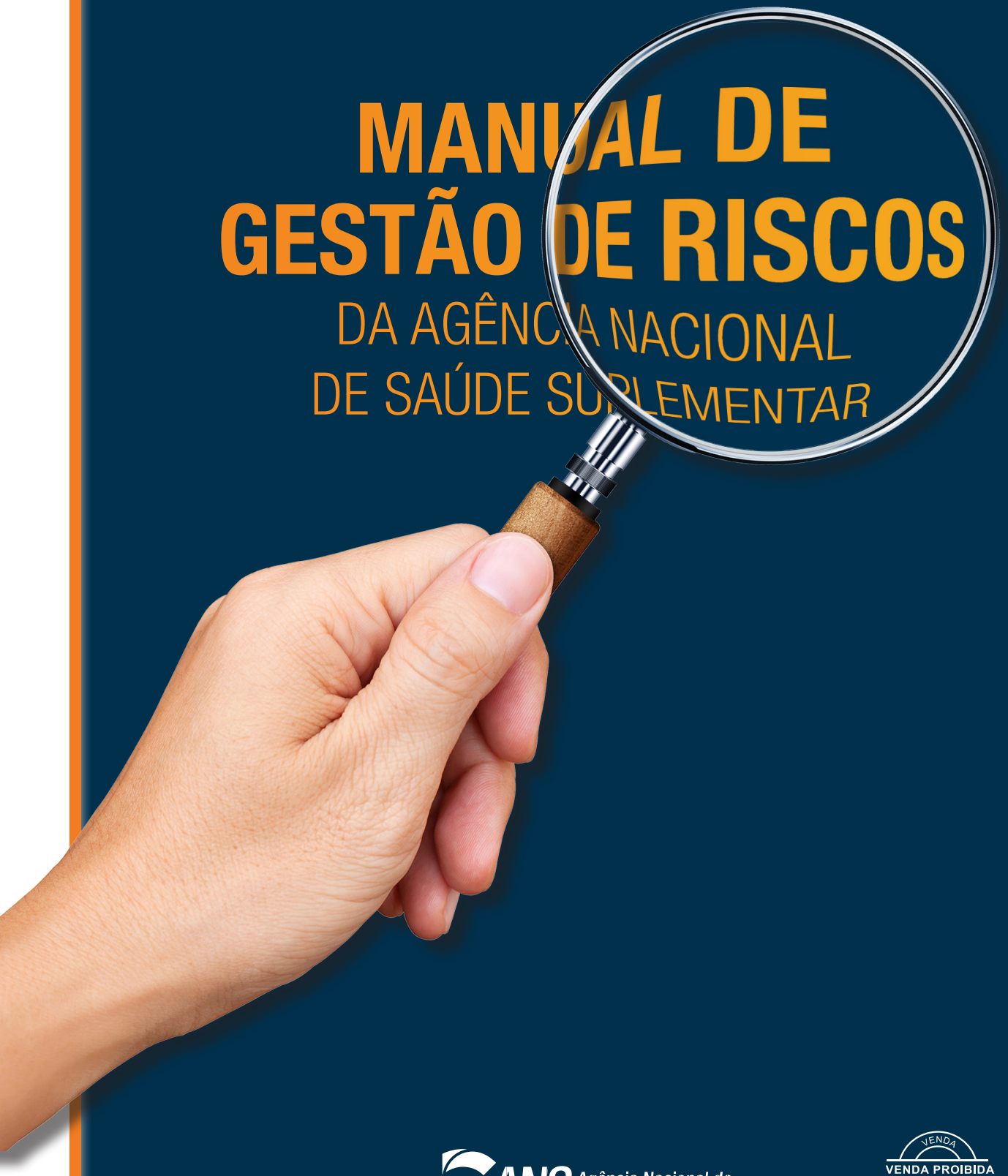
AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR

MANUAL DE GESTÃO DE RISCOS

DA AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR



ANS Agência Nacional de Saúde Suplementar

VENDA PROIBIDA

Rio de Janeiro
2018

Atualizado em 16/11/2018

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR
PRESIDÊNCIA
GABINETE
GERÊNCIA GERAL DE ANÁLISE TÉCNICA DA PRESIDÊNCIA
COORDENADORIA DE AVALIAÇÃO DE RISCOS INSTITUCIONAIS

MANUAL DE GESTÃO DE RISCOS
DA AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR

ANS Agência Nacional de Saúde Suplementar
Rio de Janeiro
2018

2018. Agência Nacional de Saúde Suplementar.
Esta obra é disponibilizada nos termos da Licença Creative Commons – Atribuição – Não Comercial – Sem Derivações. Compartilhamento pela mesma licença 4.0 Internacional. É permitida reprodução parcial ou total desta obra, desde que citada a fonte.
O conteúdo desta, e de outras obras da Agência Nacional de Saúde Suplementar, pode ser acessado na página www.ans.gov.br

www.ans.gov.br

Versão *online*

Elaboração, distribuição e informações
Agência Nacional de Saúde Suplementar – ANS
Presidência – PRESI
Gabinete – GAB/PRESI
Gerência-Geral de Análise Técnica – GGATP/GAB/PRESI
Coordenadoria de Avaliação de Riscos Institucionais – COARI/GGATP/GAB/PRESI
Av. Augusto Severo, 84 – Glória
CEP 20.021-040
Rio de Janeiro, RJ – Brasil
Tel.: +55(21) 2105-0000
Disque ANS 0800 701 9656
www.ans.gov.br

Diretoria de Desenvolvimento Setorial – DIDES
Diretoria de Fiscalização – DIFIS
Diretoria de Gestão – DIGES
Diretoria de Normas e Habilitação das Operadoras – DIOPE
Diretoria de Normas e Habilitação dos Produtos – DIPRO

Projeto Gráfico
Gerência de Comunicação Social – GCOMS/SEGER/DICOL

Normalização
Biblioteca/CGECO/GEQIN/DIGES

Ficha Catalográfica

A 265m Agência Nacional de Saúde Suplementar (Brasil). Presidência. Gabinete. Gerência-Geral de Análise Técnica da Presidência. Coordenadoria de Avaliação de Riscos Institucionais.
Manual de gestão de riscos da Agência Nacional de Saúde Suplementar [recurso eletrônico] / Agência Nacional de Saúde Suplementar. Presidência. Gabinete. Gerência-Geral de Análise Técnica da Presidência. Coordenadoria de Avaliação de Riscos Institucionais. – Rio de Janeiro: ANS, 2018.
2,8MB; ePUB.

1 Gestão de Risco. I. Título

CDD 658.4

Catalogação na fonte – Biblioteca ANS

SUMÁRIO

Apresentação	5
PARTE I – CONTEXTUALIZAÇÃO	7
1. Risco	7
2. Gestão de Riscos	8
3. Princípios da Gestão de Riscos	9
4. Atores da Gestão de Riscos	10
4.1 Gestores de Riscos	10
4.2 Agentes de Riscos	10
4.3 CGRC – Comitê de Governança, Riscos e Controles	10
4.4 COMARI – Comitê de Avaliação de Riscos	11
4.5 GGATP – Gerência Geral de Análise Técnica da Presidência	11
4.6 COARI – Coordenadoria de Avaliação de Riscos Institucionais	11
PARTE II – PROCESSO DE AVALIAÇÃO DE RISCOS	13
5. Processo de Avaliação de Riscos	13
5.1 Processo de Planejamento	15
5.1.1 Iniciando o planejamento	15
5.1.2 Preenchendo o QAR	16
a) Preenchendo o Cabeçalho	16
b) Descrição do Processo	16

c) Quais os Produtos/Serviços resultantes desse processo e a quem se destina?	17
d) Identificação dos Objetivos e Riscos do Processo/Atividade	18
d.1) Processo/Atividade e Objetivos	18
d.2) Riscos	19
d.3) Causas e Efeitos	20
d.4) Controles Atuais	23
5.1.3 Finalizando o QAR	24
5.2 Processo de Execução	25
5.2.1 Iniciando a execução	26
a) Preenchendo a aba "RISCO"	26
b) Preenchendo a aba "DADOS"	27
c) Preenchendo a aba “ANÁLISE”	32
c.1) Avaliando: “Residual” *versus* “Tolerável”	33
c.2) Definindo o tratamento do risco	34
ANEXO I – QAR	35
ANEXO II – AR	36
BIBLIOGRAFIA	39

APRESENTAÇÃO

O Manual de Gestão de Riscos da ANS é uma publicação destinada à prática da gestão de riscos. Foi elaborado pela Coordenadoria de Avaliação de Riscos Institucionais da ANS com o objetivo de apresentar, de forma sintética, os conceitos e princípios que norteiam o tema, além de servir como guia para os agentes e gestores na realização do processo de avaliação de riscos.

O Manual está estruturado em duas partes: Contextualização e Processo de Avaliação de Riscos, onde estão descritos os conceitos, a gestão, os princípios e os atores da gestão de riscos, bem como a metodologia utilizada pela ANS. Permite compreender a aplicação prática dos conceitos e descreve o passo a passo no preenchimento dos artefatos utilizados pela ANS no processo de avaliação de riscos, com conteúdo e linguagem simples, de forma que qualquer pessoa que deseje compreender e gerir os riscos em seus processos de trabalho possa fazê-lo.

A base teórico-conceitual do Manual está pautada na Política de Gestão de Riscos da ANS (Resolução Administrativa - RA nº 60/2014) e nas normas ISO 31000[1], ISO 31010[2] e COSO[3]. Outros direcionadores são os atos normativos publicados recentemente pelo Ministério do Planejamento Desenvolvimento e Gestão e pelos órgãos de controle interno e externo, bem como as boas práticas de gestão de riscos adotadas pelas equipes de trabalho envolvidas na implementação da ferramenta na ANS.

