

 GESTÃO EM SAÚDE	POLÍTICA INSTITUCIONAL		
	GESTÃO DE RISCOS E CONTROLE INTERNO		
	Setor/Área:	Código:	Versão:
	Presidência	PL-02	03

1. OBJETIVO

Estabelecer diretrizes e fundamentos para o fortalecimento do sistema de controle interno e da gestão de riscos organizacionais, assegurando a integridade institucional, a transparência, a conformidade com as legislações vigentes, os princípios da governança organizacional e os padrões de qualidade preconizados pela Organização Nacional de Acreditação (ONA).

Esta política tem como finalidade garantir que os processos institucionais operem com segurança, legalidade, eficiência e integridade, promovendo a identificação, a análise, a mitigação, o monitoramento e o tratamento dos seguintes tipos de riscos:

- a) **Riscos clínico-assistenciais:** relacionados à segurança do paciente, à prática assistencial e aos desfechos clínicos dos serviços de saúde;
- b) **Riscos não clínicos:** associados à gestão de infraestrutura, equipamentos, recursos humanos, suprimentos, tecnologias da informação e demais recursos de apoio institucional;
- c) **Riscos jurídicos e regulatórios:** decorrentes de descumprimento de normas legais, contratuais, administrativas ou regulatórias aplicáveis à organização;
- d) **Riscos financeiros:** vinculados à sustentabilidade econômica, à integridade contábil, à execução orçamentária e à gestão de recursos públicos ou privados;
- e) **Riscos operacionais:** relacionados à falha de processos internos, sistemas, pessoas ou eventos externos que impactem a entrega de produtos e serviços;
- f) **Riscos de imagem e reputação:** referentes à percepção pública, à confiança social e à credibilidade institucional junto aos stakeholders;
- g) **Riscos estratégicos:** ligados à formulação, à execução ou ao desvio dos objetivos e metas organizacionais;
- h) **Riscos de integridade e corrupção:** envolvendo práticas indevidas, fraudes, subornos, lavagem de dinheiro, conflitos de interesse ou desvios éticos.
- i) **Riscos relacionados a proteção de dados:** Envolvendo situações que podem comprometer a confidencialidade, a integridade ou a disponibilidade de dados pessoais.

Esta Política orienta a atuação preventiva e responsiva das equipes, assegurando um ambiente organizacional proativo, transparente e comprometido com a melhoria contínua, a segurança institucional e a excelência na gestão.

2. APLICAÇÃO

Esta Política compõe o Programa de Integridade da S3 Gestão em Saúde e aplica-se, obrigatoriamente, a todos os integrantes da instituição: dirigentes, colaboradores, terceiros, parceiros, fornecedores, voluntários, estagiários, consultores e demais partes interessadas.

3. BASE LEGAL

Esta Política foi elaborada com fundamento na legislação vigente e nas melhores práticas de

Elaborado por:	Revisado por:	Autorizado por:	Data:	Página
Paula Amorim	NQSP	Dr. Yurgan Targe	15/07/2026	Página 1 de 7

 GESTÃO EM SAÚDE	POLÍTICA INSTITUCIONAL		
	GESTÃO DE RISCOS E CONTROLE INTERNO		
	Setor/Área:	Código:	Versão:
	Presidência	PL-02	03

governança, controle interno e gestão de riscos, considerando o contexto das organizações sociais e dos serviços de saúde. Destacam-se as seguintes normas e diretrizes:

- a) Lei nº 9.637/1998 – Dispõe sobre a qualificação de entidades como organizações sociais e estabelece obrigações quanto à gestão, à transparência e à eficiência na execução dos contratos de gestão.
- b) Lei nº 8.666/1993 e Lei nº 14.133/2021 – Dispõem sobre licitações e contratos da Administração Pública, incluindo aspectos de risco contratual e mecanismos de controle.
- c) Lei nº 8.080/1990 – Lei Orgânica da Saúde, que organiza as ações e serviços do SUS com base nos princípios da integralidade, descentralização, hierarquização e controle social.
- d) Lei nº 12.846/2013 – Lei Anticorrupção, que trata da responsabilização objetiva de pessoas jurídicas por atos lesivos à administração pública.
- e) Decreto nº 11.129/2022 – Regulamenta a Lei Anticorrupção e estabelece critérios de avaliação de programas de integridade e gestão de riscos.
- f) Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD), aplicável ao tratamento de dados sensíveis e pessoais nas atividades institucionais.
- g) Lei nº 9.784/1999 – Regula o processo administrativo no âmbito da Administração Pública Federal, incluindo o dever de motivação, controle e responsabilização.
- h) RDC ANVISA nº 36/2013 – Institui ações para a segurança do paciente em serviços de saúde e obriga a implementação de processos de gestão de riscos.
- i) Portaria GM/MS nº 529/2013 – Institui o Programa Nacional de Segurança do Paciente (PNSP), com foco na prevenção e mitigação de riscos nos ambientes assistenciais.
- j) Portaria GM/MS nº 1.863/2023 – Atualiza diretrizes do PNSP, reforçando a cultura de segurança e exigindo planos de gestão de riscos nos serviços de saúde.
- k) Manual Brasileiro de Acreditação ONA – versão vigente – Documento técnico de referência nacional que estabelece padrões de qualidade e segurança para organizações prestadoras de serviços de saúde, incluindo diretriz específica para gerenciamento de riscos clínicos, não clínicos, jurídicos, reputacionais, estratégicos e financeiros.
- l) ISO 31000:2018 – Gestão de Riscos – Diretrizes;
- m) ISO 37001:2016 – Sistema de Gestão Antissuborno;
- n) ISO 37301:2021 – Sistema de Gestão de Compliance;
- o) Referenciais da Controladoria-Geral da União (CGU) – especialmente o *Guia de Integridade para Organizações Sociais*;
- p) Referenciais do Tribunal de Contas da União (TCU) – com ênfase nos *Modelos de Três Linhas de Defesa, Mapa de Riscos e Boas Práticas em Governança e Gestão de Riscos*.

4. DEFINIÇÕES

Para fins desta Política, adotam-se as seguintes definições:

Elaborado por:	Revisado por:	Autorizado por:	Data:	Página
Paula Amorim	NQSP	Dr. Yurgan Targe	15/07/2026	Página 2 de 7

 GESTÃO EM SAÚDE	POLÍTICA INSTITUCIONAL		
	GESTÃO DE RISCOS E CONTROLE INTERNO		
	Setor/Área:	Código:	Versão:
	Presidência	PL-02	03

- a) **Apetite ao Risco:** grau de exposição ao risco que a alta direção está disposta a aceitar na busca pelos objetivos institucionais.
- b) **Canal de Denúncias:** meio seguro, sigiloso e acessível para o recebimento de relatos de condutas indevidas.
- c) **Colaboradores:** todas as pessoas que, independentemente da relação de trabalho, cargo ou função, estabeleçam vínculo direto de pessoalidade, subordinação e representação dentro da estrutura organizacional da instituição, sejam eles empregados, prestadores de serviços ou voluntários, trabalhando dentro ou fora das suas dependências, e nos locais onde há atuação da instituição.
- d) **Comitê de Ética:** instância institucional de apoio, deliberação e investigação de inconformidades e riscos.
- e) **Compliance:** expressão derivada do verbo inglês “to comply”, que significa agir com integridade e estar em conformidade, cumprindo e fazendo cumprir leis, decretos, normativos, regulamentos e instruções aplicáveis às operações e atividades da instituição, que, na hipótese de não cumprimento (não conformidade), podem gerar sanções, perda financeira e/ou danos à reputação e à imagem institucional.
- f) **Controle Interno:** Conjunto de políticas, normas, procedimentos, atividades e mecanismos estabelecidos para fornecer segurança razoável quanto à eficácia e eficiência das operações, confiabilidade das informações, proteção dos ativos, conformidade com leis e regulamentos e mitigação dos riscos.
- g) **Due Diligence:** procedimento metódico de diligência prévia, que tem por objetivo a análise de informações e documentos visando conhecer a pessoa física ou a pessoa jurídica e seus administradores com a qual a instituição se relaciona ou pretende se relacionar.
- h) **Gerenciamento de Riscos:** Processo contínuo e estruturado de identificar, avaliar, priorizar, responder, monitorar e comunicar riscos, proporcionando maior segurança para a tomada de decisões e aumentando a probabilidade de alcance dos objetivos institucionais.
- i) **Integrantes:** todos os associados, inclusive aqueles eleitos para os cargos do Conselho de Administração, do Conselho Fiscal, da Diretoria Executiva, ou órgãos da estrutura organizacional, que participem e representem a S3 Gestão em Saúde dentro ou fora das suas dependências, e nos locais onde há atuação da instituição.
- j) **Mapa de Riscos:** representação visual dos riscos identificados e sua classificação quanto à probabilidade e impacto.
- k) **Matriz de Riscos:** instrumento que cruza a probabilidade de ocorrência de um risco com o impacto causado, permitindo priorização.
- l) **Programa de Integridade (Compliance):** conjunto de instrumentos, processos, controles e procedimentos internos que garantem que a instituição esteja aderente ao arcabouço legal, à regulamentação infralegal, às recomendações dos órgãos reguladores e financiadores de projetos, aos procedimentos operacionais e políticas internas, ao Código de Conduta Ética da instituição, e aos demais instrumentos normativos aplicáveis.

