EMSERH
Empresa Maranhense de Serviços Hospitalares

POLÍTICA DE
CONTROLE INTERNO, CONFORMIDADE E GESTÃO DE RISCOS

2023

Política de Controle Interno, Conformidade e Gestão de Riscos [recurso eletrônico] / Arlenne Meneses, Jorge Filho, Leandro Silva – 1. ed. – São Luís: EMSERH, 2023.

20p.

1. Normativo. 2. Política. 3. Controle Interno. 4. Conformidade. 5. Gestão de Riscos.

CDD: 342
CDU: 341.3511

EMPRESA MARANHENSE DE SERVIÇOS HOSPITALARES
Avenida Borborema, 25, Quadra 16, Calhau|
CEP: 65071-360 |São Luís – MA |
Telefone: (98) 3235-7333 | Site: emserh.gov.ma.br

ELABORAÇÃO

Arlenne Manoella Freitas Meneses – Secretária Executiva do Conselho de Administração;
Jorge Luís Moura Nascimento Filho – Chefe do Núcleo de Controle Interno da Gestão;
Leandro Marques da Silva – Gerente de Governança.

APROVAÇÃO

COMISSÃO DE ELABORAÇÃO E REVISÃO DE NORMATIVOS (Portaria nº 026/2023/GAB/EMSERH, 11 de janeiro de 2023)
(Aprovado na 19º reunião ordinária, realizada em 20 de setembro de 2023)

Christiano Batista Mesquita – Presidente da Comissão de Sindicância;
Francisco Assis do Amaral Neto – Presidente da Comissão Setorial de Licitação;
Jorge Carlos Araújo de Araújo – Diretor Executivo de Gestão de Pessoas;
Leandro Marques da Silva – Gerente de Governança;
Lídia Cunha Schramm – Chefe do Núcleo Jurídico;
Marianna Laila Pereira Sena – Assessora Institucional da Presidência;
Paulo Eduardo Pacheco Cardoso Ronchi – Diretor Executivo de Planejamento, Governança e Inovação;
Silvana Carla Costa Dos Santos – Coordenadora do Comitê de Auditoria Estatutária;
Vânia Paula Moura Martins – Auditora Interna;
Wanderson Rafael Mendonça Batista – Diretor Executivo Financeiro.

DIRETORIA EXECUTIVA – EMSERH (Aprovado na 21º reunião ordinária, realizada em 23 de outubro de 2023)

Marcello Apolônio Duailibe Barros – Presidente;
Jessyca Costa Xavier - Diretora Executiva de Engenharia e Manutenção;
Jorge Carlos Araújo de Araújo - Diretor Executivo de Gestão de Pessoas;
Letícia Helena do Vale Façanha – Diretora Executiva Administrativa;
Paulo Eduardo Pacheco Cardoso Ronchi – Diretor Executivo de Planejamento, Governança e Inovação;
Ricardo Martins Castro – Diretor Executivo Clínico;
Wanderson Rafael Mendonça Batista – Diretor Executivo Financeiro;

CONSELHO DE ADMINISTRAÇÃO – EMSERH (Aprovado na 10º reunião ordinária, realizada em 30 de outubro de 2023)

Edmilson Silva Diniz Filho – Presidente do Conselho de Administração;
Allan Kardec Dualibe Barros Filho – Membro do Conselho de Administração;
Conceição Domingas Costa Dos Santos – Membro do Conselho de Administração;
Danyellen Castro Veloso – Membro independente do Conselho de Administração;
Gregória Barbosa – Membro do Conselho de Administração;
George Castro Figueira de Mello – Membro do Conselho de Administração;
Marcello Apolônio Duailibe Barros – Presidente da EMSERH;
Violeta Maria Soares Filgueiras – Membro independente do Conselho de Administração;

DIAGRAMAÇÃO

Leandro Marques da Silva – Gerente de Governança.

SUMÁRIO

POLÍTICA DE CONTROLE INTERNO, CONFORMIDADE E GESTÃO DE RISCOS

CAPITULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º A presente Política tem por finalidade estabelecer o direcionamento estratégico e as diretrizes para as atividades corporativas de controle interno, conformidade e gestão de riscos da Empresa Maranhense de Serviços Hospitalares - EMSERH.

Art. 2º A presente política se aplica à EMSERH, incluindo as unidades sob sua administração, bem como toda pessoa a ela vinculada que tenha acesso privilegiado à informação relevante, e está fundamentada nos seguintes instrumentos legais:

I - Estatuto Social da EMSERH;

II - Regimento Interno da EMSERH;

III – Lei Federal nº 12.846, de 1º de agosto de 2013;

IV - Código de Conduta e Integridade da EMSERH;

V - Lei Federal nº. 6.404, de 15 de dezembro de 1976;

VI - Lei Federal nº. 12.527, de 18 de novembro de 2011;

VII - Lei Estadual nº. 10.217, de 23 de março de 2015;

VIII - Lei Federal nº. 13.303, de 30 de junho de 2016;

IX - Decreto Federal nº. 8.945, de 27 de dezembro de 2016;

X – Instrução Normativa Conjunta MP/CGU nº 01/2016.

§ 1º A política de controle interno, conformidade e gestão de riscos, integra o Sistema de Gerenciamento de Riscos da EMSERH, o qual consiste no conjunto de instrumentos de governança e de gestão que suportam a concepção, implementação, monitoramento e melhoria contínua da gestão de riscos através de toda a organização e compreende, entre outros: política, estruturas organizacionais, planos, relacionamentos, responsabilidades, atividades, processos e recursos.

§ 2º Integram-se e alinham-se à política de controle interno, conformidade e gestão de riscos, as normas internas que regulamentam aspectos específicos dessas atividades no âmbito da EMSERH.

