Instituto Sustenta

PÚBLICO

MANUAL DE COMPLIANCE

Manual de Gestão do Compliance e Anticorrupção Institucional

MA-003



Responsável
COMITÊ MULTIDISCIPLINAR

institutosustenta.org.br

Controle de Versões do Documento

Versão	Data	Elaborador	Revisor	Observações
1.0	**01/07/2024**	Comitê Multidisciplinar	Comitê Multidisciplinar	Criação inicial

Informações sobre a Utilização e Controle do Documento

Somente a versão eletrônica disponibilizada no repositório oficial de documentos (ECM) do Instituto Sustenta é considerada válida. Cópias impressas ou arquivos extraídos não são controlados. Alterações de versão serão comunicadas às partes interessadas por meio dos canais institucionais. Em caso de divergências, prevalece a versão vigente no ECM.

Sumário

1. Apresentação Institucional e Diretrizes Gerais 9
1.1 Finalidade do Manual e Escopo de Aplicação 9
1.2 Abrangência de Partes Interessadas 9
1.3 Princípios Éticos e Cultura de Integridade 10
1.4 Base Normativa e Legal 10
1.5 Missão, Visão e Valores de Compliance e Anticorrupção 11
1.6 Estrutura Documental (Políticas, Normas, Procedimentos e Registros) 11
1.7 Gestão do Conhecimento, Comunicação e Treinamento 12
2. Contexto da Organização 14
2.1 Entendimento da organização e do seu contexto (interno e externo) 14
2.1.1 Fatores internos — exemplos (checklist) 15
2.1.2 Fatores externos — exemplos (checklist) 15
2.1.3 Ferramental recomendado 15
2.2 Partes interessadas e suas necessidades/expectativas 16
2.2.1 Identificação e requisitos (exemplo orientativo) 16
2.2.2 Matriz de Partes Interessadas e Criticidade (exemplo) 17
2.3 Escopo do SGC/SGAS 18
2.3.1 Declaração de escopo (modelo para aprovação) 18
2.3.2 Exclusões (se houver) 18
2.3.3 Interfaces relevantes 18
2.4 Integração do SGAS ao SGC e a outros sistemas 18
2.4.1 Mapa de integração (exemplo) 18
2.4.2 Papéis e responsabilidades (RACI de alto nível) 19
2.5 Obrigações de compliance (catálogo e matriz) 20
2.5.1 Catálogo de obrigações — modelo 20
2.6 Avaliação de riscos de compliance e de suborno (visão geral) 20
2.6.1 Critérios e taxonomias (resumo) 20
2.6.2 Exemplo de riscos e controles vinculados ao contexto 21
2.7 Comunicação do contexto e conscientização 21
3. Liderança e Governança 22
3.1 Compromisso e liderança da Alta Direção e do Conselho 22
3.2 Política de Compliance e Antissuborno 22
3.3 Papéis, responsabilidades e autoridades 23
3.4 Tom de topo, cultura e clima de integridade 24
3.5 Recursos e competências 25

3.6 Incentivos e consequências (disciplinares e reconhecimentos) 25
3.7 Comunicação interna e externa 26
3.8 Mecanismos de supervisão e reporte 26
3.9 Conflitos de interesse e segregação de funções (governança aplicada) 26
3.10 Due diligence de alta gestão e terceiros estratégicos (governança) 27
3.11 Integração com auditoria interna/externa e órgãos de controle 27
4. Planejamento 28
4.1 Ações para abordar riscos e oportunidades 28
4.2 Avaliação de riscos de compliance e riscos de suborno 29
4.2.1 Metodologia (passo a passo) 29
4.2.2 Apetite e tolerância a risco (modelo) 29
4.2.3 Critérios de avaliação (escalas) 30
4.2.4 Matriz de riscos (modelo consolidado) 30
4.2.5 Due diligence (DD) de terceiros — abordagem baseada em risco 30
4.2.6 Temas sensíveis (critérios mínimos a definir) 31
4.3 Objetivos de compliance e antissuborno e planejamento para atingi-los 31
4.3.1 Estabelecimento de objetivos (modelo SMART) 31
4.3.2 Plano para atingir objetivos (exemplo) 31
4.4 Planejamento de mudanças 32
4.5 Indicadores (KPIs/KRIs) sugeridos 32
4.6 Boas práticas 33
5. Apoio 33
5.1 Recursos 33
5.2 Competência e Treinamento (EAD e presencial) 34
5.3 Conscientização e Comunicação 34
5.4 Informação Documentada (Documentos e Registros) 35
5.5 Due Diligence de Terceiros (fornecedores, parceiros, consultores, doadores, beneficiários críticos) 35
5.6 Canais de Denúncia e Proteção ao Denunciante 36
5.7 Incentivos e Consequências (Disciplina/Reconhecimentos) 37
5.8 Gestão de Contratos e Cláusulas de Integridade 37
5.9 Ferramentas Tecnológicas de Integridade 37
5.10 Privacidade e Proteção de Dados (interface com LGPD) 38
5.11 Gestão do Conhecimento 38
6. Operação 39
6.1 Planejamento e Controle Operacionais 39

6.2 Controles Antissuborno Específicos 40
6.2.1 Brindes, Presentes e Hospitalidades 40
6.2.2 Conflitos de Interesse 40
6.2.3 Pagamentos de Facilitação 41
6.2.4 Interações com Agentes Públicos (e privados de alto risco) 41
6.2.5 Compras, Contratações e Cartões Corporativos/Caixa Miúdo 41
6.3 Due Diligence Reforçada para Interações de Maior Risco 42
6.4 Controles em Projetos, Convênios e Termos de Fomento 42
6.5 Gestão de Investigações Internas e Respostas a Violações 43
6.6 Cooperação com Autoridades e Órgãos de Controle 43
6.7 Fluxos Operacionais (Modelos) 44
6.7.1 Fluxo — Compras/Contratos (resumo) 44
6.7.2 Fluxo — Brindes/Hospitalidades 44
6.7.3 Fluxo — Denúncias/Investigações 44
6.8 RACI Operacional (alto nível) 44
6.9 Indicadores Operacionais (sugestões) 45
6.10 Periodicidades Consolidada (cap. 6) 45
6.11 Saídas do Capítulo (entregáveis mínimos) 46
7. Avaliação de Desempenho 46
7.1 Monitoramento, Medição, Análise e Avaliação 46
7.1.1 Escopo do monitoramento 46
7.1.2 Papel e responsabilidades 46
7.1.3 Metodologia de medição 46
7.1.4 Painel de Indicadores (modelo) 47
7.2 Auditorias Internas 47
7.2.1 Princípios 47
7.2.2 Programa Anual de Auditorias (modelo) 48
7.2.3 Planejamento de auditoria (passos) 48
7.2.4 Classificação de achados (exemplo) 48
7.2.5 Amostragem (diretrizes) 49
7.3 Análise Crítica pela Direção 49
7.3.1 Insumos (inputs) mínimos 49
7.3.2 Saídas (outputs) esperadas 49
7.3.3 Roteiro da reunião (modelo) 50
7.4 Relato e Transparência 50
7.5 Maturidade do Programa (diagnóstico anual) 51

7.6 Não Conformidades, Ações Corretivas e Melhoria (ponte para o Cap. 8) 51
7.7 Saídas do Capítulo (entregáveis mínimos) 51
8. Melhoria 52
8.1 Objetivo e Princípios 52
8.2 Tipos de Entradas para Melhoria 52
8.3 Processo de Tratamento de Não Conformidades (NC) e Ação Corretiva (CAPA) 53
8.3.1 Fluxo (modelo) 53
8.3.2 Regras Gerais 53
8.3.3 Análise de Causa — Métodos Recomendados 53
8.3.4 Plano de Ação Corretiva (CAPA) 53
8.3.5 Verificação de Eficácia 54
8.4 Oportunidades de Melhoria (OM) e Inovação 54
8.5 Integração com Gestão de Riscos e Mudanças 54
8.6 Documentos, Registros e Controle no ECM 55
8.7 Indicadores (KPIs/KRIs) — Melhoria 55
8.8 Boas Práticas 56
8.9 Saídas do Capítulo (entregáveis mínimos) 56
9. Políticas e Procedimentos Específicos do Instituto Sustenta 56
9.1 Código de Conduta e Integridade 56
9.2 Política Antissuborno 57
9.3 Política de Conflito de Interesses 57
9.4 Política de Brindes, Presentes e Hospitalidades 58
9.5 Política de Doações, Patrocínios e Parcerias Socioambientais 58
9.6 Política de Contratações e Due Diligence de Terceiros 59
9.7 Política de Relacionamento com o Setor Público 59
9.8 Política de Investigações Internas e Medidas Disciplinares 60
9.9 Política de Proteção ao Denunciante e Não Retaliação 60
9.10 Política de Privacidade e Proteção de Dados (interface com LGPD) 61
9.11 Modelos e Cláusulas Padrão (resumo para o ECM) 61
9.12 Responsabilidades e Governança das Políticas 62
9.13 Indicadores Consolidados do Capítulo (sugestões) 63
10. Indicadores, Registros e Evidências 63
10.1 Princípios Gerais 63
10.2 Taxonomia de Registros (padrão ECM) 63
10.3 Tabela de Retenção e Descarte (mínimo recomendado) 65
10.4 Mapa Requisito → Controle → Evidência (exemplos) 66

10.5 Dicionário de Indicadores (KPIs/KRIs) 67
10.5.1 Governança & Cultura 67
10.5.2 Riscos & Due Diligence 67
10.5.3 Operação & Canal 68
10.5.4 Conflitos/Brindes/Setor Público 68
10.5.5 Melhoria & Auditoria 68
10.6 Amostragem de Evidências (por risco) 69
10.7 Qualidade de Dados e Validação 69
10.8 Dashboards e Relatórios (modelos) 69
10.9 Roteiro de Evidências por Tema Sensível (checklists) 69
10.10 Periodicidades Consolidadas (cap. 10) 70
10.11 Papéis e Responsabilidades 70
11. Anexos Operacionais 71
11.1 Modelos e Formulários (para ECM) 71
11.1.1 Declaração de Conflito de Interesses (Modelo) 71
11.1.2 Formulário de Brindes, Presentes e Hospitalidades 71
11.1.3 Checklist de Compras/Contratos 71
11.1.4 Dossiê de Due Diligence de Terceiros (Capa Padrão) 71
11.1.5 Plano de Investigação Interna (Template) 72
11.1.6 Relatório Conclusivo de Investigação (Template) 72
11.1.7 CAPA — Ação Corretiva (Modelo) 72
11.1.8 Checklist de Prestação de Contas (Convênios/Projetos) 72
11.1.9 Termo de Ciência e Adesão ao Código/Políticas 72
11.1.10 Cláusulas Contratuais Padrão (pacote) 72
11.2 Roteiro de Treinamento Anual (EAD) e Termos 73
11.2.1 Trilhas Obrigatórias (por público) 73
11.2.2 Grade e Metas 73
11.2.3 Termos Padrão (para EAD) 73
11.3 Tabela de Classificação de Riscos (exemplo para matriz) 73
11.4 Fluxogramas (representação textual simplificada) 74
11.4.1 Denúncias e Investigações 74
11.4.2 Compras e Contratações 74
11.4.3 Doações/Patrocínios/Parcerias 74
11.4.4 Conflitos de Interesses 74
11.4.5 Relacionamento com Setor Público 75
11.5 Glossário de Termos 75

12. Matriz de Conformidade 75
12.1 ISO 37001 — Sistema de Gestão Antissuborno 75
12.2 ISO 37301 — Sistema de Gestão de Compliance..... 81
12.3 Matriz de Conformidade Legal — Lei 12.846/2013 e Decreto 11.129/2022..... 85

1. Apresentação Institucional e Diretrizes Gerais

1.1 Finalidade do Manual e Escopo de Aplicação

Este Manual estabelece princípios, políticas e controles que compõem o **Sistema de Gestão de Compliance (SGC)** e o **Sistema de Gestão Antissuborno (SGAS)** do Instituto Sustenta. Aplica-se **a toda a organização** (diretoria, conselho, gerências, colaboradores, estagiários e voluntários) e **a todas as partes interessadas** com as quais o Instituto se relaciona (fornecedores, parceiros, consultores, patrocinadores, doadores e beneficiários), em qualquer atividade, projeto, convênio, termo de fomento ou parceria com os setores público e privado. Baseia-se nas normas ISO 37001:2025 e ISO 37301:2021/Amd 1:2024 e observa a legislação brasileira aplicável. (ISO)

Nota explicativa: Este manual é normativo. As **políticas** e **procedimentos** dele decorrentes detalham responsabilidades e controles operacionais. Nem todos os controles são obrigatórios em todos os cenários; devem ser aplicados segundo **proporcionalidade e risco** (ver Cap. 4 – Planejamento).

1.2 Abrangência de Partes Interessadas

Partes internas: Conselho, Diretoria Executiva, Comitê de Integridade (quando instituído), liderança, equipes, estagiários e voluntários.
Partes externas: Fornecedores, parceiros de projeto, consultores, doadores, patrocinadores, beneficiários, órgãos de controle e o público em geral.

Quadro 1 — Envolvimento mínimo por parte interessada

Parte interessada	Responsabilidades mínimas	Interações previstas	Documentos/Registros esperados
Conselho/Alta Direção	Aprovar políticas, prover recursos, definir apetite de risco, dar “tom do topo”	Reuniões trimestrais com Compliance	Atas, plano anual, análise crítica
Diretoria/Lideranças	Implementar controles e mitigar riscos	Reuniões mensais de status	Planos de ação, indicadores, RCAs
Colaboradores/Voluntários	Cumprir políticas, reportar suspeitas	Treinamentos obrigatórios	Termos de ciência, certificados EAD
Fornecedores/Parceiros	Atender cláusulas de integridade	Due diligence, contrato, monitoramento	Cadastros, checklists, aditivos

Parte interessada	Responsabilidades mínimas	Interações previstas	Documentos/Registros esperados
Órgãos públicos	Cumprir normas e deveres legais	Convênios, prestações de contas	Ofícios, comprovações, relatórios

1.3 Princípios Éticos e Cultura de Integridade

O Instituto Sustenta pauta-se por: **legalidade, integridade, transparência, imparcialidade, responsabilização, confidencialidade, prevenção, proporcionalidade, não retaliação e melhoria contínua**. A Alta Direção lidera pelo exemplo, assegurando independência e autoridade das funções de compliance e antissuborno e fomentando a cultura de integridade (“**tom do topo**”). Esses pilares estão alinhados às diretrizes das normas ISO 37001 e ISO 37301. (ISO)

Boas práticas culturais:

- Mensagens periódicas da Alta Direção reforçando “tolerância zero ao suborno”;
- Campanhas internas (pílulas de compliance, quizzes e cases reais);
- Inclusão de objetivos de integridade nas metas gerenciais (sem incentivos que estimulem risco indevido).

1.4 Base Normativa e Legal

Normas técnicas de referência:

- **ISO 37001:2025 – Anti-bribery management systems — Requirements with guidance for use** (2ª edição). (ISO)
- **ISO 37301:2021 — Compliance management systems — Requirements with guidance for use + Amendment 1:2024 (Climate action changes).** (ISO)

Marco regulatório brasileiro principal:

- **Lei nº 12.846/2013 (Lei Anticorrupção)**; **Decreto nº 11.129/2022** (regulamenta e substitui o Decreto nº 8.420/2015). (Planalto)

Outras referências frequentes: LGPD (Lei nº 13.709/2018), Lei de Lavagem de Dinheiro (Lei nº 9.613/1998), Lei de Improbidade Administrativa (Lei nº 8.429/1992, redações vigentes). (Usadas de forma complementar e quando aplicável.)

Quadro 2 — Mapa de correspondência (exemplos)

Tema	ISO 37001	ISO 37301	Marco legal BR
Política antissuborno	5.2; 8.3	5.2	Lei 12.846/2013 (arts. 7º e 16), Dec. 11.129/2022
Due diligence de terceiros	8.2; 8.3	8.2	Dec. 11.129/2022 (critérios de integridade)

Tema	ISO 37001	ISO 37301	Marco legal BR
Canal de denúncia	8.9	7.4; 8.3	Dec. 11.129/2022 (mecanismos de integridade)
Treinamento	7.3	7.3	Programas de integridade exigidos em convênios/editalícios

Nota: A matriz de conformidade completa será apresentada no Cap. 12.

1.5 Missão, Visão e Valores de Compliance e Anticorrupção

Missão: "Promover uma cultura de integridade que previna, detecte e responda a riscos de compliance e suborno, preservando a confiança da sociedade e a sustentabilidade dos projetos."
Visão: "Ser referência no terceiro setor pela maturidade e efetividade do SGC/SGAS, com melhoria contínua e governança transparente, alinhada à ISO 37301 e ISO 37001." (ISO)
Valores: Integridade, Transparência, Responsabilidade, Equidade, Imparcialidade, Confidencialidade, Coragem para denunciar, Proporcionalidade, Melhoria contínua.

1.6 Estrutura Documental (Políticas, Normas, Procedimentos e Registros)

A informação documentada é controlada no repositório oficial (ECM). Apenas a versão vigente neste repositório é válida.

Quadro 3 — Hierarquia e controle de documentos

Nível	Documento	Conteúdo essencial	Responsável	Aprovação	Revisão
N1	**MA-003 – Manual de Compliance e Anticorrupção**	Diretrizes e requisitos do SGC/SGAS	Compliance	Conselho/Diretoria	Anual
N2	**Políticas** (Código de Conduta; Antissuborno; Conflitos de Interesse; Brindes/Doações; Rel. com o Setor Público; Due Diligence de Terceiros; Canal de Denúncias; Investigações; Proteção ao	Regras corporativas	Compliance + Jurídico	Diretoria	Anual

Nível	Documento	Conteúdo essencial	Responsável	Aprovação	Revisão
	Denunciante; Privacidade/LGPD)				
N3	**Procedimentos/POPs**	Como executar controles	Áreas/processos	Gestor da área	12–24 meses
N4	**Formulários/Modelos**	Checklists, DD, declarações, relatórios, fluxos	Donos de processo	Compliance	Sob demanda
N5	**Registros/Evidências**	Logs, atas, relatórios, certificados, contratos	Donos de processo	N/A	Conforme tabela abaixo

Registros e evidências (mínimo recomendado):

- **Treinamentos:** listas de presença, certificados EAD, trilhas concluídas, datas e notas;
- **Canal de Denúncias:** protocolos, triagem, investigações, pareceres e medidas;
- **Due Diligence:** dossiês por risco (KYE/KYS/KYP), validações e aprovações;
- **Compras/Contratos:** TRs, cotações, justificativas, comparativos e cláusulas de integridade;
- **Governança:** atas do Conselho/Diretoria, análises críticas, planos de ação e indicadores;
- **Comunicação:** comunicados, campanhas e evidências de divulgação;
- **Auditorias:** plano anual, relatórios, não conformidades e ações corretivas.

