

Revisão:	Data de Elaboração:	Data de publicação:	Data de revisão:
00	22/07/2021	18/02/2022	18/02/2023
Unidade Responsável:		Aprovada por:	
Comitê do Sistema de Integridade da H&P		Diretoria da H&P	

SUMÁRIO

1.	OBJETIVO.....	2
2.	APLICAÇÃO.....	2
3.	AMBIENTE NORMATIVO.....	2
4.	PRINCÍPIOS DA GESTÃO DE RISCOS.....	2
5.	COMPETÊNCIAS E RESPONSABILIDADES.....	4
5.1.	Diretoria da H&P.....	4
5.2.	Comitê de Governança, Ética, Riscos e Sustentabilidade.....	4
5.3.	Gestor de Governança, Riscos e Compliance.....	5
5.4.	Proprietários de Riscos.....	5
6.	PROCESSO DE GESTÃO DE RISCOS.....	5
6.1.	Contexto e critérios.....	6
6.2.	Identificação e Análise de riscos.....	7
6.3.	Avaliação de riscos.....	8
6.4.	Tratamento de riscos.....	8
6.5.	Comunicação e reporte.....	9
6.6.	Monitoramento.....	10
7.	PROGRAMA DE GESTÃO DE RISCOS.....	10
8.	COMITÊ DE GOVERNANÇA, ÉTICA, RISCOS E SUSTENTABILIDADE.....	11
9.	DISPOSIÇÕES FINAIS.....	11
	HISTÓRICO DE REVISÕES.....	12
	GLOSSÁRIO.....	12

1. OBJETIVO

A Política de Gestão de Riscos (“Política”) tem como objetivo estabelecer princípios, diretrizes e responsabilidades para a gestão de riscos da Herkenhoff & Prates (“H&P”). A gestão de riscos na H&P tem como objetivo auxiliar a tomada de decisão com vistas a prover segurança no cumprimento da missão e no alcance dos objetivos institucionais. Esta Política integra o Sistema de Integridade da H&P e institui seu Programa de Gestão de Riscos que consiste no conjunto de instrumentos de governança e de gestão que suportam a concepção, implementação, monitoramento e melhoria contínua da gestão de riscos e compreende, entre outros: política, manual, estruturas organizacionais, planos, responsabilidades, processos e recursos.

2. APLICAÇÃO

As regras contidas nesta Política devem ser respeitadas pelos sócios, comitês de assessoramento, diretores executivos, colaboradores próprios ou não, estagiários, menores aprendizes, prestadores de serviço e por qualquer pessoa que atue em nome da H&P ou que com ela se relacione. A implantação da gestão de riscos é direcionada pela diretoria da H&P e executada de forma integrada por toda a empresa, sendo aplicável aos seus diversos processos de trabalho, projetos e ações. O processo de gestão dos riscos é integrado ao planejamento estratégico, à governança, aos controles internos e às práticas do Sistema de Integridade da H&P.

3. AMBIENTE NORMATIVO

Esta Política foi elaborada em consonância com todas as leis e regulamentações aplicáveis, incluindo, mas sem limitação: Diretrizes COSO ERM:2017; ABNT NBR ISO/IEC 31.000:2018; Código de Conduta da H&P.

4. PRINCÍPIOS DA GESTÃO DE RISCOS

Buscando ser eficaz em todos os níveis, a gestão de riscos da H&P observa os seguintes princípios que servem de base para sua aplicação e interpretação:

- **Criação e proteção dos valores institucionais:** a gestão de riscos da H&P contribui para a realização de seus objetivos, promovendo inovação e ação empreendedora responsáveis de modo a agregar valor à empresa e a seu ambiente institucional;
- **Integração e aplicação contínua a todos os processos, atividades e projetos da H&P:** A gestão de riscos da H&P faz parte das responsabilidades de seus colaboradores e é parte integrante de todos os seus processos, atividades e projetos;
- **Integração no processo de tomada de decisões:** a gestão de riscos auxilia a diretoria da H&P e os tomadores de decisão a fazer escolhas conscientes, priorizando ações e distinguindo entre formas alternativas de ação;
- **Uso de melhores fontes disponíveis:** o processo de gestão de riscos na H&P é baseado nas melhores fontes disponíveis considerando suas limitações e incertezas associadas para avaliar quaisquer riscos e oportunidades;
- **Abordagem sistemática, estruturada e oportuna:** a H&P utiliza-se de uma abordagem sistemática, oportuna e estruturada para a gestão de riscos visando contribuir para a eficiência e para os resultados consistentes, comparáveis e confiáveis;
- **Customização e consideração dos fatores humanos e culturais:** a gestão de riscos da H&P considera os objetivos institucionais, o ambiente interno e externo e seu perfil de risco, reconhecendo também a influência dos fatores humanos e culturais em todos os aspectos da gestão;
- **Transparência e inclusão:** a gestão de riscos da H&P busca o envolvimento apropriado e oportuno das partes interessadas, possibilitando que seus conhecimentos, pontos de vista e percepções sejam considerados e resultem em um processo mais inclusivo e fundamentado;
- **Dinamicidade, interatividade e adaptabilidade:** a gestão de riscos da H&P acompanha as modificações que possam propiciar o surgimento, a mudança ou o desaparecimento de riscos. O processo de gestão de riscos deve antecipar, detectar, reconhecer e responder a alterações e eventos, oportunamente e apropriadamente;
- **Implantação em ciclos de revisão e melhoria contínua:** a gestão de riscos da H&P é melhorada continuamente a cada ciclo de gestão,

incorporando as lições aprendidas, as experiências e o aprendizado institucional.

5. COMPETÊNCIAS E RESPONSABILIDADES

5.1. Diretoria da H&P

- Patrocinar a gestão de riscos e seus instrumentos na H&P, zelando pelos princípios e diretrizes estabelecidos nesta Política;
- Aprovar a esta Política e suas revisões;
- Direcionar a implantação da gestão de riscos na H&P;
- Integrar o processo de gestão dos riscos ao planejamento estratégico, à governança e aos controles internos de gestão da H&P;
- Assegurar a alocação dos recursos necessários à implantação desta Política e de controles internos efetivos;
- Aprovar o apetite, a tolerância e definir os critérios de riscos da H&P;
- Deliberar sobre recomendações e relatórios apresentados pelo Comitê.

5.2. Comitê de Governança, Ética, Riscos e Sustentabilidade

- Disseminar cultura voltada para identificação, avaliação e tratamento de riscos;
- Deliberar sobre temas relacionados à gestão de riscos e controles internos;
- Deliberar sobre a metodologia, procedimentos e práticas inerentes ao processo de gestão de riscos e controles internos;
- Propor o apetite, a tolerância e os critérios de riscos da H&P;
- Avaliar a adequação, suficiência e eficácia do Programa de Gestão de Riscos da H&P;
- Elaborar recomendações e relatórios sobre temas relacionados a esta Política;
- Deliberar sobre a priorização dos riscos e submeter recomendação e proposição à Diretoria;
- Realizar reportes periódicos à Diretoria sobre os indicadores do Programa de Gestão de Riscos;

- Convocar, quando necessário, o Gestor de Governança, Riscos e Compliance, os coordenadores das áreas e os proprietários de riscos para prestar esclarecimentos;
- Propor a revisão desta Política.

5.3. Gestor de Governança, Riscos e Compliance

- Orientar a capacitação dos colaboradores da H&P sobre a gestão de riscos;
- Prestar assistência técnica e metodológica sobre gestão de riscos e controles internos às áreas da H&P para a implementação das recomendações do Comitê e das deliberações da Diretoria;
- Acompanhar a execução das ações de tratamento de riscos;
- Monitorar a efetividade, a eficiência e a eficácia dos processos de gestão de riscos e dos controles internos da H&P;
- Receber relatos de riscos identificados pelos Proprietários de Riscos e dar devido encaminhamento;
- Elaborar recomendações e relatórios sobre temas relacionados a esta Política;
- Realizar reportes periódicos ao Comitê sobre os indicadores do Programa de Gestão de Riscos.