A ANS vem estruturando e implementando sua Gestão de Riscos desde 2013, reconhecendo a importância desse componente da governança para a administração pública e os benefícios que traz para a instituição e para o cumprimento de seus objetivos. Como primeiro produto desse trabalho, foi publicada em 2014 a Cartilha de Gestão de Riscos, que descreve detalhadamente a Política de Gestão de Riscos da ANS. A Cartilha está disponível para consulta no portal da ANS na internet em http://www.ans.gov.br/images/stories/A_ANS/Transparencia_Institucional/gestao_de_riscos/cartilha-gestao-de-riscos.pdf

A expectativa é que este Manual atenda às necessidades dos gestores e colaboradores, auxiliando-os a controlar e mitigar riscos e contribuindo para a melhoria dos processos internos, fazendo com que o processo de gestão de riscos seja incorporado à cultura da ANS.

Boa leitura!

[1] ASSOCIAÇÃO BRASILEIRA DE NORMALIZAÇÃO TÉCNICA. NBR ISO 31000:2018 gestão de riscos: diretrizes e princípios: Rio de Janeiro: ABNT, 2018.
[2] ABNT ISO/IEC 31010:2009 – Gestão de Riscos – Técnicas para o processo de avaliação de riscos".
[3] COMMITTEE OF SPONSORING ORGANIZATIONS OF TREADWAY COMMISSION. Internal control: integrated framework: executive summary. [S.l.]: COSO, 2013. Disponível on-line em: https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf. Acesso em: 14 set. 2017.

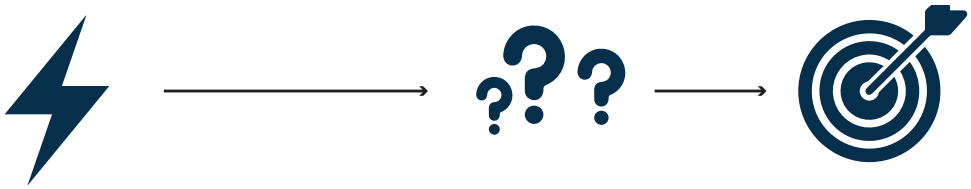
PARTE I – CONTEXTUALIZAÇÃO

1. RISCO

Risco é o efeito da incerteza nos objetivos ou a possibilidade de que um evento [4] ocorra e afete, positivamente ou negativamente, os objetivos.

Cabe destacar que **problemas** são diferentes de **riscos**. Quando identificados, os problemas devem ser considerados como riscos concretizados. Nossa análise considera o efeito da incerteza nos objetivos, ou seja, causas e consequências de eventos futuros e incertos. Assim, nosso foco não é tratar ou resolver problemas diretamente, mas, caso seja identificado que existe a possibilidade de um evento ocorrer novamente, o evento futuro poderá ser tratado como risco.

[4]Evento: incidente ou ocorrência de fontes internas ou externas que pode causar impacto negativo (riscos negativos), positivo (riscos positivos ou oportunidades) ou ambos sobre os objetivos.



RISCO É O EFEITO DA **INCERTEZA** NOS **OBJETIVOS**

Efeito é um desvio em relação ao esperado - positivo e/ou negativo

Incerteza é o estado, mesmo que parcial, da deficiência das informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência ou sua probabilidade.

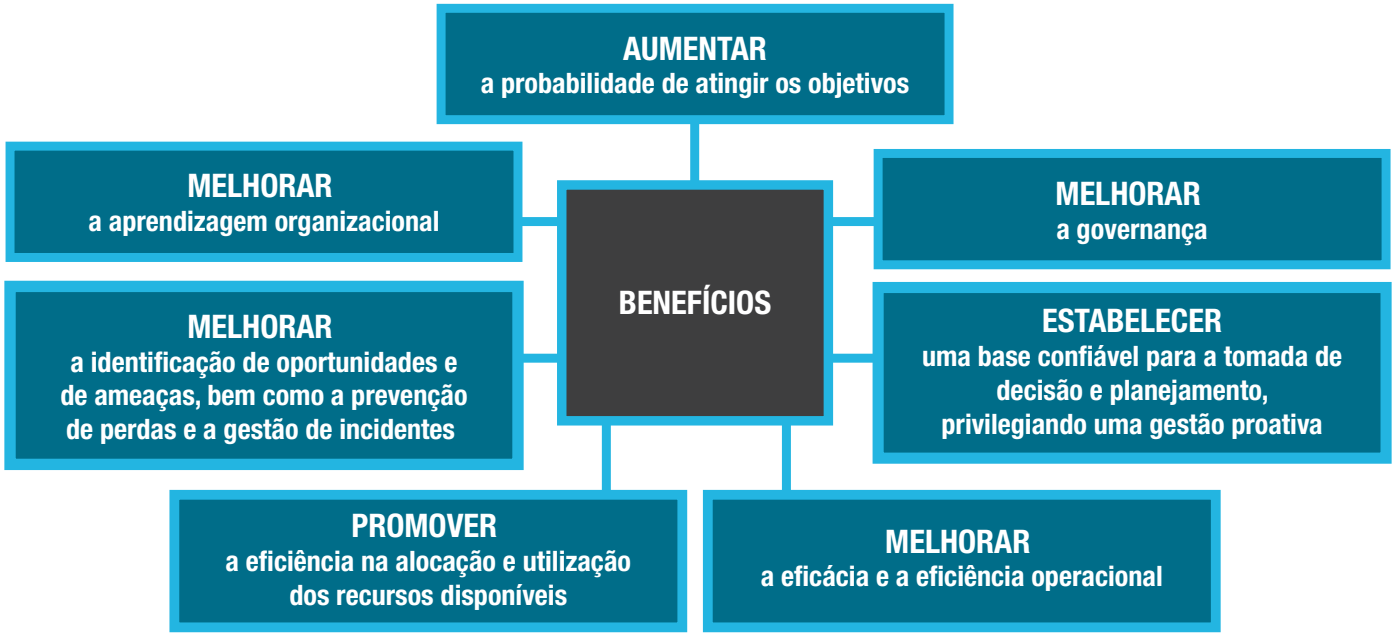
Sem conhecer e tratar os riscos envolvidos, o trabalho pode não atingir os resultados esperados

2. GESTÃO DE RISCOS

Segundo a norma ABNT ISO 31000, a gestão de riscos é definida como "atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos". Nossa Política de Gestão de Riscos traduziu esse conceito como "o conjunto de ações direcionadas ao desenvolvimento, disseminação e implantação de metodologias de gerenciamento de riscos[5] institucionais, objetivando apoiar a melhoria contínua de processos de trabalho, projetos e a alocação e utilização eficaz dos recursos disponíveis, contribuindo para o cumprimento dos objetivos da ANS" (Resolução Administrativa nº 60, de 15/07/2014).

[5] Gerenciamento de Riscos: processo contínuo que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar eventos capazes de afetar, positiva ou negativamente, os objetivos, processos de trabalho e projetos da ANS, nos níveis estratégico, tático e operacional. (RA nº 60/2014)

A adoção da gestão de riscos permite alcançar diversos benefícios para a Agência, entre eles:



3. PRINCÍPIOS DA GESTÃO DE RISCOS

A gestão de riscos na ANS está fundamentada nos seguintes princípios, conforme disposto na Política de Gestão de Riscos RA nº 60/2014/ANS:

- Agregar valor e proteger o ambiente institucional.
  Contribuindo para a realização demonstrável dos objetivos e para a melhoria do desempenho.

- Ser parte integrante dos processos organizacionais.
  Não sendo uma atividade autônoma, faz parte das responsabilidades da administração e é elemento integrante de todos os processos organizacionais, incluindo o planejamento estratégico e todos os processos de gestão de projetos e gestão de mudanças.

- Subsidiar a tomada de decisões.
  Auxiliando os tomadores de decisão a fazer escolhas conscientes, priorizar ações e distinguir entre formas alternativas de ação.

- Abordar explicitamente a incerteza.
  Considerando a incerteza, a natureza dessa incerteza e como ela pode ser tratada.

- Ser sistemática, estruturada e oportuna.
  Contribuindo para a eficiência e para os resultados consistentes, comparáveis e confiáveis.

- Ser baseada nas melhores informações disponíveis.
  Baseando-se em diversas fontes de informação. Convém que os tomadores de decisão se informem e levem em consideração quaisquer limitações dos dados ou de escopo.

- Ser feita sob medida, alinhada com o contexto interno e externo da ANS e com o perfil do risco.
  Não sendo um processo "de prateleira", deve ser adequada e compatível com a organização.

- Considerar fatores humanos e culturais.
  Reconhecendo as capacidades, percepções e intenções do pessoal interno e externo que podem facilitar ou dificultar a realização dos objetivos da organização.

- Ser transparente e inclusiva.
  Envolvendo, apropriada e oportunamente, as partes interessadas, em particular os tomadores de decisões em todos os níveis da organização.

- Ser dinâmica, interativa e capaz de reagir a mudanças.
  Percebendo e reagindo às mudanças, continuamente, sabendo que novos riscos surgem, alguns se modificam e outros desaparecem.

- Apoiar a melhoria contínua da entidade.
  Melhorando os processos da organização, inclusive a maturidade do próprio processo de gestão de riscos, justamente por ser ele parte integrante de sua cultura.

4. ATORES DA GESTÃO DE RISCOS

GESTORES
DE RISCOS

4.1 GESTORES DE RISCOS

Todos aqueles que são responsáveis pelo gerenciamento de um processo de trabalho ou um projeto é considerado um "Gestor de Riscos". A ele é atribuída a competência de informar o início do processo de avaliação de riscos, com apoio dos demais atores envolvidos da Gestão de Riscos e dos servidores e colaboradores envolvidos nas atividades sob sua gestão. Caso o Gestor de Riscos seja responsável por mais de um processo de trabalho, ele deve informar um cronograma de execução, priorizando as avaliações de acordo com a criticidade envolvida.

Os Gestores de Riscos também são responsáveis pela classificação dos riscos envolvidos nos seus processos de trabalho. Para os casos onde o nível de risco residual esteja acima do nível de risco tolerável, ele deverá estabelecer um plano de tratamento, a fim de reduzir os riscos a níveis aceitáveis.

