1. OBJECTIVO

Estabelecer uma abordagem sistemática e estruturada para a identificação, análise, avaliação, tratamento, comunicação e monitorização dos riscos que possam afectar o cumprimento dos objectivos estratégicos, operacionais, ambientais, de qualidade e de *compliance* da ENDIAMA E.P., promovendo a tomada de decisões fundamentadas, a protecção dos recursos, a prevenção de não conformidades, e a melhoria continua do Sistema de Gestão Integrado (SGI).

2. CAMPO DE APLICAÇÃO

Este procedimento aplica-se a todos os processos, áreas, projectos e niveis hierárquicos da ENDIAMA E.P., incluindo as interacções com partes interessadas e empresas participadas, sempre que haja exposição a riscos com impacto nos objectivos estratégicos, operacionais, ambientais, de qualidade ou de *compliance*.

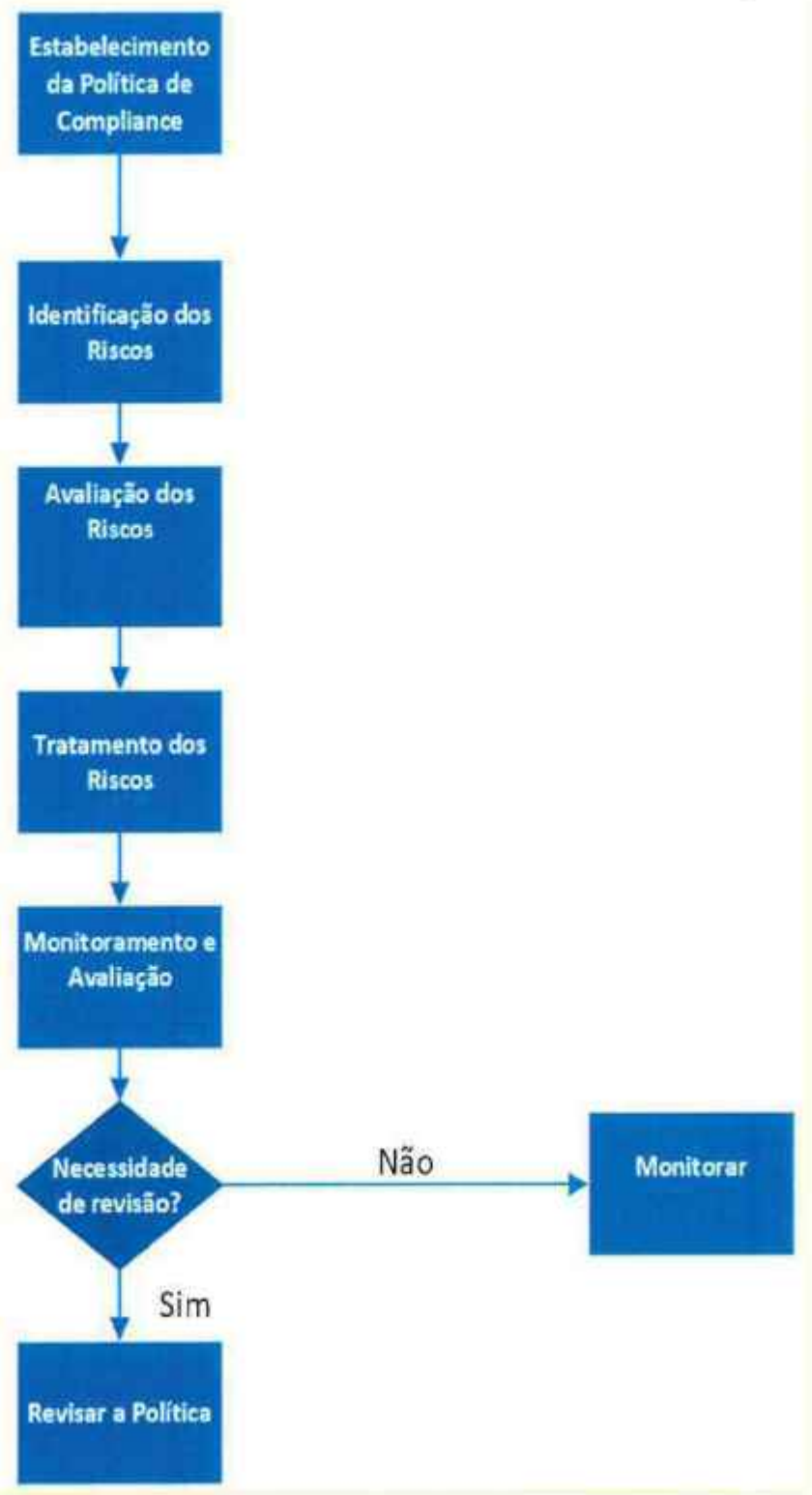
Inserido na abordagem integrada de Gestão de Riscos e Compliance (GRC), este procedimento orienta a identificação, avaliação, tratamento e monitorização de riscos no âmbito do Sistema de Gestão Integrado (SGI).

