

MGCIA

Modelo de Governança Corporativa na Era da Inteligência Artificial

Versão 1.0

AUTORES

João Souza Neto

José Carneiro de Carvalho Neto

Ricardo Alexandre Santos Brasil

Gustavo Ramirez

Sumário

- 1** Resumo Executivo
 - 2** Fundamentação Conceitual
 - 3** Matriz Manter — Adaptar — Criar
 - 4** Princípios do MGCI
 - 5** Arquitetura do MGCI
 - 6** Descrição Detalhada de Cada Domínio
 - 7** Papéis e Responsabilidades — Visão Consolidada
 - 8** Modelo de Tomada de Decisão
 - 9** Gestão e Supervisão de Riscos
 - 10** Monitoramento e Indicadores
 - 11** Assurance
 - 12** Aplicação Proporcional do Modelo
 - 13** Tratamento Específico da IA Agêntica
-

1. Resumo Executivo

O MGCIA — Modelo de Governança Corporativa na Era da Inteligência Artificial — propõe como a governança corporativa brasileira deve evoluir para que Conselhos de Administração, Alta Administração e demais estruturas de governança possam direcionar, supervisionar e monitorar adequadamente o uso da IA, seus riscos, oportunidades, impactos e geração de valor.

O modelo preserva a lógica, os princípios e a estrutura do Código das Melhores Práticas de Governança Corporativa do IBGC (6ª edição) — não o substitui nem cria uma governança paralela. Ele identifica onde a IA exige que elementos do Código sejam mantidos, adaptados ou criados (Matriz MANTER-ADAPTAR-CRIAR, Seção 3), e organiza a resposta em 8 domínios de governança, cada um com responsabilidades específicas para Conselho, Alta Administração e Gestão.

O delta mais significativo identificado é a IA agêntica: sistemas que agem de forma autônoma e assíncrona em nome da organização não têm paralelo direto no Código IBGC atual e, por isso, recebem tratamento dedicado na Seção 13, que abrange autonomia, identidade, privilégios, delegação, supervisão humana, rastreabilidade e reversibilidade.

O MGCIA é proporcional: uma pequena empresa que usa IA de forma limitada não precisa implementar os 8 domínios com a mesma profundidade que uma instituição financeira que usa agentes autônomos nas decisões de crédito. A Seção 12 detalha essa aplicação proporcional.

2. Fundamentação Conceitual

2.1 Premissa metodológica

O MGCIA parte da premissa de que a Governança Corporativa não deve ser substituída por uma "Governança de IA" paralela. A IA é um novo objeto de supervisão — como já foram, em seu tempo, a tecnologia da informação, os riscos ambientais e a conduta ética — e deve ser absorvida pelos mesmos órgãos, papéis e princípios que já governam a organização, com as adaptações estritamente necessárias.

3. Matriz Manter — Adaptar — Criar

Esta matriz indica, para cada elemento do Código IBGC, se a IA exige que ele seja mantido como está, adaptado ao seu escopo ou que um elemento inteiramente novo seja criado.

Elemento do Código IBGC / da governança corporativa	Classificação	Justificativa
Princípio da Integridade	MANTER	Aplica-se integralmente; ganha relevância quando decisões passam a ser tomadas com apoio de sistemas autônomos.
Princípio da Transparência	ADAPTAR	Precisa passar a cobrir a explicabilidade algorítmica, não apenas a divulgação financeira e societária.
Princípio da Equidade	ADAPTAR	Precisa passar a cobrir o viés algorítmico e o tratamento desigual gerados por sistemas automatizados.
Princípio da Responsabilização	ADAPTAR	Precisa assumir a responsabilidade por ações executadas por agentes de IA em nome de humanos.

Elemento do Código IBGC / da governança corporativa	Classificação	Justificativa
Princípio da Sustentabilidade	MANTER	O conceito amplo de impacto sobre stakeholders já abrange os impactos sociais da IA.
Papel do Conselho (direcionar e monitorar)	ADAPTAR	O papel se mantém, mas exige uma nova competência: literacia em IA para supervisionar de forma não protocolar.
Estrutura de auditoria e controles internos	ADAPTAR	Precisa passar a auditar novos objetos: modelos, dados de treinamento, logs de decisão de agentes.
Gestão de riscos (COSO ERM)	ADAPTAR	É preciso incorporar formalmente duas novas categorias: risco algorítmico e risco agêntico.
Conduta e conflito de interesses	MANTER	Aplica-se às decisões humanas sobre a adoção e o uso de IA, sem necessidade de reformulação.
Matriz de direitos decisórios sobre IA	CRIAR	O Código atual não define quem decide sobre o uso de um sistema autônomo — conceito que está ausente.
Identidade, privilégios e ciclo de vida de agentes autônomos	CRIAR	Elemento inteiramente novo, sem equivalente em nenhuma estrutura tradicional de governança corporativa.
Supervisão humana proporcional à autonomia	CRIAR	Não existe, no Código IBGC, o conceito de calibrar supervisão à reversibilidade de uma ação automatizada.
Governança de dados e ciclo de vida de modelos	CRIAR	Controles internos tradicionais não contemplam a qualidade nem a proveniência dos dados de treinamento.
Mecanismo de interrupção e reversibilidade de ações agênticas	CRIAR	Não há, na governança corporativa tradicional, o conceito de "parar" uma decisão em execução autônoma.

