GERENCIAMENTO DE RISCOS E CONTROLES INTERNOS

N/GC/004/00

Data: 21/12/2022

GOVERNANÇA CORPORATIVA **NORMA**

GERENCIAMENTO DE RISCOS E CONTROLES INTERNOS

Nota da versão:

Versão 00 – Alteração da atividade de classificação para Governança Corporativa; inclusão dos instrumentos de vinculação; atualização dos órgãos citados na norma; alteração dos itens 5.15 e 6.3, 6.3.1, 6.3.2 e 6.3.3; e inclusão dos itens 6.5.e 6.6.

SUMÁRIO

GERENCIAMENTO DE RISCOS E CONTROLES INTERNOS

1 OBJETIVO

Estabelecer as diretrizes, procedimentos e conceitos para o gerenciamento dos riscos e controles internos.

2 APLICAÇÃO

Aplica-se a todos os órgãos da Empresa.

3 INSTRUMENTOS DE VINCULAÇÃO

- Lei 13.303 de 30 de junho de 2016 – Dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios.
- Decreto 8.945 de 27 de dezembro de 2016 – Regulamenta, no âmbito da União, a Lei nº 13.303, de 30 de junho de 2016, que dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios.
- Resolução CGPAR nº 033 de 04 de agosto de 2022 – A Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR) - Dispõe acerca da implementação de políticas de Conformidade e Gerenciamento de Risco pelas empresas estatais federais e dá outras providências.
- Instrução Normativa Conjunta MPOG/CGU nº 01, de 10 de maio de 2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal.
- Decreto 9.203 de 23 de novembro de 2017, que dispõe sobre a política de Governança da Administração Pública Federal direta, autárquica e fundacional, e alterações posteriores;
- Portaria CGU 1.089 de 25 de abril de 2018, que estabelece orientações para que os órgãos e as entidades da Administração Pública Federal tomem medidas inibidoras de fraudes e corrupção, e alterações posteriores;
- Política de Gestão de Riscos Corporativos vigente;

- Política de Continuidade de Negócios vigente;
- Norma ABNT NBR ISO 31000:2018– Gestão de Riscos – Princípios e diretrizes.
- Norma ABNT ISO GUIA 73:2009 – Gestão de Riscos – Vocabulário.
- Norma ABNT NBR ISO 31010:2012 – Gestão de Riscos – Técnicas para o processo de avaliação de riscos.
- Norma ABNT NBR ISO 31004:2015 – Gestão de Riscos – Guia para implementação da ABNT ISO 31000.
- COSO (Committee of Sponsoring Organizations of the Treadway Commission) – Gerenciamento de Riscos Corporativos versão 2017.
- COSO (Committee of Sponsoring Organizations of the Treadway Commission) – Estrutura Integrada de Controles Internos, versão 2013.
- Modelo de Três Linhas do Instituto dos Auditores Internos do Brasil, versão 2020.

4 ÓRGÃOS CITADOS NA NORMA

Sigla	Função principal
n/a	Conselho de Administração
COAUD	Comitê de Auditoria Estatutário
n/a	Diretoria Executiva
COGE	Comitê de Gestão Estratégica
DCON	Órgão responsável pela gestão de riscos corporativos e controles internos
AUDI	Órgão responsável pela auditoria interna

5 CONCEITUAÇÃO

5.1 Análise PESTAL

Ferramenta de análise das perspectivas agregadas às decisões mercadológicas, que buscam avaliar as variáveis políticas, econômicas, sociais, tecnológicas, ambientais e legais (PESTAL), que interferem ou impactam o negócio.

5.1.1 Variável política

São variáveis determinadas pelas políticas governamentais e variações na legislação que provocam mudanças na estrutura e funcionamento e relações de negociação da organização.

5.1.2 Variável econômica

São variáveis caracterizadas por impactar significativamente nos negócios a partir de mudanças ocorridas em caráter geral, podendo ser estas positivas ou negativas, estimuladoras ou desestimuladoras.

5.1.3 Variável sociocultural

São variáveis referentes à sociedade. Neste contexto incluem-se tradições, valores, cultura, educação e aspectos demográficos.

5.1.4 Variável tecnológica

São aquelas compreendidas no contexto dos avanços tecnológicos e que modificam absoluta ou relativamente a estrutura de mercado ou ambiente de determinada atividade econômica.

5.1.5 Variável ambiental

São variáveis que dizem respeito ao meio ambiente. Neste contexto incluem-se reciclagem, eliminação de resíduos e sustentabilidade.

5.1.6 Variável legal

São variáveis determinadas pelas inclusões ou alterações na legislação e o impacto que possa ter sobre as operações comerciais e financeiras.

5.2 Análise de riscos

Análise que permite que uma organização considere como os riscos potenciais podem impactar a realização dos objetivos. Os riscos são ***avaliados*** com base em duas perspectivas – probabilidade e impacto – para que haja o cálculo do nível de risco.

5.3 Apetite a risco

Apetite ao Risco é o nível máximo de risco que a instituição está disposta a aceitar ou incorrer para alcançar seus objetivos estratégicos e cumprir o seu plano de negócio.

5.4 Avaliação de riscos

Processo de comparar os resultados da análise de riscos para determinar se o risco e/ou sua magnitude é aceitável ou tolerável para a organização. Assim, a partir da avaliação, é decidido quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento.

5.5 Avaliação dos controles

Medidas aplicadas no âmbito do DATAPREV, para gerenciar os riscos e aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados, por intermédio da avaliação do desenho e operação dos controles existentes.

5.6 Base de ocorrências

Base de dados no qual são relatados os históricos de todos os eventos de riscos, contendo: Ocorrência; Risco relacionado; Datas; Detalhamento da Ocorrência; Causas; Perdas.

5.7 Controle

O que se faz para mitigar riscos, assegurando, assim, com certa razoabilidade, que objetivos sejam alcançados.

5.8 Controle interno da gestão

Processo que engloba o conjunto de regras, manual de atribuições, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos organizacionais serão alcançados.

