

INSTITUTO MEMORIAL DO AGRESTE

POLÍTICA DE GESTÃO DE RISCOS

*Programa de Integridade · **Edição 2026***
Versão 01 — Edição Institucional Definitiva

MANUTNEDOR
IMA – Instituto Memorial do Agreste
CNPJ 24.262.537/0001-98

UNIDADE HOSPITALAR
Hospital Memorial de Pernambuco – HMP
CEBAS · Utilidade Pública Municipal · SUS/ CNES

CARUARU – PERNAMBUCO
Edição Institucional · 2026

Objeto

Esta Política estabelece diretrizes, responsabilidades e critérios para o gerenciamento de riscos de integridade no âmbito do Hospital Memorial de Pernambuco – HMP.

Ficha Técnica

Documento	Política de Gestão de Riscos
Código	HMP.POL.001
Versão	01
Edição	2026
Classificação	Pública
Mantenedora	IMA – Instituto Memorial do Agreste · CNPJ 24.262.537/0001-98
Unidade	Hospital Memorial de Pernambuco – HMP · CNES 4222466
Abrangência	Todas as unidades, colaboradores, corpo clínico, terceiros, fornecedores, prestadores de serviço, representantes e parceiros
Base legal	Código de Ética e Conduta; Política Antifraude e Anticorrupção; Política de Canal de Denúncias; legislação trabalhista, civil, penal, sanitária, anticorrupção, proteção de dados e demais normas aplicáveis. COSO ERM II.
Vigência / Revisão	Bienal, ou antes, diante de alteração normativa, contratual ou institucional relevante

Elaborador	Aline Melissa Santos Oliveira	Resp. Área de Integridade	11/09/2026
Revisor	Flaviano Neves de Andrade	Diretor Administrativo	13/09/2026
Aprovador	Sidney Souza Araújo Ribeiro	Diretor Presidente	17/09/2026

SUMÁRIO

1. Objetivo
2. Abrangência
3. Referências e fundamentos
4. Conceitos essenciais
5. Diretrizes do gerenciamento de riscos
6. Estrutura de governança e responsabilidades
7. Categorias e níveis de decisão
8. Apetite, tolerância e limites de exposição
9. Processo institucional de gestão de riscos
10. Identificação e descrição dos riscos
11. Avaliação da probabilidade
12. Avaliação do impacto
13. Cálculo e classificação do risco inerente
14. Identificação e avaliação dos controles
15. Determinação do risco residual ou nível final
16. Respostas aos riscos e planos de ação
17. Monitoramento, comunicação e reporte
18. Uso obrigatório da planilha institucional
19. Capacitação e cultura de riscos
20. Revisão da política e disposições finais

1. Objetivo

A presente Política estabelece o modelo de gestão de riscos do Hospital Memorial de Pernambuco – HMP, definindo princípios, responsabilidades, critérios, instrumentos e rotinas para reconhecer, analisar, priorizar, tratar, acompanhar e comunicar os eventos que possam afetar o alcance dos objetivos institucionais.

A gestão de riscos deverá apoiar a tomada de decisão, a segurança do paciente, a continuidade assistencial, a integridade, a sustentabilidade econômico-financeira, o cumprimento das obrigações legais e contratuais e a proteção da reputação institucional. A finalidade não é eliminar toda incerteza, mas assegurar que os riscos sejam conhecidos, avaliados de forma consistente e mantidos dentro dos limites aprovados pela Alta Administração.

Esta Política também regulamenta o uso da planilha oficial de Identificação e Monitoramento de Riscos, tornando obrigatórios os parâmetros de probabilidade, impacto, classificação, controles, risco residual, resposta, plano de ação e acompanhamento definidos neste documento.

2. Abrangência

Esta Política aplica-se à Alta Administração, conselhos, diretoria, gestores, coordenadores, responsáveis técnicos, corpo clínico, colaboradores, terceiros, fornecedores e parceiros que participem de processos, projetos, contratos, serviços ou decisões capazes de gerar exposição ao HMP.

Todas as unidades, departamentos e setores deverão manter seus riscos atualizados na ferramenta institucional, respeitando a metodologia única aqui estabelecida. A aplicação independe do vínculo formal e alcança atividades assistenciais, administrativas, financeiras, operacionais, tecnológicas, regulatórias e estratégicas.

3. Referências e fundamentos

O modelo do HMP adota como referência principal o COSO Enterprise Risk Management – Integrating with Strategy and Performance, observando critérios e parâmetros de toda

a sua cadeia evolutiva, desde 2004, com publicação da sua última versão em 2017 pelo Committee of Sponsoring Organizations of the Treadway Commission – COSO. O framework integra o gerenciamento de riscos à estratégia, à definição de objetivos e ao desempenho organizacional.

