I. Objetivo:

A Política de Gestão de Riscos tem por finalidade estabelecer as diretrizes a serem observadas no processo de gestão de riscos da Cogna ("Companhia") e suas controladas/subsidiárias, de forma a assegurar que os riscos sejam conhecidos e monitorados continuamente pela Companhia e que o ambiente de gestão de riscos esteja em conformidade com a legislação e a regulamentação vigentes.

As atividades de gerenciamento de riscos são realizadas por estruturas específicas como políticas, análise de processos, entrevistas, elaboração de matrizes de riscos, dentre outras. Nesta Política é apresentada a estrutura operacional e as diretrizes da gestão de riscos da Companhia, assim como as responsabilidades de cada área envolvida nesse processo.

O processo de gestão de riscos visa possibilitar a tempestiva educação, análise, planejamento, tratamento, comunicação e monitoramento dos riscos as quais a Companhia está exposta.

II. Área Tutora:

Diretoria de Compliance (DC)

III. Áreas Envolvidas:

Esta política se aplica a todas as áreas, unidades e empresas do grupo Cogna.

IV. Conceitos:

Gestão de Riscos: Atividades estruturadas com objetivo de identificar, prevenir e mitigar eventos que possam prejudicar ou impossibilitar o atingimento dos objetivos e estratégias de negócio da Companhia. Este processo tem por objetivos: i) aumentar a probabilidade de atingimento dos objetivos; ii) melhorar a capacidade de identificar oportunidades e ameaças; iii) alocar de forma mais eficaz os recursos para tratativa dos riscos mais significantes.

Risco Inerente: Representa o nível de risco geral de um evento, sem considerar a atuação dos controles existentes como instrumentos de mitigação.

Universo de Riscos: Totalidade de riscos que podem impactar a Companhia.

Categorias de Riscos: Trata-se da Linguagem Comum de Riscos (LCR) que busca uniformizar internamente e externamente as referências aos diversos riscos que podem impactar a Companhia. Na Companhia, são classificados como:

1. **Estratégicos:** Riscos que podem prejudicar o núcleo do modelo de negócios da Companhia. Desafiam a lógica das escolhas estratégicas, ameaçam a competitividade e prejudicam a capacidade de se alcançar ou manter um desempenho excepcional.

2. **Financeiros:** Riscos que podem afetar de forma adversa as finanças da Companhia, principalmente devido à fatores relacionados ao mercado (câmbio, juros, inflação, etc) e crédito. São decorrentes de variações de valores de ativos e passivos no mercado, descumprimento de obrigações financeiras de contrapartes, alto custo ou incapacidade de cumprir suas obrigações financeiras, ineficiência na alocação do capital ou falhas nos reportes financeiros.

3. **Operacionais:** Riscos decorrentes das falhas de processos e controles, falta de consistência e adequação dos sistemas de informação, bem como oriundos de erros ou fraudes que prejudiquem ou impossibilitem o exercício das atividades da companhia.

4. **Legais/Regulatórios:** Riscos relacionados a sanções legais ou regulatórias, de perda financeira ou de reputação que a empresa pode sofrer como resultado da falha no cumprimento da aplicação de leis, acordos e regulamentos.

5. **Tecnologia**: Riscos que podem expor os ativos de informação da Companhia a ameaças conhecidas ou desconhecidas através de ataques cibernéticos.

Riscos ao Programa de Integridade, Ética e Conduta: Subcategoria de risco que atualmente compõe a categoria de Riscos Estratégicos, no Dicionário de Riscos da Companhia. Conforme definido na Portaria CGU nº 1.089/2018, riscos à Integridade são riscos provenientes de ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção e, conforme apresentado no Guia Prático de Gestão de Riscos para a Integridade, também elaborado pelo Ministério da Transparência e Controladoria Geral da União, comummente, são atos de caráter quase sempre doloso, praticado por uma pessoa ou por um grupo de pessoas, que envolve afronta aos princípios da administração pública (legalidade, impessoalidade, moralidade, publicidade e eficiência) sendo destacados como uma quebra à impessoalidade e/ou moralidade.

