



POLÍTICA DE GESTÃO DE RISCOS DE INTEGRIDADE

1. INTRODUÇÃO E OBJETIVO

A BRASÍLIA SEGURANÇA, atuante em vigilância patrimonial com serviços 24h motorizada, armada/desarmada, monitoramento integrado, aérea e sustentável (ex.: carros elétricos), opera em um ambiente de alta regulação com licitações públicas e interações com entes governamentais do DF (hospitais, Caesb, rodoviárias, entre outros).

Esta Política de Gestão de Riscos de Integridade estabelece diretrizes claras para identificar, avaliar, mitigar e monitorar riscos que possam comprometer a ética, a conformidade e a sustentabilidade da empresa.

O objetivo é proteger a reputação, evitar sanções e apoiar o crescimento, integrando a gestão de riscos ao Programa de Integridade existente desde junho de 2019, com treinamentos iniciais, Código de Conduta e Ética e ciência ampla de colaboradores, clientes, fornecedores e subcontratados, sob apoio da alta direção e Comitê de Ética e Integridade (CEI) liderado pelo *Compliance Officer*.

2. PRINCÍPIOS GERAIS

- **Transparência:** Todos os riscos serão documentados e comunicados, com evidências armazenadas em nuvem para auditorias;
- **Proporcionalidade:** Foco em riscos altos (corrupção, LGPD) com apetite baixo, e médios (interpessoal) com tolerância controlada;
- **Responsabilidade Compartilhada:** O Comitê de Ética e Integridade (CEI) supervisiona, mas cada área executa (ex.: operacional mitiga riscos em postos de vigilância);
- **Atualização Contínua:** Revisão anual ou após incidentes, alinhada à Portaria CGU nº 226/2025 para demonstração de efetividade;
- **Integração ao Negócio:** Riscos são avaliados em licitações, contratos e serviços 24h, sem paralisar operações dispersas.



3. IDENTIFICAÇÃO DE RISCOS

Riscos são identificados por meio de questionários, treinamentos, auditorias internas e relatórios operacionais (ex.: ARGUS para jornada de vigilantes).

As fontes principais incluem:

- ✓ Interações com agentes públicos (fiscais, gestores de contratos, entre outros): Favores ou influência indevida em licitações;
- ✓ Terceiros (fornecedores, subcontratados): Golpes, subcontratações irregulares e falsificação de CNVs/armamento;
- ✓ Operacional (postos dispersos): Assédio em vigilância isolada, desvios de conduta e atestados falsos;
- ✓ Administrativo: Vazamentos de dados sensíveis (LGPD) e fraudes internas;
- ✓ Estratégico: Subnotificação de denúncias interpessoais e percepções punitivas de *Compliance*.

A identificação ocorre trimestralmente, com *workshops* anuais no CEI e relatórios anônimos via Canal de Denúncias.

4. AVALIAÇÃO E APETITE AO RISCO

Os Riscos são avaliados por probabilidade (baixa a alta) e impacto (financeiro, reputacional, legal), resultando em nível de risco (baixo, médio, alto).

O apetite ao risco da BRASÍLIA SEGURANÇA é baixo, considerando o setor regulado: toleramos médio para riscos operacionais rotineiros (ex.: conflitos interpessoais em postos), mas zero para corrupção, para evitar entraves em licitações.

Escala 1-5 (1=baixo apetite/tolerância mínima; 5=alto apetite/risco aceitável).

MATRIZ DE APETITE AO RISCO

CATEGORIA DE RISCO	DESCRIÇÃO	APETITE AO RISCO (1-5)	JUSTIFICATIVA	LIMITES DE TOLERÂNCIA
Corrupção e Integridade (ex.: <i>due diligence</i> ausente, favores com servidores)	Riscos de atos lesivos à administração pública, como influência indevida em licitações ou subcontratações irregulares em vigilância.	1 (Baixo)	Setor público exige zero tolerância; viola Lei 12.846/2013 e diagnóstico mostra gaps em terceiros.	Nenhum risco aceitável; mitigação imediata e zero incidentes.
Reputacional (ex.: assédio, subnotificação de denúncias)	Danos à imagem por escândalos em postos ou percepções punitivas de compliance em >4 mil vigilantes.	1-2 (Baixo)	Afeta contratos com SES, IGES, CAESB; diagnóstico destaca cultura em maturação fraca.	Máximo 1 incidente por ano; monitoramento mensal de denúncias.
Operacional (ex.: desvios de conduta, comunicação dispersa)	Atrasos ou erros em supervisão de vigilância 24h, assédio em postos isolados ou ruídos em ARGUS.	2-3 (Médio-Baixo)	Necessário para dinamismo de serviços dispersos, mas sem comprometer conformidade (NRs, CNVs).	Máximo R\$ 100.000 em perdas anuais; <i>due diligence</i> em 100% contratos públicos.
Legal/Regulatório (ex.: LGPD, sanções CGU)	Inabilitações ou processos por vazamentos de dados ou não conformidade em licitações de segurança.	1 (Baixo)	Alto risco em entes públicos; diagnóstico destaca informalidade manual como brecha.	Zero sanções; revisão anual alinhada à Portaria CGU nº 226/2025.

