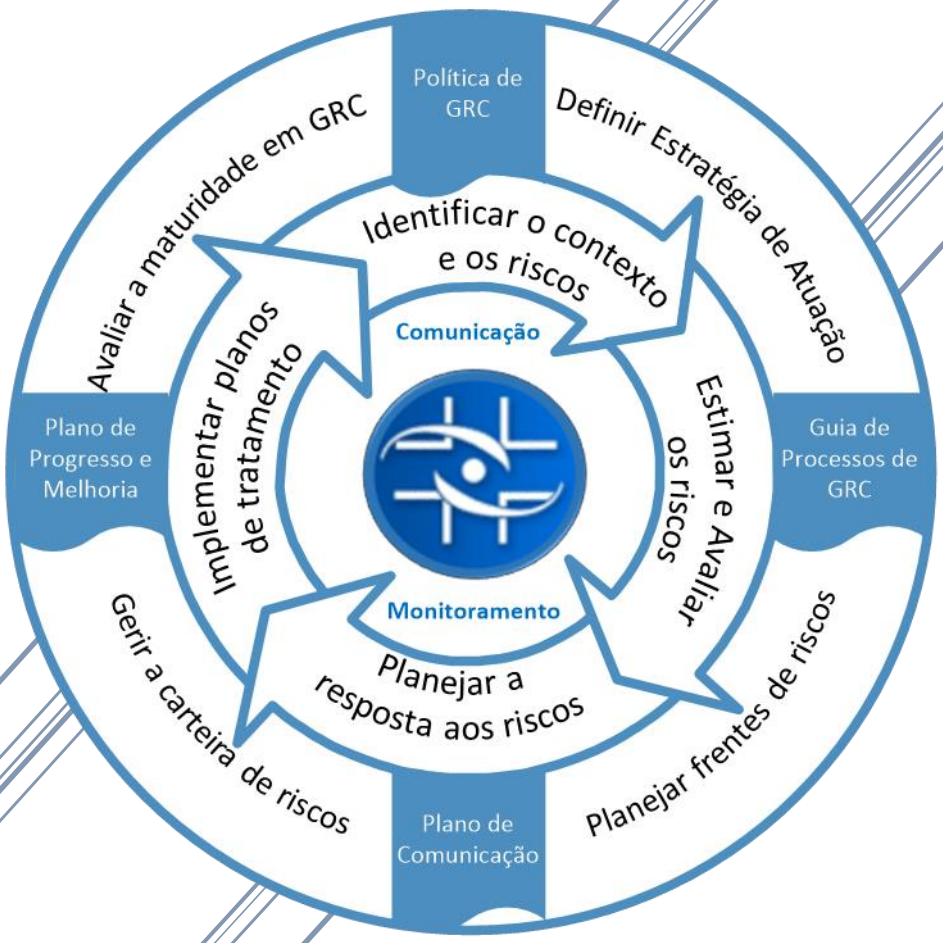
Gestão de Riscos Corporativos

Guia Prático de GRC



ANVISA

2018

Expediente

Diretor-Presidente
William Dib

Diretores
Alessandra Bastos Soares
Fernando Mendes Garcia Neto
Renato Alencar Porto

Adjuntos de Diretores
Patrícia Tiana Pacheco Lamarão
Bruno Araújo Rios
Meiruze Sousa Freitas
Rogério Luiz Zeraik Abdalla

Chefe de Gabinete
Marcus Aurélio Miranda de Araújo

Assessor-Chefe de Planejamento
Gustavo Henrique Trindade da Silva

Organização
Wildenildo Oliveira dos Santos
Gustavo de Freitas Alves

Colaboração
Mary Anne Fontenele Martins
Marcelo Ivo Silva de Lima
Luiz Henrique Alves da Cunha

Revisão
Patricia Fernanda Toledo Barbosa
Marcelo Ivo Silva de Lima
Fabiano Ferreira de Araújo

Equipe Técnica
Patricia Fernanda Toledo Barbosa
Wildenildo Oliveira dos Santos
Fabiano Ferreira de Araújo
Mary Anne Fontenele Martins
Marcelo Ivo Silva de Lima
Atila Coelho Correa
Luiz Henrique Alves da Cunha

Consultor Técnico
Gustavo de Freitas Alves

Sumário

Apresentação

Na Anvisa, a Gestão de Riscos Corporativos (GRC) atende às recomendações da Controladoria Geral da União (CGU) e aos requisitos da INC nº 01/2016 MPDG e CGU; além de estar alinhada aos ditames do Art. 17 do Decreto 9.203, de 20 de novembro de 2017, da Presidência da República. Para atender às recomendações dos órgão de controle foi instituída a Política de Gestão de Riscos Corporativos da Anvisa, por meio de Portaria Anvisa n° 854 , de 30 de maio de 2017, que estabelece os objetivos, princípios, conceitos, diretrizes, atribuições e responsabilidades a serem observadas para a execução da gestão de riscos corporativos, bem como orienta quanto à identificação, análise, avaliação, tratamento, monitoramento e comunicação dos riscos corporativos na Agência.

A Política de Gestão de Riscos é a declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos e, portanto, pilar central do desenvolvimento do processo de gerenciamento de riscos que subsidia o processo de tomada de decisão na instituição.

Este Guia objetiva favorecer a execução da GRC no âmbito tático e operacional da Agência, permitindo que todo e qualquer agente de risco ou gerente de unidade organizacional tenha a capacidade de identificar e gerir seus riscos de forma independente e sistemática, com a mesma qualidade do gerenciamento feito por especialistas no assunto; por meio da exposição ordenada dos passos do processo de Gestão de Riscos Corporativos da Anvisa.

O Guia é composto de contextualização da GRC na Anvisa, governança, método, processo e ferramentas que apoiaram às unidades organizacionais na identificação, análise, avaliação, registro, tratamento e comunicação dos eventos de risco sob suas respectivas responsabilidades; permitindo que a média gestão possa compartilhar de suas inquietações com as instâncias decisórias pertinentes, fortalecendo os controles internos da gestão e contribuindo para a melhoria do desempenho institucional.

Introdução

Na última década, a gestão de riscos vem se transformando em um processo estratégico e de vital importância para as organizações públicas. Trata-se de uma abordagem que privilegia o alcance de resultados em qualquer organização, de forma que sua mitigação, por meio de controles apropriados, tem potencial de garantir maior eficácia da gestão pública.

Nos termos da nossa política de GRC, em seu art. 4º, inciso XXII, **risco** é efeito da **incerteza**, evento capaz de afetar positivamente (oportunidade) ou negativamente (ameaça) os objetivos, processos de trabalho, programas e projetos nos níveis estratégico, tático ou operacional. Os riscos surgem da incerteza natural dos cenários econômico, político e social e podem se apresentar como desafios ou oportunidades, na medida em que dificultem ou facilitem o alcance dos objetivos organizacionais (ABNT, 2009).

O instrumento de governança para lidar com a incerteza é a Gestão de Riscos Corporativos (GRC). A gestão de riscos permite tratar com eficiência as incertezas, seja pelo aproveitamento das oportunidades, seja pela redução da probabilidade e/ou impacto de eventos negativos, a fim de melhorar a capacidade de gerar valor e fornecer garantia razoável do cumprimento dos seus objetivos.

Destaque-se que a GRC pode ser aplicada a uma ampla gama de atividades, incluindo estratégias, decisões, operações, processos, programas, projetos, produtos, serviços e, suas etapas, podem servir a qualquer tipo de risco, independentemente de sua natureza, quer tenha consequências positivas ou negativas para o cumprimento da missão institucional.

A aplicação da metodologia de Gestão de Riscos Corporativos atende, portanto, à recomendação do TCU e da CGU, para que a Anvisa adote medidas para gerenciar seus riscos institucionais, implementando uma política e um processo de gestão de riscos, conforme o Acórdão nº 673/2015, bem como o estabelecido na Instrução Normativa Conjunta n.º 1 (MPOG/CGU), de 10 de maio de 2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal (BRASIL, 2016).

Governança em GRC:

O maior desafio para a implantação de um processo de GRC consiste em conseguir integrar adequadamente o processo aos instrumentos de governança e controle da organização. Assim, com fins de superar este entrave, a governança de GRC na Anvisa contempla duas principais direções: a primeira top down, em que as informações circulam de cima para abaixo, definindo objetivos, prioridades, procedimentos e metodologias; e a segunda bottom up, de baixo para cima, escalando decisões, responsabilidade e comunicando resultados; em consonância com o previsto na Portaria Anvisa nº 854/2017, em seu Art. 5º, onde se delimita o direcionamento e os níveis de execução da GRC na Agência, como segue:

> *Art. 5º O direcionamento para a implantação da gestão de riscos corporativos é dado pela Diretoria Colegiada da Anvisa (Dicol) e gerenciado nos três níveis de gestão, de forma integrada, devendo ser assegurados meios para que esse processo ocorra.*

Em seu Capítulo III, Artigo 9º ao 13, a Política de GRC da Anvisa atribui e descreve as responsabilidades segundo a estrutura organizacional da Agência, em um modelo de governança capaz de integrar o processo decisório, o de gestão tático-operacional e o processo de GRC, apontando atribuições e reponsabilidades ao Diretor-presidente, para à Diretoria Colegiada, ao Comitê de Riscos, à Secretaria Executiva do Comitê de Riscos e aos Gestores das Unidades Organizacionais; bem como a direção da informação, uma vez que cabe às instâncias decisórias definir objetivos e prioridades, à secretaria executiva apoiar o processo e os envolvidos, e ao gestores das unidades organizacionais aplicar o processo, com fins de manter os riscos identificados em patamar aceitável, além de comunicar os resultados às instâncias decisórias e de monitoramento.

