



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 1/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			

1. OBJETIVO

O objetivo desta Política é estabelecer princípios, diretrizes e responsabilidades para a Gestão de Riscos do Grupo SADA, assegurando que o processo esteja integrado à cultura e às decisões organizacionais, de forma a criar e proteger valor, apoiar a inovação, fortalecer a governança, proteger ativos tangíveis e intangíveis e promover a resiliência e a perenidade sustentável dos negócios, em conformidade com as melhores práticas nacionais e internacionais de gestão de riscos.

2. RESPONSABILIDADE E AUTORIDADE

RESPONSABILIDADE

Coordenação de Governança e Riscos (GRC)

- Implementar o processo de Gestão de Riscos do Grupo SADA;
- Zelar pela aplicação da metodologia de gestão de riscos em conformidade com a norma ABNT NBR ISO 31000.
- Coordenar o mapeamento de riscos corporativos e setoriais, apoiando gestores das áreas;
- Assessorar as áreas de negócio na identificação e avaliação do impacto dos diversos tipos de riscos envolvidos, bem como criticar e revisar tal avaliação e colaborar com a implementação de controles internos;
- Participar do mapeamento de processos do Grupo SADA em conjunto com a área de Controles Internos/Controladoria, quando tratar-se de riscos com impacto nas demonstrações financeiras;
- Apoiar, quando demandada, a Gerência de Qualidade, Gerência do SESMT, Coordenação de Meio Ambiente e Gerência de Segurança da Informação, no processo de gestão de riscos de qualidade, segurança do trabalho, meio ambiente e segurança da informação.
- Gerir a ferramenta corporativa (software) de Governança e Gerenciamento de riscos, realizando a Governança do processo e suportando as áreas de negócio na definição do plano de ação;
- Monitorar a gestão de riscos em parceria com as demais áreas e comitês de riscos do Grupo SADA;
- Acompanhar a implementação dos planos de ação estabelecidos;
- Validar os planos de contingência elaborados para os riscos críticos;
- Consolidar e reportar trimestralmente o cenário de risco ao Comitê Executivo de Riscos;
- Desenvolver e aplicar treinamentos e capacitações em gestão de riscos;
- Assegurar a manutenção da política de gestão de riscos verificando o seu cumprimento;
- Atuar como ponto focal para dúvidas e suporte técnico relacionado a riscos;
- Assegurar a revisão anual dos riscos corporativos e das áreas de negócio;

Elaborado/Revisado por: Aline Faria
Santos Rabelo de Azevedo

Aprovado por: DANIELA MARIA MEDIOLI



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 2/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			

- Disseminar, continuamente, a cultura de gestão de riscos e controles internos no Grupo SADA, promovendo todas as comunicações, treinamentos e indicadores necessários para o processo.
- Apoiar a integração da gestão de riscos com os processos de planejamento estratégico, sustentabilidade (ESG) e compliance, incluindo riscos emergentes (climáticos, reputacionais, tecnológicos e de terceiros).
- Apoiar os processos de resposta a crises e continuidade dos negócios, em conjunto com as áreas responsáveis.

Gerência de Controladoria

- Realizar mapeamento de processos do Grupo SADA em conjunto com área de GRC, nos casos de riscos com impacto financeiro, ou seja, que podem afetar reportes e demonstrações financeiras e/ou gerar impacto de caixa (riscos econômico-financeiros);
- Estabelecer controles para fins de mitigação dos riscos identificados nos processos;
- Suportar os trabalhos da auditoria interna e externa caso aplicável;
- Auxiliar na elaboração das políticas necessárias para formalizar as diretrizes e controles desenhados;
- Reportar de forma recorrente ao GRC os riscos identificados ao longo do mapeamento dos processos, bem como os respectivos controles desenhados.

Gerência de Qualidade, Gerência do SESMT, Coordenação de Meio Ambiente e Gerência de Segurança da Informação

- Realizar mapeamento de riscos nos casos de risco de qualidade, segurança do trabalho, ambientais e segurança da informação, respectivamente, conforme respectivas políticas e/ou procedimentos.
- Estabelecer controles para fins de mitigação dos riscos identificados nos processos e realizar a gestão dos riscos, incluindo o adequado reporte, conforme respectivas políticas e/ou procedimentos.
- As gerências mencionadas poderão contar com o apoio da área de GRC para inclusão dos riscos e controles no sistema automatizado de monitoramento de riscos.

Gestores Corporativos e das Áreas de Negócio

- Identificar e avaliar os riscos inerentes às atividades sob sua responsabilidade;
- Definir as ações mitigatórias em conjunto com a Coordenação de Governança e Riscos;
- Aprovar controles e planos de ação à respectiva Diretoria e buscar os recursos necessários para mitigar os riscos;
- Implementar e acompanhar os planos de tratamento dos riscos;
- Garantir que os controles internos sejam implementados e executados de forma efetiva;
- Elaborar Planos de Contingência para os riscos classificados como críticos ou que apresentem potencial para interromper operações, afetar significativamente stakeholders, comprometer a segurança de pessoas, gerar danos ambientais ou causar prejuízos materiais relevantes;



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 3/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			

- Comunicar tempestivamente à Coordenação de Governança e Riscos qualquer alteração nos riscos mapeados, bem como o surgimento de novos riscos que afetem o grau de exposição de risco do Grupo SADA;
- Incentivar as equipes a adotarem comportamento preventivo e responsável.
- Integrar a avaliação de riscos ao processo de definição de metas, indicadores e iniciativas estratégicas de suas áreas.

