BOOK DE GESTÃO DE RISCOS CORPORATIVOS

ESTRATÉGICO E TÁTICO

ANVISA
Agência Nacional de Vigilância Sanitária

Book de Gestão de Riscos Corporativos

ANVISA
Agência Nacional de Vigilância Sanitária

ESCRITÓRIO
DE PROCESSOS

Apoio: ELO GROUP

Julho 2021

Palavras chave: 1. Riscos 2. Tático 3. Estratégico 4. GRC 5. Processos
6. Ferramentas 7. Anvisa

SUMÁRIO

S

1 INTRODUÇÃO 04

2 *FRAMEWORK* DO PROCESSO 08

3 DETALHAMENTO DOS PROCESSOS 18

4 ATORES, PERFIS E COMPETÊNCIAS 24

5 MATERIAIS DE APOIO 30

6 SIGLAS E TERMOS 54

1

Introdução

Introduzir conceitos e premissas da Gestão de Riscos Corporativos

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 política de Gestão de Riscos Corporativos (GRC) da Anvisa, em seu art. 4º, inciso XXII, risco é definido como 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.

Destaca-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, que tenha consequências positivas ou negativas para o cumprimento da missão institucional

A proposta de aplicação da metodologia de GRC atende, portanto, às recomendações do Tribunal de Contas da

União (TCU) e Controladoria-Geral da União (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. Também, contemplando controles internos, métodos de gestão de riscos e fatores de governança, conforme disposto na Instrução Normativa Conjunta n.º 1 (MPOG/CGU), de 10 de maio de 2016, sobre âmbito do Poder Executivo federal (BRASIL, 2016).

Para tanto, este *Book* está organizado em seis partes. A primeira corresponde à introdução. A segunda parte apresentará a visão macro dos processos por meio de um *framework* que interliga todos os processos previstos para GRC. A terceira parte trata os processos de forma individual e detalhada.

A quarta apresentará os atores envolvidos na GRC e suas responsabilidades. A quinta parte apresenta o conjunto de ferramentas a serem utilizadas para a realização e operacionalização dos processos detalhados na parte três. Por fim, a sexta parte corresponde às siglas e termos utilizados neste *Book.*

[1] *Introdução do Guia Prático de GRC da Anvisa. 2018*

2

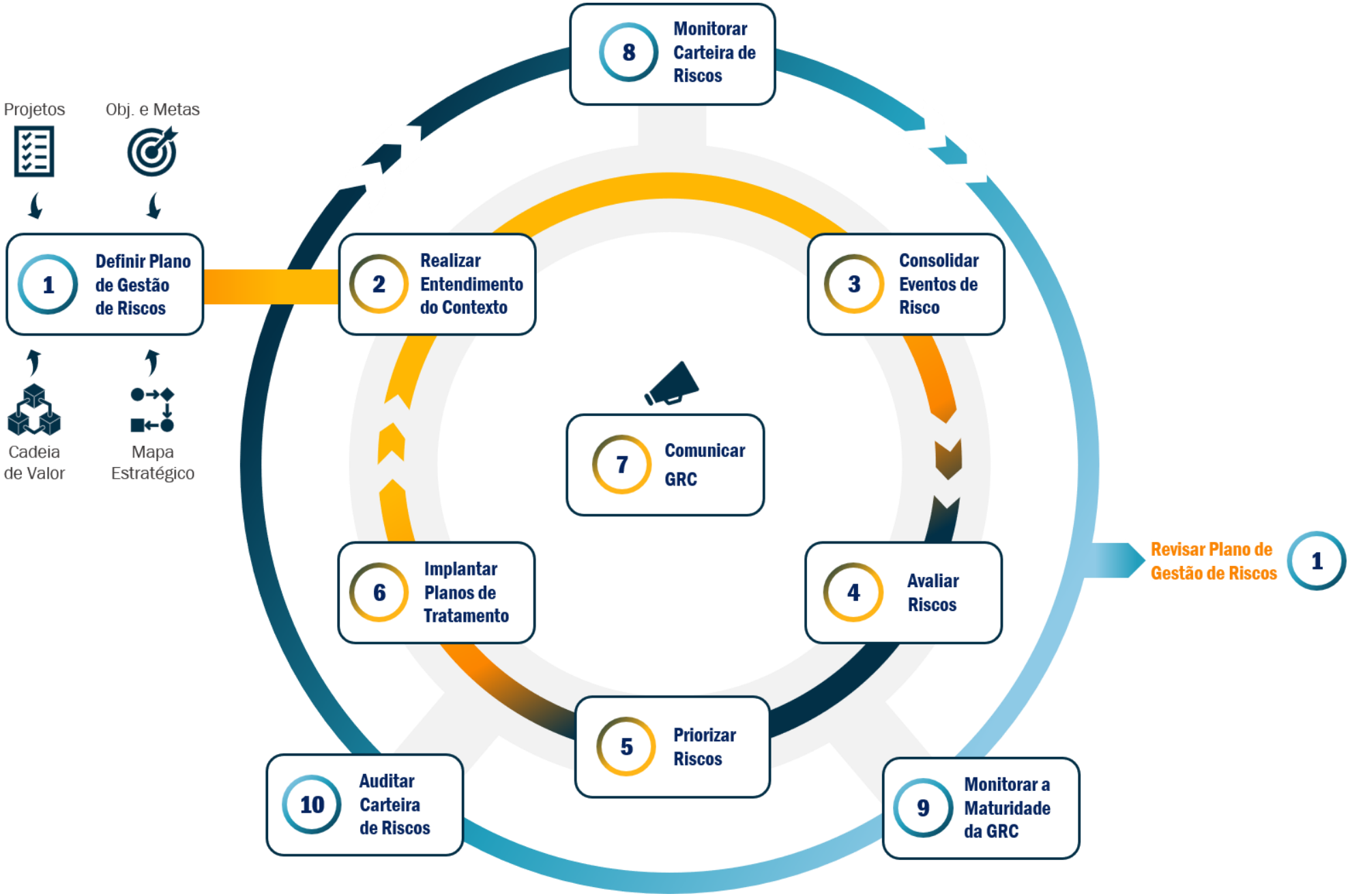
Framework do Processo

Apresentar a interação dos processos entre si de forma macro.

Para melhor entendimento das sequências de execução dos processos da metodologia de Gestão de Riscos Corporativos (GRC) e suas correlações e dependências foi elaborado um *Framework* do novo Ciclo de GRC da Anvisa.

Tal conjunto de processos que compõe a metodologia pode ser aplicado tanto para identificação e gestão de riscos estratégicos quanto táticos.

O *framework* de GRC é composto por 10 processos. Estes processos podem ser divididos em 2 grandes ciclos no que se refere à execução e à avaliação da carteira de riscos. Primeiramente, temos o ciclo de dentro – execução – com o processo 1 sendo o *input* para o começo do ciclo. Nesse processo, insumos como projetos, objetivos, metas, mapa estratégico e cadeia de valor são essenciais para uma boa execução. Definido o plano de gestão de riscos, inicia-se o ciclo de execução da carteira de riscos, contemplando os processos 2, 3, 4 5 e 6. O processo 7 de comunicação da GRC encontra-se no centro dos dois ciclos, pelo fato de a comunicação ocorrer ao longo de todos os processos. Em seguida, temos o ciclo de fora que contempla os processos 8, 9 e 10. Estes processos são processos de avaliação, ou seja, eles monitoram e auditam o que está sendo feito ou já foi feito durante a execução. Por fim, o ciclo de avaliação tem um possível *output* como “Revisar Plano de Gestão de Riscos”. Neste caso, ao identificar a necessidade de revisão, deve-se redirecionar para o processo 1 e revisitar o *framework* novamente.


Projetos
Obj. e Metas
1 Definir Plano de Gestão de Riscos
Cadeia de Valor
Mapa Estratégico
2 Realizar Entendimento do Contexto
3 Consolidar Eventos de Risco
4 Avaliar Riscos
5 Priorizar Riscos
6 Implantar Planos de Tratamento
7 Comunicar GRC
8 Monitorar Carteira de Riscos
9 Monitorar a Maturidade da GRC
10 Auditar Carteira de Riscos
Revisar Plano de Gestão de Riscos 1

O primeiro processo refere-se à definição do plano de gestão de riscos. Este está fora do ciclo de execução em si, uma vez que, com o objeto definido, esse processo será revisitado apenas quando houver a necessidade de atualização ou criação de um plano de gestão de riscos, como no caso de mudança de contexto ou de prioridades estratégicas. Sendo assim, seu objetivo principal é definir o objeto da gestão de riscos, escopo e cronograma para ao final ter um plano formalizado. Ademais, projetos, metas, cadeia de valor e mapa estratégico são insumos chaves para a execução do deste primeiro processo.

Definido o objeto da gestão de riscos, será necessário realizar o entendimento do contexto. Esse processo tem como objetivo levantar e categorizar percepções de risco, podendo ser repetido ou revisitado ao longo do ciclo sempre que uma nova percepção de risco for identificada.

Após o levantamento e categorização de percepções de riscos, o processo 3 consolida essas percepções de risco em eventos de risco, ou seja, agrupa ou insere novos eventos de riscos na carteira de riscos original. Dessa forma, o processo se conclui com a consolidação dos riscos na **Ferramenta de Identificação de Contexto e Instrumentos.**

Com os riscos consolidados, será preciso avaliá-los. Sendo assim, no processo 4, é realizado Workshop GRC para que seja feita a avaliação de cada risco. Concluída a avaliação dos riscos, inicia-se o processo 5 para priorizá-los. É importante ressaltar que a priorização dos riscos táticos poderá ser feita no processo 4, uma vez que não é necessária uma formalização da avaliação dos riscos, como é exigido para os riscos estratégicos.

Feita a priorização dos riscos, o próximo passo é elaborar um plano de tratamento para os riscos.