Elaborado por:	Revisado por:	Autorizado por:	Data:	Página
Paula Amorim	NQSP	Dr. Yurgan Targe	15/07/2026	Página 3 de 7

 GESTÃO EM SAÚDE	POLÍTICA INSTITUCIONAL		
	GESTÃO DE RISCOS E CONTROLE INTERNO		
	Setor/Área:	Código:	Versão:
	Presidência	PL-02	03

- m) **Risco:** possibilidade de ocorrência de eventos que possam impactar negativa ou positivamente os objetivos da instituição.
- n) **Risco Residual:** Nível de risco remanescente após a implementação dos controles e das ações de tratamento.
- o) **Risco de Não Conformidade:** possibilidade de a instituição sofrer sanções legais ou administrativas, perdas financeiras, danos de imagem e/ou reputação, bem como outros danos decorrentes de descumprimento ou falhas na observância do arcabouço legal, da regulamentação infralegal, das recomendações dos órgãos reguladores e financiadores de projetos, dos procedimentos operacionais e do Código de Conduta Ética, das políticas institucionais, e dos demais instrumentos normativos aplicáveis;
- p) **Terceiros e Parceiros:** todas as pessoas físicas ou jurídicas que não sejam classificadas como Integrantes ou Colaboradores, mas que mantenham relação profissional ou comercial, ou que realizem operações representando a instituição.

5. DIRETRIZES

As diretrizes desta Política visam garantir que a S3 Gestão em Saúde disponha de uma estrutura sólida, preventiva e proativa de controle interno e gestão de riscos, assegurando a conformidade legal, a sustentabilidade institucional e a segurança nas decisões e processos.

A mensuração, identificação e gerenciamento de perigos/riscos é fundamental para a segurança dos processos, dos pacientes e colaboradores, pois possibilita ações para inibir a potencialidade de danos, assim como definição de conduta das equipes envolvidas. A ferramenta para mapeamento de riscos utilizada pela S3, é baseada na metodologia Análise de Modos de Falhas e Efeitos (FMEA) adaptada à necessidade organizacional. É um método utilizado para prevenir falhas e analisar os riscos de um processo, através da identificação de causas e efeitos para identificar as ações que são utilizadas para eliminar ou diminuir as falhas.

É recomendado que o processo de mapeamento de riscos seja realizado utilizando o formulário FOR-INS-NQSP-006.

5.1 Compromisso da Alta Direção (Diretoria Executiva)

A alta liderança deve atuar como exemplo de conduta ética e promover, de forma ativa, a cultura de integridade, governança e responsabilidade na organização, garantindo os recursos necessários à implementação das práticas de controle interno e gestão de riscos.