5.4. Proprietários de Riscos

- Avaliar os riscos no âmbito das áreas, processos e atividades que lhes são afetos;
- Implementar a gestão de riscos em sua área e gerenciá-los de forma a mantê-los em um nível de exposição aceitável;
- Assegurar a implementação dos planos de ação para mitigação de riscos;
- Comunicar tempestivamente os riscos identificados ao Gestor de Governança, Riscos e Compliance;
- Definir as ações e os controles necessários para o tratamento dos riscos no âmbito de sua área.

6. PROCESSO DE GESTÃO DE RISCOS

O processo de gestão de riscos da H&P foi definido com base nas diretrizes COSO ERM:2017 e ABNT NBR ISO/IEC 31.000:2018 adaptadas às suas

especificidades e cultura institucional. Este processo contempla o estabelecimento de contexto e critérios, a identificação, a análise, a avaliação, o tratamento de riscos, a comunicação e reporte com partes interessadas e o monitoramento contínuo conforme diretrizes gerais apresentadas abaixo. O detalhamento do processo de gestão da H&P, seus procedimentos e instrumentos constam em seu Guia de Gestão de Riscos.

6.1. Contexto e critérios

- ✓ O estabelecimento de contexto e critérios visa personalizar o processo de gestão de riscos para que este esteja de acordo com as necessidades da H&P;
- ✓ O contexto do processo de gestão de riscos é estabelecido a partir do entendimento histórico da empresa e de uma visão abrangente de todos os fatores que podem influenciar sua capacidade de atingir seus resultados; considerando, mas não está limitado a:
 - **Ambiente externo:** fatores sociais, culturais, políticos, legais, jurídicos, regulatórios, financeiros, tecnológicos, econômicos e/ou ambientais, em âmbito internacional, nacional, regional ou local e fatores e tendências que afetem os objetivos institucionais. Também se incluem aqui os relacionamentos, percepções, valores, necessidades e expectativas das partes interessadas externas, as relações e compromissos contratuais e a complexidade das redes de relacionamento e dependências;
 - **Ambiente interno:** visão, missão e valores; governança, estrutura organizacional, funções e responsabilidades; estratégia, objetivos e políticas; cultura institucional; normas, diretrizes e modelos adotados, além das capacidades entendidas em termos de recursos e conhecimentos (por exemplo, capital, tempo, pessoas, processos, sistemas, tecnologias), dados, sistemas de informação e fluxos de informação, cultura, percepções e valores dos servidores de carreira e agentes de contrato temporário e relacionamentos com partes interessadas internas.
- ✓ Os critérios de riscos são utilizados para avaliar a significância do risco e devem refletir os valores, os objetivos e os recursos da H&P. Os critérios mais importantes são:
 - Escala de probabilidade;

- Escala de impacto;
- Matriz de Riscos;
- Apetite de Riscos;
- Eficácia dos controles;
- Diretrizes para priorização e tratamento.

6.2. Identificação e Análise de riscos

- ✓ A identificação de riscos é o processo de encontrar, reconhecer e descrever os riscos que possam ajudar (oportunidades) ou impedir o alcance dos objetivos da H&P;
- ✓ Na etapa de identificação é formulada uma lista de riscos que considera diferentes fontes de informação internas e externas obtidas por diferentes técnicas como dados históricos, análises teóricas, entrevistas, opiniões de especialistas e de partes interessadas;
- ✓ Os riscos da H&P são identificados e classificados de acordo com sua natureza conforme as seguintes categorias:
 - **Estratégico:** Conjunto de tendências e eventos externos que podem influenciar a trajetória de crescimento da H&P, prejudicar o seu valor para os clientes ou afetar diretamente o atingimento do plano estratégico;
 - **Operacional:** Risco relacionado a possibilidade de ocorrência de perda resultantes de falha, deficiência ou inadequação de quaisquer processos internos envolvendo pessoas, sistemas ou de eventos externos e inesperados;
 - **Legal:** Possibilidade de perdas decorrentes de multas, penalidades ou indenizações resultantes de ações de órgãos de supervisão e controle, bem como perdas decorrentes de decisão desfavorável em processos judiciais ou administrativos;
 - **Financeiro:** Risco relacionado às operações financeiras da H&P e com a insuficiência de recursos financeiros para realização de suas atividades ou para honrar os seus compromissos;
 - **Integridade:** Evento relacionado a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta que podem comprometer os valores e padrões preconizados pela H&P e a perda de reputação;
 - **Cibernético:** Refere-se aos riscos que podem expor os ativos de informação da H&P, aos ataques cibernéticos, a