5.9 Escala de Impacto

Ferramenta pela qual os riscos são analisados e classificados sob quatro critérios para mensuração de seu impacto, quais sejam:

- Impacto à Imagem - Perda de credibilidade da DATAPREV;
- Impacto Operacional – Afeta entrega de produtos e serviços;
- Impacto Regulatório – Pode acarretar ações de caráter corretivo, pecuniário ou até mesmo interrupção das atividades;
- Impacto Financeiro – Pode afetar o orçamento ou a receita da organização ou afetar negativamente o retorno financeiro esperado de um investimento ou, ainda, imputar em algum prejuízo à DATAPREV.

5.10 Escala de Probabilidade

Ferramenta que possibilita que os eventos de risco sejam classificados conforme sua frequência em 5 diferentes níveis: 1. Muito Baixa (Improvável); 2. Baixa (Rara); 3. Média (Possível); 4. Alta (Provável); 5. Muito Alta (Praticamente certa).

- Probabilidade Muito Baixa: Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.
- Probabilidade Baixa: Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.
- Probabilidade Média: Possível. De alguma forma, o evento deverá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.
- Probabilidade Alta: Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.
- Probabilidade Muito Alta: Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.

5.11 Etapas da metodologia de gerenciamento de riscos

Atividades necessárias para a operacionalização da gestão de riscos, por meio da definição de um processo de gerenciamento de riscos que consiste em especificar contexto (objetivo), identificar, analisar e avaliar riscos, priorizar riscos, definir respostas aos riscos (controle), comunicar e monitorar.

5.12 Gestão do Controle Interno

Abrange a aplicação do ciclo PDCA sobre os 'requisitos' e etapas do ciclo de vida do controle interno.

5.13 Inventário de Riscos

Instrumento que proporciona uma visão executiva da gestão de risco em toda a organização.

5.14 Matriz de Riscos (Mapa de calor)

Posiciona os eventos de risco conforme seus graus de probabilidade e de impacto. A matriz de riscos (mapa de calor) é particularmente útil para enxergar grupos de risco. As siglas apresentadas na Matriz de Riscos são referentes à: RB – Risco Baixo; RM – Risco Moderado; RA – Risco Alto; RC – Risco Crítico.

Os riscos com baixa probabilidade de ocorrerem, mas com altíssimo impacto são denominados como Cisne Negro (*Black Swan*).

5.15 Modelo das Três Linhas

Modelo anteriormente conhecido como Três Linhas de Defesa. Este modelo é utilizado para auxiliar na identificação de estruturas e processos que melhor contribuam para que as organizações possam alcançar seus objetivos e facilitar uma forte governança e gerenciamento de riscos.

1ª Linha

Controles internos e riscos da gestão executados por todos os agentes públicos responsáveis pela condução de atividades e tarefas, no âmbito dos processos finalísticos e de apoio dos órgãos e entidades do poder executivo federal. Na DATAPREV, em se tratando de processos, os responsáveis por exercer essa atividade são os guardiões dos processos e/ou os gestores dos processos; em se tratando de programas, são aqueles definidos pelos responsáveis dos programas.

2ª Linha

Supervisão e monitoramento dos controles internos e riscos são executados por instâncias específicas, como comitês, diretorias ou assessorias específicas para tratar de riscos, controles internos, integridade e *compliance*. Na DATAPREV, essa atividade encontra-se a cargo da área de riscos corporativos, integridade e

compliance e demais áreas de supervisão.

3ª Linha

Constituída pelas auditorias internas no âmbito da administração pública, uma vez que são responsáveis por proceder à avaliação da operacionalização dos controles internos da gestão (primeira linha) e da supervisão dos controles internos (segunda linha). Na DATAPREV, essa função é exercida pelo órgão responsável pela auditoria interna.

5.16 Matriz SWOT

Representação visual das forças, fraquezas, oportunidades e ameaças de uma organização. A sigla refere-se aos termos em inglês (*Strenghts, Weaknesses, Opportunities, Threats*). A matriz SWOT é útil principalmente para sintetizar os resultados de pesquisas internas e externas.

5.17 Metodologia 5W2H

Auxilia o gestor a definir e priorizar as ações que serão executadas com vistas à mitigação dos riscos de acordo com a sua classificação. A metodologia base utilizada nessa matriz é 5W2H – *What* (O que será feito?), *Why* (Por que será feito?), *Where* (Onde será feito?), *When* (Quando será feito?), *Who* (Por quem será feito?), *How* (Como será feito?) e *How much* (Quanto custará?).

5.18 Objetivo

É aquilo que se pretende realizar/cumprir.

5.19 Planilha Documentadora de Riscos

O instrumento de apoio com as informações consolidadas dos riscos identificados e com a fórmula automática da operação. A fórmula baseia-se na média dos resultados entre os quatro critérios de impactos multiplicado pelo valor dado para probabilidade.

5.20 Plano para tratamento do risco

Esquema dentro da estrutura de gestão de riscos que especifica as ações, os recursos a serem aplicados para gerenciar riscos, incluindo procedimentos, práticas, atribuição de responsabilidades, sequência e cronologia das atividades.

5.21 Risco

Efeito da incerteza nos objetivos. Assim, entende-se evento de risco como um evento futuro identificado que venha a ter impacto no cumprimento dos objetivos, ao qual é possível associar uma distribuição de probabilidades de ocorrência.

5.22 Riscos à integridade

Eventos relacionados a fraudes, a desvio de conduta de ética, a prática de corrupção, a conflito de interesses e outros que de alguma forma possam comprometer os valores e padrões da DATAPREV.

5.23 Riscos estratégicos

Riscos associados com as decisões estratégicas da organização para atingir os seus objetivos de negócios, e/ou decorrentes da falta de capacidade ou habilidade da Empresa para proteger-se ou adaptar-se a mudanças no ambiente externo.

5.24 Riscos financeiros

Eventos que podem comprometer a capacidade da DATAPREV de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou incertezas associadas aos retornos financeiros esperados de um investimento.

5.25 Risco inerente

Risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto.

5.26 Riscos operacionais

Eventos que podem comprometer as atividades da DATAPREV, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas.

5.27 Riscos regulatórios

Eventos derivados de alterações legislativas ou normativas, inadequação a requisitos regulatórios ou multas aplicadas por descumprimento de dispositivos legais e perdas financeiras oriundas de decisões desfavoráveis em processos judiciais, que podem comprometer as atividades da DATAPREV.

5.28 Risco residual

Risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco.