A Figura 1, a seguir, traz uma representação sintética do modelo de governança da gestão de risco na Anvisa e as respectivas atribuições dos diversos atores envolvidos:

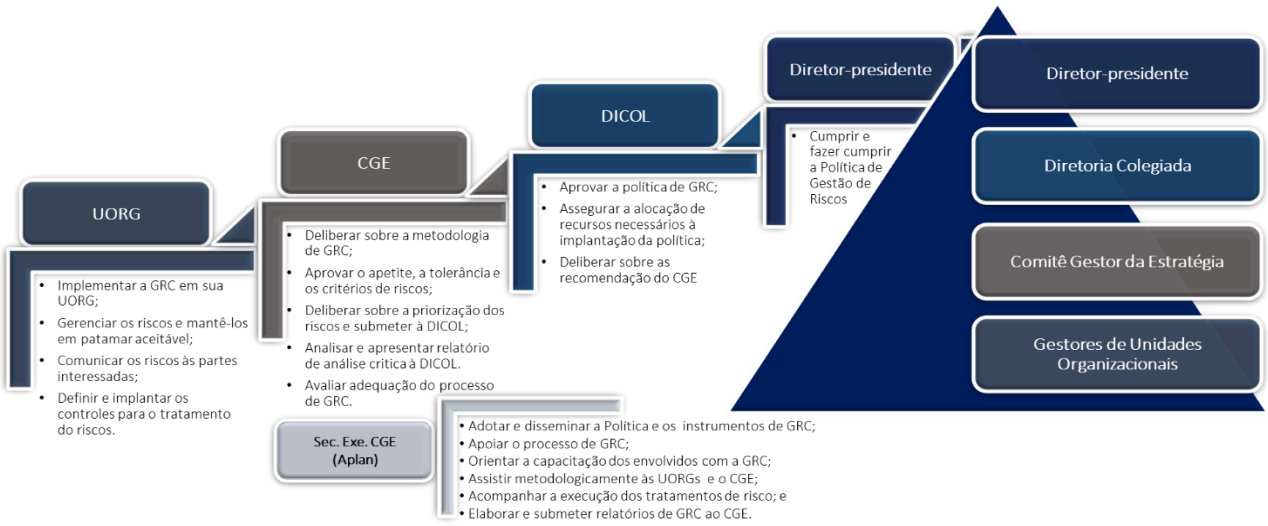


Figura 1 - Governança da GRC Anvisa

Fonte: Assessoria de Planejamento - Aplan/Anvisa

Logo, a responsabilidade por estabelecer, manter, monitorar e aperfeiçoar os controles internos da gestão é da alta administração, sem prejuízo das responsabilidades dos gestores das unidades organizacionais nos seus respectivos âmbitos de atuação.

Ainda, conforme o modelo de três linhas de defesa previstos pelo IIA (The Institute of Interna Auditors), o controle da gerência de cada unidade organizacional representa a primeira linha de defesa no gerenciamento de riscos, as diversas funções de controle de riscos e supervisão de conformidade estabelecidas pela gerência são a segunda linha de defesa enquanto que a avaliação independente, ação de auditoria, é a terceira. Cada uma dessas três "linhas" desempenha um papel distinto dentro da estrutura mais ampla de governança da organização.

A Figura 2, a seguir, traz a representação sintética do modelo proposto pelo IIA.

Figura 2 – Modelo Três Linhas de Defesa, segundo o IIA
Fonte: Adaptado do Guidance on the 8th EU Company Law Directive da ECIIA/FERMA, artigo 41

Portanto, as ações e medidas de controle implantadas pelos gestores das unidades organizacionais representam a primeira linha de defesa no gerenciamento de riscos da Anvisa, enquanto que o as ações de supervisão e monitoramento do Comitê Gestor da Estratégia (CGE), instância que assimilou as atribuições do Comitê de Riscos da Anvisa, conforme Port. 847/2017,corresponde à segunda linha e as ações de Auditoria Interna à 3ª linha de defesa em riscos da Agência.

Considerando que este Guia pretende favorecer a execução da GRC no âmbito tático e operacional da Agência e que, conforme § 1º do Art. 13 da Portaria n° 854/2017, os **agentes de riscos** são todos os gestores das unidades organizacionais diretamente subordinadas ou vinculadas às diretorias da Agência. É oportuno lembrar que é papel do agente de risco, dentre outras atribuições.

Art. 13. Cabe aos agentes de riscos corporativos:

I. Implementar a gestão de riscos corporativos em sua unidade organizacional;

II. *Gerenciar os riscos corporativos de sua respectiva unidade organizacional, de forma a mantê-los em um nível de exposição aceitável;*
III. *Comunicar tempestivamente, à Secretaria Executiva do Comitê, os riscos não mapeados, sejam eles novos ou não identificados anteriormente;*
IV. *Definir as ações e os controles necessários para o tratamento dos riscos corporativos no âmbito de sua unidade organizacional.*

Apetite e tolerância ao risco:

O apetite e a tolerância ao risco são conceitos complementares na gestão dos riscos de uma organização. Se por um lado, o **apetite ao risco** define o processo normal de aceitação ou não aceitação de risco pela organização no seu dia a dia; por outro, a **tolerância ao risco** trata da exceção, ou seja, do quanto tolera-se que o risco fuja esporadicamente de sua zona de aceitação. A tolerância está, portanto, relacionada com a margem/variação de aceitação do risco (ABNT 2009).

Em consonância com a Norma ISO 31000/2009, a Política de GRC da Anvisa define o **apetite ao risco** como a **quantidade e tipos de riscos** corporativos que a Anvisa está disposta a aceitar; já a **tolerância ao risco** como o **nível de variação aceitável** quanto à realização dos objetivos da Agência.

Segundo a Portaria 854/2017, os **tipos de risco** que podem afetar o alcance dos objetivos da Anvisa. São:

I. **riscos operacionais**: eventos que podem comprometer as atividades da instituição, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;
II. **riscos de imagem ou reputação:** eventos que podem comprometer a confiança da sociedade, parceiros, governo, setor regulado e/ou fornecedores em relação à capacidade da instituição em cumprir sua missão;
III. **riscos legais:** eventos derivados de inovações ou alterações legislativas ou normativas que podem comprometer as atividades da instituição; e
IV. **riscos orçamentários e financeiros:** eventos que podem comprometer a capacidade da instituição de dispor dos recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, ou acarretar prejuízo ao erário.

Com o advento do Plano de Integridade da Anvisa, de dezembro de 2017, o risco de integridade foi incorporado às tipologias de risco que podem afetar os objetivos da Agência; sendo definido conforme a seguir:

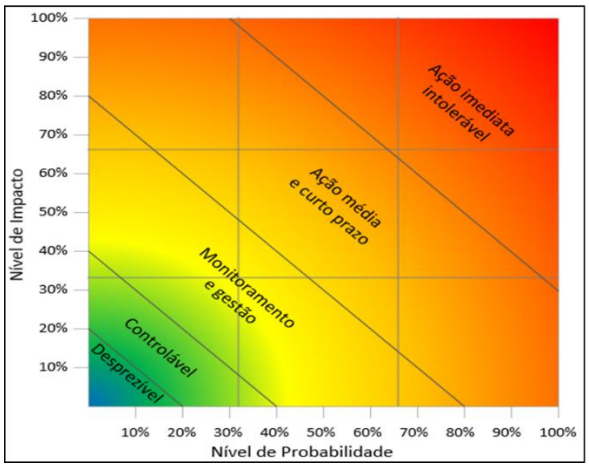
V. **risco de integridade:** vulnerabilidade institucional que pode favorecer ou facilitar práticas de corrupção, fraudes, irregularidades e desvios éticos e de conduta[1].

[1] Plano de integridade da Anvisa 2018/2019

No que tange à tolerância ao risco, o Comitê Gestor da Estratégia deliberou sobre os critérios que apontam para os limites de variação do risco, atribuindo recortes ao **nível de risco** aceitável pela Agência, com parâmetros alinhados à escala expressa pela combinação do nível de probabilidade e do nível de impacto do risco para a Agência.

Pela metodologia aprovada, a cada 20 pontos de variação na escala de nível de risco teremos um recorte da escala de tolerância; ao tempo em que será considerado em **patamar aceitável**, o risco que se encontre em **até 20 pontos na escalde de nível de risco**.

A Figura 4, a seguir, traz uma representação gráfica dos níveis de riscos, em um **mapa de riscos** e, ao lado, uma tabela com o detalhamento dos níveis de tolerância e os critérios definidos pela Anvisa.



