MISSÃO

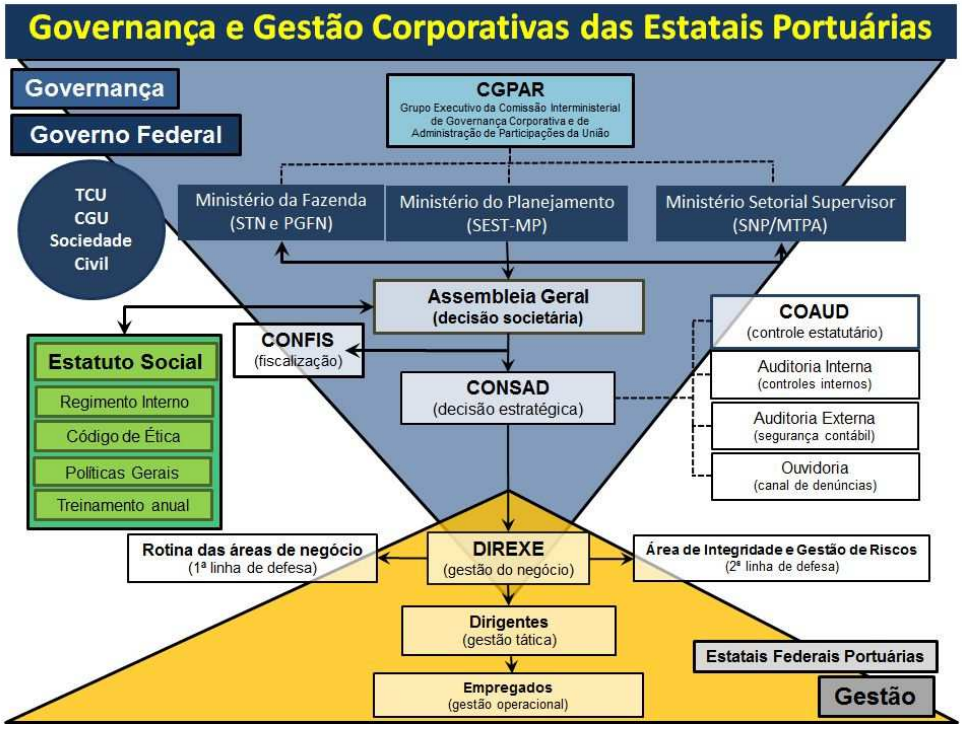
A Companhia Docas do Ceará, nos termos do seu Programa de Gerenciamento de Risco, tem a missão de gerir os riscos das suas atividades de Autoridade Portuária do Porto de Fortaleza, tendo como premissa a eliminação e/ou mitigação dos eventos de riscos, garantindo os resultados da sua eficácia administrativa e operacional, com adoção de práticas de gestão de risco adequadas à natureza e às especificações das suas competências necessárias aos padrões de controle considerando aos índices adotados nas administrações públicas do Brasil.

POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS

A Companhia Docas do Ceará, por meio desta Política de Gestão de Riscos e Controles Internos, tem o compromisso de assegurar que os eventos de riscos inerentes às suas atividades administrativas e operacionais sejam identificados, avaliados, tratados, monitorados e comunicados à Administração em tempo adequado para tomada de decisões, minimizando o impacto do risco e/ou explorando melhor as oportunidades, através de seus controles internos e adequada a sua governança de riscos, a fim de alinhar o nível de exposição aos riscos com as diretrizes da CDC.

JUSTIFICATIVA

A estrutura de governança e gestão corporativas das empresas estatais portuárias, representada pelo diagrama da Figura 1, demanda a subordinação desta empresa estatal às diretrizes e políticas públicas do governo federal voltadas às modernas práticas gestão.



Fonte: Elaboração SEST, adaptação CGU.

Portanto, em atendimento à política de governança instituída pela Instrução Normativa Conjunta Nº 1, da Controladoria Geral da União - CGU e do Ministério do Planejamento, Desenvolvimento e Gestão - MP, de 10 de maio de 2016, pela Lei nº 13.303, de 30 de junho de 2016 e pelo Decreto nº 8.945, de 27 de dezembro de 2016, fica instituída a Política de Gestão de Riscos que tem por finalidade estabelecer os princípios, diretrizes e responsabilidades, fazendo parte de um conjunto de instrumentos de governança e de gestão, que suportam a concepção, implantação e melhoria.

Adicionalmente, foi considerado neste texto as considerações e orientações constantes no Referencial Básico de Combate à Fraude e Corrupção, do Tribunal de Contas da União – TCU, que compila o conhecimento prático que vem sendo aplicadas por organizações públicas e privadas, dentro e fora do Brasil, no combate à fraude e corrupção, como objetivo estratégico a ser implantado na empresa, que passará a fazer parte da política da empresa.

Além da política de governança, no sentido de formatar o desenvolvimento deste material foram empregadas as normas e referências a seguir discriminadas:

CONCEITOS

Para fins desta Política de Gestão de Riscos e Controles Internos considera-se:

I. **Accountability:** conjunto de procedimentos adotados pelas organizações públicas e pelos indivíduos que as integram que evidenciam sua responsabilidade por decisões tomadas e ações implementadas, incluindo a salvaguarda de recursos públicos, a imparcialidade e o desempenho das organizações;

II. **Apetite a risco**: nível de risco que uma organização está disposta a aceitar;

III. **Compliance:** designação utilizada na prevenção e detecção de falta de conformidade com leis e regulamentações nacionais e estrangeiras, que possam ser cometidas pela administração, empregados e parceiros de negócios da Companhia;

IV. **Gerenciamento de riscos:** processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização;

V. **Governança:** compreende a essência dos mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução da política corporativa e à prestação de serviços da CDC em combinação com os processos e estruturas implantadas com o intuito de alcançar suas metas e os seus objetivos;

VI. **Linhas de defesa:** nível de interação das responsabilidades no gerenciamento de riscos e fortalecimento da governança dentro da CDC. A primeira linha é representada pelos gestores das áreas, responsáveis diretos pela execução de seus processos e respectivos riscos. A segunda é a área do Comitê de Gestão de Risco e Controles

Internos, que atua na identificação de falhas de performance de controles e de identificação de desvios de políticas e procedimentos internos, e a terceira é a área da Coordenadoria de Auditoria Interna, que atua na realização de testes substantivos de controles internos e identificação de desvios operacionais e financeiros decorrentes de falhas e/ou riscos nos processos;