5.29 Supervisão

Prover consultoria e assessoria em controle interno, observando a segregação de função, para a promoção das atividades: sistematizar, processar, gerenciar, monitorar e comunicar, as respostas do Sistema de Controle Interno da Empresa.

5.30 Tabela de resposta a riscos

Para cada risco identificado, será prevista uma resposta, que pode ser de 4 tipos: **evitar**, **aceitar**, **compartilhar/transferir** ou **mitigar**.

5.31 Tabela de classificação de Nível de Risco

Tabela que permite classificar o nível de risco de forma a hierarquizar a importância dos riscos, conforme suas classificações de probabilidade e impacto.

5.32 Tratamento de riscos

Consiste na definição de ações de tratamento para os riscos, bem como o estabelecimento de indicadores de riscos que serão utilizados na etapa de monitoramento e análise dos riscos.

6 DIRETRIZES BÁSICAS

Os órgãos e Entidades da Administração Pública Federal são orientados a seguir, na sua estrutura de controles internos[1], o modelo das três linhas, com funções que devem se relacionar, de maneira clara, e os responsáveis por ela devem conhecer os papéis e as responsabilidades de todos os envolvidos, provendo uma atuação coordenada e eficiente, sem sobreposições ou lacunas.

[1] *O Committee of Sponsoring Organizations of the Treadway Commission (COSO), em sua obra "Internal Control – Integrated Framework" define o controle interno como um processo conduzido pelo conselho de administração, pela administração e pelo corpo de empregados de uma organização, com a finalidade de possibilitar uma garantia razoável quanto à realização dos objetivos nas seguintes categorias: Eficácia e eficiência das operações; Confiabilidade das demonstrações financeiras; e Conformidade com leis e regulamentos cabíveis.*

A Gestão de Risco, por sua vez, se refere às atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos.

De acordo com a Política de Gestão de Riscos Corporativos da DATAPREV, os princípios que devem ser observados são:

a. A gestão de riscos deve considerar, explicitamente, as incertezas, a natureza dessas incertezas, e como elas podem ser tratadas;

b. A gestão de riscos deve ser parte integrante de todos os processos da organização, nos diferentes níveis;

c. Os riscos devem ser considerados em todas as decisões e a sua gestão deve ser realizada de maneira integrada.

d. As ações de resposta devem considerar as possíveis consequências de curto, médio e longo prazos e devem ser priorizadas de acordo com a agregação ou preservação de valor para DATAPREV;

e. A gestão de riscos deve ser sistemática, racional, transparente, dinâmica, iterativa, adaptável a mudanças e coerente com o Plano Estratégico Institucional (PEI) da DATAPREV.

6.1 Metodologia de Gestão de Riscos

A Metodologia de Gestão de Riscos da DATAPREV objetiva estabelecer e estruturar as etapas necessárias para a operacionalização da Gestão de Riscos na DATAPREV. Ela foi concebida em 7 etapas, a saber:

a. Estabelecer contexto

b. Identificar riscos

c. Analisar riscos

d. Avaliar riscos

e. Tratar riscos

f. Monitorar e analisar

g. Comunicar

Essas etapas podem ser vistas no Anexo IV – Etapas para gestão de riscos e serão descritas a seguir:

6.1.1 Estabelecer o contexto

Etapa que consiste em definir o ambiente para o gerenciamento dos riscos. Compreende a identificação dos fatores internos e externos, que podem influenciar o atingimento dos "objetivos" na definição dos parâmetros para as próximas fases do gerenciamento e o apetite ao risco para o contexto específico, caso ele não tenha sido definido de forma ampla pela Empresa.

Esta etapa é iniciada a partir das necessidades de avaliação da estratégia. Com esses insumos, é possível realizar a análise do ambiente externo, com o uso da Análise PESTAL e partes da análise SWOT (oportunidades e ameaças), e realizar a análise do ambiente interno, com partes da análise SWOT (forças e fraquezas).

6.1.2 Identificar Riscos

A identificação de riscos deve reconhecer e descrever os eventos de riscos aos quais a Empresa está exposta. **Envolve mapear as fontes** de risco, suas causas e consequências potenciais, **dados históricos, análises teóricas, informações de especialistas entre outros.** Este mapeamento da identificação responde aos questionamentos conforme Anexo VII – Guia de Identificação de Riscos.

Na etapa de identificação dos riscos devem ser consideradas as seguintes categorias de riscos estabelecidas na Política de Riscos Corporativos da DATAPREV conforme Anexo III – Escala de Impacto: Riscos Estratégicos, Riscos Operacionais, Riscos Financeiros e Riscos Regulatórios e Riscos à Integridade.

O Diagrama *Bow Tie* (Anexo II) é o instrumento prático e visual para registro das informações relativas aos riscos. O evento a ser estudado deve ser posicionado no centro do diagrama, suas causas (fatores de risco) à esquerda, e seus efeitos (impactos) à direita, permitindo, assim, a visualização da relação entre os elementos do sistema modelado.

6.1.3 Analisar Riscos

A análise de riscos permite que a empresa considere como os riscos **potenciais** podem impactar a realização dos objetivos. Os riscos são classificados com base em duas perspectivas – probabilidade e impacto – para que haja o cálculo do nível de risco.

O nível do risco é expresso pela combinação da probabilidade de ocorrência do evento e das consequências resultantes no caso de materialização do evento, ou seja, do impacto nos objetivos.

Dessa forma, o processo é iniciado pela definição do grau do impacto dos riscos nos quatro fatores pré-determinados: Imagem, Finanças, Operações e Regulatório. Posteriormente é definido a probabilidade de cada um dos riscos levantados ocorrer. Por fim, é realizado o cálculo no nível de riscos. O procedimento será exemplificado, hipoteticamente, a seguir.

a. Notas atribuídas aos graus de impacto:
   - Imagem: Exposição temporária, reflexo moderado na reputação/credibilidade (3);
   - Operacional: Afeta entre 10% e 30% a entrega de produtos ou serviços (2);
   - Regulatório: Determina ações de caráter corretivo (3);
   - Financeiro: Afeta mais de 25% da receita líquida anual (5);
   - Resultado do Grau de Impacto = 3.

b. Notas atribuídas ao grau de probabilidade:
   - Nível de Probabilidade = 4 Alta (Provável, circunstâncias indicam grandes possibilidades)

c. Nível do Risco
   - Grau de Impacto X Grau de Probabilidade = 3 X 4 = 12
   - O valor de 12 seria classificado na matriz de riscos como um Risco Alto (RA)

d. Os riscos são analisados e classificados sob quatro critérios para mensuração de seu impacto:
   - Impacto à Imagem - Perda de credibilidade da DATAPREV;
   - Impacto Operacional – Afeta entrega de produtos e serviços;
   - Impacto Regulatório – Pode acarretar em ações de caráter corretivo, pecuniário ou até mesmo interrupção das atividades;

– Impacto Financeiro – Pode afetar a receita da DATAPREV.