Legenda			
Níveis de tolerância		Agentes	Detalhamento
Acima de 65%	Intolerável	Diretores ou Gerentes gerais/ equivalentes	Situações problema que possam impedir a organização de continuar funcionando.
41 a 65%	Crítico	Gerentes gerais/ equivalentes	Situações problema que possam impedir parte da organização de continuar funcionando.
21 a 40%	Moderado	Gerentes/ Coordenador	Situações problema que possam afetar o funcionamento de unidades organizacionais com suas atividades.
11 a 20%	Controlável	Todos	Situações problema que possam afetar o andamento dos trabalhos.
Abaixo de 10%	Desprezível	Sem necessidade	Situações que não acarretam problemas

Figura 4 - Níveis de risco e Níveis de Tolerância ao risco
Fonte: Assessoria de Planejamento - Aplan/Anvisa

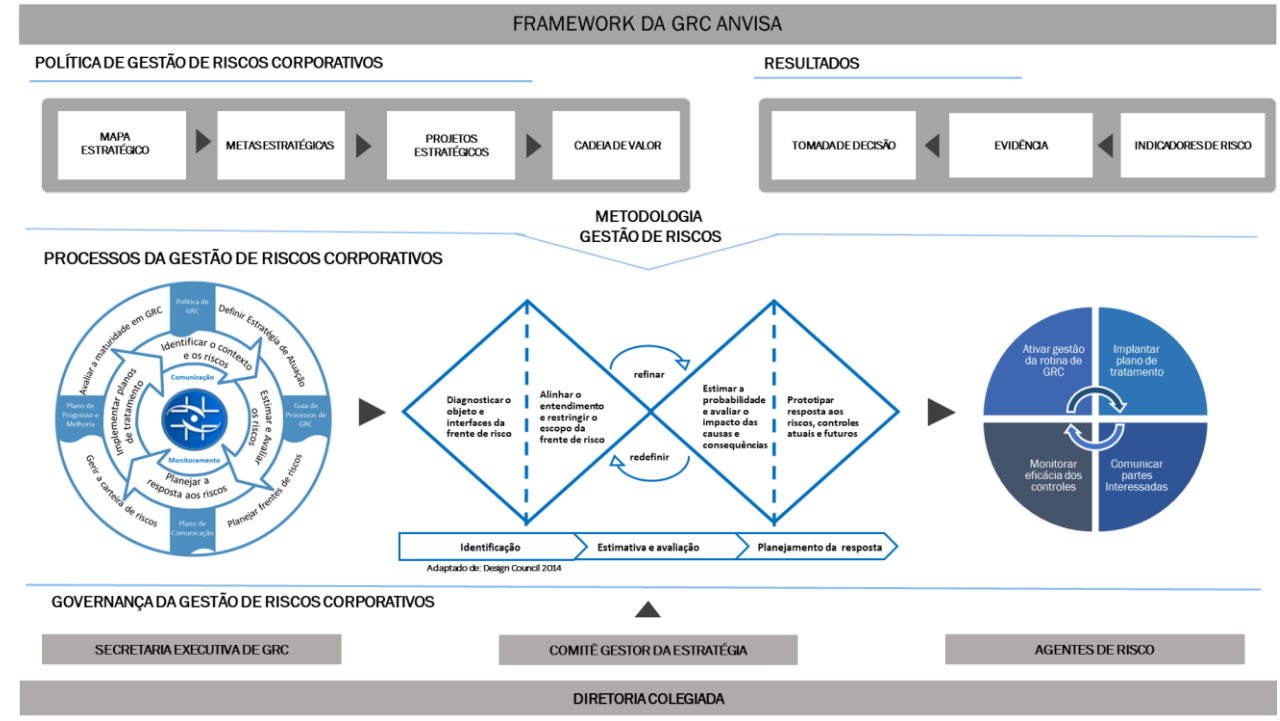
Comunicação e Monitoramento: É por meio do nível de risco, derivado dos níveis de probabilidade e impacto, que é possível identificar os riscos prioritários dada a magnitude do evento de risco. O registro de risco armazenará o resultado da avaliação dos riscos, e cabe a apreciação e monitoramento deste registro pelos Diretores e membros do Comitê Gestor da Estratégia. Os riscos de nível mais elevado, considerados intoleráveis, requerem comunicação e ações imediatas, além de ser monitorados de maneira mais atuante.

Metodologia

A Gestão de Riscos Corporativos é um processo contínuo, que consiste no desenvolvimento de um conjunto de ações destinadas a **controlar os riscos** com potencial de afetar os objetivos de programas, projetos ou processos de trabalho da Anvisa nos níveis estratégico, tático e operacional, a fim de mantê-los em um patamar aceitável, conforme parâmetros de **apetite** e **tolerância** ao risco aprovados pela Agência.

A metodologia de GRC construída pela Anvisa inspirou-se em modelos consagrados como a ISO 31000, COSO ERM e Management of Risk – M_o_R, (ABNT, 2009; COSO, 2004; OGC, 2010). Ela aglutina o modelo de governança e o processo de trabalho previstos na Política de GRC da Agência em um conjunto de passos inter-relacionados que visam trazer uma estrutura padronizada, indutiva e focada em resultados.

A Figura 33, a seguir, apresenta o framework da metodologia de Gestão de Riscos Corporativos da Anvisa:



https://www.designcouncil.org.uk/news-opinion/design-process-what-double-diamond

Figura 3 - Framework da metodologia de GRC da Anvisa
Fonte: Assessoria de Planejamento - Aplan/Anvisa

A metodologia de gestão de riscos na Anvisa está, portanto, alinhada à política de gestão de riscos e aos instrumentos da gestão da estratégia; dirigida por quatro documentos orientadores: uma política, um guia do processo, um plano de comunicação e um plano de progresso e melhoria; quatro ações estruturantes: estratégia de atuação, planejamento das frentes de riscos, gestão da certeira de riscos e avaliação periódica da maturidade em GRC; materializada em cinco etapas do processo: identificação do contexto e dos riscos, estimativa e avaliação, implementação dos planos de tratamento, além de um processo continuo e transversal relacionado à comunicação e monitoramento dos riscos entre as partes interessadas; focada em resultados; e suportada por um modelo de governança com papeis e atribuições definidas.

Importa que todas essas ações estejam em alinhamento com o mapa estratégico e cadeia de valor da Anvisa, amparadas pelas melhores informações disponíveis, em um processo dinâmico e cíclico, focado em resultados e na melhoria da governança da Agência.

Ciclo de GRC

Para otimizar a aplicação do método e o desdobramento das etapas do processo, a Aplan propôs seu desdobramento em um ***Ciclo de GRC***, além da aplicação de sua dinâmica em um ***Canvas Ágil de Gestão de Riscos Corporativos***, ferramenta inspirada na metodologia *Agile* e no *Business Model Canvas* de gestão estratégica. Além dessas, conformou um portal para registro do risco e um painel de controle para a gestão da carteira de riscos. Adicionalmente, propôs ainda uma ferramenta para avaliação de maturidade que subsidiará um plano de progresso e melhoria no que se refere à gestão de riscos na Anvisa.

A **Erro! Fonte de referência não encontrada.** 5, a seguir, apresenta o Ciclo de G RC e seu link com as etapas do processo, além dos instrumentos e ferramentas que suportam sua aplicação.

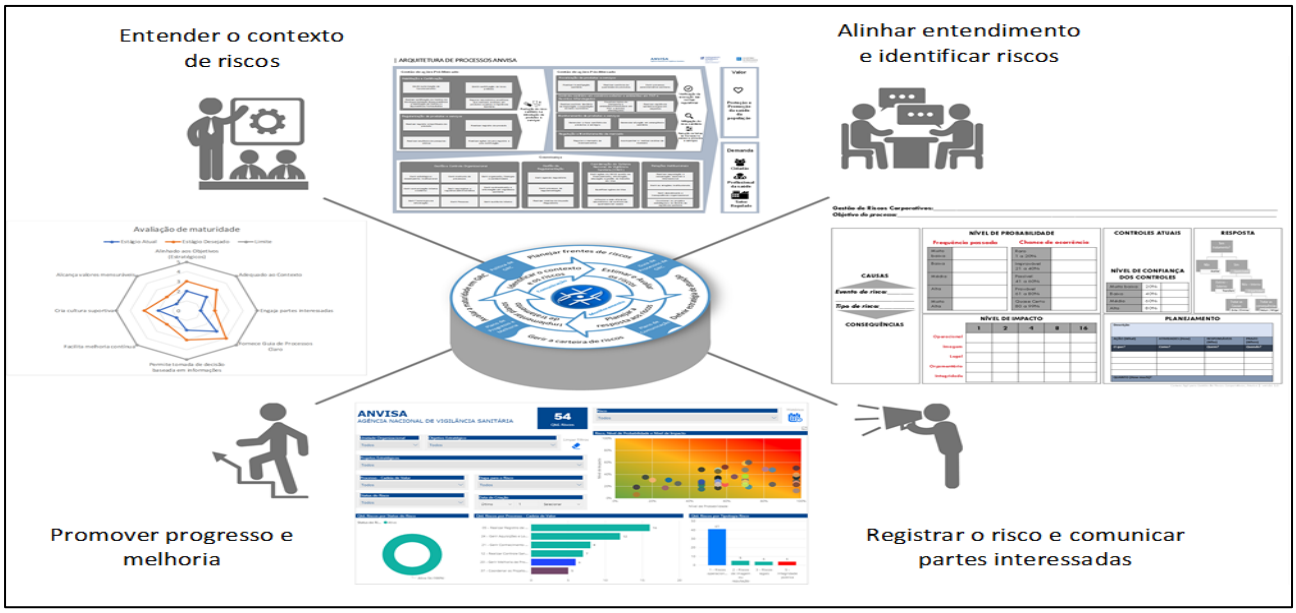


Figura 5 – Ciclo de GRC da Anvisa
Fonte: Assessoria de Planejamento - Aplan/Anvisa

O contexto do risco remete aos campos de atuação da Anvisa e o universo em que está inserida. Para fins deste Guia, consideramos cada objeto de aplicação da Gestão de Riscos Corporativos uma Frente de Riscos. Conforme apontado no framework da metodologia, a GRC está alinhada à gestão estratégica e se aplica tanto ao mapa estratégico; quanto às metas estratégicas. aos projetos estratégicos e aos processos da cadeia de valor.