VII. **Política de gestão de riscos:** declaração das intenções e diretrizes gerais da CDC relacionadas à gestão de riscos;

VIII. **Risco**: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade;

IX. **Risco inerente:** risco a que a CDC está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

X. **Risco residual:** risco a que a CDC está exposta após a implementação de ações gerenciais para o tratamento do risco;

XI. **Controles internos da gestão:** conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de empregados da CDC, destinados a enfrentar os riscos e fornecer segurança razoável na consecução dos seguintes objetivos gerais a serão alcançados:

   i. Execução ordenada, ética, econômica, eficiente e eficaz das metas;
   ii. Cumprimento das obrigações de *accountability*;
   iii. Cumprimento das leis e regulamentos aplicáveis;
   iv. Salvaguarda dos recursos para evitar perdas, mau uso e danos pessoais, patrimoniais e ambientais.

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Seção I

Da finalidade e abrangência

Art. 1º A Política de Gestão de Riscos e Controles Internos da CDC tem por finalidade estabelecer os princípios, diretrizes e responsabilidades mínimas a serem observados e seguidos para a gestão de integridade, de riscos e de controles internos do plano estratégico, programas, projetos e processos da CDC.

Art. 2º A Política de Gestão de Riscos e Controles Internos da CDC e suas eventuais normas complementares, metodologias, manuais e procedimentos aplicam-se a todos os níveis de gestão da CDC, abrangendo as diretorias, coordenadorias e prestadores de serviço, estagiários, consultores externos e quem, de alguma forma, desempenhe atividades na CDC.

Seção II

Das definições

Art. 3º Para fins desta Política de Gestão de Risco e Controles, considera-se risco a possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento das Metas e objetivos da CDC. O risco é medido em termos de impacto e de probabilidade.

CAPÍTULO II

DOS PRINCÍPIOS, OBJETIVOS E DIRETRIZES.

Seção I

Dos princípios

Art. 4º São princípios da Política de Gestão de Riscos e Controles Internos a serem seguidos pela CDC:

I - liderança, integridade, responsabilidade, compromisso, transparência,

complaince e accountability;

II - a gestão de riscos realizada de forma sistemática, estruturada e oportuna, competindo à alta administração a supervisão do desenvolvimento e do desempenho dos controles internos da gestão, respeitados os objetivos da empresa e o interesse público;

III - níveis de exposição a riscos adequadamente pré-definidos;

IV - procedimentos de controle interno proporcionais ao risco, destinados a agregar valor à organização, observado a relação custo-benefício;

V - mapeamento dos processos internos de modo a identificar as vulnerabilidades que impactam as metas e os objetivos da CDC, de forma que sejam adequadamente identificados os riscos a serem eliminados ou mitigados e, consequentemente, servindo de ferramenta gerencial para a tomada de decisões, no aperfeiçoamento do planejamento estratégico da CDC e na melhoria contínua dos processos organizacionais;

VI - utilização do modelo de governança, envolvendo a gestão de riscos, e controles internos para apoio à melhoria contínua dos processos organizacionais;

VII - atuação da gestão de riscos e controles internos de forma dinâmica e formalizada por meio de metodologias e normas adequadas, e quando convenientes manuais e procedimentos;

VIII - capacitação continuada dos empregados na gestão de riscos e controles internos, em todos os níveis da organização;

IX - identificação e tratamento dos riscos de forma descentralizada, com responsabilização dos gestores de cada área, envolvendo os processos e atividades que lhes são afetos;

X - coerência e harmonização da estrutura de competências e responsabilidades de todos os níveis de gestão da CDC, com a clara definição dos responsáveis pelos controles internos da gestão;

XI - disseminação de informações necessárias ao fortalecimento da cultura de gestão de riscos e controles internos;

XII - coordenação centralizada da alocação de recursos e definição de

políticas;

XIII - realização de avaliações periódicas para verificar a eficácia da gestão de integridade, riscos e dos controles internos da gestão, comunicando o resultado aos responsáveis pela adoção de ações corretivas, inclusive a alta administração;

XIV - adequado suporte de tecnologia da informação para apoiar os processos de integridade, riscos e a implementação dos controles internos da gestão;

XV - compromisso da alta administração de atrair, desenvolver e reter pessoas com competências técnicas, em alinhamento com os objetivos institucionais;

XVI - identificação e avaliação das mudanças internas e externas à CDC que possam afetar significativamente os controles internos da gestão.

§ 1º Para uma efetiva gestão de riscos e controles internos, os princípios devem ser aplicados de forma integrada, como um processo, e não apenas individualmente, sendo compreendidos por todos na organização.

§ 2º Os gestores e demais agentes da governança institucional da CDC devem contribuir para aumentar a confiança na forma como são geridos os recursos colocados à sua disposição, reduzindo a incerteza dos membros da sociedade.

§ 3º A identificação dos riscos será feita pelo nível hierárquico mais próximo de sua ocorrência.

§ 4º A Política de Gestão de Riscos, Governança e Controles Internos da CDC tem como premissa o alinhamento ao Plano Estratégico da CDC.

Seção II

Dos objetivos

Art. 5º São objetivos da Gestão de Riscos e Controles Internos da CDC:

I - apoiar a missão e a sustentabilidade institucional, pela garantia

razoável de alcance dos objetivos estratégicos através da redução dos riscos a níveis aceitáveis;

II - proporcionar a eficiência, a eficácia e a efetividade operacional, mediante execução ordenada, ética e econômica dos processos de trabalho;

III - produzir informações íntegras e confiáveis à tomada de decisões, ao cumprimento de obrigações de transparência e à prestação de contas;

IV - prover acesso tempestivo, aos responsáveis pela tomada de decisão, de informações suficientes quanto aos riscos envolvidos, inclusive para determinar questões relativas à delegação;

V - assegurar a conformidade com as leis e regulamentos aplicáveis;

VI - salvaguardar e proteger bens, ativos e recursos públicos contra desperdício, perda, mau uso, dano, utilização não autorizada ou apropriação indevida;

VII - agregar valor por meio da melhoria dos processos de tomada de decisão e de tratamento adequado dos riscos e seus impactos decorrentes de sua materialização.