Os eventos de risco são classificados conforme sua frequência em 5 diferentes níveis: 1. Muito Baixa (Improvável); 2. Baixa (Rara); 3. Média (Possível); 4. Alta (Provável); 5. Muito Alta (Praticamente certa) conforme Anexo VI – Escala de Probabilidade.

O nível de risco é uma forma de hierarquizar a relevância dos riscos conforme suas classificações de frequência e impacto. A Tabela de classificação de nível de Risco - Anexo XI, demonstra a classificação e a faixa.

6.1.4 Avaliar Riscos

A avaliação de riscos é o processo de comparar os resultados da análise de riscos para determinar se o risco e/ou sua magnitude são aceitáveis para a organização. Assim, a partir da avaliação, é decidido quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento. Esta etapa consiste na definição do apetite ao risco aprovado pelo Conselho de Administração. É importante que essa ação seja repetida anualmente para que possa sempre ser verificado o contexto em que a organização está inserida.

Em seguida, comparam-se os resultados da análise de riscos, com o auxílio da Matriz de Riscos, para determinar quais são aceitáveis ou toleráveis para a organização, de acordo com o apetite ao risco definido anteriormente. Por fim, os riscos que são priorizados para tratamento.

O apetite ao risco do processo organizacional deve ser estabelecido no início do processo de gerenciamento de riscos. Uma vez definido, a unidade declara que:

a. Todos os riscos cujos níveis estejam dentro da(s) faixa(s) de apetite a risco podem ser aceitos, e uma possível priorização para tratamento deve ser justificada;

b. Todos os riscos cujos níveis estejam fora da(s) faixa(s) de apetite a risco serão tratados e monitorados, e uma possível falta de tratamento deve ser justificada.

Nesta fase o produto gerado é a Matriz de Riscos (Mapa de Calor) conforme Anexo VIII. Este instrumento posiciona os eventos de risco conforme seus graus de frequência e de impacto. A matriz de riscos é particularmente útil para enxergar grupos de risco. As siglas apresentadas na matriz de riscos são referentes à: RB – Risco Baixo; RM – Risco Moderado; RA – Risco Alto; RC – Risco Crítico.

6.1.5 Identificar controles existentes

Nesta fase deve-se verificar a existência dos controles, como foram configurados e qual a sua situação quanto à operação (Anexo I).

6.1.6 Tratar Riscos

Etapa que consiste na definição de ações de tratamento para os riscos, bem como o estabelecimento de indicadores de riscos que serão utilizados na etapa de monitoramento e análise dos riscos. A primeira ação consiste na definição das ações a serem tomadas, com o auxílio da tabela de abordagens aos riscos (Anexo X). Posteriormente à fase de definição das abordagens aos riscos, é elaborado um conjunto de ações de tratamento por intermédio da Matriz Básica de Controles Internos (Anexo IX) e, em seguida, deverão ser estabelecidos os indicadores de risco que serão acompanhados. A Tabela de abordagens aos riscos especifica os tipos de ação de tratamento e controle que podem ser definidas para cada risco.

6.1.7 Monitorar e Analisar Riscos

Com o entendimento de que os resultados do Monitoramento e da Análise Crítica podem impactar o próprio processo de gestão de riscos, é prevista uma revisão anual desses componentes (Melhoria Contínua). Porém, mudanças no contexto da empresa também podem provocar a necessidade de implantação de melhorias de forma antecipada.

O monitoramento no âmbito do processo de gerenciamento de riscos, deve ser realizado principalmente pela unidade responsável pelo processo organizacional, de forma a:

a. Garantir que os controles sejam eficazes e eficientes;

b. Analisar as ocorrências dos riscos;

c. Detectar mudanças que possam requerer revisão dos controles e/ou do Plano de Tratamento;

d. Identificar os riscos emergentes.

6.1.8 Comunicar

A comunicação aos envolvidos é um dos aspectos mais importantes do processo de gestão de riscos. Nesse sentido, as ações de comunicação devem abordar questões relacionadas ao risco propriamente dito, suas causas, suas consequências e as medidas que estão sendo tomadas para tratá-los, para diferentes esferas decisórias da DATAPREV. A comunicação

deve ser estabelecida de modo formal. O órgão responsável por riscos corporativos e controles internos na DATAPREV deverá elaborar o Relatório de Riscos Consolidados e enviá-lo mensalmente ao Comitê de Gestão Estratégica e à Diretoria Executiva, e, trimestralmente, ao Comitê de Auditoria Estatutário e ao Conselho de Administração.

Os riscos que recaem sobre o cumprimento dos objetivos estratégicos serão comunicados ao Conselho de Administração e ao Comitê de Auditoria Estatutário pelo órgão responsável por riscos corporativos e controles internos na DATAPREV; os demais riscos devem ser comunicados mensalmente a esse órgão contendo a percepção do gestor do processo bem como incidentes e eventos recorrentes.

6.1.9 Recursos e Orçamentos

Cada controle interno adotado deverá descrever os recursos e orçamento necessário à sua execução. No caso de alocação interna deverá ser informada a quantidade de horas e os equipamentos disponibilizados para atender ao controle.

6.2 Governança

A atividade de Governança deve promover a efetividade dos principais controles internos administrativos, quando necessário, orientar a adoção de medidas apropriadas para a melhoria do processo de governança no cumprimento dos seguintes objetivos: supervisionar o desempenho organizacional com orientação para o gerenciamento eficaz dos controles internos administrativos para *accountability*; apoiar o monitorar os indicadores relacionadas aos principais controles internos das áreas apropriadas; e acompanhar as atividades e a comunicação das informações entre as áreas operacionais, diretorias e Conselho e, se houver demandas as entidades de externas.