O processo 6 começa inicialmente com a harmonização dos controles que foram levantados no Workshop GRC no Processo 4 (Avaliar Riscos), ou seja, as unidades deverão indicar os controles considerados mais eficazes e viáveis de serem implementados em suas rotinas de mitigação dos riscos. Com a priorização dos controles, o próximo processo será o de elaboração do plano de tratamento. É nessa etapa que as unidades devem definir etapas, prazos e custos para implementação dos controles. Sendo assim, o processo será finalizado com o plano de tratamento e os controles sendo implementados. Além disso, é possível perceber pela figura que o ciclo é finalizado, uma vez que a parte de execução é concretizada.

Seguindo a sequência dos processos, a ordem seria o processo 7. Porém, é importante ressaltar que o processo 7 "Comunicar Gestão de Riscos" ocorre ao longo de todo o *framework* GRC, uma vez que a necessidade de comunicação pode ocorrer em qualquer momento das etapas de GRC. A corneta no centro da figura representa a comunicação ao longo de todo o ciclo GRC.

Dando continuidade, finalizamos o ciclo de execução e iniciamos o ciclo de avaliação. Com os controles e os planos de tratamento implementados, será necessário monitorar a carteira de riscos para verificar se os controles estão sendo eficientes. O processo 8 tem como objetivo fazer o monitoramento dos riscos e controles e direcionar encaminhamentos ou ações com base nos resultados obtidos no próprio monitoramento.

Em seguida, o processo 9 "Monitorar a Maturidade da GRC" tem como objetivo analisar a maturidade dos processos da Gestão de Riscos Corporativos na Anvisa. Dessa forma, são definidas dimensões para avaliação e coleta de insumos.

Ao final do processo, é possível criar um relatório com os insumos coletados para maior entendimento da maturidade dos processos de modo que medidas possam ser tomadas para a melhoria continua da cultura e dos processos da GRC na Anvisa. Em seguida, o processo 10 tem como objetivo realizar a auditoria nas unidades e disponibilizar insumos e pontos de atenção e melhoria para as áreas.

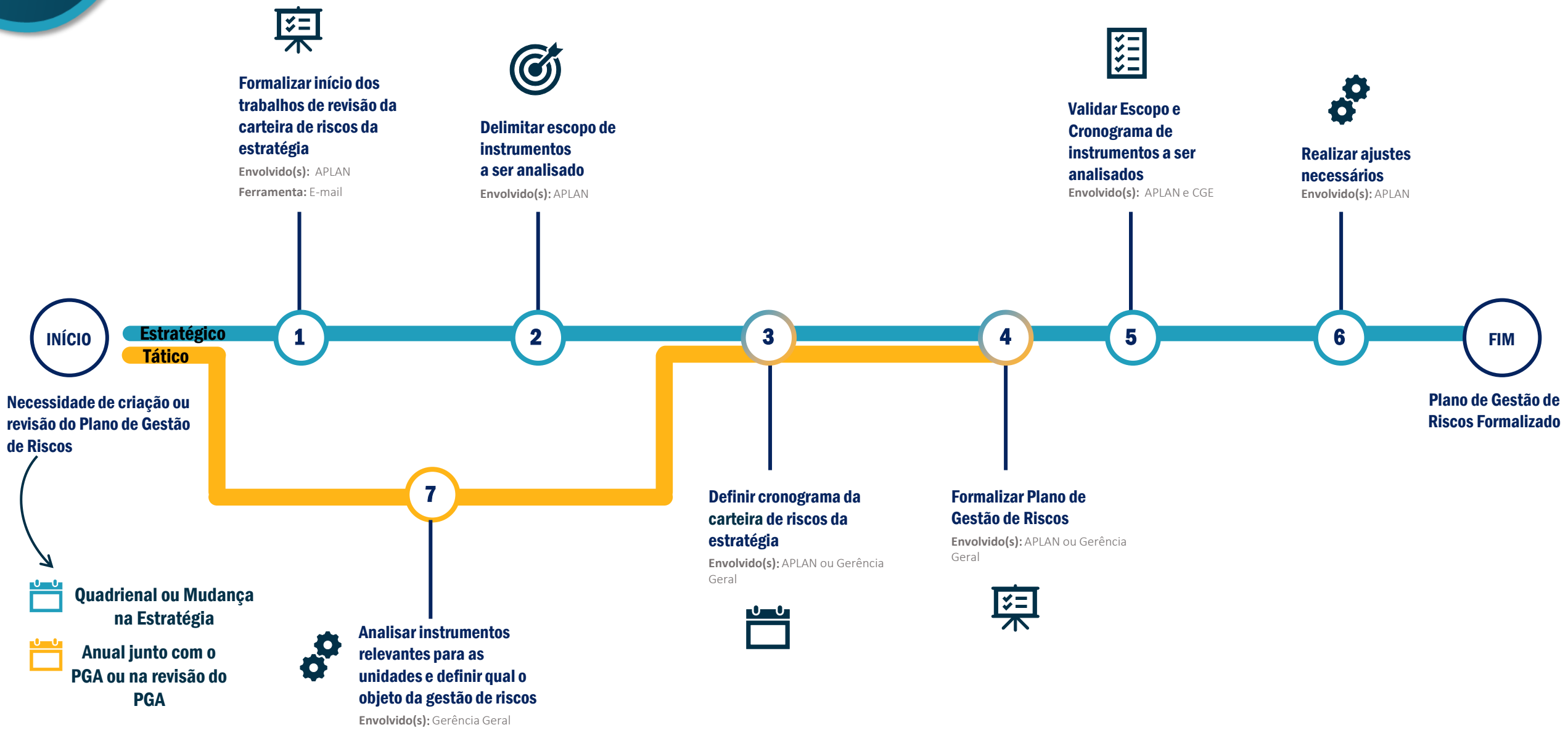
Por fim, é possível verificar na figura que, com o monitoramento das etapas de GRC, é possível identificar a necessidade de revisar a carteira de riscos. Sendo assim, deve-se direcionar para o processo 1 e todos os ciclos revisitados. Ademais, uma vez que a carteira de riscos é formada e finalizada, o próximo passo pode ser apenas fazer uma revisão ou começar um novo processo de GRC seguindo todo o *framework* novamente.

3

Detalhamento dos Processos

Apresentar o detalhamento individual de cada processo.

P1 DEFINIR PLANO DE GESTÃO DE RISCOS



DESCRIÇÃO

No que se refere aos riscos estratégicos, esse processo ocorre quando há a necessidade de criar, revisar, atualizar ou mudar a carteira de riscos da estratégia, seja por uma mudança na estratégia geral da Anvisa ou um novo ciclo que se inicia. No que se refere aos riscos táticos, esse processo ocorre quando há a necessidade de revisar, criar ou mudar a carteira de riscos tático, seja anualmente junto com o Plano de Gestão Anual (PGA) ou na revisão do PGA.

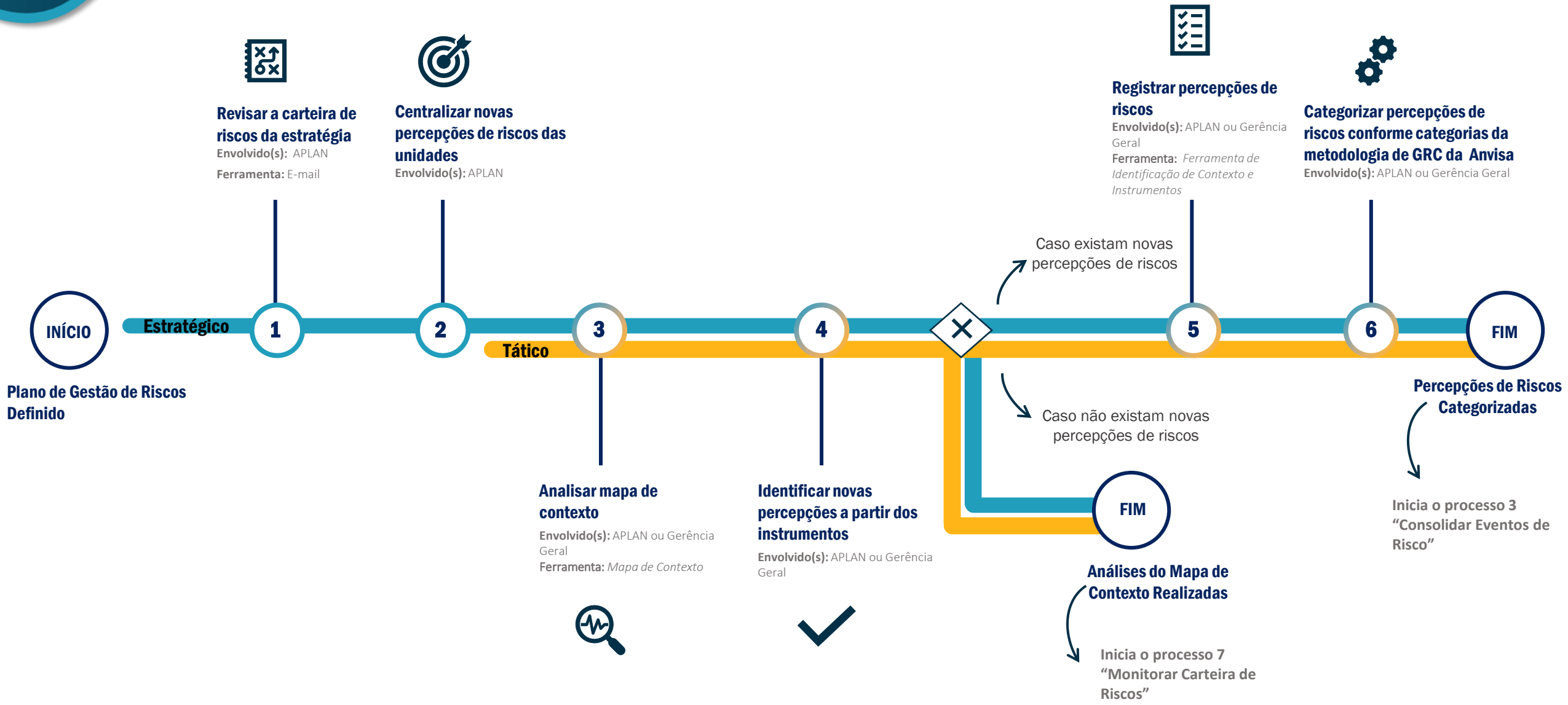
Seu principal objetivo é ter um plano de gestão de riscos formalizado. Sendo assim, o escopo/objeto de análise e o cronograma devem ser definidos nesse processo.