Fraude: Ato intencional praticado por um ou mais indivíduos da organização (empregados ou terceiros), envolvendo o uso de propositado de falsidades para obter uma vantagem injusta ou ilegal. No âmbito do direito penal, um crime de fraude consiste em qualquer ato ilegal de iludir terceiros com o intuito de prejudicá-los.

Corrupção: Ato tipificado pelo Código Penal (Decreto-Lei nº 2.848, de 7 de dezembro de 1940) como crime contra a Administração Pública, sendo discriminado em Corrupção Passiva (*"Solicitar ou receber, para si ou para outrem, direta ou indiretamente, ainda que fora da função ou antes de assumi-la, mas em razão dela, vantagem indevida, ou aceitar promessa de tal vantagem"*) e Corrupção Ativa (*"Oferecer ou prometer vantagem indevida a funcionário público, para determiná-lo a praticar, omitir ou retardar ato de ofício"*)

Fator de Risco: Situações e/ou circunstâncias que podem levar ao aumento da probabilidade de materialização de um risco.

Cultura de Riscos: Atitude geral da Companhia na abordagem de riscos.

Apetite ao Risco: Nível de risco que a Companhia está disposta/preparada a tolerar na busca pela realização de sua estratégia e atingimento de seus objetivos de negócio.

Dono do Risco (*Risk Owner*): Pessoa/Área com responsabilidade e autoridade para gerenciar determinado risco.

Grau de exposição ao risco (Nível de severidade): Nível relativo de gravidade de certo risco para a Companhia, obtido através da combinação dos seguintes conceitos:

I. **Probabilidade de ocorrência:** Grau de possibilidade de o risco ser materializado. Está intimamente relacionando ao grau de maturidade da estrutura de controles na sua eficácia na mitigação do Risco (ex.: Alta maturidade de controles implica em menor probabilidade de ocorrência / Baixa maturidade de controles implica em maior probabilidade de ocorrência).

II. **Impacto da ocorrência:** Grau de criticidade que a Companhia será atingida caso o risco venha a se materializar. Pode estar relacionado a perdas financeiras, operacionais, de reputação, entre outras. É calculado como um produto da: (i) gravidade, (ii) velocidade e (iii) complexidade de recuperação.

Tolerância ao Risco: É a aplicação do apetite estabelecido pela Companhia a se expor a determinado risco. Pode resultar em 3 cenários (graus de exposição):

- **Exposição Inaceitável:** O risco está acima do nível de tolerância / apetite da Companhia e deve ser mitigado;
- **Ponto de atenção:** O risco está no limite do nível de tolerância / apetite da Companhia e deve ser avaliado se ações mitigatórias devem ser implementadas;
- **Exposição aceitável:** O risco está dentro dos limites de tolerância da Companhia.

Resposta ao Risco: Ação direcionada para alterar o nível de exposição a um risco impactando a sua probabilidade e/ou impacto.

Risco Residual: Nível de risco remanescente após a implementação de uma ou mais respostas ao risco inerente.

Dicionário de Riscos: Modelo gráfico utilizado pela Companhia para consolidar todos os riscos mapeados e os dividir nas categorias (descritas acima) e subcategorias.

Mapa de Priorização de Riscos: Também conhecido como “mapa de calor” ou “heat map” representa a plotagem dos riscos em uma matriz como efeito da combinação de impacto e probabilidade para cada risco avaliado.

Key Risk Indicators (KRI): Principais indicadores de risco da Companhia. Funcionam como sinais de alerta e embasamento para a tomada de decisões pelos *Risk Owners* indicando as mudanças no nível de risco de uma organização ou de seus negócios e a necessidade ou não da implementação de respostas adicionais.

V. Papéis e Responsabilidades:

A. Conselho de Administração:

1. Aprovar estratégia e objetivos de curto, médio e longo prazo da Companhia;
2. Aprovar a Política de Gestão de Riscos da Companhia, incluindo as atribuições dos órgãos da Companhia responsáveis por sua implementação e acompanhamento, conforme previstas nesta política;
3. Aprovar Análise Geral de Riscos (AGR), apresentada no mínimo anualmente, pelo Comitê de Auditoria e Risco;
4. Aprovar o nível de Apetite ao Risco; e
5. Aprovar eventuais exceções relacionadas à Política de Gestão de Riscos, mediante recomendações realizadas pelo Comitê de Auditoria e Risco.