A Política também se harmoniza com princípios de controle interno, integridade, segurança do paciente, governança, proteção de dados, continuidade de negócios e demais normas legais, regulatórias e contratuais aplicáveis ao HMP.

- COSO Enterprise Risk Management – Integrating with Strategy and Performance (2017).
- COSO Internal Control – Integrated Framework (2004) e (2013), no que se refere ao desenho, execução e avaliação dos controles internos.
- Legislação sanitária, trabalhista, ambiental, anticorrupção, proteção de dados, prestação de contas e normas do contrato de gestão, quando aplicáveis.
- Protocolos de segurança do paciente, políticas institucionais, regimentos, manuais e procedimentos operacionais do HMP.

4. Conceitos essenciais

Risco: efeito da incerteza sobre os objetivos, podendo representar ameaça, perda, desvio de resultado ou oportunidade que exija decisão institucional.

Evento de risco: ocorrência ou conjunto de circunstâncias que pode afetar objetivos, processos, pacientes, trabalhadores, recursos, informações ou a reputação do HMP.

Causa: condição, fragilidade ou fator que favorece a ocorrência do evento de risco.

Consequência: resultado possível do evento, incluindo danos assistenciais, operacionais, financeiros, legais, reputacionais, ambientais ou humanos.

Risco inerente: exposição existente antes da consideração dos controles atualmente implantados.

Controle: ação, regra, barreira, sistema, conferência ou mecanismo destinado a prevenir, detectar, reduzir ou corrigir o risco.

Risco residual ou nível final: exposição que permanece após a consideração do desenho e do funcionamento dos controles existentes.

Proprietário do risco: gestor com autoridade e responsabilidade para acompanhar o risco, decidir sobre sua resposta e assegurar a execução do plano de ação.

Responsável pelo controle: pessoa ou área incumbida de executar e evidenciar o controle.

Apetite a risco: nível e tipo de risco que o HMP aceita assumir na busca de seus objetivos.

5. Diretrizes do gerenciamento de riscos

O gerenciamento de riscos deve estar integrado ao planejamento, à execução, ao monitoramento dos indicadores e à avaliação do desempenho. A análise de riscos não será atividade isolada ou meramente documental, mas parte dos processos de decisão e de prestação de contas.

Em alinhamento ao COSO ERM, o HMP organizará sua atuação em cinco componentes inter-relacionados:

- Governança e cultura: definição de responsabilidades, exemplo da liderança, valores éticos, competências e supervisão.
- Estratégia e definição de objetivos: análise do contexto, do apetite a risco e dos riscos associados às escolhas estratégicas.
- Desempenho: identificação, avaliação, priorização e resposta aos riscos que afetam objetivos e resultados.
- Revisão e aprimoramento: avaliação de mudanças, desempenho do gerenciamento de riscos e necessidade de ajustes.
- Informação, comunicação e reporte: produção de dados confiáveis, comunicação tempestiva e relatórios adequados aos níveis decisórios.

Devem ser observados os princípios da proporcionalidade, prevenção, rastreabilidade, responsabilidade, segregação de funções, transparência, melhoria contínua e uso de evidências.

6. Estrutura de governança e responsabilidades

6.1 Alta Administração e Conselhos

- Aprovar esta e demais políticas institucionais, o apetite a risco e os limites de tolerância.
- Supervisionar os riscos estratégicos, críticos e aqueles que ultrapassem a tolerância institucional.
- Assegurar estrutura, recursos e autoridade para o funcionamento do processo de gestão de riscos.
- Deliberar sobre riscos que possam comprometer a continuidade assistencial, a segurança do paciente, a integridade ou a sustentabilidade do HMP.

6.2 Instância de Integridade, Riscos ou Compliance

- Coordenar a metodologia, manter a planilha e o cadastro institucional de riscos.
- Orientar gestores, consolidar informações e emitir relatórios gerenciais.
- Verificar a consistência das avaliações, monitorar planos de ação e propor melhorias.
- Comunicar exposições relevantes e atrasos críticos à Alta Administração.

6.3 Gestores setoriais e proprietários de riscos

- Identificar e manter atualizados os riscos de seus processos.
- Avaliar probabilidade, impacto, controles e risco residual com base em evidências.
- Definir resposta, responsável, prazo, indicador e evidência dos planos de ação.
- Comunicar alterações relevantes, incidentes, falhas de controle e riscos emergentes.