4. Princípios do MGCIA

O MGCIA preserva os cinco princípios do Código IBGC e adiciona quatro princípios específicos, necessários para tratar os elementos classificados como CRIAR na Seção 3.

4.1 Princípios preservados do Código IBGC

- Integridade, Transparência, Equidade, Responsabilização e Sustentabilidade — mantidas com o escopo ampliado descrito na Matriz MANTER-ADAPTAR-CRIAR.

4.2 Princípios específicos do MGCIA

- Supervisão Humana Proporcional:** o nível de intervenção humana em uma decisão de IA deve ser proporcional à reversibilidade, ao escopo dos dados e ao impacto potencial da ação.
- Explicabilidade Proporcional ao Risco:** decisões de IA de maior impacto devem ser explicáveis em linguagem acessível a não especialistas, e não apenas tecnicamente defensáveis.
- Confiança Verificável:** a confiança depositada em um sistema de IA deve ser sustentada por evidências auditáveis — rastreabilidade das decisões, testes de viés, logs — e não apenas por afirmações do fornecedor ou da área técnica.
- Resiliência Algorítmica:** a organização deve ser capaz de detectar, interromper e se recuperar de uma falha de IA, incluindo a capacidade técnica e organizacional de reverter uma ação automatizada.

5. Arquitetura do MGCIA

O MGCIA se organiza em 8 domínios, mapeados aos capítulos do Código IBGC, preservando a lógica dos órgãos de governança do modelo original.

Domínio	Capítulo IBGC correspondente	Pergunta central que o domínio responde
1. Estratégia e Geração de Valor com IA	Cap. 1 — Fundamentos / Cap. 2 — Sócios	Como pretendemos gerar valor com IA?
2. Direcionamento e Apetite a Risco de IA	Cap. 3 — Conselho de Administração	Quais riscos de IA estamos dispostos a aceitar?
3. Papéis, Responsabilidades e Direitos Decisórios	Cap. 3–4 — Conselho / Diretoria	Quem pode decidir sobre o uso da IA?
4. Dados, Modelos e Ciclo de Vida da IA	Cap. 4 — Gestão (controles internos)	Como sabemos se os dados e os modelos são confiáveis?
5. Supervisão Humana e Autonomia de Agentes	Sem equivalente direto — domínio novo	Como governamos sistemas de IA com diferentes níveis de autonomia?
6. Riscos, Conformidade e Terceiros	Cap. 5 — Órgãos de fiscalização e controle	Como tratamos os riscos de IA e os fornecedores de IA?
7. Transparência, Accountability e Stakeholders	Cap. 6 — Conduta	Como asseguramos transparência e accountability perante quem é afetado pela IA?
8. Monitoramento, Indicadores e Assurance	Cap. 5 — Auditoria / Conselho Fiscal	Como verificamos se a governança de IA está efetivamente funcionando?