1.7 Gestão do Conhecimento, Comunicação e Treinamento

Treinamento obrigatório: integração anual via **EAD**, com **assinatura digital** de termos de ciência e adesão às políticas. Programas específicos por função e risco (ex.: compras, captação de recursos, relacionamento com o setor público). (Requisito conectado às seções 7.2/7.3 das normas.) (ISO)

Comunicação:

- Interna: intranet/ECM, e-mail institucional, reuniões de área, sinalizações em ambientes e pílulas de integridade;

- Externa: site institucional, cláusulas contratuais, editais/termos de fomento e comunicação com autoridades.

Canais oficiais:

- **Canal de Denúncias** (24/7, com opção de anonimato);
- **Canal de Dúvidas** (e-mail institucional);
- **Agenda de Compliance** (calendário de treinamento, auditorias e prazos regulatórios).

Indicadores Sugeridos (orientativos)

Indicador	Definição	Meta inicial	Periodicidade	Observações
Cobertura de treinamento	% de pessoas obrigadas que concluíram EAD no período	≥ 95%	Trimestral	Segmentar por área/risco
Tempo de apuração	Mediana de dias entre recebimento e conclusão da investigação	≤ 45 dias	Mensal	Excluir casos complexos justificados
Efetividade do canal	% de denúncias com indícios confirmados	10–30%	Trimestral	Acompanhado com cautela
Due diligence no prazo	% de terceiros de risco com DD concluída antes da contratação	100%	Mensal	Classificar por faixa de risco
Conflitos de interesse	% de declarações anuais entregues	≥ 98%	Anual	Alta/baixa materialidade
Ações corretivas eficazes	% de NCs com eficácia verificada	≥ 90%	Trimestral	Pós-auditoria interna
Comunicação ativa	Nº de campanhas/mensagens da liderança por ano	≥ 6	Anual	Evidenciar “tom do topo”

Nota: metas devem ser calibradas após a **primeira linha de base** (primeiro ciclo anual).

Periodicidades (mínimos)

- **Treinamento EAD obrigatório:** anual (com reciclagens sob demanda);
- **Auditoria interna do SGC/SGAS:** anual;
- **Análise crítica pela direção:** ao menos anual;
- **Revisão de políticas-chave:** anual ou quando houver mudança normativa relevante;

- **Revisão de matriz de riscos:** anual e sempre que houver alteração significativa de contexto.

Exemplos de Controles (introdução — detalhamento operacional no Cap. 6)

- **Brindes/Hospitalidades:** limites monetários, registro obrigatório e aprovação prévia por risco;
- **Doações/Patrocínios:** critérios, due diligence da entidade beneficiária e rastreabilidade;
- **Relacionamento com o setor público:** agenda transparente, registro de reuniões, vedação a "pagamentos de facilitação";
- **Contratações:** segregação de funções, cotações comparáveis, cláusulas anticorrupção e sanções contratuais.

Responsabilidades de Alto Nível (resumo)

Função	Responsabilidades
Conselho/Alta Direção	Patrocinar o SGC/SGAS, aprovar políticas, prover recursos, revisar desempenho
Compliance/Integridade	Manter o manual, orientar áreas, monitorar riscos, reportar à Alta Direção
Gestores de Processo	Implementar controles e manter registros/evidências
Todos os Colaboradores/Voluntários	Cumprir regras, concluir treinamentos, reportar suspeitas
Terceiros (fornecedores/parceiros)	Atender cláusulas contratuais de integridade e submeter-se à DD

Conexão com Normas/Leyes

Este capítulo atende, de forma introdutória, às seções **4–7** das ISO 37001/37301 (contexto, liderança, planejamento e apoio), preparando o detalhamento nos capítulos seguintes, e ancora o programa nos dispositivos da Lei 12.846/2013 e do Decreto 11.129/2022. (ISO)

2. Contexto da Organização

2.1 Entendimento da organização e do seu contexto (interno e externo)

Objetivo: identificar fatores internos e externos que influenciam a capacidade do Instituto Sustenta de alcançar os objetivos do SGC/SGAS, inclusive exposição a riscos de compliance e suborno.

2.1.1 Fatores internos — exemplos (checklist)

- **Governança e estrutura**: Estatuto/Regimento; Conselho/Comitês; níveis decisórios; segregação de funções.
- **Modelo operacional**: portfólio de projetos socioambientais; captação de recursos; compras e contratações; execução e prestação de contas.
- **Cultura e pessoas**: maturidade ética; rotatividade; voluntariado; treinamentos; incentivos.
- **Processos e sistemas**: mapeamento (processo-a-processo), matrizes de responsabilidade (RACI), ERP/ECM, canal de denúncias.
- **Recursos**: orçamento; recursos tecnológicos; competências críticas (compras, jurídico, compliance, projetos).
- **Controles existentes**: políticas vigentes; cláusulas contratuais; trilhas EAD; auditorias; due diligence de terceiros.

2.1.2 Fatores externos — exemplos (checklist)

- **Regulação e políticas públicas**: leis e decretos aplicáveis; requisitos de convênios/termos de fomento; exigências de financiadores.
- **Partes interessadas externas**: órgãos de controle, ministérios, tribunais de contas, doadores, patrocinadores, beneficiários, imprensa.
- **Ambiente socioeconômico**: dependência de editais; variações orçamentárias públicas; regionalidade dos projetos.
- **Risco de integridade por área geográfica**: índice de percepção de corrupção/local, histórico de fraudes setoriais, relações com agentes públicos.
- **Mercado de fornecedores**: concentração, histórico de sanções, dependência de consultores ou "captadores".

2.1.3 Ferramental recomendado

A) Análise PESTLE (Político, Econômico, Social, Tecnológico, Legal, Ambiental) — revisar 1x/ano.
B) SWOT de Integridade — forças, fraquezas, oportunidades, ameaças ligadas ao compliance/antissuborno.
C) Mapa de Processos (nível macro e nível operacional) — identificar pontos de controle e riscos.
D) Heatmap de Riscos de Integridade — consolidar riscos por processo, projeto e terceiro.

Modelo — PESTLE resumida (exemplo):

Dimensão	Observações ligadas à integridade	Controles/Respostas preliminares
Político	Relação com órgãos públicos em convênios	Registro de interações; agenda de transparência
Econômico	Dependência de recursos de edital	Due diligence de financiadores; segregação nas prestações
Social	Voluntariado e parceiros locais	Termos de conduta; treinamento simplificado
Tecnológico	Sistemas de compras e ECM	Perfis de acesso; logs; reconciliações
Legal	Regras de integridade em fomento	Cláusulas anticorrupção; matriz de conformidade legal
Ambiental	Projetos socioambientais	Critérios de doações/patrocínios; rastreabilidade

Registros/Evidências sugeridos: atas da análise de contexto, versões aprovadas da PESTLE/SWOT, mapa de processos (PDF/visio), heatmap anual, plano de ação decorrente.

Periodicidade: revisão **anual** ou quando houver mudanças relevantes (novo programa, marco legal, expansão geográfica).

Indicadores (orientativos):

- % de processos críticos mapeados com riscos e controles identificados (meta ≥ 90%).
- % de ações do plano de contexto concluídas no prazo (meta ≥ 85%).

2.2 Partes interessadas e suas necessidades/expectativas

Objetivo: compreender requisitos de quem pode afetar ou ser afetado pelo SGC/SGAS.

2.2.1 Identificação e requisitos (exemplo orientativo)

Parte interessada	Necessidades/Expectativas	Requisitos típicos de integridade	Resposta/Controle
Conselho/Alta Direção	Transparência, conformidade, reputação	Relatórios claros e periódicos	Análise crítica anual; KPIs; plano de integridade
Doadores/Patrocinadores	Uso correto de recursos, rastreabilidade	Prestação de contas, due diligence	Fluxo de PC; segregação; auditoria

Parte interessada	Necessidades/Expectativas	Requisitos típicos de integridade	Resposta/Controle
Órgãos de Controle	Conformidade legal, controles internos	Políticas e evidências	Matriz legal; auditorias; canal 24/7
Beneficiários	Ética, não discriminação	Código de Conduta	Termos de conduta; canais de queixa
Fornecedores/Consultores	Regras claras, pagamento em dia	Cláusulas anticorrupção, DD	Política de terceiros; lista de sanções
Colaboradores/Voluntários	Ambiente íntegro, proteção	Não retaliação; treinamentos	Canal de denúncia; EAD anual; sanções

2.2.2 Matriz de Partes Interessadas e Criticidade (exemplo)

Parte	Influência	Exposição a risco de suborno	Criticidade	Dono do relacionamento
Órgãos públicos	Alta	Alta	Muito alta	Diretoria/Relacionamento Institucional
Fornecedores críticos	Média	Alta	Alta	Suprimentos/Compliance
Doadores institucionais	Alta	Média	Alta	Captação/Financeiro
Beneficiários	Média	Baixa	Média	Coordenação de Projetos

Registros/Evidências: cadastro de partes interessadas (planilha/ECM), requisitos mapeados, evidências de comunicação (circulares, site, editais), feedbacks e pesquisas de satisfação.

Periodicidade: revisão **anual** e sempre que houver novo stakeholder estratégico.

Indicadores:

- % de requisitos de partes interessadas incorporados a políticas/processos (meta ≥ 80%).
- Tempo médio de resposta a manifestações de stakeholders (meta ≤ 10 dias úteis).

2.3 Escopo do SGC/SGAS

Objetivo: formalizar **onde** e **como** o SGC/SGAS se aplica no Instituto Sustenta.

2.3.1 Declaração de escopo (modelo para aprovação)

"O Sistema de Gestão de Compliance e Antissuborno do Instituto Sustenta aplica-se a todos os processos, pessoas (colaboradores, conselheiros, voluntários), unidades, projetos e relações com terceiros (fornecedores, parceiros, consultores, doadores e beneficiários), abrangendo captação de recursos, planejamento, execução, compras/contratações, gestão financeira, monitoramento, comunicação e prestação de contas, em todo território de atuação do Instituto."

2.3.2 Exclusões (se houver)

- Processos **terceirizados integralmente**: permanecem sob controle do Instituto por meio de cláusulas, SLAs e auditorias de terceiros.
- Atividades **fora de jurisdições** não atendidas pelo Instituto: devem ser explicitadas.

2.3.3 Interfaces relevantes

- **SGC ↔ SGAS:** políticas integradas, matriz de riscos única com vistas diferentes (compliance/antissuborno).
- **SGC/SGAS ↔ LGPD:** privacidade nas denúncias/investigações e nos cadastros de terceiros.
- **SGC/SGAS ↔ Gestão de Projetos:** gates de integridade (captação, contratação, execução, prestação de contas).

Registros/Evidências: declaração de escopo aprovada pela Alta Direção; diagrama de cobertura; lista de exclusões e justificativas; registro de interfaces.

Indicadores:

- % de contratos/projetos cobertos por políticas de integridade (meta = 100%).
- Nº de exceções autorizadas e justificadas por período (tendência decrescente).

2.4 Integração do SGAS ao SGC e a outros sistemas

Objetivo: garantir coerência, evitar sobreposição e lacunas de controle.

2.4.1 Mapa de integração (exemplo)

Sistema/Disciplina	Pontos de contato com SGC/SGAS	Benefícios esperados
Governança/Conselho	Aprovação de políticas; análise crítica; gestão de riscos	Alinhamento estratégico e "tom do topo"

Sistema/Disciplina	Pontos de contato com SGC/SGAS	Benefícios esperados
Gestão de Riscos	Matriz única; critérios; apetite e tolerância	Priorização e foco em riscos materiais
Compras e Contratos	Due diligence; cláusulas; segregação	Redução de riscos com terceiros
Financeiro/Contábil	Pagamentos; registros; reconciliações	Rastreabilidade e prevenção a fraudes
Projetos/Operações	Gates de integridade por fase	Conformidade em campo
Jurídico	Sanções; investigações; suporte normativo	Segurança jurídica
TI/Segurança da Informação	ECM; trilhas; proteção de dados	Evidências robustas e LGPD
RH	Treinamentos; consequências; onboarding	Cultura e disciplina

2.4.2 Papéis e responsabilidades (RACI de alto nível)

Atividade	Conselho	Diretoria	Compliance	Dono do Processo	Jurídico
Aprovar políticas	A	R	C	C	C
Avaliar riscos	C	A	R	R	C
Due diligence	C	C	R	R	C
Treinamentos	C	A	R	C	C
Auditorias internas	C	A	R	C	C
Investigação	C	A	R	C	R
R = responsável; A = aprovador; C = consultado.					

Registros/Evidências: matriz RACI aprovada; organograma; termos de referência das funções de Compliance/Antissuborno; trilhas de auditoria de sistemas; evidências de integração (atas, fluxos, KPIs cruzados).

Periodicidade: revisão **anual** ou quando houver mudança estrutural.

Indicadores:

- % de processos com RACI publicado no ECM (meta ≥ 95%).
- Nº de retrabalhos por conflito de papéis (meta: tendência de queda).

2.5 Obrigações de compliance (catálogo e matriz)

Objetivo: identificar, manter e atualizar as **obrigações de compliance** aplicáveis (legais, regulatórias, contratuais e voluntárias).

2.5.1 Catálogo de obrigações — modelo

Fonte	Descrição/escopo	Responsável por manter	Evidência de atendimento	Periodicidade de verificação
Legislação anticorrupção	Proibições, sanções, programas de integridade	Jurídico/Compliance	Políticas; treinamentos; canal	Semestral
Editais/Convênios	Cláusulas específicas de integridade	Projetos/Jurídico	Contratos; prestações aprovadas	Por contrato
LGPD	Tratamento de dados em denúncias/DD	TI/Jurídico/Compliance	Avisos; controles de acesso; DPA	Semestral
Padrões ISO	Requisitos SGC/SGAS	Compliance	Matriz de conformidade	Anual

Registros/Evidências: catálogo no ECM (com versão e histórico), matrizes de rastreabilidade (requisito → processo → controle → evidência), alertas de atualização legal.

Indicadores:

- % de obrigações mapeadas com dono e evidência (meta ≥ 95%).
- Nº de descumprimentos detectados (meta = 0; classificar por gravidade).

2.6 Avaliação de riscos de compliance e de suborno (visão geral)

(Detalhamento metodológico completo no Cap. 4 – Planejamento; aqui, a conexão com o contexto.)

2.6.1 Critérios e taxonomias (resumo)

- **Fontes de risco**: interação com agentes públicos, compras, doações/patrocínios, consultorias, captação, viagens/hospitalidades, caixa miúdo/cartões, prestações de contas.

- **Consequências**: legais, financeiras, reputacionais, operacionais.
- **Controles existentes**: políticas, segregações, aprovações, trilhas, contratos.
- **Avaliação**: probabilidade x impacto (escalas qualitativas/quantitativas), com **critérios documentados** e validados.

2.6.2 Exemplo de riscos e controles vinculados ao contexto

Processo/Contexto	Risco de integridade	Controles previstos	Evidências
Captação de recursos	Oferta indevida a agente público	Política antissuborno; registro de interações; 4-olhos	Agenda, atas, logs
Compras locais em campo	Favorecimento/colusão	Cotações comparáveis; segregação; sanções contratuais	Mapa de cotações, contratos
Doações e patrocínios	Desvio de finalidade	Due diligence; rastreabilidade; aprovação	Dossiê DD; relatórios
Prestação de contas	Inserção de despesas impróprias	Checklist; dupla conferência; auditoria	PC aprovada; trilhas ERP

Periodicidade: reavaliação de riscos **anual** e a cada mudança relevante (novo projeto/região, novo parceiro/fornecedor crítico, mudança legal).

Indicadores:

- % de riscos críticos com plano de tratamento ativo (meta = 100%).
- Lead time médio do ciclo de avaliação de riscos (meta ≤ 60 dias).

2.7 Comunicação do contexto e conscientização

Objetivo: assegurar que as pessoas **conheçam** o contexto e saibam **como** isso se traduz em controles.

Boas práticas:

- **One-pager** anual de contexto e riscos principais (linguagem simples), publicado no ECM e apresentado em reuniões de equipes.
- **Pílulas EAD** com exemplos do dia a dia (brindes, conflitos, interação com agentes públicos, compras).
- **Sessões de onboarding** para novos colaboradores/voluntários (inclui assinatura digital de termos).

Registros/Evidências: materiais de comunicação, listas de presença/certificados EAD, prints do ECM, mensagens da Alta Direção.

Indicadores:

- % de colaboradores que afirmam “entender os riscos do seu processo” (pesquisa anual; meta ≥ 85%).
- Nº de dúvidas recebidas e respondidas por trimestre (tendência: manter saudável; não decrescente à força).

3. Liderança e Governança

3.1 Compromisso e liderança da Alta Direção e do Conselho

Objetivo: assegurar que o Conselho/Alta Direção estabeleça o **tom do topo**, integre a integridade à estratégia e disponibilize **recursos, autoridade e independência** para o SGC/SGAS.

Diretrizes:

- A Alta Direção declara **tolerância zero** a suborno e violações de compliance, comunica expectativas e dá exemplo.
- Integra o SGC/SGAS aos objetivos estratégicos, orçamento e gestão de riscos corporativos.
- Garante que a função de Compliance/Antissuborno tenha **acesso direto** e **sem barreiras** ao Conselho/Comitê de Auditoria/Integridade.
- Assegura recursos **humanos, financeiros e tecnológicos** adequados e proporcionais ao risco.

Registros/Evidências:

- Declaração formal de compromisso assinada; comunicados periódicos da liderança; atas de reuniões com pauta de integridade; alocação orçamentária; organograma aprovado; plano anual de compliance.

Periodicidade mínima:

- Mensagens de liderança: **semestral** (mín. 2/ano).
- Revisão de recursos do SGC/SGAS: **anual** (no ciclo orçamentário).

3.2 Política de Compliance e Antissuborno

Objetivo: estabelecer princípios, responsabilidades e obrigações aplicáveis a todas as partes interessadas.

Conteúdo mínimo da política:

1. **Propósito e escopo** (toda a organização e terceiros relevantes).
2. **Princípios** (legalidade, imparcialidade, transparência, não retaliação, melhoria contínua).
3. **Proibições** (suborno ativo/passivo, pagamentos de facilitação, fraudes, obstrução de investigações).
4. **Temas sensíveis** (brindes/hospitalidades, doações/patrocínios, conflitos de interesse, relacionamento com o setor público).
5. **Deveres de reporte** e **proteção ao denunciante** (anonimato e confidencialidade quando cabível).
6. **Incentivos/Consequências** (critérios de reconhecimento e sanções disciplinares proporcionais).
7. **Governança** (papéis, canais, aprovações, revisão).
8. **Treinamento e aceitação** (assinatura digital).