confidencialidade das informações e às operações de tecnologia.

- ✓ A análise de riscos é o processo de compreender a natureza do risco e determinar o nível do risco, fornecendo a base para a avaliação de riscos e para as decisões quanto ao tratamento dos riscos;
- ✓ O nível de risco é expresso pela combinação da probabilidade da ocorrência do evento e suas consequências caso se concretize, em termos de magnitude do impacto nos objetivos;
- ✓ O processo de análise de riscos envolve:
 - Apreciação das causas dos riscos (fontes de risco e respectivas vulnerabilidades);
 - Avaliação da probabilidades de ocorrência;
 - Análise dos seus efeitos quanto ao impacto gerado (consequências positivas ou negativas), caso o risco se materialize;
- ✓ A análise de riscos da H&P é realizada com base nos parâmetros apresentados em sua matriz de risco contida no Guia de Gestão de Riscos.

6.3. Avaliação de riscos

- ✓ A avaliação de riscos é o processo de comparar os resultados da análise de riscos com os critérios de riscos para determinar se o risco e/ou sua magnitude é aceitável ou tolerável para a tomada de decisões sobre as futuras ações;
- ✓ Estas decisões podem incluir:
 - Se um determinado risco precisa de tratamento;
 - Se uma determinada atividade deve ser realizada;
 - As prioridades do tratamento;
- ✓ Após realizada a avaliação de riscos, a H&P estabelecerá uma ordem de prioridade para o tratamento de riscos de acordo com o seu apetite a risco.

6.4. Tratamento de riscos

- ✓ O tratamento de riscos tem como objetivo a seleção e implementação das opções mais viáveis e adequadas para modificar os riscos;
- ✓ Uma vez implementado, o tratamento fornece novos controles ou modifica os existentes;

- ✓ As opções de tratamento de riscos são:
 - **Evitar o risco:** não iniciar ou descontinuar a atividade que dará origem ao risco;
 - **Transferir o risco:** compartilhar ou transferir uma parte do risco a terceiros;
 - **Mitigar o risco:** reduzir o impacto ou a probabilidade de ocorrência do risco;
 - **Aceitar o risco:** aceitar ou tolerar o risco sem que nenhuma ação específica seja tomada, pois ou o nível do risco é considerado baixo ou a capacidade da H&P para tratar o risco é limitada ou o custo é desproporcional ao benefício.
- ✓ Selecionar a opção mais adequada de tratamento de riscos envolve equilibrar os custos e esforços de implementação com os benefícios decorrentes deste tratamento;
- ✓ Depois de terem sido selecionadas as opções de tratamento de cada risco, elas deverão ser agrupadas em planos ou estratégias de tratamento de risco;
- ✓ Os planos de tratamento devem:
 - Identificar responsabilidades, prazos, o resultado esperado dos tratamentos, recursos necessários, medidas de desempenho e o processo de análise crítica a ser implementado;
 - Monitorar e avaliar a eficácia e o progresso do plano de tratamento;
 - Documentar de maneira prática as opções de tratamento escolhidas.