AGENTES
DE RISCOS

4.2 AGENTES DE RISCOS

Os Agentes de Riscos auxiliarão os Gestores de Riscos no processo de avaliação riscos. Terão o papel de "facilitadores" desse processo, promovendo e acompanhando todas as fases definidas nesse manual.

Eles serão responsáveis pela consolidação das informações levantadas durante a execução do trabalho e envio dos artefatos devidamente preenchidos para a Coordenadoria de Avaliação de Risco Institucional, após o "de acordo" do Gestor do Risco.

CGRC
COMITÊ DE GOVERNANÇA,
RISCOS E CONTROLES

4.3 CGRC – COMITÊ DE GOVERNANÇA, RISCOS E CONTROLES

Criado pela Resolução Administrativa nº 67, de 11/05/2017, esse Comitê é composto pela Alta Administração da ANS (Diretores) e funcionará com o apoio do Auditor-Chefe da Agência. A Gerência-Geral de Análise Técnica da Presidência (GGATP) prestará assistência ao CGRC através do monitoramento das recomendações proferidas por ele.

As principais decisões relacionadas à Gestão de Riscos fazem parte das atribuições desse Comitê, conforme estabelecido na RA nº 67/2017, e tem efeito vinculante para toda a ANS. Entre elas, destacamos:

- Supervisionar a institucionalização de estruturas adequadas de governança, gestão de riscos e controles internos;
- Supervisionar a promoção do desenvolvimento contínuo dos agentes públicos e incentivar a adoção de boas práticas de governança, de gestão de riscos e de controles internos;
- Aprovar política, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos e dos controles internos; e
- Liderar e supervisionar a institucionalização da gestão de riscos e dos controles internos, oferecendo suporte necessário para sua efetiva implementação no órgão ou entidade.

COMARI
COMITÊ DE AVALIAÇÃO
DE RISCOS

4.4 COMARI – COMITÊ DE AVALIAÇÃO DE RISCOS

O COMARI é um comitê composto pelos Diretores-Adjuntos e Chefes de Órgãos Vinculados, sob coordenação da Presidência. Sua atuação é de forma consultiva e colaborativa com o CGRC, supervisionando, coordenando, estabelecendo prioridade, fomentando e propondo padrões relacionados às práticas de gestão de riscos.

GGATP
GERÊNCIA GERAL
DE ANÁLISE TÉCNICA
DA PRESIDÊNCIA

4.5 GGATP – GERÊNCIA GERAL DE ANÁLISE TÉCNICA DA PRESIDÊNCIA

Entre as responsabilidades institucionais da GGATP, incluem-se a contribuição para a implementação da Gestão de Riscos, o aperfeiçoamento das rotinas operacionais da ANS e seus controles internos, bem como a prestação de assistência ao CGRC.

COARI
COORDENAÇÃO DE
AVALIAÇÃO DE RISCO

4.6 COARI – COORDENADORIA DE AVALIAÇÃO DE RISCOS INSTITUCIONAIS

A COARI é a unidade operacional responsável pela implantação da Gestão de Riscos na ANS.

Acompanha a realização dos processos de avaliação de riscos pelo Gestores e Agentes de Riscos, disseminando os conceitos e capacitando os servidores para a realização das tarefas. Tem o papel de consolidar as informações e resultados gerados pelos trabalhos de avaliação de riscos, a fim de compor o mapa de riscos da Agência e preparar os relatórios gerenciais para informe aos Comitês.

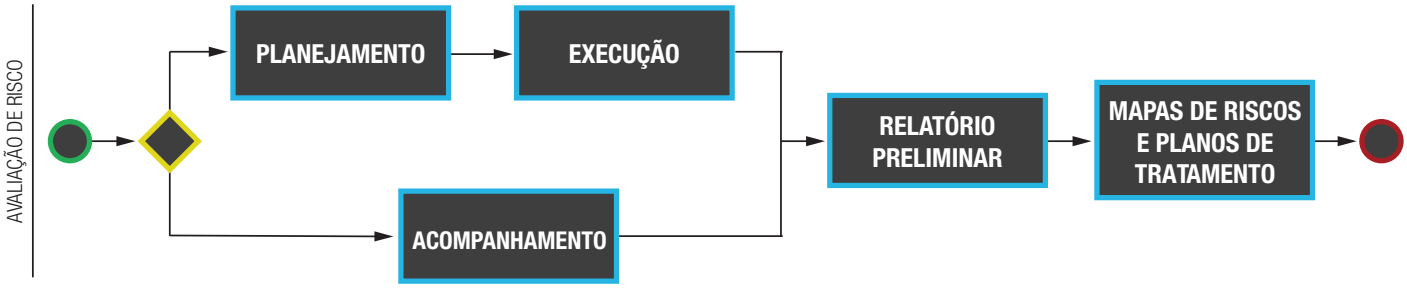
PARTE II – PROCESSO DE AVALIAÇÃO DE RISCOS

5. PROCESSO DE AVALIAÇÃO DE RISCOS

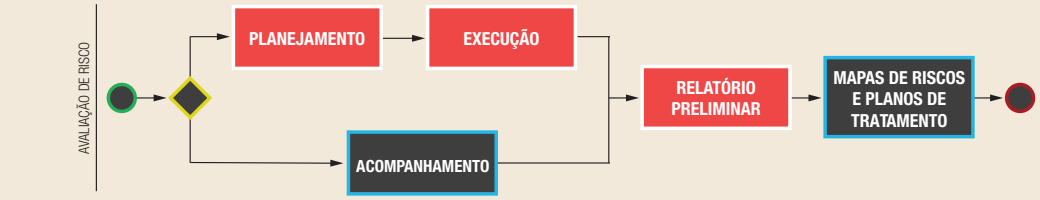
O processo de avaliação de riscos foi dividido em 5 processos:

- ✓Planejamento;
- ✓Execução;
- ✓Relatório Preliminar
- ✓Acompanhamento; e
- ✓Mapas de Riscos e Planos de Tratamento

FLUXOGRAMA DO PROCESSO DE AVALIAÇÃO DE RISCOS



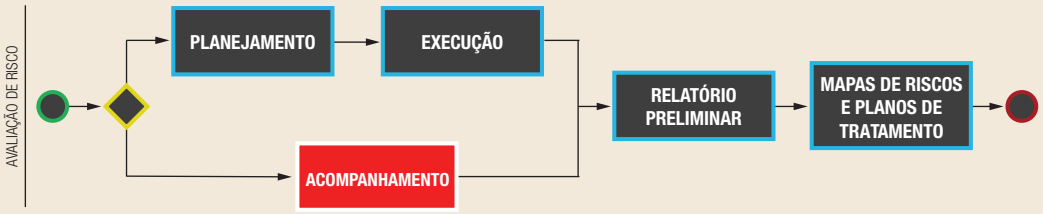
DETALHANDO OS PROCESSSOS:



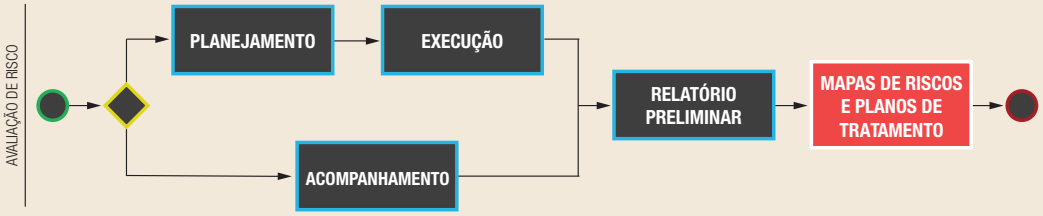
Os processos de **Planejamento, Execução e Relatório Preliminar** são sempre realizados sequencialmente, em uma das 3 situações:

✓Quando ocorre uma primeira avaliação de riscos de um processo de trabalho;
✓Quando o Gestor de Risco percebeu mudanças significativas no processo de trabalho, desde a última avaliação, e entende que novos riscos podem ter surgido; ou
✓Quando a última avaliação de riscos do processo de trabalho atingiu o prazo máximo de validade de 2 anos[6]. Nesse caso, automaticamente, o processo passa a ser elegível a uma nova avaliação de riscos. Processos de trabalho com maior criticidade podem, por decisão do Gestor de Riscos, ter um "prazo de validade" menor que 2 anos.

[6] RA nº 60/2014, Art. 8º O gerenciamento de riscos deve ser feito em ciclos não superiores a dois anos, abrangendo os processos de trabalho, sistemas informatizados, gestão orçamentária, gestão de pessoas e legislação, com vistas reduzir os eventos de riscos negativos, assim como, quando for o caso, potencializar os eventos de riscos positivos (oportunidades).

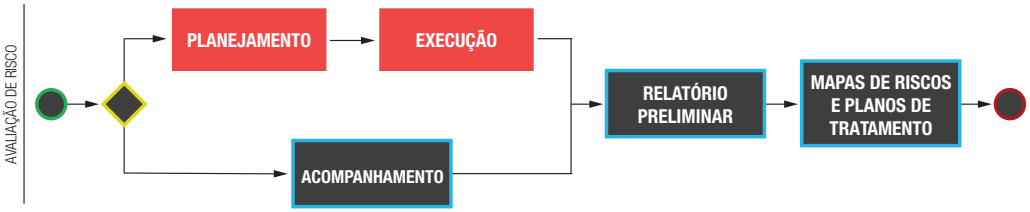


No processo de **Acompanhamento**, os riscos e os planos de tratamento apontados em Processos de Avaliação de Riscos realizados serão tempestivamente avaliados pelo Gestor de Riscos, com o apoio do Agente de Riscos.



O processo de **Mapas de Riscos e Planos de Tratamento** refere-se ao controle, consolidação e organização das informações geradas, e sua divulgação aos níveis competentes, estando a cargo da COARI.

Os processos de **Relatório Preliminar**, de **Acompanhamento** e de **Mapas de Riscos** e **Planos de Tratamento** **não serão** objeto desse manual, onde trataremos exclusivamente do **Planejamento** e da **Execução** das avaliações de riscos.