Seção III

Das diretrizes

Art. 6º São Diretrizes da Gestão de Riscos e Controles Internos da CDC:

I - estruturar a gestão de riscos da CDC com base nas premissas da metodologia do *Committee of Sponsoring Organizations of the Treadway Commission - COSO*, ISO 31000 e de boas práticas;

II - basear as decisões de gestão de riscos no autoconhecimento e diagnóstico de vulnerabilidades;

III - prover os cargos de direção a partir da identificação de perfis e capacitação adequada;

IV - desenvolver e implementar atividades de controle da gestão que considere a avaliação de mudanças, internas e externas, que contribuam

para identificação e avaliação de vulnerabilidades que impactam os objetivos institucionais;

V - capacitar os gestores e demais empregados na gestão de riscos e controles internos, em todos os níveis da organização, de forma planejada e continuada;

VI - estabelecer procedimentos de controle interno proporcionais ao risco, destinados a agregar valor à organização, observada a relação custo-benefício;

VII - incorporar aos contratos de serviço de terceiros firmados pela CDC a dimensão da Política expressa nesta política.

CAPÍTULO III

DA ESTRUTURA DA POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS

Seção I

Do modelo da Gestão de Riscos e Controles Internos

Art. 7º A operacionalização da Gestão de Riscos e Controles Internos será descrita pelo Gerenciamento de Riscos, que contemplará, no mínimo, as seguintes etapas:

I - entendimento do contexto: etapa em que são identificados os objetivos relacionados ao processo organizacional e definidos os contextos externo e interno a serem levados em consideração ao gerenciar riscos;

II - identificação de riscos: etapa em que são identificados possíveis riscos para objetivos associados aos processos organizacionais;

III - análise de riscos: etapa em que são identificadas as possíveis causas e consequências do risco;

IV - avaliação de riscos: etapa em que são estimados os níveis dos riscos identificados;

V - priorização de riscos: etapa em que são definidos quais riscos terão suas respostas priorizadas, levando em consideração os níveis calculados na etapa anterior;

VI - definição de respostas aos riscos: etapa em que são definidas as respostas aos riscos, de forma a adequar seus níveis ao apetite estabelecido para os processos organizacionais, além da escolha das medidas de controle associadas a essas respostas;

VII - atividades de controles internos: são as políticas e os procedimentos estabelecidos e executados para mitigar os riscos que a organização tenha optado por tratar. Também denominadas de procedimentos de controle, devem estar distribuídas por toda a organização, em todos os níveis e em todas as funções. Incluem uma gama de controles internos da gestão preventivos e detectivos, bem como a preparação prévia de planos de contingência e resposta à materialização dos riscos;

VIII - informação e comunicação: informações relevantes devem ser identificadas, coletadas e comunicadas, a tempo de permitir que as pessoas cumpram suas responsabilidades, não apenas com dados produzidos internamente, mas, também, com informações sobre eventos, atividades e conexões externas, que possibilitem o gerenciamento de riscos e a tomada de decisão. A comunicação das informações produzidas deve atingir todos os níveis, por meio de canais claros e abertos que permitam que a informação flua em todos os sentidos, de modo que todos os servidores recebam mensagem clara da alta administração sobre as responsabilidades de cada agente. A CDC deve comunicar as informações necessárias ao alcance dos seus objetivos para todas as partes interessadas;

IX - monitoramento: tem como objetivo avaliar a qualidade da gestão de riscos e dos controles internos da gestão, por meio de atividades gerenciais contínuas e/ou avaliações independentes, buscando assegurar que estes funcionem como previsto e que sejam modificados apropriadamente, de acordo com mudanças nas condições que alterem o nível de exposição a riscos, podendo ser:

a) de natureza contínua da organização: inclui a administração e as atividades de supervisão e outras ações que os servidores executam ao cumprir suas responsabilidades;

b) avaliações específicas: são realizadas com base em métodos e procedimentos predefinidos, cuja abrangência e frequência dependerão da avaliação de risco e da eficácia dos procedimentos de monitoramento contínuo.

§ 1º Os gestores de risco são os responsáveis pela avaliação dos riscos no âmbito das unidades, processos e atividades que lhes são afetos. A instância superior da governança de gestão de riscos da CDC deve avaliar os riscos no âmbito da organização, desenvolvendo uma visão de riscos de forma consolidada.

§ 2º O Gerenciamento de Gestão de Riscos contemplará critérios predefinidos de avaliação.

Art. 8º Na priorização da implantação da Gestão de Riscos e Controles Internos serão considerados, em especial:

I - os projetos e ações de desdobramento dos objetivos estratégicos da CDC;

II – a integridade, rastreabilidade, disponibilidade e da segurança das informações, em particular as de acesso restrito, e patrimonial, com ênfase na prevenção de riscos do trabalho;

III - a conformidade dos processos administrativos e operacionais.

Art. 9º A revisão ou atualização do Plano de Riscos ocorrerá articulada com Planejamento Estratégico da CDC, bem como com o Plano de Auditoria Interna Anual.

Seção II

Das instâncias, competências e responsabilidades da governança de gestão de riscos.

Art. 10 São instâncias da Governança de Riscos na CDC em que se possibilita a adequada sinergia entre as áreas:

I – Conselho de Administração e Alta Administração (Diretor-Presidente e demais Diretorias)

II- o Comitê de Gestão de Risco;

II - os Gestores de Risco; e

III - os empregados.