6.4 Responsáveis pelos controles

- Executar os controles na frequência prevista e conservar evidências verificáveis.
- Comunicar falhas, indisponibilidades, exceções ou descumprimentos.

6.5 Auditoria Interna ou função equivalente

- Avaliar de forma independente a governança, a metodologia, a eficácia dos controles e a confiabilidade das informações de riscos.
- Não assumir a propriedade dos riscos nem a execução rotineira dos controles que posteriormente serão auditados.

6.6 Todos os profissionais

- Cumprir controles, comunicar riscos e colaborar com avaliações, treinamentos e planos de ação.

7. Categorias e níveis de decisão

Os riscos deverão ser classificados de modo a facilitar a análise consolidada, a atribuição de responsabilidades e o reporte. Devem se basear na metodologia COSO ERM II e variações, sendo subdividida na forma expressa a seguir:

FIXAÇÃO DE OBJETIVOS - COSO II ERM	
ESTRATÉGICOS	Metas em níveis elevados e alinhadas com a missão
OPERACIONAIS	Utilização eficaz e eficiente dos recursos
COMUNICAÇÃO	Confiabilidade de informações e relatórios
CONFORMIDADE	Cumprimento de leis e regulamentos aplicáveis

8. Apetite, tolerância e limites de exposição

O apetite a risco orienta as decisões de aceitação, tratamento e escalonamento. Enquanto não houver declaração específica aprovada para cada objetivo estratégico, serão aplicadas as diretrizes mínimas desta Política.

- Apetite inexistente ou mínimo: morte ou dano grave evitável ao paciente, corrupção, fraude, suborno, violação intencional de lei, assédio, retaliação, desvio de recursos, falsificação, vazamento grave de dados e riscos capazes de interromper serviços essenciais.

- Apetite baixo: riscos regulatórios, ocupacionais, ambientais, de privacidade, continuidade e qualidade assistencial. A aceitação exige controles robustos e monitoramento frequente.
- Apetite moderado e controlado: inovação, transformação digital, revisão de processos e iniciativas estratégicas que possuam benefício demonstrável, responsável definido, controles proporcionais e aprovação competente.

Nenhum gestor poderá aceitar individualmente risco classificado como crítico. Riscos altos somente poderão ser tolerados temporariamente quando houver justificativa formal, plano de ação aprovado e monitoramento pela instância competente.

9. Processo institucional de gestão de riscos

O ciclo de gestão de riscos será contínuo e compreenderá: contextualização; identificação; análise do risco inerente; identificação e avaliação dos controles; determinação do risco residual; priorização; definição da resposta; elaboração do plano de ação; monitoramento; comunicação; revisão e encerramento.

O processo deverá ser realizado sempre que houver criação ou alteração relevante de processo, implantação de serviço, mudança normativa, contratação crítica, projeto estratégico, incidente grave, resultado de auditoria, falha de controle, mudança tecnológica ou alteração significativa no contexto interno ou externo.

A revisão dos riscos avaliados e do processo de monitoramento deverá ser realizado anualmente. Contudo, a avaliação deverá ser realizada continuamente conforme a necessidade de monitoramento e execução de planos de ação.

10. Identificação e descrição dos riscos

A identificação deverá partir dos objetivos do processo e considerar fatores internos e externos, incidentes anteriores, reclamações, auditorias, indicadores, notificações, mudanças regulatórias, dependências críticas, vulnerabilidades e expectativas das partes interessadas.

A redação deverá ser clara e estruturada, preferencialmente no formato causa–evento–consequência: “Devido a [causa], pode ocorrer [evento], resultando em [consequência]”. Não deverão ser registrados como risco apenas a ausência de controle, o problema já ocorrido sem incerteza ou formulações genéricas que impeçam avaliação objetiva.

Na planilha oficial, os campos Risco Principal, Descrição do Risco e Riscos Inerentes deverão ser preenchidos de forma complementar. “Risco Principal” será uma síntese; “Descrição” apresentará causa, evento e consequência; e “Riscos Inerentes” registrará fatores de exposição existentes antes dos controles.

11. Avaliação da probabilidade

A probabilidade representa a possibilidade de ocorrência do evento no horizonte considerado. A avaliação deverá utilizar histórico, frequência, volume de operações, mudanças previstas, exposição e opinião técnica fundamentada, utilizando a escala qualitativa de 1 a 5.