6. Descrição Detalhada de Cada Domínio

DOMÍNIO 1 Estratégia e Geração de Valor com IA

Objetivo	Assegurar que o uso da IA esteja explicitamente conectado ao propósito e à estratégia de geração de valor de longo prazo da organização, evitando adoção oportunista ou desconectada do negócio.
Justificativa	O Código IBGC parte do princípio de que a governança existe para preservar e otimizar o valor econômico de longo prazo. A IA introduz uma nova fonte de valor (produtividade, novos produtos, eficiência) e uma nova fonte de risco de destruição de valor (decisões automatizadas erradas em escala), o que exige que a tese de valor seja explicitada, e não presumida.
Princípios relacionados	Integridade; Sustentabilidade; Responsabilização.
Responsabilidades do Conselho	Aprovar a tese estratégica de uso de IA e o apetite a risco associado; avaliar se investimentos em IA estão alinhados ao propósito declarado da organização.
Responsabilidades da Alta Administração	Traduzir a tese estratégica em um portfólio de iniciativas de IA priorizadas; reportar ao Conselho o valor gerado e os riscos incorridos.
Responsabilidades da Gestão	Executar e mensurar iniciativas de IA; alimentar indicadores de valor (produtividade, receita, redução de custo, risco evitado).
Principais práticas de governança	Business case obrigatório para iniciativas de IA acima de um limiar de impacto; revisão periódica do portfólio de IA pelo Conselho; declaração pública de propósito de uso de IA.
Principais riscos tratados	Investimento em IA sem retorno mensurável; adoção por pressão competitiva, sem análise de valor; concentração do valor em poucos fornecedores de modelos fundacionais.
Mecanismos de controle e supervisão	Pauta recorrente de IA no Conselho; métricas de ROI de IA reportadas trimestralmente; política de aprovação de investimento por faixa de valor.
Indicadores sugeridos	% de iniciativas de IA com business case aprovado; valor gerado atribuível a IA; % do portfólio de IA alinhado à estratégia declarada.
Evidências esperadas	Atas de Conselho com deliberações sobre estratégia de IA; documento de tese estratégica; relatórios de valor gerado.
Relação com os demais domínios	Direciona o apetite a risco do Domínio 2; fornece critérios de priorização para o Domínio 4.
Fontes que fundamentam o domínio	Código IBGC (Cap. 1 — Fundamentos, geração de valor); NIST AI RMF (Govern); ISO/IEC 42001 (contexto da organização).

DOMÍNIO 2 Direcionamento e Apetite a Risco de IA (Conselho)

Objetivo	Estabelecer o papel do Conselho de Administração como órgão que direciona e supervisiona — mas não executa — a governança de IA, definindo o apetite a risco algorítmico da organização.
Justificativa	O Código IBGC atribui ao Conselho o papel de orientar e monitorar a gestão. A IA amplia a velocidade e a escala das decisões tomadas em nome da organização, exigindo que o Conselho declare explicitamente quanto risco algorítmico está disposto a aceitar — algo ausente das declarações de apetite a risco tradicionais.
Princípios relacionados	Responsabilização; Integridade.
Responsabilidades do Conselho	Aprovar declaração de apetite a risco de IA; definir limites de autonomia que exigem sua aprovação direta; avaliar a própria competência em IA (necessidade de capacitação ou membro especialista).
Responsabilidades da Alta Administração	Propor a declaração de apetite a risco para aprovação do Conselho; reportar desvios em relação ao apetite aprovado.
Responsabilidades da Gestão	Operar dentro dos limites aprovados; escalar exceções.
Principais práticas de governança	Declaração formal de apetite a risco de IA, revisada anualmente; capacitação continuada do Conselho em IA; avaliação de competência em IA na matriz de skills do Conselho.
Principais riscos tratados	Conselho sem capacitação suficiente para supervisionar a IA (aprovação sem análise real); ausência de limites claros de autonomia, o que leva à expansão silenciosa do uso de IA em nível estratégico.
Mecanismos de controle e supervisão	Matriz de skills do Conselho incluindo competência em IA; relatório periódico de aderência ao apetite a risco de IA.
Indicadores sugeridos	% de membros do Conselho com capacitação formal em IA; nº de desvios do apetite a risco reportados no período.
Evidências esperadas	Declaração de apetite a risco assinada; atas de capacitação do Conselho; matriz de competências.
Relação com os demais domínios	Recebe insumos do Domínio 1; direciona os Domínios 3 e 6.
Fontes que fundamentam o domínio	Código IBGC (Cap. 3 — Conselho de Administração); G20/OECD Principles of Corporate Governance; UK Corporate Governance Code 2024 (Provision 29); King V (Princípio 1 — Liderança; dados e tecnologia).

