dinheiro no contexto aplicável é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para prevenção à lavagem de dinheiro no contexto aplicável.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de prevenção à lavagem de dinheiro no contexto aplicável estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema prevenção à

lavagem de dinheiro no contexto aplicável deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C18 Caderno de controle — concorrência leal e troca de informações

LEITURA EXECUTIVA Este caderno converte o compromisso sobre concorrência leal e troca de informações em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para concorrência leal e troca de informações é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para concorrência leal e troca de informações.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de concorrência leal e troca de informações estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema concorrência leal e troca de informações deve integrar a avaliação de entrada. Se a resposta depender de premissa não

confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C19 Caderno de controle — canal de denúncias e proibição de retaliação

LEITURA EXECUTIVA Este caderno converte o compromisso sobre canal de denúncias e proibição de retaliação em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para canal de denúncias e proibição de retaliação é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para canal de denúncias e proibição de retaliação.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de canal de denúncias e proibição de retaliação estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema canal de

denúncias e proibição de retaliação deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C20 Caderno de controle — triagem, investigação e cadeia de custódia

LEITURA EXECUTIVA Este caderno converte o compromisso sobre triagem, investigação e cadeia de custódia em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para triagem, investigação e cadeia de custódia é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para triagem, investigação e cadeia de custódia.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de triagem, investigação e cadeia de custódia estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema triagem,

investigação e cadeia de custódia deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C21 Caderno de controle — decisão, sanção, remediação e causa raiz

LEITURA EXECUTIVA Este caderno converte o compromisso sobre decisão, sanção, remediação e causa raiz em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para decisão, sanção, remediação e causa raiz é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para decisão, sanção, remediação e causa raiz.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de decisão, sanção, remediação e causa raiz estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema decisão, sanção, remediação e causa raiz deve integrar a avaliação de entrada. Se a resposta depender de premissa não

confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C22 Caderno de controle — aconselhamento prévio e consulta de compliance

LEITURA EXECUTIVA Este caderno converte o compromisso sobre aconselhamento prévio e consulta de compliance em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para aconselhamento prévio e consulta de compliance é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para aconselhamento prévio e consulta de compliance.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de aconselhamento prévio e consulta de compliance estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema

aconselhamento prévio e consulta de compliance deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C23 Caderno de controle — treinamento por risco e comunicação contínua

LEITURA EXECUTIVA Este caderno converte o compromisso sobre treinamento por risco e comunicação contínua em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para treinamento por risco e comunicação contínua é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para treinamento por risco e comunicação contínua.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de treinamento por risco e comunicação contínua estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema treinamento

por risco e comunicação contínua deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C24 Caderno de controle — cláusulas de integridade e direitos de auditoria

LEITURA EXECUTIVA Este caderno converte o compromisso sobre cláusulas de integridade e direitos de auditoria em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para cláusulas de integridade e direitos de auditoria é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para cláusulas de integridade e direitos de auditoria.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de cláusulas de integridade e direitos de auditoria estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema cláusulas de

integridade e direitos de auditoria deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C25 Caderno de controle — monitoramento de transações e sinais de alerta

LEITURA EXECUTIVA Este caderno converte o compromisso sobre monitoramento de transações e sinais de alerta em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para monitoramento de transações e sinais de alerta é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para monitoramento de transações e sinais de alerta.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de monitoramento de transações e sinais de alerta estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema

monitoramento de transações e sinais de alerta deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C26 Caderno de controle — auditoria independente e testes de eficácia

LEITURA EXECUTIVA Este caderno converte o compromisso sobre auditoria independente e testes de eficácia em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para auditoria independente e testes de eficácia é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para auditoria independente e testes de eficácia.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de auditoria independente e testes de eficácia estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema auditoria

independente e testes de eficácia deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C27 Caderno de controle — indicadores, reporte e análise crítica da direção

LEITURA EXECUTIVA Este caderno converte o compromisso sobre indicadores, reporte e análise crítica da direção em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para indicadores, reporte e análise crítica da direção é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para indicadores, reporte e análise crítica da direção.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de indicadores, reporte e análise crítica da direção estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema indicadores,

reporte e análise crítica da direção deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

5.C28 Caderno de controle — plano de melhoria e preparação para avaliação externa

LEITURA EXECUTIVA Este caderno converte o compromisso sobre plano de melhoria e preparação para avaliação externa em uma rotina verificável. Aplica-se a decisões, relações comerciais, contratações, pagamentos, interações públicas, terceiros e atividades profissionais em nome da VGF e deve ser usado antes da decisão, durante a execução e na revisão de eficácia. O objetivo é permitir que qualquer leitor compreenda o que deve ser feito, quem decide, qual evidência comprova a prática e quando o tema precisa ser escalado.

Objetivo, resultado e critério de aceitação

O resultado esperado para plano de melhoria e preparação para avaliação externa é uma decisão coerente com Lei 12.846/2013, Decreto 11.129/2022, ISO 37001:2025, ISO 37301:2021, Lei 14.133/2021 e compromissos CertiGov, baseada em risco, documentada no nível proporcional ao impacto e passível de reconstrução por terceiro independente. O controle é considerado implementado somente quando há responsável designado, critério prévio, execução demonstrável, tratamento de exceções e verificação periódica.