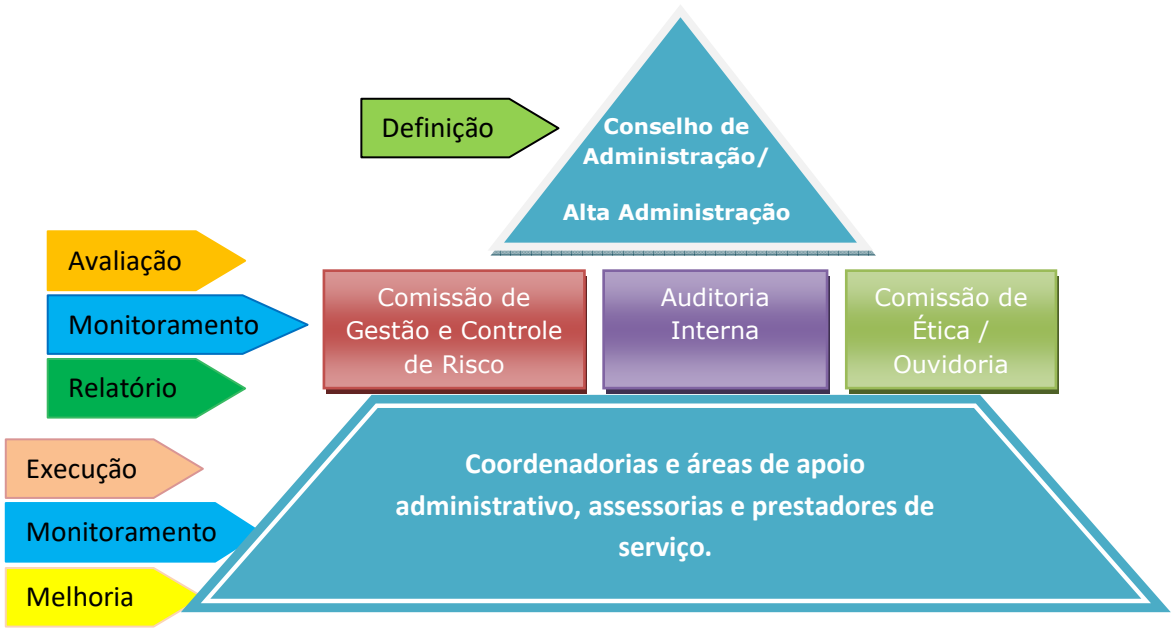


Figura 2 - instâncias, competências e responsabilidades da gestão de riscos e controles internos.

Art. 11 Fica instituído o Comitê de Gestão de Riscos, conforme Portaria nº Portaria nº0029/2017, com prazo de vigência até maio/2018 com as seguintes competências:

I - promover práticas e princípios de conduta e padrões de comportamentos éticos;

II - institucionalizar as estruturas adequadas de gestão de riscos e controles internos;

III - promover o desenvolvimento contínuo dos gestores de riscos e demais empregados e incentivar a adoção de boas práticas de gestão de riscos e de controles internos;

IV - garantir a aderência às regulamentações, leis, códigos, normas e padrões, com vistas à condução das políticas e à prestação de serviços de interesse público;

V - promover a integração dos empregados na gestão de riscos e pelos controles internos;

VI - promover a adoção de práticas que institucionalizem a responsabilidade dos gestores na prestação de contas, na transparência e na efetividade das informações;

VII – elaborar a política, diretrizes, metodologias e mecanismos para comunicação e institucionalização da gestão de riscos e dos controles internos;

VIII - supervisionar o mapeamento e avaliação dos riscos potenciais que podem comprometer a prestação dos serviços da CDC;

IX - liderar e supervisionar a institucionalização da gestão de riscos e dos controles internos, oferecendo suporte necessário para sua efetiva implementação na CDC;

X – propor a Alta Administração os limites de exposição a riscos considerando o Apetite de Risco da CDC;

XI – propor e supervisionar o método de priorização de temas e macroprocessos para gerenciamento de riscos e implementação dos controles internos da gestão;

XII - emitir recomendação para o aprimoramento da gestão de riscos e dos controles internos;

XIII – solicitar o apoio institucional da Alta Administração para promover a Gestão de Riscos, em especial os seus recursos, o relacionamento entre as partes interessadas e o desenvolvimento contínuo dos empregados; e

XIV - monitorar as recomendações e orientações deliberadas pelo Comitê de Gestão.

XV - desenvolver/ajustar metodologias de gestão de risco adequadas à CDC;

XVI - propor orçamento e demandar treinamentos e outros recursos para gestão dos riscos;

XVII - coordenar as ações dos gestores de risco;

XVIII - promover a disseminação do conhecimento gestão de riscos;

XIX- monitorar a eficácia da gestão de riscos para fins de promover o aprimoramento, a aprendizagem e melhorias;

XX - elaborar e manter atualizado documento identificando o contexto da gestão de risco na CDC; e

XXI – propor os critérios e indicadores a serem usados na avaliação da gestão de risco em cada processo;

XXII- coordenar a avaliação da política de gestão de riscos.

Parágrafo único – O Comitê de Gestão de Risco reunir-se-á no mínimo semestralmente, para avaliação das ações em execução e deliberação quanto à necessidade e a viabilidade de implementação de novas ações.

Art. 12 O Comitê de Gestão de Riscos e Controles da CDC ficará composto pelos seguintes membros:

I - Presidente da CDC, que o presidirá;

II – demais membros definidos na Portaria nº nº0029/2017:

§ 1º No exercício de suas funções, o Comitê será apoiado pela Coordenadoria de Auditoria Interna.

§ 2º Em caso de afastamento ou impedimento legal de algum de seus representantes, as atividades inerentes ao Comitê de Gestão de Risco serão desempenhadas pelo substituto designado.

Art. 13 A Alta Administração da CDC ficará com a responsabilidade de acompanhar a implantação e implementação desta política.

Art. 14 São competências da Alta Administração da CDC:

I - aprovar o plano de gestão de riscos, incluindo a definição, priorização e limites do Apetite de Risco à exposição ao risco, bem como as estratégias para evitá-los.

II - aprovar os critérios e indicadores a serem usados na avaliação da gestão de risco em cada processo;

III – aprovar o orçamento proposto pelo Comitê de Risco e os treinamentos e demais recursos para gestão dos riscos;

VI - acompanhar as ações do Comitê de Gestão de Riscos e Controles Internos;

VIII – apreciar os resultados da avaliação da política de gestão de riscos.

Art. 15 A participação dos membros no Comitê de Gestão de Risco, a qualquer tempo, será considerada serviço de natureza relevante e não ensejará qualquer tipo de remuneração.

Art. 16 Cada risco mapeado e avaliado deve estar associado a um gestor de risco formalmente identificado.

§ 1º Gestor de risco é o detentor de cargo ou função de chefia, institucionalmente definido na estrutura organizacional da CDC, como responsável por um ou mais processos de trabalho.

§ 2º São responsabilidades do gestor de risco:

I - assegurar que o risco inerente ou residual seja gerenciado de acordo com a política de gestão de riscos;

II - monitorar o risco inerente ou residual ao longo do tempo, de

modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com a política de gestão de riscos; e

III - garantir que as informações adequadas sobre o risco inerente ou residual estejam disponíveis em todos os níveis da organização.

