

# POLÍTICA DE GESTÃO DO RISCO ORGANIZACIONAL



Janeiro 2019

DI-038/1

# ÍNDICE

ENQUADRAMENTO .....	2
1. PRINCÍPIOS .....	3
2. ESTRUTURA .....	6
2.1. Liderança e Compromisso .....	7
2.2. Integração .....	7
2.3. Comunicação e consulta .....	8
2.4. Governação e Responsabilidades .....	8
2.5. Implementação .....	10
2.6. Monitorização e Revisão da Estrutura .....	10
3. PROCESSOS .....	11

## ENQUADRAMENTO

A consolidação das melhores práticas de gestão do risco organizacional, alinhadas com o enquadramento da norma ISO 31000:2018, e as orientações da ISO 9001:2015, ISO 17025:2018 e ISO 27001: 2013<sup>1</sup>, sustentou a evolução da abordagem do Infarmed ao risco e a necessidade da elaboração de uma Política de Gestão do Risco Organizacional.

A Política de Gestão do Risco no Infarmed (PGRI) foi aprovado pelo seu Conselho Diretivo, como um documento autónomo, e comunicada de uma forma abrangente às várias partes interessadas, externas e internas.

A PGRI enuncia os Princípios que orientam as características da gestão do risco, comunicando o seu valor e explicando a sua intenção e finalidade. Os princípios constituem a base para a gestão do risco e são chave no estabelecimento da Estrutura da Gestão do Risco e dos Processos da Gestão do Risco do Infarmed.

---

<sup>1</sup> NP ISO 31000:2018 - Gestão do Risco - Linhas de Orientação, IPQ, 2018

NP ISO 9001:2015 – Sistemas de Gestão da Qualidade

NP EN ISO/IEC 17025:2018 - Requisitos gerais de competência para laboratórios de ensaio e calibração

NP ISO/IEC 27001:2013 – Sistemas de Gestão de Segurança da Informação

# 1. PRINCÍPIOS

Os princípios estão alinhados com os enunciados na norma ISO 31000:2018, constituindo a base para a gestão do risco no Infarmed e estabelecendo orientações para a definição da estrutura e dos processos da gestão do risco da organização. Estes princípios permitem ao Infarmed gerir os efeitos da incerteza nos seus objetivos.

Os Princípios da Gestão do Risco no Infarmed são:

- i. **Criação e proteção do valor definido pelas atribuições e missão presentes na sua Lei orgânica.**

A finalidade principal da gestão do risco no Infarmed é melhorar o desempenho da organização, promover e encorajar a inovação e suportar a consecução dos objetivos estratégicos e operacionais que realizarão a sua Visão e Missão, definidos na Lei Orgânica e Instrumentos de Gestão. A gestão do risco servirá também para assegurar que serão considerados atributos e valores mais difíceis de medir como a reputação, cumprimento de exigências legais e regulatórias nacionais e internacionais, bem como os valores da organização, o respeito pelo trabalhador e indivíduo, e ambiente.

- ii. **Integração nos processos organizacionais**

Para evitar que a gestão do risco seja percebida como uma tarefa administrativa adicional, ou vista como um exercício burocrático e irrelevante para a criação de valor, a gestão do risco deverá ser parte integrante de todas as atividades do Infarmed. Assim, a estrutura de gestão do risco deverá ser concretizada integrando as suas componentes no sistema de gestão e de tomada de decisão do Infarmed. O processo de gestão do risco deverá estar integrado nas atividades que geram risco, seja em fase de planeamento, execução ou controlo. Por exemplo, a gestão do risco deve estar incorporada nos processos de planeamento e avaliação estratégica, nos processos de planeamento e avaliação do Ciclo Anual de Gestão (SIADAP, Plano e Relatório de Atividades), e restantes processos de negócio e suporte do sistema de gestão da qualidade.

### iii. Estruturada, abrangente e inclusiva

Uma abordagem estruturada e abrangente da gestão do risco contribui para resultados consistentes e comparáveis. Isto implica que as práticas organizacionais no Infarmed tenham em conta os riscos associados a todas as decisões e a utilizações de critérios de risco consistentes, que sejam simultaneamente relacionados com os objetivos do Infarmed e com o âmbito das suas atividades e funções. Por outro lado, o envolvimento apropriado e oportuno das partes interessadas do Infarmed permite que o seu conhecimento, pontos de vista e perceções sejam considerados. Isto resulta numa gestão do risco mais consciencializada e informada.