Coordenação de Auditoria Interna (GRC)

- Elaborar o plano anual de Auditoria, podendo ser utilizada como referência a matriz de riscos do Grupo;
- Realizar auditoria interna para avaliar a efetividade dos controles estabelecidos em matrizes de controle, conforme Plano Anual de Auditoria;
- Reportar trimestralmente os resultados das auditorias internas ao Comitê Executivo de Riscos e Vice-Presidência Executiva.

Colaboradores

- Cumprir as diretrizes desta Política;
- Atuar de forma preventiva, identificando e comunicando à liderança potenciais riscos, incidentes ou não conformidades que possam evoluir para crises ou riscos relevantes;
- Participar dos treinamentos oferecidos sobre Gestão de Riscos;
- Cooperar ativamente no fornecimento de informações durante o processo de mapeamento e monitoramento de riscos.

AUTORIDADE

Gerencia de Governança, Riscos e Compliance

- Estabelecer a metodologia de Governança e Gerenciamento de Riscos do Grupo SADA, abertura e encerramento de seus ciclos, bem como validar o escopo dos trabalhos com o Comitê Executivo de Riscos;
- Conduzir as reuniões do Comitê Executivo de Riscos.
- Garantir que a Política de gestão de riscos seja revisada, no mínimo, a cada 2 (dois) anos, ou sempre que houver mudanças significativas na estratégia, estrutura organizacional ou regulamentação aplicável.

Comitê Executivo de Riscos

- Aprovar a Matriz de Risco do Grupo SADA;
- Analisar criticamente os reportes trimestrais de risco, propondo ações de melhoria contínua;
- Avaliar a efetividade do processo de gestão de riscos, no tocante à definição, revisão e monitoramento dos riscos priorizados;
- Avaliar a eficácia das ações tomadas para abordar riscos e oportunidades.
- Aprovar Planos de Contingência para os riscos classificados como críticos ou que apresentem potencial para interromper operações, afetar significativamente stakeholders, comprometer a segurança de pessoas, gerar danos ambientais ou causar prejuízos materiais relevantes



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 4/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			

- Patrocinar e monitorar a evolução da maturidade em gestão de riscos, assegurando recursos e integração ao modelo de governança corporativa;

Alta Direção (Diretores Operacionais e Áreas Corporativas)

- Assegurar que a gestão de riscos esteja integrada nos processos, projetos e decisões estratégicas de sua respectiva unidade ou área;
- Disponibilizar recursos adequados (humanos, tecnológicos e financeiros) para a implementação das ações de gestão de riscos sob sua responsabilidade;
- Patrocinar e promover a cultura de gestão de riscos entre gestores e colaboradores de sua unidade, reforçando sua importância como parte do modelo de governança;
- Comunicar periodicamente à Vice-Presidência Executiva e à Gerência de GRC sobre os principais riscos, planos de ação e evolução da maturidade em sua área;
- Garantir a análise crítica periódica dos riscos de sua unidade, assegurando que estejam alinhados ao apetite de risco definido pela organização.

Vice-Presidência Executiva

- Aprovar esta política;
- Aprovar os parâmetros de impacto de risco, conforme apetite ao risco da organização.
- Patrocinar e monitorar a evolução da maturidade em gestão de riscos, assegurando recursos e integração ao modelo de governança corporativa.

3. TERMINOLOGIA

Riscos: Efeito da incerteza sobre os objetivos estabelecidos. Possibilidade da ocorrência de um evento, oriundo de fontes internas ou externas, capaz de afetar os objetivos da organização. Pode representar tanto ameaças quanto oportunidades.

Evento: ocorrência ou situação que pode causar impacto nos objetivos da organização.

Gestão de Riscos: processo contínuo que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar eventos capazes de afetar os objetivos, processos de trabalho e projetos do grupo SADA, positiva ou negativamente.

Oportunidade: circunstância que pode gerar impactos positivos, agregando valor ou ampliando a capacidade de alcance dos objetivos organizacionais.

Ameaça: circunstância que pode gerar impactos negativos, prejudicando a capacidade da organização em alcançar seus objetivos.

Fator de Risco: elemento interno ou externo que aumenta a probabilidade de ocorrência ou a severidade de um risco.

Apetite ao Risco: nível de risco que o Grupo SADA está disposto a buscar, manter ou assumir.



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 5/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			

Matriz de Riscos: Representação gráfica do risco considerando a relação entre impacto e probabilidade, utilizada para priorização do risco e tomada de decisão.

Controle: medida existente ou implementada para prevenir, detectar, reduzir ou transferir risco. Pode ser de natureza preventiva, detectiva ou corretiva.

Partes Interessadas (Stakeholders): indivíduos, grupos ou organizações que podem afetar, ser afetados ou perceber-se afetados por uma decisão, atividade ou risco da organização.

GRC: Gerência de Governança, Riscos e Compliance.

4. ABRANGÊNCIA

Esta Política abrange todas as Empresas do Grupo SADA, incluindo suas unidades, áreas, processos, projetos, produtos e serviços. Aplica-se a todos os colaboradores, gestores, fornecedores, prestadores de serviço e parceiros de negócio que desempenhem atividades sob responsabilidade do Grupo.