Art. 17 Cabem aos empregados, no âmbito da execução de suas tarefas, a responsabilidade pela operacionalização dos controles internos da gestão e pela identificação e comunicação de possíveis riscos aos Gestores de Risco.

Art. 18 O Diretor-Presidente da CDC é o principal responsável pelo estabelecimento da estratégia da organização e da estrutura de gerenciamento de riscos, incluindo o estabelecimento, a manutenção, o monitoramento e o aperfeiçoamento dos controles internos da gestão.

CAPÍTULO IV

Dos instrumentos

Art. 19 São instrumentos do Programa de Gestão de Riscos e Controles da CDC:

I – os Gestores de Risco de cada coordenadoria da CDC;

II – o plano de riscos;

III - a capacitação planejada e continuada;

IV - as normas, os manuais e os procedimentos; e

V - a solução de tecnologia de informação e demais recursos necessários a implantação e implementação da Gestão de Risco e Controles Internos da CDC.

VI - a legislação vigente, bem como, no que couber, em padrões, técnicas e conceitos reconhecidamente adotados pelos órgãos de controle.

Art. 20. Esta política encontra sua fundamentação na legislação vigente, bem como, no que couber, em padrões, técnicas e conceitos reconhecidamente adotados pelos órgãos de controle:

a) Instrução Normativa Conjunta CGU e Ministério do Planejamento nº 01/2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal;

b) Resoluções da Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR), números 10 a 18, de 10/05/2016;

c) Lei 12.846/2013, de 01/08/2013, que dispõe sobre a responsabilidade administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública;

d) Decreto 8.420/2015, de 18/03/2015, que regulamenta a Lei 12.846/2013;

e) Lei 13.303, de 30/06/2016, 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;

f) Decreto 8.945/2016, de 27/12/2016, que regulamenta a Lei 13.303/2016;

g) Normas ABNT (Associação Brasileira de Normas Técnicas) ISO 9001:2015, 31000:2012;

h) COSO (Committee of Sponsoring Organizations of the Treadway Commission).

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

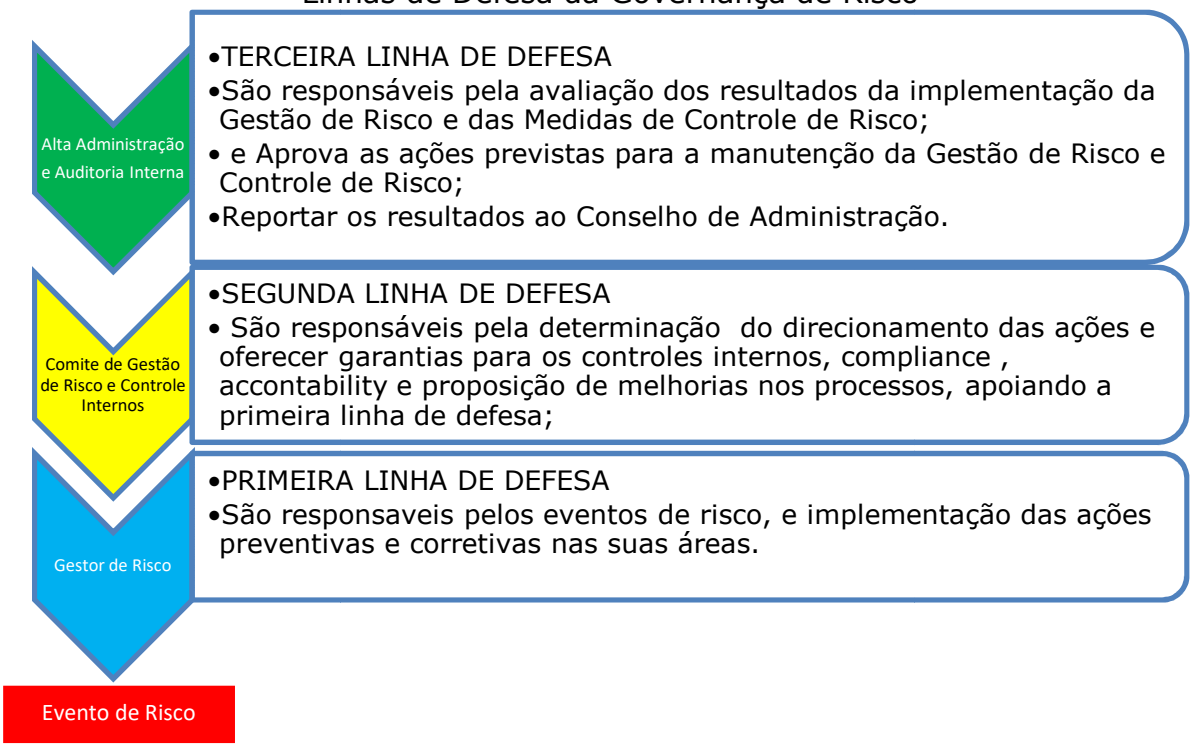
Art. 20 A metodologia de Gerenciamento de Riscos será elaborada pelo Comitê de Gestão de Risco e Controles Internos e será aprovada pela Alta Administração da CDC, no prazo de 180 dias, contados da apresentação do Plano de Riscos.

Art. 21 Os casos omissos ou excepcionalidades serão solucionados pelo Comitê de Gestão de Risco e Controles Internos da CDC.

Art. 22 A aprovação do Plano de Riscos ocorrerá em até 360 dias após a aprovação da metodologia.

ANEXO 1

Linhas de Defesa da Governança de Risco



ANEXO 2

METODOLOGIA DE GERENCIAMENTO DE RISCO

1. A Gestão de Risco está incorporada em todas as áreas da CDC, e é de responsabilidade de todos os empregados o cumprimento dos procedimentos definidos nesta Política de Gestão de Risco. Outros empregados específicos podem ter responsabilidades explícitas na Gestão de Riscos, sendo de responsabilidade de todos os empregados da CDC, tornarem atores proativos na Gestão de Riscos.
2. O Procedimento de Gestão de Risco é uma ferramenta de detalhamento do processo para a identificação, análise, tratamento, monitoramento e comunicação dos riscos. Isso inclui os procedimentos básicos em gerenciamento de risco, bem como o estabelecimento de registro de risco, de modo a assegurar a relação da CDC para com o risco identificado.