Registros/Evidências: versão publicada no ECM; histórico de revisões; comprovação de ciência/aceite (assinaturas digitais); trilha de comunicação.

Periodicidade de revisão: anual ou por mudança normativa/relevante.

3.3 Papéis, responsabilidades e autoridades

Estrutura recomendada:

- **Conselho/Comitê de Integridade**: supervisiona o SGC/SGAS; aprova políticas e plano anual; recebe reports do Compliance; decide sobre casos sensíveis e conflitos de interesse da Alta Direção.
- **Diretoria Executiva**: assegura recursos; integra o SGC/SGAS aos processos; responde por implementação e desempenho.
- **Função de Compliance e Antissuborno** (pode ser uma área ou designação formal): mantém o MA-003; orienta áreas; monitora riscos; conduz treinamentos; coordena canal de denúncias e investigações (em conjunto com Jurídico/Auditoria quando aplicável); reporta ao Conselho/Comitê com **independência**.
- **Gestores de Processo**: implementam controles, mantêm registros, executam due diligence de terceiros conforme diretrizes.
- **Todos(as)**: cumprir políticas, participar de treinamentos, **reportar** suspeitas de boa-fé.

Requisitos de independência e autoridade (mínimos):

- Carta/Termo de Nomeação do(a) Responsável por Compliance com direito a **acesso à alta gestão** e autonomia técnica.

- Proibição de **interferência indevida** em apurações e relatórios; salvaguardas contra conflito de interesses (ex.: Compliance não acumula funções que possam auditar a si próprio nos temas críticos).

Quadro 3.3 — RACI de alto nível

Atividade	Conselho	Diretoria	Compliance	Jurídico	Dono do Processo	Auditoria Interna/Externa
Aprovar políticas	A	C	C	C	C	I
Atualizar políticas	I	C	R	C	C	I
Avaliação de riscos	C	A	R	C	R	I
Treinamentos	I	A	R	C	C	I
Canal de denúncias	C	I	R	C	I	I
Investigações	C	A	R	R	C	C
Due diligence de terceiros	I	A	R (método)	C	R (execução)	I
Relato ao Conselho	A (recebe)	I	R	C	I	I

A = aprovador, R = responsável, C = consultado, I = informado.

Registros/Evidências: organograma; cartas de nomeação; RACI publicado no ECM; atas do Comitê de Integridade; plano anual de compliance; relatórios trimestrais ao Conselho.

Periodicidade: reuniões do Comitê/Conselho sobre integridade **trimestrais** (mínimo).

3.4 Tom de topo, cultura e clima de integridade

Objetivo: fortalecer comportamentos esperados e desestimular condutas de risco.

Práticas recomendadas:

- **Mensagens da liderança** em marcos do ano (início do ciclo orçamentário, Dia Internacional Anticorrupção, lançamento de projetos).
- Inclusão de **metas de integridade** nas avaliações de liderança (sem incentivos que estimulem risco indevido).

- **Campanhas e pílulas** contínuas (casos práticos, quizzes, vídeos curtos).
- **Clima de segurança psicológica**: estímulo a dúvidas, feedbacks e reporte de boa-fé.

Registros/Evidências: campanhas, comunicados, materiais EAD, registros de town halls; pesquisa de clima de integridade.

Periodicidade: campanhas **contínuas**; pesquisa de clima **anual**.

3.5 Recursos e competências

Objetivo: assegurar pessoas capacitadas e ferramentas adequadas.

Requisitos mínimos:

- **Plano de recursos** do SGC/SGAS (pessoas, orçamento, tecnologia: canal 24/7, ECM, ferramentas de DD, trilhas de auditoria).
- **Matriz de competências** por função crítica (Compliance, Compras, Captação, Projetos, Financeiro).
- **Programa de capacitação** com trilhas por risco (ex.: relacionamento com setor público, doações/patrocínios, compras).

Registros/Evidências: plano orçamentário; descrição de cargos; matriz de competências; grade anual de treinamentos; comprovantes de contratação de ferramentas.

Periodicidade: revisão **anual**; atualização ad hoc por mudanças de risco.

3.6 Incentivos e consequências (disciplinares e reconhecimentos)

Objetivo: alinhar comportamentos ao padrão ético esperado.

Diretrizes:

- **Reconhecimentos**: valorização pública, métricas de integridade nas metas, prêmios por boas práticas.
- **Consequências**: medidas proporcionais, graduadas e consistentes (advertência, suspensão de acesso, desligamento, comunicação a autoridades, rescisão contratual de terceiros).
- **Imparcialidade e devido processo** nas apurações; **não retaliação** a denunciantes e testemunhas de boa-fé.

Registros/Evidências: política de consequências; registros de comitês disciplinares; rastreabilidade de medidas; cláusulas contratuais de sanção a terceiros.

Periodicidade: revisão **anual**; aplicação sempre que houver violação.

3.7 Comunicação interna e externa

Objetivo: garantir entendimento e transparência.

Canais mínimos:

- **Interno**: intranet/ECM, e-mail, reuniões de equipe, dashboards de indicadores.
- **Externo**: site institucional (seção Integridade), contratos/edital com cláusulas padrão, relatório anual de integridade (quando aplicável).

Conteúdo recorrente:

- Política vigente; como usar o canal de denúncias; exemplos práticos; estatísticas consolidadas (sem dados pessoais); aprendizados de auditorias.

Registros/Evidências: prints de páginas, newsletters, relatórios públicos, FAQs.

Periodicidade: calendário **semestral** de comunicação; atualização imediata quando houver mudança relevante.

3.8 Mecanismos de supervisão e reporte

Objetivo: garantir visibilidade do desempenho e tomada de decisão.

Relatórios mínimos:

- **Mensal** (para Diretoria): status de treinamentos, denúncias recebidas x tratadas, due diligence de terceiros por risco, ações corretivas.
- **Trimestral** (para Conselho/Comitê): panorama de riscos, indicadores-chave, casos relevantes, recursos, temas críticos.
- **Anual**: relatório de gestão do SGC/SGAS e **análise crítica da direção** (insumos para plano do próximo ciclo).

Registros/Evidências: relatórios consolidados, atas de análise crítica, planos de ação e follow-up; dashboards exportados.

Periodicidade: conforme acima; **análise crítica anual** obrigatória.

3.9 Conflitos de interesse e segregação de funções (governança aplicada)

Diretrizes:

- **Declaração anual** de conflito por todos (inclui Conselhos/Diretoria, colaboradores, voluntários críticos e terceiros-chave).

- **Gestão de impedimentos**: registros de abstenção em decisões; substituições temporárias; rodízio em funções críticas (compras/contratos, prestação de contas).
- **Segregação mínima**: quem **solicita** não **aprova**; quem **aprova** não **paga**; quem **paga** não **concilia**; exceções justificadas e autorizadas.

Registros/Evidências: formulários de conflito; atas com registro de impedimentos; matriz de segregação; log de exceções.

Periodicidade: coleta **anual** e na **admissão**; revisão a cada mudança de função.

3.10 Due diligence de alta gestão e terceiros estratégicos (governança)

Diretrizes:

- **Alta gestão e conselheiros**: verificação de integridade na entrada e **revalidação** periódica.
- **Terceiros estratégicos** (consultores de relacionamento, representantes, parceiros de captação, beneficiários relevantes): **due diligence reforçada** antes da contratação/apoio e monitoramento durante o vínculo.

Registros/Evidências: dossiês de DD; pareceres; decisões de contratação; cláusulas contratuais anticorrupção; reavaliações.

Periodicidade: pré-contratação e **anual** para revalidação; por evento se houver alerta.

3.11 Integração com auditoria interna/externa e órgãos de controle

Diretrizes:

- **Plano anual de auditoria interna** abrangendo riscos de integridade e testes de controles; coordenação com Compliance para evitar sobreposição/lacunas.
- **Cooperação** com auditorias externas e órgãos de controle (fornecimento de informações, preservando confidencialidade e LGPD).
- **Follow-up** de recomendações até a comprovação de eficácia.

Registros/Evidências: plano de auditoria; relatórios; matriz de achados; evidências de ações corretivas; comunicações com órgãos de controle.

Periodicidade: auditoria interna **anual** (mínimo) e conforme escopo de financiadores/contratos.

Indicadores sugeridos (orientativos)

Código	Indicador	Definição	Meta inicial	Periodicidade
GOV-01	Comunicação da liderança	Nº de mensagens/town halls de integridade	≥ 6/ano	Anual
GOV-02	Cobertura de treinamento	% público-alvo com EAD concluído	≥ 95%	Mensal
GOV-03	Recursos do SGC/SGAS	% execução do orçamento vs. plano	≥ 90%	Trimestral
GOV-04	Reuniões de supervisão	% de reuniões do Comitê realizadas vs. previstas	100%	Trimestral
GOV-05	Independência em investigações	% de casos sem conflito/ingerência	100%	Trimestral
GOV-06	Gestão de conflitos de interesse	% de declarações anuais entregues	≥ 98%	Anual
GOV-07	Ações da análise crítica	% concluídas no prazo	≥ 85%	Semestral

Nota: metas deverão ser recalibradas após o **primeiro ciclo anual** (linha de base).

Boas práticas adicionais

- **Carta de Mandato** do(a) Responsável por Compliance, publicada no ECM.
- **Relatório público de integridade** (síntese anual) para transparência com a sociedade.
- **Programa de reconhecimento** a equipes com boas práticas de integridade.
- **Checklist de governança** para novos projetos/convênios com "gates" de integridade.

4. Planejamento

4.1 Ações para abordar riscos e oportunidades

Objetivo: definir como o Instituto Sustenta identifica, avalia e trata **riscos** de compliance e de suborno, bem como **oportunidades** de melhoria do SGC/SGAS.

Diretrizes gerais:

- Utilizar abordagem **baseada em risco**, proporcional ao porte e exposição do Instituto.
- Considerar riscos **por processo, projeto, região e terceiro** (fornecedores, parceiros, consultores, doadores, beneficiários críticos).

- Documentar **apetite** e **tolerância** a risco (ver 4.2.2) e traduzir em **controles**, **metas** e **planos** (ver 4.3).
- Tratar também **oportunidades** (ex.: digitalização de due diligence, contratos padrão, centralização de compras).

Registros/Evidências: plano anual de riscos; atas das oficinas de risco; lista de oportunidades priorizadas; plano de ação com prazos e responsáveis.

Periodicidade: ciclo **anual** + reavaliação por evento (ex.: novo convênio, nova região, mudança legal relevante).

4.2 Avaliação de riscos de compliance e riscos de suborno

4.2.1 Metodologia (passo a passo)

1. **Identificação** de riscos por fonte/área: entrevistas, oficinas, análise de dados (denúncias, auditorias), benchmark setorial.
2. **Classificação** por categoria: suborno, fraude, conflito de interesse, licitações/compras, doações e patrocínios, relacionamento com setor público, prestação de contas, dados pessoais (LGPD), lavagem de dinheiro, etc.
3. **Avaliação** (probabilidade x impacto) com escalas padronizadas e critérios objetivos.
4. **Mapeamento de controles** existentes e avaliação de eficácia.
5. **Cálculo da exposição residual** e **priorização** (heatmap).
6. **Plano de tratamento** (evitar, reduzir, compartilhar/transferir, aceitar com monitoramento).
7. **Monitoramento** via indicadores (KPIs/KRIs), auditoria e análise crítica.

4.2.2 Apetite e tolerância a risco (modelo)

- **Apetite**: nível de risco **residual** que a Alta Direção aceita **conscientemente** para perseguir objetivos.
- **Declaração orientativa** (exemplo para aprovação):

"O Instituto Sustenta possui **apetite muito baixo** para riscos de suborno e fraude, **baixo** para riscos de conformidade regulatória, e **moderado** para riscos operacionais não relacionados à integridade, desde que haja controles compensatórios e supervisão adequada."

- **Tolerância**: limites mensuráveis (thresholds). Exemplos:
  - 0 (zero) casos de **pagamentos de facilitação**;
  - ≥ 95% de **due diligence** concluídas **antes** da contratação de terceiros de risco;

- 100% de **declarações anuais** de conflito de interesse.

4.2.3 Critérios de avaliação (escalas)

Probabilidade (P)

1 = Rara | 2 = Improvável | 3 = Possível | 4 = Provável | 5 = Quase certa

Impacto (I) — considerar financeiro, legal, reputação, operacional, pessoas/beneficiários
1 = Insignificante | 2 = Baixo | 3 = Moderado | 4 = Alto | 5 = Crítico

Cálculo da Nota de Risco (NR): NR = P x I

Faixas sugeridas: 1–5 (Baixo) | 6–12 (Médio) | 15–25 (Alto/Crítico)

4.2.4 Matriz de riscos (modelo consolidado)

Nº	Processo/Contexto	Risco	Causas	Controles existentes	P	I	NR	Nível	Tratamento proposto	Dono	Prazo
01	Captação com setor público	Oferta/promessa indevida (suborno)	Intermediários; metas agressivas	Política antissuborno; registro de agenda; 4-olhos	3	5	**15**	Alto	Evitar + reforçar segregação; treinamento	Dir. Rel. Institucional	90 d
02	Compras locais em campo	Favorecimento/colusão	Concentração de fornecedores	3 cotações; comitê; cláusulas	4	4	**16**	Alto	Sistema de compras; DD reforçada	Suprimentos	120 d
03	Doações a parceiros	Desvio de finalidade	Parceiro sem histórico	DD básica; contrato padrão	3	3	**9**	Médio	Monitorar indicadores; visitas	Projetos	180 d
04	Prestação de contas	Inserção de gastos impróprios	Pressão por prazo	Checklist; dupla conferência	3	4	**12**	Médio	Automação e trilhas ERP	Financeiro	120 d

Evidências: planilhas/relatórios no ECM; heatmap aprovado; plano de tratamento assinado; status mensal de ações.

4.2.5 Due diligence (DD) de terceiros — abordagem baseada em risco

Classificação de risco (exemplo):

- **Baixo**: fornecedor de baixo valor e sem interação com setor público → **DD simplificada** (cadastro, sanções/listas, aceite de Código).
- **Médio**: impacto moderado e/ou interação indireta com setor público → **DD padrão** (documentos societários, beneficiário final, referências).

- **Alto/Crit.**: representantes, consultores, captação, parceiros com acesso a recursos públicos → **DD reforçada** (verificações negativas aprofundadas, integridade financeira, entrevistas, cláusulas reforçadas e auditorias).

Saídas e evidências: dossiê DD por terceiro; parecer de risco; aprovações; cláusulas anticorrupção; plano de monitoramento.

4.2.6 Temas sensíveis (critérios mínimos a definir)

- **Brindes/Hospitalidades**: limites monetários, registro e aprovação prévia acima de limiares; vedação a períodos de licitação/negociação.
- **Doações/Patrocínios**: critérios de elegibilidade; segregação; comprovação de entrega; rastreabilidade.
- **Pagamentos de facilitação**: **proibidos**; respostas e reporte imediato pelo canal.
- **Interação com agentes públicos**: agenda registrada, local institucional, duas pessoas presentes quando possível, atas.
- **Cartão corporativo/caixa miúdo**: políticas de uso, comprovantes, reconciliação.

4.3 Objetivos de compliance e antissuborno e planejamento para atingi-los

4.3.1 Estabelecimento de objetivos (modelo SMART)

Código	Objetivo	Métrica	Meta	Prazo	Responsável
OBJ-01	Elevar a eficácia do canal de denúncias	% de casos com indícios confirmados	10–30%	12 meses	Compliance
OBJ-02	Ampliar cobertura de treinamento	% do público-alvo com EAD concluído	≥ 95%	12 meses	RH/Compliance
OBJ-03	Fortalecer DD de terceiros críticos	% de DD concluída antes da contratação	100%	6 meses	Suprimentos/Compliance
OBJ-04	Reduzir retrabalho em PC	Nº de ajustes pós-auditoria	−30%	12 meses	Financeiro/Projetos

4.3.2 Plano para atingir objetivos (exemplo)

- **Recursos**: orçamento para ferramenta de DD e canal 24/7; horas de treinamento; apoio jurídico.

- **Cronograma**: Gantt/roadmap com marcos trimestrais.
- **Responsáveis**: RACI por objetivo.
- **Indicadores de processo** (leading) e **resultado** (lagging).
- **Comunicação**: campanha interna e seção dedicada no ECM.

Evidências: plano aprovado; cronograma; relatórios de progresso; dashboards.

4.4 Planejamento de mudanças

Objetivo: garantir que alterações relevantes (estruturais, legais, tecnológicas, geográficas, de parceiros ou de processos) sejam avaliadas **antes** da implementação, prevenindo riscos de integridade.

Fluxo sugerido:

1. **Proposição da mudança** (área demandante) → formulário padrão no ECM;
2. **Avaliação de impacto** (Compliance + áreas impactadas) → riscos, controles, treinamento, contratos;
3. **Decisão/Aprovação** (Diretoria/Comitê, conforme materialidade);
4. **Implementação controlada** (piloto, comunicação, atualização de documentos);
5. **Pós-implementação** (verificação de eficácia; lições aprendidas).

Evidências: formulários de mudança; parecer de compliance; aprovações; atualização de políticas/POPs; registro de lições aprendidas.

Periodicidade: contínua (por evento); revisão do processo de mudança: **anual**.

4.5 Indicadores (KPIs/KRIs) sugeridos

Código	Indicador	Definição	Meta inicial	Periodicidade
RSK-01	Avaliações de risco realizadas	% de áreas/projetos críticos com avaliação anual	≥ 90%	Trimestral
RSK-02	Planos de tratamento no prazo	% de ações vencidas concluídas	≥ 85%	Mensal
RSK-03	DD concluída antes da contratação	% de terceiros de risco com DD prévia	100%	Mensal
RSK-04	Exceções autorizadas	Nº de exceções a políticas por trimestre	Tendência decrescente	Trimestral

Código	Indicador	Definição	Meta inicial	Periodicidade
RSK-05	Incidentes por tema sensível	Nº de incidentes em brindes, doações, interação com setor público	≤ baseline −20% em 12 meses	Mensal
RSK-06	Efetividade de controles	% de testes de controle "eficazes" em auditoria	≥ 90%	Anual

4.6 Boas práticas

- **Oficinas de risco** multissetoriais, com facilitação de Compliance e registro de decisões.
- **Biblioteca** de riscos e controles por processo, para acelerar revisões.
- **Heatmap dinâmico** em dashboard (integração com ECM/ERP).
- **Contratos padrão** com cláusulas anticorrupção e gatilhos de auditoria/rompimento.
- **Checklists** de integridade por fase do projeto (captação → execução → prestação de contas).
- **Teste de estresse** para cenários críticos (ex.: grande convênio público, operação em nova região).

5. Apoio

5.1 Recursos

Objetivo: assegurar recursos **humanos, financeiros, tecnológicos e infraestruturais** suficientes e proporcionais ao risco.

