ANEXO ÚNICO DA RESOLUÇÃO SF/COMITÊ DE GOVERNANÇA E ESTRATÉGIA Nº 01/2024

1. Modelo das Três Linhas (The IIA) como referencial dos papeis e responsabilidades dos servidores/áreas da SF no processo de gerenciamento de riscos:

2. Processo de gerenciamento de riscos (Manual de Gestão de Riscos CGM, 2023)

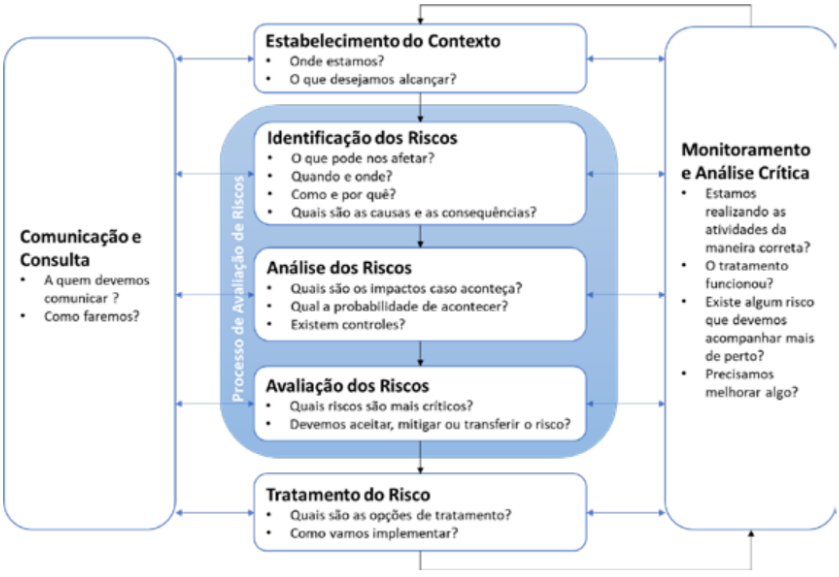

Figura 04: Processo de Gestão de Riscos baseada na norma ISO 31000[4]

3. Critérios para avaliação dos riscos e controles:

Probabilidade de Ocorrência do Risco		
Probabilidade	**Descrição da probabilidade, desconsiderando os controles**	**Peso**
Muito baixa	**Improvável**. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Baixa	**Rara.** De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Média	**Possível.** De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	5
Alta	**Provável.** De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	8
Muito alta	**Praticamente certa.** De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.	10

Impacto do Risco		
Impacto	**Descrição do impacto nos objetivos, caso o evento ocorra**	**Peso**
Muito baixo	**Mínimo impacto** nos objetivos (estratégicos, desempenho, conformidade, comunicação etc.).	1
Baixo	**Pequeno impacto** nos objetivos (idem).	2
Médio	**Moderado impacto** nos objetivos (idem), porém **recuperável.**	5
Alto	**Significativo impacto** nos objetivos (idem), de **difícil reversão.**	8
Muito Alto	**Catastrófico** impacto nos objetivos (idem), de forma **irreversível.**	10

Forma de Cálculo do Risco Residual **Risco Residual = Risco Inerente x Fator de Nível dos Controles Internos**		
Nível dos Controles Internos		
Nível	**Descrição**	**Fator de Avaliação dos Controles**
Inexistente	**Controles inexistentes**, mal desenhados ou mal implementados, isto é, não funcionais.	1
Fraco	Controles 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 do risco.	0,2

4. Modelo Matriz de Riscos por nível de risco:

MATRIZ DO RISCO

IMPACTO	**MUITO ALTO (10)**					
	ALTO (8)					
	MÉDIO (5)					
	BAIXO (2)					
	MUITO BAIXO (1)					
		MUITO BAIXA (1)	**BAIXA (2)**	**MÉDIA (5)**	**ALTA (8)**	**MUITO ALTA (10)**
		PROBABILIDADE				

Risco Extremo
Risco Alto
Risco Médio
Risco Baixo

MATRIZ DE RISCO
PROBABILIDADE
Risco Alto: com consequências muito relevantes que afetem o alcance dos objetivos. Para o nível de risco alto, o gestor da macroárea deverá reportar o evento ao Gabinete da SF que tomará ciência do risco identificado e solicitará o plano de ação e adoção de medidas que reduzam o nível do risco ao aceitável.
Risco Extremo: com consequências extremas que afetem o alcance dos objetivos de forma irreversível. Para o nível de risco extremo, o gestor da macroárea deverá reportar o evento ao Gabinete da SF que tomará ciência do risco identificado e solicitará o plano de ação para adoção de medidas que reduzam o nível do risco ao aceitável, devendo necessariamente conter ações de contingência e adoção de medidas que reduzam o impacto do risco, caso concretizado.
Risco baixo e muito baixo: com consequências de baixo impacto, que não impeçam o alcance dos objetivos. Situação na qual cabe ao gestor responsável decidir por mitigar ou aceitar o risco no caso de os benefícios superarem os custos de mitigação.
Risco moderado: com consequências relevantes, porém que não impeçam o alcance dos objetivos. Situação na qual cabe ao gestor responsável pela macroárea decidir por mitigar o risco no caso de os benefícios superarem os custos de mitigação.
IMPACTO