	PONTUAÇÃO	DESCRITOR	DESCRIÇÃO
PROBABILIDADE	5	Quase certo	Evento repetitivo e constante.
	4	Provável	Evento usual, com história de ocorrência amplamente conhecido.
	3	Possível	Evento esperado, de frequência reduzida, e com histórico de ocorrência parcialmente conhecido.
	2	Improvável	Evento casual e inesperado, sem histórico de ocorrência.
	1	Rara	Evento extraordinário, sem histórico de ocorrência.

Os parâmetros de frequência são orientadores e deverão ser ajustados ao volume e à natureza do processo.

12. Avaliação do impacto

O impacto representa a gravidade das consequências caso o evento ocorra. Assim como realizado com a escala de probabilidade, entende-se, também, esta avaliação sob duas óticas, a primeira tratando do impacto de eventos já ocorridos, baseando-se em histórico real, e a segunda ótica se tratando do impacto estimativo que poderá ser obtido se o risco se concretizar, neste caso, quando não houver histórico anterior.

IMPACTO	TIPO	CLASSIFICAÇÃO
	5	CATASTRÓFICO
	4	GRANDE
	3	MODERADO
	2	PEQUENO
	1	INSIGNIFICANTE

13. Cálculo e classificação do risco inerente

O nível de risco inerente será calculado pela multiplicação da Probabilidade pelo Impacto: NRi = P × I. A planilha institucional deverá manter fórmula automática no campo NÍVEL DE RISCO e bloquear a substituição manual do resultado, salvo autorização da área gestora da metodologia.

Pontuação	Nível	Cor	Diretriz de resposta	Plano de ação
<= 7	Baixo	Verde	Pode ser aceito com controles de rotina e monitoramento periódico.	Conforme decisão do gestor.
8 a 13	Moderado	Amarelo	Tolerar somente com controles definidos e avaliação de melhoria.	Obrigatório quando houver fragilidade de controle.
14 a 19	Alto	Laranja	Reduzir, compartilhar, evitar ou justificar tolerância temporária.	Obrigatório.
>= 20	Crítico	Vermelho	Ação imediata, escalonamento e decisão da Alta Administração.	Obrigatório e prioritário.

A classificação representa prioridade relativa. Riscos com impacto 5 nas dimensões de segurança do paciente, integridade, legalidade ou continuidade poderão ser escalados ao nível superior, ainda que a multiplicação resulte em faixa inferior.

14. Identificação e avaliação dos controles

Cada controle deve possuir descrição objetiva, responsável, frequência, evidência, natureza e finalidade. Não serão considerados controles afirmações genéricas como “equipe treinada”, “gestão acompanha” ou “processo é conferido” sem definição de como, por quem, quando e com qual evidência.

Os controles poderão ser preventivos, detectivos ou corretivos; manuais, automatizados ou híbridos; e deverão ser avaliados quanto ao desenho e à efetividade operacional.

15. Determinação do risco residual ou nível final

O risco residual corresponde à exposição remanescente após considerar os controles em funcionamento. Se necessário, o proprietário do risco deverá reavaliar, separadamente, a probabilidade e o impacto residuais, justificando como os controles reduzem a chance de ocorrência e/ou a gravidade das consequências, em documento escrito a parte. Uma métrica aceitável para definição de risco residual será a redução pela metade no nível final de risco obtido na avaliação, contando com o fato de que, em casos de riscos altos ou críticos, poderão ser reduzidos desta forma mediante a correta execução dos plano de ação.

A pontuação residual não poderá ser inferior àquela sustentada pelas evidências dos controles. Controles ineficazes ou sem comprovação não produzirão redução na avaliação que deverá ser realizada pela área responsável pela Integridade.

16. Respostas aos riscos e planos de ação

A resposta deverá ser compatível com a natureza, prioridade e custo-benefício do risco, podendo ser:

- Evitar: interromper, não iniciar ou redesenhar a atividade que gera exposição incompatível.
- Reduzir: implementar ou fortalecer controles para diminuir probabilidade e/ou impacto.
- Compartilhar ou transferir: distribuir parte da exposição por contrato, seguro, parceria ou outro mecanismo, sem transferir a responsabilidade institucional.
- Aceitar: manter a exposição dentro do apetite, com controles e monitoramento definidos.
- Explorar: adotar medida para ampliar oportunidade positiva, quando compatível com a estratégia e os limites institucionais.

Todo plano de ação deverá conter, no mínimo: ação específica; responsável nominal ou funcional; prazo; recursos necessários; indicador ou critério de conclusão; evidência; status; percentual de execução; risco residual esperado e data de reavaliação. Prazos vencidos deverão ser justificados e submetidos à instância superior.