Diretrizes:

- Orçamento anual específico para SGC/SGAS (canal 24/7, ferramenta de due diligence, ECM, EAD, consultorias e auditorias).
- Pessoal com tempo alocado e competências aderentes (Compliance, Jurídico, Compras, Projetos, Financeiro, TI, RH).
- Independência operacional da função de Compliance e acesso direto à Alta Direção/Conselho (vide Cap. 3).

Registros/Evidências: peça orçamentária aprovada; plano de recursos; contratos de ferramentas; organograma; carta de mandato de Compliance. **Periodicidade:** revisão anual (ciclo orçamentário) e por evento relevante. **Indicadores sugeridos:** % execução do orçamento de compliance; nº de FTEs dedicados x exposição a risco; cobertura de ferramentas (ex.: % de terceiros críticos avaliados no sistema).

5.2 Competência e Treinamento (EAD e presencial)

Objetivo: garantir que as pessoas sejam **competentes** para desempenhar seus papéis com integridade.

Escopo de trilhas:

- **Integração obrigatória anual (EAD)** para todo o público (colaboradores, conselheiros, voluntários), com **assinatura digital** de termo de ciência.
- **Trilhas por risco/função**: compras/contratos; captação/rel. institucional; projetos (execução e prestação de contas); financeiro/contábil; liderança; canal de denúncias e investigações; terceiros críticos (empreiteiros, consultores, representantes).
- **Reciclagens e conteúdos "pílula"** (vídeos curtos, quizzes, estudos de caso).

Matriz de competências (exemplo):

Função	Competências mínimas	Evidências
Compliance	ISO 37001/37301; gestão de riscos; investigação; LGPD	Currículo, certificados, avaliações
Compras/Contratos	Integridade em compras; cláusulas; segregação	Lista de presença; POPs assinados
Projetos	Regras de convênios; controles de gastos; prestação de contas	Certificação EAD; provas
Financeiro	Reconciliações; trilhas; prevenção a fraudes	Relatórios de controle; checklists
Liderança	Tom de topo; consequências; gestão de conflitos	Atas; metas; mensagens oficiais

Registros/Evidências: plano anual de treinamento; catálogos EAD; certificados; lista de presença; trilhas e notas; termos assinados digitalmente.
Periodicidade: anual (obrigatório) + sob demanda.
Indicadores: cobertura de treinamento (%); índice de retenção (pós-teste ≥ 80%); NPS do treinamento.

5.3 Conscientização e Comunicação

Objetivo: assegurar que todos **conheçam** políticas, canais e comportamentos esperados.

Canais e peças mínimas:

- **Interno:** intranet/ECM, e-mail, murais digitais, reuniões de equipe, town halls, newsletter de integridade.

- **Externo:** página de integridade no site, cláusulas padrão em contratos/edital, FAQ sobre o canal de denúncias.

Plano de comunicação (exemplo de calendário):

- **Mensal:** pílulas de integridade (temas sensíveis, "o que fazer se...").
- **Trimestral:** mensagem da Alta Direção; case real (anonimizado) com aprendizados.
- **Anual:** relatório de integridade (indicadores estratégicos e lições aprendidas).

Registros/Evidências: peças, prints, newsletters, pautas e atas, relatórios de campanha.
Indicadores: alcance (% do público exposto); taxa de abertura de e-mails; nº de dúvidas recebidas e respondidas.

5.4 Informação Documentada (Documentos e Registros)

Objetivo: estabelecer controles para criação, atualização, aprovação, acesso, retenção e descarte.

Regras mínimas:

- **Repositório oficial (ECM)**: única fonte de verdade.
- **Controle de versões**: numeração, histórico, aprovadores.
- **Metadados obrigatórios**: dono, vigência, confidencialidade, aplicabilidade.
- **Retenção**: tabela de temporalidade por tipo de registro (denúncias, investigações, contratos, DD, treinamentos, auditorias).
- **Proteção de dados**: alinhamento à LGPD para documentos com dados pessoais (ver 5.10).

Registros/Evidências: política de gestão documental; logs de acesso; backups; trilhas de auditoria.
Indicadores: % de documentos com metadados completos; % de registros arquivados dentro do prazo; nº de acessos não autorizados (meta 0).

5.5 Due Diligence de Terceiros (fornecedores, parceiros, consultores, doadores, beneficiários críticos)

Objetivo: prevenir riscos por meio de **avaliação proporcional ao risco** antes da contratação/apoio e ao longo do relacionamento.

Classificação de risco e escopos (síntese):

- **Baixo** → cadastro + aceite do Código + checagem básica (listas de sanções).

- **Médio** → documentação societária; beneficiário final; referências; cláusulas padrão; checagens negativas.
- **Alto/Crítico** (representantes, consultores de relacionamento, parceiros com acesso a recursos públicos) → **DD reforçada**: verificação reputacional aprofundada, integridade financeira, entrevistas, auditoria prévia, cláusulas saneadoras (rompimento, auditoria, não subcontratação sem consentimento).

Workflow mínimo:

1. **Solicitação e classificação** → 2) **DD** → 3) **Parecer** (apto; apto com mitigação; inapto) → 4) **Contrato com cláusulas** → 5) **Monitoramento** (revalidação anual/por gatilho).

Registros/Evidências: dossiês DD; classificação de risco; pareceres; aprovações; cláusulas; revalidações.
Indicadores: % de terceiros críticos com DD concluída **antes** da contratação (meta 100%); tempo médio de DD; nº de reprovações.

5.6 Canais de Denúncia e Proteção ao Denunciante

Objetivo: disponibilizar canal **independente, acessível 24/7**, com opção de **anonimato**, tratamento imparcial e **não retaliação**.

Requisitos mínimos:

- Múltiplos acessos (web, telefone, e-mail dedicado), linguagem simples e acessível.
- **Política do canal** (escopo, confidencialidade, prazos, garantias, sanções por má-fé).
- **SLA** de triagem e investigação; matriz de materialidade/criticidade.
- **Relato periódico** ao Conselho/Comitê (estatísticas consolidadas).
- Integração com **LGPD** (consentimento quando aplicável; minimização de dados).

Fluxo macro:

Recebimento → Triagem → Plano de investigação → Coleta de evidências → Parecer → Medidas → Feedback ao denunciante (quando possível) → Encerramento e lições aprendidas.

Registros/Evidências: protocolos; relatórios de triagem e investigação; pareceres;

medidas adotadas; comunicação ao denunciante.

Indicadores: tempo médio de apuração (meta ≤ 45 dias); % de casos com indícios confirmados (10–30%); % de feedbacks enviados.

5.7 Incentivos e Consequências (Disciplina/Reconhecimentos)

Objetivo: alinhar condutas ao padrão ético.

Diretrizes:

- **Reconhecimentos**: prêmios anuais, menções, critérios de integridade nas metas.
- **Consequências**: medidas graduadas e proporcionais (advertência a rescisão/representação às autoridades).
- **Devido processo** e **imparcialidade**; registro e rastreabilidade de decisões; **não retaliação**.

Registros/Evidências: política de consequências; atas de comitês; registros disciplinares; justificativas.
Indicadores: % de medidas com documentação completa (meta 100%); reincidência por tema.

5.8 Gestão de Contratos e Cláusulas de Integridade

Objetivo: assegurar **cláusulas anticorrupção** e mecanismos de controle em todos os contratos relevantes.

Cláusulas mínimas:

- Proibição de suborno/pagamentos de facilitação; cumprimento de políticas; **direito de auditoria**; **rompimento por justa causa**; **não subcontratar** sem autorização; **declaração de beneficiário final**; compromisso com o **canal de denúncias**.

Registros/Evidências: minutas padrão; checklists de integridade; parecer jurídico; contratos assinados; logs de auditoria.

Indicadores: % de contratos relevantes com cláusulas padrão (meta 100%); nº de auditorias contratuais realizadas.

5.9 Ferramentas Tecnológicas de Integridade

Objetivo: dar **suporte digital** ao SGC/SGAS.

Mínimo recomendado:

- **ECM** (gestão documental e registros);
- **Canal de denúncias** (SaaS 24/7);
- **Plataforma de EAD** (certificados e trilhas);
- **Ferramenta de due diligence** (listas de sanções, mídia negativa, beneficiário final);
- **Dashboards** (indicadores e heatmap de riscos);

- **Controle de acessos e logs** (TI/Segurança da Informação).

Registros/Evidências: contratos; manuais; relatórios de uso; logs e trilhas; planos de continuidade.
Indicadores: disponibilidade (≥ 99%); tempo de resposta a incidentes TI; nº de integrações ativas (ECM↔ERP↔DD↔EAD).

5.10 Privacidade e Proteção de Dados (interface com LGPD)

Objetivo: tratar dados pessoais **com base legal e segurança**, especialmente em **denúncias, investigações e due diligence**.

Diretrizes:

- **Minimização** de dados; finalidade explícita; prazos de retenção; controles de acesso por perfil.
- **Avaliação de impacto** quando necessário (DPIA/RIPD).
- **Avisos de privacidade** específicos para canal de denúncias e DD.
- **Base legal** adequada (legítimo interesse, obrigação legal, exercício regular de direitos, etc.).
- **Compartilhamento** com autoridades conforme lei e devido processo.

Registros/Evidências: políticas de privacidade; registros de tratamento; contratos com operadores; incidentes e respostas.

Indicadores: nº de incidentes de privacidade (meta 0); % de operações com base legal mapeada (100%).

5.11 Gestão do Conhecimento

Objetivo: reter e difundir conhecimentos críticos de integridade.

Práticas:

- **Base de conhecimento** no ECM (FAQs, lições aprendidas, modelos).
- **Comunidades de prática** (compras, projetos, captação).
- **Pós-projeto**: registro de aprendizados de integridade (o que funcionou/o que ajustar).

Registros/Evidências: páginas do ECM; atas; relatórios de pós-projeto; métricas de uso.
Indicadores: taxa de reutilização de modelos; nº de lições incorporadas em políticas.

Saídas do capítulo (entregáveis mínimos)

1. Plano anual de recursos e capacitação do SGC/SGAS.

2. Trilhas EAD publicadas e termos de ciência com **assinatura digital**.
3. Política e **manual do canal de denúncias** com SLAs e garantias.
4. Minutas padrão com **cláusulas anticorrupção** e checklists de integridade.
5. Processo e ferramenta de **due diligence** com níveis por risco.
6. Regras de **informação documentada** (ECM) e tabela de retenção.
7. Integrações tecnológicas (ECM, EAD, DD, dashboards) ativas.
8. Controles LGPD aplicados a denúncias, investigações e DD.

Indicadores consolidados do capítulo (sugestões)

Código	Indicador	Meta inicial	Periodicidade
SUP-01	Cobertura de treinamento obrigatório (EAD)	≥ 95%	Mensal
SUP-02	DD prévia para terceiros de risco	100%	Mensal
SUP-03	Tempo médio de apuração de denúncias	≤ 45 dias	Mensal
SUP-04	Contratos relevantes com cláusulas padrão	100%	Trimestral
SUP-05	Documentos com metadados completos no ECM	≥ 95%	Trimestral
SUP-06	Disponibilidade das plataformas (canal/EAD/ECM)	≥ 99%	Mensal
SUP-07	Incidentes de privacidade	0	Mensal

6. Operação

6.1 Planejamento e Controle Operacionais

Objetivo: implementar e manter controles operacionais para prevenir, detectar e responder a riscos de compliance e suborno.

Diretrizes gerais:

- Controles definidos por **processo, projeto e terceiro**, a partir da matriz de riscos (Cap. 4).

- **Gates de integridade** nas fases de **captação → contratação/convênio → execução → prestação de contas → encerramento**.
- **Exceções** a políticas: somente com **justificativa formal**, aprovação do responsável por Compliance e da diretoria competente, com registro no ECM.

Registros/Evidências: plano de controles por processo; evidências dos gates; planilhas/checklists assinadas; relatório mensal de exceções.

Indicadores: % de projetos que passaram por todos os gates (meta 100%); nº de exceções e tendência.

6.2 Controles Antissuborno Específicos

6.2.1 Brindes, Presentes e Hospitalidades

Regras mínimas:

- **Proibidos**: dinheiro, equivalentes (vales), brindes/hospitalidades durante licitações/negociações, itens sem log/identificação, brindes com valor acima do limite anual acumulado.
- **Limites monetários** (definir em política): valores por item e por ano por parte interessada; limiar que exige **aprovação prévia**.
- **Registro obrigatório**: toda oferta **dada** e **recebida**; recusas também devem ser registradas.

Fluxo:
Solicitação (formulário) → verificação de conflito/limite → aprovação (quando necessário) → registro no **Livro de Brindes e Hospitalidades** → guarda de evidências (convite, agenda, comprovantes).

Registros/Evidências: formulário; livro de brindes (ECM); aprovações; notas fiscais (se aplicável).
Indicadores: nº de registros vs. baseline; % de aprovações prévias quando exigidas; incidentes.

6.2.2 Conflitos de Interesse

Regras mínimas:

- **Declaração anual** de conflitos por todos, mais atualização por evento (mudança de função, novo projeto, contratação de parente/empresa ligada).
- **Gestão de impedimentos**: abstenção de decisão; substituição temporária; escalonamento quando envolver alta gestão.

Registros/Evidências: formulários anuais; atas com impedimentos; log de exceções.
Indicadores: % de declarações entregues (meta ≥ 98%); nº de casos com mitigação implementada.

6.2.3 Pagamentos de Facilitação

- **Vedação absoluta**.
- **Resposta esperada:** recusa, reporte imediato ao Canal de Denúncias, registro de evidências (datas, nomes, local, circunstâncias).
- **Plano de contingência:** contato com liderança/Compliance; alternativas legais para liberar processo (ofícios, protocolos, agendamento oficial).

Registros/Evidências: protocolos de denúncia; parecer de compliance; comunicação com autoridade/órgão.

Indicadores: nº de tentativas reportadas; tempo de resposta.

6.2.4 Interações com Agentes Públicos (e privados de alto risco)

Regras mínimas:

- **Agenda oficial**: local institucional, quando possível com **duas pessoas** do Instituto; registrar participantes, pauta e decisões.
- **Documentação**: ofícios, e-mails institucionais; evitar canais pessoais; arquivos no ECM.
- **Transparência**: evitar encontros sem pauta/objetivo; prestar contas de aquisições/entregas vinculadas a recursos públicos.
- **Proibições**: qualquer vantagem indevida; patrocínios/doações atreladas a decisões públicas; intermediações opacas.

Registros/Evidências: agendas; atas; fotos institucionais quando apropriado; documentos protocolados.

Indicadores: % de interações com ata/registro; nº de não conformidades em fiscalização.

6.2.5 Compras, Contratações e Cartões Corporativos/Caixa Miúdo

Princípios: segregação de funções, **competitividade**, **rastreabilidade** e **proporcionalidade**.

Mínimos operacionais:

- **Cotações comparáveis** (ex.: 3, quando viável); justificativa formal quando não possível.
- **Due diligence** conforme risco do fornecedor (Cap. 5.5).
- **Cláusulas de integridade** em contratos (Cap. 5.8).
- **Cartão corporativo/caixa miúdo**: limites, categorias elegíveis, **comprovantes obrigatórios**, reconciliação mensal por terceiro (quem reconcilia não aprova).

Registros/Evidências: mapas de cotação; parecer de DD; contratos assinados; relatórios de reconciliação; logs de aprovações.

Indicadores: % de compras com cotações adequadas; reconciliações concluídas no prazo (meta 100%); achados de auditoria.

6.3 Due Diligence Reforçada para Interações de Maior Risco

Aplicável a: representantes/consultores com contato com setor público, parceiros de captação, beneficiários críticos, projetos em áreas de alto risco.

Escopo adicional:

- Pesquisa reputacional avançada; beneficiário final; integridade financeira; verificação de processos/penalidades; entrevistas; visitas (quando cabível).
- **Cláusulas reforçadas**: auditoria, rompimento por justa causa, proibição de subcontratação sem anuência, reporte de interações com agentes públicos.
- **Monitoramento contínuo**: revalidação anual e por gatilhos (mudança societária, notícia negativa, autuação).

Registros/Evidências: dossiê reforçado; matriz decisória (apto/apto com mitigação/inapto); aprovações.

Indicadores: % de terceiros críticos com revalidação anual; tempo médio de DD; casos reprovados.

6.4 Controles em Projetos, Convênios e Termos de Fomento

Gates de integridade (modelo):

1. **Captação**: análise de integridade do financiador/edital; matriz de riscos; cláusulas exigidas.
2. **Contratação/Convênio**: validação de cláusulas, plano de compliance do projeto, RACI, treinamento inicial.
3. **Execução**: compras com segregação; relatórios parciais; monitoramento de indicadores; gestão de mudanças.
4. **Prestação de contas**: conferência 4-olhos; documentação completa e no prazo; resposta a diligências.
5. **Encerramento**: lições aprendidas de integridade; arquivamento; comunicação de resultados.

Registros/Evidências: checklists por gate; atas; relatórios; planilhas de PC; ofícios. **Indicadores:** % de projetos com gates cumpridos (meta 100%); retrabalho em PC (meta: −30% em 12 meses).

6.5 Gestão de Investigações Internas e Respostas a Violações

Princípios: imparcialidade, **confidencialidade**, **não retaliação**, **cadeia de custódia** de evidências.

Fluxo macro:

1. **Recebimento/triagem** (classificação por materialidade/criticidade; SLA de resposta inicial),
2. **Plano de investigação** (escopo, prazos, equipe sem conflito),
3. **Coleta e preservação de evidências** (documentos, entrevistas, logs),
4. **Análise e parecer** (conclusões, responsabilidade, recomendações),
5. **Decisão e medidas** (disciplinares, contratuais, correções de processo, comunicação a autoridades quando necessário),
6. **Feedback** ao denunciante (quando possível) e **lições aprendidas**.

Salvaguardas:

- Investigadores com **independência**; suporte jurídico; registro de todos os passos.
- **Proteção de dados** e minimização de informações pessoais.

Registros/Evidências: protocolos; plano de investigação; atas de entrevistas; parecer; comprovação de medidas; feedback.

Indicadores: tempo médio de apuração (≤ 45 dias); % de planos concluídos; reincidência por tema.

6.6 Cooperação com Autoridades e Órgãos de Controle

Diretrizes:

- **Prontidão documental** (ECM); respostas tempestivas; canal único de comunicação oficial.
- **Preservação de evidências** e confidencialidade; alinhamento com Jurídico.
- **Relato voluntário** quando aplicável, conforme devidos processos e análise de riscos.

Registros/Evidências: ofícios; protocolos; atas; inventário de documentos enviados; comprovantes de recebimento.

Indicadores: cumprimento de prazos; nº de diligências atendidas sem ressalvas.