A abrangência contempla a gestão integrada de riscos estratégicos, operacionais, financeiros, de conformidade, ambientais, sociais, tecnológicos, de terceiros e reputacionais, assegurando que sejam considerados tanto os impactos internos quanto os efeitos sobre clientes, fornecedores, partes interessadas e a sociedade em geral.

5. DIRETRIZES

O objetivo do estabelecimento da Gestão de Riscos é oferecer uma abordagem estruturada e integrada aos processos de gestão para avaliar, controlar, comunicar e monitorar eventos, sejam eles riscos negativos (ameaças) ou positivos (oportunidades).

A Gestão de Riscos do Grupo SADA está alinhada à sua estratégia e corrobora com o seu esforço na construção de pilares sustentáveis do seu negócio, devendo apoiar o planejamento estratégico, proteger e agregar valor à organização, bem como subsidiar o processo de tomada de decisão da Alta Direção do grupo.

Princípios do Gerenciamento de Riscos

Com base nas diretrizes da norma ABNT NBR ISO 31000, os seguintes princípios norteiam a Gestão de Riscos do Grupo SADA:

- Criação e proteção de valor para a organização
- Integração do gerenciamento de riscos a todas as atividades e processos organizacionais
- Tomada de decisão estruturada e abrangente
- Análise baseada nas melhores informações disponíveis
- Consideração de fatores humanos e culturais
- Transparência e envolvimento das partes interessadas



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 6/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			

- Dinamismo e capacidade de adaptação, pois riscos podem surgir, se modificarem ou desaparecer. O gerenciamento de riscos deve antecipar, detectar, reconhecer e responder a estas mudanças e eventos de uma maneira apropriada e oportuna.
- Melhoria contínua: gerenciamento de riscos é melhorado continuamente por meio do aprendizado e experiências.
- Responsabilidade compartilhada: a gestão de riscos é responsabilidade de todos os níveis da organização, devendo a Alta Direção assegurar governança eficaz e patrocínio institucional.
- Consideração de riscos emergentes, incluindo aspectos ambientais, sociais, tecnológicos e reputacionais.
- Personalização: a gestão de riscos deve ser adaptada ao contexto interno e externo, aos objetivos, à estrutura e às operações de cada unidade de negócio do Grupo SADA.
- Inclusividade: a gestão de riscos deve considerar as partes interessadas internas e externas, garantindo que percepções, suas necessidades e expectativas sejam avaliadas no processo decisório.

Tipologia de Riscos

A tipologia de riscos refere-se à classificação sistemática dos diferentes tipos de riscos que podem impactar o Grupo SADA, considerando suas origens, naturezas e possíveis consequências. Essa categorização tem como objetivo facilitar a identificação, análise e tratamento dos riscos, permitindo que cada área da empresa compreenda e gerencie adequadamente as ameaças e oportunidades inerentes ao seu contexto de atuação.

- **Riscos Estratégicos** refere-se a ameaças e oportunidades que podem afetar os objetivos de longo prazo do Grupo SADA, colocando em risco sua capacidade de cumprir sua missão, visão e metas institucionais. Estão relacionados às escolhas estratégicas da organização, à dinâmica do ambiente externo e às mudanças estruturais de mercado. São riscos que comprometem o posicionamento futuro da organização, sua competitividade e sua sustentabilidade no longo prazo. Incluem os riscos de continuidade de negócios, ou seja, riscos de interrupções severas decorrentes de crises externas (pandemias, desastres naturais, greves, crises energéticas ou falhas críticas de TI) que comprometam a operação de fábricas e transporte.

Exemplos: mudanças regulatórias e legais que impactem diretamente o modelo de negócios; fatores macroeconômicos e geopolíticos; dependências de parceiros estratégicos; estratégias corporativas mal formuladas ou executadas (fusões, expansões, etc), mudanças de mercado (novos competidores disruptivos, perda de contratos estratégicos), dentre outros.

- **Riscos Econômico-financeiros:** são aqueles que podem impactar a saúde financeira da organização, comprometendo sua liquidez, rentabilidade, estrutura de capital, capacidade de investimento e continuidade operacional. Envolvem incertezas relacionadas ao ambiente econômico, às condições de mercado, ao desempenho financeiro interno e às obrigações financeiras assumidas pela empresa. Exemplos: risco de liquidez (insuficiência de caixa, atrasos significativos



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 7/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			

em recebíveis, inadimplência); risco de crédito (inadimplência de clientes relevantes, parceiros com baixa capacidade financeira); risco de mercado (variação de taxas de juros, oscilações cambiais, volatilidade de preços); risco macroeconômico (recessão, inflação, instabilidade política); risco orçamentário; risco tributário; risco de fraude financeira (manipulação de demonstrações financeiras, desvio de recursos, pagamentos indevidos ou superfaturados), riscos de estrutura de capital (grau elevado de endividamento, custo de capital incompatível com retorno de investimentos, etc).