Art. 3º Para fins desta Política, consideram-se os seguintes conceitos:

I - Alta Administração: pessoa ou grupo de pessoas que dirige e controla uma organização no mais alto nível, ficando restrito esse conceito aos membros do Conselho de Administração e da Diretoria Executiva da EMSERH;

II - Risco: o é o efeito da incerteza sobre objetivos estabelecidos. É a possibilidade de ocorrência de eventos que afetem a realização ou alcance dos objetivos, combinada com o impacto dessa ocorrência sobre os resultados pretendidos;

III – Gerenciamento de riscos: processo sistematizado e integrado que tem como objetivo identificar o apetite ao risco no ambiente de negócios e minimizar ou neutralizar as ameaças;

IV – Gestão de riscos: conjunto de atividades coordenadas para identificar, analisar, avaliar, tratar e monitorar riscos com o fim de conferir razoável segurança ao alcance dos objetivos;

V – Identificação de riscos: Processo de busca, reconhecimento e descrição de riscos, que envolve a identificação de suas fontes, causas e consequências potenciais que possam ter algum impacto na consecução dos objetivos. A identificação de riscos pode envolver dados históricos, análises teóricas, opiniões de pessoas informadas e de especialistas e as necessidades das partes interessadas;

VI – Análise de riscos: processo de compreender a natureza e determinar o nível de risco, de modo a subsidiar a avaliação e o tratamento de riscos;

VII – Avaliação de riscos: determina o grau de exposição da empresa ao risco (dado pela probabilidade de ocorrência e impacto do evento), a mensuração (quantificação das estimativas de perdas) e o tratamento dado aos riscos (tomada de uma decisão básica por parte da empresa: a de evitar ou aceitar o risco);

VIII – Monitoramento dos riscos: constante acompanhamento, por parte do conselho, comitês e da diretoria executiva, da eficácia e adequação do processo. Mede o desempenho da gestão de riscos, por meio de indicadores chave de risco, análise do ritmo de atividades, operações ou fluxos atuais em comparação com o que seria necessário para o alcance de objetivos ou manutenção das atividades dentro dos critérios de risco estabelecidos;

IX – Comunicação dos riscos: processo de documentar e reportar as informações sobre o resultado do processo de gestão de riscos para tomada de decisão, contribuindo para que o ambiente corporativo reflita os valores e a cultura de riscos desejada pela organização;

X – Apetite ao risco: é o nível de risco que uma organização está disposta a aceitar na busca do alcance de seus objetivos;

XI – Controles internos: são as ações estabelecidas por meio de políticas e procedimentos, desempenhadas em todos os níveis da organização, em vários estágios dentro do processo organizacional e no ambiente tecnológico, que ajudam a garantir o

cumprimento das diretrizes determinadas pela Administração para mitigar os riscos à realização dos objetivos;

XII – Auditoria: atividade independente que reúne diversas funções como a avaliação e consultoria para adicionar valor e melhorar as operações de uma organização. Atua na estrutura e no processo de gestão de riscos, em todos os níveis relevantes das atividades organizacionais, ou seja, procurando testar os aspectos sistêmicos da gestão de riscos em vez de situações específicas;

XIII – Matriz de riscos: Ferramenta de gerenciamento de risco, orientada por duas dimensões: probabilidade e impacto, que permite, graficamente, a visualização dos riscos que necessitam de mais atenção, possibilitando a tomada de decisões e a realização de medidas preventivas para tratar esses riscos;

XIV – Governança: combinação de processos e estruturas implantadas pela alta administração da organização, para informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas dessas atividades para a sociedade;

XV – 1ª Linha de defesa: funções que gerenciam e têm propriedade de riscos, contemplando a gestão operacional e os procedimentos rotineiros de riscos e controles internos. Nesse nível se identificam, avaliam e mitigam riscos por meio do desenvolvimento e da implementação de políticas e procedimentos internos que possam oferecer garantia razoável de que as atividades estejam de acordo com as metas e objetivos;

XVI – 2ª Linha de defesa: funções que supervisionam riscos, sendo constituída por áreas de riscos e controles internos, comitês ou outras estruturas organizacionais estabelecidas para garantir que a primeira linha funcione como pretendido no que diz respeito à gestão de riscos e controles. Seu papel é coordenar as atividades de gestão de riscos, orientar e monitorar a implementação das práticas de gestão de riscos por parte da gestão operacional, apoiar a definição de metas de exposição a risco, monitorar riscos específicos, bem como ajudar a definir controles e/ ou monitorar riscos e controles da primeira linha de defesa.

XVII – 3ª Linha de defesa: constituída pela auditoria interna. Fornece avaliações (asseguraçõ̃es) independentes e objetivas sobre os processos de gestão de riscos, controles internos e governança aos órgãos de governança e à alta administração para atingimento de metas. Tais avaliações devem abranger uma grande variedade de objetivos (incluindo eficiência e eficácia das operações; salvaguarda de ativos; confiabilidade e integridade dos processos administrativos; conformidade com leis e regulamentos) e elementos da estrutura de gestão de riscos e controle interno em todos os níveis da estrutura organizacional da entidade.

XVIII – Stakeholders: Os grupos e indivíduos cujos interesses são atendidos ou impactados pelas ações EMSERH.

Art. 4º A EMSERH está organizada pelas premissas da boa governança e esta Política representa a base dos demais documentos relativos ao Controle Interno, Conformidade e Gestão de Riscos, necessários ao ordenamento jurídico interno para a organização integrada das regras macro e micro do complexo Sistema de Gerenciamento de Riscos, Conformidade e Controles Internos.