### iv. Personalizada e considerando os fatores humanos e culturais

A estrutura e os processos da gestão do risco do Infarmed têm por base o estipulado na ISO 31000:2018, embora personalizados e proporcionados aos contextos externo e interno do Infarmed assim como aos seus objetivos. Os processos de gestão do risco do Infarmed deverão considerar as especificidades em termos de domínios funcionais, técnico-científicos, e o conhecimento e competências específicas dos decisores em cada nível de decisão, deste os dirigentes superiores (Conselho Diretivo e seus assessores), Dirigentes Intermédios e as suas Unidades Orgânicas, etc.

Por outro lado, é fundamental reconhecer que o sucesso da aplicação da gestão do risco no Infarmed está dependente do comportamento humano dos seus dirigentes e trabalhadores bem como da cultura do organismo, que necessitam ser cuidadosamente considerados pois influenciam significativamente todos os aspetos da gestão do risco em cada nível e fase.

### v. Dinâmica e baseada na melhor informação possível.

Os riscos podem surgir, mudar ou desaparecer como resultado das mudanças nos contextos externo e interno do Infarmed. Os processos de gestão do risco devem ter uma ênfase na antecipação, deteção, reconhecimento e resposta a essas mudanças e eventos de um modo apropriado e oportuno. A gestão do risco será suportada por informação histórica e atual, assim como nas expectativas futuras. A gestão do risco terá em consideração as limitações e incertezas associadas à informação e expectativas. A informação deverá ser oportuna, clara e estar disponível às partes interessadas relevantes.

#### vi. Melhoria contínua

A gestão do risco é melhorada continuamente com a aprendizagem e a experiência. O objetivo da melhoria contínua poderá incidir sobre:

- Melhorar o nível da integração da gestão do risco na atividade geral;
- Melhorar a qualidade da apreciação do risco;
- Melhorar a estrutura;
- Melhorar a celeridade da tomada de decisão;

O Infarmed tem uma abordagem faseada em termos de evolução da maturidade da gestão do risco em termos da sofisticação ao nível da estrutura, processos, governança. A melhoria contínua deverá basear-se em indicadores de progresso qualitativos e quantitativos.

## 2. ESTRUTURA

A estrutura da gestão do risco refere-se às disposições (incluindo práticas, processos, sistemas, recursos e cultura) dentro do sistema de gestão da organização que permitem que o risco seja gerido.

A estrutura da gestão do risco do Infarmed tem o objetivo de integrar a gestão do risco em todas as suas atividades e funções significativas. A eficácia da gestão do risco dependerá da sua integração na governação do Infarmed, incluindo a tomada de decisão. Isto requer o apoio das partes interessadas, incluindo os seus dirigentes superiores, dirigentes intermédios, gestores da qualidade, gestores de projetos e técnicos.

A Figura 1 esquematiza a Estrutura da Gestão do Risco no Infarmed.

