ANEXO I – PORTARIA SF 244, DE 09 DE NOVEMBRO DE 2020

Mapa de Calor

Impacto ⇨ / Probabilidade ⇩	Muito baixo	Baixo	Médio	Alto
Alta	Risco Moderado (4x1=4)	Risco Elevado (4x2=8)	Risco Elevado (4x3=12)	Risco Extremo (4x4=16)
Média	Risco Baixo (3x1=3)	Risco Moderado (3x2=6)	Risco Elevado (3x3=9)	Risco Elevado (3x4=12)
Baixa	Risco Baixo (2x1=2)	Risco Moderado (2x2=4)	Risco Moderado (2x3=6)	Risco Elevado (2x4=8)
Muito baixa	Risco Baixo (1x1=1)	Risco Baixo (1x2=2)	Risco Baixo (1x3=3)	Risco Moderado (1x4=4)

Mapa de calor é uma ferramenta que pode ser utilizada para a análise de riscos, apresentando de forma simples e visual suas relevâncias através do cruzamento das probabilidades e dos níveis de impacto.

Nível do risco é expresso pela combinação da probabilidade da ocorrência do evento e de suas consequências caso se concretize, em termos da magnitude do impacto nos objetivos.

- Nível de Risco (Risco Inerente) = Probabilidade x Impacto

A análise de riscos é o processo de compreender a natureza do risco e determinar o nível de risco. Ela fornece a base para a avaliação de riscos, bem como para as decisões quanto ao tratamento dos riscos.

Fator de Avaliação de Controles

Nível	Descrição	Fator
Inexistente	Controles inexistentes, mal desenhados ou mal implementados, isto é, não funcionais.	1
Fraco	Controles têm abordagens ad hoc, 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

Controle é uma medida que está (ou pretende estar) modificando o risco, podendo ser qualquer processo, política, dispositivo, prática ou outras ações.

Os controles internos da gestão podem ser definidos como sendo o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de servidores, destinados a enfrentar os riscos e fornecer segurança razoável na consecução da missão da entidade.

- Risco residual = Risco Inerente x Fator de Avaliação dos Controles