CAPÍTULO II
DOS PRÍNCIPIOS

Art. 5º A política de controle interno, conformidade e gestão de riscos, será orientada pelos valores da EMSERH, bem como pelos seguintes princípios:

I – inovação: fomentar a inovação e ação empreendedora responsáveis;

II – integração: a gestão de riscos é parte integrante de todas as atividades organizacionais, diretamente relacionada com a melhoria do desempenho das atividades, à conformidade legal e regulatória, à qualidade dos serviços, à geração de valor, à governança e à reputação;

III – responsabilidade**:** zelo dos agentes de governança na definição de estratégias e na execução de ações para a aplicação de recursos públicos, e na obrigação da empresa e seus empregados de responsabilizarem-se por suas decisões e pela prestação de contas de sua atuação de forma voluntária, assumindo integralmente a consequência de seus atos e omissões;

IV – transparência: As informações devem ser completas, precisas e claras para a adequada tomada de decisão das partes interessadas na gestão das atividades;

V – compromisso: dever do agente público, de se vincular, assumir, agir ou decidir pautado em valores éticos que norteiam a relação com os envolvidos na prestação de serviços à sociedade, prática indispensável à implementação da governança.

CAPÍTULO III
DOS OBJETIVOS

Art. 6º São objetivos da Política de Controle interno, Conformidade e Gestão de riscos:

I – reduzir o impacto negativo dos riscos sobre as metas organizacionais, por meio da adoção de controles internos, concebidos e implementados pelo próprio gestor para aumentar a probabilidade de alcance dos objetivos da organização;

II – assegurar que os responsáveis pela tomada de decisão, em todos os níveis da EMSERH, tenham acesso tempestivo a informações suficientes quanto aos riscos aos quais está exposta a organização, inclusive para determinar questões relativas à delegação, se for o caso;

III – agregar valor à organização por meio da melhoria dos processos de tomada de decisão e do tratamento adequado dos riscos e dos impactos negativos decorrentes de sua materialização;

IV - disseminar a cultura da gestão de riscos, controles internos e conformidade com os preceitos éticos, a legislação nacional e internacional, os princípios, as políticas e os normativos internos e as boas práticas de Governança Corporativa e Integridade;

V – assegurar a conformidade com as leis e regulamentos aplicáveis, incluindo normas, políticas, programas, planos e procedimentos de governo e da própria EMSERH.

CAPÍTULO IV
DAS DIRETRIZES

Art. 7º A Política de controle interno, conformidade e gestão de riscos será orientada pelas seguintes diretrizes:

I – o processo de controle interno, conformidade e gestão de riscos na EMSERH, deverá contemplar o estabelecimento do contexto, a identificação, a análise, a avaliação e o tratamento de riscos, a comunicação e consulta com partes interessadas, o monitoramento e a melhoria contínua;

II – a gestão de riscos deverá ser baseada na Metodologia de Gestão de Riscos e Controles Internos, sustentada por uma ferramenta corporativa e executada conforme um processo operacional, sendo esta sistematizada e suportada pelas premissas da metodologia do Committee of Sponsoring Organizations of the Treadway Commission (COSO) e de boas práticas;

III – as metodologias e ferramentas implementadas deverão possibilitar a obtenção de informações úteis à tomada de decisão para a consecução dos objetivos institucionais e para o gerenciamento e a manutenção dos riscos dentro de padrões definidos pelas instâncias supervisoras;

IV – a medição do desempenho da gestão de riscos deverá ser realizada mediante atividades contínuas ou de avaliações independentes ou a combinação de ambas;

V – a gestão de riscos e controles internos deverá ser medida, monitorada e avaliada por meio de relatórios e indicadores de desempenho;

VI – a gestão de riscos e controles internos da EMSERH deverá ser organizada nas seguintes dimensões:

a) **riscos operacionais** (inclusive os riscos à integridade): risco de perdas resultantes direta ou indiretamente de falha ou inadequação de processos internos, pessoas e sistemas ou de eventos externos.

b) **riscos estratégicos:** risco de longo prazo ou risco de oportunidade relacionado aos objetivos estratégicos e às estratégias adotadas para alcançá-los.

c) **riscos legais:** qualquer ameaça que a empresa pode sofrer por descumprimento à legislação, tornando-a sujeita a aplicação de penalidades. Serão considerados os riscos tributários, trabalhista, regulatório, de litígio e de fraude.

d) **riscos financeiros/orçamentários:** eventos que podem comprometer a capacidade do órgão ou entidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações.

e) **riscos de imagem/reputação:** eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do órgão ou da entidade em cumprir sua missão institucional.

f) **riscos de impacto à saúde humana:** eventos que demandam o emprego urgente de medidas de prevenção, de controle e de contenção de riscos, de danos e de agravos à saúde pública em situações que podem ser epidemiológicas (surtos e epidemias), de desastres, ou de desassistência à população.

VII – o comprometimento da alta direção, de forma inequívoca, deve permitir aos responsáveis pela área de gestão de riscos e controles internos o acesso irrestrito às áreas e às informações necessárias exclusivamente à realização de suas atividades, com a garantia da independência na sua atuação;

VIII – a sugestão da prioridade de gestão de riscos será realizada pelo Núcleo de Controle Interno da Gestão, submetida à apreciação do Comitê de Controle de Riscos, da Diretoria Executiva, do Comitê de Auditoria Estatutário e aprovada pelo Conselho de Administração por meio do Planejamento de Atividades do Núcleo de Controle Interno da Gestão – PLANCIG;