3. DEFINIÇÕES E ABREVIATURAS

RISCO	É o efeito da incerteza sobre os objectivos, podendo traduzir-se por um desvio positivo ou negativo em relação ao que se espera alcançar. Este efeito pode resultar de uma ou mais causas e manifestar-se por meio de eventos que afectem, de forma directa ou indirecta, os resultados estratégicos, operacionais, ambientais, de qualidade ou de *compliance* da organização.
EVENTO	É um incidente ou uma ocorrência gerada com base em fontes internas ou externas, que afecta a realização dos objetivos.
APETITE AO RISCO	Apetite ao risco é o nível de risco que a organização está disposta a aceitar na prossecução dos seus objectivos estratégicos, considerando a sua cultura, capacidade de gestão, valores institucionais, obrigações legais e contexto operacional. Representa os limites qualitativos e/ou quantitativos de exposição ao risco que são considerados aceitáveis pela gestão e pelo órgão directivo, servindo como guia para a tomada de decisão, a alocação de recursos e a definição de respostas a riscos.
COSO	Committee of Sponsoring Organizations of the Treadway Commission. (Comitê das Organizações Patrocinadoras da Comissão Treadway).É um modelo que orienta as práticas de gestão de riscos corporativos e controlo interno.

CONTROLO INTERNO	Conjunto de políticas, procedimentos e práticas adoptadas por uma organização para garantir a eficiência operacional, a confiabilidade das informações financeiras e o cumprimento de normas, minimizando riscos, prevenindo fraudes e garantindo a protecção do patrimônio da empresa.
ENTERPRISE RISK MANAGEMENT (ERM)	É um processo estruturado e contínuo que ajuda as organizações a identificar, avaliar e gerir os riscos que podem impactar as suas operações e objectivos estratégicos.
FAMÍLIA DE RISCO	Categorização dos riscos de acordo com sua natureza ou origem, facilitando a sua análise e gestão.
GNACC	Gabinete de Normalização, Auditoria, *Compliance* e Controlo de Qualidade
ISO 31000	Norma Internacional que fornece directrizes sobre gestão de riscos, promovendo uma abordagem sistemática

4. FLUXOGRAMA



5. DESCRIÇÃO

A metodologia adoptada reconhece que o risco está presente em todos os níveis de decisão e que a sua gestão eficaz contribui para a criação e protecção de valor, o fortalecimento da cultura de integridade e a tomada de decisões informadas. O processo de gestão de riscos estrutura-se num ciclo contínuo e interligado, composto pelas seguintes etapas fundamentais:

1. Estabelecimento do contexto – Definição clara do âmbito da análise de riscos, incluindo factores internos e externos que possam influenciar a exposição e a capacidade de resposta da organização;

2. Identificação dos riscos – Reconhecimento sistemático dos eventos que possam comprometer os objectivos da organização;

3. Análise dos riscos – Avaliação detalhada das causas, consequências, probabilidade e impacto dos riscos identificados;

4. Avaliação e priorização dos riscos – Comparação dos níveis de risco com critérios predefinidos (ex. apetite ao risco) para apoiar a tomada de decisões;

5. Tratamento dos riscos – Selecção e implementação de opções de resposta, tais como mitigação, partilha, aceitação ou eliminação;

6. Monitorização e revisão – Verificação contínua da eficácia das respostas implementadas, reavaliação dos riscos e adaptação do processo em função das alterações no contexto;

7. Comunicação e consulta – Diálogo estruturado e permanente com as partes interessadas internas e externas, garantindo transparência, alinhamento e responsabilização.

Esta abordagem permite à ENDIAMA E.P., gerir os riscos de forma proactiva e integrada, promovendo uma actuação eficaz, sustentável e em conformidade com os princípios de responsabilidade, ética e desempenho exigidos ao seu sector de actividade.

5.1 Entender o Contexto – Passo 1

Esta etapa corresponde à compreensão e análise do objecto da gestão de riscos, tendo por base o contexto interno e externo da ENDIAMA E.P. A gestão de riscos pode ser aplicada em diversos níveis – estratégico, operacional, por programa, projecto ou actividade específica – sendo por isso essencial definir com clareza o âmbito da aplicação, os objectivos a alcançar e o respectivo alinhamento com os objectivos organizacionais globais.

Fontes Internas de Risco

As fontes internas de risco estão associadas a factores endógenos à estrutura da ENDIAMA E.P., originando-se dos seus próprios processos, colaboradores, sistemas, práticas de gestão ou ambiente interno de controlo. Estas ocorrências incluem, por exemplo, falhas operacionais, erros humanos, ausência de competências, ineficiências processuais, deficiências tecnológicas ou desajustes na cultura organizacional.