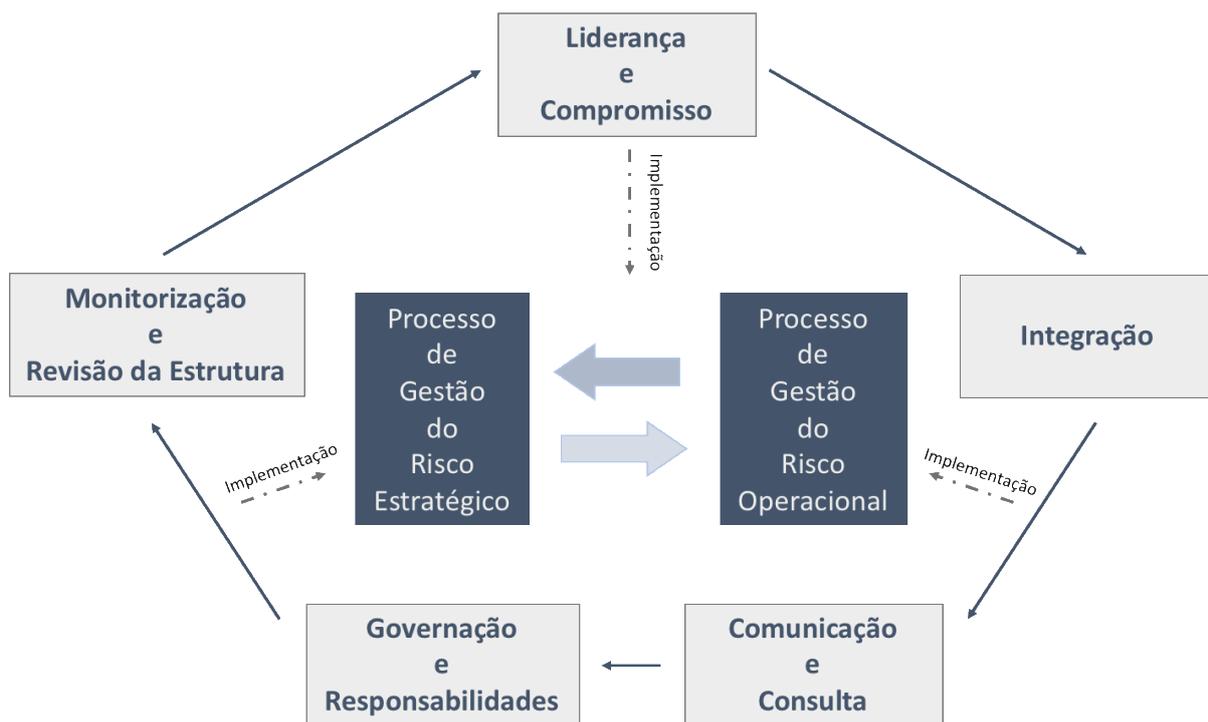


Figura 1 - Estrutura da Gestão do Risco no Infarmed

## 2.1. Liderança e Compromisso

A Gestão do Risco no Infarmed é assumido por todo o Conselho Diretivo (CD) como prioritário. O Conselho Diretivo é um ativo patrocinador do projeto de desenvolvimento da Estratégia de Gestão do Risco Organizacional, em linha com o estabelecido na norma ISO 31000:2018, e nesse contexto elaborou e homologou a Política de Gestão do Risco do Infarmed que define o conjunto de princípios subjacentes.

O CD é, também, responsável pela aprovação do Manual da Gestão do Risco Organizacional.

O CD do Infarmed assume a responsabilidade de gerir o risco dentro da organização, delegando a supervisão da gestão do risco na Unidade de Supervisão da Gestão do Risco, a sua implementação nos dirigentes e responsáveis de acordo com os vários níveis da organização e assegura que os recursos humanos, financeiros e materiais necessários para um adequado planeamento e implementação da gestão do risco.

É linha orientadora do CD do Infarmed que a elaboração da estrutura e dos processos sejam participativos e envolvam os seus dirigentes e trabalhadores, sendo de realçar a importância de uma comunicação ativa e transparente, bem como a capacitação das pessoas da organização para uma gradual e correta implementação da gestão do risco nas atividades e funções.

## 2.2. Integração

O Infarmed procura desenvolver uma gestão do risco organizacional que tenha em consideração o contexto externo e interno e as necessidades específicas de cada área funcional e das suas competências e capacidades instaladas, e a cultura da organização e de cada Unidade Orgânica (UO). Existe um enfoque na criação das condições para que a gestão do risco seja uma parte, e não separada, da finalidade, governação, estratégia, objetivos e operações da organização.

## 2.3. Comunicação e consulta

O CD do Infarmed assume a importância da comunicação transparente e a consulta aos seus dirigentes e técnicos para apoiar na definição da estrutura e processos da gestão do risco e facilitar a sua aplicação eficaz. A comunicação envolve a partilha da informação e dos documentos relevantes com a audiência adequada. A consulta envolve, também, participantes que forneçam *feedback* na expectativa de que contribuirá para, e moldará, decisões ou outras atividades relacionadas com a gestão do risco.

No contexto da comunicação e consulta, são considerados os seguintes eventos:

- Comunicação e disponibilização da Política da Gestão do Risco do Infarmed;
- Realização de Workshops para discussão dos processos de gestão do Risco Estratégicos e Operacionais e dos manuais previstos;
- Formação sobre os conceitos da gestão do risco e dos processos de gestão do risco;
- Divulgação no sistema de informação interno dos planos de riscos elaborados;
- Explicitação de mecanismos de *feedback* relativamente aos processos;
- Participação ativa na monitorização e revisão do sistema de gestão do risco.