3. A Gestão de Risco envolve, também, os acidentes/incidentes do trabalho, segurança, saúde ocupacional e proteção ao meio ambiente, aos quais são cobertos por procedimentos definidos na Política de Meio Ambiente e Programas específicos da CDC.

4. Visão Geral

4.1 A Política de Gestão de Risco e os Procedimentos de Gestão de Risco da CDC estão alinhados as recomendações da Instrução Normativa MP/CGU nº01/2016.
4.2 Os riscos serão identificados, analisados, tratados, monitorados e relatados em uma base contínua, a níveis nomeados no âmbito das diretrizes acordadas pela Alta Administração com responsabilidades sobre o Planejamento e Desempenho Estratégico da CDC.

5. Ferramenta da Gestão de Risco

5.1. Modelo de Gestão de Risco
O Modelo de Gestão de Risco integra os Princípios da Gestão de Risco e o Processo de Gerenciamento de Risco. O processo de Gerenciamento de Risco consiste das seguintes etapas:

- Identificação do risco;
- Análise do risco;
- Tratamento do risco;
- Monitoramento; e

- Registro do risco.

5.2 Contextualização

Como parte do processo de gerenciamento de risco, é obrigação dos empregados usar o modelo de registro de risco da CDC, conforme anexo. Esse registro permitirá uma melhor visualização dos históricos dos tratamentos dados aos riscos identificados na CDC.

5.3 Identificação

Este processo consiste na identificação dos eventos de risco que podem impedir ou atrasar a realização das metas e objetivos estratégicos da CDC. Cada empregado designado nas áreas da CDC precisará delinear os seguintes itens para a consecução dessa etapa:

- **Evento de Risco** – fazer uma breve descrição do risco; e
- **Gestor do Risco** – é pessoa responsável pelo risco e, também, pela garantia que o risco é gerido de forma eficaz.
- **Apetite do Risco** - é a quantidade de riscos, no sentido mais amplo, que a Comissão de Gestão de Risco definirá na disposição limite em aceitar sua busca para agregar valor. O apetite do risco reflete toda a filosofia administrativa da empresa. Sendo de suma importância sua consideração na influência cultural e no estilo operacional a ser conduzido. A Comissão de Gestão de Risco deverá considerar qual a forma a ser adotada, sendo sua análise feita de forma qualitativa, categorizando-o como **ELEVADO, MODERADO OU BAIXO,** sendo cada um priorizado dentro das ações de cada Gestor de Risco.

Um evento de risco é um incidente ou uma ocorrência gerada com base em processos internos ou de demandas externas, que afeta a realização dos objetivos da CDC. Os eventos de risco podem causar impacto negativo, positivo ou ambos. No caso do evento de risco já ter ocorrido, o Gestor do Risco deverá utilizar a classificação do risco, para estabelecer sua classificação de consequências, e estabelecer a resposta ao risco apropriada com base na prioridade adequada. A tabela 1 indicará a classificação do risco.

O Gestor do Risco é o membro da área (coordenador, preferencialmente) designado da CDC à Comissão de Gestão de Risco, o qual terá como responsabilidade manter a Gestão do Risco dentro dos parâmetros exigidos.

Ao identificar os riscos, os empregados envolvidos na atividade ou processo serão incentivados a adotar procedimentos, de modo a oferecer total enfoque nos meios adequados, para mitigar os riscos de alto nível que possam impactar nas atividades da CDC.

5.4 Análise de Risco

Consiste em delinear as causas, impactos e tratamentos existentes, de modo a avaliar as consequências e a probabilidade do risco, para posterior determinação da sua classificação de risco. Atualmente, a Auditoria Interna da CDC desenvolve o Plano Anual de Auditoria Interna na qual são avaliados os riscos conforme preconizado na Matriz de Risco, e a partir dessa identificação, é elaborado o Plano Anual de Auditoria Interna, tendo seus resultados submetidos a apreciação da Alta Administração, bem como disponibilizado aos órgãos de controles externos.

Diante disso, a Comissão de Gestão de Risco, em conjunto com a Auditoria Interna e os Gestores dos Riscos das áreas envolvidas, deverão delinear uma revisão do Plano de Auditoria Interna com abrangência na Política de Gestão de Riscos e Controles Internos de modo a adequar a este novo contexto, sem prejuízo das atividades de auditoria interna já desenvolvidas, utilizando-se dos seguintes itens:

- **Causas** – origem do risco e/ou mecanismo de falhas que promoveram seu acontecimento;
- **Impactos** – quais as consequências ou resultados que a CDC possa esperar se resolver assumir o risco;
- **Tratamentos existentes** – tratamentos existentes na CDC que possam ser implementados, os quais podem ser políticas administrativas ou procedimentos gerenciais ou mesmo barreiras físicas, se for o caso;
- **Classificação da Probabilidade** – hipótese ou chances de ocorrer o risco;
- **Classificação das Consequências** – extensão na qual o risco poderá afetar a CDC, se este ocorrer;
- **Classificação do Risco** – produto da classificação da consequência e classificação da probabilidade, pela qual define a magnitude do risco.
- **Resposta ao Risco** – a medida que o risco for classificado com base na sua probabilidade e sua consequência, a resposta ao seu impacto deverá ser iniciada com o tratamento a ser definido pelo Gestor da Ação, e acompanhado pelo Gestor do Risco. O Gestor da Ação escolhe a resposta ao risco - evitando, aceitando, reduzindo ou compartilhando sua ação, desenvolvendo as medidas necessárias para serem

aplicadas ao risco, de modo a permitir o alinhamento do risco com a tolerância e com o apetite a risco definidos pela Comissão de Gestão de Risco.

- **Priorização da resposta ao risco** – a priorização será determinada com base na Classificação do Risco, já definida na tabela 1 (abaixo).

A priorização da resposta ao risco terá como fundamento as seguintes condições:

Evento de Riscos BAIXO é classificado entre os valores de 0,5 a 2 e serão tratados como prioridade 3;
Evento de Riscos MODERADO é classificado entre os valores de 5 a 30 e serão tratados como prioridade 2;
Evento de Riscos ELEVADO é classificado entre os valores de 50 a 500 e serão tratados como prioridade 1.