DOMÍNIO 3 Papéis, Responsabilidades e Direitos Decisórios em IA

Objetivo	Definir com clareza quem, na organização, tem autoridade para decidir sobre o quê em relação à IA — da aprovação de um novo caso de uso à autorização de um agente para agir sobre um sistema de produção.
Justificativa	A IA agêntica torna a pergunta "quem decide" mais urgente do que nunca: decisões antes tomadas por uma pessoa passam a ser tomadas, em parte, por um sistema que age em nome de alguém. Sem uma matriz explícita de direitos decisórios, a responsabilidade se dilui.
Princípios relacionados	Responsabilização; Equidade.
Responsabilidades do Conselho	Aprovar a matriz de direitos decisórios para casos de uso e agentes de alto risco (Domínio 5).
Responsabilidades da Alta Administração	Nomear os owners responsáveis por cada sistema/agente de IA; aprovar a matriz de direitos decisórios para os demais casos.
Responsabilidades da Gestão	Operar dentro dos direitos decisórios definidos; manter o registro das decisões delegadas a sistemas de IA.
Principais práticas de governança	Matriz RACI de IA por caso de uso; registro formal de quem responde por cada agente ou sistema; processo de aprovação de novos agentes com um owner nomeado.
Principais riscos tratados	Decisão sem dono identificável; delegação implícita de autoridade a um sistema, sem aprovação formal; conflito entre áreas quanto a quem responde por uma ação de IA.
Mecanismos de controle e supervisão	Inventário de IA com campo obrigatório 'owner'; aprovação documentada antes da entrada em produção.
Indicadores sugeridos	% de sistemas/agentes de IA com owner nomeado; tempo médio entre a identificação e a nomeação do owner.
Evidências esperadas	Matriz de direitos decisórios; inventário de IA com campo de responsabilidade preenchido.
Relação com os demais domínios	Aplica o apetite a risco do Domínio 2; fornece a base para a supervisão humana do Domínio 5.
Fontes que fundamentam o domínio	Código IBGC (Cap. 3–4 — papéis do Conselho e da Diretoria); ISO/IEC 38500 (responsabilidade pelo uso de TI); NIST AI RMF (Govern 1.1 e 4.1).

DOMÍNIO 4 Dados, Modelos e Ciclo de Vida da IA

Objetivo	Governar a qualidade, a proveniência e o ciclo de vida completo dos dados e dos modelos utilizados por sistemas de IA, da concepção ao descomissionamento.
Justificativa	Decisões de IA são apenas tão confiáveis quanto os dados e modelos que as sustentam. O Código IBGC trata de controles internos de forma genérica, mas não antecipa a necessidade de governança específica para dados de treinamento, vieses e linhagem de modelos — hoje central na ISO/IEC 42001 e na função Map do NIST AI RMF.
Princípios relacionados	Integridade; Equidade.
Responsabilidades do Conselho	Assegurar a existência de uma política de governança de dados e de modelos de IA; questionar a gestão sobre a qualidade e os vieses dos dados em casos de uso críticos.
Responsabilidades da Alta Administração	Aprovar a política de dados e os modelos de IA; assegurar orçamento para a qualidade dos dados.
Responsabilidades da Gestão	Implementar controles de qualidade, de linhagem e de avaliação de viés; documentar as limitações de cada modelo.
Principais práticas de governança	Ficha técnica (model card) por sistema de IA; avaliação de viés antes da entrada em produção; gestão de ciclo de vida (retreinamento, descomissionamento).
Principais riscos tratados	Vieses históricos reproduzidos em decisões automatizadas; dados de treinamento sem base legal (LGPD); modelos desatualizados operando sem revalidação.
Mecanismos de controle e supervisão	Repositório central de model cards; testes de viés documentados; revisão periódica obrigatória de modelos em produção.
Indicadores sugeridos	% de modelos com model card completo; nº de avaliações de viés no período; idade média dos modelos sem revalidação.
Evidências esperadas	Model cards; relatórios de avaliação de viés; registros de treinamento/descomissionamento.
Relação com os demais domínios	Fornece a base técnica para a taxonomia de risco utilizada nos Domínios 5 e 6.
Fontes que fundamentam o domínio	ISO/IEC 42001 (dados e ciclo de vida); NIST AI RMF (Map); LGPD (art. 20); EU AI Act (Art. 10 — governança de dados de treinamento).

DOMÍNIO 5 Supervisão Humana e Autonomia de Agentes de IA (Governança de IA Agêntica)