17. Monitoramento, comunicação e reporte

O monitoramento deverá verificar a evolução da exposição, a execução dos controles, o cumprimento dos planos de ação, a alteração do contexto e a ocorrência de incidentes. O proprietário do risco manterá a planilha atualizada e comunicará imediatamente qualquer aumento relevante.

Nível residual	Revisão mínima	Reporte	Ação diante de aumento	Responsável pela supervisão
Baixo	Semestral	Relatório setorial	Atualizar avaliação e controles	Gestor do setor
Moderado	Trimestral	Gestão local/área de riscos	Reavaliar plano e tolerância	Gestor e área de riscos
Alto	Mensal	Diretoria/Alta Gestão	Ação corretiva e escalonamento	Diretoria responsável
Crítico	Contínuo e, no mínimo, mensal	Alta Administração e conselho competente	Resposta imediata, contingência e decisão formal	Alta Administração

Devem ser definidos indicadores-chave de risco sempre que possível. O relatório anual/consolidado de riscos deverá apresentar riscos por categoria e unidade, evolução da exposição, controles frágeis, planos vencidos ou ineficientes, incidentes, riscos emergentes e decisões pendentes.

A comunicação deverá respeitar necessidade, tempestividade, sigilo e nível de decisão. Riscos com potencial de dano grave, fraude, corrupção, interrupção assistencial, vazamento de dados ou descumprimento legal relevante não deverão aguardar o ciclo periódico de reporte.

18. Uso obrigatório da planilha institucional

A planilha oficial de Identificação e Monitoramento de Riscos será o instrumento padrão para registro, consolidação e acompanhamento, até que seja substituída por sistema institucional formalmente aprovado.

Deverá ser preenchida pelos gestores responsáveis e conter, obrigatoriamente, a unidade, departamento, setor, período, nível de decisão, fixação de objetivo, risco principal, descrição, fatores inerentes, controles existentes, probabilidade, impacto, nível de risco, posição em relação ao apetite e necessidade de plano de ação.

A metodologia atualmente aplicada na planilha, na qual o NÍVEL DE RISCO decorre da multiplicação da Probabilidade pelo Impacto, fica formalmente adotada por esta Política.

É vedada a exclusão de registros, alteração de fórmulas, listas, critérios ou cores sem autorização. As versões deverão ser armazenadas em repositório institucional controlado, com identificação de data, responsável, unidade e histórico de alterações. Informações confidenciais ou pessoais deverão observar as regras de acesso e proteção de dados.

19. Capacitação e cultura de riscos

A gestão de riscos depende de linguagem comum e participação das áreas. O HMP promoverá capacitação inicial e periódica para gestores, proprietários de risco, responsáveis por controles e equipes envolvidas. O conteúdo deverá abranger identificação, descrição, probabilidade, impacto, controles, risco residual, planos de ação, monitoramento e uso correto da planilha.

A comunicação de riscos, incidentes e falhas de controle realizada de boa-fé deverá ser incentivada como instrumento de prevenção e aprendizagem. A metodologia não será utilizada para ocultar problemas, produzir classificações artificialmente baixas ou punir a comunicação responsável.

20. Revisões, atualizações e disposições finais

Esta Política deverá ser revisada, no mínimo, a cada dois anos ou antes desse prazo quando houver alteração relevante no modelo de gestão, no framework de referência, na legislação, nos objetivos estratégicos, na estrutura institucional ou na metodologia da planilha.

A análise dos riscos deverá ser realizada mensalmente pelas áreas responsáveis, de forma contínua e integrada, com o objetivo de identificar alterações no contexto, avaliar a efetividade dos controles existentes, acompanhar os planos de ação e reconhecer riscos novos ou emergentes. A consolidação institucional desse processo ocorrerá a cada 12 (doze) meses, em reunião colegiada com a participação do gestor da área, da área de Integridade e da Alta Gestão, ocasião em que serão avaliados os resultados do ciclo de gerenciamento de riscos e definidas as diretrizes para o período subsequente. A partir dessa análise consolidada, serão estabelecidas as prioridades futuras para tratamento dos riscos, avaliações sobre a efetividade dos planos de ação e, quando aplicável, as necessidades de revisão, atualização ou elaboração de políticas, procedimentos e demais instrumentos do Programa de Integridade, promovendo a melhoria contínua do sistema de governança, riscos e integridade.

Casos omissos e divergências de interpretação serão submetidos à instância responsável pela gestão de riscos e, quando necessário, à Alta Administração. A aceitação formal de riscos não afasta o cumprimento de obrigações legais, técnicas, éticas e contratuais.

A Política entra em vigor após aprovação e divulgação institucional, revogando orientações internas incompatíveis com seus critérios.