Apesar de poder ser realizada em qualquer objeto (atividades, subprocessos, processos de trabalho, macroprocessos, projetos, iniciativas ou mesmo áreas), este manual considerará que a avaliação de riscos está sendo feita em um "processo de trabalho"[7]. Os procedimentos descritos neste documento, via de regra, poderão ser aplicados a todos os possíveis objetos, sem nenhuma ou com pouca adaptação necessária.

[7] Processo de trabalho: atividade que gera um produto reconhecível e imediato, a partir de um insumo bem definido. Um processo de trabalho possui apenas um início que, assim como o seu fim, é bem definido, gerando um produto claramente reconhecido. (Mapeamento de processos na ANS: manual de orientação para o mapeamento de processos "as is", 2016).

5.1 PROCESSO DE PLANEJAMENTO

O Processo de Planejamento tem como objetivos principais:

✓Estabelecer o contexto: descrever o item que será avaliado, apontando de forma clara quais os objetivos, e as fontes de riscos[8] que fazem parte do processo, estabelecendo também o escopo de atuação.
✓Identificar os riscos: preparar uma lista dos eventos, suas causas[9] e seus efeitos (ou consequências)[10], que podem ocorrer e afetar o atingimento dos objetivos do que está sendo avaliado, com nenhum ou pouco julgamento de valor quanto a criticidade desses riscos. Adicionalmente, indicar os controles[11] atuais utilizados para prevenir as causas e detectar os efeitos dos riscos identificados.

Nesse processo, utilizaremos o artefato chamado Questionário de Avaliação de Riscos – QAR (anexo I).

[8]Fonte de risco: Elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco, podendo ser, por exemplo pessoas, processos, sistemas, infraestrutura física ou organizacional, tecnologia de produto ou de produção ou eventos externos (não-gerenciáveis)
[9]Causa: vulnerabilidade associada a uma fonte de riscos
[10]Efeito (ou consequência): resultado de um evento que afeta o objetivo
[11]Controles: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, destinados a enfrentar os riscos, de forma preventiva ou corretiva.

5.1.1 INICIANDO O PLANEJAMENTO

✓O Gestor de Riscos deverá designar o processo de trabalho que será avaliado. Caso esse Gestor tenha mais de um processo sob sua responsabilidade, deve informar um cronograma com a sequência de processos que serão avaliados e uma estimativa de data (mês e ano) para finalização (emissão do artefato do processo de Execução).

O Agente de Riscos e o Gestor de Riscos devem comunicar à COARI o início do processo de avaliação de riscos, qual o processo está avaliando e, se for o caso, o cronograma dos próximos trabalhos quando existentes.

A COARI poderá solicitar a participação nas reuniões do Processo de Planejamento a fim de acompanhar o processo de avaliação de riscos. A participação da COARI poderá ocorrer também por solicitação do Gestor do processo ou do Agente de Riscos.
Recomenda-se que cada Agente de Riscos realize a avaliação de riscos de um processo de trabalho por vez.

5.1.2 PREENCHENDO O QAR

A) PREENCHENDO O CABEÇALHO

Inicie o preenchimento do QAR identificando adequadamente no topo do formulário as informações de referência do processo de trabalho cujos riscos serão geridos:

COORDENAÇÃO DE AVALIAÇÃO DE RISCO

Questionário de Avaliação de Riscos

Processo:		N° do Processo **NNN/2017/ÓRGÃO**
Gestor:	Agente de riscos:	Data:

B) DESCRIÇÃO DO PROCESSO

Realize uma ou mais reuniões com o Gestor de Riscos para obter as informações necessárias sobre o processo de trabalho. O objetivo da etapa é descrever o processo como ele é.

O que se pretende não é mapear ou redesenhar formalmente o processo de trabalho avaliado, mas sim conhecê-lo, os seus objetivos e as fontes de riscos presentes em suas atividades. A preocupação deve ser apenas e tão somente descrever como ele é efetivamente executado. As eventuais propostas de mudanças ou as dificuldades na realização do processo serão discutidas oportunamente no processo de Execução, em que estaremos aptos a definir planos de tratamento necessários para gerenciar os níveis de riscos que serão conhecidos.

É importante frisar o detalhamento da descrição do processo de trabalho: objetivos, etapas, procedimentos, atividades, recursos humanos (*peopleware*), equipamentos (*hardware*), sistemas de informação requeridos (*software*) e materiais, além de outras fontes de riscos que sejam parte integrante desse fluxo de informações e tomadas de decisão. Quanto mais detalhada a descrição do processo de trabalho, mais fácil será a visualização dos eventos que podem ocorrer e afetar os objetivos.

Uma das informações cruciais nesse ponto é descrever quais os objetivos do processo. Uma vez que risco é definido como "a possibilidade de que um evento interno ou externo ocorra e afete, positivamente (risco positivo ou oportunidade) ou negativamente (risco negativo) ***os objetivos***", será preciso ter claramente identificado os objetivos do processo de trabalho, e o porquê desse processo existir. Todo o trabalho de avaliação de riscos será feito em cima dos eventos que podem afetar os objetivos.

Uma maneira prática de descrever um processo é pensar, após identificados os objetivos, na sequência temporal que ocorre o fato gerador que o inicia, atividades que transformam esse fato gerador, tomadas de decisão sobre o que fazer com os dados e informações que estão percorrendo o fluxo, como também nos subprodutos e os produtos finais gerados, sempre considerando as fontes de riscos envolvidas e o "mundo real" de hoje, como é, e não um "mundo ideal", como deveria ser.

Nesse item 1 do QAR, existe uma sugestão de roteiro para a descrição, apresentada abaixo. Essa parte do questionário é apenas um lembrete sobre o que descrever e pode ser apagada quando finalizar a descrição.

COORDENAÇÃO DE AVALIAÇÃO DE RISCO

Questionário de Avaliação de Riscos

Processo: N° do Processo **NNN/2018/ÓRGÃO**

Gestor: Agente de riscos: Data:

1. Descrição do Processo.

[Descreva o fluxo de trabalho, considerando:

- *Os objetivos do processo de trabalho avaliado*
- *As etapas, os procedimentos e as atividades que compõem o processo*
- *Os recursos humanos, materiais e de sistemas de informação requeridos para a execução do processo*
- *As infraestruturas físicas envolvidas (exemplos: localização, instalações e controle de acesso físico)*
- *A estrutura organizacional relacionada ao processo (exemplos: funções e responsabilidades regimentais, fluxos de informação e comunicação, centralização e delegação de responsabilidades)*
- *O volume de transações mensal ou em outra base temporal*
- *Os eventos externos que, ainda que não sejam gerenciáveis, tenham impactos sobre o processo]*

Ao realizar as etapas anteriores, você poderá aproveitar a descrição do processo de trabalho para desenvolver uma representação gráfica, como um fluxograma, apontando onde ocorrem as atividades e seus objetivos, os momentos de tomada de decisão, o fluxo da informação ou de documentos e a utilização de software, hardware e peopleware, além de outras fontes de riscos. O resultado desse esforço será uma melhor visualização de pontos de risco, ou seja, quais são os eventos de riscos e onde eles poderão ocorrer.

C) QUAIS OS PRODUTOS/SERVIÇOS RESULTANTES DESSE PROCESSO E A QUEM SE DESTINA?

Para responder ao item 2 do QAR, aponte quais são produtos ou serviços gerados pelo processo que está sendo avaliado, e a quem são destinados esses resultados.

A intenção aqui é reforçar os objetivos do processo de trabalho, não deixando dúvidas do porquê de sua existência.

D) IDENTIFICAÇÃO DOS OBJETIVOS E RISCOS DO PROCESSO/ATIVIDADE

D.1) PROCESSO/ATIVIDADE E OBJETIVO

Na tabela da questão 3 a ser preenchida, deve ser informado qual o processo e seu objetivo geral (ou qual atividade do processo e seu objetivo específico).

Processo/ Atividade:	QUAL É O PROCESSO/ATIVIDADE?
Objetivo:	QUAL É O OBJETIVO DO PROCESSO/ATIVIDADE?
Risco:	
Causas:	
Efeitos:	
Controles Atuais:	

Finalizada a descrição do processo e apontados os produtos ou serviços resultantes, vamos trabalhar em cima dos objetivos, dos eventos que os afetam, das suas causas e dos seus efeitos, bem como dos controles atuais que os gerenciam.

Além do objetivo geral do processo como um todo, apontado na descrição, tenha atenção para atividades críticas do processo e seus objetivos específicos. Pense quais eventos podem afetar também todos esses objetivos. A tabela deve ser usada tanto para identificação dos objetivos gerais como também para os objetivos específicos.

Uma sugestão é começar "pelo todo", ou seja, começar pelo processo e seu objetivo ou objetivos gerais. Depois de identificar os riscos (ou seja, os eventos, bem como as causas, os efeitos e os controles atuais) que podem afetar esses objetivos, passe para as atividades críticas e seus objetivos específicos. Novos riscos podem surgir os quais não foram identificados quando se analisou o objetivo geral, e estes quando identificados deverão ser descritos.

D.2) RISCO

Processo/ Atividade:	
Objetivo:	
Risco:	QUAIS EVENTOS PODEM AFETAR ESSES OBJETIVOS?
Causas:	
Efeitos:	
Controles Atuais:	

Depois de identificados os objetivos que serão avaliados, realize reuniões com o Gestor do Risco (e equipe) para identificar todos os eventos que podem afetar esses objetivos. Promova, por exemplo, reuniões de "brainstorming"[12] para que as ideias sejam apresentadas.

[12] Brainstorming: Ferramenta para, isoladamente ou em conjunto com outros métodos, incentivar o pensamento criativo, em discussões de alto nível ou para análise crítica mais detalhada, em qualquer fase do processo de avaliação de riscos.

É importante lembrar que, nesse momento do processo de avaliação de riscos, deve-se procurar não fazer, ou fazer o mínimo possível, de julgamento de valor quanto a probabilidade e o impacto associados ao risco. Considere o máximo possível de eventos que podem afetar o atingimento dos objetivos, mas pondere se realmente vale a pena a inclusão dos famosos "cisnes negros"[13].