## 2.4. Governação e Responsabilidades

O Conselho Diretivo do Infarmed considera que a gestão do risco é uma componente integrante da gestão da organização, na medida que implica a coordenação de atividades para as quais são identificados os efeitos da incerteza na realização dos objetivos. Neste contexto, e de acordo com o estabelecido na norma ISO 31000:2018, “Gestão do Risco” refere-se à arquitetura que a organização utiliza (princípios, estrutura e processos), e “gerir o risco” significa a aplicação dessa arquitetura a decisões, atividades e decisões específicos.

O CD do Infarmed assume a responsabilidade de gerir o risco dentro da organização, delegando a supervisão da Gestão do Risco na Unidade de Supervisão da Gestão do Risco – atualmente uma unidade informal criada para o propósito da supervisão da Gestão do Risco - e a sua implementação nos dirigentes das unidades orgânicas e responsáveis de acordo com os vários níveis da organização.

A governação da Gestão do Risco é composta pelos seguintes elementos:

- i. Conselho Diretivo (CD)
- ii. Unidade de Supervisão da Gestão do Risco (USGR)
- iii. Diretores de Direção (DDs) e respetivos Diretores de Unidade (DUs)
- iv. Gestores da Qualidade (GQs)
- v. Donos do Risco (DR)

As responsabilidades de cada elemento são as seguintes:

**i. Responsabilidades do CD:**

- Definição e elaboração da gestão do risco (política, princípios, estrutura e processos);
- Garantir a comunicação, consulta interna e formação;
- Alocar os recursos humanos, financeiros e materiais para a gestão do risco;
- Gerir o risco dentro da organização;
- Delegar responsabilidades na gestão do risco, nomeadamente na Unidade de Supervisão da Gestão do Risco;
- Assegurar a monitorização, revisão e melhoria do sistema de gestão do risco.

**ii. Responsabilidades da USGR:** A Unidade de Supervisão da Gestão do Risco (USGR) é composta por um elemento com responsabilidade de Assessoria ao CD na área da Gestão do Risco, que coordena a unidade, o Diretor de Planeamento e Qualidade, e outros elementos da orgânica considerados relevantes.

As responsabilidades da USGR são:

- Verificar o cumprimento do estabelecido nos elementos da estrutura de gestão do risco;
- Assegurar que a gestão do risco está integrada na gestão do organismo ao nível dos processos estratégicos e operacionais;
- Monitorizar que a organização tem uma compreensão atualizada e abrangente dos seus riscos e que os riscos estão dentro dos critérios de risco estabelecidos e têm ações corretivas sempre que esses critérios o justifiquem;
- Requerer a monitorização e o reporte regulares da estrutura de gestão do risco e dos processos e avaliar a sua eficácia;
- Agilizar a gestão do risco nas áreas de interfaces e partilhadas por várias UOs.

**iii. Responsabilidades dos DDs e respetivos DUs:**

- Garantir uma gestão do risco integrada nos processos de planeamento e execução da sua unidade orgânica;
- Garantir o cumprimento do estipulado no processo de gestão do risco operacional e simultaneamente assegurar a devida adaptação face às especificidades da UO;
- Reportar necessidades de melhoria ou evolução do estabelecido na estrutura da gestão do risco;
- Assegurar que a especificidade das pessoas, cultura, requisitos de área, competências e capacidade da sua unidade orgânica são consideradas na elaboração, monitorização e revisão da estrutura da gestão do risco.

- vi. **Responsabilidades dos GQs:** Garantir uma gestão do risco integrada nos processos no âmbito do Sistema de Gestão da Qualidade;
- vii. **Responsabilidade do DR:** Garantir que o risco é gerido de forma adequada e que as atividades identificadas são cumpridas nos prazos estabelecidos.

## 2.5. Implementação

A implementação da Estrutura da Gestão do Risco traduz-se, em termos de Planeamento, em documentos específicos e encontra-se refletida diretamente nos procedimentos do Sistema de Gestão da Qualidade do Infarmed:

- Matriz de Gestão dos Riscos Estratégicos
- Matriz de Gestão dos Riscos Operacionais
- Matriz de Gestão dos Riscos de Corrupção e Infrações Conexas
- Matriz de Gestão dos Riscos de Segurança da Informação

A execução das matrizes operacionaliza a Gestão do Risco no Infarmed.