5.2 A Estratégia do Controle Interno e da Gestão de Riscos

A gestão de riscos deve estar integrada à estratégia, à governança e aos processos de gestão da organização, sendo considerada um elemento essencial para apoiar a tomada de decisões e contribuir para o alcance dos objetivos institucionais. O gerenciamento de riscos deve ocorrer de forma contínua, sistemática e proporcional à natureza, complexidade e criticidade das atividades desenvolvidas.

Elaborado por:	Revisado por:	Autorizado por:	Data:	Página
Paula Amorim	NQSP	Dr. Yurgan Targe	15/07/2026	Página 4 de 7

 GESTÃO EM SAÚDE	POLÍTICA INSTITUCIONAL		
	GESTÃO DE RISCOS E CONTROLE INTERNO		
	Setor/Área:	Código:	Versão:
	Presidência	PL-02	03

5.3 A identificação dos Riscos

De forma permanente, a S3 deve identificar, mapear e atuar para identificar e mitigar os riscos aos quais está exposto. Cada unidade deve realizar mapeamento dos riscos organizacionais, riscos assistenciais e riscos de processos conforme metodologia padronizada. Com uma equipe dedicada e capacitada, somada a procedimentos de controle interno e a um programa de gestão de riscos estruturado, deve direcionar o foco para os resultados esperados, permitindo que a unidade priorize as atividades e otimize a aplicação dos recursos disponíveis, de forma legal e ética, nos seus fins estatutários.

Cada unidade deverá promover a identificação tempestiva dos riscos que possam afetar seus objetivos, considerando fatores internos e externos, bem como mudanças no ambiente regulatório, tecnológico, econômico e operacional. A identificação dos riscos deverá contemplar, sempre que aplicável, aspectos estratégicos, operacionais, financeiros, legais, regulatórios, tecnológicos, reputacionais, ambientais, relacionados à proteção de dados, à continuidade dos negócios e à integridade institucional.

A identificação dos riscos começa com a análise de cenário interno e externo, utilizando a metodologia padronizada da análise de SWOT. Depois disso, riscos operacionais e assistenciais são desdobrados na matriz de risco de cada processo.

5.4 Tratamento dos riscos

O tratamento dos riscos deverá ser realizado por meio da definição e implementação de medidas compatíveis com o nível de exposição identificado e com o apetite ao risco estabelecido pela organização. As estratégias adotadas poderão envolver a mitigação, eliminação, compartilhamento, transferência ou aceitação do risco, desde que fundamentadas em análise técnica e devidamente aprovadas pelas instâncias competentes.

As barreiras de prevenção aos riscos devem ser formalizadas no mapeamento de processos e riscos e revisadas sistematicamente conforme procedimento operacional de cada unidade.

Os controles internos deverão ser concebidos, implementados e mantidos de forma a reduzir a exposição aos riscos, assegurando a confiabilidade das informações, a eficiência e eficácia dos processos, a proteção dos ativos, a conformidade com os requisitos legais e regulatórios e a continuidade das operações. Os controles deverão ser periodicamente avaliados quanto à sua efetividade, sendo revisados sempre que identificadas deficiências, alterações nos processos ou mudanças no contexto organizacional.

5.5 Comunicação, Treinamento e Conscientização

O sucesso de um Programa de Integridade e do Gerenciamento de Riscos depende da comunicação, disseminação e promoção das regras e expectativas de conduta da instituição aos seus públicos. A comunicação e o treinamento são os meios mais eficazes e eficientes para que a instituição possa capacitar e sensibilizar seus públicos quanto às suas prerrogativas e responsabilidades, fortalecendo o conceito da cultura organizacional ética.

Todos os públicos envolvidos devem ser periodicamente capacitados quanto aos princípios, práticas e responsabilidades da gestão de riscos e controle interno, com ações de comunicação, treinamentos técnicos e campanhas educativas.