Por se tratar de riscos sob controlo directo da organização, a resposta deverá ser eminentemente proactiva, com vista à prevenção de impactos negativos através da implementação de mecanismos de controlo e melhoria contínua.

Fontes Externas de Risco

As fontes externas de risco dizem respeito a factores exógenos, que escapam ao controlo directo da ENDIAMA E.P., mas que podem afectar significativamente a sua actuação e o cumprimento dos seus objectivos. Estas ocorrências estão ligadas ao ambiente político, económico, social, tecnológico, ambiental ou sectorial em que a organização opera.

Entre os exemplos incluem-se: variação das taxas de juro, flutuação do crédito, avanços tecnológicos disruptivos, concorrência internacional, instabilidade política, conflitos sociais, catástrofes ambientais, pandemias ou alterações legislativas imprevistas.

Nestas situações, a capacidade de intervenção da ENDIAMA E.P., é limitada, pelo que a resposta tende a ser reactiva, centrada na antecipação de cenários e na preparação de planos de contingência que permitam mitigar os efeitos negativos de forma célere e eficaz.

Assim, a consciência institucional sobre os riscos externos é essencial para assegurar a prontidão da organização e a robustez da sua capacidade de resposta, garantindo a continuidade e a resiliência das suas operações.

5.2 Identificação e Análise de Riscos – Passo 2

A etapa de identificação dos riscos envolve reconhecimento, descrição e registo do evento de risco, com a caracterização das suas prováveis causas e possíveis consequências, caso o evento ocorra, sendo que se considera evento um incidente ou uma ocorrência gerada com base em fontes internas ou externas, que afecta a realização dos objectivos.

O risco será descrito nos termos abaixo:

a) **Causa**: condições que dão origem à possibilidade de um evento ocorrer, também chamadas de factores de riscos e podem ter origem no ambiente interno e externo;

b) **Risco**: probabilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objectivos.

c) **Consequência**: possível impacto nos objectivos definidos, caso o risco se materialize.

Depois de se ter(em) definido o(s) risco(s), as suas causas e consequências, classificam-se esses riscos, de acordo com as seguintes categorias/famílias:

Categorias/Famílias de Risco	Descrição e Exemplos
Financeiros	Eventos inesperados que possam ter um impacto financeiro negativo na organização: Risco de mercado (alterações em taxas de juros, câmbios,*commodities* etc.) Risco de crédito (não pagamento de dívidas) Risco de liquidez (falta de recursos financeiros)
Operacionais	Eventos que podem comprometer as actividades, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas. Incluem: Ausência de competências; Falhas tecnológicas; Erros humanos;

	Ataques cibernéticos; Falhas de sistemas de TI; Vulnerabilidades de software; Desperdício de recursos naturais; Mudanças climáticas; Acidentes de trabalho; Fraudes internas.
Estratégicos	Relacionam-se com decisões de negócio que podem afectar os objectivos a médio e longo prazo, como: Decisões erradas de investimento; Mudanças nas condições de mercado; Novas regulamentações que impactam a operação.
Conformidade/Compliance ou Regulamentares	Associados ao cumprimento de normas, leis ou regulamentações específicas do sector ou do país onde a empresa actua. Exemplos: Penalidades por não cumprimento de leis ambientais; Violações de regulamentações de saúde e segurança; Incumprimento no pagamento dos impostos.
Governação/Organizacionais	Surgem quando há falhas nos mecanismos de governação, o que pode incluir: Conflitos de interesses dentro da direcção ou gestão; Falta de transparência nas decisões e nas comunicações com as partes interessadas; Desalinhamento estratégico entre os objectivos da empresa e as expectativas dos acionistas ou reguladores; Gestão de riscos que não responde às ameaças de forma eficaz.
Integridade	Eventos relacionados com a corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, que possam comprometer os valores preconizados pela empresa e a realização de seus objectivos. Exemplos: Abuso de poder/influência; Conflito de interesses; Uso indevido ou manipulação de dados e informações; Práticas antiéticas de acordo com o Código de ética e conduta aprovado; Nepotismo; Uso de posição ou de poder em favor de interesses indevidos.
Reputacionais	Eventos que podem comprometer a confiança da sociedade em relação à capacidade da empresa em cumprir sua missão institucional interferindo na sua imagem. Exemplos: Escândalos públicos; Críticas nas redes sociais; Publicidade negativa.