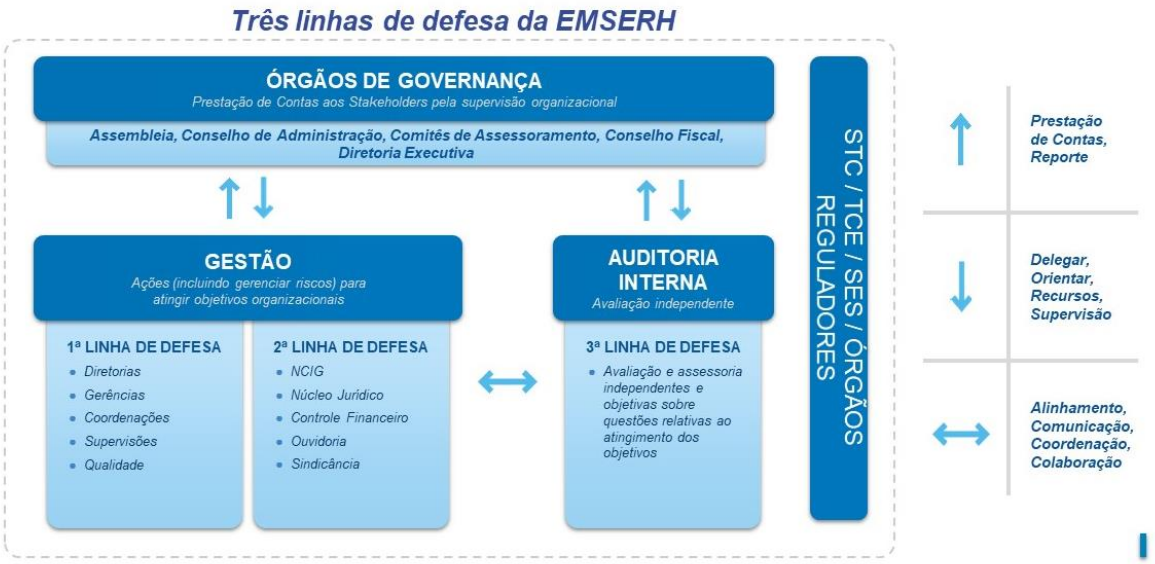
IX – o monitoramento do desempenho da gestão de riscos deve ser realizado pela Diretoria Executiva, com periodicidade mínima trimestral, e o registro deve ocorrer em todas as etapas do processo, na ferramenta de gerenciamento de riscos adotada pela empresa;

X – a capacitação dos empregados e agentes que exercem cargo ou função na EMSERH, nos temas afetos a essa Política, deve ser desenvolvida de forma continuada, por meio de soluções educacionais, em todos os níveis;

XI – o gerenciamento de riscos nas contratações utilizará os procedimentos previstos no REGULAMENTO INTERNO DE LICITAÇÕES E CONTRATOS DA EMSERH – RILC, voltados a evitar possíveis riscos que possam comprometer a efetividade do planejamento da contratação, da seleção do fornecedor e da gestão contratual;

CAPÍTULO V
DO SISTEMA DE GESTÃO DE RISCOS

Art. 8º O Sistema de Gestão de Riscos da EMSERH é formado por 3 (três) linhas de defesa que definem as responsabilidades da gestão de riscos, conformidade e controles internos que operam simultaneamente, conforme abaixo ilustrado:



Art. 9º Os Órgãos de Governança da EMSERH, representados pelo Conselho de Administração, Comitês de Assessoramento, Conselho Fiscal e Diretoria Executiva têm por responsabilidade determinar a direção da organização, definindo a visão, missão, valores e apetite organizacional a riscos, delegando a responsabilidade pelo atingimento dos objetivos da organização à gestão, juntamente com os recursos necessários. Além destas responsabilidades, são papéis dos Órgãos de Governança:

I – aceitar a prestação de contas pela supervisão da organização perante os stakeholders;

II – envolver os stakeholders, para monitorar seus interesses e se comunicar de forma transparente sobre o atingimento dos objetivos;

III – cultivar uma cultura que promova comportamento ético e com responsabilidade;

IV – estabelecer estruturas e processos para governança, incluindo comitês auxiliares, conforme necessário.

V – delegar responsabilidades e oferecer recursos à gestão para atingir os objetivos da organização.

VI – determinar o apetite organizacional a riscos e exercer a supervisão do gerenciamento de riscos (incluindo controle interno).

VII – manter a supervisão da conformidade com as expectativas legais, regulatórias e éticas.

VIII – estabelecer e supervisionar uma função de auditoria interna independente, objetiva e competente.

Art. 10 A 1ª Linha de defesa, representada pelas Diretorias, Gerências, Coordenações, Supervisões e Qualidade, têm por responsabilidade realizar a gestão de riscos e controles em suas áreas de atuação, devendo identificar, avaliar, controlar e reduzir as incertezas que possam interferir no alcance dos objetivos organizacionais da EMSERH, sendo seu papel:

I – liderar e dirigir ações (incluindo gerenciamento de riscos) e aplicação de recursos para atingir os objetivos da organização;

II – manter um diálogo contínuo com o órgão de governança e reportar: resultados planejados, reais e esperados, vinculados aos objetivos da organização e riscos;

III – estabelecer e manter estruturas e processos apropriados para o gerenciamento de operações e riscos (incluindo controle interno);

IV – garantir a conformidade com as expectativas legais, regulatórias e éticas.