6.3 Implantação por meio do modelo das três linhas

A aplicação desta Norma será escalonada por etapas e gradual junto aos responsáveis pelos programas e processos em cada linha, de modo que os controles não deixem lacunas ou duplicações.

6.3.1 Primeira Linha

A Diretoria Executiva deve avaliar os riscos e propor controles pertinentes para uma gestão eficiente do Plano Estratégico Institucional, na etapa de elaboração do quinquênio, assim como, em cada período de revisão, de acordo com calendário definido.

Os patrocinadores e responsáveis pelos programas devem avaliar os riscos e propor controles para uma gestão eficiente do Plano de Ação, de acordo com calendário definido.

Os gestores dos processos devem identificar/ avaliar os riscos e propor controles pertinentes para os processos da Cadeia de Valor, sob sua gestão, observando sempre o período de revisão/elaboração do Plano Estratégico Institucional, de forma a mitigar os possíveis impactos que possam ser atrelados à estratégia

Estes controles devem ser avaliados e monitorados pelos gestores superiores, verificando sua execução e propondo melhorias. É importante que os gestores avaliem se os controles internos propostos aos riscos, estão de acordo com o apetite ao risco da organização.

Cabe aos gestores evidenciar sua necessidade de recursos e orçamento visando estruturar os controles internos propostos, inclusive quanto a capacitação.

Nesta fase, que consiste na proposta dos controles internos que mitigam riscos, os gestores podem utilizar uma avaliação da 2° Linha junto aos responsáveis pela 1° Linha.

Segundo o Instituto de Auditores Independentes – IIA, esses são os principais papéis da 1ª linha:

a. Liderar e dirigir ações (incluindo gerenciamento de riscos) e aplicação de recursos para atingir os objetivos da organização.

b. Manter um diálogo contínuo com o órgão de governança e reportar: resultados planejados, reais e esperados, vinculados aos objetivos da organização; e riscos.

c. Estabelecer e manter estruturas e processos apropriados para o gerenciamento de operações e riscos (incluindo controle interno).

d. Garantir a conformidade com as expectativas legais, regulatórias e éticas.

6.3.2 Segunda Linha

Nesta fase a 2° linha fará a análise formal dos controles internos e riscos alinhados aos controles definidos no 1°ciclo.

Serão avaliados quanto a controles e períodos previamente acordados e critérios segundo suas atribuições, para a conformidade e mitigação dos eventos de risco.

A qualidade dos controles internos será objeto de observação.

Será verificado se os controles internos sugeridos estão alinhados com a mitigação dos riscos da organização e principalmente, sobre os resultados e objetivos alcançados.

Segundo o Instituto de Auditores Independentes – IIA, esses são os principais papéis da 2ª linha:

a. Fornecer expertise complementar, apoio, monitoramento e questionamento quanto ao gerenciamento de riscos, incluindo: o desenvolvimento, implantação e melhoria contínua das práticas de gerenciamento de riscos (incluindo controle interno) nos níveis de processo, sistemas e entidade.

b. O atingimento dos objetivos de gerenciamento de riscos, como: conformidade com leis, regulamentos e comportamento ético aceitável; controle interno; segurança da informação e tecnologia; sustentabilidade; e avaliação da qualidade.

c. Fornecer análises e reportar sobre a adequação e eficácia do gerenciamento de riscos (incluindo controle interno).

6.3.3 Terceira Linha

A 3° linha de acordo com seu planejamento irá avaliar de modo independente se os controles internos estão de acordo com os riscos que buscam mitigar.

Devem fornecer às partes envolvidas *feedback* sobre a efetividade e o atendimento dos objetivos dos processos e os riscos a eles vinculados.

Segundo o Instituto de Auditores Independentes – IIA, esses são os principais papéis da 3ª linha:

a. Mantém a prestação de contas primária perante o órgão de governança e a independência das responsabilidades da gestão.

b. Comunica avaliação e assessoria independentes e objetivas à gestão e ao órgão de governança sobre a adequação e eficácia da governança e do gerenciamento de riscos (incluindo controle interno), para apoiar o atingimento dos objetivos organizacionais e promover e facilitar a melhoria contínua.

c. Reporta ao órgão de governança prejuízos à independência e objetividade e implanta salvaguardas conforme necessário.

6.4 Matriz RACI

Dentro do escopo de um processo de gerenciamento de riscos, deve ser observada a Matriz de Responsabilidade RACI apresentada no quadro abaixo.

A Matriz de Responsabilidade RACI define Responsável, Autoridade, Consultado e Informado para o processo de gerenciamento de riscos na DATAPREV. São elementos da Matriz RACI:

a. Responsável: quem executa a atividade;

b. Autoridade: quem aprova a tarefa ou produto. Pode delegar a função, mas mantém a responsabilidade;

c. Consultado: quem pode agregar valor ou é essencial para a implementação;

d. Informado: quem deve ser notificado de resultados ou ações tomadas, mas não precisa se envolver na decisão.

Durante as etapas do processo de gerenciamento de riscos da DATAPREV, é importante que a comunicação observe os agentes ou unidades apontadas como consultados ou informados na Matriz RACI.

Etapas/Atividades	CA	COAUD	Comitê Estratégico	DIREX	Área de Riscos	Área Executora	AUDI
1. Estabelecimento do Contexto							
1.1. Realizar análise do ambiente externo					C	R A	
1.2. Realizar análise do ambiente interno					C	R A	
1.3. Realizar análise dos objetivos					C	R A	
2. Identificação dos Riscos							
2.4. Identificação dos riscos					C	R A	
3. Análise de Riscos							
3.5. Definir grau de probabilidade e impacto					C	R A	
3.6. Calcular nível de risco					C	R A	
4. Avaliação de Riscos							
4.7. Consolidar Matriz de Risco (mapa de calor)					C	R A	
4.8. Priorizar riscos para tratamento			A		C	R	
5. Tratamento dos riscos							
5.9. Elaborar plano de resposta					C	R	
5.10. Validar plano de resposta			R A		C		
5.11. Executar tratamento dos riscos (plano de resposta)					C	R A	
5.12. Estabelecer indicadores de riscos					C A	R	
6. Monitoramento de riscos							
6.13. Registrar ocorrências de riscos					I	R A	
6.14. Monitorar a execução do plano de resposta					R A		
6.15. Monitorar os indicadores de riscos					R A	C	I
7. Comunicação de riscos							
7.16. Elaborar relatório de riscos		I	C	A	R		
7.17. Submeter relatório de riscos	A	I	I	R	I	I	

Legenda
R = Responsável: quem executa a tarefa.
A = Autoridade: quem aprova a tarefa ou produto. Pode delegar a função, mas mantém a responsabilidade.
C = Consultado: quem pode agregar valor ou é essencial para a implementação.
I = Informado: quem deve ser notificado de resultados ou ações tomadas, mas não precisa ser envolver na decisão.