OBSERVAÇÕES:

! A formalização do início dos trabalhos de revisão da carteira de riscos da estratégia poderá ser feita por e-mail para comunicar toda a Agência que o processo de GRC acontecerá.

! O cronograma deverá conter todas as etapas e possíveis datas para a realização de todos os processos de GRC, para que seja feito um pré-agendamento das reuniões e workshops.

P2 REALIZAR ENTENDIMENTO DO CONTEXTO



DESCRIÇÃO

Esse processo ocorre quando, após definido o plano de gestão de riscos, deseja-se realizar o entendimento do contexto dos riscos estratégicos ou táticos, a fim de verificar se existem novas percepções de riscos que devem ser analisadas, visando a atualização de novos eventos de riscos em uma carteira de riscos existente ou a definição de nova carteira de riscos. Dessa forma, o processo só estará concluído com as percepções de risco categorizadas. Sendo assim, deverá se fazer as análises necessárias, além de coletar as percepções com as unidades para atingimento de tal resultado.

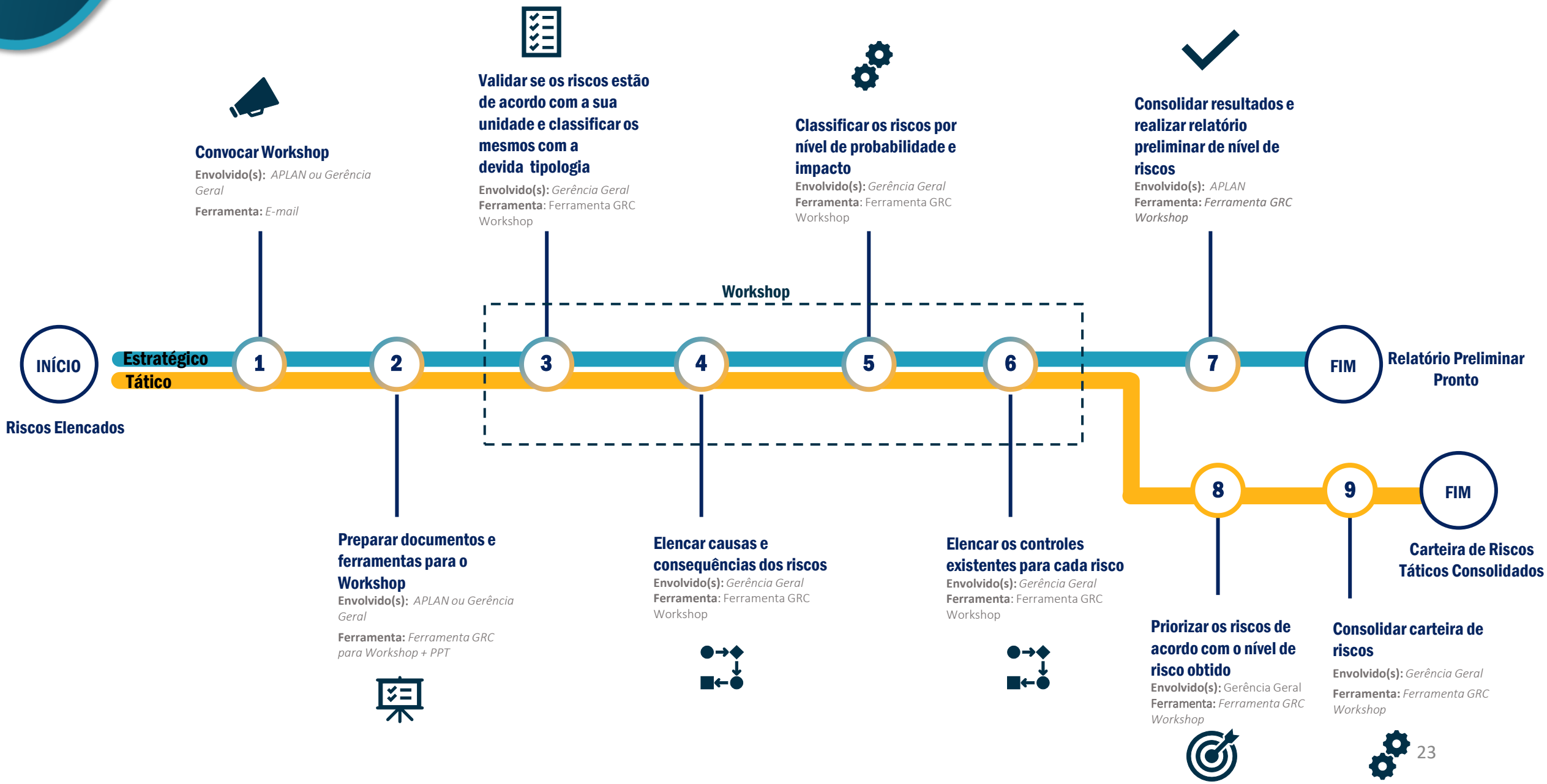
OBSERVAÇÕES:

! Para a realização da análise de contexto, deverá se analisar cada uma das dimensões do mapa de contexto apresentado a seguir, assim como as megatendências, SWOT e PESTAL do plano estratégico, metas estratégicas, processos críticos e OKRs para levantar as percepções de riscos.

Mapa de Contexto elaborado por EloGroup

P3 CONSOLIDAR EVENTOS DE RISCO

P4 AVALIAR RISCOS



DESCRIÇÃO

Esse processo ocorre quando, uma vez que os riscos foram elencados ou novos riscos foram contemplados na carteira de riscos, deseja-se então fazer a avaliação deles. A avaliação dos riscos será realizada durante um **Workshop que possui 5 etapas** que serão detalhadas a seguir:

- **1ª Etapa:** Validar se os riscos apresentados na ferramenta estão de acordo com o que foi discutido anteriormente, ou seja, se aqueles riscos de fato são riscos que afetam sua unidade.

- **2ª Etapa:** Feita a avaliação dos riscos deverá se classificar a tipologia dos riscos, podendo os riscos serem classificados como: operacional, imagem, legal, financeiro e integridade.

- **3ª Etapa:** Após classificar a tipologia dos riscos, deverá se elencar as causas e consequências dos riscos.

- **4ª Etapa:** Após elencar as causas e consequências, deverá se classificar os riscos por nível de probabilidade e impacto, ambas em uma escala de 1 a 5, sendo 1 como uma probabilidade ou um impacto muito baixo e 5 sendo uma probabilidade ou um impacto muito alto.

- **5ª Etapa:** Feita a classificação por nível de probabilidade e impacto, deverá se elencar os controles existentes para cada risco. Além disso, indicar se o controle é novo ou se já existe a mais tempo, o tipo de controle, se ele é preventivo ou de atenuação e classificar com uma nota de 1 a 5, sendo 1 para controle ineficiente e 5 para controle muito forte.

OBSERVAÇÕES:

! O Workshop será realizado na Ferramenta Workshop GRC.

P5 PRIORIZAR RISCOS (ESTRATÉGICOS)

INÍCIO

Riscos Elencados e Avaliados

Estratégico

1 — Avaliar probabilidade e impacto dos riscos elencados pelas unidades
Envolvido(s): *CGE*
Ferramenta: *: Ferramenta de priorização*

2 — Fazer ajustes caso necessário
Envolvido(s): *CGE*
Ferramenta: *: Ferramenta de priorização*

3 — Selecionar riscos prioritários
Envolvido(s): *CGE*
Ferramenta: *: Ferramenta de priorização*

4 — Consolidar apontamentos dos membros do CGE com as respostas prévias das unidades
Envolvido(s): *APLAN*
Ferramenta: *Ferramenta de priorização*

5 — Priorizar riscos de acordo com os riscos inerentes obtidos
Envolvido(s): *CGE*
Ferramenta: *Ferramenta de priorização*

6 — Consolidar carteira de riscos da estratégia
Envolvido(s): *APLAN ou Gerência Geral*
Ferramenta: *: Ferramenta de priorização*

7 — Validar carteira de riscos da estratégia
Envolvido(s): *Diretoria*
Ferramenta: *: Ferramenta de priorização*