[13] Cisnes negros: Eventos de baixíssimas probabilidades, mas de impactos "devastadores". A queda de um meteoro, por exemplo.

RISCO ≠ PROBLEMA

Recomendações da Auditoria Interna, Ouvidoria, Corregedoria, Procuradoria e CGRC devem servir de insumo para a etapa de identificação de riscos.

D.3) CAUSAS E EFEITOS

Processo/ Atividade:	
Objetivo:	
Risco:	
Causas:	FONTE DE RISCOS + VULNERABILIDADES
Efeitos:	IMPACTO OU CONSEQUÊNCIA NO OBJETIVO - VER MATRIZ DE RISCOS
Controles Atuais:	

Um risco ou evento é composto de causas (fontes de riscos associadas a vulnerabilidades[14]) e efeitos.

[14]Vulnerabilidade: Ineficiências, inadequações ou deficiências em uma fonte de risco. Quaisquer deficiências em processos de trabalho, projetos, legislação, sistemas informatizados, gestão de pessoal, recursos logísticos, recursos orçamentários e de segurança da informação, que possam comprometer o atingimento dos objetivos estratégicos, a imagem e a missão da ANS.

CAUSA	EVENTO OU RISCO	CONSEQUÊNCIA
=	=	=
FONTE DE RISCO	INCIDENTE	IMPACTA UM OBJETIVO
+	+	+
VULNERABILIDADE	IRREGULARIDADE	GANHO/PERDA

Importante atentar para a leitura a ser feita desse painel:

- Uma ou mais causas geram um risco;
- Um risco gera um ou mais efeitos; e
- Uma causa **não** gera um efeito diretamente.
- Uma vez que qualquer uma das causas identificadas pode gerar um risco, esse risco concretizado pode gerar qualquer um dos efeitos listados.

CAUSAS

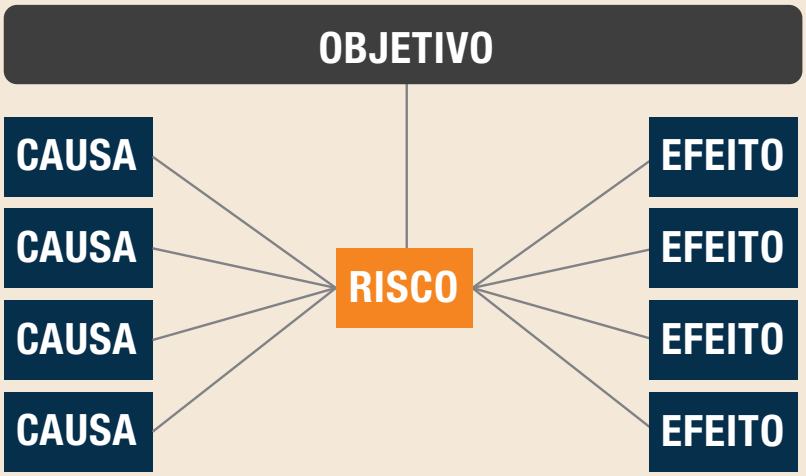
Para as fontes de riscos que são parte do processo de trabalho, considere as vulnerabilidades associadas a elas que, se ocorrerem, podem afetar o atingimento dos objetivos. Fontes de riscos associadas a vulnerabilidades são causas de riscos.

Exemplos de vulnerabilidades associadas a fontes de riscos:

FONTE	VULNERABILIDADE	FONTE	VULNERABILIDADE
PESSOAS	- Em número insuficiente - Sem capacitação - Perfil inadequado - Desmotivadas	**INFRAESTRUTURA ORGANIZACIONAL**	- Falta de clareza quanto as funções e responsabilidades - Deficiências nos fluxos de informação e comunicação - Centralização de responsabilidades - Delegações exorbitantes
PROCESSOS	- Mal concebidos - Sem manual ou instruções formalizadas - Ausência de segregação de funções	**INFRAESTRUTURA FÍSICA**	- Localização Inadequada - Instalações ou layout inadequados - Inexistência de controles de acesso físico
SISTEMAS	- Obsoletos - Sem integração - Sem manuais de operação - Inexistência de controles de acesso lógico/backups	**TECNOLOGIA**	- Técnica de produção ultrapassada/ produto obsoleto - Inexistência de investimentos em pesquisa e desenvolvimento - Tecnologia sem proteção de patentes - Processo produtivo sem proteção contraespionagem

"Eventos externos" também são consideradas fontes de riscos que, caso surjam vulnerabilidades associadas a eles e formem uma causa de risco, via de regra, não se tem o gerenciamento da situação para reduzir sua probabilidade de ocorrência. Independentemente disso, devemos considerar esses eventos externos na identificação das causas .

Durante as sessões de “brainstorming” é possível que os eventos listados possam ser tratados como causas do risco, ou mesmo como efeito. A dica é agrupar todos os eventos listados da seguinte forma:



Eventos que reúnam “fonte de risco” e “vulnerabilidade”: considere-os como **CAUSA** do risco. Em geral, esses eventos não atingem diretamente os objetivos. Eles geram um evento imediatamente após ocorrerem que, esse sim, afeta o objetivo

Eventos que ocorrerão se o objetivo não for atingido: considere-os como **EFEITOS** que serão percebidos em uma das 5 áreas de impactos descritas em nossa Matriz de Riscos[15].

Eventos que afetem diretamente o objetivo: considere-os como **RISCOS** propriamente ditos.

[15]Matriz de Riscos: Combinações possíveis de probabilidade e de impacto para definição do nível de risco em análise. As definições ali descritas servem de referencial para a alocação das probabilidades das causas e dos impactos dos efeitos, com o objetivo de reduzir a subjetividade inerente a um processo de análise qualitativa.

EFEITOS

A Matriz de Riscos, em sua dimensão IMPACTO, define 5 áreas para agrupar os tipos de impactos, conforme o quadro abaixo:

	ÁREAS DE IMPACTO				
	DESEMPENHO: INTERRUPÇÃO E RETOMADA	**LEGAL & COMPLIANCE**	**AMBIENTE DE TRABALHO SEGURANÇA**	**ATIVOS & FINANCEIRO**	**MÍDIA & REPUTAÇÃO**
VARIÁVEIS CONSIDERÁVEIS	- Interrompe operações ou entregas? - Afeta conclusão de programas ou projetos? - Quem é necessário para corrigir?	- Litígios ou multas como consequência? - Viola leis, normas ou regulamentos?	- Afeta pessoas? - Afeta patrimônio?	- Afeta ativos de infraestura? - Impactos do orçamento? - Falhas de acesso lógico ou físico?	- Afeta imagem da Agência? - Traz exposição na mídia? - Quem representa a Agência frente à mídia?

Neste momento, deverão ser descritos na tabela do item 3 os efeitos (consequências) dos riscos identificados em cada um dos objetivos podendo-se utilizar a Matriz acima como referência cruzando os riscos com as áreas de impacto.

D.4) CONTROLES ATUAIS

Processo/ Atividade:	
Objetivo:	
Risco:	
Causas:	
Efeitos:	
Controles Atuais:	PREVENIR CAUSAS
	DETECTAR EFEITOS.

Agora, passa-se às informações de controles atuais. Para cada causa e efeito listados, apontar, de acordo com o processo de trabalho descrito, o que é realizado para:

✓Prevenir as causas: identificar o que é feito para reduzir a probabilidade de ocorrência daquela causa.
✓Detectar os efeitos: identificar o que é feito para reduzir o impacto daquele efeito (eliminar o efeito por completo, ou a níveis aceitáveis, e no menor prazo possível).

Nessa etapa deve ser rigorosamente observada a descrição apenas dos controles existentes.

5.1.3 FINALIZANDO O QAR

Finalizado o quadro do item 3 do QAR, o Agente de Risco deve realizar uma revisão para se certificar que as informações presentes em todo o artefato estão de acordo com o processo de avaliação de riscos e conceitos relacionados. Em seguida, deve validar o QAR e eventuais anexos (fluxograma, atas de reunião, etc.) com o Gestor de Riscos e, após sua aprovação, encaminhar todo o material para a COARI.

Os riscos identificados na fase do Planejamento serão incluídos pela COARI no Mapa de Riscos, e serão atualizados com base no resultado apurado nos procedimentos do processo de Execução (análise, avaliação e, eventual, tratamento dos riscos).

5.2 PROCESSO DE EXECUÇÃO

O Processo de Execução tem como objetivos principais:

- ✓Analisar o nível de risco inerente[16] (probabilidade e impacto) e o grau de eficácia dos controles, de modo a definir o nível de risco residual[17].
- ✓Avaliar, comparando o nível de risco residual com o risco tolerável[18].
- ✓Definir o plano de tratamento, quando o nível de risco residual for maior que o risco tolerável.

[16] Risco Inerente: nível de risco ao qual se estaria exposto caso não houvesse nenhum controle implantado.
[17] Risco residual: probabilidade x impacto após considerar os controles atuais existentes ou o nível de risco existente considerando os controles.
[18] Risco tolerável: nível aceitável de risco para o que está sendo avaliado.

Assim, ao longo do processo de Execução, os riscos identificados no Planejamento terão seus elementos decompostos e analisados (causa, efeito, probabilidade, impacto, controles atuais, e os níveis de riscos inerente e residual), bem como será desenvolvida a comparação com os níveis de riscos pretendidos (nível de risco tolerável) e o tratamento a ser aplicado, sempre que cabível.

Durante as análises no processo de Execução, novos riscos podem eventualmente ser identificados. Nesse caso, deve-se retornar ao QAR, atualizar o quadro do item 3 com as informações, e a nova versão enviada para a COARI, apontando as alterações realizadas.

Nesse processo, utilizaremos o artefato chamado Avaliação de Riscos – AR (anexo II). A responsabilidade pelo preenchimento do artefato, pelas análises e pelos resultados apurados é do Gestor de Risco, que poderá ter o auxílio do Agente de Riscos para realizar os procedimentos, ou de outro servidor que esteja apto a realizar o processo de avaliação de riscos. Ressalta-se que o uso de terceiros para a condução desse processo não exime a responsabilidade do Gestor de Riscos que deverá validar o resultado final para encaminhamento à COARI.