6.7 Fluxos Operacionais (Modelos)

6.7.1 Fluxo — Compras/Contratos (resumo)

Solicitação → Análise de necessidade → Cotações → Due diligence → Parecer de Compliance (por risco) → Aprovação → Contrato com cláusulas → Entrega/Recebimento → Pagamento → Reconciliação → Arquivamento.

6.7.2 Fluxo — Brindes/Hospitalidades

Solicitação/Registro → Verificação de limites e conflito → Aprovação (se exigida) → Registro no Livro → Arquivamento.

6.7.3 Fluxo — Denúncias/Investigações

Recebimento → Triagem (SLA) → Plano → Coleta/Entrevistas → Parecer → Medidas → Feedback → Encerramento → Lições aprendidas.

(Fluxogramas detalhados podem ser incluídos no Anexo 11.4.)

6.8 RACI Operacional (alto nível)

Atividade	Conselho	Diretoria	Compliance	Jurídico	Compras	Projetos	Financeiro	RH	TI
Aprovar políticas e limites	A	C	C	C	I	I	I	I	I
Brindes/Hospitalidades (aprovações)	I	A	R (critérios)	C	C	I	I	I	I
Conflitos de interesse	I	A	R	C	C	C	C	R (coleta)	I
Compras/Contratos	I	A	C	C	R	C	C	I	I
Due diligence de terceiros	I	A	R (metodologia)	C	R (execução)	C	C	I	I
Canal de denúncias	I	I	R	C	I	I	I	I	C (plataforma)
Investigações	I	A	R	R	C	C	C	C	C

Atividade	Conselho	Diretoria	Compliance	Jurídico	Compras	Projetos	Financeiro	RH	TI
Prestação de contas	I	A	C	C	C	R	R	I	I

6.9 Indicadores Operacionais (sugestões)

Código	Indicador	Definição	Meta inicial	Periodicidade
OPR-01	Gates de integridade cumpridos	% de projetos com todos os gates concluídos	100%	Mensal
OPR-02	Due diligence concluída no prazo	% de terceiros de risco com DD prévia	100%	Mensal
OPR-03	Reconciliação financeira tempestiva	% de reconciliações no prazo	100%	Mensal
OPR-04	Tempo de resposta no canal	Mediana entre denúncia e triagem	≤ 5 dias úteis	Mensal
OPR-05	Tempo de investigação	Mediana de dias para encerrar casos	≤ 45 dias	Mensal
OPR-06	Conflitos de interesse	% de declarações anuais entregues	≥ 98%	Anual
OPR-07	Brindes/hosp. regulares	% de registros conformes vs. total	≥ 95%	Trimestral
OPR-08	Achados críticos de auditoria	Nº e % resolvidos no prazo	100%	Trimestral

6.10 Periodicidades Consolidada (cap. 6)

- **Revisão de limites e políticas sensíveis** (brindes, conflitos, cartões): **anual**.
- **Revalidação de terceiros críticos**: **anual** ou por gatilho.
- **Prestação de contas**: conforme convênio/contrato; **controle mensal** interno.
- **Relatórios operacionais**: **mensais** para diretoria; **trimestrais** para Conselho/Comitê.

6.11 Saídas do Capítulo (entregáveis mínimos)

1. **Políticas operacionais** publicadas (brindes/hosp., conflitos, compras/contratos, cartões, relacionamento com setor público).
2. **Fluxos e checklists** por gate de projeto/convênio (captação → encerramento).
3. **Livro de Brindes e Hospitalidades** e **Registro de Interações com o Setor Público**.
4. **Dossiês de Due Diligence** com classificação por risco e revalidações.
5. **Matriz de Conflitos de Interesse** e log de impedimentos.
6. **Procedimento de Investigações Internas** com SLAs e salvaguardas.
7. **Relatórios operacionais** e **dashboards** com indicadores do capítulo.

7. Avaliação de Desempenho

7.1 Monitoramento, Medição, Análise e Avaliação

Objetivo: acompanhar, de forma sistemática, a eficácia do SGC/SGAS e seus controles, permitindo decisões tempestivas da Direção/Conselho.

7.1.1 Escopo do monitoramento

- **Controles-chave**: canal de denúncias, due diligence de terceiros, compras/contratações, brindes/hospitalidades, conflitos de interesse, relacionamento com setor público, prestação de contas.
- **Processos de suporte**: gestão documental (ECM), trilhas EAD, gestão de mudanças, proteção de dados.
- **Projetos/convênios**: cumprimento de "gates" de integridade e resultados de auditorias/visitas.

7.1.2 Papel e responsabilidades

- **Compliance/Integridade**: consolida indicadores, valida dados, emite relatórios mensais/trimestrais, recomenda ações.
- **Donos de Processo**: medem indicadores operacionais, garantem qualidade e pontualidade dos dados.
- **Diretoria/Conselho**: analisam tendências, determinam recursos/correções e priorizam temas críticos.

7.1.3 Metodologia de medição

- **Periodicidade** definida por risco (mensal p/ canal e compras; trimestral p/ DD; anual p/ conflitos).

- **Qualidade dos dados**: fonte registrada no ECM, trilhas de auditoria, critérios de cálculo padronizados.
- **Análise de tendência**: médias móveis, variação vs. meta, heatmap de risco por indicador.
- **Lições aprendidas**: cada desvio relevante gera análise de causa e ação corretiva (ver Cap. 8).

7.1.4 Painel de Indicadores (modelo)

Código	Indicador	Definição	Meta	Freq.	Responsável	Ações quando < meta
GOV-02	Cobertura EAD	% público-alvo com EAD concluído	≥ 95%	Mensal	RH/Compliance	Plano de reforço + comunicação
RSK-03	DD antes da contratação	% terceiros de risco com DD prévia	100 %	Mensal	Suprimentos/Compliance	Bloqueio sistêmico + revisão de fluxo
OPR-05	Tempo de investigação	Mediana de dias/caso encerrado	≤ 45	Mensal	Compliance/Jurídico	Reforço de equipe/escopo
OPR-03	Reconciliação tempestiva	% reconciliações no prazo	100 %	Mensal	Financeiro	Ações corretivas e coaching
CTX-01	Mapeamento de processos	% processos críticos mapeados	≥ 90%	Trimestral	Donos de Processo	Cronograma + apoio metodológico

Registros/Evidências: planilhas/dashboards no ECM, metodologia de cálculo, trilhas de sistema, relatórios de consolidação e atas de reuniões de acompanhamento.

7.2 Auditorias Internas

Objetivo: verificar, de forma independente e sistemática, se o SGC/SGAS está conforme, implementado e eficaz, e se atende às normas e à legislação aplicável.

7.2.1 Princípios

- **Independência e imparcialidade**: auditores não auditam processos pelos quais sejam responsáveis.

- **Abordagem baseada em risco**: priorização de áreas/temas críticos.
- **Evidência objetiva**: amostragem, entrevistas, observação e análise documental.
- **Rastreabilidade**: planejamento → execução → achados → ações corretivas → verificação de eficácia.

7.2.2 Programa Anual de Auditorias (modelo)

Elemento	Descrição
Objetivos	Conformidade com ISO 37001/37301, políticas internas e marcos legais; eficácia de controles; verificação de ações do Cap. 4 (riscos)
Escopo	Canal de denúncias, investigações, DD de terceiros, compras/contratos, brindes/hospitalidades, conflitos de interesse, relacionamento com setor público, gestão documental, EAD
Critérios	MA-003; políticas/procedimentos; requisitos ISO aplicáveis; leis/decretos; cláusulas contratuais
Frequência	Ciclo anual com foco ampliado em áreas de maior exposição
Recursos	Equipe interna qualificada; apoio de auditor externo quando necessário
Método	Planos de auditoria por processo; checklists; amostragem; testes; entrevistas; walkthroughs
Saídas	Relatórios com achados (classificação por gravidade), evidências, causas, riscos, recomendações e prazos

7.2.3 Planejamento de auditoria (passos)

1. **Plano anual** aprovado pela Alta Direção/Conselho.
2. **Anúncio de escopo** a áreas auditadas; solicitação de documentos.
3. **Reunião de abertura**: confirmação de critérios, cronograma, canais.
4. **Execução**: testes e entrevistas; registro de evidências.
5. **Reunião de encerramento**: apresentação de achados preliminares.
6. **Relatório final**: classificação, responsáveis e prazos.
7. **Acompanhamento**: verificação de eficácia das ações corretivas.

7.2.4 Classificação de achados (exemplo)

- **Crítico**: risco alto/violações legais/possível dano relevante; ação imediata.
- **Maior**: não conformidade significativa/controle ineficaz; prazo curto (≤ 30 dias).
- **Menor**: desvio pontual/documental; prazo regular (≤ 60 dias).
- **Oportunidade de melhoria**: recomendação sem desvio.

7.2.5 Amostragem (diretrizes)

- **Amostra mínima por risco**:
    - Alto: 25–40 itens ou 100% quando universo pequeno/estratégico.
    - Médio: 10–20 itens.
    - Baixo: 5–10 itens.
- **Amostragem dirigida**: focar períodos de maior risco (licitações, picos de execução, regiões/terceiros críticos).

Registros/Evidências: plano anual; planos de auditoria por processo; relatórios; matriz de achados; pareceres de eficácia; atas de reuniões.

Periodicidades-chave: auditoria **anual** (mínimo); follow-up **mensal** dos achados até encerramento.

Indicadores sugeridos:

- % de auditorias realizadas vs. plano (meta 100%).
- % de achados **encerrados** no prazo por gravidade (meta ≥ 90%).
- % de testes de controle "eficazes" (meta ≥ 90%).
- Tempo médio de fechamento de achados críticos (meta ≤ 30 dias).

7.3 Análise Crítica pela Direção

Objetivo: avaliar, em nível estratégico, a **adequação, suficiência e eficácia** do SGC/SGAS, definindo prioridades e recursos para o ciclo seguinte.

7.3.1 Insumos (inputs) mínimos

- Resultados de **monitoramento e indicadores** (tendências e desvios);
- **Relatórios de auditoria interna/externa** e follow-up;
- **Status de ações corretivas e oportunidades de melhoria**;
- **Avaliação de riscos** (atualizações e incidentes);
- **Cumprimento de objetivos e metas** (Cap. 4);
- **Feedbacks de partes interessadas** (incluindo órgãos de controle e financiadores);
- **Mudanças relevantes** (legais, estruturais, tecnológicas, geográficas, parceiros);
- **Recursos** (orçamento/equipe/ferramentas) e **competências**;
- **Conformidade legal e contratual** (eventos, sanções, notificações).

7.3.2 Saídas (outputs) esperadas

- **Decisões** sobre recursos (humanos, financeiros, tecnológicos);

- **Ajustes** em políticas, objetivos e metas;
- **Revisão** do apetite/tolerância a risco;
- **Prioridades** de auditoria e monitoramento para o próximo ciclo;
- **Planos de ação** com prazos e responsáveis;
- **Comunicação** das conclusões às partes interessadas relevantes.

7.3.3 Roteiro da reunião (modelo)

1. Abertura e objetivos;
2. Painel de indicadores e riscos;
3. Achados de auditoria e eficácia das ações;
4. Desempenho de DD, canal e temas sensíveis;
5. Recursos e competências;
6. Deliberações e aprovações;
7. Encaminhamentos e prazos.

Registros/Evidências: ata assinada; apresentações; lista de decisões; plano pós-reunião no ECM.

Periodicidade: anual (mínimo) — recomenda-se **semestral** em períodos de maior risco.

Indicadores:

- % de decisões implementadas no prazo (meta ≥ 85%).
- Nº de reiterações de temas recorrentes (meta: tendência decrescente).

7.4 Relato e Transparência

Objetivo: assegurar prestação de contas interna/externa proporcional ao risco e às exigências contratuais.

Diretrizes:

- **Relatórios trimestrais** ao Conselho/Comitê de Integridade com indicadores, eventos críticos e plano de ação.
- **Relatório anual de integridade** (versão pública, quando aplicável): resultados agregados, iniciativas, aprendizados; preservar confidencialidade e LGPD.
- Atender **requisitos de financiadores/órgãos de controle** quanto a relatórios de integridade e auditorias.

Registros/Evidências: relatórios, publicações, comprovações de envio/recebimento, versões arquivadas no ECM.

7.5 Maturidade do Programa (diagnóstico anual)

Objetivo: medir a evolução do SGC/SGAS e priorizar melhorias.

Modelo de maturidade (exemplo, 1 a 5):

1. **Inicial** (ad hoc)
2. **Básico** (políticas publicadas; controles iniciais)
3. **Padronizado** (processos definidos; medições regulares)
4. **Gerenciado** (KPIs/KRIs; auditorias eficazes; análise crítica robusta)
5. **Otimizado** (melhoria contínua; insights preditivos; integração total a decisões)

Evidências: checklist anual com critérios objetivos, pontuação e plano de evolução.

Indicadores: nível médio por domínio (governança, riscos, operação, suporte, mensuração); variação anual (+≥0,5 ponto desejado).

7.6 Não Conformidades, Ações Corretivas e Melhoria (ponte para o Cap. 8)

Objetivo: assegurar tratamento eficaz de desvios identificados em monitoramentos, auditorias e denúncias.

Fluxo resumido:

Detecção → Registro no ECM → Análise de causa (ex.: 5 Porquês/Ishikawa) → Plano de ação (quem/como/quando) → Implementação → Verificação de eficácia → Encerramento.

Registros: ticket/NC; análise de causa; evidências de implementação; verificação de eficácia; lições aprendidas.

Indicadores: % de NCs encerradas no prazo; % com eficácia comprovada; reincidência por tema/processo.

7.7 Saídas do Capítulo (entregáveis mínimos)

1. **Metodologia de monitoramento e medição** com indicadores definidos e publicados no ECM.
2. **Painel (dashboard)** ativo com KPIs/KRIs e trilhas de auditoria.
3. **Programa anual de auditorias internas** aprovado e executado.
4. **Relatórios de auditoria** e **matriz de achados** com plano de ação e verificação de eficácia.
5. **Ata de Análise Crítica** com decisões e priorizações para o ciclo seguinte.

6. **Relatórios de integridade** (internos e/ou públicos) conforme aplicável.
7. **Diagnóstico anual de maturidade** com plano de evolução.

Periodicidades consolidadas (cap. 7)

- Indicadores críticos: **mensal**; consolidação gerencial: **trimestral**;
- Auditoria interna: **anual** + follow-up **mensal**;
- Análise crítica: **anual** (recomendado **semestral**);
- Relato público (quando aplicável): **anual**.

8. Melhoria

8.1 Objetivo e Princípios

Objetivo: assegurar que desvios, incidentes, achados de auditoria e oportunidades gerem **aprendizado organizacional** e **aumento de eficácia** do SGC/SGAS, com **prevenção de recorrência**.
Princípios: foco em **causa-raiz**, proporcionalidade ao risco, rastreabilidade no **ECM**, verificação de eficácia e **retroalimentação** para riscos (Cap. 4), operação (Cap. 6) e governança (Cap. 3/7).

8.2 Tipos de Entradas para Melhoria

- **Não conformidades (NCs):** descumprimentos de requisito normativo, legal ou interno (política, POP, contrato).
- **Achados de auditoria:** crítico, maior, menor, oportunidade de melhoria.
- **Incidentes** de integridade (ex.: falhas em compras, conflitos não declarados, desvios em prestação de contas).
- **Resultados de indicadores** (KPIs/KRIs fora da meta).
- **Lições aprendidas** de projetos, denúncias/investigações e análises críticas.
- **Mudanças de contexto** (novas leis, novos modelos operacionais, novas regiões).

Registros/Evidências: tickets/NCs no ECM; relatórios de auditoria; dashboards; relatórios de caso; atas de análise crítica; formulários de lições aprendidas.

8.3 Processo de Tratamento de Não Conformidades (NC) e Ação Corretiva (CAPA)

8.3.1 Fluxo (modelo)

1. **Registro da NC** (área origem ou Compliance) no ECM →
2. **Conter/Isolar** risco imediato (ação imediata, se necessário) →
3. **Análise de Causa** (método adequado) →
4. **Plano de Ação Corretiva** (quem/como/quando/recursos) →
5. **Implementação** e evidências →
6. **Verificação de Eficácia** (pós-implementação) →
7. **Encerramento** com lições aprendidas e atualização de documentos/processos.

8.3.2 Regras Gerais

- **Prazo de abertura:** até **5 dias úteis** após identificação.
- **Classificação de gravidade:** crítico/maior/menor (alinha prazos e nível de aprovação).
- **Aprovação:** Compliance valida **causa-raiz** e **plano**; gravidade crítica requer **Diretoria/Conselho**.
- **Evidências obrigatórias:** prints/documentos, atas, logs, treinamentos realizados, versões revisadas de políticas/POPs.

8.3.3 Análise de Causa — Métodos Recomendados

- **5 Porquês** (simples, para desvios pontuais).
- **Ishikawa** (causas por dimensão: Pessoas, Processo, Política, Tecnologia, Materiais, Ambiente).
- **A3/PDCA** (problemas complexos, integração com indicadores).
- **Análise de Barreiras/Controles** (bow-tie simplificado).

Registro mínimo da análise: problema, evidências, causas imediatas, causas-raiz, controles ausentes/ineficazes, riscos correlatos, proposta de ação.

8.3.4 Plano de Ação Corretiva (CAPA)

Requisitos mínimos:

- **Ações SMART** (específicas, mensuráveis, responsáveis, prazos, custo/benefício).
- **Tipos de ação:** revisão de política/POP, reforço de segregação, treinamento focalizado, automação/tecnologia, alteração de contrato, reforço de due diligence, ajustes nos indicadores.

- **Risco residual esperado** após a ação.

Aprovação: Compliance + Dono do Processo; casos críticos com Diretoria/Conselho.

8.3.5 Verificação de Eficácia

- **Critérios objetivos**: indicador voltou à meta? reincidência zero em período de observação? teste de controle eficaz em auditoria?
- **Período de observação** típico: 60–90 dias (ajustar por risco).
- **Resultado: "Eficaz"**, **"Parcialmente eficaz"** (gera ação complementar), **"Ineficaz"** (nova análise de causa).

Registros/Evidências: relatórios de verificação; prints de indicadores; resultados de testes; ata de validação.

8.4 Oportunidades de Melhoria (OM) e Inovação

Objetivo: canalizar sugestões que **reduzam risco**, **simplifiquem controles** ou **aumentem eficiência**.

Pipeline (modelo): Ideia → Triagem (Compliance + Dono do Processo) → Priorização por impacto/viabilidade → Piloto → Escala → Padronização (política/POP).

Exemplos de OM:

- Digitalização de checklists de prestação de contas;
- Integração ECM ↔ ERP ↔ ferramenta de due diligence;
- Cláusulas padrão "inteligentes" (templates com variáveis por risco);
- Dashboards de "gates de integridade" por projeto.