Objetivo	Calibrar o nível de autonomia concedida a sistemas e agentes de IA com base na reversibilidade e no impacto de suas ações, garantindo uma supervisão humana proporcional.
Justificativa	Este é o domínio onde reside o delta mais evidente em relação ao Código IBGC: ele não contempla a hipótese de um sistema agir de forma autônoma e assíncrona em nome da organização. IA agêntica introduz identidade própria de agente, delegação de privilégios e interação agente-agente — elementos sem paralelo na governança corporativa tradicional.
Princípios relacionados	Responsabilização; Integridade; Supervisão Humana Proporcional (princípio específico do MGCIA).
Responsabilidades do Conselho	Aprovar os níveis máximos de autonomia permitidos para agentes que atuam em processos de alto impacto; ser informado sobre incidentes envolvendo agentes de alto risco.
Responsabilidades da Alta Administração	Definir e manter atualizada a taxonomia de risco dos agentes; aprovar exceções ao escalonamento de autonomia.
Responsabilidades da Gestão	Implementar os níveis de supervisão (observador, aprovador, controlador); manter a identidade, os privilégios e as credenciais de cada agente sob gestão ativa.
Principais práticas de governança	Agent Naming Service; credenciais efêmeras; dupla aprovação para ações irreversíveis; mecanismo de interrupção (kill switch) testado periodicamente.
Principais riscos tratados	Autonomia mal calibrada para o risco da ação; ausência de identidade rastreável do agente; incapacidade de interromper um agente em execução; delegação em cascata entre agentes sem supervisão humana em nenhum ponto.
Mecanismos de controle e supervisão	Registro de identidade e de privilégios por agente; testes periódicos do mecanismo de interrupção; auditoria das trilhas de decisão agêntica.
Indicadores sugeridos	% de agentes de alto risco com dupla aprovação configurada; tempo médio de resposta a um comando de interrupção; nº de ações de agentes revertidas por intervenção humana.
Evidências esperadas	Registro de agentes; logs de decisão assinados criptograficamente; relatórios de teste do mecanismo de interrupção.
Relação com os demais domínios	Aplica a matriz de direitos decisórios do Domínio 3; alimenta a gestão de incidentes do Domínio 6 e o monitoramento do Domínio 8.
Fontes que fundamentam o domínio	NIST AI RMF (Manage); ISO/IEC 42001 (controles de operação); EU AI Act (Art. 14 — supervisão humana); PL 2338/2023 (supervisão humana para sistemas de alto risco).

DOMÍNIO 6 Riscos, Conformidade Regulatória e Terceiros

Objetivo	Integrar o risco algorítmico à estrutura corporativa de gestão de riscos e conformidade já existente, e estender a due diligence de terceiros para cobrir fornecedores de IA e modelos fundacionais.
Justificativa	O Código IBGC já trata a gestão de riscos e o compliance como funções de controle. O desafio da IA é de escopo, não de estrutura: é preciso incorporar riscos algorítmicos (viés, alucinação, uso indevido, dependência de poucos fornecedores de modelos fundacionais) ao mesmo processo, sem criar uma trilha paralela.
Princípios relacionados	Integridade; Sustentabilidade; Responsabilização.
Responsabilidades do Conselho	Aprovar a integração formal do risco de IA à matriz de riscos corporativos; supervisionar exposição a fornecedores concentrados de modelos fundacionais.
Responsabilidades da Alta Administração	Assegurar que o processo de gestão de riscos (COSO ERM) trate explicitamente de riscos de IA; aprovar política de due diligence de terceiros de IA.
Responsabilidades da Gestão	Executar avaliação de risco por caso de uso; conduzir due diligence de fornecedores de IA; monitorar a conformidade com a LGPD, a EU AI Act (quando aplicável) e a PL 2338/2023 (quando em vigor).
Principais práticas de governança	Inclusão de riscos de IA na matriz de riscos corporativos; cláusulas contratuais específicas de IA com fornecedores; avaliação de impacto para casos de uso de alto risco.
Principais riscos tratados	Dependência excessiva de um único provedor de modelo fundacional; não conformidade com a LGPD, a EU AI Act e o PL 2338/2023; uso de Shadow AI por terceiros na cadeia de fornecimento.
Mecanismos de controle e supervisão	Matriz de riscos corporativos com categoria específica de IA; contratos padronizados com cláusulas de auditoria e de direito à explicação; registro de fornecedores de IA avaliados.
Indicadores sugeridos	% de fornecedores de IA com due diligence concluída; nº de riscos de IA na matriz com plano de tratamento; nº de não conformidades regulatórias identificadas.
Evidências esperadas	Matriz de riscos atualizada; relatórios de due diligence de terceiros; pareceres de conformidade regulatória.
Relação com os demais domínios	Recebe insumos dos Domínios 4 e 5; alimenta os indicadores do Domínio 8.
Fontes que fundamentam o domínio	COSO ERM; Código IBGC (Cap. 5 — Auditoria/gerenciamento de riscos); LGPD; EU AI Act; PL 2338/2023 (em tramitação na Câmara dos Deputados).