B. Comitê de Auditoria e Risco:

1. Supervisionar continuamente, no mínimo anualmente, o processo de Gestão de Riscos da Companhia, reportando fatos relevantes ao Conselho de Administração conforme necessidade;
2. Aprovar a metodologia e abordagem de Gestão de Riscos; e
3. Apresentar ao Conselho de Administração (no mínimo anualmente) a avaliação do processo de Gestão de Riscos; e
4. Avaliar (no mínimo anualmente) a adequação de estrutura de Governança responsável pela Gestão de Riscos, seu orçamento, metodologia e outros aspectos relacionados à Gestão de Riscos da Companhia e submetê-los ao Conselho de Administração.

C. Presidência:

1. Atuar como responsável em última instâ ncia pela Gestão dos Riscos da Companhia, garantindo a implantação de modelo eficiente de Gestão de Riscos através da definição de recursos humanos, financeiros e materiais que garantam a adequada operacionalização desta função; e
2. Promover a integração da Gestão de Riscos com os ciclos de gestão e planejamento da Companhia.

D. Vice-Presidências/Diretorias/Áreas de Negócio:

1. Validar o Universo de Riscos da Companhia, atuando proativamente na identificação de eventos que potencialmente podem impactar negativamente a Companhia no atingimento de seus objetivos;
2. Atuar como "*Owners"* dos riscos aos quais a Companhia está exposta, identificando e gerenciando os mesmos, tomando medidas necessárias para mantê-los no nível de apetite estabelecido e validado pelo Conselho de Administração;
3. Propor níveis de Apetite ao Risco relacionados às suas atividades para validação pelo Conselho de Administração;
4. Implementar e garantir a manutenção contínua das respostas estabelecidas aos riscos (controles internos, seguros, etc.), assegurando que os riscos residuais estejam alinhados ao nível de Apetite ao Risco estabelecidos e validados; e
5. Acompanhar os KRIs e as estratégias de mitigação dos riscos.

E. Gerência de Gestão de Riscos (Diretoria de Compliance):

1. Estabelecer estrutura/metodologia de Gestão de Riscos da Companhia e apresentar para validação do Comitê de Auditoria e Risco;
2. Realizar manutenções na Política de Riscos, submetendo para aprovação do Conselho de Administração sempre que mudanças representativas no processo forem implementadas;
3. Consolidar informações sobre os riscos aos quais a Companhia está exposta;
4. Atuar como facilitador junto ao Conselho de Administração, Comitê de Auditoria e Risco, Presidência, Vice-Presidências e Diretorias Executivas no cumprimento de suas respectivas atribuições relacionadas à Gestão de Riscos;
5. Consolidar informações sobre avaliações e monitoramento de riscos da Companhia, reportando tais informações nas reuniões trimestrais do Comitê de Auditoria e Risco;
6. Atuar na disseminação da cultura de Riscos, Controles Internos e *Compliance* entre os colaboradores da Companhia;
7. Coordenar a Análise Geral de Riscos (AGR), cujo ciclo completo será concluído integralmente no decorrer de dois anos, realizando avaliação em todas as áreas de negócios com objetivo de atualizar percepções sobre riscos e necessidades de aprimoramentos;
8. Fornecer informações necessárias ao Presidente e Comitê de Auditoria de Risco para realização (no mínimo anualmente) de avaliação do processo de gestão de riscos como um todo; e
9. Submeter anualmente ao Comitê de Auditoria e Riscos a estrutura responsável pela Gestão de Riscos e seu respectivo orçamento para desempenho de suas funções e atribuições.