## 2.6. Monitorização e Revisão da Estrutura

Para avaliar a eficácia da estrutura da gestão do risco, o Infarmed compromete-se a:

- Medir periodicamente o desempenho da estrutura da gestão do risco em relação ao seu objetivo, planos de implementação, indicadores e comportamento esperado;
- Determinar a adequabilidade da estrutura e processos ao apoio da consecução dos objetivos da organização;
- Avaliar se as mudanças internas e externas à organização deverão ter impacto na estrutura de gestão do risco.

A Monitorização e Revisão são duas atividades distintas, sendo que a Monitorização implica a vigilância de rotina do desempenho real da Gestão do Risco face ao esperado e a Revisão implica a verificação periódica ou pontual, visando identificar mudanças no contexto externo ou nas práticas das áreas do domínio de atuação do Infarmed, ou alterações nas práticas da própria organização.

A responsabilidade global das atividades de Monitorização e Revisão é do Conselho Diretivo que delega na Unidade de Supervisão da Gestão do Risco.

## 3. PROCESSOS

De acordo com a norma ISO 31000:2018, o processo da gestão do risco envolve a aplicação sistemática de políticas, procedimentos e práticas nas atividades de comunicação e consulta, estabelecimento do contexto e na apreciação, tratamento, monitorização, revisão, registo e reporte do risco. No âmbito da gestão do risco no Infarmed, foram consideradas duas aplicações específicas do processo da gestão do risco, correspondente a duas tipologias de risco:

### Riscos Estratégicos:

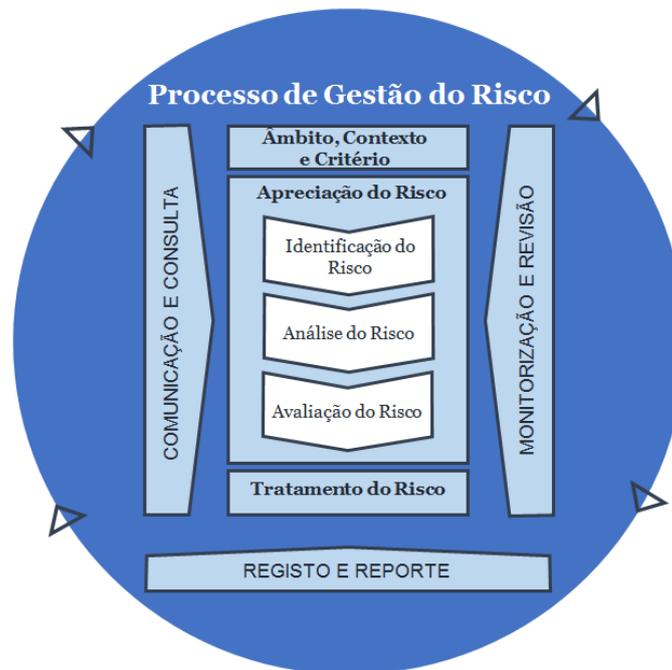
- Riscos associados ao cumprimento dos Objetivos Estratégicos e Iniciativas Estratégicas, traduzidos no Plano Estratégico;
- Riscos ligados a decisões de nível estratégico enquadrados em contexto de iniciativas governamentais ou Europeias;

### Riscos Operacionais

- Riscos associados aos objetivos operacionais das unidades orgânicas, presentes no QUAR e Plano de Atividades;
- Riscos associados aos processos das atividades definidas no âmbito da gestão da qualidade;
- Riscos de Corrupção e Infrações Conexas;
- Riscos associados à Segurança da Informação
- Riscos associados a incumprimentos dos enquadramentos regulatórios e legislativos;
- Riscos associados ao planeamento e execução de programas e projetos;
- Riscos associados à Segurança e Saúde Ocupacional;
- Riscos ambientais;
- Riscos técnicos.

Assim, cada tipologia de risco tem o seu processo de gestão do risco específico, ou seja, o Processo de Gestão dos Risco Estratégico e o Processo de Gestão do Risco Operacional, e dentro do Processo de Gestão do Risco Operacional haverá instanciação para os diversos subtipos de Riscos Operacionais.