Alinhar o entendimento, constitui-se de ação essencial para a fase de identificação dos riscos: envolve o levantamento das melhores informações disponíveis em um esforço para se entender o **contexto** e o respectivo **objetivo da frente de riscos** com fins de identificar os principais eventos que possam impactar nos objetivos da Agência. Em síntese, pretende delimitar o escopo da frente de riscos e suas respectivas interfaces.

O Canvas Ágil de GRC, ferramenta-padrão formulada pela e para a Anvisa, foi construído para otimizar o processo de GRC, de regra, em oficinas com gestores e especialistas no projeto/processo ou frente de risco, a fim de coletar e registar informações pertinentes às etapas do processo de forma dinâmica e ágil. Ele contempla as três primeiras etapas do processo de GRC: “Identificação”, “Estimativa e Avaliação” e “Planejamento da Resposta” ao risco. Cada uma delas permite uma reflexão quanto ao evento de risco a ser tratado e contém uma linha de tempo abrangendo “Passado”, “Presente” e “Futuro”, favorecendo uma imersão nas discussões quanto ao risco.

A Figura 6, a seguir, apresenta a visão geral do *Canvas Ágil de GRC,* contendo as três primeiras etapas do Processo de GRC e uma linha de tempo em cada etapa, abrangendo passado, presente e futuro, permitindo que haja uma reflexão mais profunda nas discussões quanto ao risco.

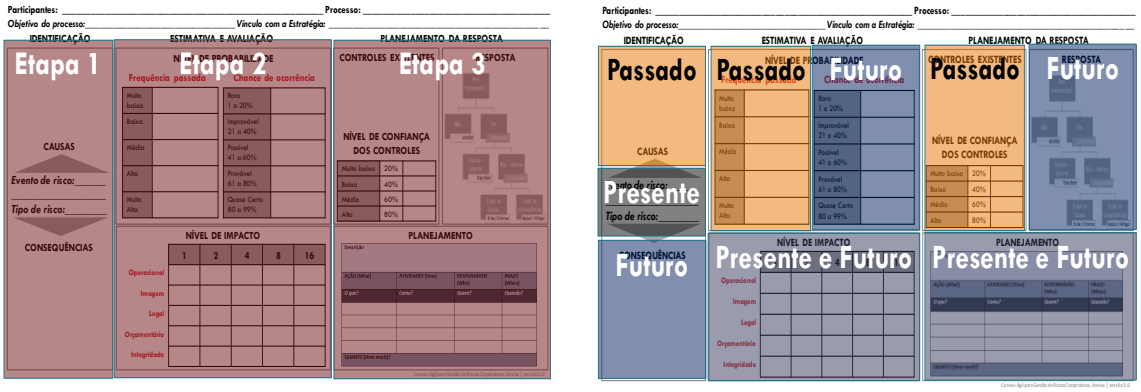


Figura 6 - Visão geral do Canvas Ágil de GRC
Fonte: Assessoria de Planejamento - Aplan/Anvisa

As sessões de workshop para aplicação do Canvas abordam uma dinâmica para buscar as melhores informações a partir do feeling e da experiência dos especialistas e gestores envolvidos; entretanto, o esforço anterior para se entender o **contexto de risco** e o **objetivo da frente de risco** é essencial para se delimitar o escopo das discussões.

Ao final da etapa de planejamento da resposta, terceira etapa do processo, é essencial **registrar e comunicar** os riscos identificados e o conjunto de ações a eles relacionadas às partes interessadas, com fins de assegurar o devido tratamento e a materialização das ações necessárias à eliminação ou mitigação dos riscos, bem como o necessário monitoramento dos resultados alcançados.

Com fins de favorecer o registro dos eventos de riscos e a gestão da carteira de riscos, bem como a necessária comunicação entre as partes interessadas, a Aplan disponibilizou um portal de riscos, na plataforma Sharepoint, onde cada unidade organizacional poderá registrar as informações a ela relacionadas e gerir seus respectivos riscos com segurança e agilidade. A plataforma eletrônica está disponível no seguinte endereço https://anvisabr.sharepoint.com/sites/GRC-Anvisa e os acesso disponibilizados por

unidade organizacional vinculada às diretorias. A figura 7, a seguir, apresenta uma visão geral da ferramenta e suas funcionalidades:

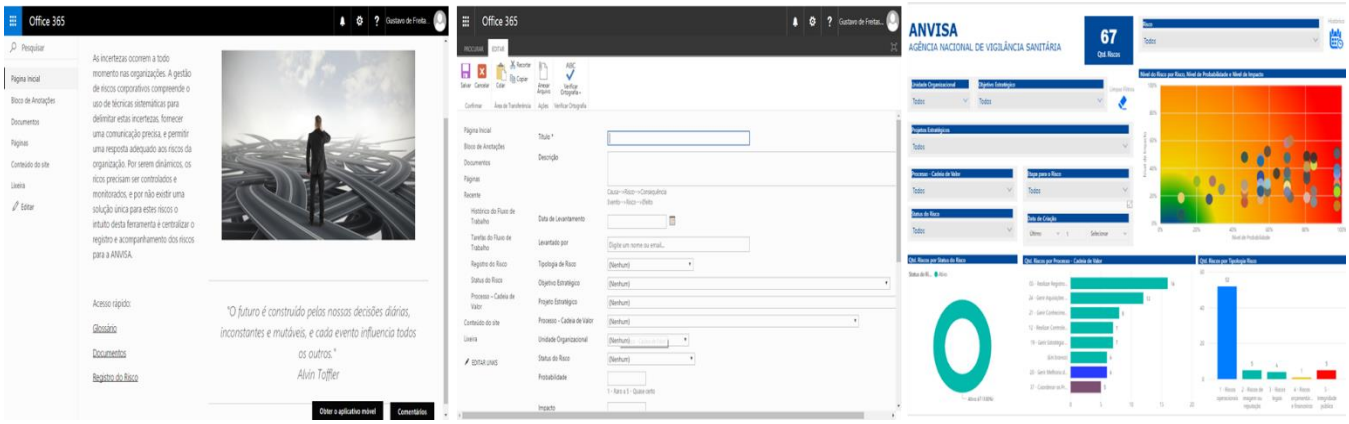


Figura 7 – Portal de registro e gestão do risco
Fonte: Assessoria de Planejamento - Aplan/Anvisa

Processo de GRC

Conforme apontado anteriormente, o modelo de governança instituído pretende integrar o processo decisório, a gestão tático-operacional e o processo de GRC, apontando atribuições e reponsabilidades a cada uma das partes envolvidas na gestão de riscos da Agência.

Assim, com fins de apoiar os gestores da unidades organizacionais, favorecer a execução da GRC no âmbito tático e operacional da Agência e ainda cumprir com seu papel de difusor da GRC na Agência, a Aplan concentrou esforços em simplificar o processo de GRC e sua aplicação nas diversas frentes de risco, conforme **Erro! Fonte de referência não encontrada.**8, a seguir:

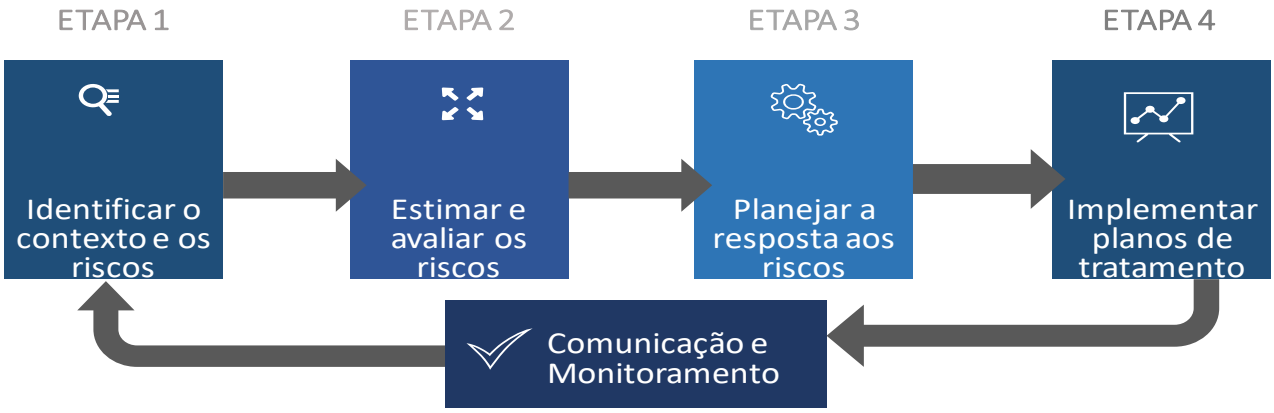


Figura 8 – Processo de GRC da Anvisa
Fonte: Assessoria de Planejamento - Aplan/Anvisa

Para cada etapa do processo existe uma gama de passos que devem ser seguidos e ferramentas que podem ser utilizadas conforme detalhado no Canvas Ágil de Riscos e descrito nas etapas subsequentes.