6.5 Continuidade de Negócio

A gestão dos riscos conforme esta norma, para continuidade de negócio, deve observar: a Política de Continuidade de Negócio, o Sistema de Gestão de Continuidade de Negócio e o Plano Diretor de Continuidade de Negócios.

6.6 Disposições Gerais

Detalhamento e orientações para prática desta norma constam do *site* 'conexão', aba 'Gestão', item 'Riscos e Controles Internos'. link: *https://www-conexao/gestao/riscos-e-controles-internos* (em 26/09/2022).

As situações não previstas nesta norma devem ser dirimidas junto ao órgão responsável pela gestão de riscos corporativos e controles internos da Dataprev.

7 VIGÊNCIA

Esta Norma entra em vigor a partir desta data e revoga a N/PO/017/01.

MARCELO LINDOSO BAUMANN DAS NEVES
SUPERINTENDENTE DE GOVERNANÇA, RISCOS E COMPLIANCE
Responsável pela elaboração

ROGÉRIO LINEU ARITA
SUPERINTENDENTE JURÍDICO SUBSTITUTO
Responsável pela chancela

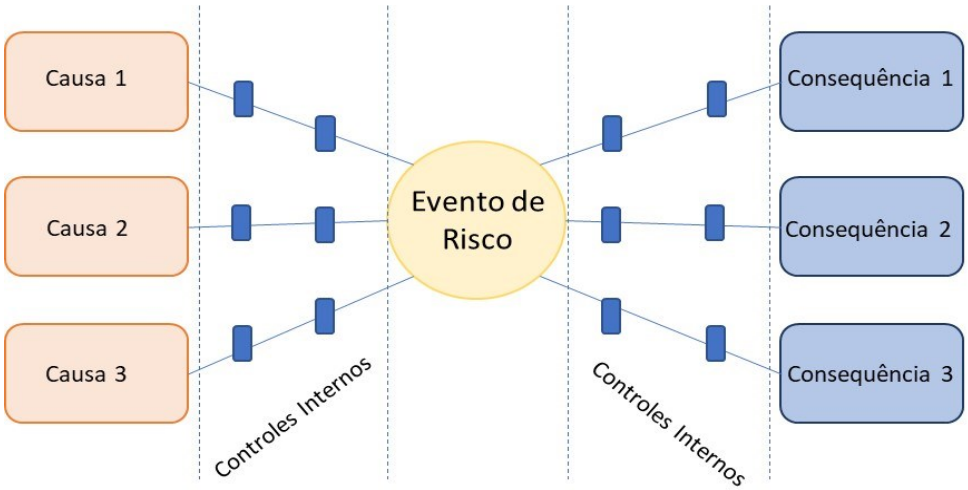
ISABEL LUIZA RAFAEL MACHADO DOS SANTOS
DIRETORA JURÍDICA, DE RISCOS, GESTÃO E GOVERNANÇA CORPORATIVA
Responsável pela aprovação

ANEXO I – AVALIAÇÃO DOS CONTROLES

Desenho do Controle	
Nota	**Descrição**
1	Não há procedimento de controle.
2	Há procedimentos de controle, mas não são adequados e não estão formalizados.
3	Há procedimentos de controle formalizados, mas não estão adequados (insuficientes).
4	Há procedimentos de controle adequados (suficientes), mas não estão formalizados.
5	Há procedimentos de controle adequados (suficientes) e formalizados.

Operação do Controle	
Nota	**Descrição**
1	Não há procedimento de controle.
2	Há procedimentos de controle, mas não são executados.
3	Os procedimentos de controle estão sendo parcialmente executados.
4	Os procedimentos de controle são executados, mas sem evidência de sua realização.
5	Os procedimentos de controle são executados e com evidência de sua realização.