Nota 1: Caso o evento de risco esteja associado a duas ou mais categorias de classificação, deverá ser escolhida a categoria que reflita o aspecto mais relevante quanto ao impacto que o evento de risco poderá trazer, caso se materialize

5.3 Avaliação de Riscos – Passo 3

A avaliação de riscos é importante porque:

- Avalia os riscos com base na probabilidade de sua ocorrência e impacto que poderiam causar nos resultados, permitindo que a organização considere os níveis de riscos;
- Verifica a existência de controlos internos e sua eficiência em mitigar os riscos;
- Fornece a base para decisões sobre se o risco necessita de ser tratado e como;
- Considera e trata de forma cuidadosa factores como cenários, incertezas, complexidade e conectividade, assim como divergência de opiniões, inclinações, percepções e julgamentos.

5.3.1 - Cálculo do risco inerente (risco bruto, sem considerar qualquer controlo)

A avaliação da probabilidade (P) utiliza a relação de aspecto avaliativo, frequência e valor do peso para apurar o risco, em cinco níveis, conforme descrito na tabela 1.

Tabela 1 - Critérios Utilizados na Avaliação da Probabilidade

Probabilidade	Descrição da probabilidade, desconsiderando os controlos	Frequência	Peso
Muito baixa	**Improvável:** Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade	< 10 %	1
Baixa	**Rara:** De forma inesperada ou casual o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade	≥ 10 < 40 %	2
Média	**Possível:** De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	≥ 40 < 75 %	3
Alta	**Provável:** De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	≥75 ≤ 90 %	4
Muito alta	**Praticamente certa:** De forma inequívoca, o evento ocorrerá, as	≥ 90 %	5

	circunstâncias indicam claramente essa possibilidade.		

A seguir deverá ser avaliado o Impacto (I) resultante da materialização do evento de risco, mediante os critérios estabelecidos na tabela 2.

Tabela 2 - Critérios Utilizados na Avaliação de Impacto

Impacto	Descrição do impacto, caso o evento ocorra	Peso
Muito baixo	Mínimo impacto nos objectivos. Impacto financeiro insignificante. Impacto operacional desprezível, sem impacto mensurável. Impacto insignificante nas metas estratégicas da organização. Problemas legais menores, sem consequências significativas. Impacto insignificante na segurança. Impacto ambiental irrelevante ou desprezível. Impacto insignificante ou mínimo sobre os sistemas de TI e a infraestrutura tecnológica. Nenhum impacto visível na reputação. Impacto insignificante na gestão ou estrutura organizacional.	1
Baixo	Pequeno impacto nos objectivos. Impacto financeiro leve que não afecta o resultado geral. Pequenos problemas operacionais que causam pequenas interrupções, mas são rapidamente resolvidos. Impacto leve nas decisões estratégicas, mas sem comprometer significativamente os resultados. Não conformidade menor, resultando em notificações ou advertências, sem multas. Impacto leve, com incidentes de segurança menores facilmente geridos. Impacto leve, com efeitos ambientais mínimos, facilmente mitigáveis Impacto leve nos sistemas de TI, com interrupções temporárias, mas sem efeito prolongado. Impacto leve e temporário na reputação, sem efeito prolongado. Impacto leve, com pequenas dificuldades na gestão ou execução de projectos.	2
Médio	Moderado impacto nos objectivos, porém recuperável. Aumento de custos ou perdas financeiras visíveis. Interrupções moderadas em processos-chave que podem afectar o desempenho a curto prazo.	3

	Impacto visível nas decisões estratégicas, afectando a capacidade de alcançar os principais objectivos. Não conformidade moderada que resulta em multas menores ou obrigações legais adicionais. Incidentes de segurança moderados que exigem atenção e podem afectar algumas áreas. Impacto ambiental moderado que pode resultar em multas ou reparações locais. Impacto visível na infraestrutura tecnológica, afectando a produtividade a curto prazo. Impacto visível na reputação, afectando a confiança de algumas partes interessadas Impacto visível na estrutura organizacional, com perturbações que requerem ajustes.	
Alto	Impacto significativo nos objectivos, de difícil reversão. Impacto significativo nas finanças, podendo reduzir lucros ou provocar grandes despesas. Interrupções significativas nas operações, com impacto directo na produtividade ou entrega. Impacto significativo nas metas estratégicas, afetando a competitividade e o desempenho no mercado. Não conformidade significativa, com penalidades severas, incluindo multas ou processos legais. Impacto significativo na segurança, comprometendo a proteção de instalações e informações. Impacto ambiental significativo, podendo resultar em sanções regulamentares e acções corretivas. Impacto significativo, com interrupções prolongadas ou perda de dados que afectam o desempenho da organização. Impacto significativo na reputação, resultando em perda de clientes e confiança do público. Impacto significativo, afectando a eficácia geral da gestão e a capacidade de atingir metas.	4
Muito alto	Impacto catastrófico nos objectivos, de forma irreversível. Impacto financeiro devastador, ameaçando a viabilidade da organização. Paralisação total das operações, acfetando a continuidade do negócio. Impacto devastador, comprometendo a viabilidade a longo prazo da organização. Problemas legais graves que podem comprometer a continuidade do negócio. Falha de segurança grave com consequências devastadoras para a organização. Impacto ambiental devastador, com danos irreparáveis e grandes sanções.	5

	Impacto catastrófico, comprometendo a continuidade dos serviços ou a segurança dos dados. Impacto devastador na reputação, com perda irreversível de confiança. Impacto grave que ameaça a sobrevivência organizacional.	