Essa matriz reflete o apetite conservador da BRASÍLIA SEGURANÇA: baixo para integridade (prioridade máxima) e médio para operacional, equilibrando crescimento com proteção. Riscos acima do apetite exigem ação imediata.

5. MITIGAÇÃO E CONTROLES

Para cada risco identificado, aplica-se:

- Medidas Preventivas: Exemplos: Treinamentos bimestrais (foco em campo, como assédio); *due diligence* obrigatória para terceiros, procedimentos escritos para registros no ARGUS;

- Controles Detectivos: Exemplos: Auditorias trimestrais em postos e admin (ex.: verificação de CNVs e denúncias); Canal de Denúncias com resposta em 45 dias (CEI);
- Resposta a Incidentes: Exemplos: Plano de contingência com escalonamento ao CEI e alta gestão; suporte psicológico para vítimas de assédio;

MATRIZ DE RISCOS DE INTEGRIDADE (PRINCIPAIS RISCOS IDENTIFICADOS NO DIAGNÓSTICO)

RISCO PRINCIPAL	DESCRIÇÃO (BASEADO EM ENTREVISTADOS)	PROBABILIDADE (BAIXA / MÉDIA / ALTA)	IMPACTO (BAIXO / MÉDIO / ALTO)	NÍVEL DE RISCO	MITIGAÇÃO PRINCIPAL
Falta de Due Diligence para Terceiros	Ausência de checagem formal em fornecedores/subcontratados, expondo a golpes e irregularidades em vigilância armada	Alta	Alto	Alto	Implementar POP com questionários e consultas externas (CGU/TCU).
Informalidade em Controles Operacionais	Processos manuais em denúncias e supervisão dispersa, gerando brechas em CNVs e atestados falsos.	Média	Médio	Médio-Alto	Apps para triagem e auditorias mensais em ARGUS.
Pressões e Facilidades em Licitações	Pedidos de favores ou influência indevida por agentes públicos em contratos DF	Média	Alto	Alto	Treinamentos específicos e cláusulas anti-corrupção em contratos.
Assédio	Falsificação de documentos ou assédio em postos isolados de vigilância 24h	Média	Médio	Alto	Exigência de requisitos mínimos e palestras em supervisão.

RISCO PRINCIPAL	DESCRIÇÃO (BASEADO EM ENTREVISTADOS)	PROBABILIDADE (BAIXA / MÉDIA / ALTA)	IMPACTO (BAIXO / MÉDIO / ALTO)	NÍVEL DE RISCO	MITIGAÇÃO PRINCIPAL
Treinamentos e Cultura Insuficientes	Anuais e difíceis de consultar, levando a esquecimento em vigilantes dispersos	Alta	Médio	Médio-Alto	Guias digitais de bolso e treinamentos periódicos adaptados.
Subnotificação de Denúncias	Canal subutilizado para interpessoais (assédio, brigas), com apurações reativas sem procedimentos padronizados	Média	Médio	Médio	Divulgação em postos e POP para apurações com suporte RH.

Essa matriz lista os 6 principais riscos do diagnóstico consolidado, priorizados por relevância setorial. Nível de risco = combinação de probabilidade e impacto (alto se ambos médios/alto).

6. MONITORAMENTO E REVISÃO

- Indicadores Chave: Exemplos: Número de riscos mitigados (meta: 80% em 6 meses); taxa de adesão a treinamentos (>90%); incidentes reportados (reduzir 50%);
- Ferramentas: *Dashboard* simples no Excel/OneDrive para rastrear; relatórios trimestrais ao CEI e alta gestão;
- Revisão: Anual ou após mudanças regulatórias (ex.: nova Portaria CGU);
- Treinamento: Obrigatório para todos, com foco em apetite ao risco.

7. RESPONSABILIDADES

- Alta Gestão: Aprovar política e alocar recursos; liderar exemplo ético (Acionistas, Diretores e CEO).
- CEI: Supervisionar identificação e mitigação; revisar matrizes anualmente;
- Áreas Operacionais: Reportar riscos em postos; aplicar controles diários.



- RH/Compliance: Atualizar matrizes e conduzir *due diligence*.
- Todos os Colaboradores: Reportar riscos via Canal; aderir a controles.