- **Riscos Operacionais:** Riscos associados a falhas, insuficiências ou inadequações nos processos internos operacionais. São riscos relacionados ao funcionamento diário da organização e à capacidade de entregar serviços de forma segura, eficiente e consistente. São riscos que podem causar interrupções, ineficiências, retrabalhos, perdas financeiras, danos as pessoas, impactos à qualidade. Exemplos: falhas de processos (processos manuais suscetíveis a erro humano, ausência de padronização, falhas na gestão de documentos; falhas de pessoas (erros operacionais por falta de treinamento, desalinhamento de competências, alta rotatividade que afeta a continuidade da operação); falhas de sistemas e tecnologia; falhas de equipamentos e infraestrutura; riscos logísticos (atrasos, extravio de cargas); riscos relacionados a terceiros (fornecedores sem capacidade técnica, contratos com falhas operacionais).
- **Riscos de Compliance (conformidade) e Integridade:** Decorrentes de descumprimentos de leis, regulamentos, normas internas, código de conduta, políticas corporativas e princípios éticos que regem a atuação do Grupo SAD. Incluem situações que podem comprometer a integridade institucional, causar impactos reputacionais, gerar sanções legais, administrativas ou financeiras. São riscos que ameaçam a conformidade legal, a ética corporativa, a transparência e a condução responsável do negócio. Exemplos: descumprimentos de leis, regulamentos e normas em geral; corrupção, fraude e suborno; conflito de interesses (tomada de decisões influenciada por interesses pessoais, relações com fornecedores); não cumprimento de políticas de brindes, desrespeito a normas de conduta profissional, práticas de assédio moral ou sexual, uso indevido de bens da empresa; riscos de lavagem de dinheiro e financiamento ao terrorismo, dentre outros.
- **Riscos Concorrenciais:** Decorrentes de práticas empresariais que podem violar as leis de defesa da concorrência, limitar a livre competição ou gerar vantagens indevidas no mercado. Exemplos: acordos ou práticas anticompetitivas (formação de cartel para fixação de preços, divisão de mercado, troca de informações sensíveis com concorrentes), abuso de posição dominante (preços predatórios, práticas de exclusividade forçada); manipulação de concorrências públicas ou privadas), etc.
- **Riscos Legais e regulatórios:** Riscos associados a processos judiciais existentes e futuros, de natureza cível, trabalhista, criminal, administrativos e tributário. Podem gerar perdas financeiras, penalidades, restrições operacionais, passivos jurídicos.
- **Riscos de Qualidade:** riscos relacionados ao não atendimento aos requisitos de qualidade de clientes, incluindo devoluções, recalls e campanhas de campo, bem



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 8/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			

como impactos decorrentes de não conformidades em auditorias, inspeções ou certificações aplicáveis.

- **Riscos de Tecnologia da Informação:** Riscos de defasagem ou dificuldade de acompanhar a velocidade dos avanços tecnológicos, causados pela falha de investimento, infraestrutura tecnológica e sistêmica inadequadas, dependência de tecnologias obsoletas que comprometa a capacidade de inovar e manter a organização relevante no mercado a longo prazo. Riscos de paralisação das operações e negócios decorrentes de falhas sistêmicas ocasionadas por erro humano ou por eventos externos alheios ao controle da organização.
- **Riscos de Segurança da Informação e Proteção de Dados Pessoais:** Riscos associados a *cybersecurity*, ou seja, de violação da segurança do ambiente tecnológico da organização por agentes internos ou externos, que podem ocasionar vazamento de dados próprios ou de terceiros. Não conformidade com as normas e regulamentos de privacidade e proteção de dados pessoais, em especial da Lei Geral de Proteção de Dados Pessoais (LGPD), que pode afetar a imagem da organização, a confiabilidade, integridade e disponibilidade de informações, além de penalidades financeiras significativas. Podem incluir: ataques cibernéticos, roubo e sequestro de informações confidenciais, perda de dados, falha de segurança da rede e outros. Riscos associados ao uso de inteligências artificiais que impactem questões éticas de privacidade de dados ou uso incorreto de algoritmos.
- **Riscos de Responsabilidade Social, Práticas Trabalhistas e Direitos Humanos:** são aqueles decorrentes da possibilidade da organização, direta ou indiretamente, causar, contribuir ou estar associada a impactos negativos sobre pessoas, colaboradores, comunidades, grupos vulneráveis e demais partes interessadas. Exemplos: violação de direitos humanos (trabalho infantil, trabalho forçado ou condições degradantes); práticas trabalhistas inadequadas (falta de condições seguras de trabalho, saúde ocupacional ou bem-estar, violação a liberdade de associação); discriminação e desigualdade; impactos em comunidades (operações que afetem negativamente a saúde, segurança, mobilidade ou qualidade de vida); riscos na cadeia de fornecimento (fornecedores ou intermediários associados a violações trabalhistas, condutas inadequadas de terceiros em nome da organização).
- **Riscos Ambientais:** decorrentes da possibilidade de que as atividades, processos, serviços ou relações da organização causem impactos negativos ao meio ambiente ou sejam afetados por condições ambientais adversas. Esses riscos abrangem danos a recursos naturais, poluição, emissões, desperdícios, gestão inadequada de resíduos, dentre outros.
- **Riscos Reputacionais ou de Imagem:** riscos específicos de perda de confiança por parte de clientes, sociedade, órgãos reguladores e parceiros, decorrentes de falhas de produto, crises de imagem, incidentes ambientais, trabalhistas ou de integridade.