NOTA2 : Risco inerente é o risco a que uma organização está exposta sem considerar quaisquer medidas de controlo que reduzam, ou possam reduzir, a probabilidade de sua ocorrência ou de seu impacto.

A multiplicação entre os valores da probabilidade (Tabela 1) e impacto (Tabela 2) define o nível do risco inerente, que, como citado na Nota 2, é o nível do risco sem considerar quaisquer controlos que reduzem, ou podem reduzir, a probabilidade da sua ocorrência ou do seu impacto.

$$RI = NP \times NI$$

Em que:

RI = nível do risco inerente

NP = nível de probabilidade do risco

NI = nível de impacto do risco

Matriz de Riscos Inerente - RI = NP x NI						
Nível de Risco		**Probabilidade**				
Extreme (R ≥ 16) Alto (R ≥ 9 e R < 16) Médio (R ≤ 4 e R < 9) Baixo Impacto (R < 4)		1	2	3	4	5
Impacto	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5

5.3.2 Factor de Ponderação do Impacto – FP

O factor de ponderação serve como uma ferramenta para ajustar a relevância ou peso de um risco em análise. Ele é especialmente útil para refletir a gravidade do impacto de um risco quando este se materializa. Abaixo, estão descritos os diferentes níveis de ponderação do

impacto, com base na gravidade crescente, de 1 (sem necessidade de ponderação) até 10 (impacto catastrófico).

Tabela 3 - Níveis de Ponderação do possível impacto

Factor de Ponderação	Descrição	Factorde Ponderação
Sem Necessidade de Ponderação	Refere-se a um impacto insignificante ou muito baixo. A organização considera que o risco tem um impacto tão pequeno que não requer nenhum ajuste especial no cálculo do risco. **Exemplo:** Pequenos erros administrativos ou atrasos mínimos que não afetam as operações, receitas ou reputação da organização. **Consequência:** O efeito deste risco seria tão leve que a sua gestão não exige atenção especial ou acção imediata. Pode ser monitorizado, mas geralmente não justifica intervenção activa.	1
Impacto Baixo	O impacto do risco é leve e pode causar perturbações mínimas, sem comprometer a integridade ou a continuidade da operação. **Exemplo:** Pequenas falhas operacionais que causam inconvenientes, mas são resolvidas rapidamente e sem custos significativos. **Consequência:** O impacto é notado, mas geralmente não altera os resultados ou os processos de forma significativa. A organização pode implementar medidas corretivas simples, mas o risco é considerado tolerável e pode ser gerido dentro das operações normais.	2
Impacto Moderado	O impacto é moderado e afecta algumas áreas da operação, mas sem comprometer a viabilidade ou os objetivos principais da organização. **Exemplo:** Atraso na entrega de um projeto importante ou falha de um equipamento que interrompe temporariamente uma parte significativa das operações. **Consequência:** Embora o risco não seja crítico, ele pode gerar custos financeiros adicionais ou atrasos que impactam a produtividade. Serão necessárias ações de mitigação para evitar maiores complicações.	5
Impacto Importante	O impacto é significativo e pode comprometer várias áreas da organização, afectando directamente o cumprimento de metas ou o funcionamento de operações-chave. **Exemplo:** Uma falha importante no sistema de TI que afecta toda a organização ou um problema de conformidade que resulta em multas pesadas. **Consequência:** As consequências deste risco são graves, e podem incluir perdas financeiras substanciais, atrasos críticos, ou dano à reputação. Medidas preventivas mais robustas e planos de contingência	8

	precisam de ser implementados para reduzir a probabilidade de ocorrência ou minimizar o impacto.	
Impacto Catastrófico	O impacto é catastrófico e pode colocar em risco a continuidade da organização. Este nível de impacto representa uma ameaça directa à sobrevivência da operação, com efeitos a longo prazo. **Exemplo:** Desastres como incêndios, grandes falhas de segurança que expõem dados confidenciais ou perda completa de infraestrutura crítica, que podem resultar em falência ou fecho da organização. **Consequência:** Este é o nível mais elevado de impacto, exigindo acção imediata e contínua para evitar a ocorrência. Planos de resposta a crises e medidas de mitigação avançadas são obrigatórios. A organização deve se preparar para riscos de grande escala, com potenciais consequências devastadoras para a sua reputação, finanças e operações.	**10**