6.5. Comunicação e reporte

- ✓ A comunicação e a consulta às partes interessadas internas e externas acontecem durante todas as fases do processo de gestão de riscos, em diferentes graus de formalidade e interação de acordo com a situação ou decisão a ser estabelecida;
- ✓ A comunicação e a consulta apropriadas buscam:
 - Desenvolver uma coerência organizacional, identificando áreas críticas para realizações de estratégias conjuntas que ajudarão a atingir os objetivos da H&P e mostraram como o seu sucesso será monitorado;
 - Tornar a gestão de riscos parte rotineira dos negócios da H&P;

- Melhorar o entendimento que as partes interessadas têm de riscos e de seu processo de gestão;
 - Garantir que as diversas visões das partes interessadas sejam levadas em consideração;
 - Garantir que todos os colaboradores da H&P estejam cientes que seus papéis e responsabilidades.
- ✓ Os resultados do processo de gestão de riscos serão apresentados ao Comitê de Governança, Ética, Riscos e Sustentabilidade da H&P (“CGERS”) por meio de relatos periódicos;
 - ✓ O reporte é parte integrante da governança da H&P e garante que as informações sobre este processo estão disponíveis, monitoradas e apropriadamente comunicadas.

6.6. Monitoramento

- ✓ O monitoramento contínuo têm por finalidade assegurar e melhorar a qualidade e a eficácia da concepção, da implementação e dos resultados do processo de gestão de riscos;
- ✓ O progresso na implementação dos planos de tratamento de riscos proporciona uma medida de desempenho e seus resultados devem ser incorporados na gestão, na mensuração e na apresentação de informações (tanto externa quanto internamente) a respeito do desempenho da H&P;
- ✓ O monitoramento deve ocorrer em todos os estágios do processo e incluem o planejamento, a coleta e a análise de informações, os registros de resultados e o fornecimento de retorno.

7. PROGRAMA DE GESTÃO DE RISCOS

O Programa de Gestão de Riscos da H&P consiste no conjunto de instrumentos de governança e de gestão que suportam a concepção, implementação, monitoramento e melhoria contínua da gestão de riscos.

O Programa de Gestão de Riscos conta com ações de:

- *Produção e disseminação de informações, independente do formato, que descrevam as responsabilidades individuais dos destinatários desta Política no âmbito de gestão de riscos;*
- *Fornecimento de treinamentos, orientações e aconselhamentos para os colaboradores da H&P e terceiros, incluindo, mas não se*

- limitando a cursos online, workshops, reuniões internas, conversas regulares, palestras, dentre outras iniciativas; comungando conteúdos disponibilizados no formato digital e presencial;*
- o *Incorporação de preocupações e cuidados com riscos em todos os seus processos, atividades e projetos, incluindo, mas não se limitando a rotinas administrativas, atividades de pesquisa, prestação de serviços, atividades de cunho acadêmico, dentre outras;*
 - o *Identificação e aprofundamento da avaliação dos riscos que podem comprometer o alcance dos objetivos da H&P;*
 - o *Definir, criar e implementar planos de ação e políticas para mitigar os riscos identificados, além de manter uma avaliação contínua dos cenários com vistas a avaliar se as medidas implementadas não requerem novas diretrizes e atitudes.*

Este Programa é operacionalizado pelo Comitê de Governança, Ética, Riscos e Sustentabilidade da H&P, (“CGERS”) e composto pela Política de Gestão de Riscos da H&P, pelo Guia de Gestão de Riscos da H&P e seus instrumentos e pela ferramenta H&P Risk.

8. COMITÊ DE GOVERNANÇA, ÉTICA, RISCOS E SUSTENTABILIDADE

O Comitê de Governança, Ética, Riscos e Sustentabilidade da H&P (“Comitê” ou “CGERS”), instituído nos termos estabelecidos pela Política Antissuborno e Anticorrupção da H&P é responsável por validar, monitorar e salvaguardar os princípios corporativos da governança, integridade, ética, riscos, transparência e sustentabilidade de acordo com seu regimento interno, incluindo os dispostos nesta Política.

9. DISPOSIÇÕES FINAIS

Em razão da complexidade e ao nível de maturidade dos temas afetos à H&P, o Processo de Gestão de Riscos será efetivado de forma gradual e contínua, de acordo com os critérios definidos na metodologia e aprovados pelo Comitê de Governança, Ética, Riscos e Sustentabilidade da H&P.