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 9/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			

Estrutura organizacional para a Gestão de Riscos

O Grupo SADA possui um fluxo integrado de Gestão de Riscos, baseado no modelo das Três Linhas, do IIA – Instituto dos Auditores Internos:



Comitê Executivo de Riscos

O Comitê Executivo de Riscos atua como o representante da alta direção do Grupo SADA no âmbito do gerenciamento de riscos, sendo responsável por supervisionar, orientar e validar as principais diretrizes, estratégias e decisões relacionadas à gestão de riscos corporativos. Este comitê garante o alinhamento entre as políticas de risco e os objetivos estratégicos da organização, promovendo uma cultura de responsabilidade, transparência e participação nas tomadas de decisão.

O Comitê Executivo de Riscos é formado pelos representantes das seguintes áreas:



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 10/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			

- Vice-presidência Executiva
- Vice-presidência de Transporte e Logística
- Diretoria Financeira
- Diretoria Jurídica
- Diretoria de Gente e Gestão
- Diretoria de Sustentabilidade
- Gerência Executiva de Relações Institucionais
- Gerência GRC
- Diretores das áreas corporativas e de negócio, conforme objeto da pauta.

O comitê reunir-se-á **trimestralmente** e os Diretores das áreas corporativas e de negócio serão convocados para composição do comitê conforme as pautas das reuniões. A reunião do Comitê será conduzida pela Gerente da área de GRC.

Compete ao Comitê:

- Aprovar a Matriz de Riscos Corporativa
- Revisar periodicamente o apetite ao risco da organização
- Deliberar sobre planos de contingência e continuidade de negócios
- Validar os relatórios de risco encaminhados à Alta Direção.

O Comitê poderá ser convocado extraordinariamente sempre que identificado risco crítico, evento emergencial ou situação que exija resposta rápida.

O Comitê deve assegurar que sejam contemplados riscos estratégicos, financeiros, operacionais, de conformidade, tecnológicos, ESG, reputacionais e de terceiros.

O Comitê é responsável por garantir a comunicação tempestiva dos principais riscos e tendências à Alta Direção e demais partes interessadas relevantes.

PROCESSO DE GESTÃO DE RISCOS

1. Etapas do processo de Gestão de Riscos

O processo de gestão de riscos do Grupo SADA é conduzido de forma estruturada e contínua, com base nas diretrizes da norma ABNT NBR ISO 31000 e compreende as seguintes etapas, representadas na figura abaixo:



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 11/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			



(i) **Identificação de riscos:** Nesta fase são mapeados todos os possíveis riscos que podem afetar o Grupo SADA em observância aos processos estabelecidos e tipologia. O propósito da identificação de riscos é encontrar, reconhecer e descrever riscos que possam ajudar ou impedir que uma organização alcance seus objetivos.

(ii) **Análise de riscos:** Envolve a avaliação detalhada dos riscos identificados. O objetivo é compreender a natureza dos riscos, as causas, consequências, probabilidades e impacto possível.

- **Causa do risco:** é o fator, situação ou condição que pode dar origem ao risco.
- **Consequência:** é o resultado ou efeito gerado pela materialização do risco.
- **Probabilidade:** é a medida da chance de um evento de risco ocorrer. Refere-se à frequência ou à possibilidade de materialização do risco dentro de determinado período ou contexto.
- **Impacto:** é a medida da intensidade das consequências que a ocorrência de um risco pode gerar.

A **análise de probabilidade** de ocorrência do risco leva em consideração a seguinte escala estruturada em cinco níveis:

ESCALA	PROBABILIDADE	FREQUÊNCIA	DESCRIÇÃO
5	85% < 100%	Mais de 1 vez por mês	Esperado ocorrer na maioria das vezes
Muito Alta (Quase Certo)			
4	50% < 85%	Mais de 1 vez por semestre até 1 vez por mês	Provável que ocorra em grande parte das vezes
Alta (Provável)			



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 12/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			

3	15% < 50%	1 vez por ano a uma vez por semestre	Pode ocorrer em algum momento
Média (Possível)			
2	5% < 15%	Menos de uma vez por ano	Poderia ocorrer em circunstâncias excepcionais
Baixa (Rara)			
1	< 5%	Menos de uma vez em 5 anos	Poderia acontecer em circunstâncias raras
Muito Baixa (Improvável)			

No Grupo SADA, a **análise de impacto** leva em consideração as seguintes dimensões: imagem e reputação, financeiro, conformidade, operacional, saúde e segurança, estratégia e perenidade, também estruturados em uma escala de 5 níveis (muito baixo, baixo, médio, alto, muito alto).

O detalhamento dos parâmetros de avaliação de impacto do risco consta no Anexo desta Política.

(iii) **Avaliação de riscos:** Uma vez identificados, os riscos são avaliados quanto à sua criticidade, visando a priorização e decisão quanto ao tratamento. A priorização e tratamento dos riscos levará em conta os seguintes critérios:

RE	Risco Crítico	Nível de risco muito além do apetite a risco . Qualquer risco nesse nível deve ser comunicado ao Comitê Executivo de Risco e ter uma resposta imediata .
RA	Risco Alto	Nível de risco além do apetite a risco . Qualquer risco nesse nível deve ser comunicado ao Comitê Executivo de Riscos e ter uma ação tomada em curto período de tempo .
RM	Risco Moderado	Nível de risco dentro do apetite a risco . Requer atividades de monitoramento específicas e atenção da Gerência na manutenção de respostas e controles para manter o risco nesse nível ou reduzi-lo.
RB	Risco Baixo e Muito Baixo	Nível de risco dentro do apetite a risco , geralmente nenhuma ação é necessária, mas requer atividades de monitoramento específicas e atenção da Gerência na manutenção dos controles para manter o risco nesse nível.