Cálculo do Risco Inerente Ponderado (RIP) = Probabilidade × (Impacto × Fator de Ponderação)

O Factor de ponderação no cálculo de riscos é fundamental para ajustar a análise de acordo com o impacto que um determinado risco pode ter na organização. Esta ferramenta garante que os riscos mais graves sejam tratados com a devida prioridade, mesmo que suas probabilidades sejam menores. Com factores de ponderação, a gestão de riscos torna-se mais eficaz e alinhada aos objectivos estratégicos e capacidade da organização

Matriz de Risco Inerente Ponderado - RIP = NP x (NIxFPI)

Classificação do Nível de Risco - RI		**Ponderaçao - FPI**				
Extremo (R ≥ 200) Alto (R ≥ 50 e R < 200) Médio (R ≥ 20 e R < 50) Baixo Impacto (R < 20)		**1**	**2**	**5**	**8**	**10**
Impacto x probabilidade	25	25	50	125	200	250
	20	20	40	100	160	200
	16	16	32	80	128	160
	15	15	30	75	120	150
	12	12	24	60	96	120
	10	10	20	50	80	100
	9	9	18	45	72	90
	8	8	16	40	64	80
	6	6	12	30	48	60

	5	5	10	25	40	50
	4	4	8	20	32	40
	3	3	6	15	24	30
	2	2	4	10	16	20
	1	1	2	5	8	10

5.3.3 - Análise dos Controlos Existentes

Esta actividade da metodologia empregará a técnica "*Bow Tie*" que consiste em identificar as causas e consequências associadas aos riscos já conhecidos na etapa anterior, complementado pelos controlos preventivos que actuam nas causas e pelos controlos de atenuação (reactivos) que visam minimizar o impacto das consequências. Os controlos deverão existir e estar operacionais para prevenir a materialização do risco ou minimizar as suas consequências. Uma vez levantados os controlos, deve ser realizada "Avaliação dos Controlos Existentes", com base na experiência a nivel do sector, processos, projectos, acções ou factores críticos de sucesso levantados na identificação dos riscos. Os controlos podem ser avaliados conforme a escala identificada na tabela 4.

Tabela 4 - Avaliação do grau de eficiência dos controlos existentes

Nivél de Eficácia dos Controlos Existentes	Descrição	RC - Risco dos controlos existentes
Inexistente (0)	Os controlos são inexistentes ou sem efectividade para o propósito segundo o qual foram implementados	1
Fraco (0,2)	Os controlos não cumprem com o seu propósito na forma idealizada ou são utilizados segundo critérios individuais sem qualquer padronização de procedimentos.	0,8
Média (0,4)	Os controlos implementados mitigam parcialmente o nível de risco, por estarem definidos de forma insuficiente, porque o seu âmbito de actuação é limitado e as técnicas e ferramentas utilizadas são inadequadas.	0,6
Alta (0,6)	Controlos implementados e sustentados por ferramentas adequadas e, embora passíveis de aperfeiçoamento, mitigam o risco satisfatoriamente.	0,4
Muito alta (0,8)	Controlos implementados podem ser considerados como a "melhor prática", mitigando todos os aspectos relevantes do risco.	0,2

5.3.4 - Cálculo do Risco Residual

Após a avaliação dos controlos existentes (tabela 4), calcula-se o risco residual. O nível de risco residual corresponde ao valor final da multiplicação entre o valor do risco inerente e o factor de avaliação dos controlos internos existentes.

A classificação dos níveis de risco é efectuada a partir do cálculo das variáveis do risco por meio das fórmulas descritas abaixo:

Nivel de Risco Residual (NRR) = RIP x FC

NRR = nível do risco residual

RIP = risco inerente ponderado

FC = Grau de Eficiência dos Controlos Existentes

Nota 3: O valor de risco residual pode fazer com que o risco se enquadre em uma faixa de classificação de risco diferente da faixa definida para o risco inerente ponderado.

Matriz de Risco Residual - RR = RIP X RC						
Classificação do Nível de Risco - RI		**Risco de Controlo - RC**				
Extremo (R ≥ 200)		0,2	0,4	0,6	0,8	1
Alto (R ≥ 50 e R < 200)						
Médio (R ≥ 20 e R < 50)						
Baixo Impacto (R < 20)						
Risco Inerente Ponderado	250	50	100	150	200	250
	200	40	80	120	160	200
	160	32	64	96	128	160
	150	30	60	90	120	150
	128	25,6	51,2	76,8	102,4	128
	125	25	50	75	100	125
	120	24	48	72	96	120
	100	20	40	60	80	100
	96	19,2	38,4	57,6	76,8	96
	90	18	36	54	72	90