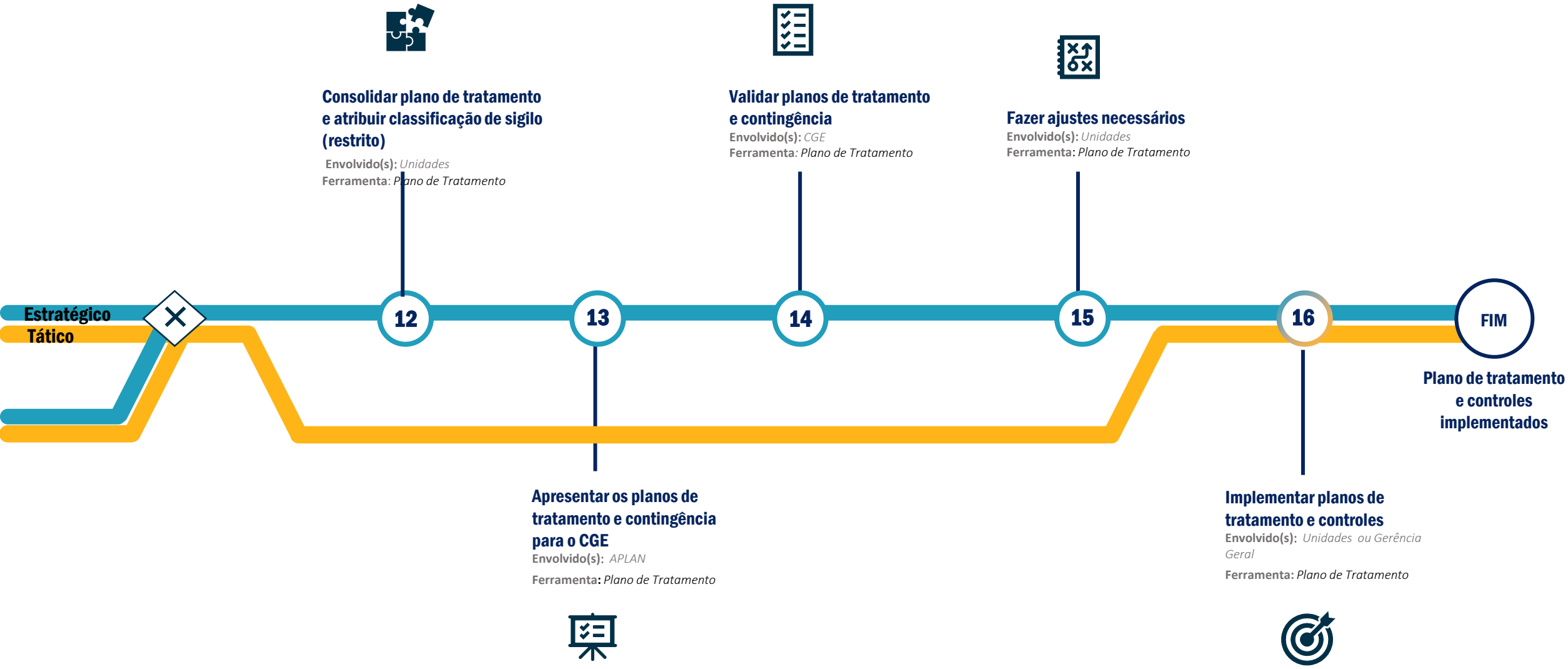
FIM

Carteira de riscos consolidada

Tático

Priorização dos Riscos Táticos ocorre junto do Workshop no Processo "4. Avaliar Riscos"

P6 IMPLANTAR PLANO DE TRATAMENTO


Consolidar plano de tratamento e atribuir classificação de sigilo (restrito)
Envolvido(s): Unidades
Ferramenta: Plano de Tratamento
Validar planos de tratamento e contingência
Envolvido(s): CGE
Ferramenta: Plano de Tratamento
Fazer ajustes necessários
Envolvido(s): Unidades
Ferramenta: Plano de Tratamento
Estratégico
Tático
12
13
14
15
16
FIM
Plano de tratamento e controles implementados
Apresentar os planos de tratamento e contingência para o CGE
Envolvido(s): APLAN
Ferramenta: Plano de Tratamento
Implementar planos de tratamento e controles
Envolvido(s): Unidades ou Gerência Geral
Ferramenta: Plano de Tratamento

DESCRIÇÃO

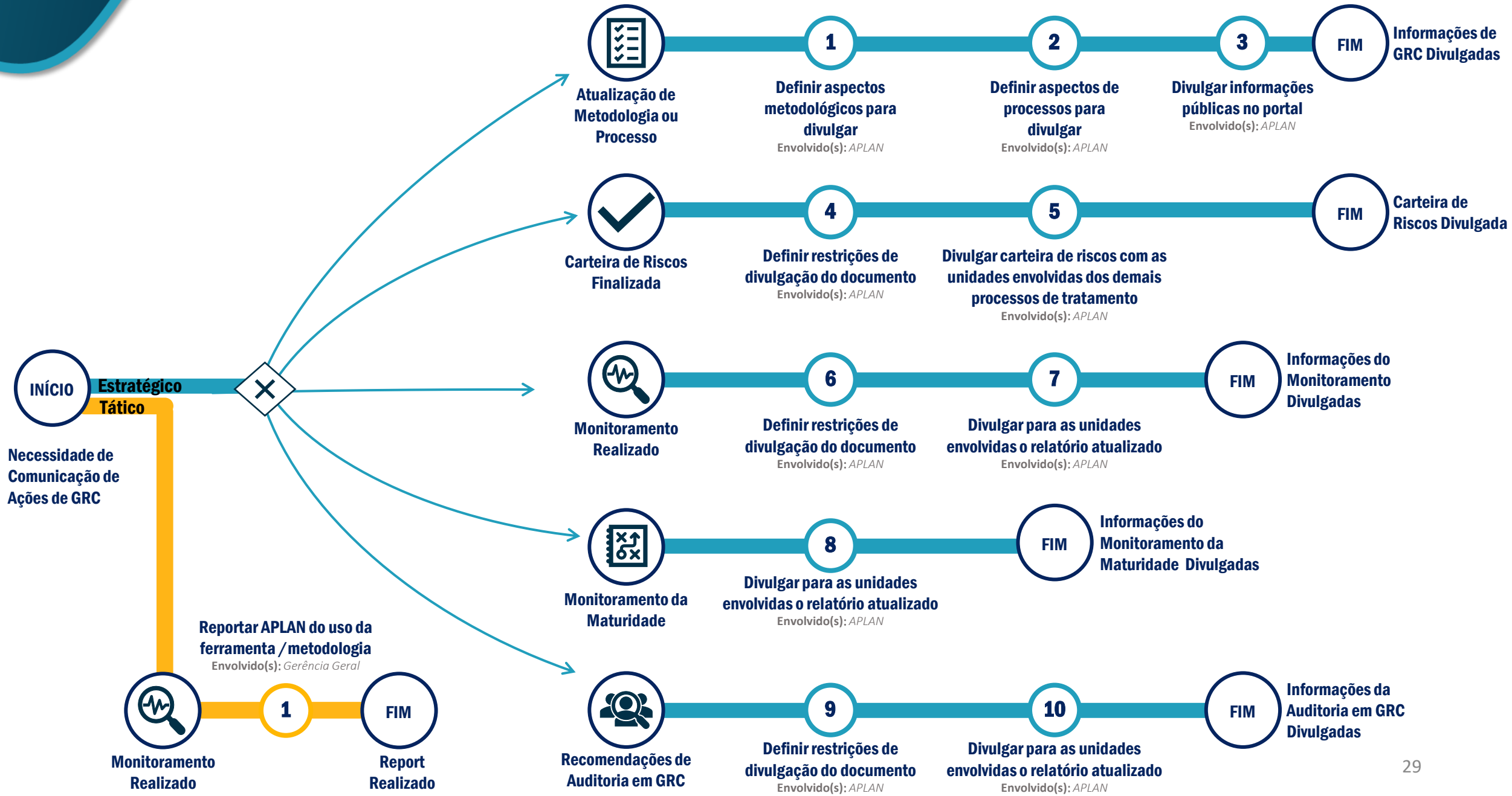
Uma vez que se tem os riscos priorizados e a carteira de riscos consolidada, é preciso realizar a harmonização dos controles que foram propostos no Workshop GRC no caso dos riscos estratégicos. Após a reunião, com os controles harmonizados, o objetivo do processo é criar um plano de tratamento da unidade para cada um dos riscos. Sendo assim, o processo apenas finaliza com os planos de tratamento e os controles que foram priorizados anteriormente implementados.

OBSERVAÇÕES:

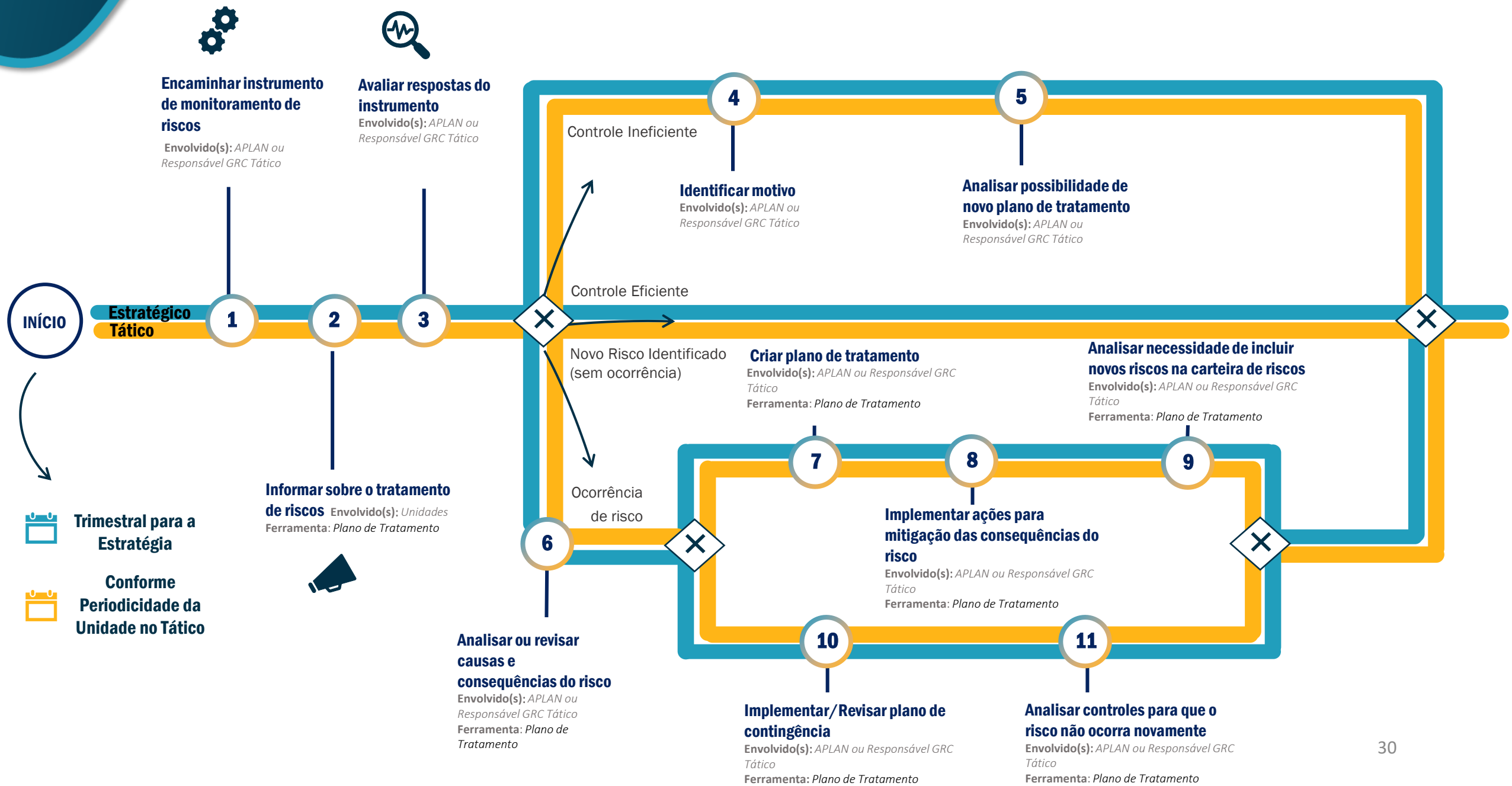
! Na reunião de harmonização de controles estratégicos, as unidades deverão harmonizar os controles, ou seja, as unidades precisarão selecionar aqueles controles que elas julgam mais efetivos e que elas gostariam de implementar em suas áreas.