A Figura 9 , a seguir, traz uma visão geral do *Canvas Ágil de GRC* e a sequência de passos relacionados a cada etapa do processo.

Figura 9 - Passos do Canvas Ágil de GRC
Fonte: Assessoria de Planejamento - Aplan/Anvisa

Etapa 1 - Identificar o contexto e os riscos

Objetivo: Na Etapa 1 devemos identificar os eventos de risco a partir do contexto em que estamos inseridos, elaborar um título para o evento de risco, apontar a tipologia que melhor representa a natureza do risco, além das causas e consequências relacionadas a cada evento.

1 Passo 1: Objetivo da frente de riscos

Ao entender o contexto do risco obtemos elementos suficientes para cumprir os passos 1, 2, 3 e 4 do *Canvas Ágil de GRC*. Logo, é indispensável compreender o contexto interno e externo da frente de risco, passando pela definição de seu **objetivo**, suas **atividades**, os **stakeholders**, as **legislações** e **regulamentos**, os **recursos humanos**, **materiais** e de **TI** envolvidos, bem como os produtos e serviços resultantes do projeto/processo em análise. Para a execução desta etapa sugere-se a utilização do **formulário de contexto de risco**. Parte destas informações comporão o cabeçalho do Canvas.

Dica: Ao lidar com os riscos inicialmente identificados como **percepções de riscos** constatamos que, por vezes, há uma relação de interdependência entre eles; sugerindo que um evento de riscos pode ser causa ou consequência de outro já identificado. Para a execução desta etapa sugere-se a utilização da **tabela de percepções e análise de risco**. Com ela é possível organizar o registro das percepções e suas respectivas referências, além de agrupa-las por fontes/categorias, tipo de vulnerabilidade (*GAPs*) e se estão mais associadas à Causas ou Consequências do evento. Perceba que todo risco tem sua causa ligada a fontes e vulnerabilidades; ao tempo que as consequências estão ligadas à materialização do risco.

Estas informações devem ser coletadas junto aos gestores e grupo focal de especialistas envolvidos nas ações mais representativas da frente de riscos, mas também podem ser encontradas em documentos como relatórios de auditorias, pareceres, fluxos do processo, estrutura analítica do projeto e outros documentos relacionados ao contexto da frente de riscos.

2 Passo 2: Evento de riscos

A identificação do risco foca em criar um único **registro** que contém a descrição do **evento de risco**. Portanto, uma vez organizadas as percepções de riscos, passa-se à elaboração de um título capaz de agrupar múltiplas percepções em um único **evento**. O conjunto das percepções de riscos tendem a ser categorizadas para formar um único **evento de risco**.

Esta é a atividade mais difícil da identificação, dado que o título do evento é a síntese de como os gestores e especialistas no processo irão representar de forma clara tanto o contexto quanto o risco que se deseja enfrentar. O evento de risco remete a tudo que possa **atrasar**, **inibir** ou **impedir** que os objetivos sejam alcançados.

Dica: O registro dos eventos de risco é realizado em etapa anterior ao workshop, com fins de se ganhar tempo e evitar discussões laterais, e é formalizado por meio do Formulário de Contexto de Riscos.

3

Passo 3: Tipologia do Risco Ainda, como parte da etapa de identificação do contexto e risco, pretende-se apontar no passo "3", a **tipologia** dominante de cada risco. Nos termos da Portaria n° 854/2017, as tipologias correspondem à classificação dos tipos de riscos que podem afetar o alcance de objetivos da Agência, observadas as características de sua área de atuação.

A Figura 10, a seguir, traz a descrição de cada uma dessas tipologias. Vale lembrar que, não raro, um risco pode impactar em mais de uma tipologia, contudo, sempre existirá uma que é mais dominante em detrimento às demais.

Operacional	Imagem	Legal	Financeiro	Integridade
Comprometem as atividades da instituição: falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas	Comprometem a confiança da sociedade, parceiros, governo, setor regulado e/ou fornecedores em relação à capacidade da instituição em cumprir sua missão	Inovações ou alterações legislativas ou normativas que podem comprometer as atividades da instituição	Compromete a disposição dos recursos orçamentários e financeiros à realização de suas atividades; compromete execução orçamentária, ou acarretar prejuízo ao erário	Refere-se ao alinhamento consistente e aderência a valores éticos compartilhados, princípios e normas para garantir e priorizar os interesses públicos sobre os privados.

Figura 10 - Tipologias de Riscos e suas definições na Anvisa
Fonte: Assessoria de Planejamento - Aplan/Anvisa

Comunicação e Monitoramento: Uma vez que os registros de riscos foram elaborados, é possível condensar o contexto do risco e suas respectivas tipologias utilizando uma linguagem apropriada às partes interessadas, buscando uma comunicação precisa. Nesta etapa, sugere-se a utilização do **formulário de abertura da frente de riscos** e do **questionário de contexto de riscos,** tanto para o registro das informações no processo SEI, quanto para a comunicação às partes interessadas; neste caso, o Diretor Supervisor e o CGE, por meio da Secretaria Executiva de GRC.

4

Passo 4: Causas e Consequências:

O quarto passo da etapa 1 é apontar as **Causas** e **Consequências** relacionadas a cada evento de risco que, nos termos da Política de GRC da ANVISA, em seu Art. 4°, **causa** é definida como uma fonte de risco que, sozinha ou em combinação, tem o potencial intrínseco de gerar riscos, enquanto **consequência** é o resultado de um evento que afeta os objetivos pretendidos.

Sugere-se que a partir deste ponto, as atividades sejam realizadas em workshop com a participação de gestores e grupo ampliado de especialistas envolvidos nas ações da frente de riscos, com fins de se obter a melhor informação possível. Neste passo os participantes devem registrar cada percepção de causa ou consequência em *"posts"* individuais, a fim de favorecer a impessoalidade no levantamento de novas causas e consequências, sem o viés das percepções já levantadas anteriormente. Tal qual ocorre com a identificação dos eventos de riscos, os registros de causas e consequências semelhantes em sua essência, poderão ser agrupados para formar uma única causa ou consequência, reduzindo assim o volume de registros relacionados a cada evento, por conseguinte dos possíveis tratamentos necessários.

Dica: Cabe ressaltar que as percepções registradas na **tabela de percepções e análise de risco**, não precisam ser levadas ao workshop, dado que estas já serviram ao seu propósito na definição dos eventos de risco.

Comunicação e Monitoramento: Em que pese este passo estar contido na etapa 1 do processo, entende-se que o conjunto de informações relacionadas às causa e efeitos de cada evento de risco têm mais sentido quando apresentadas junto com os resultados das etapas 2 e 3 do processo, como parte integrante do **Relatoria de Análise de Riscos**.

Etapa 2 - Estimar e avaliar os riscos

Objetivo: Nesta etapa, pretende-se pontuar o **nível de probabilidade e nível de impacto** utilizando as escalas e critérios definidos, para que seja possível calcular o **nível de risco** e sua respectiva magnitude face aos critérios de tolerância ao risco aprovados pela alta gestão.

Esta etapa contempla os passos "5" e "6" do *Canvas Ágil de GRC* e consiste de uma análise qualitativa e quantitativa acerca de cada evento de risco em termos de **nível de probabilidade** e **nível de impacto**. O resultado desta análise aponta para o **nível de risco** de cada evento que, por sua vez, remete à **tolerância** e **apetite ao risco**.

Dica: Enquanto a análise mede e estima individualmente cada risco de forma isolada a avaliação, por sua vez, considera os riscos em conjunto, contribuindo para a priorização que está associada com o nível de risco. Nos termos de nossa Política, o **nível de risco** refere-se à magnitude do risco, expressa pela combinação de sua probabilidade e impacto; enquanto que **tolerância ao risco** é o nível de variação aceitável quanto ao alcance dos objetivos da Anvisa.

5 **Passo 5: Nível de Probabilidade**

Para a execução do passo 5 do *Canvas Ágil de GRC* precisamos identificar o **nível de probabilidade** que, em nossa metodologia, tenta suprir a carência de séries históricas e superar o viés dogmático da estatística estrito senso por meio de uma análise segmentada em duas dimensões, que possibilitam um olhar para o passado e para o futuro do

evento, ou seja, é composto pela **frequência** ou ocorrência passada e pela **probabilidade** ou chance de ocorrência do evento (futuro), com pesos de 30% e 70% respectivamente.

