

LOGOTIPO ÓRGÃO	NOME DO ÓRGÃO			
	PROCEDIMENTO OPERACIONAL PADRÃO			
	Número: XXXXXXX	Revisão: XX	Folha: 1/10	Vigência: XX/XX/XXXX
Título: Gestão de Riscos				
Elaborador: XXXXXXXXXXXX		Aprovador: XXXXXXXXXXXX		

1. INTRODUÇÃO

A Gestão de Riscos é um processo contínuo destinado a identificar, analisar, avaliar, tratar e monitorar eventos que possam comprometer o alcance dos objetivos da Vigilância Sanitária (Visa) e a eficácia do Sistema de Gestão da Qualidade (SGQ).

No âmbito do SGQ, a gestão de riscos pode abranger quatro dimensões complementares:

- **Riscos estratégicos** – relacionados aos objetivos institucionais e à missão da Visa;
- **Riscos de processos** – associados ao desempenho dos processos incluídos no escopo do SGQ;
- **Riscos operacionais** – relacionados à execução das atividades e rotinas;
- **Riscos organizacionais** – relacionados à estrutura, governança, recursos, conformidade e integridade institucional.

O objetivo é reduzir incertezas, apoiar decisões e aumentar a confiabilidade dos resultados institucionais.

2. OBJETIVO

Estabelecer diretrizes mínimas para a gestão de riscos estratégicos, de processos, operacionais e organizacionais no âmbito do SGQ da Visa.

3. ABRANGÊNCIA

Este procedimento se aplica às atividades, processos e serviços desenvolvidos pelo(a)... *Nome do Órgão*, incluídos no escopo do SGQ.

4. REFERÊNCIAS

- ABNT- Associação Brasileira de Normas Técnicas. NBR ISO 9000:2015 - Sistema de Gestão da Qualidade: Fundamentos e Vocabulário. Rio de Janeiro, ABNT, 2015.

LOGOTIPO ÓRGÃO	NOME DO ÓRGÃO			
	PROCEDIMENTO OPERACIONAL PADRÃO			
	Número: XXXXXXX	Revisão: XX	Folha: 2/10	Vigência: XX/XX/XXXX
Título: Gestão de Riscos				
Elaborador: XXXXXXXXXXXX		Aprovador: XXXXXXXXXXXX		

- ABNT- Associação Brasileira de Normas Técnicas. NBR ISO 9001:2015 - Sistemas de gestão da qualidade — Requisitos. Rio de Janeiro, ABNT, 2015.
- Guia para Implementação de Sistema de Gestão da Qualidade no Sistema Nacional de Vigilância Sanitária – 2ª edição. Disponível em <https://www.gov.br/anvisa/pt-br/centraisdeconteudo/publicacoes/sistema-nacional-de-vigilancia-sanitaria/publicacoes-de-projetos/guia-para-implantacao-de-sistema-de-gestao-da-qualidade-sgg-em-unidades-do-sistema-nacional-de-vigilancia-sanitaria-snvs-1/view>. Acesso em 26/12/2025.
- *WHO Global Benchmarking Tool (GBT) for evaluation of national regulatory system of medical products: manual for benchmarking and formulation of institutional development plans*. Geneva: World Health Organization; 2023. Licence: CC BY-NC-SA 3.0 IGO. Disponível em <https://iris.who.int/server/api/core/bitstreams/91701fd2-2b3c-46f7-aa56-04a9e69537bb/content>. Acesso em 26/12/2025.
- *WHO Guideline on the Implementation of Quality Management Systems for National Regulatory Authorities - WHO Technical Report Series*, Nº. 1025, 2020. Disponível em: https://www.who.int/docs/default-source/medicines/norms-and-standards/guidelines/trs1025/trs1025-annex13.pdf?sfvrsn=8e6a17ee_2. Acesso em 26/12/2025.

5. DEFINIÇÕES

Para melhor entendimento deste procedimento, aplicam-se as seguintes definições:

- **Causa:** fator que pode gerar o evento de risco;
- **Consequência:** impacto caso o risco se concretize;
- **Controle:** ação preventiva ou corretiva adotada para reduzir o risco;
- **Evento de risco:** situação que pode impedir ou dificultar o alcance do resultado esperado;
- **Nível de risco inerente (NRI):** nível de risco antes da aplicação de controles;
- **Nível de risco residual (NRR):** nível de risco após a implementação de controles;

LOGOTIPO ÓRGÃO	NOME DO ÓRGÃO			
	PROCEDIMENTO OPERACIONAL PADRÃO			
	Número: XXXXXXX	Revisão: XX	Folha: 3/10	Vigência: XX/XX/XXXX
Título: Gestão de Riscos				
Elaborador: XXXXXXXXXXXX		Aprovador: XXXXXXXXXXXX		