Art. 11 A 2ª Linha de defesa, representada pelo Núcleo de Controle Interno de Gestão, Núcleo Jurídico, Controle Financeiro, Ouvidoria e Sindicância, têm por responsabilidade fornecer assistência no gerenciamento dos riscos, conformidade e controles internos de forma a monitorar, assessorar, orientar, testar, analisar e reportar sobre a adequação e eficácia dos assuntos relacionados ao gerenciamento de riscos, incluindo:

I – desenvolvimento, implantação e melhoria contínua das práticas de gerenciamento de riscos (incluindo controle interno) nos níveis de processo, sistemas e entidade;

II – o atingimento dos objetivos de gerenciamento de riscos, como: conformidade com leis, regulamentos e comportamento ético aceitável; controle interno; segurança da informação e tecnologia; sustentabilidade; e avaliação da qualidade;

Art. 12 A 3ª Linha de defesa, representada pela Auditoria Interna, tem como responsabilidade, aferir a adequação do controle interno, a efetividade do gerenciamento dos riscos e dos processos de governança. São papéis da Auditoria Interna:

I – Manter a prestação de contas primária perante o órgão de governança e a independência das responsabilidades da gestão;

II – Comunicar a avaliação e assessoria independentes e objetivas à gestão e ao órgão de governança sobre a adequação e eficácia da governança e do gerenciamento de riscos

(incluindo controle interno), para apoiar o atingimento dos objetivos organizacionais e promover e facilitar a melhoria contínua;

III – Reporta ao órgão de governança prejuízos à independência e objetividade e implanta salvaguardas conforme necessário;

IV – Acompanhar as atividades, processos e procedimentos no âmbito da EMSERH, visando comprovar o cumprimento das metas, o alcance dos objetivos e a adequação da gestão;

V –propor as medidas preventivas e corretivas dos desvios detectados e verificar o cumprimento e a implementação pela EMSERH de recomendações ou determinações efetuadas pela Secretaria de Transparência e Controle, pelo Tribunal de Contas do Estado e pelo Conselho Fiscal da EMSERH;

Art. 13 Os Órgãos de Governança, como as principais partes interessadas atendidas pelo sistema são responsáveis por garantir que as Linhas de defesa sejam aplicadas aos processos de gerenciamento de riscos, conformidade e controles internos desta empresa.

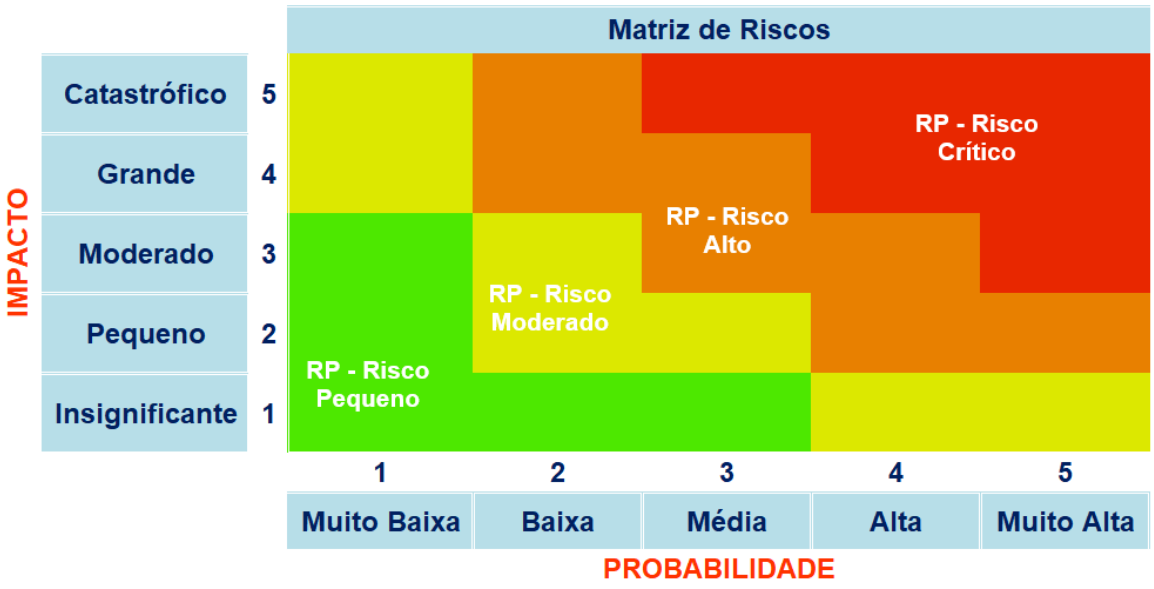
CAPÍTULO VI
DA GESTÃO DE RISCOS
Seção I – Da Estrutura

Art. 14. O processo de gestão de riscos inicia-se com o levantamento dos riscos, seguido da identificação e classificação dos mesmos. Após a identificação e classificação dos riscos são verificadas as atividades de controles existentes nos processos, visando reduzir as possibilidades de erros e eventuais irregularidades.

Art. 15. A análise dos riscos é realizada qualitativamente e quantitativamente visando a definição dos atributos de impacto e da probabilidade, utilizados na priorização dos riscos a serem tratados.

Art. 16. A avaliação dos riscos determina a significância do nível e do tipo de risco, classificando-os como Pequeno, Moderado, Alto ou Crítico.

Art. 17. Com o objetivo de visualizar e, ao mesmo tempo, implementar uma forma de tratamento de cada risco, o resultado da avaliação dos riscos será apresentado em um mapa de riscos, chamada de Matriz de Riscos. Com a divisão da matriz em quadrantes, pode-se avaliar a criticidade dos riscos. Quanto maior for a probabilidade e o impacto de um risco, maior será seu nível de criticidade, conforme modelo abaixo:



Art. 18. O tratamento consiste em estipular uma resposta estratégica ao risco mapeado e avaliado, por meio de um Plano de Ação visando reduzir o risco a um nível aceitável. As ações são planejadas para priorizar as causas identificadas como grandes potencializadoras do risco, de acordo com o nível do risco identificado, objetivando:

I – evitar (eliminar completamente os elementos de exposição a um risco específico);

II – reduzir/mitigar (implementar controle para reduzir a probabilidade ou a consequência dos riscos ou até mesmo de ambos);

III – transferir/compartilhar (neste caso requer um parceiro com interdependência financeira e que esteja disposto a aceitar o risco);

IV – aceitar/tolerar (aceitar o risco dentro do seu apetite previamente estabelecido).