O Quadro 1, a seguir, apresenta a composição do nível de probabilidade e suas dimensões:

Quadro 1 – Nível de Probabilidade

Probabilidade 70% / Frequência 30%	1 - Raro	2 - Improvável	3 - Possível	4 - Provávle	5 - Quase certo
	1 a 20%	21 a 40%	41 a 60%	61 a 80%	81 a 100%
MUITO BAIXA - 1	11,50%	20,14%	28,79%	37,43%	46,08%
BAIXA - 2	16,34%	26,98%	37,62%	48,26%	58,90%
MÉDIA - 3	21,19%	33,82%	46,46%	59,09%	71,73%
ALTA - 4	26,03%	40,66%	55,29%	69,92%	84,55%
MUITO ALTA - 5	30,88%	47,50%	64,13%	80,75%	97,38%

Fonte: Assessoria de Planejamento - Aplan/Anvisa

O Quadro 2 e Quadro 3, a seguir, apresentam os critérios de pontuação da frequência (*Ocorrência passada*) e probabilidade (*Chance de ocorrência*):

Quadro 2 – Critérios da Frequência – Ocorrência passada

Grau	Categoria	Descrição	Ocorrência
1	Muito baixa	Eventos similares acontecem com uma frequência muito baixa	Quase não ocorreram no passado
2	Baixa	Outros eventos similares já aconteceram, mas são de baixa frequência	Existiram poucas ocorrências antes
3	Média	Eventos desse tipo ocorreram no passado com uma frequência regular	Ocorreram regularmente
4	Alta	Eventos similares acontecem na maioria das vezes ao no passado	Existiram bastante ocorrências antes
5	Muito alta	Outros eventos similares aconteceram com muita frequência no passado.	Ocorreram com muita frequência antes

Fonte: Assessoria de Planejamento - Aplan/Anvisa

Quadro 3 – Critérios da Probabilidade - Chance de ocorrência futura

Grau	Categoria	Descrição	Ocorrência
1	Raro 1 a 20%	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 pode ocorrer apenas em circunstâncias muito excepcionais
2	Improvável 21 a 40%	O evento não ocorre de maneira frequente na organização ou organizações similares. Os controles atuais e as circunstâncias sugerem que a ocorrência seria considerada altamente não usual	O evento pode ocorrer em algum momento, mas é improvável
3	Possível 41 a 60%	O evento pode ter ocorrido ocasionalmente na organização ou em organizações similares. Os controles atuais	O evento provavelmente ocorrerá em algumas circunstâncias

		ou as circunstâncias sugerem que há uma possibilidade plausível de ocorrência	
4	Provável 61 a 80%	Este evento pode ocorrer regularmente na organização ou organizações similares. Com os controles atuais ou circunstâncias, pode-se esperar que ocorra ao longo de 1 ano	O evento provavelmente ocorrerá na maioria das circunstâncias
5	Quase certo 81 a 100%	Este evento ocorre frequentemente na organização ou com os controles ou circunstâncias espera-se sua ocorrência	É esperado que o evento ocorra na maioria das circunstâncias

Fonte: Assessoria de Planejamento - Aplan/Anvisa

6

Passo 6: Nível de Impacto

Já para o passo "6", precisamos definir o **nível de impacto.** Nos termos de nossa Política, **impacto** é o efeito resultante da ocorrência de um evento; e como dito anteriormente, não raro, um mesmo evento pode ter impacto em várias tipologias de riscos. O nível de impacto avalia, em uma perspectiva de futuro, o efeito resultante da ocorrência do evento sobre os **tipos de risco** que podem afetar o alcance dos objetivos da Anvisa .

Para a mensuração do impacto dos riscos foi utilizado uma escala de 1 a 16 que deve auxiliar na ponderação em relação a cada tipologia, presentes no Quadro 4, conforme a seguir:

Quadro 4 – Grau de impacto para as tipologias de risco

Peso	1	2	4	8	16
Descrição	Muito Baixo	Baixo	Médio	Alto	Extremo

Assessoria de Planejamento - Aplan/Anvisa.

O Quadro 5, a seguir, apresenta os critérios de pontuação para o grau de impacto de cada tipologia de risco:

Quadro 5 – Critérios do impacto, por tipologia de risco

Grau	Operacional	Imagem	Legal	Financeiro	Integridade
16	Interrupção completa das operações ou de entrega de produtos ou serviços por período indeterminado A maioria dos programas ou projetos críticos não será concluído Intervenção externa para regularizar situação	Impacto adverso significativo Atenção extremamente negativa e consistente da mídia (meses) Perda de confiança irreconciliável Intervenção externa como resposta de governabilidade	Resultará em litígios e multas significativos Pode envolver atividades sindicais Resultará em violações (não conformidade) de legislação / regulação	Ativos de infraestrutura significativos se tornam inservíveis por um período extenso ou indeterminado Impacto crítico de longo prazo no orçamento, não recuperável no exercício financeiro atual, nem no próximo Falhas graves de segurança de acesso físico ou lógico, acarretando em funções de negócios críticas vulneráveis a ações não autorizadas	Perturbações graves quanto à conduta e ética, resultando em grande corrupção ou fraudes Grande priorização de interesses pessoais frente aos interesses públicos Abuso de poder e uso das atribuições ou cargo para benefício próprio ou articulações indevidas
8	Interrupção severa das operações ou de entrega de produtos ou serviços que impactem negativamente a imagem da Agência Um ou mais programas ou projetos críticos pode não ser concluído Intervenção de diretores para regularizar situação	Impacto adverso considerável Atenção negativa e consistente da mídia (semanas) Perda de confiança de comunidades específicas Intervenção mista (diretores e entes externos) como resposta de governabilidade	Pode resultar em litígios que requeiram o envolvimento significativo da Procuradoria Resultará em violações graves (não conformidade) de legislação / regulação	Ativos de infraestrutura significativos se tornam inservíveis por um determinado período (semanas ou meses) Impacto muito alto no orçamento, não recuperável no exercício financeiro atual, nem no próximo Falhas de segurança de acesso físico ou lógico, acarretando em funções de negócios vulneráveis a ações não autorizadas	Utilizações incorretas de verbas e fundos para interesses próprios Vazamento de informações privilegiadas ou restritas Solicitação ou recebimento de propinas ou pagamentos indevidos
4	Interrupção em operações ou em entrega de produtos ou serviços que tenham algum impacto negativo junto ao consumidor	Impacto adverso localizado (comunidades específicas) Atenção negativa da mídia (dias) Perda de confiança em processos de trabalhos de comunidades específicas	Resultará em um incidente sério, com investigação e avaliação sobre responsabilidade legal Resultará em não conformidade de legislação / regulação	Ativos de infraestrutura se tornam inservíveis por um determinado período (dias ou semanas) Impacto alto no orçamento, recuperável no exercício financeiro atual, mas requer priorização	Descaso quanto à realização das atribuições causando desperdícios de recursos públicos ou má gestão Nepotismo e uso das atribuições de forma antiética para

Grau	Operacional	Imagem	Legal	Financeiro	Integridade
	Um ou mais programas ou projetos significativamente prejudicados Intervenção interna ou contratação externa pontual para regularizar situação	Expressão de preocupação por diretores ou entes externos		Falhas de segurança de acesso físico ou lógico, acarretando em ativos roubados ou destruídos intencionalmente	influenciar agente públicos ou privados Ceder a pressões internas ou externas que permitem corrupção, e não denunciar estes casos adversos
2	Alguma interrupção das operações ou na entrega de produtos ou serviços, mas que não tenham impactos junto ao consumidor Regularização rápida (em até um mês) por equipe interna	Impacto e preocupação em comunidades locais Eventual atenção negativa da mídia	Resultará em questões legais menos complexas ou não conformidades leves de legislação / regulação, mas que podem ser tratadas pela Procuradoria	Ativos de infraestrutura não críticos se tornam inservíveis por um curto período (horas ou dias) Impacto pequeno, mas perceptível, no orçamento, recuperável no exercício financeiro atual Falhas de segurança de acesso físico ou lógico, acarretando em necessidade de reparo ou substituição de peças danificadas sem intenção	Imperícia e desleixo na condução das atribuições e tarefas Repassar informações inverídicas ou fictícias para autopromoção Tumultuar ambiente de trabalho e causar desinformação ou desserviço.
1	Impacto mínimo nas operações ou entrega de produtos ou serviços Regularização rápida através da revisão de processos de trabalho	Preocupação baseada em questões individuais Sem cobertura da mídia	Surgem questões que podem ser resolvidas por procedimentos rotineiros, e não afetarão a conformidade com legislação ou regulação	Ativos de infraestrutura não críticos se tornam inservíveis, mas que podem ser substituídos em intervalos de tempo aceitáveis Impacto mínimo no orçamento, recuperável no exercício financeiro atual Falhas de segurança de acesso físico ou lógico, acarretando em temporariamente indisponíveis	Atitudes que quebram a confiança com superiores Não desempenhar o trabalho com acurácia ou conformidade, desobedecendo regras superiores Falta de companheirismo e altruísmo com os colegas de trabalho

Fonte: Assessoria de Planejamento - Aplan/Anvisa

Etapa 3 - Planejar a resposta aos riscos

Objetivo: Nesta etapa pretende-se levantar os controles já existentes capazes de alterar o nível de riscos do evento em questão, apontar o nível de confiança para cada um deles, identificar a necessidade novos controles e prospectar novos planos e ações para o tratamento do risco.