- **Risco:** possibilidade de ocorrência de evento que pode impactar negativamente o alcance de objetivos institucionais, de processos ou organizacionais;
- **Riscos de Processos:** relacionados ao desempenho dos processos finalísticos, gerenciais e de apoio incluídos no escopo do SGQ. Exemplos: falha na execução de inspeções; inconsistência em análises técnicas; não cumprimento de prazos regulatórios;
- **Riscos estratégicos:** relacionados ao cumprimento da missão institucional, metas estratégicas, políticas públicas e posicionamento institucional. Exemplos: não cumprimento de metas estratégicas; mudanças regulatórias com alto impacto; perda de credibilidade institucional;
- **Riscos Operacionais:** relacionados à execução diária das atividades e rotinas de trabalho. Exemplos: erros humanos; falhas em sistemas; interrupção de serviços;
- **Riscos Organizacionais:** relacionados à estrutura institucional, recursos, governança e conformidade. Exemplos: insuficiência de pessoal; problemas orçamentários; fragilidades de governança; não conformidade legal.

6. SIGLAS E ABREVIATURAS

- FA: Fator de Avaliação (dos controles);
- NRI: Nível de Risco Inerente;
- NRR: Nível de Risco Residual;
- POP: Procedimento Operacional Padrão;
- SGQ: Sistema de Gestão da Qualidade;
- SNVS: Sistema Nacional de Vigilância Sanitária;
- Visa: Vigilância Sanitária.

7. RESPONSABILIDADES

A Alta Direção da Visa é responsável por aprovar este procedimento, definir diretrizes institucionais para gestão de riscos, deliberar sobre riscos classificados como altos ou

LOGOTIPO ÓRGÃO	NOME DO ÓRGÃO			
	PROCEDIMENTO OPERACIONAL PADRÃO			
	Número: XXXXXXX	Revisão: XX	Folha: 4/10	Vigência: XX/XX/XXXX
Título: Gestão de Riscos				
Elaborador: XXXXXXXXXXXX		Aprovador: XXXXXXXXXXXX		

críticos e acompanhar os principais riscos estratégicos nas reuniões de análise crítica. O responsável pelo SGQ deve orientar a aplicação da metodologia, consolidar e monitorar as análises de riscos, assegurar a manutenção dos registros como informação documentada e reportar à Alta Direção situações relevantes. Os gestores de processos e das unidades organizacionais são responsáveis por identificar, avaliar e tratar os riscos sob sua responsabilidade, implementar os controles definidos, manter os registros atualizados e comunicar alterações significativas. Os servidores devem colaborar na identificação de riscos e cumprir os controles estabelecidos.

8. PRINCIPAIS PASSOS

As etapas abaixo descrevem requisitos mínimos e podem ser aplicadas pela Visa a qualquer categoria de risco (estratégico, de processo, operacional ou organizacional).

8.1 Definição do Objeto de Análise

Antes de iniciar a avaliação de riscos, deve-se definir claramente o que está sendo analisado, que pode ser, dentre outros, um objetivo estratégico, um processo do SGQ, uma atividade específica ou uma área ou Unidade Organizacional.

Nesta etapa, deve-se identificar:

- O nome do processo, objetivo ou área analisada;
- Seu objetivo principal (resultado esperado);
- O responsável pela análise;
- A data da avaliação.

Essa definição é essencial para garantir que os riscos sejam avaliados em relação a um resultado claro e específico. As informações devem ser registradas na aba Objeto de análise do Anexo IV-A – “Formulário de Gerenciamento de Riscos”.

8.2 Identificação dos Riscos

A identificação dos riscos na Visa deve ser conduzida nos seguintes contextos:

LOGOTIPO ÓRGÃO	NOME DO ÓRGÃO			
	PROCEDIMENTO OPERACIONAL PADRÃO			
	Número: XXXXXXX	Revisão: XX	Folha: 5/10	Vigência: XX/XX/XXXX
Título: Gestão de Riscos				
Elaborador: XXXXXXXXXXXX		Aprovador: XXXXXXXXXXXX		

- durante o mapeamento de novos processos;
- periodicamente, como parte das revisões de processos já implementados;
- diante de mudanças significativas no contexto da organização ou em requisitos legais e normativos;
- como resultado de não conformidades, auditorias internas ou reuniões de análise crítica.

Para cada risco identificado, devem ser descritos:

- Evento de risco – o que pode acontecer?
- Causas – por que isso pode acontecer?
- Consequências – qual é o impacto caso ocorra?