Ainda que a responsabilidade por identificar o risco e definir a ação de tratamento seja do Gestor de Risco, o Agente de Riscos, conhecendo o contexto que está sendo avaliado (a "imersão" ocorreu durante o Planejamento), poderá (e deverá) ter um olhar crítico para garantir razoavelmente que os riscos, em especial os principais, foram identificados e estão sendo tratados de forma adequada.

Neste processo, o Agente de Riscos e o Gestor de Riscos podem utilizar, isolada ou conjuntamente, qualquer ferramenta ou técnica de avaliação de riscos, preferencialmente as sugeridas na norma ISO 31010 (What-If, FMEA, Checklist, Análise de Cenários, etc.). Se a opção da ferramenta a ser utilizada divergir da adotada nessa descrição, deverão procurar a COARI para apresentação de proposta para o desenvolvimento do trabalho e de apresentação dos resultados, para que a inovação no processo de avaliação de riscos possa ser submetida à aprovação.

5.2.1 INICIANDO A EXECUÇÃO

O AR reflete as informações obtidas no QAR, porém com viés de permitir a análise, avaliação e a definição de planos de tratamento, caso necessário. É uma planilha eletrônica dividida em três partes (“abas”): “RISCO”, “DADOS” e “ANÁLISE”.

Para cada risco e seus componentes, identificados na fase de Planejamento, serão preenchidas as duas primeiras abas, em conjunto, e gerada a terceira, a fim de atingir o objetivo primordial de analisar e avaliar o nível do risco, e definir os planos de tratamento, quando necessário.

A) PREENCHENDO A ABA RISCO

Essa aba tem praticamente a mesma formatação que o quadro dos riscos identificados no QAR. Essa disposição é proposital para facilitar a transferência do quadro do QAR (de um ambiente de “editor de texto”) para o AR (para um ambiente de “planilha eletrônica”). Cada risco identificado no QAR será transferido para uma aba “RISCO” diferente no AR.

Processo/Atividade:	
Objetivo:	

Risco 1:	
Causa:	
Efeito:	

Nível de Risco Tolerável:	

Assim, para o primeiro risco identificado no QAR, serão copiados a região da tabela onde consta o “Processo/Atividade” e o “Objetivo” para os respectivos campos no AR. Pode ser feito campo a campo ou os dois campos ao mesmo tempo, em ambos os casos através das teclas de atalho CTRL+C no QAR e CTRL+V no AR.

Devem ser copiadas apenas as células com os dados. Não incluir as células com títulos “Processo/Atividade” e “Objetivo” (apenas a parte indicada em vermelho).

Processo/Atividade:	Processo de Trabalho 1
Objetivo:	Objetivo "XPTO"

Novamente, utilizando as informações do QAR, serão copiadas as informações referentes a “Risco”, “Causas” e “Efeitos” para os respectivos campos no AR. Pode ser feito grupo a grupo ou em quatro grupos de informações ao mesmo tempo, através das teclas de atalho CTRL+C no QAR e CTRL+V no AR.

Devem ser apenas as células com os dados. Não incluir as células com os títulos “Risco”, “Causas” e “Efeitos” (apenas a parte indicada em vermelho).

Risco 1:	XXX RISCO 1 IDENTIFICADO XXX
Causa:	CAUSA A
	CAUSA B
	CAUSA C
Efeito:	EFEITO 1
	EFEITO 2
	EFEITO 3

Informa-se o nível de risco tolerável[19] para o objetivo que está sendo analisado. Deve-se escolher um dos 4 níveis de riscos que aparecem na lista suspensa da célula (“Baixo/Muito Baixo”, “Médio”, “Alto” ou “Extremo”). Ao informar o nível de risco tolerável, o Gestor de Riscos está sinalizando qual impacto é aceito nos objetivos em análise.

[19]Nível de risco tolerável: o nível de risco que está dentro de padrões considerados razoáveis..

Nível de Risco Tolerável:	Baixo / Muito Baixo

Extremo
Alto
Médio
Baixo / Muito baixo

Após transferidos todos os dados do QAR para o AR, e informado o nível de risco tolerável, passa-se para a aba “DADOS”.

B) PREENCHENDO A ABA “DADOS”

Esta aba estará com alguns campos preenchidos, automaticamente, de acordo com o que foi informado na aba “RISCO”.

Processo/Atividade:	PROCESSO DE TRABALHO 1
Objetivo:	XPTO

Risco 1:	XXX RISCO 1 IDENTIFICADO XXX								
CAUSA	CAUSA A	CAUSA B	CAUSA C						
PROBABILIDADE INERENTE									
CONTROLES ATUAIS									
PROBABILIDADE RESIDUAL									
EFEITO	EFEITO 1	EFEITO 2	EFEITO 3						
IMPACTO INERENTE									
CONTROLES ATUAIS									
IMPACTO RESIDUAL									
GERAR ANÁLISE									

Nível de risco é o resultado da probabilidade de uma causa vir a ocorrer *versus* o impacto de um efeito. De acordo com a Política de Gestão de Riscos da ANS, existem 5 classificações de níveis de riscos: Extremo, Alto, Médio, Baixo e Muito Baixo. Para fins de simplificar a apresentação do nível de risco apurado, considerando as definições de cada um deles, optou-se por considerar os níveis Baixo (de impactos pequenos) e Muito Baixo (de impactos mínimos) como um resultado único de praticamente mesma intensidade e que demandaria a mesma priorização no tratamento.

Níveis de riscos resultantes da Matriz de Riscos:

- ✓**Extremo**: Aqueles caracterizados por riscos associados à paralisação de operações, atividades, projetos, programas ou processos da ANS, causando IMPACTOS IRREVERSÍVEIS nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas;
- ✓**Alto**: Aqueles caracterizados por riscos associados à interrupção de operações, atividades, projetos, programas ou processos da ANS, causando IMPACTOS DE REVERSÃO MUITO DIFÍCIL nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas;
- ✓**Médio**: Aqueles caracterizados por riscos associados à interrupção de operações ou atividades da ANS, de projetos, programas ou processos, causando IMPACTOS SIGNIFICATIVOS nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas, porém recuperáveis; e
- ✓**Baixo/Muito Baixo**: Aqueles caracterizados por riscos associados à degradação de operações, atividades, projetos, programas ou processos da ANS, causando IMPACTOS MÍNIMOS OU PEQUENOS nos objetivos relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas.

Reforça-se que, por definição na Política, “Baixo” representa impactos pequenos nos objetivos e “Muito Baixo”, impactos mínimos. Mas os dois níveis, ao final, serão tratados como um resultado único

Tanto as análises das probabilidades, quanto dos impactos são julgamentos subjetivos. A fim de diminuir essa subjetividade, é fundamental se utilizar dos conceitos existentes na Matriz de Riscos.

PROBABILIDADE				
RARO	**IMPROVÁVEL**	**POSSÍVEL**	**PROVÁVEL**	**QUASE CERTO**
Este evento pode ter acontecido anteriormente na organização ou em organizações similares. Entretanto, na ausência de outras informações ou circunstâncias excepcionais, não seria esperado que ocorresse na organização no futuro próximo	O evento não ocorre de maneira frequente na organização ou organizações similares. Os controles atuais e as circuntâncias sugerem que a ocorrência seria considerada altamente não usual	O evento pode ter ocorrido ocasionalmente na organização ou em organizações similares. Os controles atuais ou as circunstâncias sugerem que há uma possibilidade plausível de ocorrência	Este evento pode ocorrer regularmente na organização ou em organizações similares. Com os controles atuais ou circunstâncias, pode-se esperar que ocorra ao longo de 1 ano	Este evento ocorre frequentemente na organização ou com os controles ou circunstâncias. Sua ocorrência é esperada
O evento pode ocorrer apenas em circunstâncias muito exepcionais	O evento pode ocorrer em algum momento, mas é improvável	o evento provavelmente ocorrerá em algumas circunstâncias	O evento provavelmente ocorrerá na maioria das circunstâncias	É esperado que o evento ocorra na maioria da circunstâncias

	ÁREAS DE IMPACTO				
	DESEMPENHO: INTERRUPÇÃO E RETOMADA	**LEGAL & COMPLIANCE**	**AMBIENTE DE TRABALHO SEGURANÇA**	**ATIVOS & FINANCEIRO**	**MÍDIA & REPUTAÇÃO**
VARIÁVEIS CONSIDERÁVEIS	- Interrompe operações ou entregas? - Afeta conclusão de programas ou projetos? - Quem é necessário para corrigir?	- Litígios ou multas como conseguência? - Viola leis, normas ou regulamentos?	- Afeta pessoas? - Afeta patrimônio?	- Afeta ativos de infraestura? - Impactos do orçamento? - Falhas de acesso lógico ou físico?	- Afeta imagem da Agência? - Traz exposição na mídia? - Quem representa a Agência frente à mídia?

Dessa forma, considerando o julgamento a ser realizado pelo Gestor do Risco, as informações a serem preenchidas nessa aba serão:

Com relação às CAUSAS: as probabilidades inerentes de cada uma das causas listadas, ou seja, qual a chance dessa causa vir a ocorrer se nada for feito para preveni-la. Cada causa possui abaixo um campo chamado "PROBABILIDADE INERENTE"[20], o qual deverá ser preenchido selecionando a lista disponível ("Raro", "Improvável", "Possível", "Provável" ou "Quase Certo").

Na sequência, descrever os controles atuais que hoje modificam essa probabilidade, e que foram descritos no QAR.

Por fim, com base no julgamento da eficácia desses controles, informar qual a probabilidade residual. Para definir a probabilidade ajustada ou residual, a leitura a ser feita é: **A eficácia do "controle ALFA" sobre a "causa A" leva a probabilidade inerente "3 – Possível" para qual probabilidade ajustada?** Então, é escolhida na lista suspensa ("Raro", "Improvável", "Possível", "Provável" ou "Quase Certo") que existe no campo chamado "PROBABILIDADE RESIDUAL"[21] qual a nova probabilidade.