Registros/Evidências: backlog de OM, critérios de priorização, atas de decisão, resultados de pilotos.

Indicadores: % de OM implementadas vs. priorizadas; prazo médio de implantação; ganho estimado de tempo/custo; redução de riscos.

8.5 Integração com Gestão de Riscos e Mudanças

- **Riscos (Cap. 4):** toda NC crítica/maior **retroalimenta** a matriz de riscos; reavaliar probabilidade/impacto e controles.
- **Mudanças (Cap. 4.4):** CAPAs que alterem processos, sistemas, papéis ou contratos disparam o **fluxo de mudança** (análise de impacto, comunicação, treinamento e atualização documental).
- **Auditorias (Cap. 7.2):** achados geram CAPA e permanecem **abertos** até eficácia comprovada.

8.6 Documentos, Registros e Controle no ECM

Documentos: Procedimento de Melhoria (este capítulo), instrução de trabalho de análise de causa, políticas revisadas, POPs revisados.
Registros: tickets/NCs, análises de causa, planos de ação, evidências de implementação, verificações de eficácia, lições aprendidas, backlog de OM.

Metadados obrigatórios: Nº do registro; origem (auditoria, denúncia, indicador, projeto); gravidade; dono; prazos; status; vínculo com risco/controle; itens documentais impactados.

Retenção mínima sugerida:

- **NCs/Investigações**: conforme tabela de retenção (recomenda-se ≥ 5 anos após encerramento ou por exigência legal/contratual).
- **Auditorias**: relatórios e CAPAs por ≥ 5 anos.
- **Treinamentos decorrentes**: ≥ 3 anos.

8.7 Indicadores (KPIs/KRIs) — Melhoria

Código	Indicador	Definição	Meta inicial	Periodicidade
MEL-01	**NCs encerradas no prazo**	% de NCs com CAPA concluída dentro do prazo	≥ 90%	Mensal
MEL-02	**Eficácia de CAPA**	% de CAPAs classificadas "eficazes"	≥ 85%	Trimestral
MEL-03	**Recorrência**	Nº de reincidências do mesmo tipo/processo	Tendência decrescente	Trimestral
MEL-04	**Tempo de ciclo de CAPA**	Mediana dias: abertura → eficácia verificada	≤ 90 dias	Mensal
MEL-05	**Implementação de OM**	% de oportunidades priorizadas implementadas	≥ 70%/ano	Trimestral
MEL-06	**Atualização documental**	% de políticas/POPs atualizados após CAPA	100%	Trimestral

8.8 Boas Práticas

- **“Do incidente ao insight”**: cada NC crítica vira **case de aprendizado** (anonimizado) no EAD.
- **Ciclos Kaizen** de 30 dias para problemas operacionais recorrentes.
- **Revisões “pré-mortem”** em projetos de alto risco (antecipar falhas).
- **Pareamento** Compliance + Dono do Processo para acelerar CAPAs complexas.
- **Gatilhos automatizados** no ECM (alertas de prazo, status e aprovação).

8.9 Saídas do Capítulo (entregáveis mínimos)

1. **Procedimento de Melhoria e CAPA** padronizado e publicado.
2. **Formulários/Modelos** (NC/CAPA, 5 Porquês, Ishikawa, A3/PDCA, verificação de eficácia).
3. **Backlog de Oportunidades de Melhoria** com critérios de priorização.
4. **Relatórios periódicos** de NCs/CAPAs/OM para Diretoria e Conselho.
5. **Atualizações documentais** derivadas de CAPAs (políticas/POPs) no ECM.
6. **Lições aprendidas** incorporadas aos treinamentos EAD.

9. Políticas e Procedimentos Específicos do Instituto Sustenta

Aplicabilidade: todas as pessoas vinculadas ao Instituto (conselheiros, diretores, colaboradores, estagiários, voluntários) e **terceiros relevantes** (fornecedores, parceiros, consultores, doadores e beneficiários críticos).

Governança: cada política deve ser aprovada pela Alta Direção e revista **anualmente** ou quando houver mudança relevante.

Forma: publicação no ECM, com **assinatura digital** de ciência/aceite e versionamento controlado.

9.1 Código de Conduta e Integridade

Objetivo: consolidar princípios, valores e comportamentos esperados.

Conteúdo mínimo:

- Princípios (integridade, legalidade, imparcialidade, transparência, não retaliação).
- Condutas vedadas (suborno, fraude, assédio, discriminação, retaliação, uso indevido de ativos).
- Conflitos de interesse (declaração e gestão).
- Uso de recursos do Instituto (cartões, equipamentos, dados).
- Canal de denúncias (acesso, confidencialidade, garantias).
- Consequências disciplinares (graduação e devido processo).

Registros/Evidências: versão vigente; aceite digital; campanhas de divulgação; FAQs.
Indicadores: % de aceite digital (meta = 100%); nº de dúvidas recebidas e respondidas; reincidências por tema.

9.2 Política Antissuborno

Objetivo: proibir e prevenir **qualquer** forma de suborno e vantagem indevida, direta ou indireta.

Conteúdo mínimo:

- Proibição de suborno ativo e passivo; **pagamentos de facilitação** proibidos.
- Interações com agentes públicos e privados (ver 9.7).
- Brindes, presentes e hospitalidades (ver 9.4) — limites e aprovação.
- Doações e patrocínios (ver 9.5) — critérios e rastreabilidade.
- Terceiros (representantes/consultores) — due diligence reforçada (ver 9.6).
- Registro e reporte obrigatório de tentativas de solicitação/oferta.

Fluxo de resposta a tentativa de suborno (resumo): recusa → registro → reporte ao canal → avaliação de Compliance/Jurídico → medidas (disciplinar/contratual/institucional).
Registros/Evidências: formulários de incidente; pareceres; decisões; comunicações oficiais.
Indicadores: nº de tentativas reportadas; tempo de resposta; % de casos com medidas aplicadas.

9.3 Política de Conflito de Interesses

Objetivo: prevenir, identificar e tratar situações em que interesses privados interfiram no interesse institucional.

Diretrizes:

- **Declaração obrigatória anual** e por evento.

- Proibições e salvaguardas (ex.: participação em decisões que envolvam parentes/empresas vinculadas).
- Regra de ouro de **segregação e abstenção**.
- Registro de **impedimentos** em atas e sistema.

Fluxo (síntese): identificação → declaração → análise de Compliance → medidas (abstenção, substituição, blindagem de informação) → registro → monitoramento. **Registros/Evidências:** formulários; pareceres; atas com impedimento; log de exceções. **Indicadores:** % de declarações entregues (meta ≥ 98%); nº de casos com mitigação registrada.

9.4 Política de Brindes, Presentes e Hospitalidades

Objetivo: gerir riscos de influência indevida em interações institucionais.

Parâmetros (ajustar valores):

- **Proibido**: dinheiro/vales; itens em licitações/negociações; brindes sem identificação; hospitalidades de luxo.
- **Limites**: valor máximo por item e **teto anual** por parte interessada; limiar para **aprovação prévia**.
- **Registro obrigatório** de tudo que for **ofertado** e **recebido** (inclusive recusas), no **Livro de Brindes/Hospitalidades**.

Fluxo: solicitação/registro → verificação de conflito/limite → aprovação (se aplicável) → registro e arquivamento. **Registros/Evidências:** formulários; aprovações; livro (ECM); notas/convites. **Indicadores:** % de registros conformes; nº de exceções; incidentes por tema.

9.5 Política de Doações, Patrocínios e Parcerias Socioambientais

Objetivo: garantir finalidade pública/estatutar e **rastreabilidade**.

Critérios mínimos:

- **Elegibilidade** do beneficiário (estatuto, regularidade fiscal, histórico).
- **Due diligence proporcional** ao risco; **beneficiário final** quando cabível.
- Contrato/termo com **cláusulas de integridade** e metas/entregas.
- **Proibição** de contrapartidas indevidas (ex.: favorecer decisões públicas).
- **Prestação de contas**: comprovações, indicadores e avaliação de impacto.

Registros/Evidências: dossiê do beneficiário; parecer de DD; contrato; relatórios de entrega; evidências de comunicação institucional.

Indicadores: % de operações com DD prévia; % de prestações aprovadas sem ressalva; casos indeferidos por integridade.

9.6 Política de Contratações e Due Diligence de Terceiros

Objetivo: prevenir riscos na **cadeia de fornecimento e parceria**.

Diretrizes:

- **Classificação de risco** do terceiro (baixo/médio/alto/crítico).
- **Escopo de DD** conforme risco (simplificada, padrão, reforçada).
- **Cotações comparáveis** (quando viável) e justificativas formais.
- **Cláusulas padrão** anticorrupção, direito de auditoria, rompimento por justa causa, vedação de subcontratação sem anuência.
- **Revalidação** anual de terceiros críticos e **monitoramento por gatilhos** (notícia negativa, mudança societária).

Fluxo: requisição → classificação → DD → parecer (apto/apto c/ mitigação/inapto) → contratação → monitoramento/revalidação.

Registros/Evidências: dossiês de DD; pareceres; contratos; revalidações; relatórios de monitoramento.
Indicadores: % de terceiros de risco com DD **antes** da contratação (meta 100%); tempo médio de DD; nº de reprovações.

9.7 Política de Relacionamento com o Setor Público

Objetivo: assegurar integridade nas interações com agentes/entidades públicas.

Regras mínimas:

- **Agenda formal** (participantes, pauta, objetivos, local institucional).
- **Dois representantes** do Instituto quando possível.
- **Documentação oficial** (ofícios, e-mails institucionais) e **registro no ECM**.
- **Vedado** oferecer, prometer, solicitar ou aceitar vantagem indevida; **pagamentos de facilitação** proibidos.
- **Transparência** em convênios/termos de fomento (publicidade dos resultados, prestações dentro do prazo).

Registros/Evidências: atas/agendas; ofícios; comprovações de entrega; fotos institucionais quando aplicável.

Indicadores: % de interações com ata/registro; nº de não conformidades em fiscalizações.

9.8 Política de Investigações Internas e Medidas Disciplinares

Objetivo: garantir **imparcialidade, confidencialidade** e **não retaliação**.

Diretrizes:

- **Triagem com SLA** e matriz de materialidade/criticidade.
- **Plano de investigação** (escopo, prazos, equipe sem conflito).
- **Cadeia de custódia** de evidências; proteção de dados.
- **Relatório conclusivo** com recomendações (disciplinares, contratuais, processuais, reporte a autoridades).
- **Medidas proporcionais** e graduadas; **devido processo**.

Registros/Evidências: protocolos; planos; atas de entrevistas; parecer; evidências de medidas; feedback ao denunciante (quando possível).

Indicadores: tempo de apuração (mediana ≤ 45 dias); % de casos com medidas implementadas; reincidência.

9.9 Política de Proteção ao Denunciante e Não Retaliação

Objetivo: proteger pessoas que reportam **de boa-fé**.

Garantias:

- **Confidencialidade** e, quando possível, **anonimato**.
- **Proibição de retaliação** (direta/indireta) — medidas disciplinares em caso de violação.
- **Acolhimento e suporte** (orientações, encaminhamentos, proteção de dados).
- **Feedback** sobre o desfecho, dentro dos limites legais.

Registros/Evidências: política publicada; registros de proteção aplicados; acompanhamento de possíveis retaliações.

Indicadores: nº de alegações de retaliação; % tratadas dentro do SLA; satisfação do denunciante (quando mensurável).

9.10 Política de Privacidade e Proteção de Dados (interface com LGPD)

Objetivo: tratar dados pessoais de forma **lícita, transparente e segura**, especialmente em denúncias, **investigações** e **due diligence**.

Diretrizes:

- **Bases legais** adequadas (obrigação legal, exercício regular de direitos, legítimo interesse, etc.).
- **Minimização** e **limitação de finalidade**; **prazos de retenção** definidos.
- **Controles de acesso** por perfil; **registro de operações** (logs).
- **Termos de privacidade** específicos para canal de denúncias e DD.
- **Contratos com operadores** com cláusulas de proteção de dados.
- **Gestão de incidentes** (notificação, contenção, lições aprendidas).

Registros/Evidências: inventário de tratamentos; termos de privacidade; acordos com operadores; relatórios de incidente.

Indicadores: nº de incidentes de privacidade (meta 0); % de operações com base legal mapeada (meta 100%).

9.11 Modelos e Cláusulas Padrão (resumo para o ECM)

A) Cláusula Anticorrupção (contratos):

"A CONTRATADA declara ciência e adesão às políticas de integridade do Instituto Sustenta, comprometendo-se a **não oferecer, prometer, solicitar, autorizar ou conceder** qualquer vantagem indevida a agentes públicos ou privados. Fica assegurado ao Instituto o **direito de auditoria**, e a **rescisão por justa causa** em caso de violação, sem prejuízo de perdas e danos e comunicação às autoridades."

B) Cláusula de Direito de Auditoria:

"O Instituto poderá, diretamente ou por terceiros por ele designados, auditar documentos e registros relacionados ao contrato, mediante aviso prévio, preservando confidencialidade e dados pessoais."

C) Cláusula de Beneficiário Final (terceiros):

"A CONTRATADA declara e manterá atualizado o **beneficiário final** e estrutura societária, comunicando alterações em até X dias."

D) Declaração de Conflito de Interesses (modelo curto):

- Dados do signatário; vínculo; descrição do potencial conflito; medidas propostas de mitigação; assinatura digital.

E) Formulário de Brindes/Hospitalidades:

- Data; parte ofertante/recebedora; descrição; valor estimado; objetivo; fase do processo (se houver); aprovação (se exigida); decisão; registro no livro.

F) Matriz de Penalidades (síntese):

- Advertência escrita; suspensão; rescisão contratual; descredenciamento; comunicação às autoridades; critérios de gradação (intencionalidade, reincidência, dano, risco).

9.12 Responsabilidades e Governança das Políticas

Política	Dono (owner)	Aprovador	Apoios	Revisão mínima
Código de Conduta	Compliance	Conselho/Diretoria	RH/Jurídico	Anual
Antissuborno	Compliance	Conselho/Diretoria	Jurídico/Projetos	Anual
Conflito de Interesses	Compliance	Diretoria	RH/Jurídico	Anual
Brindes/Hospitalidades	Compliance	Diretoria	Suprimentos/Jurídico	Anual
Doações/Patrocínios	Projetos	Diretoria	Compliance/Jurídico	Anual
Contratações/DD Terceiros	Suprimentos	Diretoria	Compliance/Jurídico	Anual
Relacionamento Setor Público	Rel. Institucional	Diretoria	Compliance/Jurídico	Anual
Investigações/Disciplina	Compliance	Diretoria	Jurídico/RH	Anual
Proteção ao Denunciante	Compliance	Diretoria	RH/Jurídico	Anual
Privacidade/LGPD	Jurídico/TI	Diretoria	Compliance	Anual

9.13 Indicadores Consolidados do Capítulo (sugestões)

Código	Indicador	Meta inicial	Frequência
POL-01	Políticas publicadas com aceite digital	100%	Trimestral
POL-02	Contratos com cláusulas padrão de integridade	100%	Trimestral
POL-03	Terceiros críticos com DD prévia	100%	Mensal
POL-04	Prestação de contas sem ressalvas	≥ 90%	Trimestral
POL-05	Declarações anuais de conflito entregues	≥ 98%	Anual
POL-06	Incidentes por tema sensível (tendência)	−20% em 12 meses	Mensal

10. Indicadores, Registros e Evidências

10.1 Princípios Gerais

- **Unicidade e rastreabilidade:** toda evidência reside no **ECM** e é vinculada ao processo, ao requisito normativo e ao controle correspondente.
- **Proporcionalidade ao risco:** maior granularidade e retenção para processos/terceiros de **alto risco**.
- **Integridade e confidencialidade:** controles de acesso por perfil, logs e backups; dados pessoais conforme **LGPD**.
- **Auditabilidade:** trilhas completas (quem criou/alterou/aprovou, quando e por quê), versões congeladas (“read-only”) para auditorias.

10.2 Taxonomia de Registros (padrão ECM)

Nomenclatura: Área_Processo_TipoRegistro_Ano_Mês_ID

Ex.: COMPLIANCE_DD_TERCEIROS_2025_03_000123

Classe	Subclasse	Exemplos de Registros	Dono do Registro	Sigilo*
Governança	Conselho/Comitês	Atas, planos anuais, análises críticas	Secretaria/Compliance	Restrito
Políticas/POPs	Documentos normativos	Políticas, POPs, modelos, histórico de versões	Compliance	Interno
Riscos & Controles	Matriz/Heatmap/Planos	Matriz de riscos, planos de tratamento, testes de controle	Compliance/Donos	Interno
Terceiros	Due Diligence	Dossiês, pareceres, revalidações, cláusulas	Suprimentos/Compliance	Restrito
Compras/Contratos	Cotações/Contratos	Mapas, aprovações, contratos assinados, aditivos	Suprimentos/Jurídico	Interno
Canal de Denúncias	Casos/Investigações	Protocolos, triagens, relatórios, medidas	Compliance/Jurídico	Confidencial
Projetos/Convênios	Gates/PC	Checklists de gate, prestações de contas, diligências	Projetos/Financeiro	Interno
Treinamentos	EAD/Presenciais	Trilhas, listas,	RH/Compliance	Interno

Classe	Subclasse	Exemplos de Registros	Dono do Registro	Sigilo*
		certificados, termos assinados		
Auditorias	Planejamento/Achados	Planos, relatórios, matriz de achados, CAPA	Auditoria/Compliance	Restrito
Privacidade	LGPD	Inventário de tratamento, DPIA/RIPD, incidentes	Jurídico/TI	Confidencial

* **Sigilo:** Interno (todos os colaboradores), Restrito (apenas áreas envolvidas), Confidencial (acesso sob necessidade; casos sensíveis).