Para identificação dos riscos relacionados a processos, deve ser considerada a lista de riscos padronizados constante no Anexo IV-B – “Lista padronizada de Eventos de Riscos e Controles”.

Os riscos identificados devem ser registrados na aba de Identificação, Avaliação e Priorização de Riscos, conforme Anexo IV-A.

8.3 Análise do Risco

8.3.1 Avaliar o Risco Inerente

Cada risco identificado deve ser avaliado quanto a sua gravidade. A avaliação deve considerar a probabilidade e o impacto do evento de risco ocorrer, conforme detalhado a seguir:

a) Probabilidade

Qual a chance de o evento ocorrer?

Pode ser classificada, por exemplo, como:

- Improvável (1): Evento improvável sob condições normais e sem histórico de ocorrência;
- Pouco Provável (2): Evento já ocorreu uma vez ou pode ocorrer raramente;

LOGOTIPO ÓRGÃO	NOME DO ÓRGÃO			
	PROCEDIMENTO OPERACIONAL PADRÃO			
	Número: XXXXXXX	Revisão: XX	Folha: 6/10	Vigência: XX/XX/XXXX
Título: Gestão de Riscos				
Elaborador: XXXXXXXXXXXX		Aprovador: XXXXXXXXXXXX		

- Provável (3): Evento já ocorreu algumas vezes e pode voltar a ocorrer;
- Muito provável (4): Evento já ocorreu repetidas vezes e provavelmente voltará a ocorrer muitas vezes.

b) Impacto

Caso o risco ocorra, qual será o efeito sobre o objeto analisado?

- Baixo (1): Consequências insignificantes caso o evento ocorra;
- Moderado (2): Consequências menores, afetando atividades, processos ou aspectos secundários;
- Alto (3): Consequências relevantes em atividades, processos ou aspectos secundários ou menores em processos e atividades prioritários;
- Muito Alto (4): Consequências relevantes em processos, atividades ou aspectos prioritários.

A partir da avaliação da probabilidade e impacto, é possível definir o nível de risco inerente (NRI), ou seja, o risco intrínseco ao objeto de análise, sem considerar eventuais controles já implementados pela Visa, conforme matriz a seguir:

MATRIZ DE RISCO					
IMPACTO	Muito Alto (4)	Moderado (4)	Alto (8)	Inaceitável (12)	Inaceitável (16)
	Alto (3)	Baixo (3)	Moderado (6)	Alto (9)	Inaceitável (12)
	Moderado (2)	Baixo (2)	Moderado (4)	Moderado (6)	Alto (8)
	Baixo (1)	Baixo (1)	Baixo (2)	Baixo (3)	Moderado (4)
		Improvável (1)	Pouco Provável (2)	Provável (3)	Muito Provável (4)
PROBABILIDADE					

A avaliação do impacto e probabilidade dos riscos identificados deve ser registrada na aba de Identificação, Avaliação e Priorização de Riscos, conforme Anexo IV-A.

LOGOTIPO ÓRGÃO	NOME DO ÓRGÃO			
	PROCEDIMENTO OPERACIONAL PADRÃO			
	Número: XXXXXXX	Revisão: XX	Folha: 7/10	Vigência: XX/XX/XXXX
Título: Gestão de Riscos				
Elaborador: XXXXXXXXXXXX		Aprovador: XXXXXXXXXXXX		

8.3.2 Avaliar os Controles e o Risco Residual

Para cada evento de risco registrado, a Visa deve avaliar a efetividade dos controles já implementados, conforme apresentado a seguir:

Avaliação da Efetividade dos Controles Implementados	Condição	Fator de Avaliação (FA)
Inexistente	Controles são inexistentes, mal concebidos ou não funcionais.	1,0
Fraco	Controles são aplicados caso a caso, com alta dependência de pessoas.	0,8
Mediano	Controles mitigam apenas alguns aspectos relevantes do risco.	0,6
Satisfatório	Controles são sustentados por ferramentas adequadas e mitigam o risco de forma adequada.	0,4
Forte	Controles representam a "melhor prática" e mitigam o risco robustamente.	0,2

O Nível de Risco Residual (NRR) é apurado mediante a multiplicação do Fator de Avaliação (FA) dos controles já implementados pelo Nível de Risco Inerente (NRI), conforme a fórmula $NRR = NRI \times FA$. O NRR calculado define a necessidade e a prioridade das ações de tratamento dos riscos na etapa seguinte.

Nível de Risco Residual (NRR)	Pontuação	Ação de Tratamento
Inaceitável	≥ 12	Requer ação prioritária para evitar o risco. Pode envolver a interrupção do processo organizacional.
Alto	≥ 7 a < 12	Requer ação para manejar o risco. Pode envolver mitigação ou transferência.
Moderado	≥ 4 a < 7	A ação é desejável se os recursos estiverem disponíveis.
Aceitável	< 4	Nenhuma ação é necessária.