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 13/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			

A priorização deverá estar validada em conformidade com o apetite e tolerância ao risco definidos pela Alta Direção.

(iv) Tratamento de riscos: Etapa onde as ações são planejadas e implementadas para lidar com os riscos identificados e analisados nas etapas anteriores. Nesta etapa será definida a resposta ao risco:

- **Mitigar (reduzir):** implementar controles ou ações que diminuam a probabilidade de ocorrência e/ou o impacto do risco.
- **Aceitar:** decidir conscientemente conviver com o risco, quando o nível residual do risco está dentro do apetite ao risco ou quando o custo de mitigação é maior que o benefício.
- **Compartilhar (transferir):** transferir total ou parcialmente o risco a terceiros, por meio de contratos, seguros, terceirizações.
- **Evitar:** eliminar a exposição ao risco, interrompendo ou não realizando a atividade que lhe dá origem.

Planos de Contingência e Resposta

Para os **riscos classificados como críticos** ou que apresentem potencial para interromper operações, afetar significativamente stakeholders, comprometer a segurança de pessoas, gerar danos ambientais ou causar prejuízos materiais relevantes, deverão ser elaborados **planos de contingência**.

Os planos de contingência têm como objetivo reduzir os impactos da materialização do risco e garantir a continuidade mínimas das operações essenciais, estabelecendo ações preventivas, corretivas e reativas que devem ser adotadas em situações de emergência.

O plano de contingência deve conter:

- Descrição do risco e cenários possíveis;
- Ações preventivas para evitar ou reduzir a probabilidade de ocorrência;
- Ações de resposta imediata em caso de materialização (emergência, contenção, comunicação);
- Procedimentos de continuidade para manter ou restabelecer operações essenciais;
- Responsáveis pelo acionamento, coordenação e execução das ações;
- Fluxo de comunicação interna e externa, incluindo stakeholders relevantes;
- Recursos necessários (equipamentos, sistemas, equipes, etc)
- Critérios de retomada

Os planos de contingência devem ser elaborados pelas áreas responsáveis pelo risco, e aprovados pelo Comitê Executivo de Riscos. Os planos de contingência deverão ser **revisados anualmente** ou quando houver mudanças significativas na operação, infraestrutura ou análise de riscos.

(v) Registro e relato: Tem por objetivo documentar de forma clara, estruturada e consistente todas as informações relevantes relacionadas aos riscos identificados, às análises realizadas, às decisões tomadas e às ações de tratamento implementadas.



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 14/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			

Os relatórios de risco serão elaborados pela Coordenação de GRC, validados pelas Gerências e Diretorias responsáveis pelos riscos e apresentados trimestralmente ao Comitê Executivo de Riscos para análise crítica e deliberações.

O relatório conterá:

- Mapa/matriz de Riscos
- Resumo dos riscos prioritários e suas avaliações finais
- Resumo dos planos de ação, status de implementação e responsáveis

Os relatórios deverão também subsidiar a tomada de decisão estratégica e, quando aplicável, a comunicação a stakeholders externos relevantes, como clientes, órgãos reguladores e seguradoras.

(vi) Monitoramento e Análise crítica: Na etapa de monitoramento, deve-se acompanhar continuamente a eficácia das ações implementadas e revisar o tratamento dos riscos quando necessário. Novos riscos podem surgir, e os riscos existentes podem mudar, exigindo ajustes nas estratégias de tratamento. A análise crítica consiste na revisão periódica e estruturada do processo de gestão de riscos, realizada pelo Comitê Executivo de Riscos.

Devem ser incorporadas lições aprendidas de incidentes passados e comparações com benchmarks de mercado para aprimoramento contínuo.

O processo de monitoramento dos riscos prevê:

- **Riscos Estratégicos:** monitoramento **semestral** pela Coordenação de Riscos e reportados ao Comitê Executivo de Riscos;
- **Demais riscos** sob a gestão da Coordenação de Riscos serão objeto de monitoramento **trimestral**, com reportes ao Comitê Executivo de Riscos em formato de relatório.

Análise do Comitê Executivo de Riscos

Durante a avaliação crítica do relatório de riscos pelo Comitê Executivo de Riscos, alguns itens essenciais devem ser considerados para garantir uma análise abrangente e efetiva. Entre eles, destacam-se:

- **Clareza na identificação dos riscos:** Verificar se todos os riscos relevantes para o negócio foram devidamente identificados e descritos de forma objetiva.
- **Classificação e priorização:** Avaliar se os riscos foram classificados quanto à sua magnitude e prioridade, considerando o alinhamento com o apetite de risco definido pela organização.
- **Efetividade dos controles internos:** Revisar a robustez dos controles implementados, avaliando tanto o desenho quanto a eficácia operacional destes mecanismos.
- **Plano de ação e tratamento:** Analisar se as estratégias de tratamento estão bem estruturadas, incluindo cronogramas, responsáveis e indicadores de acompanhamento.
- **Análise dos riscos residuais:** Considerar o nível de exposição que permanece após as ações de mitigação e se este está compatível com os objetivos estratégicos e a tolerância da organização.
- **Monitoramento contínuo:** Certificar-se de que há processos eficazes para o acompanhamento dos riscos e revisão frequente dos planos de resposta.