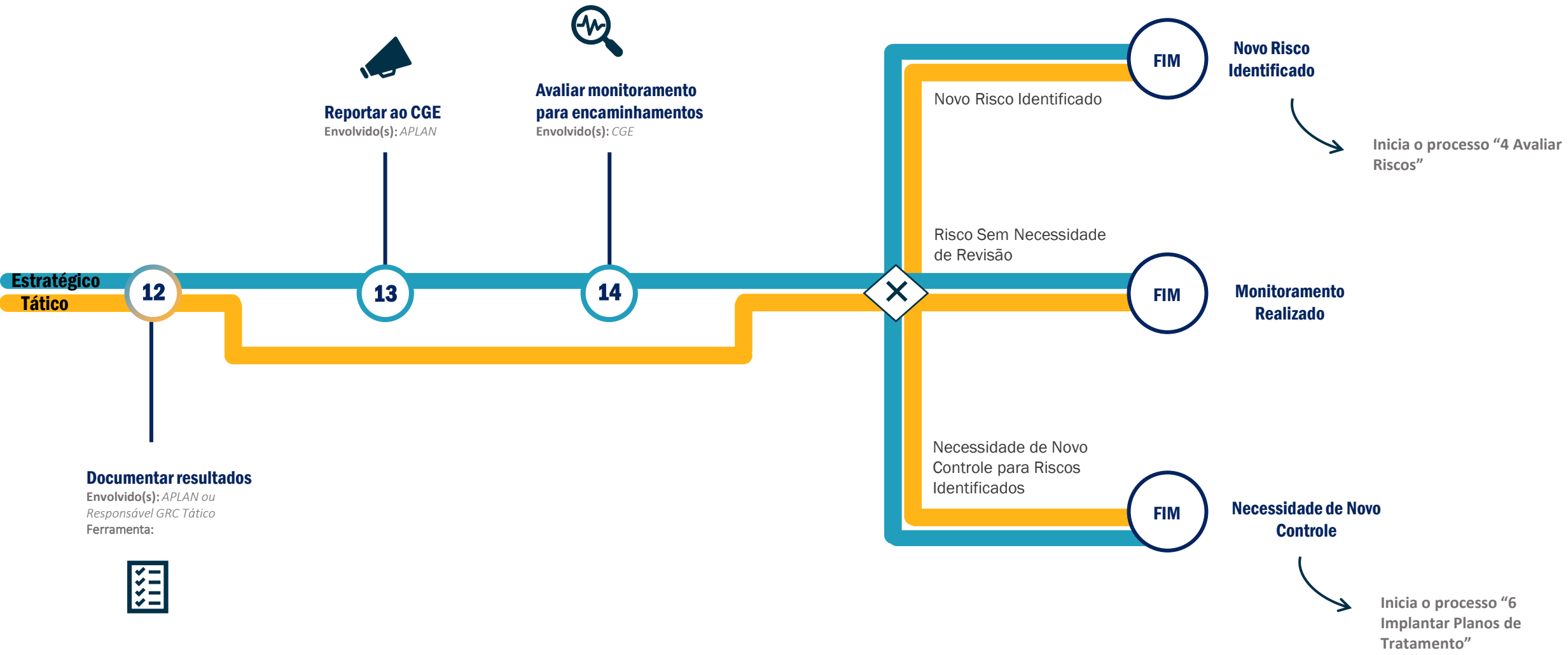
! A reunião de harmonização de controles é realizada na Ferramenta Harmonização de Controles.