Com os tratamentos existentes ajustados a Gestão de Risco, a Comissão de Gestão de Risco usará a tabela 1 (abaixo) para determinar a classificação de risco identificado nas áreas.

A Comissão de Gestão de Risco precisará considerar a probabilidade de ocorrência do risco (variando de 'Rara' para 'quase certa') e a consequência se o risco é percebido (variando de 'Insignificante' para 'Catastrófica').

Tabela 1 – Tabela de Classificação de Risco

		Classificação da Consequência				
Classificação da Probabilidade		Insignificante	Menor	Moderada	Séria	Catastrófica
		1	3	10	30	100
Quase Certa	5	5	15	50	150	500
Provável	2	2	6	20	60	200
Média	1	1	3	10	30	100
Improvável	0,5	0,5	1,5	5	15	50
Rara	0,2	0,2	0,6	2	6	20

5.5 Tratamento

Consiste em implementar um tratamento atual e/ou futuro envolvendo medidas gerencias, a fim de prevenir e/ou mitigar o risco. A Comissão de Gestão de Risco precisará delinear, em conjunto com o Gestor do Risco da área envolvida, os seguintes requisitos:

- **Tratamento Atual** – tratamento imediato que irá corrigir e/ou mitigar a ocorrência do risco;

- **Tratamento Futuro** – tratamento específico que irá prevenir e/ou evitar e/ou mitigar a ocorrência do risco;
- **Gestor da Ação** – pessoa responsável, designado pelo Gestor do Risco da área, na qual o risco foi identificado para implementar o tratamento futuro; e
- **Resolução/Data de Revisão** – data prevista para solucionar ou revisar o tratamento dado a um risco;

Todo Pessoal deve identificar todos os tratamentos futuros que serão implementados, ou no curto prazo ou a longo prazo, para prevenir e/ou mitigar o evento de risco. Os tratamentos de risco devem ser proporcional ao indicativo da classificação de risco.

O Gestor da ação (fiscal do contrato/fiscal do projeto), em consulta com a Comissão de Gestão de Risco, é responsável por assegurar que o tratamento de risco seja aplicado em conformidade com a data de revisão/resolução. O risco deve ser reduzido ou minimizado, seguindo a continuação dos tratamentos existentes e a implementação de tratamentos futuros.

Após a implementação do tratamento, ele se tornará parte do processo gerencial ou tarefa habitual, e a partir desse ponto, deverá ser considerado um tratamento existente.

5.6 Monitoramento

Continuamente, deve-se avaliar e monitorar os riscos e os tratamentos dados com o objetivo de manter a eficácia, e adequação da gestão de riscos da CDC.

O Gestor do Risco, em consulta com os respectivos responsáveis, e apoio da Comissão de Gestão de Risco, deverão rever alguns pontos importantes na consolidação do processo, quais sejam;

- Evento de risco, causa e impacto;
- Classificação do risco, para garantir que ele é apropriado e;
- Tratamentos Existentes e Futuros, incluindo as datas de revisão e resolução, em ordem, para determinar se outros tratamentos ainda são necessários.
- Eficácia da medida, quando se determina que o gerenciamento de riscos é eficaz, a Comissão de Gestão de Risco terá a garantia razoável que: o risco foi mitigado ou reduzido de classificação, quando este não puder ser totalmente eliminado; atenderem aos objetivos administrativos e/ou operacionais que estão sendo alcançados; a comunicação por relatórios é confiável;e as leis e os regulamentos cabíveis estão sendo observados.

5.7 Relatório

A fim de permitir uma visão geral por parte da Alta Administração da CDC, a Comissão de Gestão de Risco deverá fornecer um relatório anual contendo as atualizações e resultados aferidos no período de implantação da Gestão de Risco, com o intuito de garantir que os riscos estão sendo avaliados e adequadamente gerenciados e tratados.

5.7.1 Relatório Resumido

Opcionalmente, a Comissão de Gestão de Risco poderá elaborar um Relatório Resumido para ser apresentado ao Conselho de Administração da CDC, de modo que esses resultados possam ser compilados ao Planejamento e Gestão Estratégica da CDC. O relatório de resumo fornecerá uma análise profunda dos riscos e identificará as áreas potenciais de preocupação para a CDC.

Caberá a Alta Administração da CDC, em conjunto com a Comissão de Gestão de Risco, determinar se os riscos identificados no período de controle (semestral ou anual) de fato, são riscos significativos para a CDC, e se devem ser ou não incluídos no registro.

6. Atribuições e Responsabilidades

5.1 A Comissão de Gestão de Risco é responsável pela revisão das práticas de gestão de risco da CDC. Isso inclui supervisionar o registro de risco das áreas envolvidas, e garantir que os riscos significativos para a CDC são relatados nos registros.

5.2 Os membros do Conselho de Administração da CDC são responsáveis pela Política de Gestão de Risco, incluindo a supervisão do desenvolvimento, monitoramento e revisão dos registros de riscos, considerando os seus impactos no Planejamento e Desempenho Estratégico da CDC.

7. Glossário de Termos

Termo	**Definição**
Gestor da Ação	Pessoa responsável pela implementação do tratamento futuro.
Causas	A origem do risco e/ou os mecanismo que geram a falha.
Classificação da Consequência	A extensão na qual o risco afetará a empresa, se este ocorrer.
Tratamentos Existentes	Os tratamentos existentes que estão em vigência , os quais podem incluir procedimentos gerenciais ou administrativos, ou

	barreiras físicas.
Tratamentos Futuros	Tratamento específico que podem prevenir e/ou mirigar um evento de risco.

8. Revisão deste Programa

Este Programa poderá ser revisado na medida em que novas normativas ou medidas de gerenciamento de risco sejam incorporadas, considerando os resultados alcançados ou por determinação da Alta Administração, bem como atender a recomendações dos órgãos de controles externos.

ANEXO 3

MAPEAMENTO DO PROCESSO

Nesse mapeamento, os processos de cada área são avaliados pelo nível de impacto que representam a empresa. As áreas deverão preencher as planilhas para permitir a visualização dos processos e seu nível de segurança quanto à prevenção dos riscos. A medida que estes riscos forem identificados, cada Gestor de Área, em conjunto com a Comissão de Gestão de Risco, definiram a Classificação do Risco e sua prioridade, a fim de estabelecer as Respostas ao Risco.