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 15/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			

- **Emergência de novos riscos:** Observar a capacidade de identificar e reagir a riscos emergentes, bem como a atualização contínua do relatório.
- **Comunicação e transparência:** Avaliar se o relatório de riscos promove a comunicação adequada com todas as partes interessadas e se as informações são apresentadas de forma clara e acessível.

(vii) Comunicação e consulta: A comunicação e consulta são processos essenciais para apoiar a tomada de decisão, promover a compreensão compartilhada dos riscos e fortalecer a cultura de gestão de riscos em todo o Grupo SADA.

Todas as partes interessadas relevantes (internas e quando for o caso, externas), devem receber informações relevantes, tempestivas e adequadas sobre riscos, controles, responsabilidades e decisões estratégicas relacionadas ao tema.

2. Risco Inerente, Residual e Controles

A gestão de riscos do Grupo SADA considera tanto os riscos inerentes quanto os riscos residuais em suas análises.

O **risco inerente** é o nível de risco existente antes da aplicação de controles ou medidas de tratamento, refletindo a exposição natural de risco da organização. O risco inerente é o resultado da probabilidade X impacto do risco.

A redução do risco inerente depende da implementação de controles internos, que são classificados em:

- **Preventivos:** evitam a ocorrência do risco (ex: segregação de funções, políticas e procedimentos);
- **Detectivos:** identificam rapidamente a ocorrência do risco (ex: auditorias, conciliações, monitoramentos automatizados);
- **Corretivos:** reduzem os efeitos após a ocorrência do evento (ex: planos de contingência, backups, seguros)

Os controles devem ser definidos considerando os fatores de risco identificados, uma vez que estes representam as causas ou condições que podem levar à materialização do risco. Os controles devem ser periodicamente testados, revisados e documentados, garantindo rastreabilidade, conformidade regulatória e possibilidade de auditoria independente.

O **risco residual** é o nível de risco que permanece após a implementação de controles e planos de mitigação, representando a exposição efetiva da empresa. A mensuração do risco residual se dá pela avaliação dos controles implementados, que deve considerar o desenho do controle (se o controle foi adequadamente planejado para tratar o risco) e a efetividade da execução (se o controle está sendo aplicado de forma consistente e eficaz na prática).

Os controles serão avaliados conforme os seguintes critérios:

Nível do controle	Descrição	Fator de avaliação
Inexistente	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais	1



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 16/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			

Fraco	Controles com abordagem pontual, tendem a ser aplicados caso a caso, a responsabilidade é individual, havendo elevado grau de confiança no conhecimento das pessoas	0,8
Mediano	Controles implementados mitigam alguns aspectos do risco, mas não contemplam todos os aspectos relevantes do risco devido a deficiências no desenho ou nas ferramentas utilizadas	0,6
Satisfatório	Controles implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente	0,4
Forte	Controles implementados podem ser considerados a “melhor prática” mitigando todos os aspectos relevantes ao risco	0,2

O risco residual será calculado levando-se em consideração o valor do risco inerente, multiplicado pelo fator de avaliação (peso) do controle.

A análise do risco residual deverá indicar claramente se o risco está dentro do apetite definido pela organização, e, quando não estiver, deverá ser obrigatoriamente acompanhado de plano de ação com prazos, responsáveis e indicadores de acompanhamento.

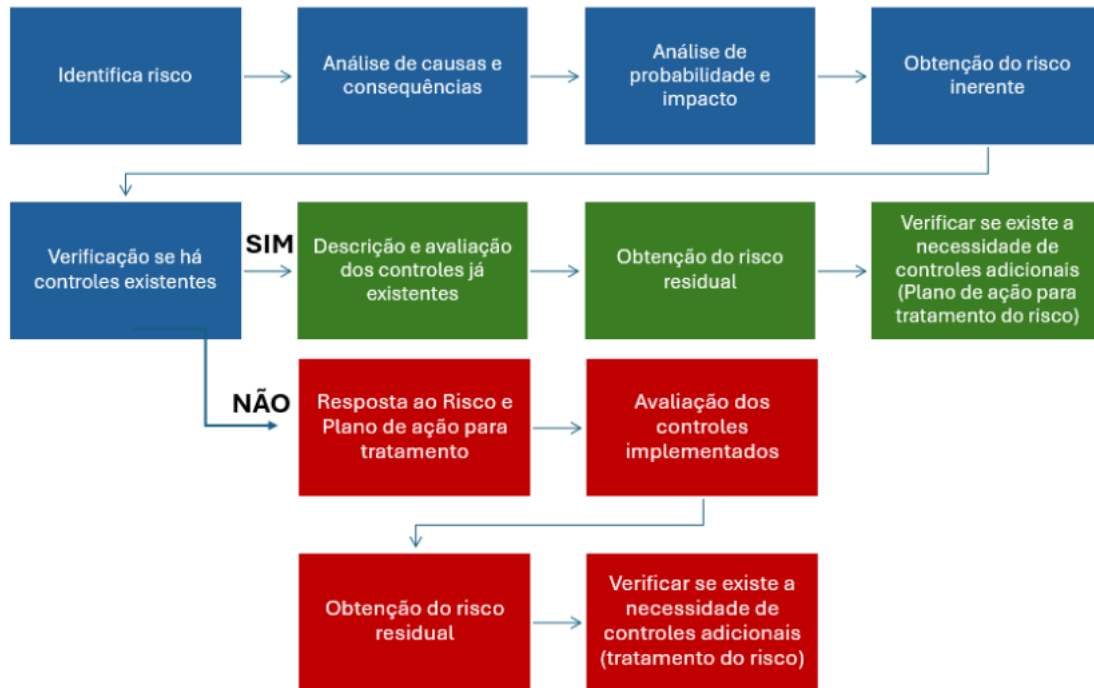
O risco residual servirá de base para decisões referentes à necessidade ou não de tratamento adicional, conforme o risco se encontre ou não dentro do apetite ao risco e critérios de priorização.