DOMÍNIO 7 Transparência, Accountability e Impactos a Stakeholders

Objetivo	Assegurar que decisões e ações de IA que afetam pessoas — colaboradores, clientes, comunidades — sejam transparentes, explicáveis e passíveis de contestação.
Justificativa	O princípio da Responsabilização do Código IBGC já cobre a prestação de contas dos administradores. A IA estende essa exigência às próprias decisões automatizadas, que podem afetar diretamente terceiros sem intervenção humana — um novo tipo de "ato" pelo qual a organização é responsável.
Princípios relacionados	Transparência; Equidade; Responsabilização; Explicabilidade Proporcional ao Risco (princípio específico do MGCIA).
Responsabilidades do Conselho	Supervisionar a política de transparência de IA da organização perante os stakeholders; ser informado sobre reclamações ou contestações relevantes relativas a decisões automatizadas.
Responsabilidades da Alta Administração	Aprovar política de comunicação sobre uso de IA (quando e como informar que uma decisão envolveu IA); assegurar canal de contestação.
Responsabilidades da Gestão	Implementar avisos sobre o uso de IA nas interações relevantes; operar um canal de revisão humana para decisões contestadas (LGPD, art. 20).
Principais práticas de governança	Política de divulgação do uso de IA; canal formal de contestação e revisão humanas; relatório de impacto social de IA, quando aplicável.
Principais riscos tratados	Decisões automatizadas sem possibilidade de contestação; falta de transparência sobre o uso de IA, gerando perda de confiança; impactos desproporcionais sobre grupos específicos, sem detecção.
Mecanismos de controle e supervisão	Canal de contestação com SLA definido; auditoria periódica de reclamações relacionadas às decisões de IA.
Indicadores sugeridos	Nº de contestações recebidas e tempo médio de resposta; % de decisões de alto impacto com aviso prévio sobre o uso de IA.
Evidências esperadas	Registro do canal de contestação; política de transparência publicada; relatórios de impacto.
Relação com os demais domínios	Recebe insumos do Domínio 5; reporta ao Domínio 8.
Fontes que fundamentam o domínio	Código IBGC (Cap. 6 — Conduta); LGPD (art. 20); EU AI Act (Art. 50 — transparência); PL 2338/2023 (direitos das pessoas afetadas).

DOMÍNIO 8 Monitoramento, Indicadores e Assurance

Objetivo	Assegurar que a governança de IA seja continuamente monitorada e verificada de forma independente, fechando o ciclo entre o que o Conselho aprovou e o que efetivamente ocorre na operação.
Justificativa	O Código IBGC atribui à auditoria (interna, independente, conselho fiscal) o papel de verificar se a governança está funcionando. A IA exige que esse papel se estenda a evidências específicas — logs de decisão, testes de viés, registros de supervisão humana — que não constavam dos objetos de auditoria tradicionais.
Princípios relacionados	Responsabilização; Integridade; Confiança Verificável (princípio específico do MGCIA).
Responsabilidades do Conselho	Assegurar que a auditoria interna/externa tenha escopo e competência para avaliar a governança de IA; receber relatório periódico consolidado de indicadores de IA.
Responsabilidades da Alta Administração	Aprovar o plano de auditoria de IA; garantir recursos para o monitoramento contínuo.
Responsabilidades da Gestão	Manter dashboards de indicadores de IA; disponibilizar evidências para auditoria.
Principais práticas de governança	Auditoria de IA aplicando o Modelo das Três Linhas; dashboard consolidado de KPIs/KRIs reportado à Alta Administração e ao Conselho; testes adversariais (red teaming) periódicos.
Principais riscos tratados	Ausência de competência técnica na auditoria para avaliar sistemas de IA; indicadores existentes, mas que não chegam ao Conselho; auditoria limitada à documentação, sem verificação técnica efetiva.
Mecanismos de controle e supervisão	Plano de auditoria de IA com periodicidade definida; capacitação técnica da auditoria interna em IA; relatório trimestral consolidado ao Conselho.
Indicadores sugeridos	Cobertura de auditoria do inventário de IA (%); nº de achados de auditoria de IA em aberto; tempo médio de remediação dos achados.
Evidências esperadas	Relatórios de auditoria de IA; atas do Conselho com apresentação de indicadores; plano de auditoria aprovado.
Relação com os demais domínios	Consolida indicadores de todos os demais domínios; fornece ao Conselho (Domínio 2) a informação para ajustar o apetite a risco.
Fontes que fundamentam o domínio	Código IBGC (Cap. 5 — Auditoria Independente, Conselho Fiscal); IIA Modelo das Três Linhas; ISO/IEC 42001 (auditoria interna e revisão pela gestão); COSO ERM (monitoramento).

7. Papéis e Responsabilidades — Visão Consolidada

Síntese cruzada dos 8 domínios, mostrando o papel predominante de cada órgão de governança.