[20]Probabilidade inerente a chance de algo acontecer antes de serem aplicados os controles existentes.

[21]Probabilidade ajustada ou residual: o quanto de probabilidade estima-se que permanece, mesmo com a aplicação dos controles atuais.

CAUSA	CAUSA A	CAUSA B	CAUSA C		
PROBABILIDADE INERENTE	3-POSSÍVEL	3-PROVÁVEL	3-POSSÍVEL		
CONTROLES ATUAIS	CONTROLE ALFA	CONTROLE BETA	CONTROLE ALFA		
PROBABILIDADE RESIDUAL	2-IMPROVÁVEL				

1 - Raro
2 - Improvável
3 - Possível
4 - Provável
5 - Quase Certo

1 - Raro
2 - Improvável
3 - Possível
4 - Provável
5 - Quase Certo

Com relação aos EFEITOS: o impacto inerente para cada efeito identificado, ou seja, qual será o nível do impacto se esse risco se concretizar e nada for feito para detectar o efeito. Cada efeito possui abaixo um campo chamado "IMPACTO INERENTE"[22] o qual deverá ser preenchido selecionando a lista disponível ("Muito Baixo", "Baixo", "Médio", "Alto" ou "Extremo").

Na sequência, descrever os controles atuais que hoje modificam esse impacto, e que foram descritos no QAR.

Por fim, com base no julgamento da eficácia desses controles, informar qual o impacto residual. Para definir o impacto ajustado ou residual, a leitura a ser feita é: **A eficácia do "controle CHARLIE" sobre o "efeito 1" leva o impacto inerente "8 – Alto" para qual impacto ajustado?** Então, é escolhida na lista suspensa ("Muito Baixo", "Baixo", "Médio", "Alto" ou "Extremo") que existe no campo chamado "IMPACTO RESIDUAL"[23] qual o novo impacto.

[22] Impacto inerente: resultado de um evento, antes da aplicação dos controles existentes, que afeta os objetivos.

[23] Impacto ajustado ou residual: o quanto de impacto estima-se que permanece mesmo com a aplicação dos controles atuais.

EFEITO	EFEITO 1	EFEITO 2	EFEITO 3		
IMPACTO INERENTE	8-ALTO	8-ALTO	4-MÉDIO		
CONTROLES ATUAIS	CONTROLE CHARLIE	CONTROLE DELTA	CONTROLE DELTA		
IMPACTO RESIDUAL	4-MÉDIO				

1 - Muito Baixo
2 - Baixo
3 - Médio
4 - Alto
5 - Extremo

Caso não tenham sido identificados controles atuais sobre as causas e/ou os efeitos, a probabilidade e/ou o impacto inerente não sofrerá qualquer alteração, pois se não existem controles atuais que gerenciem as causas e/ou os efeitos, logo, a classificação residual permanece a mesma com relação à inerente.

Após o preenchimento de todas as probabilidades e impactos inerentes, os controles atuais sobre as causas e efeitos, e as probabilidades e impactos residuais, pode-se clicar no botão “GERAR ANÁLISE”.

É importante que todos as informações sobre as causas e os efeitos listados estejam preenchidas para não dar erro na análise que será gerada.

Processo/Atividade:	PROCESSO DE TRABALHO 1
Objetivo:	XPTO

Risco 1:	XXX RISCO 1 IDENTIFICADO XXX								
CAUSA	CAUSA A	CAUSA B	CAUSA C						
PROBABILIDADE INERENTE	3-POSSÍVEL	3-PROVÁVEL	3-POSSÍVEL						
CONTROLES ATUAIS	CONTROLE ALFA	CONTROLE BETA	CONTROLE ALFA						
PROBABILIDADE RESIDUAL	2-IMPROVÁVEL								
EFEITO	EFEITO 1	EFEITO 2	EFEITO 3						
IMPACTO INERENTE	8-ALTO	8-ALTO	4-MÉDIO						
CONTROLES ATUAIS	CONTROLE CHARLIE	CONTROLE DELTA	CONTROLE DELTA						
IMPACTO RESIDUAL	4-MÉDIO								

GERAR ANÁLISE

C) PREENCHENDO A ABA "ANÁLISE"

Esta aba estará com alguns campos preenchidos, automaticamente, de acordo com o que foi informado e analisado na aba "DADOS".

Conforme comentado anteriormente, não há uma relação direta entre causa e efeito, dado que uma causa pode gerar um risco. E esse risco concretizado pode gerar qualquer um dos efeitos.

Assim, todas as combinações possíveis de causa e efeito também estarão preenchidas nessa aba, em ordem decrescente (do pior resultado para o melhor), do resultado da PROBABILIDADE x IMPACTO, de acordo com o definido na matriz de riscos adotada pela ANS. Em um primeiro momento, pode-se dizer, equivocadamente, que um efeito ocorreu em função de uma causa. Mas o que efetivamente pode ocorrer é uma causa gerar o risco. Esse risco concretizado é que vai gerar efeitos, e que pode ser qualquer um deles.

Processo/Atividade:	PROCESSO DE TRABALHO 1
Objetivo:	OBJETIVO "XPTO"

Risco 1:	XXX RISCO 1 IDENTIFICADO XXX

			NÍVEL DE RISCO RESIDUAL	NÍVEL DE RISCO TOLERÁVEL	PLANO DE TRATAMENTO	RESPONSÁVEL	PRAZO (MM/AAA)
CAUSA	CAUSA A	2- IMPROVÁVEL	MÉDIO	BAIXO / MUITO BAIXO			
EFEITO	EFEITO 1	4- MÉDIO					
CAUSA	CAUSA A	2- IMPROVÁVEL	MÉDIO	BAIXO / MUITO BAIXO			
EFEITO	EFEITO 2	4- MÉDIO					
CAUSA	CAUSA B	2- IMPROVÁVEL	MÉDIO	BAIXO / MUITO BAIXO			
EFEITO	EFEITO 1	4- MÉDIO					
CAUSA	CAUSA B	2- IMPROVÁVEL	MÉDIO	BAIXO / MUITO BAIXO			
EFEITO	EFEITO 2	4- MÉDIO					
CAUSA	CAUSA C	2- IMPROVÁVEL	MÉDIO	BAIXO / MUITO BAIXO			
EFEITO	EFEITO 1	4- MÉDIO					
CAUSA	CAUSA C	2- IMPROVÁVEL	MÉDIO	BAIXO / MUITO BAIXO			
EFEITO	EFEITO 2	4- MÉDIO					
CAUSA	CAUSA A	2- IMPROVÁVEL	MÉDIO	BAIXO / MUITO BAIXO			
EFEITO	EFEITO 3	4- MUITO BAIXO					
CAUSA	CAUSA B	2- IMPROVÁVEL	MÉDIO	BAIXO / MUITO BAIXO			
EFEITO	EFEITO 3	4- MUITO BAIXO					
CAUSA	CAUSA C	2- IMPROVÁVEL	MÉDIO	BAIXO / MUITO BAIXO			
EFEITO	EFEITO 3	4- MUITO BAIXO					

O nível de risco residual é um campo calculado automaticamente com base nas premissas e definições existentes na Matriz de Riscos e nas informações prestadas e analisadas na aba "DADOS", considerando as combinações entre probabilidades e impactos. O nível de risco tolerável reflete a informação prestada na aba "RISCO".

MATRIZ DE RISCOS: PROBABILIDADE X IMPACTO

		PROBABILIDADE				
		RARO	IMPROVÁVEL	POSSÍVEL	PROVÁVEL	QUASE CERTO
IMPACTO	EXTREMO	MÉDIO	ALTO	EXTREMO	EXTREMO	EXTREMO
	ALTO	MÉDIO	MÉDIO	ALTO	ALTO	EXTREMO
	MÉDIO	BAIXO/ MUITO BAIXO	MÉDIO	MÉDIO	MÉDIO	ALTO
	BAIXO	BAIXO/ MUITO BAIXO	BAIXO/ MUITO BAIXO	MÉDIO	MÉDIO	MÉDIO
	MUITO BAIXO	BAIXO/ MUITO BAIXO	BAIXO/ MUITO BAIXO	BAIXO/ MUITO BAIXO	BAIXO/ MUITO BAIXO	BAIXO/ MUITO BAIXO

C1) AVALIANDO: "RESIDUAL" VERSUS "TOLERÁVEL"

A avaliação do risco significa comparar o quanto ainda permanece de risco, após a aplicação dos controles atuais, com relação ao nível de risco aceitável, para decidir se será necessário tratar a situação.

			NÍVEL DE RISCO RESIDUAL	NÍVEL DE RISCO TOLERÁVEL	PLANO DE TRATAMENTO	RESPONSÁVEL	PRAZO (MM/AAA)
CAUSA	CAUSA A	2- IMPROVÁVEL	MÉDIO	BAIXO / MUITO BAIXO			
EFEITO	EFEITO 1	4- MÉDIO					

Por via de regra, se o nível de risco residual está acima do tolerável, ou seja, os controles atuais não são suficientes para levar o risco a níveis aceitáveis, deve-se definir um tratamento para ajustar a situação. Se o Gestor de Risco, nessa situação, decidir por não implementar um tratamento deverá justificar no próprio campo "Plano de Tratamento" a decisão de aceitar níveis de risco acima do que foi definido como aceitável.

C.2) DEFININDO O TRATAMENTO DO RISCO

O tratamento do risco, será realizado quando o nível de risco residual estiver acima do nível de risco tolerável e será aplicado sobre as causas e os efeitos, de modo a reduzir a probabilidade e o impacto ajustados, respectivamente.