P7 COMUNICAR GESTÃO DE RISCOS

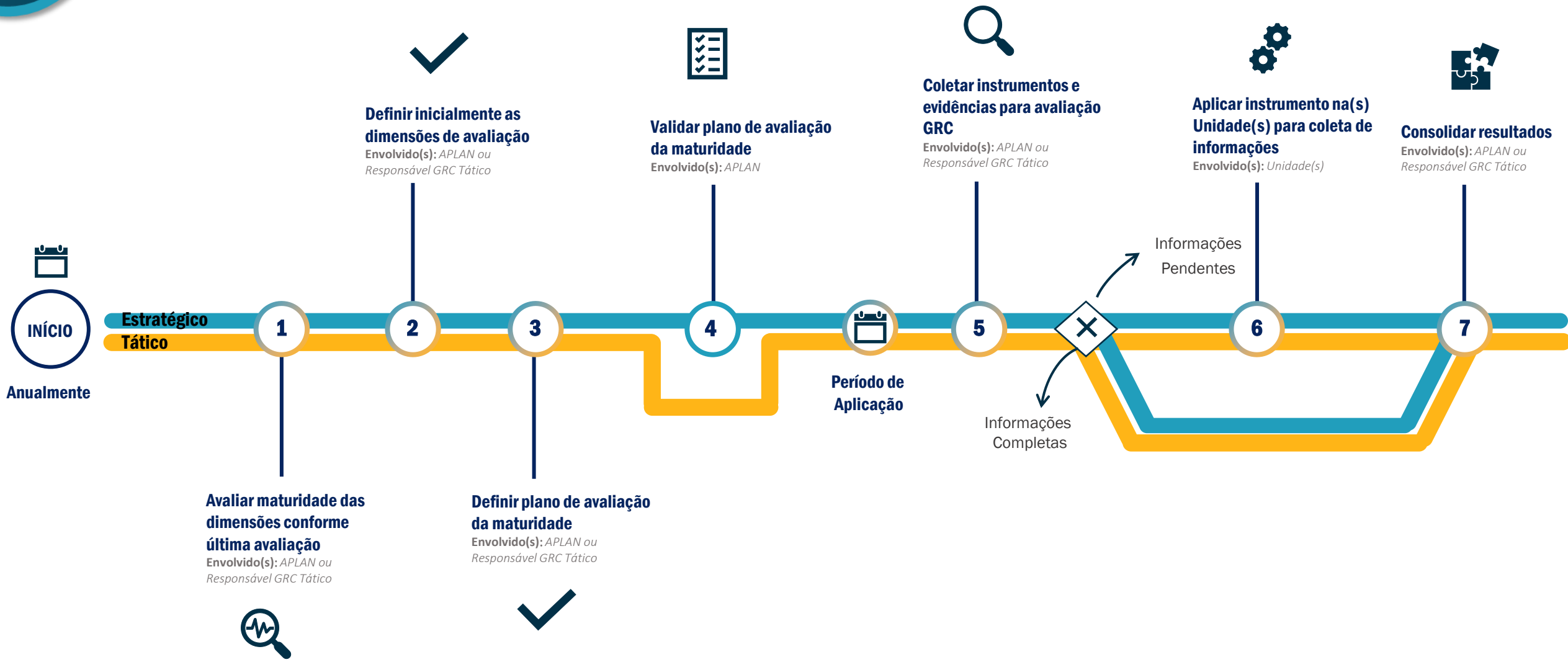


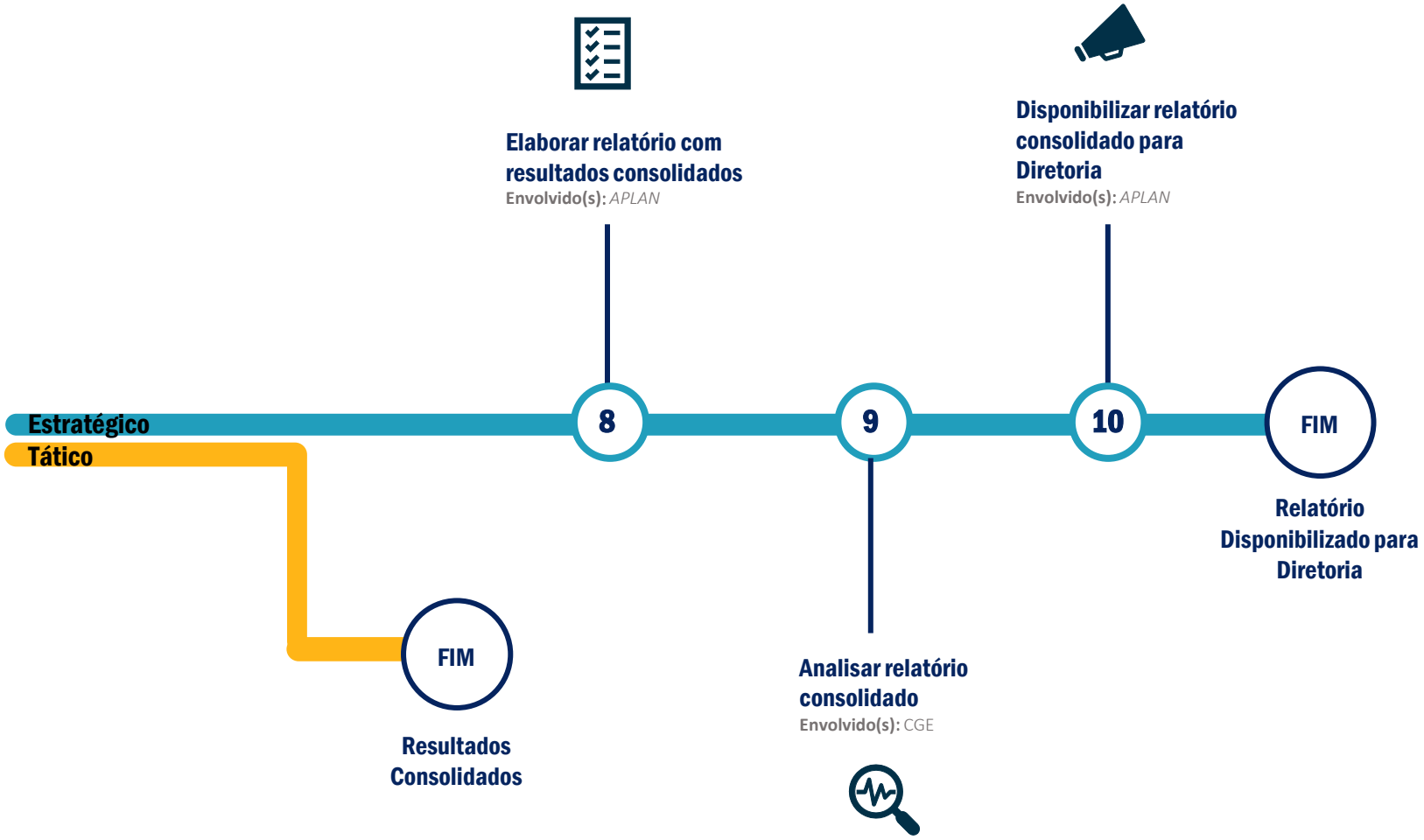
P8 MONITORAR CARTEIRA DE RISCOS




Reportar ao CGE
Envolvido(s): APLAN
Avaliar monitoramento para encaminhamentos
Envolvido(s): CGE
Estratégico
Tático
12
13
14
Documentar resultados
Envolvido(s): APLAN ou Responsável GRC Tático
Ferramenta:
Novo Risco Identificado
Risco Sem Necessidade de Revisão
Necessidade de Novo Controle para Riscos Identificados
FIM
Novo Risco Identificado
Inicia o processo "4 Avaliar Riscos"
FIM
Monitoramento Realizado
FIM
Necessidade de Novo Controle
Inicia o processo "6 Implantar Planos de Tratamento"

P9 MONITORAR A MATURIDADE DA GRC




Elaborar relatório com resultados consolidados
Envolvido(s): APLAN
Disponibilizar relatório consolidado para Diretoria
Envolvido(s): APLAN
Estratégico
Tático
8
9
10
FIM
Relatório Disponibilizado para Diretoria
FIM
Resultados Consolidados
Analisar relatório consolidado
Envolvido(s): CGE

P10 AUDITAR CARTEIRA DE RISCOS

DESCRIÇÃO

Esse processo acontece quando, no período de auditoria individual da(s) unidade(s), a equipe de auditoria realiza a auditoria dentro da(s) unidade(s) e levanta pontos relacionados à GRC estratégico para serem posteriormente analisados. Dessa forma, o processo pode ser encerrado das seguintes formas: implementação das recomendações presentes no relatório; identificação da necessidade de revisão dos riscos identificados; ou conclusão da auditoria.

OBSERVAÇÕES:

! O *Gateway* Inclusivo (com círculo dentro) permite que fluxos paralelos ocorram, dependendo de uma condição pré-determinada. Sendo assim, toda vez que for elaborado um relatório de auditoria, este deverá ser enviado às unidade interessadas. Essa condição de "sempre" está representada pelo o símbolo (/) dentro do fluxo. Porém, quando existir pontos relacionados à GRC da estratégica, além de se enviar às unidades – atividade 6 – deverá se enviar também à APLAN para que esta possa analisar os resultados e apresentar recomendações ou propostas de melhoria para o Comitê Gestor da Estratégia (CGE) – atividade 4 -, ou seja, essas ações acontecerão em paralelo uma vez que a condição "pontos relacionados à GRC Estratégica for atendida.

4

Atores, Perfis e Competências

Após a apresentação dos processos de Gestão de Riscos na ANVISA, se faz necessário apresentar os principais atores que a compõem, os perfis e competências desejados.

APLAN

Garantir a execução dos processos da GRC e realizar apoio técnico-metodológico.

CGE

Validar, aprovar e alterar documentos e processos da GRC. O CGE pode incluir, alterar e excluir riscos da carteira de riscos estratégicos. Além disso, sua avaliação possui um peso de 60% em relação às unidades na priorização dos riscos.

RESPONSÁVEL GRC / AGENTES DE RISCO CORPORATIVOS

Pessoa com a responsabilidade e autoridade para gerenciar um risco.

DIRETOR- PRESIDENTE

Cumprir e fazer cumprir a Política de Gestão de Riscos Corporativos da Agência. Além de instituir o Comitê que tratará da temática de Gestão de Riscos Corporativos e designar a Secretaria Executiva para suporte técnico e operacional ao Comitê.

DIRETORIA COLEGIADA

Responsável por aprovar a Política de Gestão de Riscos Corporativos e suas revisões. Além de assegurar a alocação dos recursos necessários à implantação da política.

UNIDADES

Executar os processos da GRC em relação aos riscos estratégicos e táticos, participar de Workshops, alimentar as ferramentas de GRC e implementar a gestão de riscos corporativos em sua unidade organizacional.

5

Ferramentas e Documentos de Apoio

Ferramentas para a operacionalização dos processos de negócio apresentados.

Para a execução dos processos da GRC, foram criadas ferramentas de apoio. Cada uma das ferramentas será apresentada a seguir com algumas informações relevantes à sua utilização.

Ferramenta de Identificação de Contexto e Instrumentos (Plano de Gestão de Riscos Corporativos)

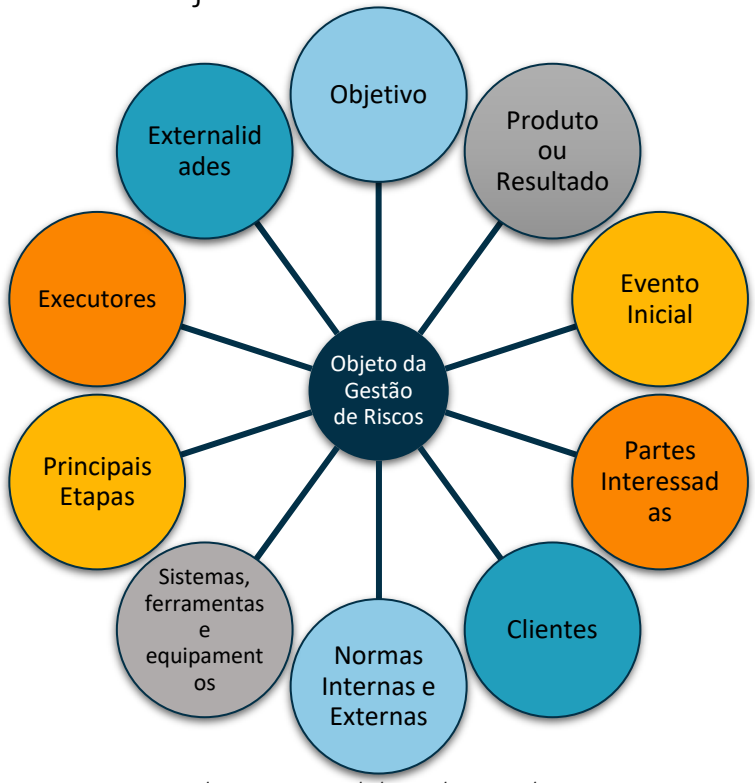
Ferramenta inicial utilizada para centralizar percepções de risco identificadas pelas unidades. Nessa ferramenta, é possível compilar todas as informações e fazer cruzamentos entre processos e objetivos estratégicos da unidade, avaliando suas relações e convertendo as percepções identificadas em eventos de risco, mantendo um histórico de dados relevantes de origem de cada evento.

(TB_1) IDENTIFICAÇÃO DE PERCEPÇÕES E EVENTOS DE RISCO — Sequência de preenchimento: Todas as colunas até "Evento de risco"

Objetivo Estratégico (2)	Processo/Etapa (1º nível)	Processo crítico (2º nível) ou evento crítico	Fonte	REF INSTRUMENTO	Responsável	Percepções de risco	Categoria da percepção	EVENTO DE RISCO

Mapa de Contexto

Lógica contida na ferramenta de identificação de contexto. Deve ser considerada para realização do entendimento do contexto no Processo 2 "Realizar Entendimento do Contexto". Com ela, é possível passar por cada dimensão levantando percepções de riscos que podem estar associadas ao objeto da Gestão de Riscos.