Domínio	Conselho	Alta Administração	Gestão
1. Estratégia e Geração de Valor com IA	Aprovar a tese estratégica de uso de IA e o apetite a risco associado...	Traduzir a tese estratégica em um portfólio de iniciativas de IA priorizadas...	Executar e mensurar iniciativas de IA...
2. Direccionamento e Apetite a Risco de IA	Aprovar declaração de apetite a risco de IA...	Propor a declaração de apetite a risco para aprovação do Conselho...	Operar dentro dos limites aprovados...
3. Papéis, Responsabilidades e Direitos Decisórios em IA	Aprovar a matriz de direitos decisórios para casos de uso e para agentes de alto risco (Domínio 5).	Nomear os owners responsáveis por cada sistema/agente de IA...	Operar dentro dos direitos decisórios definidos...
4. Dados, Modelos e Ciclo de Vida da IA	Assegurar a existência de uma política de governança de dados e de modelos de IA...	Aprovar a política de dados e os modelos de IA...	Implementar controles de qualidade, de linhagem e de avaliação de viés...
5. Supervisão Humana e Autonomia de Agentes de IA	Aprovar os níveis máximos de autonomia permitidos para agentes que atuam em processos de alto impacto...	Definir e manter atualizada a taxonomia de risco dos agentes...	Implementar os níveis de supervisão (observador, aprovador, controlador)...
6. Riscos, Conformidade Regulatória e Terceiros	Aprovar a integração formal do risco de IA à matriz de riscos corporativos...	Assegurar que o processo de gestão de riscos (COSO ERM) trate explicitamente dos riscos de IA...	Executar avaliação de risco por caso de uso...
7. Transparência, Accountability e Impactos a Stakeholders	Supervisionar a política de transparência de IA da organização perante os stakeholders...	Aprovar política de comunicação sobre uso de IA (quando e como informar que uma decisão envolveu IA)...	Implementar avisos sobre o uso de IA nas interações relevantes...
8. Monitoramento, Indicadores e Assurance	Assegurar que a auditoria interna/externa tenha escopo e competência para avaliar a governança de IA...	Aprovar plano de auditoria de IA...	Manter dashboards de indicadores de IA...

8. Modelo de Tomada de Decisão

O MGCIA propõe um modelo de direitos decisórios em quatro níveis, calibrado pela classificação de risco do caso de uso ou do agente de IA (baixo, moderado, alto ou crítico — nomenclatura compatível com a abordagem baseada em risco do EU AI Act e do PL 2338/2023).

Nível decisório	Classe de risco associada	Quem aprova
1 — Decisão delegada à Gestão Operacional	Baixo	Owner do sistema/agente, dentro de política já aprovada.
2 — Decisão delegada com aprovação da Alta Administração	Moderado	Alta Administração, com reporte periódico ao Conselho.

Nível decisório	Classe de risco associada	Quem aprova
3 — Decisão que exige aprovação do Conselho	Alto	Conselho de Administração, com parecer técnico prévio.
4 — Decisão que exige aprovação do Conselho e parecer de comitê independente	Crítico	Conselho, com parecer de comitê multidisciplinar (Domínio 5) antes da deliberação.

Este modelo se aplica tanto à aprovação de novos casos de uso e agentes quanto às exceções e aos escalonamentos identificados durante a operação (Domínio 5).

9. Gestão e Supervisão de Riscos

O MGCIA não cria uma trilha de risco paralela: propõe tratar o risco de IA como uma categoria adicional na estrutura já existente de ERM (Enterprise Risk Management), usando os cinco componentes do COSO ERM como referência para a integração.

Componente COSO ERM	Aplicação ao risco de IA
Governança e Cultura	Apetite a risco de IA aprovado pelo Conselho (Domínio 2); cultura de questionamento de decisões automatizadas.
Estratégia e Definição de Objetivos	Risco de IA considerado na definição da tese de valor (Domínio 1) e do portfólio de iniciativas.
Desempenho	Identificação e avaliação de riscos algorítmicos e agênticos por caso de uso (Domínios 4 e 5).
Revisão e Correção	Reavaliação periódica de modelos, agentes e fornecedores de IA à luz de mudanças no contexto ou de incidentes.
Informação, Comunicação e Reporte	Indicadores de risco de IA integrados ao reporte corporativo de riscos já existente (Domínio 8).

10. Monitoramento e Indicadores

Conjunto consolidado de indicadores recomendados para reporte periódico ao Conselho, reunindo os indicadores específicos definidos por domínio.