Alinhado com o estipulado pela norma ISO 31000:2018, os processos de Gestão do Risco Estratégico e Operacional do Infarmed consideraram os elementos seguintes (Figura 2):



Fonte: ISO 31000:2018

**Figura 2 - Processo Genérico de Gestão do Risco**

### Âmbito, contexto e critérios

O processo da gestão do risco aplica-se aos níveis estratégico e operacional, e dentro deste último a diferentes subtipos de riscos bem como a compreensão dos ambientes externo e interno específicos da atividade a que o processo da gestão do risco vai ser aplicado.

Foram definidos critérios para avaliar a significância do risco e para suportar os processos de tomada de decisão, e especificar a magnitude e tipo de riscos que os decisores podem ou não assumir, em relação aos objetivos, das atividades e funções.

### Apreciação do Risco

A Apreciação do Risco é o processo global de Identificação do Risco, Análise do Risco e Avaliação do Risco. A Identificação do Risco reconhece e descreve os riscos que podem ajudar ou impedir que uma organização atinja os seus objetivos e implica instanciar as fontes e as causas do risco; condições e eventos; consequências e os seus impactos nos objetivos (positivos ou negativos); e possíveis indicadores dos riscos emergentes. A Análise do Risco envolve a consideração detalhada das

incertezas, fontes e causas do risco, os eventos e as suas consequências, os controlos e a sua eficácia. Um evento pode ter múltiplas causas e consequências e pode afetar múltiplos objetivos.

A Avaliação do Risco envolve a comparação dos resultados da análise do risco com os critérios do risco estabelecidos para determinar se é requerida uma ação de Tratamento do Risco. A Avaliação do Risco é feita através da representação numa Matriz de Risco, considerando as dimensões Possibilidade e Impacto.

### Tratamento do Risco

O Tratamento do Risco implica selecionar e implementar opções para abordar o risco. O tratamento do risco envolve um processo iterativo de:

- Formular e selecionar as opções de tratamento do risco;
- Planear e implementar o tratamento do risco;
- Apreciar a eficácia desse tratamento;
- Analisar se o risco residual (após medidas de mitigação) é aceitável;
- Não sendo aceitável, considerar tratamento suplementar.

A seleção das opções a considerar no tratamento do risco envolve a análise dos potenciais benefícios que resultam da relação entre a consecução dos objetivos e os custos e o esforço ou as desvantagens da implementação. As decisões de Tratamento de Risco estão contempladas na Matriz de Gestão do Risco, e serão função dos Critérios de Risco, que orientam a prioridade de ação.

A preparação e implementação dos planos para tratamento do risco estão descritos em documentos específicos, complementados com a informação da Apreciação do Risco, nomeadamente:

- Matriz de Gestão dos Riscos Estratégicos;
- Matriz de Gestão dos Riscos Operacionais;
- Matriz de Gestão dos Riscos de Corrupção e Infrações Conexas;
- Matriz de Gestão dos Riscos de Segurança da Informação
- Processos do Sistema de Gestão Qualidade.

### Comunicação e Consulta

A Comunicação procura promover a consciencialização e a compreensão do risco, através da reunião diferentes áreas de especialização para cada etapa do processo da gestão do risco e assegurar que diferentes pontos de vista são considerados de modo apropriado na definição dos critérios do risco e na avaliação dos riscos. A Consulta envolve a obtenção de *feedback* e informação para suporte da tomada de decisão. A Comunicação e Consulta são fatores críticos para obter inclusão e pertença os decisores permeáveis ao risco.

### Monitorização e Revisão

A Monitorização e a Revisão incluem o planeamento, a recolha e a análise da informação, o registo de resultados e o fornecimento de *feedback* para que o Processo de Gestão dos Riscos possa evoluir e melhorar.

### Sistema de Registo e Reporte

O Processo de Gestão dos Riscos e os seus resultados são documentados e reportados através do sistema de informação interno do Infarmed criado para o efeito.

---

## ESTRATÉGIA DE GESTÃO DO RISCO ORGANIZACIONAL

---

**A Estratégia de Gestão do Risco Organizacional do Infarmed pode ser consultada em**

[http://www.infarmed.pt/web/infarmed/institucional/documentacao\\_e\\_informacao/documentos-institucionais](http://www.infarmed.pt/web/infarmed/institucional/documentacao_e_informacao/documentos-institucionais)