10.3 Tabela de Retenção e Descarte (mínimo recomendado)

Classe	Tipo de registro	Retenção mínima	Destino após prazo	Observações
Governança	Atas/Análises críticas	10 anos	Arquivo histórico	Projetos com recursos públicos: seguir exigência contratual
Políticas/POPs	Versões obsoletas	5 anos	Arquivo histórico	Manter última obsoleta por comparação
Riscos & Controles	Matriz/Planos	5 anos	Arquivo histórico	Manter heatmap final de cada ciclo

Classe	Tipo de registro	Retenção mínima	Destino após prazo	Observações
Terceiros	Dossiês DD	5 anos após fim do contrato	Eliminar/anonimizar	Se houver litígio, suspender descarte
Compras/Contratos	Cotações/Contratos	10 anos	Arquivo histórico	Seguir prazos de financiadores
Canal de Denúncias	Casos/Investigações	5 anos após encerramento	Eliminar/anonimizar	Ajustar à lei aplicável
Projetos/Convênios	Prestações de contas	Até 10 anos	Arquivo histórico	Ver cláusulas específicas
Treinamentos	Certificados/Termos	3 anos	Eliminar	Manter relatórios consolidados
Auditorias	Relatórios/CAPA	5 anos	Arquivo histórico	Evidências até eficácia verificada
Privacidade	DPIA/Incidentes	5 anos	Arquivo histórico	Conforme LGPD e autoridade

10.4 Mapa Requisito → Controle → Evidência (exemplos)

Requisito (norma/lei)	Controle/Política	Evidência esperada	Periodicidade
ISO 37001 — Política antissuborno	Política Antissuborno aprovada	Versão no ECM, ata de aprovação	Anual
ISO 37301 — Treinamento	EAD obrigatório e trilhas por risco	Relatórios EAD, certificados, termos	Anual / Mensal
Lei 12.846 — Integridade	Due diligence de terceiros	Dossiês, pareceres, cláusulas	Pré-contratação/Anual

Requisito (norma/lei)	Controle/Política	Evidência esperada	Periodicidade
ISO 37001 — Canal de denúncia	Canal 24/7 com SLA	Protocolos, relatórios, feedbacks	Mensal/Trimestral
ISO 37301 — Auditoria interna	Programa anual	Plano, relatórios, CAPA	Anual/Follow-up

10.5 Dicionário de Indicadores (KPIs/KRIs)

Regra: cada indicador possui **fórmula**, **fonte**, **responsável**, **frequência**, **meta**, **thresholds** (verde/amarelo/vermelho) e **ações padrão**.

10.5.1 Governança & Cultura

Código	Nome	Fórmula	Fonte	Meta	Thresholds
GOV-01	Comunicação da liderança	Nº comunicações/ano	ECM/Comunicados	≥ 6	<4 vermelho; 4–5 amarelo
GOV-02	Cobertura EAD	(Concluídos/Público-alvo)×100	EAD	≥ 95%	<90% vermelho; 90–94% amarelo

10.5.2 Riscos & Due Diligence

Código	Nome	Fórmula	Fonte	Meta	Thresholds
RSK-01	Avaliações de risco concluídas	(% áreas/projetos críticos avaliados)	Matriz de risco	≥ 90%	<75% verm.; 75–89% am.
RSK-03	DD antes da contratação	(% de terceiros de risco com DD prévia)	Sistema DD/ECM	100%	<98% amarelo; <95% verm.
RSK-06	Efetividade de controles	(% testes “eficazes”)	Auditorias	≥ 90%	<80% vermelho

10.5.3 Operação & Canal

Código	Nome	Fórmula	Fonte	Meta	Thresholds
OPR-01	Gates de integridade cumpridos	(% projetos com 100% gates)	Checklists	100 %	<95% amarelo
OPR-03	Reconciliação tempestiva	(% reconciliações no prazo)	Financeiro	100 %	<98% amarelo
OPR-04	Tempo de triagem	Mediana dias (recebimento→triagem)	Canal	≤ 5 dias úteis	>7 vermelho
OPR-05	Tempo de investigação	Mediana dias (abertura→encerramento)	Canal/ECM	≤ 45 dias	>60 vermelho

10.5.4 Conflitos/Brindes/Setor Público

Código	Nome	Fórmula	Fonte	Meta	Thresholds
CIF-01	Declarações anuais	(% entregues)	RH/ECM	≥ 98%	<95% vermelho
BRD-01	Registros conformes	(% registros sem exceção)	Livro Brindes	≥ 95%	<90% vermelho
PUB-01	Interações registradas	(% com ata/agenda)	Registro Público	≥ 95%	<90% vermelho

10.5.5 Melhoria & Auditoria

Código	Nome	Fórmula	Fonte	Meta	Thresholds
MEL-01	NCs no prazo	(% NCs encerradas dentro do prazo)	ECM/CAPA	≥ 90%	<80% vermelho
AUD-01	Execução do plano de auditoria	(% auditorias realizadas)	Auditoria	100%	<95% amarelo

Ações padrão:

- **Amarelo:** plano de reforço do processo/responsável + rechecagem em 30 dias.
- **Vermelho:** escalonamento à Diretoria; revisão de recursos/fluxo; possível auditoria focada.

10.6 Amostragem de Evidências (por risco)

Risco do processo	Tamanho de amostra sugerido	Observações
Alto/Crítico	25–40 itens ou 100% se universo pequeno	Foco em períodos/licitações sensíveis
Médio	10–20 itens	Amostragem aleatória + dirigida
Baixo	5–10 itens	Rotativa entre meses/trimestres

10.7 Qualidade de Dados e Validação

Regras mínimas:

- **Dono do dado** definido por indicador; **dupla checagem** para KPIs críticos.
- **Workflow de validação** (submissão → revisão → aprovação → publicação).
- **Trilhas**: versionamento da série histórica, justificativas para ajustes retroativos.
- **Tratamento de outliers**: política documentada (revisão metodológica vs. erro operacional).

10.8 Dashboards e Relatórios (modelos)

- **Tático (Mensal – Diretoria):** KPIs OPR/RSK/GOV, casos do canal, status de CAPA, mapa de terceiros críticos.
- **Estratégico (Trimestral – Conselho):** tendências, riscos prioritários, auditorias, recursos e decisões pendentes.
- **Projeto/Convênio (Mensal):** gates de integridade por projeto, prestações de contas, achados e lições.

Exportações: PDF “carimbado” com hash/ID da versão; planilhas com dicionário de dados.

10.9 Roteiro de Evidências por Tema Sensível (checklists)

Brindes/Hospitalidades: formulário, aprovação (se aplicável), registro no livro, comprovantes/convites, reconciliação (se houver despesas).

Conflitos de Interesse: declaração anual, análises e medidas (abstenção/substituição), registro em atas.

Relacionamento com Setor Público: ata/agenda com participantes, pauta e resultados; ofícios; e-mails institucionais; registro fotográfico institucional (se pertinente).

Due Diligence de Terceiros: questionário, documentos societários, beneficiário final, checagens negativas, parecer, aprovação, cláusulas contratuais, revalidação.

Canal/Investigações: protocolo, triagem, plano, entrevistas, evidências, parecer, medidas, feedback ao denunciante, lições aprendidas.

Compras/Contratos: mapa de cotações, justificativas, aprovações, contrato, entregas, pagamento, reconciliação.

10.10 Periodicidades Consolidadas (cap. 10)

- **Atualização de indicadores e dashboards: mensal** (críticos) e **trimestral** (estratégicos).
- **Revisão de dicionário de indicadores: anual** ou por mudança relevante.
- **Auditoria de qualidade de dados (spot-check): trimestral**.
- **Revisão da tabela de retenção: anual**.
- **Teste de restauração de backups do ECM: semestral**.

10.11 Papéis e Responsabilidades

Item	Responsável	Apoios	Aprovação
Dicionário de indicadores	Compliance	Donos de processo/TI	Diretoria
Publicação de dashboards	Compliance	TI/Donos	Diretoria
Manutenção da tabela de retenção	Jurídico/Compliance	TI/Áreas	Diretoria
Auditoria de dados	Auditoria/Compliance	Donos/TI	Conselho/Diretoria

11. Anexos Operacionais

11.1 Modelos e Formulários (para ECM)

11.1.1 Declaração de Conflito de Interesses (Modelo)

Metadados: Código doc.; Versão; Vigência; Dono; Classificação (Restrito).
Campos:

1. Identificação (nome, cargo/vínculo, área)
2. Descrição do possível conflito (pessoa/empresa relacionada; relação de parentesco/societária; processo/decisão afetada)
3. Período/recorrência do conflito
4. Medidas propostas (abstenção, substituição, blindagem de informação)
5. Análise de Compliance/Jurídico (parecer e risco)
6. Deliberação do aprovador (Diretoria/Comitê)
7. Registro em ata (nº/data)
8. Assinatura digital

11.1.2 Formulário de Brindes, Presentes e Hospitalidades

Campos: Data; Parte ofertante/recebedora; Descrição; Valor estimado; Finalidade/ocasião; Processo/negociação em curso? (sim/não); Enquadra nos limites? (sim/não); Aprovação prévia (se aplicável: nome/data); Decisão (aceito/recusado/doado); Observações; Registro no Livro (ID).

11.1.3 Checklist de Compras/Contratos

Itens mínimos:

- Requisição aprovada; 3 cotações comparáveis (ou justificativa); análise técnica; due diligence concluída conforme risco; parecer de Compliance (quando gatilhos); minuta padrão com cláusulas de integridade; aprovação final; recebimento/aceite; pagamento com documentos; reconciliação; arquivamento.

  Campo de exceções: descrição, motivo, aprovações, data.

11.1.4 Dossiê de Due Diligence de Terceiros (Capa Padrão)

Seções:
A) Identificação e classificação de risco (baixo/médio/alto/crítico)

B) Documentos societários e beneficiário final

C) Checagens (sanções, mídia negativa, restrições setoriais)

D) Referências e histórico

E) Avaliação de integridade financeira (quando aplicável)

F) Entrevistas/visitas (alto/crítico)

G) Parecer (apto / apto com mitigação / inapto) + mitigadores

H) Cláusulas contratuais especiais

I) Plano de monitoramento e gatilhos de revalidação

J) Aprovações e assinaturas digitais

11.1.5 Plano de Investigação Interna (Template)

Campos: Protocolo do caso; Natureza (suborno/fraude/conflito/outro); Criticidade; Equipe (sem conflito); Escopo e objetivos; Metodologia (documentos, entrevistas, forense); Cronograma e SLA; Cadeia de custódia; Regras de confidencialidade/LGPD; Relatórios intermediários; Produto final; Armazenamento e retenção.

11.1.6 Relatório Conclusivo de Investigação (Template)

Estrutura: Resumo executivo; Metodologia; Fatos apurados; Evidências; Análise (nexos, políticas/leis aplicáveis); Conclusões; Responsabilidades; Recomendações (disciplinares/contratuais/processuais/autoridades); Plano de ação (se aplicável); Comunicação ao denunciante (quando possível); Anexos.

11.1.7 CAPA — Ação Corretiva (Modelo)

Campos: Nº da NC; Origem (auditoria, denúncia, indicador, projeto); Descrição; Causa-raiz (5 Porquês/Ishikawa); Ações (o que/quem/quando/recursos); Critério de eficácia; Evidências esperadas; Prazo; Status; Resultado da verificação de eficácia; Encerramento.

11.1.8 Checklist de Prestação de Contas (Convênios/Projetos)

Itens: Plano aprovado; Execução vs. orçamento; Documentos fiscais; Entregas/outputs; Amostragem de pagamentos; Conformidade de compras; Relatórios técnicos; Assinaturas; Prazos; Respostas a diligências; Arquivamento.

11.1.9 Termo de Ciência e Adesão ao Código/Políticas

Conteúdo: Declaração de leitura e concordância; compromisso de reporte de boa-fé; ciência sobre canal e não retaliação; concordância com sanções por violação; assinatura digital; data.

11.1.10 Cláusulas Contratuais Padrão (pacote)

- Anticorrupção e antissuborno (proibição e deveres)
- Direito de auditoria
- Rescisão por justa causa e sanções
- Beneficiário final / alterações societárias

- Não subcontratação sem anuência
- Proteção ao denunciante e acesso ao canal
- Proteção de dados (LGPD) e confidencialidade

11.2 Roteiro de Treinamento Anual (EAD) e Termos

11.2.1 Trilhas Obrigatórias (por público)

- **Todos**: Introdução ao Compliance e Antissuborno; Canal e Não Retaliação; Conflitos de Interesse; Brindes/Hospitalidades; Relacionamento com Setor Público; LGPD básica.
- **Gestores**: Tom do topo; Segregação de funções; Consequências; Gestão de exceções.
- **Compras/Contratos**: Integridade nas aquisições; Due diligence; Cláusulas padrão.
- **Projetos/Convênios**: Gates de integridade; Prestação de contas; Interações públicas.
- **Financeiro**: Reconciliação; trilhas de auditoria; prevenção a fraudes.
- **Terceiros críticos** (quando contratualmente cabível): Conduta esperada; uso do canal; cláusulas.

11.2.2 Grade e Metas

- Carga mínima **anual** por trilha; reciclagem por risco; **meta de cobertura ≥ 95%**.
- Avaliação de aprendizagem (pós-teste ≥ 80%).
- **Assinatura digital** de termos ao final (gerada automaticamente).

11.2.3 Termos Padrão (para EAD)

- **Termo de Ciência do Código e Políticas** (11.1.9)
- **Termo de Confidencialidade** (para acesso a casos sensíveis)
- **Termo de Não Retaliação** (para líderes/gestores)

11.3 Tabela de Classificação de Riscos (exemplo para matriz)

Nível	Descrição	Probabilidade (P)	Impacto (I)	NR = P×I	Tratamento e Escalonamento
Crítico	Risco com potencial de dano	5	5	25	Evitar/reduzir imediatamente;

Nível	Descrição	Probabilidade (P)	Impacto (I)	NR = P×I	Tratamento e Escalonamento
	legal/reputacional severo ou uso de recursos públicos				Diretoria/Conselho; auditoria dirigida
Alto	Exposição relevante e controle insuficiente	4–5	4–5	16–20	Plano de ação curto; reporte à Diretoria; monitoramento mensal
Médio	Exposição moderada ou controlada	3	3–4	9–12	Mitigar; acompanhamento trimestral
Baixo	Exposição pequena e bem controlada	1–2	1–2	1–4	Aceitar com monitoramento anual

Escalas detalhadas (referência):
P: 1 Rara | 2 Improvável | 3 Possível | 4 Provável | 5 Quase certa
I: 1 Insignificante | 2 Baixo | 3 Moderado | 4 Alto | 5 Crítico

11.4 Fluxogramas (representação textual simplificada)

11.4.1 Denúncias e Investigações

Recebimento (canal 24/7) → Triagem (SLA até 5 dias úteis; classificação por criticidade) → Plano de investigação (equipe sem conflito) → Coleta de evidências/entrevistas → Parecer (conclusões e recomendações) → Medidas (disciplinares/contratuais/processuais; reporte a autoridades se cabível) → Feedback ao denunciante (quando possível) → Encerramento → Lições aprendidas (EAD).

11.4.2 Compras e Contratações

Requisição → Análise e cotações → Due diligence por risco → Parecer de Compliance (se gatilho) → Aprovação → Contrato com cláusulas → Entrega/recebimento → Pagamento → Reconciliação → Arquivamento.

11.4.3 Doações/Patrocínios/Parcerias

Proposta → Due diligence da entidade beneficiária → Aprovação com metas/indicadores → Execução e monitoramento → Prestação de contas → Avaliação de impacto → Encerramento (lições aprendidas).

11.4.4 Conflitos de Interesses

Identificação → Declaração → Análise e parecer → Medidas (abstenção/substituição/blindagem) → Registro em ata → Monitoramento.

11.4.5 Relacionamento com Setor Público

Agendamento oficial → Reunião (preferencialmente com 2 representantes) → Ata com participantes/pauta/decisões → Protocolos/Ofícios → Registro no ECM → Prestação de contas (se aplicável).

11.5 Glossário de Termos

Apetite a risco: nível de risco residual que a Alta Direção admite conscientemente.
Ação corretiva (CAPA): ação para eliminar causa-raiz de não conformidade ou incidente.
Canal de denúncias: meio independente para relatar violações de boa-fé, com proteção ao denunciante.

Conflito de interesses: situação em que interesse privado pode influenciar decisão institucional.
Due diligence (DD): diligência prévia proporcional ao risco para avaliar integridade de terceiros.
Gates de integridade: pontos de controle obrigatórios ao longo do ciclo de projetos/convênios.
Pagamentos de facilitação: vantagens indevidas para agilizar ato público — **proibidos**.

Parte interessada: pessoa/grupo que pode afetar ou ser afetado pelo SGC/SGAS.
Risco de integridade: possibilidade de evento (suborno, fraude, descumprimento) afetar objetivos.
Tom do topo: liderança ativa da Alta Direção em favor da integridade.
Tratamento de riscos: evitar, reduzir, compartilhar/transferir ou aceitar com monitoramento.