A presente Política será revista a cada 2 (dois) anos ou sempre que necessário, no intuito de mantê-la atualizada diante de mudanças no ambiente interno ou externo

Esta Política entra em vigor na data de sua publicação.

10. HISTÓRICO DE REVISÕES

DATA	REVISÃO	DESCRIÇÃO	REVISADO POR
22/12/2021	-	Validação	Cristina Margoto
22/07/2021	-	Criação da Política	Jacqueline Torres Juliana Aschar Márcia Fabri

11. GLOSSÁRIO

- **Ataque cibernético:** Ação que constitui uma tentativa deliberada e não autorizada para acessar/manipular informações, ou tornar um sistema inacessível, não íntegro, ou indisponível.
- **Análise de riscos:** Uso sistemático de informações para identificar fontes e estimar riscos.
- **Apetite de risco:** É a quantidade de riscos, no sentido mais amplo, que a H&P está disposta a aceitar. O apetite de risco será estabelecido pela Diretoria da H&P, sendo um marco de referência na fixação de estratégias.
- **Avaliação de risco:** Processo pelo qual os riscos são analisados, considerando-se a sua probabilidade e o impacto como base para determinar o modo pelo qual deverão ser administrados. Esses riscos são avaliados quanto às suas condições de inerentes e residuais.
- **Categoria de riscos corporativos:** Classificação dos tipos de riscos corporativos definidos pela H&P que podem afetar o alcance de seus objetivos estratégicos, observadas as características de sua área de atuação.
- **Causa:** Fonte de risco que, sozinha ou em combinação, tem o potencial intrínseco de gerar riscos.
- **Colaboradores:** São todos os empregados, diretores, estagiários, menores aprendizes, empregados temporários, autônomos e demais indivíduos que mantêm algum vínculo permanente ou temporário de trabalho com a Herkenhoff & Prates.

- **Confidencialidade:** Garante a proteção das informações, permitindo que sejam acessadas apenas por indivíduos autorizados, comprovada a necessidade do acesso e o nível de responsabilidade do colaborador.
- **Consequência:** Resultado de um evento que afeta os objetivos pretendidos.
- **Controle:** Qualquer medida que mantém ou modifica o risco.
- **Critério de risco:** Referências contra os quais o impacto e a probabilidade do risco são avaliados.
- **Evento:** São incidentes ou ocorrências originados a partir de fontes internas ou externas que afetam a implementação da estratégia ou a realização dos objetivos. Os eventos podem provocar impactos positivos (oportunidades a serem aproveitadas), negativos (riscos a serem tratados) ou ambos.
- **Nível do risco:** Magnitude do risco, expressa pela combinação de sua probabilidade e impactos nos objetivos.
- **Objeto de gestão de risco:** Qualquer processo de trabalho, projeto, atividade ou ação de plano institucional.
- **Oportunidade:** Possibilidade de que um evento afete positivamente o alcance de objetivos.
- **Parte interessadas:** São aquelas que podem afetar, serem ou se consideradas afetadas pela H&P ou pelo processo de gestão de riscos. Em outras palavras, as partes interessadas são pessoas ou grupos que tenham interesse genuíno na H&P.
- **Processo de gestão de riscos:** Aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos.
- **Proprietário de riscos:** Pessoa com autoridade e responsabilidade para gerenciar um risco.
- **Resposta ao risco:** Qualquer ação de tratamento adotada para lidar com risco.
- **Risco:** Possibilidade de que um evento afete o alcance de objetivos da H&P.
- **Risco-chave:** Risco que, em função do impacto potencial à H&P, deve ser conhecido pela alta administração.

- **Risco inerente:** Risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto.
- **Risco residual:** É o risco que continua existindo depois que as opções de tratamento tiverem sido identificadas e os planos de tratamento tiverem sido implementados.
- **Tratamento do risco:** Compreende o planejamento e a realização de ações para modificar o nível do risco.
- **Tolerância aos riscos:** Limites aceitáveis quanto à realização dos objetivos corporativos.