Indicador	Frequência sugerida	Domínio de origem
% de iniciativas de IA com business case aprovado	Trimestral	1
Nº de desvios do apetite a risco de IA reportados	Trimestral	2
% de sistemas/agentes de IA com owner nomeado	Mensal	3
% de modelos em produção com model card completo	Mensal	4
% de agentes de alto risco com dupla aprovação configurada	Mensal	5
Nº de riscos de IA na matriz corporativa com plano de tratamento	Trimestral	6
Nº de contestações de decisões automatizadas e tempo médio de resposta	Mensal	7
Cobertura de auditoria sobre o inventário de IA (%)	Semestral	8

11. Assurance

O MGCIA aplica o Modelo das Três Linhas do IIA (2020) à governança de IA, preservando sua lógica original de papéis colaborativos e não sobrepostos.

Linha	Papel na governança de IA
1ª Linha — Gestão operacional	Owners de sistemas e agentes de IA (Domínio 3); execução dos controles de operação do dia a dia.
2ª Linha — Funções de risco e controle	Risco, compliance, segurança da informação, privacidade e a função específica de governança de IA (quando existente), definindo políticas e monitorando a 1ª linha.
3ª Linha — Auditoria interna	Avaliação independente da eficácia da governança de IA como um todo, reportando diretamente ao Conselho ou ao comitê de auditoria (Domínio 8).
Assurance externa complementar	Auditoria independente e, quando aplicável, certificação ISO/IEC 42001, como camada adicional de verificação para stakeholders externos.

12. Aplicação Proporcional do Modelo

Assim como o próprio Código IBGC recomenda a adaptação das práticas à realidade e ao estágio de maturidade da organização, o MGCIA não pressupõe a implementação uniforme dos 8 domínios.

Perfil da organização	Aplicação recomendada
Pequena/média empresa, uso limitado de IA (ferramentas de produtividade, sem decisões automatizadas de alto impacto)	Domínios 1, 3 e 6 em versão simplificada — inventário básico, owner nomeado, avaliação de fornecedores. Demais domínios como referência futura.
Empresa de médio/grande porte com casos de uso relevantes de IA generativa e preditiva	Domínios 1 a 4, 6, 7 e 8 implementados; Domínio 5 aplicado apenas aos casos de uso com algum grau de autonomia.
Grande organização ou setor regulado (financeiro, saúde, seguros) com IA agêntica em processos críticos	Os 8 domínios implementados em profundidade, com ênfase reforçada no Domínio 5 e na auditoria técnica especializada (Domínio 8).

13. Tratamento Específico da IA Agêntica

Elementos relevantes:

- **Níveis de autonomia:** cada agente deve ter um nível de autonomia explicitamente definido e proporcional à reversibilidade da ação (Domínio 5), e não um nível implícito herdado do modelo subjacente.
- **Autoridade para agir:** a autoridade de um agente para executar uma ação deve derivar de uma delegação humana explícita e documentada (Domínio 3), nunca de presunção.
- **Identidade dos agentes:** cada agente deve possuir identidade própria e distinta da identidade humana que o supervisiona, permitindo rastreamento individualizado de suas ações.

- **Privilégios:** os privilégios concedidos a um agente devem seguir o princípio do menor privilégio necessário à tarefa, com revisão periódica e revogação automática ao término da tarefa.
- **Delegação:** quando um agente delega parte de uma tarefa a outro agente ou a uma ferramenta, a cadeia de delegação deve permanecer rastreável até a autorização humana original.
- **Interação entre agentes:** comunicações entre agentes devem ser tratadas como potenciais vetores de risco, exigindo autenticação e registro, e não confiança implícita entre sistemas da mesma organização.
- **Acesso a ferramentas:** o acesso de um agente a ferramentas e sistemas externos deve ser mediado e registrado, nunca direto e não monitorado.
- **Supervisão humana:** deve existir, para cada agente, um nível definido de supervisão humana (observador, aprovador ou controlador), calibrado em função da classe de risco da ação.
- **Rastreabilidade:** toda ação relevante de um agente deve gerar um registro auditável, vinculado à sua identidade, ao contexto e à autorização que a originou.
- **Observabilidade:** a organização deve ser capaz de monitorar o comportamento de um agente em tempo real, e não apenas reconstituir suas ações após o fato.
- **Reversibilidade:** ações de alto impacto executadas por agentes devem, sempre que tecnicamente possível, ser concebidas para permitir a reversão.
- **Interrupção:** deve existir um mecanismo de interrupção testado (kill switch), capaz de suspender a atuação de um agente de forma imediata e confiável.
- **Accountability pelas ações dos agentes:** a responsabilidade final por uma ação executada por um agente é sempre de uma pessoa física ou jurídica identificável — nunca do próprio agente.