Aplicação operacional mínima

- Planejar: o Compliance e dono do processo ou contratação define finalidade, entradas, critérios, alçada, prazo e evidência necessária para plano de melhoria e preparação para avaliação externa.
- Executar: utilizar fluxo oficial, segregação de funções e validações proporcionais; decisões sensíveis dependem de Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
- Registrar: preservar solicitação, análise, aprovação, resultado, comunicação e eventual exceção em repositório oficial de Compliance, sistema financeiro ou dossiê contratual.
- Verificar: realizar anual, por transação de risco e sempre que houver alerta, denúncia ou mudança relevante teste de desenho e amostra de eficácia, registrando população, seleção, resultado e conclusão.
- Corrigir: desvios devem ser contidos, avaliados quanto à causa, tratados por plano com responsável e submetidos a reteste.

Elemento	Padrão verificável
Responsabilidade	Dono: Compliance e dono do processo ou contratação. Consultados: Jurídico, Financeiro, Pessoas, Segurança, Privacidade e gestor da relação. Aprovação/escalamento: Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.
Evidência mínima	Registro de entrada, análise, decisão, execução e verificação; conservação em repositório oficial de Compliance, sistema financeiro ou dossiê contratual com acesso por necessidade.
Indicadores	Percentual de casos conformes; exceções vencidas; tempo de decisão; reincidência; cobertura de treinamento; ações corretivas no prazo.
Teste e alerta	Amostra baseada em risco e revisão após mudança. Escalar imediatamente quando houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito.

Perguntas executivas para aprovação

- A finalidade e a necessidade de plano de melhoria e preparação para avaliação externa estão claras e permanecem válidas?
- Os riscos, pessoas afetadas, dependências, obrigações e possíveis conflitos foram avaliados?
- A evidência produzida permite demonstrar não apenas a existência, mas a efetividade do controle?
- Há condição de parada, prazo de reavaliação e responsável por corrigir eventual resultado adverso?

GATILHO DE PROJETO OU CONTRATO Em novo projeto, produto, fornecedor ou contrato, o tema plano de

melhoria e preparação para avaliação externa deve integrar a avaliação de entrada. Se a resposta depender de premissa não confirmada, a aprovação será condicionada; se houver vantagem indevida, agente público, fraude, conflito não mitigável, recusa de diligência, obstrução ou indício de ilícito, o caso seguirá para Função de Compliance, Comitê multidisciplinar ou Diretoria, conforme alçada e independência requerida.

6. Potenciais Registros que podem Ser Gerados

Os registros abaixo são potenciais evidências de execução. A retenção indicada é recomendação mínima e deve ser ajustada pelo inventário de dados, tabela de temporalidade, obrigação legal, ordem de preservação, contrato e necessidade de defesa de direitos. Registros sujeitos a sigilo profissional ou legal exigem segregação e acesso por necessidade de conhecer.

Registro / Evidência	Tipo	Responsável (Área dona)	Local oficial	Proteção (mínimo)	Contém dados pessoais?	Retenção mínima (recom.)	Disposição final	Classificação	Descarte seguro	Observações de conformidade
Avaliação de riscos de integridade	Matriz	Compliance + donos	Repositório CMS	Versionamento, aprovação e acesso	Possivelmente	Vigência + 5 anos	Eliminar após prazo/hold	Restrito	Exclusão segura	Revisão anual e por evento; registrar risco residual.
Declarações de conflito	Formulário	Compliance + Pessoas	Sistema/ECM restrito	MFA, segregação e logs	Sim	Vínculo + 5 anos	Eliminar após prazo	Confidencial	Exclusão segura	Atualização anual e por evento; decisões de mitigação.
Registro de brindes e hospitalidades	Registro	Compliance + Financeiro	Repositório CMS	Alçadas e trilha	Sim	5 anos	Eliminar após prazo	Interno	Exclusão segura	Incluir oferta, recusa, valor, envolvidos, agente público e aprovação.
Due diligence de terceiros	Dossiê	Contratante + Compliance	ECM contratual	Acesso mínimo, hold e logs	Sim	Contrato + 10 anos	Eliminar após prazo/hold	Restrito	Trituração/exclusão certificada	Documentar beneficiário, risco, alertas, mitigação e revisão.
Canal e investigações	Dossiê	Ouvidoria/Comitê	Repositório segregado	Criptografia, need-to-know e logs	Sim, potencialmente sensíveis	10 anos após encerramento	Eliminar após prazo/hold	Altamente restrito	Exclusão certificada	Imparcialidade, não retaliação, cadeia de custódia e privacidade.
Controles de pagamentos e despesas	Transação/log	Financeiro	ERP/repositório fiscal	Segregação, dupla aprovação e backup	Possivelmente	Prazo fiscal/legal + 5 anos	Eliminar após prazo/hold	Confidencial	Exclusão segura	Correspondência entre contrato, entrega, nota, aprovação e pagamento.
Treinamento e aceite de integridade	Certificado/log	Compliance + Pessoas	Academy Volk	Conta individual e trilha	Sim	Vínculo + 5 anos	Eliminar/anonimizar	Interno	Exclusão segura	Conteúdo por risco, avaliação e versão da política.
Atas e análise crítica do CMS	Ata/relatório	Compliance + Diretoria	Repositório de governança	Perfis, assinatura e versão	Possivelmente	10 anos	Eliminar após prazo/hold	Restrito	Exclusão segura	Registrar decisões, recursos, indicadores, riscos e ações.

FECHAMENTO O proprietário do documento deve verificar, na revisão anual, se os registros estão sendo produzidos, protegidos, retidos e descartados conforme definido. Lacunas devem gerar plano de ação com responsável e prazo.