Art. 19. O monitoramento dos Riscos consiste em supervisionar o gerenciamento de riscos, a implantação e manutenção dos planos de ação, por meio de atividades gerenciais contínuas e acompanhar os indicadores a serem instituídos pelas áreas, assim como os possíveis riscos residuais.

Art. 20. A comunicação de riscos atinge todas as partes interessadas, sendo realizada de forma clara e objetiva, respeitando as boas práticas de governança.

Seção II
Do Apetite ao Risco

Art. 21. Considerando a Matriz de Riscos, o nível de risco que a EMSERH está disposta a aceitar é denominado “Apetite ao Risco” e indica a faixa de riscos que a EMSERH pode assumir, embora tenha necessidade de tratá-los com presteza, sendo assim descritos:

I – riscos do quadrante vermelho, cujo nível de risco muito alto, são inaceitáveis para a EMSERH. Os gestores dos riscos deverão elaborar planos de ação, para execução imediata, com submissão à Diretoria Executiva para autorização, com o objetivo de reduzi-los ao nível aceitável, ou seja, situá-los nos quadrantes laranja ou amarelo;

II – riscos do quadrante laranja, com nível de risco alto, são classificados como aceitável para a EMSERH. O gestor de primeira linha poderá assumir este tipo de risco, considerando a relação custo-benefício ou por questões estratégicas. Entretanto, é obrigatório o tratamento deste risco em curto prazo;

III – riscos do quadrante amarelo, com nível de risco médio, fazem parte do Apetite aos Riscos da EMSERH, devendo ser monitorados de forma rotineira e sistemática. Os gestores podem tomar a decisão de aceitá-los, de acordo com o estabelecido nos planos de ação da unidade orgânica. São, portanto, riscos aceitáveis;

IV – riscos do quadrante verde, com nível de risco baixo, encontram-se na zona de conforto, representam pequeno problema e causam pouco ou nenhum prejuízo à empresa e, por isso, também fazem parte do Apetite ao Risco da EMSERH, podendo ser administrados.

Art. 22. A figura a seguir representa os níveis de tolerância ao risco e de apetite ao risco da EMSERH:

Apetite ao Risco	Aplicação
BAIXO	Encontram-se na zona de conforto, representam pequeno problema e causam pouco ou nenhum prejuízo à empresa
MÉDIO	Fazem parte do apetite aos riscos da EMSERH, devendo ser monitorados de forma rotineira e sistemática
ALTO	São classificados como toleráveis para a EMSERH
MUITO ALTO	Cujo nível de risco muito alto, são inaceitáveis para a EMSERH

Art. 23. No processo de aceitação dos riscos corporativos considera-se que o nível atual do risco que está dentro do apetite ao risco é assumido pela EMSERH, não existindo obrigação para realizar ações definidas para seu tratamento. No entanto, de acordo com os riscos identificados, a decisão deve ser submetida à aprovação do risco e/ou plano de ação.

Art. 24. O gerenciamento de risco da EMSERH integra-se às estratégias da empresa, com o intuito de alinhar todos os processos finalísticos existentes e praticados com esta Política. A forma de atuação possibilita a identificação das áreas com maior potencial de risco e os cenários mais críticos para, por meio de uma gestão efetiva estabelecer os indicadores chaves de risco, controlar e mitigar a exposição ao risco operacional a que a EMSERH está sujeita.

Art. 25. O acompanhamento do Apetite aos Riscos será realizado pelo Núcleo de Controle Interno da Gestão e monitorado permanentemente pela Alta Administração, através de:

I – processos efetivos de controles, em que os gestores são informados quanto às exposições a riscos e a respectiva utilização dos limites vigentes;

II – emissão de relatórios informatizados, o que facilita a comunicação e destaca as eventuais exceções dos limites, as quais requerem discussão, autorização para exceções e/ou medidas de adequação, apoiando a Alta Administração na avaliação da coesão dos resultados em relação ao apetite a riscos;

Art. 26. Todo desvio (quebra de limite) ao apetite ao risco definido pela EMSERH deve ser acompanhado de justificativa por escrito dos gestores responsáveis pelo processo e autorizado pela Diretoria Executiva.

Seção III
Da Comunicação de riscos

Art. 27. A comunicação de riscos deverá ser implementada em todas as etapas do processo de gestão de riscos. O Núcleo de Controle Interno da Gestão irá:

I – reportar ao final da etapa qualitativa (identificação, avaliação e análise dos riscos) os resultados dos trabalhos realizados à Diretoria executiva responsável pela área gestora do risco, por meio do envio do arquivo consolidado na Matriz de Riscos, contendo a classificação dos riscos como Pequeno, Moderado, Alto ou Crítico;

II – encaminhar os relatórios de monitoramento dos riscos ao conhecimento da Diretoria Executiva, Conselho de Administração, Conselho Fiscal, Comitê de Controle de Riscos e Comitê de Auditoria Estatutária;

III – submeter à Diretoria Executiva, relatório, ao fim de cada levantamento de riscos, contendo os riscos de nível crítico para aprovação do tratamento proposto no plano de ação, elaborado pelas áreas gestoras dos riscos. Após aprovação a área gestora do risco ficará responsável por acompanhar e implementar os controles aprovados;

IV – elaborar relatórios trimestrais de suas atividades, submetendo-os à Diretoria Executiva, Conselho de Administração, Conselho Fiscal, Comitê de Controle de Riscos e Comitê de Auditoria Estatutária.