Mapa de Contexto elaborado por EloGroup

Ferramenta Workshop GRC

Principal ferramenta produzida no Excel, que será utilizada pelas Unidades no Workshop de Avaliação dos Riscos presente no Processo 4 "Avaliar Riscos". Nessa ferramenta, será possível que cada unidade valide os riscos para ver se estes estão de acordo com seus processos, ou seja, para verificar se aquele risco de fato afeta sua unidade. Após validar os riscos, as unidades poderão classificar a tipologia de riscos. Em seguida, indicar suas causas e consequências. Depois, indicar controles existentes para mitigar os riscos. Por fim, avaliar a probabilidade e impacto dos riscos. É importante ressaltar que cada Unidade terá sua planilha para a realização do Workshop.

Ferramenta Workshop GRC

C, D, E. LISTA COMPLETA DE EVENTOS DE RISCO

27 0

EVENTOS DE RISCO	ALOCAÇÃO ATUAL	NOVA ALOCAÇÃO	TIPOLOGIA DE RISCO
Estrutura Organizacional			
EO1. Baixo apoio da governança (alta gestão) com as entregas previstas	✓		
EO2. Alteração na cadeia de comando e/ou na estrutura organizacional da Anvisa	✓		
EO3. Regulamentação desproporcional ou desatualizada em relação à realidade do mercado regulado	✓		
EO4. Falhas no desdobramento estratégico interno da Anvisa	✓		
	-		

AVALIAÇÃO DE PROBABILIDADE E IMPACTO

EVENTO	NOTA	PROBABILIDADE	NOTA	IMPACTO

Ferramenta de priorização – Uso exclusivo do CGE

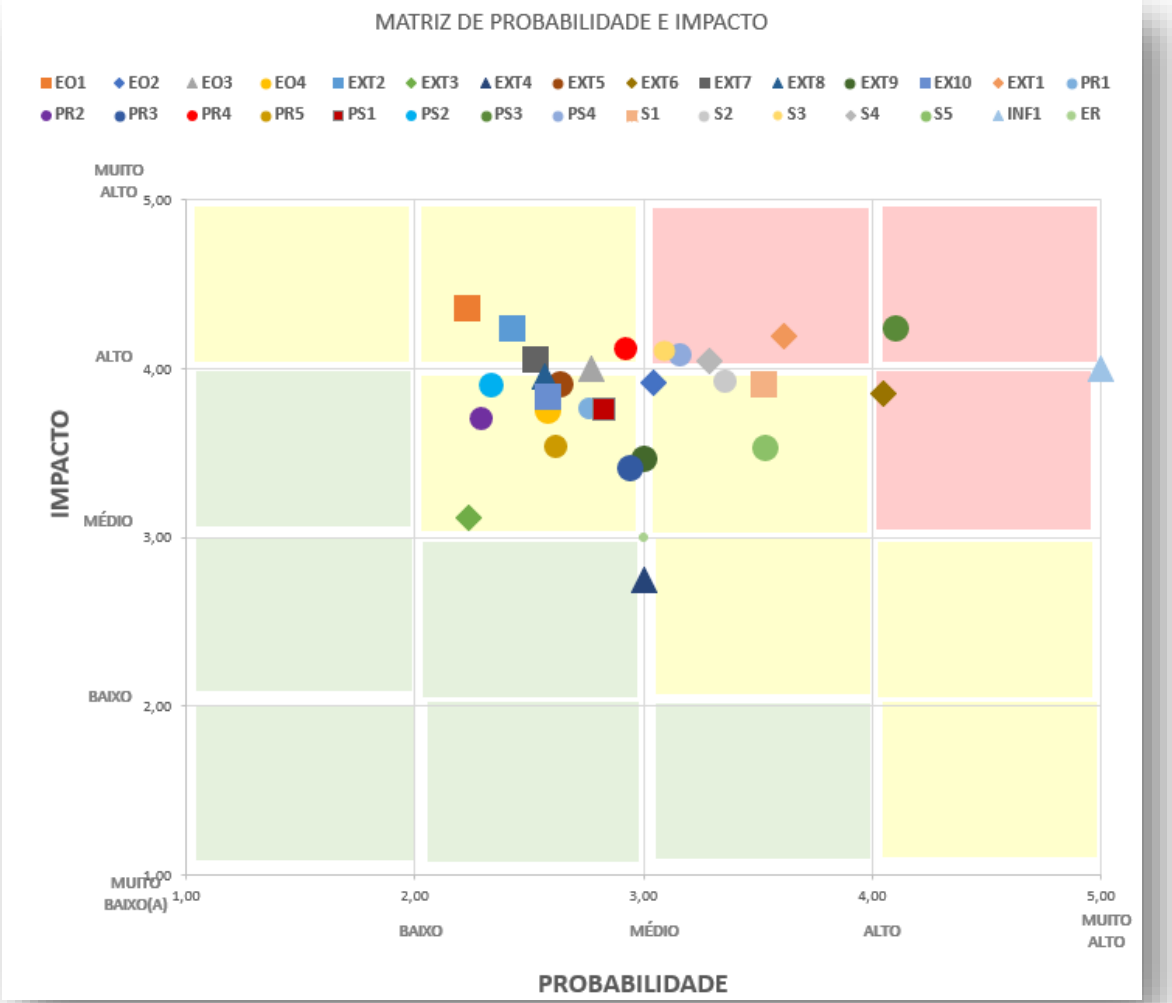
Ferramenta que será utilizada para a priorização dos riscos, etapa presente no Processo 5 "Priorizar Riscos". Desenvolvida no Excel, essa ferramenta apresenta uma consolidação das informações da ferramenta de Workshop GRC. Com dados gerados automaticamente, essa planilha permite que o CGE consiga visualizar todas as informações e avaliações feitas pelas unidades em relação aos riscos e faça sua própria priorização. Ao julgar a probabilidade e impacto de cada risco, a planilha irá calcular automaticamente a nova probabilidade e o novo impacto levando em conta um peso de 60% as notas dadas pelo CGE e 40% as notas dadas pelas unidades. Além disso, o CGE poderá comentar possíveis alterações, remoções e inclusões de riscos.

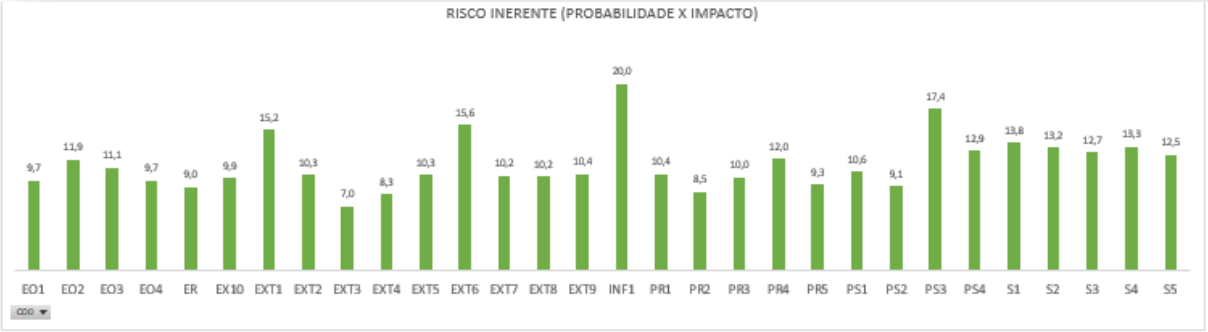
GRC ANVISA - PROBABILIDADE E IMPACTO - CGE

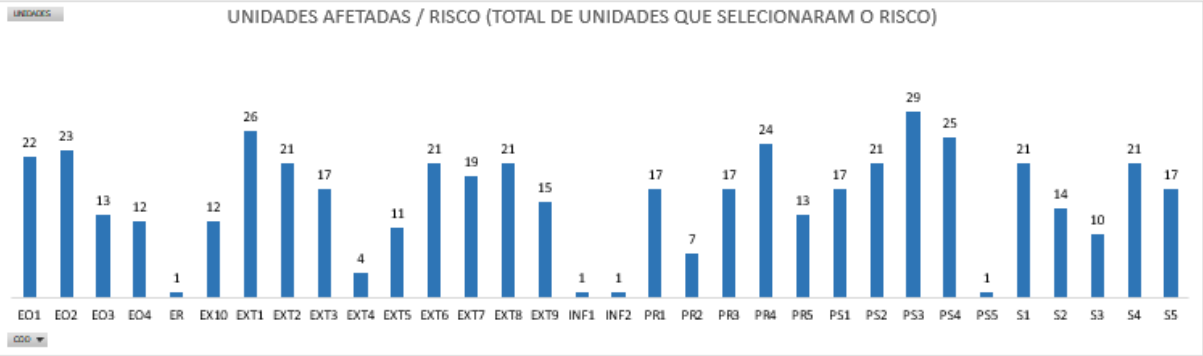
(TB_3) AVALIAÇÃO DE EVENTOS CGE						
COD	EVENTO	PROBABILIDADE	PROB TXT	IMPACTO	IMPCT TXT	RISCO INERENTE
EO1	EO1. Baixo apoio da governança (alta gestão) com as entregas previstas					0
EO2	EO2. Alteração na cadeia de comando e/ou na estrutura organizacional da Anvisa					0
EO3	EO3. Regulamentação desproporcional ou desatualizada em relação à realidade do mercado regulado					0
EO4	EO4. Falhas no desdobramento estratégico interno da Anvisa					0
EXT1	EXT1. Aumento significativo da entrada de demandas					0

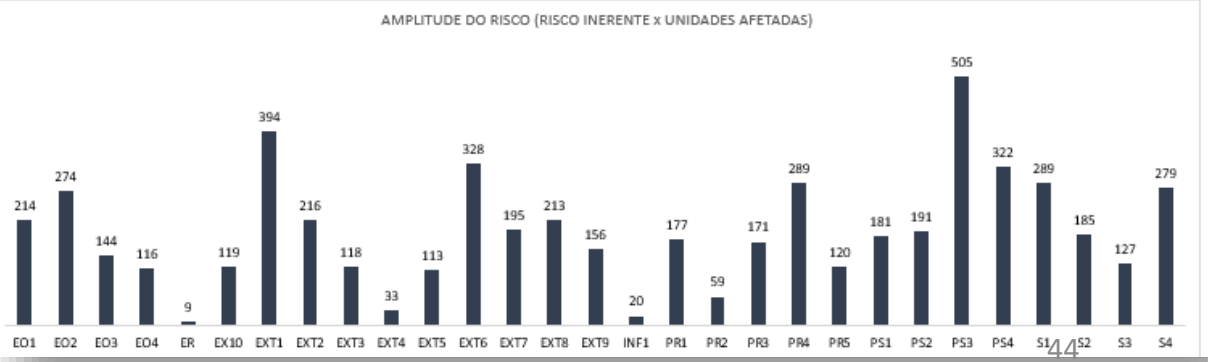
Ferramenta de priorização - CGE

A fim de apoiar o preenchimento, a ferramenta conta com visualizações gráficas compiladas de dados preenchidos pelas unidades.