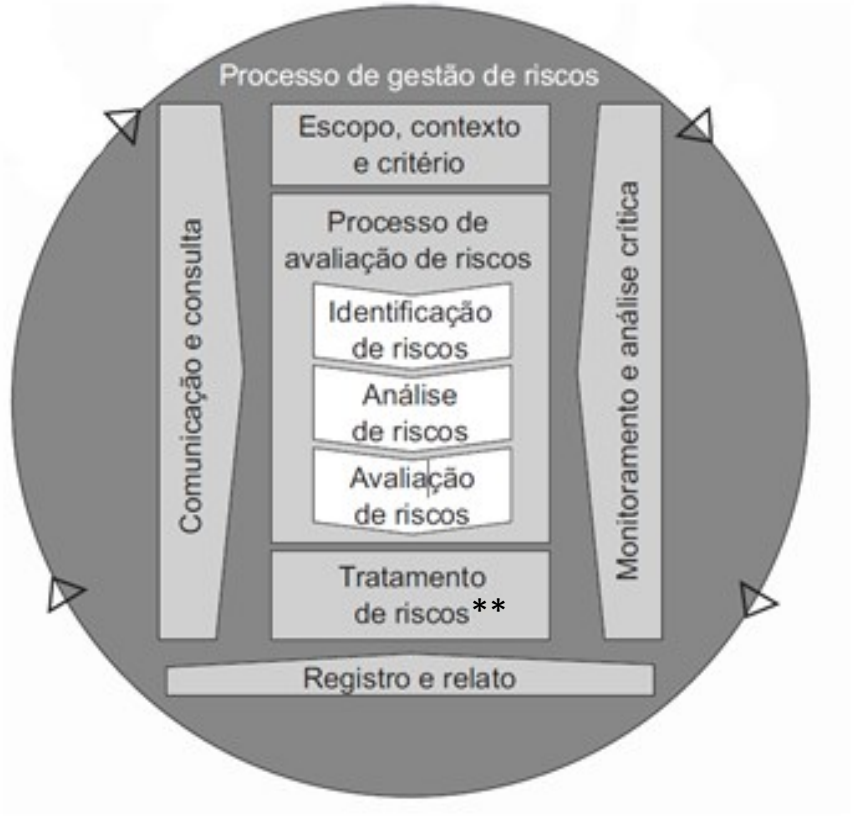
ANEXO II - DIAGRAMA BOW TIE



ANEXO III - ESCALA DE IMPACTO

	Impacto				Peso - 100%
	Imagem 25%	Operacionais 25%	Regulatórios 25%	Financeiros 25%	
Orientações para atribuição de pesos	Exposição Intensa (reputação/credibilidade seriamente afetada)	Afeta mais de 70% a sustentação/entrega de produtos ou serviços	Determina interrupção das atividades	Afeta mais de 25% da receita liquída anual	5-Muito Alto
	Exposição significativa (reputação/credibilidade sob suspeita)	Afeta entre 50% e 70 % a sustentação/entrega de produtos ou serviços	Determina ações de caráter pecuniários (muitos)	Afeta de 15% a 25% da receita liquída anual	4-Alto
	Exposição temporária (reflexo moderado na reputação/credibilidade)	Afeta entre 30% e 50 % a sustentação/entrega de produtos ou serviços	Determina ações de caráter corretivos	Afeta de 5% a 15% da receita liquída anual	3-Médio
	Exposição limitada entre as partes envolvidas (baixo reflexo na reputação/credibilidade)	Afeta entre 10% e 30 % a sustentação/entrega de produtos ou serviços	Determina ações de caráter orientativo	Afeta até 5% da receita liquída anual	2-Baixo
	Sem exposição e reflexos significativos sobre a reputação/credibilidade	Afeta menos de 10 % a sustentação/entrega de produtos ou serviços	Pouco ou nenhum impacto	Sem influência significativa	1-Muito Baixo

ANEXO IV - ETAPAS DA METODOLOGIA DE GERENCIAMENTO DE RISCOS



*ISO 31000

****Tratamento de riscos: nesta etapa ocorre a identificação, definição e implementação das ações e/ou Controles Internos.**

ANEXO V – CICLO DOS OBJETIVOS, RISCOS E CONTROLES INTERNOS

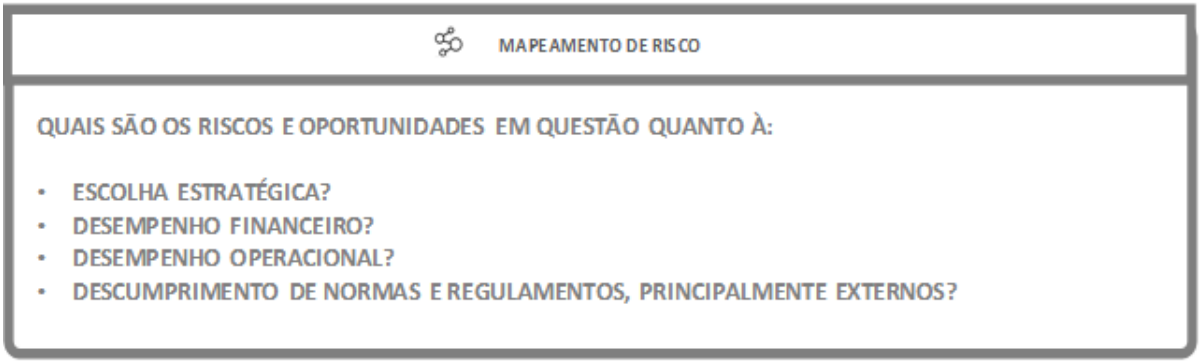
Figura 1 - Objetivos e Riscos: A razão de ser do Controle Interno

Fonte: Apostila_ISC-TCU - 2013 1 - Objetivos e Riscos

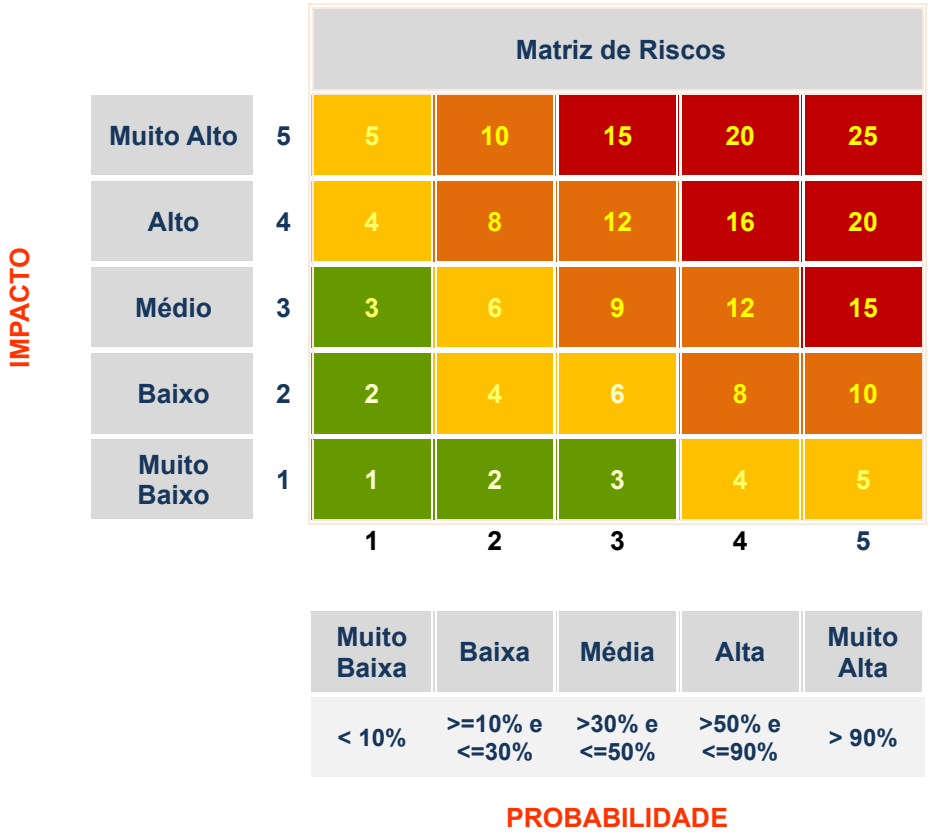
ANEXO VI - ESCALA DE PROBABILIDADE

Aspectos Avaliativos	Evento pode ocorrer apenas em circunstâncias excepcionais	Evento **pode** ocorrer em algum momento	Evento **deve** ocorrer em algum momento	Evento provavelmente ocorra na maioria das circunstâncias	Evento esperado que ocorra na maioria das circunstâncias
Frequência Observada/Esperada	Muito baixa (< 10%)	Baixa (>=10% <= 30%)	Média (>30% <= 50%)	Alta (>50% <= 90%)	Muito alta (>90%)
Peso	1	2	3	4	5