VI. Descrição do Processo:

A. Condução da Análise Geral de Riscos (AGR):

A gestão dos riscos aos quais a Companhia está exposta é exercida por todos os colaboradores das áreas de negócio da Companhia e Alta Administração, sob a figura da Primeira Linha de Defesa. Contudo, a equipe de Gestão de Riscos e Controles Internos, como parte da Segunda Linha de Defesa responsável pelo assessoramento das áreas de negócio na gestão dos riscos da Companhia, conduz, durante um ciclo de dois anos, a Análise Geral de Riscos (AGR), segundo as melhores práticas contidas no COSO ERM 2017 e na Norma ISO 31.000/2018. A seguir são descritas as etapas conduzidas:

1. **Estabelecimento de canais de comunicação e consulta** para que as informações pertinentes ao processo sejam coletadas, analisadas e validadas da forma apropriada entre a equipe de Gestão de Riscos e Controles Internos, as áreas de negócio responsáveis pelos riscos e a Administração da Companhia. Cabe destacar que esta atividade deve permear todas as demais etapas do processo.
2. **Definição do escopo, contexto e critérios** a serem adotados como premissas no processo de Análise Geral de Riscos.
    a. No que diz respeito ao escopo, deve ser definido pela equipe de Gestão de Riscos e Controles Internos, junto à Administração da Companhia se a AGR contemplará as atividades da Holding, atividades exclusivas de suas subsidiárias, etc. Cabe destacar que usualmente são conduzidas análises separadas para Cogna e para suas subsidiárias.

    b. Com relação ao contexto (interno e externo), devem ser definidos quais os fatores internos e externos que podem influenciar o sucesso em alcançar os objetivos da Companhia. Cabe destacar que tal atividade é conduzida efetivamente ao longo das entrevistas de identificação de riscos, onde os executivos apontam sua percepção sobre tais fatores.

    c. Já no que diz respeito aos critérios, a Companhia deve especificar a quantidade e o tipo de risco que pode ou não assumir em relação ao atingimento dos objetivos, bem como deve estabelecer critérios para avaliar a significância do risco e para apoiar os processos de tomada de decisão. Pode também ser entendido como o Apetite ao Risco.

3. **Identificação dos riscos** aos quais a Companhia está exposta, de forma *Top-Down*, por meio da condução de reuniões com o corpo executivo da Companhia (N1 e N2) e com membros de órgãos de Governança Corporativa da Companhia (Conselho de Administração e Comitê de Auditoria e Risco). Tais percepções podem também ser complementadas com informações provenientes de outras fontes, como: (i) AGRs anteriores, (ii) trabalhos especiais, (iii) análises de Auditoria Interna e/ou Controles Internos, (iv) inputs dos Auditores Independentes, entre outras fontes consideradas como relevantes. Cabe destacar que nesta etapa podem ser contemplados riscos de diversas categorias, conforme descrito na seção de conceitos, incluindo riscos ao Programa de Integridade, Ética e

Conduta e demais riscos relativos às atividades e operações da Companhia, sendo todas as atividades do processo de Gestão de Riscos comuns a todas as diferentes categorias.

4. **Análise dos riscos** identificados, de forma a possibilitar a elaboração do Mapa de Priorização dos Riscos (Mapa de Calor ou "*Heat Map*"), representado graficamente por uma matriz 5x5. Tal análise é conduzida por meio da determinação (junto aos responsáveis por cada um dos riscos identificados) do grau de impacto (eixo Y do mapa) e do grau de probabilidade (eixo X do mapa), resultando no grau de severidade do risco (distinguidos entre os 25 quadrantes do mapa). Nesta etapa, devem ser identificados os graus de severidade inerentes (sem a aplicação de controles/respostas para a mitigação dos riscos) e residuais (com a aplicação dos controles/respostas existentes para a mitigação dos riscos), fornecendo insumos para a etapa de Avaliação dos Riscos (descrita no item a seguir).

5. **Avaliação dos riscos** identificados, por meio da comparação: (i) dos resultados da etapa de Análise de Riscos com (ii) o apetite ao risco estabelecido (grau de severidade aceito), visando determinar para quais riscos é necessário que sejam tomadas ações adicionais para trazê-lo(s) ao grau de severidade aceito pela Companhia por meio de ações de tratamento, a serem colocadas em prática conforme prioridades definidas pela Companhia.