Ferramenta Harmonização de Controles

Principal ferramenta que será utilizada na reunião de Harmonização de Controles presente no Processo 6 "Implantar Plano de Tratamento". Desenvolvida no Excel, as Unidades poderão indicar aqueles controles que elas julgam mais efetivos e que elas gostariam de implementar em suas áreas, ou seja, a planilha apresenta uma consolidação de todos os controles registrados na Ferramenta Workshop GRC. Para realizarem a priorização, as unidades deverão analisar todos os controles da sua unidade que possuem o sinal "!" e alterar para o valor "–1", no caso de controles não priorizados, ou para o valor "1", no caso de controles que serão priorizados. Ao final da reunião, será possível visualizar todos os controles priorizados por cada unidade.

LISTAGEM DE CONTROLES

EVENTO	CONTROLE NORMALIZADO	NOTA MÉD	AVALIAÇÃO DO CONTROLI	AINT	APLA	ASCO	ASNV	ASPA	AUDI	CAJI	COGE	GADI	GELA
EO1. Baixo apoio da governança (alta gestão) com as entregas previstas	Alinhar os processos de trabalho e as normas internas e externas.	4,0	Forte	!	!		!			!		!	
EO1. Baixo apoio da governança (alta gestão) com as entregas previstas	Aperfeiçoar a governança interna da Agência e forma de funcionamento dos comitês temáticos de apoio à alta gestão	3,0	Satisfatório	!	!		!			!		!	
EO1. Baixo apoio da governança (alta gestão) com as entregas previstas	Estabelecer diálogo constante com o setor regulado para que as ações da Agência sejam apoiadas.	2,0	Mediano	!	!		!			!		!	
EO1. Baixo apoio da governança (alta gestão) com as entregas previstas	Estabelecer normativo para regulamentar processos internos.	3,0	Satisfatório	!	!		!			!		!	

Plano de Tratamento

Ferramenta que será utilizada pelos gestores das unidades para criar e monitorar os tratamentos dos riscos. Desenvolvida no Excel, essa planilha permitirá os gestores criarem controles para os riscos, indicarem responsáveis para cada um deles, definirem indicadores de eficiência da implementação do controle e controlar os monitoramentos. Além disso, a APLAN poderá verificar as unidades que estão preenchendo a ferramenta e analisar o status dos riscos de cada unidade.

Selecione a unidade usuária - >>>>>

EVENTOS DE RISCO COM DESCRITORES

GRUPO	EVENTO DE RISCO	DESCRITOR	RISCOS PRIORIZADOS		
			NÍVEL DE RISCO	PRIORIZAÇÃO	ÁREAS AFETADAS
Pessoas	PS3. Dificuldade de reposição de recursos humanos	Situação em que ocorre a diminuição do quadro de pessoal, ou o aumento da demanda na unidade organizacional sem a devida reposição, considerando a perda do conhecimento técnico, bem como o impacto no atendimento das demandas pela unidade organizacional	19,67	1	29
Pessoas	PS4. Incapacidade operacional de atendimento do volume de demandas atual	Situação em que a entrada de demandas da unidade é superior ao quantitativo de recursos humanos necessário para a sua execução	17,38	2	25
Externalidades	EXT1. Aumento significativo da entrada de demandas	Situação de aumento inesperado de demandas ou solicitações, superiores à capacidade habitual de entrega da unidade organizacional.	16,71	3	26
Sistemas	S1. Baixa capacidade operacional e de recursos para prover soluções de TI.	Situação de baixa disponibilidade ou capacidade da área de TI em atender às necessidades de seus clientes. Concorrência na capacidade operacional da equipe em conduzir os projetos de soluções de TI e as demais atividades de rotina.	15,26	4	21

SELETOR DE UNIDADE APLAN

RISCOS RELACIONADOS À UNIDADE

LISTA DE RISCOS	PRIORIZADOS	NÃO PRIORIZADO
PS4. Incapacidade operacional de atendimento do volume de demandas atual	●	
PR4. Falhas na execução do processo dificultando o alcance de metas institucionais ou prazos legais	●	
S5. Paineis gerencias pouco integrados ou com base de dados corrompidas ou não confiáveis	●	
EXT1. Aumento significativo da entrada de demandas	●	
PS3. Dificuldade de reposição de recursos humanos	●	

Plano de Tratamento

LISTA DE CONTROLES HARMONIZADOS POR RISCO

EVENTO	CONTROLE	CONTROLE PRIORIZADO	RISCO PRIORIZADO?
EO2. Alteração na cadeia de comando e/ou na estrutura organizacional da Anvisa	Comunicar periodicamente as ações e os resultados da unidade organizacional.	●	●
EO2. Alteração na cadeia de comando e/ou na estrutura organizacional da Anvisa	Estabelecer mecanismo de designação de responspáveis pelos projetos em andamento.	●	●
EO2. Alteração na cadeia de comando e/ou na estrutura organizacional da Anvisa	Realizar articulação periódica com a alta gestão e outras instâncias deliberativas (CGE. CETI, etc), buscando apoio para as ações estratégicas, reportando os avanços alcançados à diretoria.	●	●
EO2. Alteração na cadeia de comando e/ou na estrutura organizacional da Anvisa	Manter processos de trabalho atualizados, bem estabelecidos e eficientes	●	●
EO2. Alteração na cadeia de comando e/ou na estrutura organizacional da Anvisa	Realizar o planejamento tático-operacional alinhado ao planejamento estratégico, priorizando as entregas, realizando monitoramento, controle e avaliação.	●	●
EX10. Influência externa inadequada em procesos da agência (Integridade)	Promover transparência das decisões e da atuação regulatória da Agência.	●	●
EX10. Influência externa inadequada em procesos da agência (Integridade)	Elaborar pareceres com informações técnicas claras e objetivas	●	●

PLANO DE TRATAMENTO DE RISCOS

UNIDADE **APLAN**

EVENTOS DE RISCO PRIORITÁRIOS DA ESTRATÉGIA EM MONITORAMENTO

RISCO	DESCRIÇÃO	CAUSAS NA UNIDADE	CONSEQUÊNCIAS NA UNIDADE	NÍVEL DE RISCO
PR4. Falhas na execução do processo dificultando o alcance de metas institucionais ou prazos legais		meta estratégica não definida adequadamente (Ex: métrica, relevância, viabilidade)	Insumos de monitoramento das metas e dos projetos estratégicos insuficiente para uma efetiva tomada de decição pela alta gestão	

CONTROLES IMPLEMENTADOS PARA TRATAMENTO

RISCO	CONTROLE	TIPO	RESPONSÁVEL	NÍVEL DE RISCO	FORÇA DO CONTROLE

6

Siglas e Termos

Um resumo das siglas citadas ao longo do Book com o intuito de auxiliar o leitor.

- **ANVISA** – Agência Nacional de Vigilância Sanitária;
- **APLAN** – Assessoria de Planejamento;
- **CGE** – Comitê Gestor da Estratégia;
- **Diretoria** – Referente à todos os Diretores das Diretorias da Anvisa (Primeira Diretoria, Segunda Diretoria, Terceira Diretoria, Quarta Diretoria e Quinta Diretoria);
- **Responsável GRC Tático** – Responsável dentro da Unidade em questão por gerenciar e organizar a carteira de riscos táticos;
- **Gerência Geral** – Relativo a todas as Gerências Gerais presentes em cada Diretoria ou a Gerência Geral em questão realizando o processo;
- **Unidades** – Referente a todas as Unidades Organizacionais presentes na ANVISA ou a Unidade em questão realizando o processo;
- **Equipe de Auditoria** – Equipe responsável por realizar a auditoria na ANVISA;
- **Risco** - 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;

- **Tipologia de Riscos Corporativos:** Classificação dos tipos de riscos corporativos definidos pela Anvisa que podem afetar o alcance de seus objetivos estratégicos/táticos, observadas as características de sua área de atuação: operacional, legal, imagem, financeiro e integridade.
- **Tratamento do risco:** processo de seleção e implementação de ações, controles ou respostas para mitigar o risco**;**
- **Tolerância ao risco:** nível de variação aceitável no desempenho em relação à meta para o cumprimento de um objetivo específico, em nível tático ou operacional.
- **Nível de Risco** - é a magnitude de um risco, expressa em termos da combinação das consequências e de suas probabilidades;
- **Risco Inerente** - nível de risco antes da consideração de qualquer ação de tratamento (Risco Inerente = Probabilidade x Impacto).

ANVISA
Agência Nacional de Vigilância Sanitária

APLAN

Gustavo Henrique Trindade da Silva

Marina Torres Uber Bucek

Nelci dos Santos

Marcelo Ivo de Lima

Com apoio

ELO GROUP

Adriano Figueiredo de O. Gomes

Juliana Finageiv Neder

ANVISA
Agência Nacional de Vigilância Sanitária