CAPÍTULO VII
DAS COMPETÊNCIAS RESPONSABILIDADES

Art. 28. Sem prejuízo das atribuições expressas nesta Política de Controle Interno, Conformidade e Gestão de Riscos, são instâncias responsáveis pelo Sistema de Gestão de Riscos e Controles Internos da EMSERH:

I – **Conselho de Administração** é responsável por supervisionar os sistemas de gestão de riscos e controles internos e por definir os limites de apetite a riscos da empresa;

II –**Diretoria Executiva** é responsável por cumprir e fazer cumprir a política e os normativos relacionados à gestão de riscos e controles internos;

III – **Diretores** são responsáveis pela supervisão da gestão de riscos e controles internos das áreas sob sua subordinação;

IV – **Empregados** e **gestores** da empresa são responsáveis por manter os controles internos eficazes e por conduzir procedimentos de gestão de riscos e controles internos na execução de seus processos, projetos ou atividades;

V – **Auditoria Interna** é responsável por prover avaliações sobre a eficácia da governança, da gestão de riscos e dos controles internos;

VI – **Área de Governança** é responsável por assessorar a Diretoria Executiva na supervisão do sistema de governança, gestão de riscos, controles internos, conformidade e segurança da informação, competindo-lhe:

a) assegurar o alinhamento da gestão de riscos com os objetivos do planejamento estratégico institucional;

b) definir o apetite a riscos e deliberar sobre as propostas de alteração dos níveis de exposição a riscos que possam impactar o alcance dos objetivos institucionais;

c) assegurar que as informações relevantes sobre gestão de riscos estejam disponíveis para subsidiar a tomada de decisão;

d) assegurar a utilização de mecanismos de comunicação e de institucionalização da gestão de riscos;

e) criar mecanismos de transparência ativa e passiva, estabelecendo diretrizes e práticas que garantam a divulgação clara, acessível e oportuna de informações;

f) avaliar, controlar e monitorar o desempenho institucional atinente à conformidade, integridade, gestão de riscos e controle interno;

g) assegurar a realização de ações que incentivem e promovam a cultura e a capacitação na gestão de riscos; e

h) assegurar alocação dos recursos necessários à gestão de riscos.

VII – **Núcleo de Controle Interno** é responsável por assessorar o planejamento, a execução, o monitoramento e a avaliação da gestão de riscos e controles internos das gerências de sua respectiva Diretoria;

VIII – **Unidades Administrativas e Hospitalares** são responsáveis pela implementação desta política em seus segmentos de atuação, seguindo as orientações normativas emitidas sobre os temas; e

IX – **Comitê de Controle de Riscos** é responsável por:

a) fomentar o desenvolvimento da gestão de riscos nas unidades organizacionais da EMSERH e apoiar o monitoramento dos controles implementados por estas;

b) prestar apoio o Conselho de Administração quanto a análise e/ou revisão dos riscos ou ameaças que podem impedir a empresa de atingir seus objetivos e simular possíveis resultados negativos e positivos;

c) conduzir as ações de gestão de riscos e controles internos e emitir orientações para adoção e implementação desta política;

d) supervisionar os sistemas de gestão de riscos estabelecidos para a prevenção e mitigação dos principais riscos aos quais a EMSERH está exposta, inclusive os relacionados à integridade das informações contábeis e financeiras e àqueles relacionados à ocorrência de corrupção e fraude;

e) Avaliar, semestralmente, a eficácia da política de gerenciamento de risco das operações gerais da empresa, mediante a emissão relatório a ser submetido ao Conselho de Administração;

f) Avaliar os níveis de apetite por riscos da empresa e as estratégias para o seu gerenciamento, considerando os riscos individualmente e de forma integrada;

g) Emitir recomendações ao Conselho de Administração quanto à adoção de ações para reduzir desvantagens identificadas e transformá-las em oportunidades;

X – **Comitê de Auditoria Estatutário** tem a responsabilidade direta sobre a confiabilidade das comunicações externas e deve reconhecer os riscos relativos a uma comunicação confiável dos relatórios financeiros. É responsável por assessorar o Conselho de Administração no estabelecimento de políticas globais relativas à gestão de riscos.

CAPÍTULO VIII
DO CONTROLE INTERNO

Art. 29. O Controle Interno representa um conjunto de processos, procedimentos e atividades desenvolvidas pelo Conselho de Administração, Diretoria Executiva e corpo de empregados da EMSERH, com a finalidade de possibilitar uma garantia razoável quanto à realização dos objetivos nas seguintes categorias:

I – Eficácia e eficiência das operações (riscos operacionais);

II – Confiabilidade das demonstrações financeiras (relatórios financeiros);

III – Conformidade com leis e regulamentos cabíveis (compliance).

Art. 30. Compete ao Núcleo do Controle Interno da Gestão oferecer os seguintes serviços:

I – Auxiliar no desenvolvimento e implementação de políticas e procedimentos para promoção da eficiência, transparência e conformidade dentro da EMSERH;

II – Estabelecer mecanismos de monitoramento e avaliação para acompanhar o desempenho das operações da EMSERH;

III – Realizar análises detalhadas dos processos organizacionais, identificando ineficiências, gargalos e possíveis pontos de melhoria, podendo propor recomendações e soluções para otimizar os processos e aumentar a eficiência operacional;

IV – Auxiliar na identificação e avaliação dos riscos operacionais da EMSERH, podendo desenvolver controles internos para mitigar os riscos e garantir a conformidade com as políticas e regulamentações internas;

V – Auxiliar na implementação e monitoramento dos sistemas de informação e tecnologia utilizados na EMSERH, de forma a garantir que os sistemas sejam seguros, confiáveis e capazes de fornecer informações precisas para tomada de decisões;

VI – Fornecer treinamentos e capacitação para os funcionários da EMSERH, visando conscientizá-los sobre a importância dos controles internos, políticas e procedimentos.