			NÍVEL DE RISCO RESIDUAL	NÍVEL DE RISCO TOLERÁVEL	PLANO DE TRATAMENTO	RESPONSÁVEL	PRAZO (MM/AAA)
CAUSA	CAUSA A	2- IMPROVÁVEL	MÉDIO	BAIXO / MUITO BAIXO			
EFEITO	EFEITO 1	4- MÉDIO					

Lembre-se de que controles podem REDUZIR ou COMPARTILHAR a probabilidade e o impacto. Mudanças nos processos de trabalho, definição e aplicação de políticas, práticas ou quaisquer outras ações que modifiquem as probabilidades e os impactos são controles e devem ser considerados. É preciso estar atento, pois essas modificações podem criar riscos ou modificar outros riscos que não eram aqueles sob tratamento.

As demais opções com relação ao tratamento envolvem EVITAR (descontinuar o processo ou atividade que dá origem ao risco), ELIMINAR (remover a fonte de risco), ACEITAR ou AUMENTAR o risco, nas quais o Gestor de Risco deverá justificar a medida adotada.

O plano de tratamento será aplicado às causas e/ou aos efeitos, preferencialmente, que tiverem mais chances de serem reduzidos. No exemplo acima, recomenda-se pensar em controles para detectar e corrigir EFEITO 1, visto que este tem mais chances de ter o impacto reduzido de Médio para Baixou ou para Muito Baixo que a CAUSA A, onde a probabilidade poderia apenas passar de Improvável para Raro.

CONSIDERAÇÕES FINAIS

O manual abordou o processo de avaliação de riscos de acordo com as fases “Planejamento” e “Execução”.

A partir de uma narrativa didática e explicativa, cada etapa foi descrita para auxiliar, sistematizar e padronizar os procedimentos intrínsecos à implementação da avaliação de riscos nos processos consoante a metodologia adotada pela ANS .

Por fim, ressalta-se o compromisso de constante adequação deste manual às ações de desenvolvimento e melhoria associadas à Política de Gestão de Riscos dessa instituição.

ANEXO I – QAR

COORDENAÇÃO DE AVALIAÇÃO DE RISCO

Questionário de Avaliação de Riscos

Processo:

N° do Processo
NNN/2018/ÓRGÃO

Gestor:

Agente de riscos:

Data:

1. **Descrição do Processo.**
   [Descreva o fluxo de trabalho, considerando:
   - *Os objetivos do processo de trabalho avaliado*
   - *As etapas, os procedimentos e as atividades que compõem o processo*
   - *Os recursos humanos, materiais e de sistemas de informação requeridos para a execução do processo*
   - *As infraestruturas físicas envolvidas (exemplos: localização, instalações e controle de acesso físico)*
   - *A estrutura organizacional relacionada ao processo (exemplos: funções e responsabilidades regimentais, fluxos de informação e comunicação, centralização e delegação de responsabilidades)*
   - *O volume de transações mensal ou em outra base temporal*
   - *Os eventos externos que, ainda que não sejam gerenciáveis, tenham impactos sobre o processo]*

2. **Quais os produtos/serviços resultantes desse processo e a quem se destina?**

3. **Identificação dos objetivos e riscos do processo/atividade.**
   - ***Risco** é a possibilidade de que um evento ocorra e afete, positivamente ou negativamente, os objetivos (uma ou várias causas que podem gerar um evento que, quando concretizado, pode gerar um ou mais efeitos)*
   - ***Causa** é um elemento associado a uma vulnerabilidade, com potencial originar o risco*
   - ***Efeito** é o resultado (consequência) de um evento que afeta os objetivos.*
   - ***Controle atual** é a medida – qualquer processo, política, dispositivo, prática ou outras ações – que está modificando o risco (suas causas e seus efeitos)*

Processo /Atividade:	
Objetivo:	

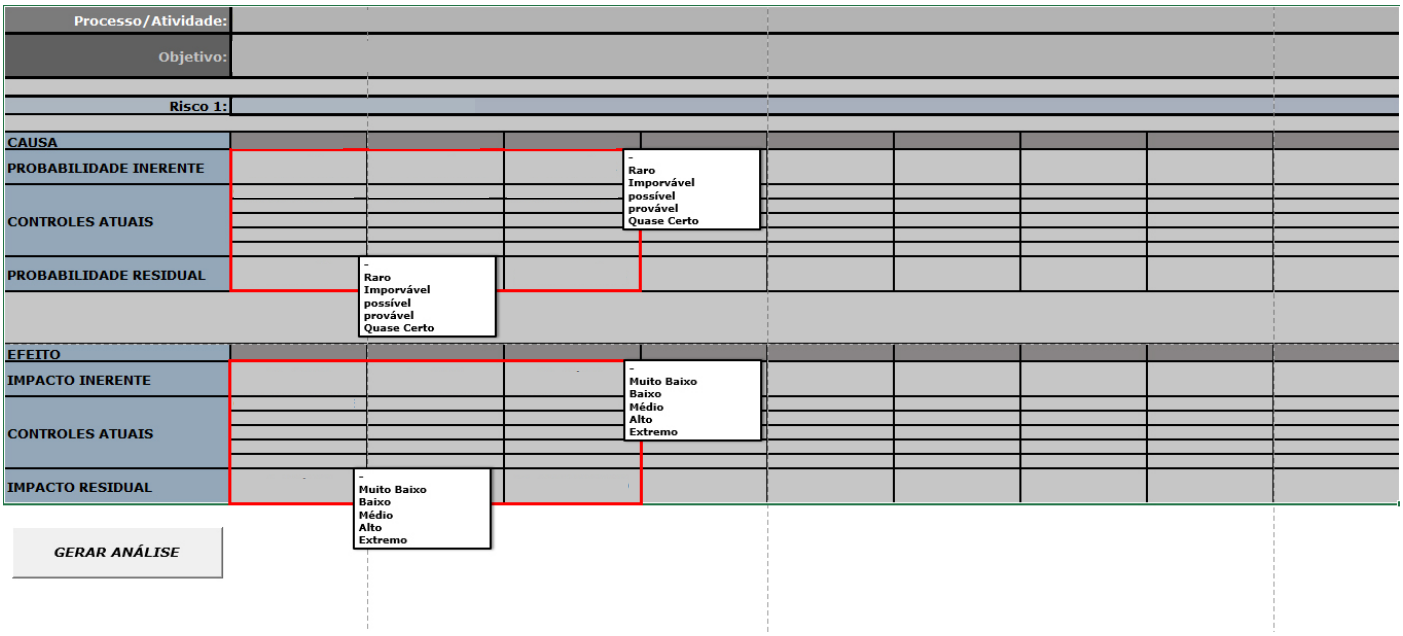
Risco:	
Causas	
Efeitos	
Controles Atuais	

ANEXO II – AR

Aba RISCO

Processo/Atividade:	
Objetivo:	
Risco 1:	
Causa:	
Efeito:	
Nível de Risco Tolerável	

Aba Dados


Processo/Atividade:
Objetivo:
Risco 1:
CAUSA
PROBABILIDADE INERENTE
CONTROLES ATUAIS
PROBABILIDADE RESIDUAL
-
Raro
Imporvável
possível
provável
Quase Certo
-
Raro
Imporvável
possível
provável
Quase Certo
EFEITO
IMPACTO INERENTE
CONTROLES ATUAIS
IMPACTO RESIDUAL
-
Muito Baixo
Baixo
Médio
Alto
Extremo
-
Muito Baixo
Baixo
Médio
Alto
Extremo
GERAR ANÁLISE

Aba Análise

Processo ou Atividade:							
Objetivo:							
Risco 1:							
			Nível de Risco Residual	Nível de Risco Tolerável	Plano de Tratamento	Responsável	Prazo (mm/aaaa)
Causa							
Efeito							
Causa							
Efeito							
Causa							
Efeito							
Causa							
Efeito							
Causa							
Efeito							
Causa							
Efeito							
Causa							
Efeito							
Causa							
Efeito							
Causa							
Efeito							

BIBLIOGRAFIA

AGÊNCIA NACIONAL DE SAÚDE SUPLEMENTAR (Brasil). **Mapeamento de processos na ANS**: manual de orientação para o mapeamento de processos “as is”. Rio de Janeiro: ANS, 2016.

_____. **Resolução administrativa n.º 60, de 15/07/2014.** Política de gestão de riscos. Rio de Janeiro: ANS, 2017.

_____. **Resolução administrativa nº 67, de 11/05/2017**. Comitê de Governança, Riscos e Controles. Rio de Janeiro: ANS, 2017.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ISO 31000 – Gestão de Riscos – Diretrizes e princípios.** Rio de Janeiro: ABNT, 2018.

_____**. ISO Guia 73:2009 – Gestão de Riscos – Vocabulário.** Rio de Janeiro: ABNT, 2009.

_____. **ISO/IEC 31010:2009 – Gestão de Riscos – Técnicas para o processo de avaliação de riscos.** Rio de Janeiro: ABNT, 2009.

BRASIL. Ministério do Planejamento, Orçamento e Gestão; BRASIL. Controladoria-Geral da União. **Instrução Normativa Conjunta CGU/MP n.º 01, de 10/05/2016.** Dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal. Brasília, DF: MPOG, CGU, 2016.

COMMITTEE OF SPONSORING ORGANIZATIONS OF TREADWAY COMMISSION. **Internal control:** integrated framework: executive summary. [S.l.]: COSO, 2013. Disponível em: <https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf>. Acesso em: 14 set. 2017.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **Risk management - Principles and guidelines,** 2009. Disponível em: <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en>. Acesso em: 20 set. 2017.

PARA MAIS INFORMAÇÕES E OUTROS ESCLARECIMENTOS, ENTRE EM CONTATO COM A ANS.
VEJA ABAIXO NOSSOS CANAIS DE ATENDIMENTO:

Disque ANS
0800 701 9656

Central de Atendimento
www.ans.gov.br

Atendimento pessoal 12 Núcleos da ANS.
Acesse o portal e confira os endereços.

Atendimento exclusivo para deficientes auditivos
0800 021 2105

Use a opção do código para ir ao portal da ANS

ans.reguladora
@ANS_reguladora
ansreguladora oficial
company/ans_reguladora

ANS Agência Nacional de Saúde Suplementar

MINISTÉRIO DA SAÚDE

GOVERNO FEDERAL