Elaborado por:	Revisado por:	Autorizado por:	Data:	Página
Paula Amorim	NQSP	Dr. Yurgan Targe	15/07/2026	Página 5 de 7

 GEST3O EM SAUDE	POLÍTICA INSTITUCIONAL		
	GESTÃO DE RISCOS E CONTROLE INTERNO		
	Setor/Área:	Código:	Versão:
	Presidência	PL-02	03

5.6 Monitoramento e Aprimoramento Contínuo

O monitoramento e a prevenção configuram ações contínuas por meio do qual a S3 Gestão em Saúde avalia se suas atividades se encontram em conformidade com os regulamentos e as regras internas e externas aplicáveis. O monitoramento tem por finalidade verificar a necessidade de melhoria dos processos estabelecidos, buscando a prevenção de ocorrências e de apuração de riscos, através da aplicação de procedimentos como o *due diligence*, a revisão de controles internos, os testes periódicos e as auditorias internas.

Os controles e os riscos devem ser monitorados regularmente por meio de indicadores, auditorias, revisões internas e relatórios gerenciais. As falhas identificadas devem ser objeto de planos de ação corretiva e revisão das práticas existentes.

5.7 Responsabilidade Compartilhada

A gestão de riscos é uma responsabilidade institucional compartilhada entre todos os níveis hierárquicos. Espera-se de todos os colaboradores comportamento ético, atenção aos riscos e engajamento no aprimoramento contínuo da gestão.

6 INVESTIGAÇÕES E SANÇÕES APLICÁVEIS

O processo de investigações e sanções aplicáveis à Ouvidoria e ao Canal de Denúncias deve ser conduzido pelo Comitê de Ética da instituição, de maneira transparente, imparcial e rigorosa, garantindo a integridade do procedimento e a proteção dos direitos de todas as partes envolvidas.

As suspeitas de violação desta Política, bem como os incidentes informados, serão investigadas imediatamente e de forma apropriada pelo Comitê de Ética. Se após as investigações ficar comprovada a ocorrência de conduta indevida, ilegal ou antiética, serão tomadas medidas corretivas imediatas e exemplares, sempre de acordo com as circunstâncias, a gravidade e a legislação aplicável.

Qualquer integrante, colaborador, terceiro ou parceiro que viole disposições desta Política estará sujeito às sanções disciplinares previstas no Código de Conduta Ética da S3 Gestão em Saúde, listadas abaixo:

- Advertência verbal;
- Advertência por escrito;
- Suspensão;
- Demissão sem justa causa;
- Demissão por justa causa;
- Exclusão do fornecedor, parceiro ou agente intermediário da instituição;
- Ação judicial cabível;
- Medidas corretivas (treinamentos, revisão de políticas, melhorias nos processos).

Elaborado por:	Revisado por:	Autorizado por:	Data:	Página
Paula Amorim	NQSP	Dr. Yurgan Targe	15/07/2026	Página 6 de 7

 GESTÃO EM SAÚDE	POLÍTICA INSTITUCIONAL		
	GESTÃO DE RISCOS E CONTROLE INTERNO		
	Setor/Área:	Código:	Versão:
	Presidência	PL-02	03

7 RESPONSABILIDADES

Cabe aos dirigentes da S3 Gestão em Saúde cumprir e fazer cumprir com todas as disposições desta Política, e assegurar que todos os integrantes, colaboradores, terceiros e parceiros de seu relacionamento sejam informados sobre seu conteúdo e a importância de sua implementação.

A adesão é obrigatória para todos os envolvidos, e suas regras e diretrizes devem ser colocadas em prática de imediato.

8 COMUNICAÇÃO

A S3 Gestão em Saúde incentiva a todos que comuniquem imediatamente ao Comitê de Ética quando suspeitarem ou detectarem violações a esta Política ou as legislações correlatas, cuja análise e investigação serão tratadas confidencialmente. Não serão admitidas retaliações e intimidações aos denunciantes.

9 HISTÓRICO DE REVISÃO

VERSÃO	DATA	DESCRIÇÃO DAS ALTERAÇÕES	RESPONSÁVEL
1	04/11/2012	Criação do Documento	Nailton Cazumbá
2	16/06/2025	Atualização do documento com ajustes textuais	Paula Amorim
3	15/07/2026	Revisão do documento para aumentar o foco na Gestão de riscos, evitando conflito com a PL01.	Paula Amorim

Elaborado por:	Revisado por:	Autorizado por:	Data:	Página
Paula Amorim	NQSP	Dr. Yurgan Targe	15/07/2026	Página 7 de 7