Superadas as etapas de identificação, estimativa e avaliação de cada evento e cientes dos limites de tolerância adotados na Anvisa, temos elementos suficientes para **planejar resposta aos riscos**, presentes nos passos "7", "8" e "9" do Canvas. Assim, é importante levantar os controles existentes e elaborar um **plano de tratamento** para os riscos quando necessário, ou seja, quando não houver controles ou quando os existentes forem considerados insuficientes para manter o nível de risco em um patamar aceitável.

Dica: Vale lembrar que há uma relação entre as **causas** e **consequências** do **evento de risco** da Etapa 1, com os **controles existentes** e o **planejamento da resposta** da Etapa 3; uma vez que estes visam **eliminar** as causas ou **mitigar** os efeitos de sua materialização.

7 Passo 7: Controles Existentes

Nos termos de nossa Política, **controle** é qualquer medida que mantém ou modifica o risco. Em geral são destinados a enfrentar os riscos e fornecer segurança razoável na consecução da missão da organização. Assim, para a execução do passo "7", é importante levantar todos os controles existentes, formais ou não, capazes de alterar o nível de risco, seja pela eliminação das causas ou mitigação dos seus efeitos. Em seguida, deve-se ponderar quanto à eficácia desses controles a fim de obter subsídios quanto à necessidade ou não de se instituir novos.

O Quadro 6, a seguir, apresenta uma escala contendo critérios de ponderação para o nível de confiança de cada controle.

Quadro 6 – Nível de confiança dos Controles Existentes

Nível de confiança no controle	Escala	Descrição
Muito Baixo	20%	Os controles existentes são ineficazes, e dificilmente se poderá reduzir a probabilidade ou o impacto do risco.
Baixo	40%	Os controles são poucos e a confiança é baixa.
Médio	60%	Existe confiança nos controles atuais do risco.
Alto	80%	Os controles são satisfatórios e o risco tem grande possibilidade de ser controlado

Fonte: Assessoria de Planejamento - Aplan/Anvisa

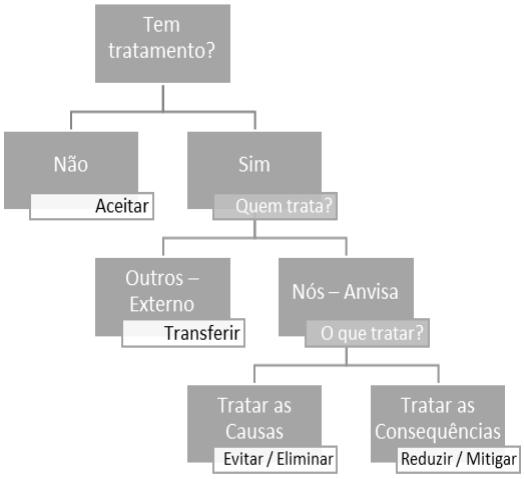
Dica: As informações obtidas durante o workshop devem ser registradas em post-its individuais com o respectivo nível de confiança. Inexistindo controles, esta parte do Canvas ficará em branco.

Dica: O levantamento e entendimento da eficácia desses controles é importante porque, em alguns casos, eles podem, em conjunto ou isoladamente, ser suficientes para manter o nível de risco em patamar aceitável.

8 **Passo 8: Resposta ao risco**

Certos da necessidade de novos controles, é importante apontar o tipo de r**esposta** ao risco e, consequentemente, o **tratamento** que será implementado para cada um deles.

Para auxiliar na definição do tipo de resposta e tratamento a ser implementado, a Figura 11 e o Quadro 7, a seguir, apresentam a gradação para o tipo de resposta e respectivo tratamento, além dos critérios que os norteiam.



Ação ou resposta ao risco	Tipo de tratamento	Descrição
Aceitar	Não há o que fazer	Existem riscos em que nada pode ser feito.
Transferir	Passar a responsabilidade	Existem riscos em que devemos passar o ônus/responsabilidade para atores externos à Anvisa. (Ex.: Seguros, terceirizados, outros)
Eliminar ou Evitar	Tratar as causas	Existem riscos que devemos tratar suas causas, evitar que ocorram para que não impactem os objetivos.
Reduzir ou mitigar	Tratar as consequências	Existem riscos que não podemos evitar, mas que podemos tratar caso venham a acontecer.

Figura 11 – Resposta ao risco; Quadro 7 – Tipo de tratamento ao risco
Fonte: Assessoria de Planejamento - Aplan/Anvisa

Dica: Vale lembrar que um mesmo evento de risco pode ter múltiplas respostas, mas esses tratamentos precisam ser decompostos para simplificar a gestão e permitir sua operacionalização.

É importante destacar que cada tipo de resposta requer um tipo de ação, ou seja, ao **aceitar** um risco as instâncias superiores da gestão devem ser comunicadas quanto às justificativas para não adoção de quaisquer respostas ou tratamentos. Assim, caso a instância superior aceite as justificativas, a responsabilidade do agente de riscos passa a ser compartilhada no caso de materialização do risco.

Ao **transferir** os riscos, pretende-se repassar o ônus de tratamento e/ou seus respectivos custos e impactos para outras agentes externos como outros órgãos, seguradoras ou empresas terceirizadas.

Dica: Não confundir a transferência do risco com os casos em que se faz necessário compartilhar o tratamento, envolvendo outras unidades organizacionais na construção de soluções. Neste caso, a resposta ao risco poderá ser conjunta e/ou, em casos extremos, os níveis superiores da gestão (CGE, Diretoria ou DICOL) poderão ser acionados e atribuir um Agente apropriado para orquestrar o tratamento.

Ao se optar por **evitar** ou **eliminar** riscos, pretende-se tratar as causas geradoras dos riscos impedindo sua materialização ou diminuindo a probabilidade de que venham a ocorrer. Por outro lado, quando o risco não pode ser evitado, devemos nos preparar para tratar as consequências ou seja, **reduzir** ou **mitigar** os efeitos de sua materialização sobre os objetivos organizacionais, por exemplo, por meio de **planos de contingência**.

9 **Passo 9: Planejamento da resposta**

Após avaliar a eficácia dos controles existentes e todas as possíveis respostas ao risco é preciso elaborar o **plano de tratamento**. Neste sentido, propõe-se uma ferramenta de gestão pratica e fácil de usar: o 5W2H.

O Quadro 8, a seguir, traz um modelo simplificado da ferramenta para ser utilizada durante o workshop, suficiente para auxiliar na prospecção inicial dos planos de ação que ajudaram a responder as principais questões do plano de tratamento, abrangendo: "o que" fazer, "como" fazer, "quem" fará, "quando" será feito e "quanto" custará para atuar sobre os riscos.

Quadro 8 – Plano de tratamento

<Descrição>			
AÇÃO (*What*)	**ATIVIDADES (*How*)**	**RESPONSÁVEIS (*Who*)**	**PRAZO (*When*)**
O que?	***Como?***	***Quem?***	***Quando?***
QUANTO (*How much*)?			

Fonte: Assessoria de Planejamento - Aplan/Anvisa

Dica: Durante o workshop podem surgir bons *insights* ou oportunidades para tratamento dos riscos, mas o consolidado do plano de tratamento deverá ser detalhado em momento posterior, após a consolidação dos resultados da Oficina.

Ao final do preenchimento da Etapa 3, o workshop terá sido finalizado, sendo necessária a consolidação das informações, posterior registro no portal de riscos e compartilhamento com as partes envolvidas, CGE e diretorias.

Com fins de favorecer a execução destas atividades, propomos o preenchimento da segunda parte da **tabela de percepções e análise de risco,** instrumento que permite

a organização dos resultados da oficina, capaz de fornecer subsídios para a consolidação do **relatório de análise de riscos** e posterior elaboração do **formulário de tratamento de riscos**. Documentos estes, que juntamente com o **formulário de abertura de frente de Risco** e o **questionário de contexto de riscos**, elaborados e preenchidos em fase previa ao Workshop, deverão compor o processo da **frente de risco** no Sistema Eletrônico de Informações - SEI.

Dica: Podem ser encontrados planos de tratamento similares ou idênticos advindos de riscos distintos. Isso reforça a necessidade de se executarem os referidos planos e possibilita a justificativa da celeridade na execução do tratamento.

Comunicação e Monitoramento: Ao final da etapa de planejamento da resposta devemos comunicar os resultados alcançados para os tomadores de decisão e às demais partes interessadas. O **relatório de análise de riscos**, pretende favorecer a comunicação e o compartilhamento dos riscos entre a unidade organizacional, seu Diretor Supervisor e o CGE, por meio da Secretaria Executiva de GRC, quanto aos riscos identificados, os resultados de sua avaliação, os mecanismos de controle existentes e os planos de tratamento pretendidos. O Conjunto de informações levantadas até este momento deverão ser registradas no **portal de registro e gestão do risco**, exclusivo da unidade organizacional, disponível na plataforma Sharepoint, em https://anvisabr.sharepoint.com/sites/GRC-Anvisa, que também alimentará o portal de GRC da Anvisa.