A metodologia é estabelecer o inventário de eventos por cada área, considerando os controles corporativos adotados, sendo estes relacionados aos controles (estratégicos, operacionais, comunicação e conformidade).

Conforme detalhado abaixo, seguem as definições:

1-Inventários de eventos

-Consiste em informar as situações potenciais comuns à atividade desenvolvida, os quais acontecendo ou não acontecendo, podem impactar diretamente nos processos gerenciados na área.

2- Controles Corporativos

Os eventos podem ser distribuídos em quatro pontos críticos nos controles corporativos:

a- **Estratégicos** (eventos que podem interferir nas metas gerenciais no nível mais elevado da CDC, os quais estão alinhados ao apoio da Missão da CDC).

Ex. Deixar de fazer balancete ou balanço anual da empresa, aplicação financeira em instituições com baixos juros, pagamento de taxas excessivas por movimentação financeira.

b- **Operacionais** (eventos que podem interferir na execução das metas gerenciais da área, sendo relativas à utilização eficaz e eficiente de recursos humanos e/ou de equipamentos/outros recursos envolvidos no processo)

Ex. Falta de conexão de rede, equipamentos obsoletos, pessoal com habilidades operacionais restritas por falta de treinamentos específicos a área;

c- **Comunicação** (eventos que podem interferir na execução das metas gerenciais da área, relativas à confiabilidade, integridade, rastreabilidade, disponibilidade, valor das informações utilizadas nos processos gerencias da área).

-Integridade – a informação é atual, completa e mantida por pessoas autorizadas.

-Disponibilidade - a informação está sempre disponível quando necessária ao pessoal autorizado.

-Confidencialidade – a informação só é acessada pelos indivíduos autorizados.

-Valor – a informação tem um alto valor para a organização.

-Rastreabilidade- a informação tem como ser mapeada da origem ao destino final.

Ex. relatórios imprecisos; falta de dados, prazo de entrega não atendido.

d- **Conformidade/Complaince** (eventos que podem interferir na execução das metas gerenciais da área, relativas ao não atendimento à legislação vigente/pertinente.

Ex. legislação atual não atendida no relatório gerencial da área, falta de informação

de legislação atualizada, prazo de atendimento legal não atendido, tempo de elaboração dos relatórios curto.

3- Processos Críticos

a)Entradas

Áreas	Informação	Forma de envio	Periodicidade de envio	NÍVEL DE CRITICIDADE DA INFORMAÇÃO RECEBIDA				
				Confiabilidade	Integridade	Rastreabilidade	Valor	Disponibilidade

Informar:

- quais áreas são responsáveis pelo envio dos dados necessários para a execução das ações gerenciais da área

-indicar forma de recebimento (por email, impresso)

-indicar periodicidade de recebimento (diário, mensal, anual);

-indicar nível de criticidade da Informação (confiabilidade, integridade, rastreabilidade, valor, disponibilidade), estabelecer grau mínimo, médio ou máximo para cada quesito;

Áreas	Nível de Controle do Evento			
	Estratégicos	Operacionais	Comunicação	Conformidade

-Indicar quais dos quatro pontos críticos se enquadram a informação da área:

b) Processo Gerencial

Qualificação do Pessoal	Nível de Atribuição (baixa, média, alta)	Treinamentos (Insuficiente, Parcial, Total, Reciclado)

Informar:

- indicar se o pessoal que se apropria da atividade tem treinamento suficiente para lidar com os níveis de responsabilidades dos eventos. Insuficiente=possui formação fora da área de atuação; Parcial =possui formação, mas necessita de treinamentos específicos; Total=possui formação e treinamentos específicos, mas não estão atualizados; Reciclado=possui formação, treinamentos específicos e reciclagem

atuais até 2 anos.

- indicar se recursos materiais são suficientes, adequados, ágeis para tratar os dados recebidos;

_____

c) Saídas

Áreas	Informação	Forma de envio	Nível de Eficácia	Periodicidade de envio	NÍVEL DE CRITICIDADE DA INFORMAÇÃO ENVIDA				
					Confiabilidade	Integridade	Rastreabilidade	Valor	Disponibilidade

Informar:

-indicar para quais as áreas são enviadas as informações tratadas;

-indicar a forma de envio;

-indicar periodicidade do envio (diária, mensal, anual);

-indicar nível de criticidade (confiabilidade, integridade, rastreabilidade, valor, disponibilidade), estabelecer grau mínimo, médio ou máximo para cada quesito enviado.

-indicar que nível de eficiência das informações passadas às áreas são recebidas (se há retrabalho por inconformidades: zero ocorrência (alta), 1 a 2 ocorrências (média) acima de 3 ocorrências no período (baixa)

Áreas	Nível de Controle do Evento			
	Estratégicos	Operacionais	Comunicação	Conformidade

-indicar quantas vezes ocorreram retrabalhos nos últimos 2 anos e de quais áreas (apontar quais eventos fora mais frequentes: Estratégicos, Operacionais, Comunicação ou Conformidade). Não necessita informar o problema específico, apenas a quantidade em relação com o evento.

4. Compatibilidade das Informações entre áreas.

Aqui, a informação processada em cada área será comparada com a informação gerada ou transmitida, e a medida que não houver compatibilidade entre os requisitos (Estratégicos, Operacionais, Comunicação e Conformidade), os gestores

farão uma alinhamento de dados para adequar os requisitos quanto aos elementos que não estejam dentro dos níveis que eliminem ou reduzam a sua Classificação de Risco.

5. Catalogação dos Eventos de Risco

Ao final do mapeamento do processo, cada Gestor de Área estabelecerá a relação de eventos de risco na sua área e a partir destes, definirá suas ações de resposta ao risco, considerando a Classificação do Risco e a sua prioridade.

Cada informação processada será classificada em dois critérios: Classificação de Probabilidade e da Consequência.

A Classificação de Probabilidade será definida segundo o grau de Ocorrência: quase certa, provável, média, improvável e rara.

A Classificação da Consequência será definida segundo o nível de consequência do risco: insignificante, menor, moderada, séria, catastrófica.

Área	Informação	Classificação de Probabilidade	Classificação da Consequência	Classificação do Risco
CODREH	DADOS INSS	1	30	Moderado
CODFIN	RECOLHIMENTO DE ISS	2	30	Elevado