ANEXO VII - GUIA DE IDENTIFICAÇÃO DE RISCOS



ANEXO VIII – MATRIZ DE RISCOS (MAPA DE CALOR)



ANEXO IX – PLANO DE AÇÃO PARA TRATAMENTO DO RISCO (PE, PA e CV)

Programas (Objetivo Estratégico[OE] / Objetivo de Plano de Ação[PA]); Processo (Cadeia de Valor):										
O Que?	*Por Que?*		*Onde?*	*Quem?*	*Como?*		*Quando?*		*Quanto?*	*Status*
Controle Proposto / Ação Proposta	Seleção: Função/Objetivo		Área de	Responsável pela	Execução da	Intervenientes	Data do	Data do	Custo	Posição da
Descrição	Tipo	Objetivos/Benefícios	Implementação	Implementação	Implementação		Início	Fim	Qualitativo	Implementação

LEGENDA:

	Tipo	Objetivo do(a)
Controle Interno Proposto	**MA**	Manual de Atribuições (Funcionais)
Controle Interno Proposto	**CV**	Cadeia de Valor (Fundamentais)
Ação Proposta de Controle	**EI**	Excepcionais (Inéditos)

Interveniente: Que intervém, que participa

Custo Qualitativo: Alto (Recurso do Plano Financeiro), Médio (Recurso de Processo transversal de cooperação), Baixo (Recurso Local e Operacional)

Obs: Funções se assemelham a Objetivos

ANEXO X - TABELA DE RESPOSTA A RISCOS

Tipo de Resposta	Ação
Evitar	Decisão informada de não se envolver, ou retirar-se de uma atividade, a fim de não ser exposto a um risco específico.
Mitigar	Resposta ao risco indicada para reduzir o nível de risco por meio da introdução de controles.
Compartilhar/transferir	Forma de tratamento de riscos que envolve a distribuição acordada de riscos com outras partes.
Aceitar	Decisão consciente de assumir um risco específico.

ANEXO XI - TABELA DE CLASSIFICAÇÃO DO NÍVEL DE RISCO

Escala de Nível de Risco	
Níveis	**Pontuação**
RC - Risco Crítico	15 a 25
RA - Risco Alto	**8 a 12**
RM - Risco Moderado	4 a 6
RP - Risco Pequeno	1 a 3

ANEXO XII - MODELO DAS TRÊS LINHAS

ANEXO XIII - CICLO PDCA

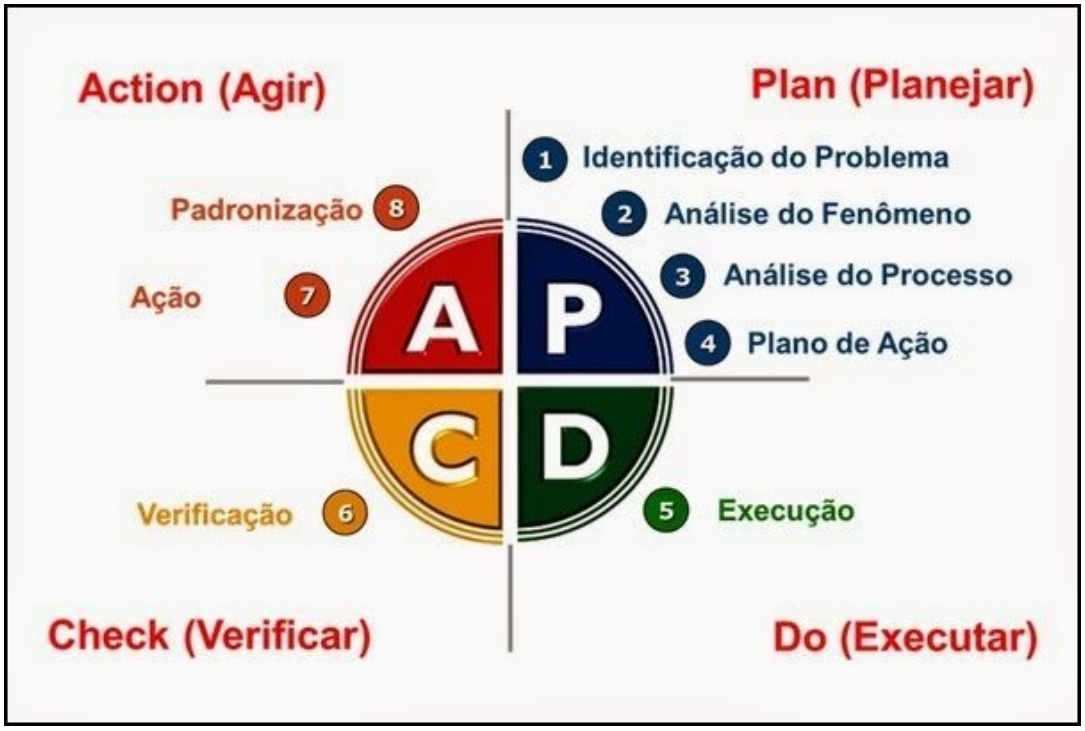


Figura 1 - PDCA

Fonte: https://blog.luz.vc/como-fazer/como-usar-o-ciclo-pdca-para-melhorar-a-sua-gestao-financeira/

Assinado digitalmente por:

Isabel Luiza Rafael Machado dos Santos (Aprovador)
Rogerio Lineu Arita (Chancelador)
Marcelo Lindoso Baumann das Neves (Elaborador)