12. Matriz de Conformidade

12.1 ISO 37001 — Sistema de Gestão Antissuborno

Bloco 1 (itens 4.1 a 6.2)

Nº do Item	Descrição (requisito)	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
4.1	Entendimento da organização e seu contexto	Contexto influencia exposição a risco de suborno	Total	Cap. 2 mapeia PESTLE, SWOT, processos e heatmap de integridade	Relatório de Contexto; PESTLE/SWOT; Heatmap no ECM; ata de aprovação

Nº do Item	Descrição (requisito)	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
4.2	Partes interessadas e expectativas	Requisitos de doadores/órgãos de controle impactam controles	Total	Cap. 2.2 matriz de stakeholders e requisitos; comunicação dedicada	Matriz de Stakeholders; evidências de comunicação; pesquisas/feedbacks
4.3	Escopo do SGAS	Define onde o sistema se aplica	Total	Cap. 2.3 declaração de escopo, exclusões e interfaces	Declaração de Escopo aprovada; diagrama de cobertura; RACI
4.4	Sistema de gestão antissuborno	Estabelecer, implementar, manter e melhorar	Total	Manual (MA-003) + políticas operacionais (Cap. 9) integradas ao SGC	Política Antissuborno; POPs; registros no ECM; revisão anual
5.1	Liderança e comprometimento	"Tom do topo" e recursos	Total	Cap. 3.1; mensagens da Alta Direção; acesso direto de Compliance ao Conselho	Atas; comunicados; orçamento dedicado; carta de mandato de Compliance
5.2	Política antissuborno	Diretrizes e proibições formais	Total	Cap. 3.2 e 9.2; proibição de facilitação; critérios p/ brindes/doações	Política aprovada; aceite digital; campanhas; evidências de divulgação
5.3	Papéis, responsabilidades e autoridades	Clarificar responsabilidades e independência	Total	Cap. 3.3 (RACI); Compliance com autonomia técnica e	RACI; organograma; termo de nomeação; atas do Comitê de Integridade

Nº do Item	Descrição (requisito)	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
				reporte ao Conselho	
6.1	Ações para abordar riscos e oportunidades	Basear controles no risco	Total	Cap. 4.1 metodologia; plano de tratamento vinculado a heatmap	Plano anual de riscos; heatmap; planos de ação; follow-up
6.2	Objetivos antissuborno e planejamento	Metas mensuráveis e plano	Total	Cap. 4.3 objetivos SMART (canal, DD, compras, PC) e cronograma	Quadro de objetivos; dashboards; relatórios de progresso

Bloco 2 — Seção 7 (Apoio)

Nº do Item	Descrição (requisito)	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
7.1	Recursos	Garantir meios adequados ao SGAS	Total	Cap. 5.1 define orçamento, pessoas, TI (canal 24/7, ECM, DD, EAD)	Peça orçamentária; contratos de ferramentas; organograma; plano de recursos
7.2	Competência	Pessoas aptas às funções críticas	Total	Cap. 5.2 matriz de competências e trilhas por risco/função	Plano anual de treinamento; certificados EAD; avaliações de

Nº do Item	Descrição (requisito)	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
					aprendizagem
7.3	Conscientização	Todos conhecem políticas/condutas	Total	Cap. 5.3 campanhas, pílulas, comunicados da liderança	Newsletters; campanhas; registros de alcance
7.4	Comunicação	Canais internos e externos eficazes	Total	Cap. 5.3 e 5.6 (canal 24/7; proteção ao denunciante)	Política do canal; relatórios trimestrais; prints do site/intranet
7.5	Informação documentada	Controle de docs e registros	Total	Cap. 5.4 (ECM, metadados, versão) + Cap. 10 (retenção)	Política documental; logs de acesso; tabela de retenção; backups

Bloco 3 — Seção 8 (Operação)

Nº do Item	Descrição (requisito)	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
8.1	Planejamento e controle operacional	Controlar riscos por processo/projeto	Total	Cap. 6.1 “gates de integridade” e exceções registradas	Planos de controle; checklists por gate; relatório de exceções
8.2	Due diligence	Avaliar terceiros proporcional ao risco	Total	Cap. 5.5 (classificação baixo/médio/alto/crítico) e 6.3 (reforçada)	Dossiês DD; pareceres; revalidaçõe

Nº do Item	Descrição (requisito)	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
					s; cláusulas contratuais
8.3	Controles antissuborno	Políticas e procedimentos específicos	Total	Cap. 6.2 (brindes/hosp., conflitos, facilitação proibida, setor público)	Livro de brindes; declarações de conflito; atas; registros de interação
8.4	Controles financeiros e não financeiros	Rastreabilidade e segregação	Total	Cap. 6.2.5 (cotações, reconciliação, cartão/caixa miúdo)	Mapas de cotação; reconciliações; logs de aprovação
8.5	Doações, patrocínios e benefícios	Prevenir uso indevido	Quando aplicável	Cap. 9.5 (critérios, rastreabilidade) e 6.4 (projetos/PC)	Contratos; relatórios; comprovações de entrega
8.6	Gestão de investigações	Responder a suspeitas/violações	Total	Cap. 6.5 (fluxo; SLAs; cadeia de custódia; LGPD)	Protocolos; planos; relatórios conclusivos; medidas aplicadas
8.7	Medidas disciplinares e corretivas	Consequências proporcionais	Total	Cap. 3.6 e 9.8 (devido processo; gradação)	Registros disciplinares; deliberações; comunicação às partes
8.8	Relacionamento com agentes públicos	Integridade nas interações	Quando aplicável	Cap. 6.2.4 e 9.7 (agenda, dois representantes, atas)	Agendas/atas; ofícios; e-mails institucionais

Nº do Item	Descrição (requisito)	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
8.9	Canal de denúncia	Acesso seguro/independente	Total	Cap. 5.6 (24/7; anonimato; não retaliação; SLAs)	Relatórios do canal; registros de feedback; estatísticas

Bloco 4 — Seções 9 (Avaliação de Desempenho) e 10 (Melhoria)

Nº do Item	Descrição (requisito)	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
9.1	Monitoramento, medição, análise	Acompanhar eficácia do SGAS	Total	Cap. 7.1 (painéis, métodos, qualidade de dados)	Dashboards; metodologia; atas de acompanhamento
9.2	Auditoria interna	Verificação independente	Total	Cap. 7.2 (programa anual, amostragem, follow-up)	Planos; relatórios; matriz de achados; CAPA
9.3	Análise crítica da direção	Decisões estratégicas	Total	Cap. 7.3 (inputs/outputs; roteiro; decisões)	Ata; lista de decisões; plano de ação
10.1	Não conformidade e ação corretiva	Prevenir recorrência	Total	Cap. 8.3 (fluxo NC→CAPA; eficácia)	Tickets/NC; análises de causa; verificação de eficácia
10.2	Melhoria contínua	Evoluir o SGAS	Total	Cap. 8.4/8.5 (OM; integração com riscos/mudanças)	Backlog de OM; pilotos; atualizações de políticas/POPs

12.2 ISO 37301 — Sistema de Gestão de Compliance

Bloco 1 — Seção 4 (Contexto da organização)

Nº do Item	Descrição (requisito)	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
4.1	Entendimento da organização e de seu contexto	Contexto condiciona requisitos e riscos de compliance	Total	Cap. 2.1 (PESTLE, SWOT, mapa de processos)	Relatório de Contexto; PESTLE/SWOT; atas de aprovação
4.2	Necessidades e expectativas das partes interessadas	Requisitos de stakeholders direcionam controles	Total	Cap. 2.2 (matriz de partes interessadas e requisitos)	Matriz de stakeholders; comunicações; pesquisas/feedback
4.3	Escopo do SGC	Define abrangência e fronteiras do SGC	Total	Cap. 2.3 (declaração de escopo e interfaces)	Declaração de escopo; diagrama de cobertura; RACI
4.4	Sistema de gestão de compliance	Estabelecer, implementar, manter e melhorar	Total	O MA-003 integra políticas (Cap. 9), riscos (Cap. 4), operação (Cap. 6)	Políticas publicadas; procedimentos; revisão anual

Bloco 2 — Seção 5 (Liderança)

Nº do Item	Descrição	Justificativa	Aplicabilidade	Como atende	Evidências possíveis
5.1	Liderança e comprometimento	“Tom do topo” e integração à estratégia	Total	Cap. 3.1 (mensagens, recursos, acesso de Compliance ao Conselho)	Atas; comunicados; orçamento; carta de mandato

Nº do Item	Descrição	Justificativa	Aplicabilidade	Como atende	Evidências possíveis
5.2	Política de compliance	Princípios e compromissos formais	Total	Cap. 3.2 e 9.1/9.2 (Política de Compliance/Antissuborno)	Política aprovada; aceite digital; campanhas
5.3	Papéis, responsabilidades e autoridades organizacionais	Clareza de papéis e independência	Total	Cap. 3.3 (RACI, independência, reporte direto)	RACI; organograma; termos de nomeação
5.4	Função de compliance	Autoridade, independência e recursos	Total	Cap. 3.3/3.5 (estrutura, competências, recursos)	Descrição de cargo; estrutura; acesso ao Conselho

Bloco 3 — Seção 6 (Planejamento)

Nº do Item	Descrição	Justificativa	Aplicabilidade	Como atende	Evidências possíveis
6.1	Ações para tratar riscos e oportunidades	Enfoque baseado em risco	Total	Cap. 4.1/4.2 (metodologia, heatmap, plano de tratamento)	Matriz de riscos; planos; heatmap no ECM
6.2	Objetivos de compliance e planejamento	Metas mensuráveis e planos	Total	Cap. 4.3 (objetivos SMART, cronograma, recursos)	Quadro de objetivos; dashboards; relatórios
6.3	Planejamento de mudanças	Controlar impactos de mudanças	Total	Cap. 4.4 (fluxo de mudança, avaliação de impacto)	Formulários de mudança; pareceres; aprovações

Bloco 4 — Seção 7 (Apoio)

Nº do Item	Descrição	Justificativa	Aplicabilidade	Como atende	Evidências possíveis
7.1	Recursos	Garantir meios suficientes	Total	Cap. 5.1 (orçamento, pessoas, TI: ECM/EAD/canal/DD)	Plano de recursos; contratos; organograma
7.2	Competência	Pessoas aptas ao papel	Total	Cap. 5.2 (matriz de competências; trilhas EAD)	Certificados; listas de presença; avaliações
7.3	Conscientização	Conhecimento das obrigações	Total	Cap. 5.3 (plano de comunicação, pílulas)	Newsletters; prints; relatórios de alcance
7.4	Comunicação	Interna e externa eficaz	Total	Cap. 5.3/5.6 (canais; proteção ao denunciante)	Política do canal; relatórios; página institucional
7.5	Informação documentada (geral)	Documentos e registros controlados	Total	Cap. 5.4 (ECM, metadados, versões) e Cap. 10 (retenção)	Política documental; logs; backups
7.5.3	Controle de informação documentada	Disponibilidade, proteção, retenção	Total	Cap. 10.3 (tabela de retenção)	Tabela de retenção; evidência de descarte/arquivamento

Bloco 5 — Seção 8 (Operação)

Nº do Item	Descrição	Justificativa	Aplicabilidade	Como atende	Evidências possíveis
8.1	Planejamento e controle operacionais	Fazer o SGC “acontece	Total	Cap. 6.1 (gates por ciclo de projeto/convê	Checklists; relatórios; log de exceções

Nº do Item	Descrição	Justificativa	Aplicabilidade	Como atende	Evidências possíveis
		r" nos processos		nio; exceções controladas)	
8.2	Due diligence e controles por risco	Prevenir violações via terceiros	Total	Cap. 5.5/6.3 (classificação e DD reforçada)	Dossiês DD; pareceres; cláusulas
8.3	Procedimentos e controles de compliance	Padronização de práticas	Total	Cap. 9 (políticas específicas) + Cap. 6 (controles operacionais)	Políticas/POPs; registros; auditorias
8.4	Preparação e resposta a não conformidades	Resiliência operacional	Total	Cap. 6.5 (investigações), 8.3 (CAPA)	Protocolos; relatórios; CAPAs
8.5	Terceirização/outsourcing	Manter controle sobre processos	Quando aplicável	Cap. 2.3.2 (exclusões), 5.8 (cláusulas), 5.5 (monitoramento)	Contratos; SLAs; auditorias de fornecedores

Bloco 6 — Seção 9 (Avaliação de desempenho)

Nº do Item	Descrição	Justificativa	Aplicabilidade	Como atende	Evidências possíveis
9.1	Monitoramento, medição, análise e avaliação	Acompanhar eficácia do SGC	Total	Cap. 7.1 (painéis; metodologia e qualidade de dados)	Dashboards; dicionário de indicadores; atas
9.2	Auditoria interna	Verificação independente	Total	Cap. 7.2 (programa anual;	Planos; relatórios; matriz de achados

Nº do Item	Descrição	Justificativa	Aplicabilidade	Como atende	Evidências possíveis
				amostragem; follow-up)	
9.3	Análise crítica da direção	Direção decide com base em evidência	Total	Cap. 7.3 (inputs/outputs; decisões e priorizações)	Ata; decisões; plano do próximo ciclo

Bloco 7 — Seção 10 (Melhoria)

Nº do Item	Descrição	Justificativa	Aplicabilidade	Como atende	Evidências possíveis
10.1	Não conformidade e ação corretiva	Remover causa e evitar recorrência	Total	Cap. 8.3 (fluxo NC→CAPA; eficácia; prazos)	Tickets/NC; análises de causa; verificação de eficácia
10.2	Melhoria contínua	Evolução sustentada	Total	Cap. 8.4/8.5/8.6 (OM; integração com riscos/mudanças; lições aprendidas)	Backlog de OM; pilotos; atualizações de documentos

12.3 Matriz de Conformidade Legal — Lei 12.846/2013 e Decreto 11.129/2022

Bloco 1 — Lei nº 12.846/2013 (itens principais 1 a 10)

Nº do Item	Descrição	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
1	**Responsabilização objetiva** da pessoa jurídica	A lei prevê responsabilização	Total	Cap. 3 (governança), 6 (controles), 7–8	Políticas aprovadas; matriz de

Nº do Item	Descrição	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
	por atos lesivos contra a Adm. Pública	**independente de dolo/culpa**		(monitorar e corrigir) estruturam prevenção e resposta	riscos; auditorias; relatórios ao Conselho
2	**Atos lesivos** tipificados (art. 5º)	Define condutas proibidas (prometer/oferecer vantagem indevida etc.)	Total	Cap. 9.2 (Política Antissuborno) com proibições explícitas e medidas	Política Antissuborno; aceite digital; campanhas; registros de treinamento
3	**Sanções administrativas** (multa e publicação extraordinária da decisão)	Necessita mecanismos para resposta e transparência	Total	Cap. 6.6 (cooperação com autoridades) e 7.4 (relato)	Comunicações oficiais; comprovantes de publicação; atas de deliberação
4	**Acordo de leniência** (arts. 16–17)	Exige critérios de colaboração e cessação do ilícito	Quando aplicável	Cap. 6.5/6.6 definem fluxo decisório (Jurídico/Conselho) e guarda de evidências	Parecer jurídico; decisão do Conselho; registros de cooperação
5	**Cálculo de multa** com atenuantes/agravantes (programa de integridade, cooperação)	Programa efetivo reduz penalidades	Total	Cap. 3–8 implementam SGC/SGAS e demonstram efetividade (KPIs)	Painéis de indicadores; auditorias; CAPAs eficazes
6	**Ressarcimento integral** do dano	Obrigação de reparar prejuízos	Quando aplicável	Cap. 6.5 (investigações) e 8 (melhoria/correções)	Relatórios conclusivos; comprovações de ressarcimento

Nº do Item	Descrição	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
7	**Publicação da decisão condenatória**	Transparência e efeito pedagógico	Quando aplicável	Cap. 7.4 (relato e transparência)	Comprovantes de publicação; prints; protocolo
8	**Competência de órgãos** para apuração/sanção	Necessidade de interação formal	Total	Cap. 6.6 centraliza interface com autoridades	Ofícios; protocolos; matriz de documentos enviados
9	**Ampla defesa e contraditório** no âmbito administrativo	Devido processo e robustez probatória	Total	Cap. 6.5 (fluxo de investigação) e 9.8 (medidas disciplinares com devido processo)	Planos de investigação; cadeia de custódia; pareceres; decisões fundamentadas
10	**Responsabilidade solidária** (consórcios/grupos de fato)	Requer due diligence reforçada e cláusulas contratuais	Quando aplicável	Cap. 5.5/6.3 (DD reforçada) e 5.8 (cláusulas)	Dossiês de DD; contratos com cláusulas; revalidações

Bloco 2 — Decreto nº 11.129/2022 (Programa de Integridade: critérios 1 a 10)

Nº do Item	Critério do Programa de Integridade (Decreto)	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
1	**Comprometimento da alta direção** (“tom do topo”)	Critério central de efetividade	Total	Cap. 3.1/3.4 (mensagens, recursos, acesso ao Conselho)	Atas; comunicados; orçamento; plano anual

Nº do Item	Critério do Programa de Integridade (Decreto)	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
2	**Padrões de conduta, código e políticas**	Regras claras e divulgadas	Total	Cap. 9.1–9.10 (pacote de políticas)	Políticas aprovadas; aceite digital; revisões anuais
3	**Treinamentos periódicos**	Disseminar cultura e orientar condutas	Total	Cap. 5.2/11.2 (EAD anual, trilhas por risco)	Catálogo EAD; certificados; taxa de cobertura
4	**Canais de denúncia acessíveis**	Mecanismo de detecção e resposta	Total	Cap. 5.6 (24/7; anonimato; SLAs; não retaliação)	Protocolos; relatórios do canal; feedbacks
5	**Proteção ao denunciante & não retaliação**	Garantir segurança e confiança	Total	Cap. 9.9 (política dedicada)	Registros de proteção; investigações de retaliação
6	**Medidas disciplinares proporcionais**	Consequências coerentes e graduadas	Total	Cap. 3.6/9.8 (matriz de penalidades; devido processo)	Registros disciplinares; deliberações; rastreabilidade
7	**Análise de perfil e riscos**	Base para controles proporcionais	Total	Cap. 4.1–4.2 (metodologia, heatmap, apetite/tolerância)	Matriz de riscos; planos de tratamento
8	**Registros contábeis e controles internos confiáveis**	Prevenir/identificar irregularidades	Total	Cap. 6.2.5 (rastreabilidade, reconciliaçã	Reconciliações; logs; trilhas de auditoria

Nº do Item	Critério do Programa de Integridade (Decreto)	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
				o); 10 (evidências)	
9	**Procedimentos específicos para licitações/contratos públicos**	Risco elevado em interação com poder público	Quando aplicável	Cap. 6.2.4 (regras de interação), 6.4 (gates em convênios), 9.7 (política)	Atas/agenda oficial; ofícios; checklists por gate
10	**Due diligence de terceiros e PEPs**	Mitigar riscos por intermediários/representantes	Total	Cap. 5.5/6.3 (DD por risco; reforçada para críticos)	Dossiês, pareceres, revalidações; cláusulas

Bloco 3 — Decreto nº 11.129/2022 (Programa de Integridade: critérios 11 a 20)

Nº do Item	Critério do Programa de Integridade (Decreto)	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
11	**Gestão de doações, patrocínios e contribuições**	Área sensível a desvio/finalidade	Quando aplicável	Cap. 9.5 (critérios e rastreabilidade), 6.4 (gates)	Contratos; relatórios; comprovações
12	**Transparência e comunicação externa**	Prestação de contas à sociedade	Total	Cap. 7.4 (relato), 3.7 (comunicação), 10 (indicadores)	Relatórios; site; publicações
13	**Independência, autonomia e recursos da função de compliance**	Efetividade e isenção	Total	Cap. 3.3/3.5 (carta de mandato, acesso, orçamento)	Nomeação; organograma; plano de recursos
14	**Monitoramento contínuo e auditoria**	Testar eficácia e corrigir rumos	Total	Cap. 7.1–7.2 (monitorar e auditar)	Dashboards; relatórios;

Nº do Item	Critério do Programa de Integridade (Decreto)	Justificativa	Aplicabilidade	Como atende (síntese do MA-003)	Evidências possíveis
					matriz de achados
15	**Gestão de consequências a terceiros**	Sanções contratuais por violação	Total	Cap. 5.8 (cláusulas), 9.6 (contratações/DD)	Contratos; registros de sanções; rescisões
16	**Controles para brindes, hospitalidades e despesas**	Prevenir vantagem indevida	Total	Cap. 6.2.1 (limites/registro), 10.9 (checklist)	Livro de brindes; formulários; aprovações
17	**Gestão de conflitos de interesse**	Decisões íntegras	Total	Cap. 6.2.2 e 9.3 (declaração anual, abstenção)	Declarações; atas; log de impedimentos
18	**Reação a indícios de irregularidades (investigar e remediar)**	Reduz dano e previne repetição	Total	Cap. 6.5 (investigações), 8 (CAPA)	Planos e relatórios; CAPAs; verificação de eficácia
19	**Integração com privacidade e proteção de dados (LGPD)**	Denúncias/DD tratam dados pessoais	Total	Cap. 5.10 (LGPD), 6.5 (confidencialidade), 10 (retenção)	Inventário de tratamentos; avisos; logs de acesso
20	**Ajustes proporcionais ao porte e risco da organização**	Critério de proporcionalidade	Total	Todo o MA-003 usa proporcionalidade (riscos, DD, metas)	Metodologia; justificativas de escala; decisões em atas