CAPÍTULO IX
DA CONFORMIDADE

Art. 31. A conformidade deve garantir que determinado processo está de acordo com as normas aplicáveis identificadas como critérios para sua execução.

Art. 32. A conformidade deve permitir a:

I – adequação legal e normativa dos processos de trabalho;

II – segregação de funções nos processos de tomada de decisão; e;

III – fiscalização pelas instâncias superiores e por órgãos de controle interno ou externo dos processos da empresa;

Art. 33. A operacionalização da conformidade deverá se pautar na busca de informações e cumprimento das leis, regulamentos e normas aplicáveis à EMSERH e no fomento à cultura de prevenção de problemas.

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 34. Esta Política deve ser acompanhada pelo Conselho de Administração, Diretoria executiva, Conselho Fiscal, Comitê de Controle de Riscos, Comitê de Auditoria Estatutário, Auditoria Interna e Núcleo de Controle Interno de Gestão no que tange à aplicação dos procedimentos e ao controle de suas diretrizes.

Art. 35. O presente documento deve ser lido e considerado em conjunto com outros padrões, normas e procedimentos aplicáveis, adotados pela EMSERH. Além disso, esta Política deve ser desdobrada em outros documentos normativos específicos, sempre alinhados às diretrizes e princípios aqui estabelecidos.

Art. 36. As demais políticas e documentos organizacionais devem observar e serem ajustados, no que couber, às diretrizes desta política.

Art. 37. A não observância desta política e seus desdobramentos normativos implicará em sanções previstas no Regime Disciplinar - apuração de irregularidades disciplinares e responsabilidade administrativa e aplicação de penalidade disciplinar, e no Código de Ética, Conduta e Integridade da EMSERH.

Art. 38. Os casos omissos e excepcionais serão analisados e tratados pela diretoria executiva e, se for o caso, reportados para decisão das instâncias competentes.

Art. 39. Esta Política será revisada a cada 2 (dois) anos e atualizada sempre que necessário.

Art. 40. Esta Política entrará em vigor na data da publicação de sua aprovação pelo Conselho de Administração e permanecerá vigente por prazo indeterminado, até que haja deliberação contrária pelo órgão competente.

REFERÊNCIAS BIBLIOGRÁFICAS

ALTOUNIAN, C.R; SOUZA, D.L; LAPA, L.R.G. Gestão e Governança Pública para Resultados: Uma visão prática. 2ª Edição. Belo Horizonte: Editora Forum, 2020.

BRASIL, Tribunal de Contas da União. Referencial básico de gestão de riscos. Brasília: TCU, Secretaria Geral de Controle Externo (Segecex), 2018. Disponível em:https://portal.tcu.gov.br/data/files/21/96/61/6E/05A1F6107AD96FE6F18818A8/Referencial_basico_gestao_riscos.pdf, acesso em 12/09/2023.

Instituto Brasileiro de Governança Corporativa. Gerenciamento de Riscos Corporativos: evolução em governança estratégica. Série Cadernos de Governança Corporativa, 19. São Paulo, 2017. Disponível em: https://www.egov.df.gov.br/wp-content/uploads/2018/03/IBGC-%E2%80%93-Gerenciamento-de-Riscos-Corporativos-%E2%80%93-2017.pdf, acesso em 12/09/2023.

SERPRO. Metodologia de Gestão de Riscos e Controles Internos. Brasília, 2021. Disponível em: https://www.transparencia.serpro.gov.br/governanca/governanca-corporativa/gestao-de-riscos/dd-ri-001-2023_merged.pdf, acesso em 12/09/2023.

BRASIL, Ministério da Saúde. Plano de Respostas às Emergências em Saúde Pública. Brasília, 2014. Disponível em: Plano de Resposta às Emergências em Saúde Pública (saude.gov.br), acesso em 12/09/2023.

BRASIL, Ministério da Saúde. Gestão de Riscos. Brasília: Coordenação de Gestão de Riscos, 2021. Disponível em: Gestão de Riscos Ministério da Saúde (saude.gov.br), acesso em 12/09/2023.

BRASIL, Portaria GM/MS nº 1.185, de 9 de junho de 2021. Institui a Política de Gestão de Riscos no âmbito do Ministério da Saúde (PGR/MS). Diário Oficial da União. Brasília, DF, Edição: 107, Seção: 1, Página: 139.

Instituto Brasileiro de Governança Corporativa. Guia de Orientação para Gerenciamento de Riscos Corporativos. Série de Cadernos de Governança Corporativa, 3. São Paulo, 2007. Disponível em: 3.pdf (usp.br), acesso em 12/09/2023.

Committee of Sponsoring Organizations of the Treadway Commission, COSO. Gerenciamento de Riscos Corporativos – Estrutura Integrada. Jersey City, AICPA 2007. Disponível em: COSOIIERMExecutiveSummaryPortuguese.pdf (mpu.mp.br), acesso em 12/09/2023.

BRASIL, Ministério da Educação. Site da EBSERH – Política de Conformidade, Controle Interno e Gerenciamento de Riscos da EBSERH. Disponível em: politica-de-conformidade-controle-interno-e-gerenciamento-de-riscos-2023.pdf (www.gov.br), acesso em 12/09/2023.

Companhia Nacional de Abastecimento. Política de Gestão de Riscos, Conformidade e Controles Internos – 10.007. SUCOR. Brasília, 2022. Disponível em: 10.007_POLITICA_RISCOS_1_6_2022_1 (1).pdf, acesso em 12/09/2022.

The Institute of Internal Auditors. Modelo das Três Linhas do IIA 2020: Uma atualização das Três Linhas de Defesa. Flórida, 2020. Disponível em: 3 linhas de defesa.pdf, acesso em 12/09/2023.