3. Visão geral do fluxo de identificação e tratamento dos riscos

O fluxo de identificação e tratamento dos riscos deve garantir que todos os riscos sejam registrados em ferramenta corporativa, analisados conforme os parâmetros definidos nesta política e acompanhados até sua conclusão. O processo inclui: identificação, análise, avaliação, tratamento, monitoramento e reporte periódico ao Comitê Executivo de Riscos. As áreas responsáveis deverão assegurar que cada risco possua um responsável designado, plano de ação quando necessário, prazo de implementação e indicadores de acompanhamento.



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 17/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			



4. Abordagem para Riscos Emergentes

O Grupo SADA reconhece que o ambiente de negócios é dinâmico e que novos riscos podem surgir, bem como os riscos existentes podem evoluir rapidamente.

Os riscos emergentes caracterizam-se como riscos novos ou em evolução, ainda não totalmente mapeados frequentemente difícil de quantificar, que pode impactar a organização no médio ou longo prazo (ex.: riscos climáticos, tecnológicos ou reputacionais).

Para garantir a adaptabilidade e resiliência, a abordagem para riscos emergentes inclui:

- **Monitoramento Contínuo do Cenário:** As áreas de negócio devem manter um monitoramento proativo do ambiente interno e externo, incluindo tendências de mercado, mudanças regulatórias, avanços tecnológicos e fatores socioeconômicos, que possam gerar novos riscos ou alterar o perfil dos riscos existentes.
- **Comunicação Imediata:** Colaboradores e gestores devem comunicar formal e tempestivamente, (prazo máximo de **5 dias**, ou antes, conforme a gravidade do risco), à Coordenação de Governança e Riscos (GRC) pelo e-mail governanca.integridade@sada.com.br, o surgimento de qualquer novo risco potencial ou alteração significativa em riscos já mapeados que possam afetar o grau de exposição do Grupo SADA. Ao ser comunicada, a área de GRC deverá reportar a identificação do Risco Emergente ao Comitê Executivo de Riscos para as análises cabíveis no prazo.



Documento: IDPLGS-090	Revisão: 2	Emissão: 13/02/2026	Página: 18/18
Informação Documentada - Política Grupo SADA			
Título: POLITICA DE GESTÃO DE RISCOS			

▪ **Avaliação e Resposta Rápida:** Riscos emergentes identificados serão submetidos a um processo acelerado de identificação, análise e avaliação, garantindo que as ações de tratamento apropriadas sejam definidas e implementadas de forma ágil, conforme as etapas do processo de Governança e Gerenciamento de Riscos descritas nesta política.

▪ **Revisão Periódica da Tipologia:** A tipologia de riscos será revisada periodicamente para incorporar novas categorias de riscos que se tornem relevantes para o Grupo SADA, assegurando que a estrutura de classificação esteja sempre atualizada.

6. DISPOSIÇÕES FINAIS

A Governança e Gerenciamento de Riscos opera de forma integrada com outras políticas e normativos internos do Grupo SADA, incluindo, mas não se limitando, ao Código de Conduta Ética (ID738), Código de Conduta Ética – Relações Terceirizadas (ID2058) e demais procedimentos que visam à conformidade e à governança corporativa. Esta integração assegura uma abordagem abrangente na proteção de valor e na sustentabilidade do negócio.

A efetividade da Governança e Gerenciamento de Riscos no Grupo SADA é intrinsecamente ligada à sinergia e ao alinhamento com outras políticas e frameworks de governança existentes. A colaboração contínua entre as áreas e a aderência a um conjunto de normativos internos são essenciais para o cumprimento dos objetivos desta política.

O Canal de Denúncias é uma ferramenta valiosa para a Governança e o Gerenciamento de Riscos, pois permite a identificação e o relato de irregularidades e más condutas que podem representar riscos para o Grupo SADA. O Grupo SADA disponibiliza o Canal de denúncias para o recebimento de relatos de descumprimento desta Política e demais premissas tratadas no Código de Conduta Ética de Relações Terceirizadas e de Colaboradores, além das demais políticas e procedimentos internos do Grupo ou da legislação vigente:

Telefone: 08008008303

Site: www.contatoseguro.com.br/gruposada

A **revisão** desta Política deverá ocorrer, no mínimo, a cada 2 (dois) anos ou sempre que houver mudanças significativas no contexto estratégico, regulatório ou operacional da organização.

7. ANEXOS

Código de Conduta Ética do Grupo SADA (ID738)

Código de Conduta Ética de Relações Terceirizadas (ID2058)