	80	16	32	48	64	80
	75	15	30	45	60	75
	72	14,4	28,8	43,2	57,6	72
	64	12,8	25,6	38,4	51,2	64
	60	12	24	36	48	60
	50	10	20	30	40	50
	48	9,6	19,2	28,8	38,4	48
	45	9	18	27	36	45
	40	8	16	24	32	40
	32	6,4	12,8	19,2	25,6	32
	30	6	12	18	24	30
	25	5	10	15	20	25
	24	4,8	9,6	14,4	19,2	24
	20	4	8	12	16	20
	18	3,6	7,2	10,8	14,4	18
	16	3,2	6,4	9,6	12,8	16
	15	3	6	9	12	15
	12	2,4	4,8	7,2	9,6	12
	10	2	4	6	8	10
	9	1,8	3,6	5,4	7,2	9
	8	1,6	3,2	4,8	6,4	8
	6	1,2	2,4	3,6	4,8	6
	5	1	2	3	4	5
	4	0,8	1,6	2,4	3,2	4
	3	0,6	1,2	1,8	2,4	3
	2	0,4	0,8	1,2	1,6	2
		0,2	0,4	0,6	0,8	1

5.4 – Tratamento do Risco – Passo 4

5.4.1 - Definição do Apetite ao Risco

O Tratamento de Riscos é a definição das opções de resposta aos riscos, de forma a adequar os seus níveis ao apetite estabelecido para os processos organizacionais, além da escolha das medidas de controlo associadas a essas respostas.

Apetite de Risco			
ACEITE	ACEITE	NAO ACEITE	NAO ACEITE
RB (Risco Baixo)	RM (Risco Médio)	RA (Risco Alto)	RE (Risco Extremo)
R < 20	20 ≤ R ≤ 50	50 < R < 200	200 ≤ R

5.4.2 - Atitude perante o Nível de Risco

Nesta etapa, serão identificados quais os riscos que serão priorizados para tratamento. Para isso, devem ser considerados os valores dos níveis de riscos residuais calculados na etapa anterior.

A faixa de classificação do risco residual deve ser considerada para a definição da atitude da área de actuação operacional em relação à priorização para tratamento. A tabela 5 mostra, por faixa de classificação, quais as acções que devem ser adoptadas em relação ao risco e as suas excepções.

Tabela 5 - Atitude perante o risco para cada Nível de Risco

Classificação	Descrição	Excepção
Risco Baixo	Nível de risco **dentro do apetite ao risco**, mas é possível que existam oportunidades de melhoria que possam ser exploradas, avaliando a relação custo x benefício.	Caso o risco seja priorizado para implementação de medidas de tratamento, essa priorização deve ser justificada pelo responsável do processo
Risco Médio	Nível de risco **dentro do apetite a risco**. Geralmente nenhuma medida especial é necessária, porém requer actividades de **monitorização** específicas e atenção na manutenção de respostas e controlos para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.	

Risco Alto	Nível de risco **além do apetite a risco**. Qualquer risco nesse nível deve ser comunicado aos responsáveis da gestão do risco para implementação de uma acção a implementar num determinado período . Postergação de medidas só com autorização do gestor da área em comum acordo com responsável pelo processo.	
Risco Extremo	Nível de risco **muito além do apetite a risco**. Qualquer risco nesse nível deve ser comunicado ao gestor do risco para implementação de acção urgente. Postergação de medidas só com autorização da área de actuação estratégica.	Caso o risco não seja priorizado para implementação de medidas de tratamento, a não priorização deve ser justificada pelo responsável pelo processo e aprovada pela área de actuação estratégica

Uma vez definido o apetite ao risco, a organização declara que:

1. Todos os riscos, cujos níveis estejam dentro da(s) faixa(s) de apetite a risco, podem ser aceites e uma possível priorização para tratamento deve ser justificada;
2. Todos os riscos, cujos níveis estejam fora da(s) faixa(s) de apetite a risco, serão tratados e monitorados e uma possível falta de tratamento deve ser justificada.

5.4.3 - Definição de Respostas aos Riscos

Esta etapa tem por objectivo efinir as opções de tratamento para os riscos priorizados na etapa anterior. Cada risco priorizado deve ser relacionado a uma opção de tratamento. A escolha da opção depende do nível do risco, conforme tabela 6.

Tabela 6 - Opções de Tratamento

Opções de tratamento	Descrição
Aceitar	Um risco normalmente é aceite quando o seu nível está na faixa de apetite a risco. Nessa situação, nenhum novo controlo precisa de ser implementado para mitigar o risco.
Mitigar	Um risco normalmente é mitigado quando é classificado como "Alto" ou "Extremo". A implementação de controlos, neste caso, apresenta um custo/ beneficio adequado. Mitigar o risco significa implementar controlos

	que possam diminuir as causas ou as consequências dos riscos, identificadas na etapa de Identificação e Análise de Riscos.
Evitar	Um risco normalmente é evitado quando é classificado como "Alto" ou "Extremo" e a implementação de controlos apresenta um custo muito elevado, inviabilizando sua mitigação, ou não haja entidades dispostas a compartilhar o risco. Evitar o risco significa encerrar o processo organizacional. Nesse caso, essa opção deve ser aprovada pela área de actuação estratégica.
Compartilhar	Um risco normalmente é compartilhado quando é classificado como "Alto" ou "Extremo", mas a implementação de controlos não apresenta um custo/ benefício adequado. Pode-se compartilhar o risco por meio de terceirização ou apólice de seguro.