Etapa 4 - Implementar planos de tratamento

Objetivo: Nesta etapa a Unidade Organizacional irá melhorar os controles existentes ou implementar novos controles, conforme previstos nos planos de tratamento elaborados na etapa anterior, a fim de trazer os riscos identificados para um patamar aceitável, dado o apetite e tolerância ao risco da organização.

Perceba que todas os passos das etapas anteriores culminam na **implementação** dos planos de tratamento. Posto que uma vez identificados os riscos e definida a necessidade de tratá-los, é necessário por em prática as repostas ora planejadas. Para a consolidação dos planos de tratamento e comunicação às partes interessadas, sugere-se a utilização do **formulário de tratamento de riscos**

Reconhecendo a capacidade limitada em termos de recursos, é necessário definir prioridades em detrimento dos riscos menos significativos e, para isso, pode-se utilizar a escala do nível de risco, ou tolerância ao riscos, a fim de ranquear quais planos devem ser implementados com maior prioridade; lembrando que o tratamento de todos os riscos é o ideal para a organização e que a aceitação do risco deve ser acompanhada de justificativa específica.

O Agente do risco, gestor da unidade organizacional, é o responsável por alocar recursos e viabilizar que o risco seja tratado. Neste sentido é este Agente que atribui e ranqueia quais riscos são prioritários para tratamento em sua unidade organizacional. A implementação dos planos de tratamento será executada pelo(s) Interlocutor(es) que o Agente definir no âmbito de sua unidade, conforme definido no plano de tratamento.

Dica: O mapa de riscos, por estar diretamente vinculado aos níveis de tolerância aos riscos, sem prejuízo de outros critérios que venham a ser adotados pelo Agente de riscos, será sempre um bom instrumento para a priorização dos planos de tratamento. Isto, porque os riscos que forem considerados intoleráveis sempre deverão ter seus planos de tratamento priorizados, vide **requisitos de apetite e tolerância ao risco** aprovados pela Agência.

Comunicação e monitoramento: O **formulário de tratamento de riscos** deverá ser compartilhado com a chefia imediata, outras unidades afetas ao risco ou à implementação do plano de tratamento, além do Diretor Supervisor e a Secretaria Executiva de GRC, para fins de comunicação ao CGE e demais diretorias. A implementação dos planos de tratamento pode durar vários meses, sendo assim, é necessário que ocorra o monitoramento na execução desses planos, para que não se desviem do objetivo principal, e para reportar às partes interessadas as evoluções e possíveis entraves quanto ao plano.

Comunicação e Monitoramento

Objetivo: A Comunicação e Monitoramento são atividades constantes no processo, por isso não estão vinculadas a uma etapa específica. Cada etapa possui elementos e informações que devem ser comunicadas e monitoradas para assegurar que os riscos sejam tratados adequadamente. Está é também a atividade que retroalimenta os fluxos de GRC, permitindo evoluções e melhorias.

Existem comunicações que ocorrem de maneira informal e pontual, como no caso de riscos que afetam apenas a unidade, enquanto outras ocorrem de maneira formal e mais abrangente, como o caso de riscos que impactam os objetivos estratégicos da Anvisa no cumprimento de sua missão institucional.

Os riscos estratégicos, aqueles relacionados a processos, projetos ou programas que impactam nos objetivos da Agência, serão registrados no **portal de registro e gestão do risco**, e para cada registro há uma notificação automática, por e-mail, para os envolvidos, sejam estes o Agente ou o interlocutor de risco, o Diretor Supervisor, ou ainda técnico ou gestor de outra unidade organizacional envolvida na identificação ou no tratamento do risco .

Uma vez registrados nesta plataforma, os riscos passam a ser monitorados e comunicados tanto pela unidade organizacional, dona do risco, quanto pela Secretaria Executiva de GRC. Para os riscos considerados estratégicos, a Aplan, unidade organizacional

que assumiu as atribuições da Secretaria Executiva de GRC, deverá elaborar relatórios periódicos ao CGE referenciando os riscos que atingem ou superam os limites de tolerância definidos pela alta gestão, e os resultados dos planos de tratamento definidos pelas respectivas unidades organizacionais, donas do risco.

Esta ação de comunicação ente Secretaria Executiva de GRC, o CGE e demais diretorias, é formalizada pelo **Sumário Executivo de GRC**, que pretende uma alinhamento e harmonização de informação para a alta gestão quanto as ações de riscos estratégicos em desenvolvimento.

Quanto ao Monitoramento, seu principal objetivo é garantir que as ações planejadas para eliminar os riscos ou mantê-los em patamar aceitável sejam executadas adequadamente ou que tenham o devido aporte de recursos da alta gestão. Os resultados deste monitoramento também deverão compor o Sumário executivo de GRC.

Os indicadores chave de risco (KRI – *Key Risk Indicators*) atuais são:

- Eventos de riscos acima da tolerância definida = (NR ≥ 0,65);
- Eventos de riscos que não tiveram atualização nos últimos 180 dias
    - Registros para revisão= Dias (Data atual – Data Criação) ≥180 → Revisão;
    - Última atualização =Dias (Data Atual – Data de Modificação);
    - Tempo Total = Dias (Data Atual – Data de Criação);
- Taxa de Parecer= (Total de registros com Relatório de Análise de Riscos do Agente do Risco/Total de registros) %;
- Taxa de Planejamento= (Total de registros com planos de tratamento/Total de registros) %;
- Taxa de Resolução= (Total de registros com status Encerrado/Total de registros) %;

Finalmente, busca-se por meio dessa atividade de comunicação e monitoramento que as partes interessadas tenham ciência e se envolvam no tratamento dos riscos, sejam estes operacionais ou estratégicos.

Repositório de documentos e modelos

Estão disponíveis no **portal de registro e gestão do risco**, além da Política e do Guia do processo, o Plano de implantação de GRC aprovado pela DICOL, o Plano da comunicação e todos os modelos de documentos, planilhas e outros artefatos para apoiar os agentes e interlocutores de risco na execução das etapas do processo de GRC. Disponíveis em: https://anvisabr.sharepoint.com/sites/GRC-Anvisa.

Os documentos são atualizados de tempos em tempos e recomenda-se o uso deste caminho para obter as versões mais recentes.

Considerações finais

A Gestão de Riscos Corporativos vem sendo reconhecida como ferramenta de apoio aos gestores e à alta direção. A Administração Pública Federal brasileira vem investindo cada vez mais nesse conjunto de práticas para permitir um melhor alcance dos objetivos organizacionais, utilizando-se de mecanismos sistêmicos para uma comunicação mais precisa e métodos que permitam a diminuição de subjetividade nas ações relacionadas a riscos.

É notável a importância de se gerenciar os riscos, principalmente se evidenciarmos os benefícios em relação aos níveis tático-operacional. Da redução da ocorrência dos eventos adversos a ganhos de produtividade, podem-se listar diversos benefícios relacionados à GRC, na medida em que se avança na sua aplicação.

Por meio deste guia prático e sua referida metodologia de apoio, espera-se que as Uorgs da Anvisa consigam realizar o processo de gestão de riscos, contado com o apoio desta Assessoria de Planejamento como uma parceira interessada em viabilizar que tais práticas gerenciais sejam incorporadas nas ações do dia-a-dia. Importante reforçar o papel de agregação de valor cotidiano das práticas de GRC, sem que tragam uma sobrecarga às atividades de rotina desempenhadas em cada unidade organizacional; nesse mesmo sentido, as atividades desenvolvidas para aplicação da metodologia, são um caminho que visa a permitir maior integração entre os participantes e uma dinâmica leve e descomplicada para tratar um assunto sobremodo estratégico e atual para a instituição Anvisa e a Administração Pública Federal.

Referências

ABNT. **ABNT NBR ISO 31000 Gestao de Riscos - Princípios e Diretrizes**. [s.l.] Associação Brasileira de Normas Técnicas, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO 31000: Gestão de riscos - Princípios e diretrizes**. [s.l: s.n.].

BRASIL. **Instrução Normativa N 01/2016**. Brasília, DF: Ministério do Planejamento Orçamento e Gestão, Controladoria Geral da União, 2016.

BRASIL. **Agência Nacional de Vigilância Sanitária - ANVISA. PORTARIA Nº 854, DE 30 DE MAIO DE 2017**Brasília, DFANVISA, , 2017.

COSO. **Enterprise Risk Management: Integrated Framework** (Commission Committee of Sponsoring Organizations of the Treadway, Ed.), 2004. Disponível em: <www.coso.org/publications.Htm>

IBGC. INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Guia de orientação para o gerenciamento de riscos corporativos** / coordenação: Eduarda La Rocque. São Paulo, SP: IBGC, 2007 (série de cadernos de governança corporativa, 3).

IIA. INSTITUTE OF INTERNAL AUDITORS. Declaração de posicionamento do IIA: **As três Linhas de defesa no gerenciamento eficaz dos riscos e controles;** São Paulo; IIA Brasil; 2013.

OGC. **Management of Risk : Guidance for Practitioners**. London: Office of Government Commerce - Axelos, 2010.