Nota 1: No cálculo do NRR, deve-se considerar apenas os controles efetivamente implementados.

O resultado da análise e avaliação dos riscos deve ser consolidado na aba de Identificação, Avaliação e Priorização de Riscos, conforme Anexo IV-A.

Essa classificação permite compreender quais riscos são mais relevantes e exigem

LOGOTIPO ÓRGÃO	NOME DO ÓRGÃO			
	PROCEDIMENTO OPERACIONAL PADRÃO			
	Número: XXXXXXX	Revisão: XX	Folha: 8/10	Vigência: XX/XX/XXXX
Título: Gestão de Riscos				
Elaborador: XXXXXXXXXXXX		Aprovador: XXXXXXXXXXXX		

atenção prioritária.

8.4 Priorização

A identificação do nível de risco residual contribui para determinar a gravidade geral de cada evento de risco e sua priorização para direcionar a tomada de decisão.

Nesta etapa, a Visa deve selecionar os eventos de risco que devem ser tratados por meio de novos controles, priorizando aqueles que estiverem com níveis de risco moderado, alto ou inaceitável.

Eventos com nível de risco residual aceitável não requerem implementação de controles adicionais.

8.5 Tratamento dos riscos

A Visa deve definir estratégias para tratar os eventos de risco que foram priorizados a partir da avaliação do risco residual.

O tratamento dos riscos envolve identificar as medidas de resposta ao risco, avaliar a viabilidade da implantação dessas medidas (custo-benefício, viabilidade técnica, tempestividade, efeitos colaterais, etc.) e elaborar plano de tratamento com os controles que serão implementados.

Os controles devem ser realistas, proporcionais ao risco e compatíveis com os recursos disponíveis e podem ser definidos a partir da relação disponível no Anexo IV-B.

Cada controle definido deve conter:

- Descrição clara da ação;
- Responsável;
- Prazo para implementação;
- Evidência que comprove sua execução;
- Situação (planejado, em implementação ou implementado).

Os eventos de risco priorizados, seus controles e respectivas informações devem ser registradas na aba “Tratamento” do Anexo IV-A.

LOGOTIPO ÓRGÃO	NOME DO ÓRGÃO			
	PROCEDIMENTO OPERACIONAL PADRÃO			
	Número: XXXXXXX	Revisão: XX	Folha: 9/10	Vigência: XX/XX/XXXX
Título: Gestão de Riscos				
Elaborador: XXXXXXXXXXXX		Aprovador: XXXXXXXXXXXX		

8.6 Monitoramento e revisão periódica dos riscos

A Visa deve monitorar os controles previstos na etapa de tratamento dos riscos a fim de verificar se os controles foram implementados e se estão funcionando conforme previsto.

O ciclo de gestão de riscos deve ser monitorado continuamente, cabendo à Visa a manutenção, atualização do Formulário de Gerenciamento de Riscos, sempre que necessário, devendo ser revisada minimamente quando:

- a implementação de ações de controle de determinado evento de risco for concluída, atualizando-se a avaliação do nível de risco residual;
- um novo risco for identificado ou um risco existente for encerrado;
- ocorrer qualquer mudança significativa no contexto interno ou externo da organização que altere a probabilidade, o impacto ou a própria existência de um risco;
- uma não conformidade ou ocorrência indicar a falha de um controle existente;
- houver mudança estrutural ou nova meta estratégica na organização.

9. INFORMAÇÃO DOCUMENTADA

A gestão de riscos deve ser formalmente registrada e mantida como informação documentada do Sistema de Gestão da Qualidade.

Os registros devem permitir rastreabilidade, acompanhamento e verificação das análises realizadas e das ações adotadas.

Os Formulários de Gerenciamento de Riscos devem ser mantidos com controle de versão e histórico das alterações realizadas.

10. ANEXOS

Anexo IV-A – Formulário de Gerenciamento de Riscos;

Anexo IV-B – Lista padronizada de Eventos de Riscos e Controles.

LOGOTIPO ÓRGÃO	NOME DO ÓRGÃO			
	PROCEDIMENTO OPERACIONAL PADRÃO			
	Número: XXXXXXX	Revisão: XX	Folha: 10/10	Vigência: XX/XX/XXXX
Título: Gestão de Riscos				
Elaborador: XXXXXXXXXXXX		Aprovador: XXXXXXXXXXXX		

228

229 **11. HISTÓRICO**

Revisão	Item	Alteração
0	N/A	Emissão Inicial