Se a opção de tratamento do risco for MITIGAR, devem ser definidas medidas de tratamento e controlo para esse risco. Essas medidas devem ser capazes de diminuir os níveis de probabilidade e/ou de impacto do risco a um nível dentro, ou mais próximo possível, das faixas de apetite a risco (risco "Baixo" ou "Médio").

5.4.4 - Planear a Resposta ao Risco

Definida a resposta a riscos, torna-se necessário elaborar um plano de acção visando a redução do grau de exposição ao risco inerente, ou seja, do risco identificado sem considerar quaisquer acções de gestão. Assim, após a efectiva implementação das acções de gestão, o risco inerente diminui o seu grau de exposição, passando a condição de risco residual. Sendo assim, além das informações apresentadas no Mapa de Riscos, o planeamento de respostas a riscos envolve a elaboração de uma a tabela - Plano de Respostas a Riscos.

Objectivo/ Processo	Evento de Risco	Resposta	O Quê?	Quando?	Onde?	Porquê	Como?

As actividades dessa etapa devem possuir uma equipa designada com atribuições e responsabilidades definidas, assim como prazos estabelecidos. Cabe ao gestor do risco a gestão das actividades e o registo das acções adoptadas, com vista à construção de um histórico de melhores práticas.

5.5 – Comunicação e Monitorização – Passo 5

Durante todas as etapas ou actividades do processo de gestão de riscos deve haver uma efectiva comunicação informativa e consultiva entre a organização e as partes interessadas, internas e externas, para:

a) Auxiliar a estabelecer o contexto apropriadamente e assegurar que as visões e percepções das partes interessadas, incluindo que necessidades, suposições, conceitos e preocupações sejam identificadas, registadas e levadas em consideração;

b) Auxiliar eassegurar que os riscos sejam identificados e analisados adequadamente, reunindo áreas diferentes de especialização;

c) Garantir que todos os envolvidos estejam cientes dos seus papéis e responsabilidades, avaliem e apoiem o tratamento dos riscos.

A organização usa canais de comunicação para suportar a gestão de riscos corporativos, promover a sua cultura e desempenho em toda a instituição. A comunicação deverá ser oportuna e adequada, além de abordar aspectos financeiros, operacionais e estratégicos. Deve ser entendida como um canal que movimenta as informações em todas as direcções – dos superiores aos subordinados, e vice-versa. A monitorização é parte integrante e essencial da gestão de riscos, cuja finalidade é:

a) Detectar mudanças no contexto externo e interno, incluindo alterações nos critérios de risco e no próprio risco, que podem requerer revisão dos tratamentos actualmente adoptados e suas prioridades, e levar à identificação de riscos emergentes;

b) Obter informações adicionais para melhorar a política, a estrutura e o processo de gestão de riscos;

c) Analisar eventos - incluindo os "quase incidentes", mudanças, tendências, sucessos e fracassos e aprender com eles; e

d) Garantir que os controlos sejam eficazes e eficientes no desenho e na operação.

A monitorização dos riscos estratégicos fornece a informação actualizada e objectiva para identificar fragilidades e possibilidades de melhorias, bem como verificar o desempenho e eficiência do Plano de Acção, operacionalizado por meio dos controlos implementados. Lembrando que os riscos mudam ao longo do tempo e devem ser monitorizados para que a organização possa realizar os ajustes necessários.

Após a aplicação do presente modelo de gestão de riscos estratégicos, para a apresentação dos resultados e acompanhamento da monitorização, uma boa prática de transparência consiste no desenvolvimento de reportes, por meio de *Dashboards*.

Por fim, na perspectiva da monitorização da evolução dos riscos estratégicos, a aferição dos indicadores chaves de risco de acordo com a periodicidade definida, permite a actualização dos cenários de relevância dos riscos.

6. DOCUMENTOS ASSOCIADOS

END.FOR.03.004 – Matriz de Riscos

END.POL.03.002 - Política de Gestão de Riscos

END.MAN.03.001 - Manual de Controlos Internos

Histórico de Revisões

Nº Revisão	Data	Descrição
00	17.10.2025	Emissão do Procedimento

Elaborado:	Verificado:	Aprovado:
17/10/25	17.10.25	17/10/25