6. Caso seja identificado que o grau de severidade dos riscos esteja em níveis superiores aos definidos pela Companhia, são então definidas as ações de **tratamento dos riscos**, por meio do aprimoramento de controles já existentes ou criação, implementação de novos controles e/ou outras respostas aplicáveis. Nesta etapa, cabe destacar que são considerados: (i) o custo vs. benefício do controle a ser desenvolvido/mantido e (ii) eventuais riscos que podem surgir decorrentes da etapa de tratamento dos riscos.
   Podem ser consideradas como opções de tratamento dos riscos:

   a. Evitar o risco (suspender/cancelar a atividade que dá origem ao risco);

   b. Compartilhar o risco (ex.: contratação de seguros);

   c. Mitigar o impacto ou a probabilidade de materialização do risco por meio do aprimoramento e/ou criação de controles/respostas ao risco;

   d. Aumentar o risco visando perseguir uma oportunidade; e

   e. Aceitar o risco a partir de decisão fundamentada do dono do risco e/ou da Administração.

7. **Monitoramento e análise crítica** do resultado do processo, com o objetivo de captar eventuais novos riscos e/ou modificações em riscos já existentes decorrentes de alterações nos objetivos da Companhia e/ou no contexto interno/externo. Cabe destacar que esta atividade deve permear todas as demais etapas do processo.

8. **Registro e relato** de todas as etapas da AGR, visando demonstrar aos envolvidos (áreas de negócio e Administração): (i) as etapas envolvidas no processo, (ii) os resultados parciais e totais do processo, (iii) uma fonte para tomadas de decisões relacionadas aos riscos de forma crítica e embasada e (iv) uma fonte para a criação de plano(s) de tratamento de riscos.

Cabe destacar que, como parte integrante das responsabilidades da Diretoria de Compliance na mitigação e riscos relacionados ao Programa de Integridade, Ética e Conduta, está a responsabilidade pela elaboração e disseminação de Instrumentos Normativos, como o Código de Conduta e a Política Anticorrupção, contendo as diretrizes a serem seguidas pelos colaboradores do ambiente corporativo e acadêmico (estagiários, aprendizes, membros do Conselho de Administração e de seus Comitês de Assessoramento, alunos, clientes, autores, fornecedores, distribuidores, parceiros comerciais, prestadores de serviços) e outras pessoas ou empresas que, de alguma forma, possam ter relacionamento com a Cogna e suas subsidiárias. Está sob responsabilidade da Diretoria de Compliance elaborar, divulgar e acompanhar e realização da treinamentos obrigatórios referentes à ambos os temas.

B. Revisão e aprovação da Análise Geral de Riscos (AGR):

No que diz respeito à revisão/aprovação do conteúdo da AGR, tanto os resultados intermediários do processo (relação de riscos mapeados, categorias de riscos, mapa de riscos sensibilizado, etc.), quanto o resultado final da Análise, contendo a visão dos riscos residuais e planos de ação para tratamento dos mesmos são apresentados para avaliação do Comitê Executivo e do Comitê de Auditoria e Risco.

VII. Documentos de Referência:

- COSO ERM 2017 (*Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework).*
- Norma ABNT Standard NBR ISO 31000:2018 - Gestão de Riscos: Princípios e Diretrizes.
- Guia de Orientação para Gerenciamento de Riscos Corporativos – IBGC (Instituto Brasileiro de Governança Corporativa).
- Declaração de Posicionamento do IIA de 2013: “As três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles”.
- Portaria CGU nº 1.089/2018.
- Guia Prático de Gestão de Riscos para a Integridade - Ministério da Transparência e Controladoria Geral da União (CGU).

VIII. Aprovação:

- Gerência de Gestão de Riscos;
- Diretoria de Compliance;
- Vice-Presidência de Finanças Cogna (CFO);
- Presidência Cogna;
- Comitê de Auditoria e Risco Cogna; e
- Conselho de Administração Cogna.